Industrial Cybersecurity Technology & Solutions

BUYER'S GUIDE H1/2021

Industrial Cyber

TAKEPOINT RESEARCH

The State of the Industrial Cyber Market

Industrial cybersecurity is not for the faint-hearted or the 9-to-5 crowd. If you are looking for a steady pace and predictable work, cybersecurity is the wrong place. During the course of regular client work and in putting together this report, I had many conversations with top security personnel at several industrial enterprises. What struck me the most is how much these professionals care deeply about the security of their company and are driven by a sense of purpose – literally to make the world a safer place. While challenges still abound, our industry has taken great strides over the last 18 to 24 months. This is the time for industrial cybersecurity to perform and shine. Put on your hard hats and strap in.

COVID-19 Impact on Cybersecurity

The COVID-19 pandemic turned out to be a change catalyst that none of us anticipated. For many industrial enterprises, the pandemic changed the way they operate. Hastily constructed short-term workarounds have morphed into the long-term status quo for many businesses. The pandemic also had a big impact on our approach to cybersecurity and appetite for risk. Some of the changes precipitated by the pandemic are positive and needed. Others not so much. While initially slowing down initiatives, over the longer-term the pandemic response created a catalyst effect, which reinvigorated security projects that were already in the works. Ultimately, cybersecurity needs and the right solutions will shake out in the marketplace.

Market Maturity: from OT/ICS Cyber to Industrial Cybersecurity

Industrial enterprises – asset owners and operators – have made significant strides in cyber awareness and are starting to take a holistic approach to industrial cybersecurity. Our recent conversations with industrial enterprise CISOs and engineering security teams are strikingly more mature than about 12 to 18 months ago. We see the focus shifting. Instead of addressing vulnerabilities in isolation, companies are thinking strategically about how to identify, quantify, and prioritize the gamut of cyber risks they face, so they can implement the right solutions to secure the industrial enterprise from end-to-end.

We also see the chasm that normally separates departments and operating silos beginning to be bridged, as organizations seek to implement a comprehensive, risk-based approach to industrial cybersecurity.

The good news is that after a couple of years of stagnation, the post-pandemic cybersecurity market is more vibrant and mature. It has certainly evolved beyond the simple 'visibility of OT assets/networks' outlook that vendors were peddling until not too long ago. The market realizes the need of industrial enterprises to understand and justify the business value of cybersecurity just as they would with any other investment. Discussions started to revolve around the need to measure and reduce residual cyber risk. The market also recognizes that the tight integration between IT, OT, IoT, 5G, and other technology will be necessary to holistically secure industrial enterprises. Industrial CISOs are looking for solution vendors who can ease their integration burden.

Industrial asset owners and operators increasingly are turning to proactive 'security by design' strategies to reduce risk. Discussions within the organization, with vendors and integrators are exploring ways to eliminate vulnerabilities by building cybersecurity into all stages of product development and delivery. While the industrial sector is not homogeneous, industrial enterprises come in all shapes, sizes and levels of cyber maturity, the wheels are clearly moving towards a proactive, 'secure by design' approach to meeting the challenges of industrial cybersecurity.

Takepoint Research along with many others now refer to this market as 'Industrial Cyber' rather than OT/ICS Cyber, representing a fundamental shift in how the vendors, service providers, consultants and industrial enterprises who comprise this market, view the cybersecurity challenge. Only when we expand the definition of cybersecurity to encompass all threat vectors and risks to industrial enterprises can we truly impact business outcomes. This shift in thinking has eclipsed previous discussions about IT/OT convergence and collaboration solutions, making them passé.

Market Vendor Evolution

Network visibility and asset inventory are now just table stakes, as specialized products and services have emerged along with vertical-specific solutions from IoMT (Internet of Medical Things) to maritime cyber. We are entering a phase of prolific expansion both in terms of cyber awareness in the boardroom and in the rise of new technologies and startups to provide needed cybersecurity solutions.

Just a couple of years ago, players voiced concerns that once the pure-play OT/ICS cybersecurity vendors had all been acquired, the market would slow down or even shrink. This is hardly the case. The Industrial Cyber market is more vibrant and promising than ever.

Even in areas that are still underserved, such as L0/L1, we see a number of vendors offering innovative ways to solve old problems. There is a new and growing focus on a risk-based approach to cybersecurity, which in itself reflects the maturity of this market compared to just 24 months ago. Indeed, there are even startups out there that can help industrial enterprises and insurance companies measure the dollar-value of their residual risk!

The challenges of product security and supply chain security have been highlighted particularly by the SolarWinds cybersecurity incident, where the supply chain was hacked and a back door was inserted into the product. This kind of risk cannot be understated. Industrial asset owners and operators must be confident that vendors have done everything possible to secure the development, delivery and complete lifecycle of their products. The number of CVE security flaws published annually and the SolarWinds hack testifies to the prevalence of this risk, and the need for better adherence to standard and more innovative solutions.

New technologies around IIoT and cloud have great promise, but we must also be vigilant of the potential risk and have a suitable plan to identify and minimize it.

Services are key to solution adoption

Cyber solution vendors know that it can be tough to sell their products without providing some serious hand holding and even add-on services. Customer skills are often in short supply and resources are spread thin, so they look to the vendor to advise and guide them through deployment, installation, and integration. Many vendors realize the need to balance their technology offering with services provided directly to the customer or via a partner.

See the Industrial Cyber Services Guide

Market Specialization

One size does not fit all. We see a more diverse range of technologies and many more specialized solutions for industrial enterprises. Cyber awareness is growing and vendors are adapting.

As risk-based cybersecurity becomes more prevalent, we see cyber startups springing up to deal with everything from industrial supply chain security to cyber risk management. We also see sub-specialties. For example, within the Cyber Risk Management solutions, some vendors calculate the dollar value of an enterprise's inherent risk and residual risk specifically to help reinsurers provide better and fairer insurance policies.

Some vendors focus on a specific industry vertical, catering to the unique requirements of these market niches. Solutions for vertical 'microcosms' typically provide a mix of COTS hardware and software, as well as vertical-specific hardware (IT/OT/IIoT/other assets) and software. Transportation (rail, maritime and automotive) and healthcare (IoMT, connected care) are just two examples of cyber-vertical solutions. Many devices in these verticals would not be considered COTS IT appliances nor classical IoT devices. Hence the need for specialized cyber solutions.

Cybersecurity for Healthcare Verticals

Healthcare Delivery Organizations (HDOs) such as hospitals use very complex and specialized technologies, the likes of which are seen in few other places. Their technology environment comprises COTS hardware/software, OT asset and IoT devices – specifically Internet of Medical Things (IoMT). Medical devices from infusion pumps to MRI machines to dialysis machines are connected, often to the same flat network.

HDOs also manage private and highly sensitive patient data that must be accessible in varying degrees to medical staff, and are expected to provide public access to the internet for patients and visitors alike. In addition to medical systems, HDOs must manage and secure access to the 'smart building,' which among other things, includes elevators, patient rooms, operating rooms, labs and pharmacy, as well as building electrical, HVAC, and water systems.

The cyber risk to such an enterprise is an ever-present danger. Medical data alone has become a prime target for cybercriminals.

Specialized vendors include CyberMDX, Cynerio, Medigate.

Cybersecurity for Transportation Verticals

Automotive

Connected cars and autonomous vehicles are growing in popularity and presence on the road. Many CPUs and millions of lines of code are deployed throughout the vehicle's inter-connected subsystems. Internet connectivity makes the connected car a cyber target. Automotive Cybersecurity solutions tend to focus on in-vehicle protection, OTA security and fleet/cloud monitoring. OEM and Tier-1 suppliers are starting to act as more and more regulations are enacted.

Specialized cyber-automotive include: Aptiv; Argus (Continental); Arilou; GuardKnox; Harman; Karamba; Upstream.

Maritime

Today, ships have more than the stars to guide them thanks to OT/ICS/IT infrastructure on board and on shore. These critical systems are also internet connected, thereby making them vulnerable to cyberattacks. Specialized solutions safeguard the shipping environment from current and emerging cyber threats and vulnerabilities.

Specialized vendors for maritime include Cydome, Mission Secure, Neptune.

Rail

The emergence of the 'Digital Train' has made railway transportation more convenient and efficient for people and freight 'passengers' alike. Digital systems monitor, control, and manage rail signaling, train scheduling, train assets, rolling stock data, and much more. Cybersecurity is needed to detect both internal and external threats to highly regulated railways systems that carry people and valuable cargo over large geographical areas.

Rail specialized vendors include Cervello, Cylus.

Please note the vendors mentioned above are only for representative purposes, and are not designed to be an exhaustive list. See the Vendors Directory for more vendors and details.

Industrial Cyber Basics: What You Need to Know

Technology Concerns

Network Segmentation in the OT/ICS network is critical. Firewalls that are not purpose-built for OT are not up to the task. Many industrial enterprises are still lagging in network segmentation of business-critical processes.

Lack of system hardening: Many IT/OT devices and workstations implement minimal hardening measures, if any.

Weak access control in both the physical and digital sense due to insufficient management can undermine the security controls that have been set in place.

Insufficient levels of Identity Management: Too many industrial enterprises lack basic authentication, auditing, and enforcement procedures that govern access to physical and digital assets - particularly for third-party and remote access.

Insufficient logging and monitoring: Industrial systems should be monitored in real-time for anomalous behavior. System logs can also help with post-attack forensics.

OT/IIoT Device-level security (L0/1) has languished on the 'too complex and costly' list for far too long. Serious blind spots and opportunities for data injection and data manipulation arise when you can't verify that the data coming from devices or the sensors is reliable.

Vulnerabilities, Product Security and the Supply Chain: It should not take a SolarWinds incident to highlight the number of CVEs in industrial assets. Too many products are released with critical security vulnerabilities that can and should be addressed prior to release. There are plenty of standards. Just need to enforce adherence.

Industrial Cloud Security is a major concern for particular verticals, such as manufacturing and building management systems (BMS), where data is exported directly into cloud-based analytics platforms.

Business Concerns

Collaboration and Risk: Many stakeholders must come together to secure the industrial environment. Cybersecurity should be a company-wide pursuit driven by risk-vs-ROI considerations and the overall risk appetite of the company.

Weak Governance: Company-wide security policies, regular risk assessments and security planning are noted by their absence in industrial enterprises

Security awareness and training: Human error and unqualified personnel are still significant causes of security breaches. Employers must provide regular training or adopt specialized solutions to help staff change risk-prone behavior.

Third party management: Many site operations rely on external suppliers and integrators to service and manage OT/ICS/IIoT devices and equipment. In addition, many industrial enterprises have their employees working from home due to the COVID-19 pandemic. Secure remote access and oversight is critical.

Incident response planning: Too many companies are just putting out fires instead of following an incident response plan. The IR plan should detail and document the process for isolating the cause of an incident and restoring operations. Without an IR plan, the ability to reduce downtime, data loss, and reputation damage from an incident is hit or miss, especially if such action has to be done remotely.

This Guide

This edition of the Industrial Cybersecurity Solutions Buyers Guide is designed to steer you through the technology weeds, and get you to the cyber solutions that can meet industrial enterprise needs. The guide provides clear and concise explanations about the many cyber solutions available to protect your industrial enterprise from internal and external threats.

We categorize the industrial cyber solutions, explain why you may need them, and provide a detailed list of vendors. The information inside shows OT asset owners, operators, purchasers, suppliers and security teams the broad array of cyber tools and vendors that are poised to assist them in their quest to secure the industrial enterprise from end-to-end.

By answering some initial questions, this guide aims to help industrial enterprises make informed decisions about securing their industrial environment, and how to build or enhance a collaborative, risk-based, industrial cybersecurity management program.

Jonathon Gordon
Directing Analyst
Takepoint Research

Industrial Technology and Solutions – Categories

The categorization framework in this guide is designed to enable Industrial Enterprises to identify, evaluate and determine what type of technology and solution may be beneficial to their organization. The categories are designed to enable an elementary assessment of solutions, it is not an exhaustive checklist. The framework is not sequential, certain solutions may be required at different points in the journey, depending on the starting point and the cyber maturity of the organization.

Categories	Sub-categories
Cyber-Physical Security and Operational Systems Health	• OT device & signal integrity • Data Manipulation and Data Injection • Predictive maintenance
Deception and Honeypots	• OT/SCADA/IIoT deception • ICS Honeypots/Honeynets
Identity and Access Management (IAM)	• IAM - Policy and role management • ID governance • MFA, SSO & PAM
Industrial IoT (IIoT) Device Security	• Embedded IoT agent • IIoT Inventory — Hardware/Software • Continuous Vulnerability Management • Device Update
IT/OT Endpoint Security and Patch Management	• Industrial IT endpoint protection • IT endpoint protection (HMIs, workstations & others) • OT endpoint (PLCs, RTUs and others) • Patch Management • Configuration Management
Network Discovery, Monitoring and Threat Detection	• Network Anomaly & Threat Detection • Network Asset Discovery & Mapping • Automated network inventory • Monitor, alert & report
Perimeter Security and Network Segmentation	• Data diode/unidirectional gateways • Industrial Firewalls • USB/removable media sanitization
Product and Supply Chain Security	• SDLC security • Product Security • Live 3rd party risk assessment
Risk Management, Governance and Compliance	• Risk exposure analysis and reporting • Risk management • Exposure reduction — vulnerability prioritization
Secure Remote Access and Zero Trust	• Multi-vendor remote access platform • Access Control and Logging • Zero-trust access • VPN Access • WFH Cybersecurity
Social Engineering and Phishing Security	• Blocking threats — Phishing, Pretexting, etc. • Inbox Cybersecurity • Mail Gateways • CBT / Training platforms • ATO (Account Takeover)

CYBER-PHYSICAL SECURITY AND OPERATIONAL SYSTEMS HEALTH

Industrial asset owners and operators are learning that when cybersecurity monitoring is just one layer removed from the level where a system breach is being attempted, the attack (and successful breach) will go undetected for longer. The same is true for operational health. A misbehaving or drifting sensor may go undetected for a considerable period of time – until the sensor goes completely haywire or starts causing apparent damage. Solutions in this category address threats to OT system security and OT system health at the lowest layers of the Purdue model, i.e., Level 0 (Process) and Level 1 (Basic Control and Safety).

The common denominator in physical layer solutions is getting accurate DATA. Without complete and accurate data, enterprises can never be sure that their OT devices are behaving correctly and operating efficiently Therefore, these solutions focus on collecting and verifying 100% of OT device data, in order to provide accurate, real-time visibility and analysis of OT asset health and security status.

Operational Threats

When OT sensors and devices misbehave due to drift, mis-calibration, and other common mishaps, they send erroneous data that cannot be trusted. Bad sensor data not only skews critical real-time decisions of local OT controllers, it also affects management decisions regarding asset maintenance, replacement, refurbishment, etc. On both counts, the risk and cost to the enterprise is high.

Cybersecurity Threats

Cyberattacks on OT systems are often preceded by reconnaissance to determine the ideal time and place to inject sensor data, manipulate sensor data, tamper with sensor wiring, or attempt to replace a sensor altogether. Cyber reconnaissance and attack activity at L0/1 can only be quickly detected if complete monitoring of the sensor data is carried out, and the sensor knows what to look for.

Typical Solution Architecture

The typical architecture for OT system health and security solutions contains:

- Physical-layer agents to monitor the sensors/devices
- Central server to collect and analyze the data
- GUI dashboard to display meaningful data, insights, and alerts

Depending on the solution, the agent component will be either a software/firmware agent installed on the device itself, or a network-based agent (hardware or software) installed between sensor assets and the PLC. The agent form factor has a direct bearing on solution cost and ease of implementation.

Why your Industrial Enterprises needs this solution

- **Assure OT device data you can trust:** When analyzing 100% of sensor data, you get a complete and accurate picture of the true status and state of your OT process.
- **Gain predictive intelligence** (i.e., early warning) on sensors and assets that are showing signs of drift, mis-calibration and probable failure, so you can fix the problem preemptively. Predictive intelligence alone is saving industrial enterprises millions in yearly OPEX, as they avoid unexpected outages and other costly damages.

- **Get real-time threat intelligence:** Find out immediately when OT/IIoT devices or data are being tampered with or have been compromised and know precisely where to investigate, so you can thwart the malicious activity.

Recommendations

L0/L1 agent-based solutions have traditionally been complex and difficult/costly to deploy at scale. Select a vendor that can address these issues.

Sample Category Vendors

- Aperio Systems, IXDen, Mission Secure, Siga-OT.

DECEPTION AND HONEYPOTS

Honeypot, Honeynet and Deception technologies are designed to divert cybercriminals away from production networks by luring them into a trap. While hackers believe they are reconnoitering and breaching the real OT network of a smart factory or smart electricity grid, they are in fact accessing a 'fully functioning' digital twin of that network.

To the attacker, the digital twin (i.e., honeypot, honeynet) looks and acts like the real thing. Honeypots lure and trap attackers by mimicking the real system, including programmable logic controllers (PLCs), a human-machine interface (HMI), and other components of an industrial control system (ICS). A Honeynet is simply a network of multiple Honeypots. Honeynets may be deployed in the cloud or on premise.

As hackers make their way through a Honeypot, the SOC team gets an unimpeded look at the reconnaissance and attack methods of the cybercriminal. Honeypots often provide early warning of a real security breach and how it is likely to be implemented, enabling the SOC team to shore up cyber defenses and prepare a fast and efficient response.

In addition, Honeypots collect valuable cyberattack data (e.g., malware payload), giving industrial enterprises a better understanding of the different methods and strategies that bad actors use.

For example, Honeypots deployed in an industrial enterprise can reveal a wealth of valuable information, including how much of the breach traffic is automatic reconnaissance scanning (precursor to attack) versus live attack traffic. Honeypots also capture the target, time and frequency of attacks.

Typical Solution Architecture

Honeypots and Honeynets are deployed in the cloud – private or public.

Why your Industrial Enterprises needs this solution

- **Gain an automated cybersecurity resource** that is seamless to deploy and simple to operate. The honeypot doesn't require fancy algorithms, constant signature updates, and never runs out of space or connections. Once the honeypot is in place, you simply wait for someone to connect to it. Then the watching begins. Its simplicity makes the Honeypot a very reliable resource.
- **Capture unauthorized activity** so you (and management) can see the bad actors and the risk that they pose. As such, honeypots not only return their own value, but can be used to justify investment in other cyber tools.
- **Be better prepared** to counter cybercriminals as they try novel methods. Honeypots provide precise and easily understood information, enabling easier and faster reaction to threats.

Recommendations

Your industrial enterprise will need to have the necessary resources (internal or outsourced) to close the loop on this valuable resource and make it actionable. Be sure to have this resource in place prior to purchasing solutions in this category.

Sample Category Vendors

- BSS Unit, TXOne (Trend Micro), TrapX.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity and Access Management (IAM) comprises a framework of business processes, policies, and technologies for management of electronic and digital identities. IAM products provide capabilities that include single sign-on (SSO), multi-factor authentication, and privileged access management (PAM). These technologies help the security team control user access - both physical and digital – to information, assets and infrastructure in the industrial enterprise.

In addition, these technologies securely store user identity and profile data and allow the enterprise to establish data governance rules to control data sharing and assure that only necessary and relevant data is accessible. Many IAMs support access control based on the different roles in the organization, with each role receiving the access permissions that are relevant to it.

PAM is based on the 'least privilege' method, which restricts access rights and permissions to the absolute minimum required to perform routine and authorized activities. PAM permissions may be assigned to users, accounts, applications, systems, IoT devices and even compute processes. 'Least privilege' adds an effective layer of protection. For example, if a cybercriminal somehow obtains credentials to access an IoT device, he cannot go beyond the 'least privilege' permissions defined for that device.

With an IAM solution in place, all individuals and services across the industrial enterprise are authenticated, authorized, and audited according to a unified policy set by management.

IAM Issues in Industrial Enterprises

Industrial Control Systems (ICS) have a number of known security hurdles when it comes to IAM.

- **Overabundance of Admin Accounts:** The number of corporate and third-party users who actively access and extract data from ICS has jumped dramatically over the past several years. The security and operations teams are increasingly providing ICS access to remote users and third-party contractors.
- **Hard-Coded Credentials:** Industrial applications and devices often have hard-coded access credentials that are relatively easy to breach, which increases the risk of compromise and unauthorized access beyond the device itself and into the overall system.
- **Wide Use of Shared Accounts:** Industrial processes often use a single set of credentials to access applications and resources. Shared accounts may be used on servers, cloud platforms, services, and databases. Shared accounts tend to have simple passwords that do not change frequently and therefore are easy to hack. Also, specific activity cannot be traced to a specific user, either internal or external.

Why your Industrial Enterprises needs this solution

- **Simplify and automate the process** of identity management, access control and authorization with the level of granularity that is needed to protect industrial process networks from a breach.

- **Remove the 'worst-practices'** that have crept into these systems that make access easy and simplify lateral movement.
- Pedantic management of user identity and access privileges is absolutely essential to **reduce the risk** of internal and external data breaches, and to **assure compliance** with regulatory and audit requirements.

Recommendations

Make sure your IAM solution is experienced in Industrial Enterprise environments and has integration with the key applications and platforms in place.

Sample Category Vendors

- Alert Enterprise, CyberArk, Xage Security.

INDUSTRIAL IOT (IIOT) DEVICE SECURITY

This guide treats IIoT as a separate category from traditional OT/ICS assets due to their proliferation and wide range of functionality and purpose. IIoT is typified by 'smart' devices, which have made their way into numerous industrial environments including electricity, oil and gas, manufacturing, chemicals, pharmaceuticals, mining, and transportation. Unlike traditional OT/ICS assets, IIoT devices are designed to be connected to the internet and communicate over IP protocols.

Not only must industrial enterprises secure the communications between a smart device and its control center, they must secure the device itself from malicious hacking, manipulation and other forms of tampering. Solutions in this category are focused on device-level protection against cyberattack.

IIoT devices are an attractive attack vector for cybercriminals because these devices are often off-the-shelf products with minimal built-in security – and hundreds of thousands if not millions of them are already deployed. For cybercriminals who want to gain entry to networks and ICS systems that control important infrastructure and services, IIoT devices provide an expansive attack surface.

Endpoint Security-by-Design

Endpoint 'security by design' typically embeds a software agent in the device firmware so it can be secured throughout its deployed lifecycle. The embedded agent continuously monitors the IIoT device and communicates with a cybersecurity detection and prevention application in the industrial OT environment. Agents should be embedded prior to product release. Installing and testing agents on already-deployed devices can be prohibitive. Security by Design for IIoT endpoints also includes the following standard practices:

Endpoint Identity: IIoT devices should support standard and secure user authentication to control access to the device and its services.

Secure Boot: IIoT devices should follow Secure Boot protocol, which ensures the integrity of the code running on the device. Secure boot is a standard, and pretty basic security mechanism for any computerized (i.e., smart) device.

Cryptographic services: IIoT devices should encrypt/decrypt communications across transport protocols, storage and applications. Using weak or non-standard security mechanisms exposes IIoT device communications to the risk of being intercepted, modified and even injected with false data which can result in device hijacking and damage.

Why your Industrial Enterprises needs this solution

IIoT and smart endpoints are proliferating and need to be secured. Otherwise, you risk exposing the industrial enterprise to numerous, unprotected points of entry.

Why IIoT vendors needs this solution

Product security and secure development are critical components of IIoT device security. (See Category 9: Product and Supply Chain Security for additional details.)

Recommendations

For industrial enterprises: While the solutions in this category offer several methods for securing IIoT devices, Industrial enterprises would do well to perform a risk-threat analysis on each smart device to determine which of the following methods and industrial standards are applicable to each IIoT device.

Sample Category Vendors

- Armis, Cybeats, Karamba Security, Mocana, Vdoo.

IT/OT ENDPOINT SECURITY AND PATCH MANAGEMENT

Industrial environments have a wide range of endpoints that require protection from cyber threats – PLCs and RTUs, SCADA servers, application and database servers, manufacturing systems, data historians, human machine interface (HMI) systems, engineering workstations (Windows, Linux) and more.

Each IT/OT endpoint system has an operating system (OS) and configuration/setup files in addition to software applications and operational components unique to each endpoint. With increasing frequency, these endpoints are accessible via the internet. The sheer number, diversity, and proprietary nature of Industrial Enterprise endpoints makes their protection a daunting challenge.

Security threats to endpoints can result from human error, human tampering, generic malware, targeted malware (phishing) and sabotage.

Endpoint Security Solution

Endpoint security or endpoint protection solutions provide a centralized method for detecting and blocking unauthorized access and risky activities on the endpoint. Endpoint Security solutions typically provide:

- Whitelist: permits only pre-registered, approved applications and services to run, effectively limiting threats and having minimal to no impact on endpoint performance.
- Anti-Virus and Anti-Malware: with frequent trusted signature and engine updates
- Device authentication for removable media
- Host-based Firewall and Network Access Control, including
  - Access control on restricted ports and networks
  - Detection and blocking of network attacks launched from internal sources
  - Wi-Fi network control

Typical Solution Architecture

The typical architecture for Endpoint Security solutions contains:

- Security Server software: installed on a centrally managed server or gateway within the network
- Client software: installed on each endpoint device. Anti-virus protection, personal firewall and USB/removable media sanitization agents fall into this category (further addressed in Category 7 of this report, Perimeter Security and Network Segmentation)

Patch Management Solution

Software patches and updates are necessary to fix bugs, keep system features current and running smoothly, and assure that connected endpoints are protected against the latest hacking and malware threats. Once again, the sheer number and diversity of Industrial Enterprise endpoints makes the patch and update process a logistical nightmare.

In addition, many OT devices are simply not patchable – either because no patch exists, or the device plays such a critical role in the process network that it cannot be removed from service to patch (i.e., no downtime). Patch Management Solutions help the industrial enterprise make order out of the chaos.

Patch Management solutions automate the installation, timing, verification, and management of the entire patch process for every system that needs it. The solution reviews all vulnerabilities and the software patches that are supposed to remediate them. These tools help to prioritize and determine which patches should be installed to remediate functionality or compliance issues, assure that the patch is installed correctly, conduct post-patch testing and verification, and manage reporting.

Typical Solution Architecture

Most automated enterprise patch management tools deploy agents on target computers. These agents create and control the connection between the centralized patch server and the computers to be patched. Only whitelist URLs, applications, and servers can deliver updates. Patch agents send alerts to the server, store patch software locally on the target computer before installation, initiate automatic retry of failed patch installations, and perform other related tasks.

Why your Industrial Enterprises needs this solution

- **Know where every IT/OT** asset stands in terms of vulnerabilities, ISO compliance, and version status. All departments and systems have access to the same data and are on the same page.
- **Protect every IT endpoint** to prevent data loss and exfiltration and block network attacks.
- Save considerable time and budget with an automated resource that simplifies and streamlines even the most complex patch management programs.
- **Gain accurate data** to prioritize patches and automatically close the loop on vulnerability remediation.

Recommendations

- Make sure the endpoint solution is built for OT environments. Many IT endpoint solutions may not work effectively or may introduce backdoor tunnels for updates.
- In the industrial environment not everything can or should be patched. Make sure to deploy additional layers of defense.

Sample Category Vendors

- Bayshore, Cisco, Kaspersky, Tosibox, TXOne (Trend Micro), Verve Industrial.

NETWORK DISCOVERY, MONITORING AND THREAT DETECTION

The solutions in this category answer the critical need for industrial enterprises to have an accurate accounting of their industrial IT/OT network assets, with complete understanding of their operations. Since manual methods always fall short and are never accurate, these solutions automate continuous Network Discovery and Monitoring processes, so the ICS environment has accurate and real-time information.

Network Asset Discovery

Network asset discovery is an automated process that continuously detects and collects data from the technology assets connected to an OT network. The Discovery process creates a real-time inventory of OT assets, including proprietary OT hardware, IoT and IIoT devices, as well as standard PCs, and the software and virtual machines running on them.

The objective of asset discovery is to create a complete and up-to-date picture of the technology landscape of the OT network. It documents and maps all devices as well as the interaction between devices. By understanding what assets are in play, organizations can identify devices that need attention to prevent or minimize disruption, while establishing behavior baselines to detect anomalies and possible threats.

Solutions may offer both passive and active discovery. While active discovery ('probe' assets and wait for response) enables richer information, it may have unintended consequences. We encourage end-users to thoroughly test active discovery in your own environment prior to deployment.

Network Anomaly and Threat Detection

Anomaly detection identifies patterns of OT device or application behavior that do not conform to 'normal' or expected behavior patterns. Anomaly detection products passively monitor and analyze network traffic to learn behavior patterns and to establish normal behavior of the network.

Initial monitoring may take several days. Once normal behavior is established, thresholds are set to flag traffic patterns and behaviors that are outside the normal range and require investigation. Continuous monitoring alerts in real-time regarding immediate threats and provides historical reporting, which can be helpful for planning and auditing purposes.

Products in this category are good at identifying zero-day attacks and other 'unknown' threats, because their detection is based on knowledge learned from your network, not on a signature list. Some vendors pair anomaly detection with external threat analysis feeds, which enables the vendor to enhance anomaly detection with external information and anonymously share it among their customer base.

Deep Packet Inspection (DPI)

Deep packet inspection examines the content or payload of network data packets sent from one device to another over a network. DPI enables you to track, identify, categorize, reroute, or block packets with undesirable code or data. DPI uses pattern or signature matching to identify the protocol.

Using DPI in an OT/ICS network requires an in-depth understanding of both TCP/IP protocols and OT protocols, such as BACnet, DNP3, EtherCAT, Modbus, PROFINET and more. DPI can alert in real-time when protocol commands are being misused or abused.

Why your Industrial Enterprises needs this solution

You can't control or protect what you can't see or don't know about. A complete and accurate network inventory is absolutely essential to the systems that use inventory data for efficient operations, and proper security coverage of all assets.

Recommendations

Accurate visibility is a means to many ends. Solutions in this category will shine a light into the dark recesses of your industrial network to the benefits of multiple applications and/or systems. Solutions in this category should provide or integrate with other categories to minimize/mitigate risk in the industrial enterprise.

Sample Category Vendors

- Claroty, Cisco, Dragos, Nozomi Networks, SCADAfence, Tenable.

PERIMETER SECURITY AND NETWORK SEGMENTATION

Perimeter Security and Network Segmentation

Product solutions in this category prevent unauthorized communications between different networks, as well as lateral movement between network segments. The traditional emphasis is on securing the perimeter between industrial OT and corporate IT networks. However, these products are also used to restrict traffic flows between zones or segments *within* the OT network and from external memory devices, such as USBs carried into production environments.

Unidirectional Gateways (hardware data diodes and accompanying software) control the flow of information, such that information can travel only in one direction. The absence of two-way data transfer prevents leakage and manipulation from taking place. Unidirectional gateways safely replicate data into the enterprise IT/cloud environment without putting the production environment at risk.

Industrial firewalls protect network boundaries by executing a set of rules to permit or deny the flow of traffic. Firewalls base their decisions on a number of criteria, including identification of OT-specific protocols and deep packet inspection techniques (see DPI in anomaly detection). Industrial firewalls should be implemented on hardened and ruggedized hardware to meet the operating requirements of OT environments.

USB Sanitization

Many cyberattacks gained entry via a simple data stick carried into the industrial facility. USB sanitization or data sanitization products is a process for the irreversible removal or destruction of data stored on a memory device or in hard copy form. Memory devices include hard drives, flash memory/SSDs, mobile devices, CDs, DVDs, and others.

Solutions in this category often comprise service kiosks outside the OT production environment, where the USB or other device can be inserted and scanned. The kiosk is a ruggedized PC/tablet that runs multiple antivirus engines and possibly Content Disarm and Reconstruction (CDR) technology to scan and certify the contents of the device.

Once the scan is complete the clean device (or a certified clean copy) can be carried safely into the production environment. Endpoints in the production environment will be configured to allow access only to clean, certified devices, which effectively prevents access by rogue and unauthorized devices (See Category 3: Endpoint security and patch management).

The Value of Network Segmentation

By dividing the network into multiple logical networks and restricting access between them, we limit the attack area which a single system can reach. An accepted reference model for making this division is the Purdue Model, adopted from the Purdue Enterprise Reference Architecture (PERA) structure. Purdue isn't new, it was developed during the late 1980s. Purdue has since then been further developed, updated, and has influenced subsequent standards. It delivers foundational language for control systems security regulatory controls, found in standards such as IEC 62443 and NIST SP800-82 benchmarks.

The Purdue model points to three important concepts for building a secure Industrial network:

- A clear demarcation between IT (Level 4-5) and OT (Level 0-3) by introducing a DMZ zone called Industrial-DMZ (IDMZ). The purpose of this IDMZ zone is to break direct communication between the IT and OT zones by placing proxy services, jump servers, and any other resources directly in this zone. This prevents outbreaks in the IT environment from entering the OT zone at all. Most attacks originate in the IT zone, as it is internet-connected and generally far more uncontrolled.
- Logical segmentation between cells in the production zones of the OT network (zone 0-1).
- A capability to allow network access for external suppliers in a controlled and restricted way to the OT network, providing access to the system they need to reach.

Why your Industrial Enterprises needs this solution

Defense in depth and network zoning/segmentation has been a best practice in OT/ICS industrial networks for many years. As the traditional perimeters become more porous and more OT assets and IIoT are connected, strategic segmentation is more important now than ever.

Recommendations

Work with vendors and/or service providers that will help you map both the business criticality and vulnerabilities of each asset. This in turn will enable you to fortify segments/zones protecting critical business processes – preventing lateral movement into these zones, and securing assets that have known vulnerabilities, but for various reasons cannot be patched.

Sample Category Vendors

- Cisco, Fortinet, Garland Technology, Mission Secure, Verve, Waterfall.

PRODUCT AND SUPPLY CHAIN SECURITY

While useful information for anyone involved in securing the industrial enterprise, this solution category is squarely aimed at OT assets and IIoT vendors – producers of traditional PLCs, distributed control systems (DCSs), industrial switches and firewalls, as well as newer IIoT devices, such a smart meters and smart cameras.

Solutions in this category provide a product security platform that automates software security tasks from end-to-end, across all stages of the product lifecycle, to ensure that all possible risks to the product supply chain are detected, prioritized, communicated, and solved efficiently. Automation reduces the manual overhead associated with product security, and allows product developers to focus on what truly puts the product(s) at risk.

Solutions in this category will help vendors design, build, ship and maintain more secure products. Every device, no matter its specific function, contains software, firmware, and configuration files. **Vendors, channel and asset owners need to be sure they are not installing counterfeit firmware or software, and are complying with the many regulatory requirements and standards instituted to reduce vulnerabilities that put products at risk.**

This category addresses security requirements both before and after product deployment by providing automated security management of the product development and delivery processes. Automation helps to shorten release cycles and assure that vendors are including known fixes and vulnerability mitigation features in their products.

There are so many security vulnerabilities to check, and these solutions cover all bases and automate the process for the product developer or vendor. For example, these solutions help vendors match individual components to Common Vulnerabilities and Exposures (CVE) databases, in order to assess whether these vulnerabilities can be exploited by the way the specific device will be used. They also automate the vendor's ability to spot software vulnerabilities and faulty device configurations that may lead to other issues.

Potential problems are enumerated and prioritized so vendors can focus development resources on the risks that matter. In addition, these products typically offer some level of remediation guidance to accelerate resolution of each issue. Products also provide a software build and ticketing system to manage the entire process.

Aligning with Standards

There are a number of standards that govern Product Security. IEC62443-4-1 is part of the IEC 62443-4:2018(E) standard that specifies the process requirements for secure development of products used in industrial automation and control systems (IACS).

IEC 62443-4:2018(E) specifies the process requirements for the secure development of products used in industrial automation and control systems. The specification is part of a series of standards that addresses the issue of security for IACS.

IEC 62443-4 defines secure development life cycle (SDL) requirements related to cybersecurity for products intended for use in IACS environments, and provides guidance on how to meet the requirements described for each element. The life-cycle description includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware.

Supply Chain Security

A typical OT supply chain comprises a number of links that include:

- Devices sourced from a wide variety of vendors
- Third-party software components in every device
- Different software distribution and verification process for every software component
- Different upgrade process for every system
- Software updates coming from multiple sources (websites, DVDs, contractors, distributors)
- Devices that need to be updated are widely distributed throughout OT facilities and assets

Installing a modified version of just one of these files in the chain can put an entire industrial production environment at risk.

Supply Chain Security solutions automate the ability of asset owners to fingerprint original firmware and software files, and compare downloaded or delivered updates with the vendor original. When software is being installed on critical, real-time OT/ICS systems, this level of visibility is necessary to manage inherent risks.

Why Asset Vendors need this solution

- Discover if software/hardware subcomponents contain known vulnerabilities/malware before they go into your product
- Know when counterfeit versions of your software updates pop up in the field
- Secure your software update delivery process, as it helps to build trust with the asset owners
- Simplify the process and reduce costs to align with industry standards and comply with evolving regulations

Why your Industrial Enterprises needs this solution

- Gain visibility and control of the upgrade process
- Know the reliability of update files before you install on critical equipment
- Save time and effort by automating the entire process and integrating with already-existing workflows

Recommendations

While the standards and requirements apply only to the developer and maintainer of the product, it is good practice for asset owners to be aware of the relevant standards and hold their vendors accountable.

Sample Category Vendors

- aDolus, Irdeto, Karamba Security, Vdoo.

RISK MANAGEMENT, GOVERNANCE AND COMPLIANCE

As the Industrial Cybersecurity market continues to mature, the focus has rightly shifted to the strategic question of risk. How do we measure, manage, minimize or prioritize the cyber risks in industrial enterprises? After all, this must surely be the overriding goal of any industrial cybersecurity undertaking. How do we know which risks to mitigate or not, and which risks we would like to pass along (i.e., to insurance) and at what value? What is our cyber risk appetite? What is our next best undertaking or investment to reduce cyber risk?

Risk Management and Compliance Management products are designed precisely for this purpose. These products begin by assessing cyber risk to the industrial enterprise either from threat of attack or from failure to meet compliance requirements. The assessment process identifies, quantifies and prioritizes all the vulnerabilities and attack vectors that threaten the industrial enterprise. Armed with this valuable risk data, CISOs can build a transparent security program, and make informed decisions based on the return on investment (ROI) and total cost of ownership (TCO) for every cybersecurity investment that the organization needs to make.

Risk assessment is a continuous and ongoing process. Evolving external threats, internal threats and new technologies pose a constantly changing risk that needs to be quantified, prioritized and communicated to others in the company. To be effective, Risk Management solutions should give all stakeholders a shared view of cyber risk and provide a common language across all departments and up to the boardroom to understand the cyber and compliance risks they face.

The solutions in this category emphasize quantification, reporting and communicating risk so that industrial cybersecurity and compliance can be addressed just like any other business decision - from a data-driven, ROI/value-based perspective. In the end, the organization decides which risks they are willing to bear, and which must be mitigated or transferred.

Governance

Many Risk Management platforms cover the entire risk portfolio from cyber vulnerabilities to regulatory compliance to governance policy. The market also offers products that specialize in governance. These solutions automate the ability to track and govern compliance with external regulations and with internal policy, in order to reduce risk.

Instead of on-site auditing teams that take weeks to assess and produce a report, Governance platforms automate the process, so that compliance can be continuously monitored and measured across the organization. Governance becomes much more efficient as compliance reports are generated automatically and compliance strategies can be implemented systematically and at scale.

Standards include: IEC-62443, NIST-CSF, NERC-CIP, ISO-27001, NIST-1800-23, NCSC-CAF & EU NIS Directive

Internal policy may include: User-defined policies, Best practice policies, third party system policies, firewall policy, Vulnerability Management policy, Endpoint Security policy.

Cyber Risk Modeling for Industrial Networks and Reinsurers

A key driver in cyber risk modeling is to reduce insurance rates for industrial enterprises and for reinsurers to better quantify the risk. When something goes wrong in an industrial process, costly damages may ensue – to the environment, to customers, to businesses, etc.

Products in this category enable industrial enterprises to model and to put a price tag on the financial impact of an attack, to facilitate a fair and appropriate risk transfer from the enterprise to the insurer. Like Risk Management, these products automate the ability of the enterprise to continuously:

- Track and map vulnerabilities
- Assess the probability of exploitation
- Estimate the business (i.e., financial) impact of an attack
- Prioritize mitigation based on ROI
- Negotiate a fair and appropriate risk transfer

The goal is to understand cybersecurity economics (risk-cost analysis) and reduce the risk in the most cost-effective way possible.

Why your Industrial Enterprises needs this solution

- **Stop overspending** on cybersecurity and compliance. Approach cybersecurity decisions based on measurable ROI for each security investment you are considering.
- Leverage automation to **simplify and accelerate risk assessment** work that used to take days/weeks and was out of date by the time it was published – if it was done at all.
- Build data-driven cybersecurity and compliance programs that **balance risk-reduction initiatives with limited budget and resources**

Recommendations

Make sure your organization is ready for this discussion, get buy-in from key stakeholders and bring a multi-disciplinary team together.

Sample Category Vendors

- aDolus, DeNexus, Radiflow, Rhebo, SecurityGate, Tenable.

SECURE REMOTE ACCESS AND ZERO TRUST

Industrial enterprises operate highly complex, multi-site and multi-vendor OT/ICS networks. Many enterprises enable privileged remote access to employees, vendors, operators, integrators, and various third-parties for legitimate purposes. For example, remote access to perform required maintenance eliminates costly travel, saves time, and ensures better service to customers.

Products in this category simplify and automate the complex task of configuring, managing and verifying remote access to OT/ICS networks. Typically, Secure Remote Access solutions are vendor-agnostic. They integrate with IAM systems (see Category 4: Identity and Access Management) for user identification and authentication functions, and support granular role-based access down to specific commands and specific OT devices.

For example, remote access to a smart meter will be allowed, but only a single configuration parameter may be accessed and no others. Normally, remote access solutions manage both read and write permissions. Read-only remote access should be provided by other solutions such as data replication via a unidirectional gateway to a DMZ.

Secure Remote Access solutions create and manage a direct, point-to-point VPN tunnel between the remote user and the device being accessed. Solutions use modular vendor-agnostic components that work seamlessly with one another and with internet, network and device protocols, allowing users to securely connect to modern IoT devices and to legacy OT systems..

Zero Trust for Industrial Enterprises

Zero Trust Access solutions take remote access to the most granular level possible, enabling industrial enterprises to limit remote access to a specific user, device, data stream, application, file, duration, etc. By granting authorization only to a limited set of interactions, hackers who manage to steal credentials no longer enjoy broad permissions that allow them to exploit their initial access as a launching pad to penetrate other parts of the network or to launch attacks from a network zone. Even if hackers get in, their hands are tied.

Zero Trust remote access solutions are designed to enable access across the layers of the OT/IoT environment – for example – from OT to DMZ to IT networks. Instead of VPN connectivity which requires an internal IP address for external users, Zero Trust solutions use a Tunnel and Proxy that fits with standard architectures and securely relays data.

Zero Trust remote access solutions support both cloud and on-premise deployment.

Why your Industrial Enterprises needs this solution

The need for remote access to the industrial environment is crucial to keep these critical systems up and running, more so since the onset of the COVID-19 pandemic.

Recommendations

- Make sure the solution is forward looking in regard to the evolving characterization of industrial cybersecurity. Traditional OT/ICS asset owners will still need vendors to securely 'dial-in' to support their asset, IIoT vendors may likewise need access to systems/devices.
- Granularity is key – lock it down as much as possible.
- IAM is a critical component of a Secure Remote Access solution – refer to Category 4: Identity and Access Management (IAM).

Sample Category Vendors

- BeyondTrust, Claroty, Fortinet, SCADAFence, Tosibox, Xage Security.

SOCIAL ENGINEERING AND PHISHING SECURITY

Cybercriminals have perfected the art of targeting the weakest link in the security chain to get what they want. Using social engineering tactics, they trick unsuspecting employees or contractors into giving up ID and password credentials, as well as other personal data. Armed with legitimate credentials, cybercriminals can walk in the front door of the industrial enterprise network, just like an employee.

Malicious actors have an array of online tools at their disposal. While the vectors, like phishing, are important, it is impulsive human behavior that cyberattackers rely on to gain access to your industrial network and data. That's why solutions in this category focus on the human side of cybersecurity, training employees to recognize cyberattacks and to know how to handle them and provide a safety net for risks they might miss.

Solutions in this category focus on training and email and messaging, which is where most social engineering, i.e., phishing attacks occur.

Automated Security Training and Awareness Platforms

In addition to periodic, frontal training sessions, or computer-based individual training, a number of products are available to automate and personalize security training programs to maximize their impact on employee security awareness and security behavior.

The automated solutions offer an intelligent platform that uses behavioral psychology methods, algorithms, and best practices to tailor an ongoing personal training programs for each employee. Training programs include simulations of phishing attacks, follow up training and reporting on employee progress toward compliance goals.

As you simulate attacks and measure employee response, you gain a better sense of where the risk lies and how to customize training programs to minimize it. For employees, immediate feedback on how they performed is an eye-opening experience that helps them pay closer attention in the future.

Secure Email Gateways (SEGs) and Inbox Security

It is good to reinforce cyber awareness training with solutions that automatically scan incoming and outgoing emails for phishing and malware content. Inbox Security and SEG products do just that.

Inbox Security solutions install a client on each employee Inbox (typically cloud) to monitor email traffic and block phishing/malware content. Employees are also given the ability to self-report emails from suspicious senders or containing suspicious links. Actively involving employees in cyber defense raises their awareness and transforms them into an army of 'boots on the ground,' who contribute valuable and timely intelligence rather than social engineering victims.

Typically, a reporting button is added to the employee Inbox display. If an email looks dicey, one click sends it directly to SecOps team for their review. Speed, efficiency, and accuracy can make all the difference in halting and remediating targeted phishing attacks. Inbox Security platforms typically feature automated remediation of the reporting Inbox and all affected email accounts in the company.

Your Industrial Enterprises needs this solution because:

- Employees need to be aware of the cyber threats that target them and engage in cyber defense. It also becomes the **best way to reduce human errors** and repel social engineering attacks.
- Automated solutions help you **save on SOC and training resources** and make detection and remediation more effective.
- Automated solutions **adapt in real-time to changing tactics** as phishers try to evade detection. Rather than watch your SOC team succumb to fatigue, these solutions don't miss a beat as attackers pivot to new techniques.

Recommendations

Take social engineering seriously. A malicious actor will look and find the easiest way into your organization. People can be hacked too!

Sample Category Vendors

- Cisco, Kaspersky, Microsoft, NTT.

aDolus Technology

The aDolus AI-powered FACT platform is an advanced aggregation, analytics, and correlation engine developed to secure the software supply chain. It derives up-to-date cybersecurity risk intelligence on software components as they flow through the ICS ecosystem: between suppliers, developers, OEMs, service providers, operators, and even those who should not have the software and may use it for malicious intent.

aDolus helps vendors/OEMs manage risk from incoming third-party software by automating compliance and governance through the entire software lifecycle. aDolus provides intelligence to help security service providers protect customers' OT assets. It also provides OT asset owners assurance that files are tamper-free, authentic, and safe before installing on critical devices.

OFFERINGS:

The **FACT Platform** protects the trust chain, keeps systems safe, and provides visibility. The platform aggregates information on the software created by manufacturers of intelligent devices used in regulated and critical industries.

Features include trust scores for software, one-click SBOMs, vulnerability discovery, malware analysis, code signing validation, product family trees, software supplier discovery, and compliance reporting.

https://www.adolus.com/
info@aDolus.com
+1 (866) 423-6587

AlertEnterprise

AlertEnterprise offers software that prevents insider threats, fraud, theft, sabotage, and acts of terrorism. Its software integrates physical access control systems (PACS) and logical systems to provide real-time control, security, and enforcement of governing policies, practices and regulations. These offerings come purpose-built for guarding vital infrastructure in sectors like oil and gas, airports, utilities, pharmaceuticals, federal agencies, financials, and healthcare.

OFFERINGS:

IT/Operational Technology Security Convergence: AlertEnterprise offers security solutions that allow organizations to continue streamlining their operations, while protecting vital operating assets from threats like cyberattacks and insider threats.

Cybersecurity: AlertEnterprise provides cybersecurity solutions for cyber and SCADA (supervisory control and data acquisition) systems. The solutions are designed to assess systems security, as well as prevent potential future threats.

Security Intelligence: Provides a unified Security Awareness and Situational Intelligence Suite that delivers security intelligence across segments like cybersecurity, physical access to facilities, and operational technology like industrial control systems or SCADA.

https://alertenterprise.com/
info@alertenterprise.com
+1 (510) 440-0840

Aperio Systems

Aperio Systems secures critical infrastructure systems across verticals, such as refining, mining, manufacturing, power utilities, and process manufacturing, against internal and external cybersecurity threats by ensuring operational data integrity. Integrating into existing SCADA and industrial control solutions, its Data Forgery Protection (DFP) technology reveals the actual state of ICS systems in the face of malicious manipulation.

Providing a last line of defense against sophisticated cyberattacks, Aperio Systems lowers the risk of shutdowns and service outages, providing operational continuity and maximum system resilience. It provides a last line of defense against sophisticated cyberattacks, reduces the risk of shutdowns and service outages, to deliver operational continuity and maximum system resilience.

OFFERINGS:

The **Aperio data integrity platform** automatically validates operational data at scale to improve data accuracy, allowing for better business decisions based on trusted, reliable data. The platform reduces operational decisions based on inaccurate data, resulting in false alarms, incorrect diagnoses, predictive maintenance failure and third-rate analytics.

https://www.aperio-systems.com/
contact@aperio-systems.com

Armis

Armis delivers its agentless, enterprise-class security platform that addresses the threat landscape of unmanaged and IoT devices. The platform helps with discovering and analyzing all managed, unmanaged, and IoT devices.

Apart from detecting devices on and off the network, Armis continuously analyzes endpoint behavior to identify risks, attacks and protects critical information and systems. It does so by identifying suspicious or malicious devices and quarantining them. Armis is a privately-held company and headquartered in Palo Alto, California.

OFFERINGS:

The **Armis platform** helps in:

- Asset discovery: Identify the make, model, operating system, and location of every device in addition to tracking connection activity through OT protocols, such as Profibus, Profinet, and Modbus.
- Risk management: Detects vulnerable devices.
- Threat detection: Monitors device behavior to detect compromises or policy violations.
- Network segmentation: Validates the integrity of existing network segmentation.
- Incident response: Stop attacks from moving laterally from device to device.
- Integration: Shares alerts and information with firewalls, NAC (network access control), SIEM, ITAM, CMDB, and other security and management systems.

https://www.armis.com/
+1 (888) 452-4011

Asset Guardian

Asset Guardian Solutions Limited (AGSL) helps safeguard process control software assets, speeding disaster recovery and optimizing change management across industries, like oil and gas, power, utilities, chemical, maritime, pharma, and food and beverages.

AGSL's investment in research and partnership with clients has transformed the company from a product to an integrated solution that protects the integrity of safety and process critical systems.

OFFERINGS:

The **Asset Guardian solution** ensures its clients meet their compliance obligations with a range of international standards by providing solutions in the following areas:

- Compliance Management
- Configuration Change Management
- Disaster Recovery
- Cyber Security Management
- Obsolescence Management
- Project Operations and Maintenance
- Consultancy Services

The Cyber Security and Disaster Recovery solution ensures overall data security and integrity. It limits unauthorized access to data and software files by providing a secure central repository.

https://www.assetguardian.com/
support@assetguardian.com
+44(0)1506 597913

AuthUSB

AuthUSB SL aims to develop resourceful solutions in the field of cybersecurity for vast areas of application. The Spanish company commits to offer reliable technology that helps users protect their devices, equipment and networks. authUSB has been developed in response to the need for organizations to protect their assets and business processes, providing a reliable, fast and straightforward deployment tool.

OFFERINGS:

The **Safe Door** is a hardware device with embedded software that allows organizations to handle any threats derived from USB (universal serial bus) storage devices. It enables the continuous monitoring of the USB memory that is being analyzed and a download of files, once verified. Information monitoring and auditing are done through the central console.

All Safe Door devices in the organization are monitored in real-time, enabling the identification of patterns and targeted attacks. Both compact and lightweight, these devices can be used in fixed locations and for mobile users.

https://www.authusb.net/en/
soporte.authusb@soporteclientes.brujula.es
+34 871 96 29 10

Bayshore

Bayshore Networks offers control and protection for industrial Operational Technology (OT) and transforms OT data for IT applications. Incorporating open, standard, and proprietary industrial protocols, the Durham, North Carolina-based company inspects OT protocol content and context, validating every command and parameter against logic-rich policies. Addressing zero-day, internal, and rapidly evolving threats, Bayshore can actively secure industrial endpoints and process control automation systems.

OFFERINGS:

SCADAfuse: SCADAfuse sits in front of critical endpoints, protecting PLCs and SCADA/DCS devices from unauthorized use, dangerous instructions and activities, and remote takeover from hostile sources. It features a bypass port pair for data in/out, requires no re-addressing of the network or assets and is fully self-contained.

OT Access: OT Access is purpose-built for manufacturing, utilities, and oil and gas industries. Available on a subscription-based model, the product delivers a reliable, policy-enforcing, secure remote access solution for OT environments.

SCADAWall: A data diode solution by Bayshore, SCADAWall enables access to OT networks and assets, which otherwise would have been cut off.

https://bayshorenetworks.com/
sales@bayshorenetworks.com
+1 (844) 200-7181

BeyondTrust

BeyondTrust offers privileged access management (PAM) solutions to prevent data breaches related to stolen credentials, misused privileges and compromised remote access.

The BeyondTrust platform empowers organizations to scale privileged security as threats evolve across endpoints, servers, cloud, DevOps, and network device environments. It combines a broad set of elite access capabilities with centralized management, reporting, and analytics, which helps take decisive and informed actions to defeat attackers.

OFFERINGS:

Privileged password and session management: Helps with discovering, managing, auditing, and monitoring privileged accounts of all types.

Endpoint privilege management: Removes excessive end-user privileges on Windows, Mac, Unix, Linux, and network devices.

Privileged remote access: Secures, manages and audits vendor and internal remote privileged access.

Remote support: Helps with accessing and supporting desktop devices and systems.

Vulnerability management: Identifies, prioritizes, and remediates vulnerabilities and informs privilege decisions with risk insights.

Change auditing: Audit, report, and recover changes across Microsoft Windows platforms. .

https://www.beyondtrust.com/
+1 (877) 826-6427

BSS Unit

BSS Unit is engaged in the ongoing development of Industrial Cyber Threat Intelligence (CTI) solutions and analyst services, with Industrial Control System (ICS) focus and deceptive technology, Industrial Honeynet Systems (IHS).

OFFERINGS:

The essence of the **Cyber Intel Matrix (CIM) system** and its success in OT environments is that it does not focus on static defense capability, but on Threat Hunting activity focusing on attack prevention and risk-threat identification with automated information collection classification even before the attack.

Within the system, analysts operate solutions such as Blackpots (custom deceptive technology honeypots that mirror any organization's network), a Malwarelab, STIX Graphs, and cyber threat intelligence.

The system collects information about attacking devices, threatening locations, methods, and information needed to identify an attacker. From this data, BSS Unit analysts can deduce motivations and specific directions of attack.

CIM has worldwide coverage based on a Blackpot system with over 150 proprietary and installed ICs.

https://bssunit.com/
rivka@axalton.com
+1 (914) 466-5976

Check Point

Check Point delivers cybersecurity solutions, including network security, endpoint security, cloud security, mobile security, data security, and security management.

OFFERINGS:

Encompassing network- and device-level IoT security, Check Point Quantum IoT Protect prevents IoT cyberattacks, adapting protections to any IoT or OT device across smart offices and buildings, healthcare and industrial environments. Delivering a zero-trust policy tailored per device, IoT Protect uses real-time threat intelligence, security services, and on-device runtime protection to deliver end-to-end prevention strategy for an evolving cyber-physical attack surface.

Among many benefits seen through deploying Quantum IoT Protect, customers see a reduction in their IoT attack surface with complete IoT device visibility and granular policies and detection and prevention of malicious IoT traffic with over 1000s of protections.

In addition, Quantum IoT Protect is part of Check Point Infinity, a consolidated cybersecurity architecture that protects business and IT infrastructure against Gen VI multi-vector 'Nano' cyber-attacks across networks, IoT devices, endpoints, cloud and mobile.

https://www.checkpoint.com/
IoT_Security_Sales@checkpoint.com
+1 (866) 488-6691

Claroty

Claroty is an industrial cybersecurity company that helps customers reveal, protect, and manage their operational technology (OT), IoT, and IIoT assets. The company is backed and adopted by industrial automation vendors, with an expansive partner ecosystem and research team.

Headquartered in New York City, Claroty has a presence in Europe, Asia-Pacific and Latin America and deployments on all seven continents.

OFFERINGS:

Claroty Platform: Its comprehensive platform connects seamlessly with customers' existing infrastructure and programs, while providing a full range of industrial cybersecurity controls for visibility, threat detection, risk and vulnerability management, and secure remote access with a reduced total cost of ownership.

Continuous Threat Detection (CTD): Extends basic cybersecurity controls to industrial networks. CTD's Enterprise Management Console (EMC) delivers visibility scales and can be effortlessly managed across all connected sites.

Secure Remote Access: As a core component of the Claroty Platform, Secure Remote Access delivers frictionless, reliable, and highly secure remote access to OT environments.

www.claroty.com
kelly.f@claroty.com
+1 862 223 9346

ConsoleWorks (TDi Technologies)

TDi Technologies provides an IT/OT cybersecurity and operations platform for privileged access users. Its patented technology uses flexibility, automation, optimization, control, and management capabilities that improve the ability to meet operational and security demands.

OFFERINGS:

The **ConsoleWorks platform** provides a unified approach to managing the entire foundation layer of infrastructure. In addition, it provides a secure, persistent connection to streamline access and control to any IT/OT device for privileged users.

The platform aims to deliver a single unified IT/OT security, compliance, operations, and automation product. It is constantly monitoring, auditing, and logging activity down to the keystroke to support regulatory, cybersecurity best practices and IT/OT operations, while providing a staunch defense against access by unauthorized users. It also supports various standards including NERC CIP, PCI DSS, SOX, FISMA, HIPAA, and NIST.

ConsoleWorks services include privileged interactive access, asset, patch and configuration monitoring, logging and situational awareness, and endpoint password management.

https://www.tditechnologies.com/
info@tditechnologies.com
+1 (972) 881-1553

The bridge to possible

Cisco helps to digitize and secure industrial operations, using its comprehensive and pre-integrated security portfolio, enabling organizations to improve their IoT/OT security posture and extend zero trust security to their industrial settings.

OFFERINGS:

Cisco Cyber Vision: a visibility and threat detection solution designed for industrial control systems to enable IT and OT to work together in securing operations and feed the SOC with OT context and security events. Built into industrial network equipment, it allows the deployment of OT security at scale without additional hardware, cabling, or out-of-band SPAN collection networks.

Cisco Secure Firewall (Firepower): Next-generation firewalls enforce filtering policies based on Cyber Vision asset profiles and security events to protect industrial zones and remote assets.

Cisco Identity Service Engine (ISE): The Network Access Controller (NAC) enables a dynamic and automated approach to policy enforcement. It leverages OT asset profiles from Cyber Vision to automate network segmentation within the OT environment.

Cisco Secure Network Analytics (Stealthwatch): The Network Traffic Security Analysis (NTA) and Network Detection and Response (NDR) solution uses telemetry to detect advanced threats and leverages Cyber Vision to extend this visibility into the OT network.

Cisco SecureX empowers the cybersecurity team to accelerate threat hunting and incident management by aggregating threat intelligence and data from multiple security technologies—Cisco and others—into one unified view.

Cisco Talos: The threat intelligence team and developer of Snort signatures, Talos also provides proactive services to strengthen security posture, enhance plans, test capabilities, and be engaged within hours to help respond and recover from a breach.

www.cisco.com/go/iotsecurity
AskIoT@cisco.com
+1 (800) 553-6387

Critifence

Critifence Technologies provides cybersecurity solutions for monitoring and controlling OT networks, focusing on critical infrastructures, SCADA, and industrial control systems, which allow monitoring and controlling OT (operational technology) networks easily and passively.

Critifence's solutions are designed to defend stable and complex OT environments by combining hardware like PLCs (programmable logic controllers) and HMIs (Human-Machine Interface). The company's development team comprises SCADA and cybersecurity experts and researchers from the Israel Defense Forces Technology and Intelligence Unit 8200.

OFFERINGS:

SCADADome: It has been designed to deal with cybersecurity threats and offers superior detection and analysis support for different protocols. SCADADome provides a secure and stable solution that allows for monitoring, detection, and analysis of SCADA, ICS, and IIoT protocols, cyber-attacks and threats in critical infrastructure.

SCADADome is currently used in various industries, including transportation, healthcare, pharmaceuticals, water, food and beverage, power and energy, and manufacturing.

http://www.critifence.com/
info@critifence.com
+972 (77) 431 6382

CyberArk

Focused on identity security, CyberArk provides privileged access management in the cloud and throughout the DevOps pipeline. The CyberArk security offering centered on privileged access management can be adopted for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads, and throughout the DevOps lifecycle.

OFFERINGS:

Core Privileged Access Security: The solution unifies enterprise password vaults, privileged session managers, and privileged threat analytics to protect the organization's most critical assets.

CyberArk Alero: It combines zero trust access, biometric multi-factor authentication, and just-in time provisioning into a single SaaS-based solution.

Application Access Manager: CyberArk's application access manager controls, manages, and audits non-human privileged access for applications, tools, containers, and DevOps.

Endpoint Privilege Manager: It reduces the risk of unmanaged admin access on endpoints.

CyberArk Privilege Cloud: A SaaS solution that provides a clear path for storing, rotating and isolating credentials, monitoring sessions securely, and delivering risk reduction to the business.

https://www.cyberark.com/
support@cyberark.com
+1 (888) 808-9005

Cybeats

Cybeats delivers an integrated cybersecurity platform that protects OT/IIoT and IoMT devices used for mission-critical applications. The company's unique secure by design approach allows device manufacturers to develop and maintain secure and protected devices in ICS (industrial control system) networks.

OFFERINGS:

Cybeats security platform solution orchestrates security, incident response, and firmware lifecycle management of OT/ICS critical infrastructure embedded devices. Used to secure and protect connected devices that have a high risk of being attacked, the platform provides continuous threat intelligence to identify potential new threats that might attack deployed devices.

The platform can also be integrated with existing SIEM (security information and event management) systems to provide detailed visibility to individual devices.

The solution facilitates security compliance and automates device manufacturer's development and product life cycle cybersecurity processes by providing SBOM (software bill of material), VA (vulnerability assessment) and SCA (software composition analysis) to the embedded device makers and their clients.

https://www.cybeats.com/
info@cybeats.com
+1 (888) 832-9232

CyberMDX

CyberMDX is a cybersecurity company that provides cloud-based cybersecurity solutions to support the Internet of Medical Things (IoMT). CyberMDX identifies and protects connected healthcare technologies to ensure operational resilience and patient safety and data privacy. Additionally, the company safeguards connected assets to ensure that healthcare and security are not compromised.

OFFERINGS:

CyberMDX Core Software Platform: The CyberMDX core software enables hospitals to identify, access, detect, and defend against potential cyber-attacks with continuous discovery of medical devices, comprehensive risk assessment, and AI-based containment and response. This ensures the operational continuity of the facility's critical assets and the security of patient and facility data.

CyberMDX sensors: The CyberMDX sensors are deployed in hardware, software, or virtual appliance form to provide superior performance and high resiliency for enterprise-class deployments. They acquire network traffic, perform deep packet inspection, convert traffic data into metadata and events, and then report it to the core software. As a result, no sensitive data is transferred out of the customer environment.

https://www.cybermdx.com/
Info@cybermdx.com
+1 (646) 794-4160

Cylus

Cylus delivers rail cybersecurity offerings that help rail and metro companies avoid safety incidents and service disruptions caused by cyber-attacks. The company aims to help mainline and urban railway companies avoid safety incidents and service disruptions caused by cyber attacks.

It offers solutions designed to address the unique requirements and needs of the railway industry, enabling it to detect cyber threats in signaling and control networks, trackside and onboard, facilitating an effective response before harm happens.

OFFERINGS:

CylusOne is used to detect cyber threats in the signaling and control networks, trackside and onboard, and facilitate a response before a mishap. Its technology uses machine learning to speed up the detection of malware and malicious behavior. It also employs AI to help determine the behavior once a threat is identified and effectively handles the response.

CylusOne is used for two purposes:

- CylusOne for Signaling: Ensures ideal security and proper rail operations without any incident.
- CylusOne for Rolling Stock: Secures the train fleets to offer operational safety and availability.

https://www.cylus.com/
info@cylus.com
+972-77-440-1178

Cynerio

Cynerio develops a platform that enables healthcare providers to secure patient data and connected medical devices from cyber threats. In addition, the platform provides device behavior learning with medical workflow analysis to provide complete visibility into what machines are doing on the network and the associated risk.

Cynerio aims to empower healthcare CISOs and give them full control over the security of their connected clinical engineering and IoT ecosystem, ensuring data protection, service continuity and patient safety. Its network-based platform delivers data-rich visibility into the function and behavior of every medical device, pinpoints the risks, and applies tailored protection to ensure operational availability and patient safety.

OFFERINGS:

Cynerio Healthcare IoT platform provides healthcare facilities with a comprehensive suite of solutions that caters to every IT need, from healthcare-safe zero trust cybersecurity to asset and risk management.

The platform covers every connected asset, whether it's medical/IoMT, enterprise IoT, or an OT system - and every threat vector, equipping hospitals with the tools, insights, and controls needed to get cyber-secure fast and stay secure.

https://www.cynerio.com/
info@cynerio.co
+1 (516) 340-3308

Darktrace

Darktrace is a cybersecurity company that uses artificial intelligence for detecting and responding to cyber threats across various digital environments, including cloud and virtualized networks, IoT, and ICS (industrial control systems).

Headquartered in Cambridge, UK, Darktrace uses self-learning AI algorithms to detect and neutralize cyber threats across various digital estates, including the cloud and networks, IoT and industrial control systems. Requiring minimal set-up, Darktrace AI protects against previously unknown vulnerabilities, ransomware, data loss and insider threat.

OFFERINGS:

Industrial Immune System: This is a fundamental AI technology for OT cyber defense. It works by passively learning what 'normal' looks like across OT (operational technology), IT, and industrial IoT, allowing it to detect even the subtlest signals of emerging cyber threats in real-time.

Cyber AI for OT environments: Capable of learning 'normal' for radically different technologies and deployment types, from decades-old PLCs to distributed sensors and industrial IoT. This allows Darktrace's self-learning AI to secure the full range of OT-centric environments and organizations.

https://www.darktrace.com/en/
info@darktrace.com
+1 (415) 229-9100

Digital Immunity

Digital Immunity is a cyber-threat protection company that bridges the gap between real time threat prevention and 24/7 mission-critical environments so that security is no longer compromised due to production. The company provides advanced cyber-threat prevention in OT, with no impact on production or system performance.

The company's patented Digital DNA mapping technology prevents advanced threats, including APTs and zero-day attacks, from executing in memory at runtime, hardening operating systems and applications, with no disruption of processes or production.

OFFERINGS:

The **DI PROTECT** line of cyber-threat prevention solutions delivers cyber-threat prevention, in memory at runtime, on critical OT workstations and servers. In addition, it hardens the operating system and its applications from tampering or the execution of foreign or malicious code.

The line is also easy to deploy, decreasing time-to-value while integrating with existing workflows, simplifying post-deployment management and reducing resource strain. The offerings provide visibility across all operating systems and applications, with deep forensics artifacts in context at the point of attack.

https://www.digitalimmunity.com/
Info@digitalimmunity.com
+1 (781) 425-8655

Dispel

Dispel provides secure remote access designed for OT (operational technology) networks. Built on Moving Target Defense architecture, Dispel helps organizations enable OT remote access while staying aligned to regulatory frameworks and compliance standards.

Dispel also implements a disposable-first infrastructure and time-centric access controls at an industrial scale. The solution helps to standardize operator and vendor access and poise the network for machine-to-machine communication and predictive analytics in the future.

OFFERINGS:

Dispel Remote Access is explicitly built for OT teams and prioritizes network uptime, availability and safety. That means a 30-second connection time, a straightforward user experience for operators and vendors, and complete control for the OT network admin. It also ensures that the team maintains invisible compliance with modern security frameworks.

Its ICS remote access helps OT organizations optimize efficiency by reducing hidden operations and maintenance (O&M) costs - specifically, employee labor costs. Labor costs can run high due to the need for 24/7 monitoring on-site.

https://dispel.io/
hello@dispel.io
+1 (917) 268-4029

Dragos

Dragos is an ICS and IIoT cybersecurity company that applies expert human intelligence and threat behavior analytics to redefine ICS (industrial control systems) cybersecurity. Its software platform and services help operators protect infrastructure sites, such as power grids, water distribution sites, oil refineries, gas pipelines and manufacturing facilities.

OFFERINGS:

The **Dragos Platform** is tailored explicitly for ICS, supervisory control and data acquisition (SCADA), and distributed control system (DCS) environments. It provides the cybersecurity team with up-to-date defensive tools that help combat industrial adversaries. It helps pinpoint malicious behavior on the ICS/OT network, provides an in-depth context of alerts, and reduces false positives for improved threat detection.

The Dragos Platform analyzes multiple data sources, including protocols, network traffic, data historians, host logs, asset characterizations, and anomalies to provide unmatched visibility of the ICS/OT environment. It also strengthens cybersecurity posture by understanding real-world threats shared at machine speed across the industrial community.

https://www.dragos.com/
+1 (855) 372-4670

DENEXUS

DeNexus delivers cyber risk modeling for industrial networks and helps to change how security professionals measure and manage OT (operational technology) cyber risk. The company enables industrial enterprises to measure and mitigate the financial impact of cyber vulnerabilities based on their data footprint. In addition, it provides insurers and reinsurers with evidence-based data leading to superior risk selection and path to profit.

Headquartered in California, DeNexus uses industry-accepted cybersecurity frameworks to feed the data using standardized processes. The output is the probability analysis and financial impact on all the threat scenarios. In addition, risk analysis results of all clients are also clustered by sector and geography to derive the predictive drivers of loss.

OFFERINGS:

The **DeRISK** is a self-adaptive SaaS analytics platform that identifies exposures and dynamically models financial value at risk. It also quantifies real-time network and cyber threat information into economic impact for the business. Powered by probabilistic inference and machine learning, the DeRISK software platform uses evidence-based data to predict where and how breaches are likely to occur in unique client contexts, translating that information into dollars at risk.

With the DeRISK platform, users get an 'inside-out' data collection approach that provides real-time visibility into the insured assets, vulnerabilities, and existing security controls. In addition, the platform also delivers an 'outside-in' data lake that includes customized threat intelligence, supply chain and contextual information.

The platform is fully compatible with the MITRE ATT&CK framework and ISA IEC 62443-3-02 standards, NIST CSF and CIS CSC.

https://www.denexus.io/
info@denexus.io
+1 (415) 944-6700

Embedded Solutions

Embedded Solutions delivers technological solutions in demanding and challenging communication network environments for network security. Its patented technologies are used initially and deployed by Israel's defense-related companies and agencies.

The core technology of Embedded Solutions incorporates mission-critical and time-critical bit level communication. It also filters meaningful or suspicious content and context at the bit level within the networks, along with filtered content and context, including MAC address, IP address, ports, keywords, and bit patterns, such as credit card numbers and ID numbers.

OFFERINGS:

BitNetSentry (BNS) is a smart gateway based on self-developed patented technology. It is a unique network security solution for transparency, low latency, flexibility, and protocol agnostic on time-critical/mission-critical networks.

The standard version of BNS Shielded Firewall includes professional support, security pre configurations, BNS capabilities to secure the firewall itself in case the malware is already inside the LAN and through there is opening a backdoor at the firewall itself, enabling the hackers to access sensitive information and carry out blackmailing and ransomware attacks.

https://embedded-solutions.co.il/
info@embedded-solutions.co.il

Enigmedia

Enigmedia develops native OT and IoT cybersecurity products to protect digital transformation initiatives in industrial environments and critical infrastructures.

Its solutions aim to secure data collection and grant data ownership, build safe communication channels, and protect industrial networks adding an advanced security overlay in conformity with IEC-62334 standard.

Enigmedia has created a unique encryption technology allowing extreme low latency encryption (below 1ms.) matching most demanding industrial requirements.

OFFERINGS:

MUGA: Zero-trust OT network security platform to protect critical and legacy assets in industrial networks and critical infrastructures.

LOTU: Ultra-secure communications over public or private networks, combining the best of VPN, with advanced security features and management tools.

ARGI: OT and IoT data capturing, edge processing and secure connection with analytics and data intelligence applications with full data-ownership.

CHAOS: unique lightweight encryption to protect extreme low latency environments, such as 61850, TSN, and 5G URLLC.

www.enigmedia.es
contact@enigmedia.es
+34943046661

Fend

Fend secures smart infrastructure by integrating predictive analytics and alerts for operators to stay on top of maintenance needs and reduce energy costs. In addition, its hardware offerings enforce a one-way flow of data, providing users with situational awareness without anyone penetrating the network connection.

Fend's cybersecurity hardware helps improve operational resilience and reduce energy consumption by providing complete visibility to connected assets. Using this information, users can identify systems that are underperforming or are in danger of unexpected failure and dispatch appropriate repair staff at the right time.

OFFERINGS:

Data Diodes: Fend offers affordable data diodes to help clients protect companies, utilities, and critical infrastructure. The data diodes connect to the network or cloud. Data diodes are ideal for securely bridging IT and OT networks by developing an internal security team.

Behavioral Analytics is a central security tool that helps with logging, reporting and analytics, and evaluates activity collected across the system.

https://www.fend.tech/
info@fend.tech
+1 (571) 970-1382

Finite State

te State defends critical devices, networks, and supply chains by leveraging massive data analysis to provide transparency to devise manufacturers and their customers. This helps to understand and mitigate risks before they are compromised.

OFFERINGS:

The **Finite State Platform** manages vulnerabilities in connected devices and provides deep analysis of device and supply chain risk factors to deliver holistic insights. The platform automatically analyzes each device, allowing users to identify risk across a comprehensive matrix of factors.

By connecting the device to the platform, users will gain access to an overall risk score, a Software Bill of Materials (SBOM), a list of existing threats and vulnerabilities, and an array of other factors that affect the security of the device. With increased regulations to ensure the safety and security of connected devices, critical networks and infrastructure. Finite State goes beyond the bare minimum and focuses on the overall security of devices and supply chain.

https://finitestate.io/

Forescout Technologies

Founded in 2000, Forescout Technologies actively defends the Enterprise of Things (EoT), spanning OT/ICS, IT, and IoT devices and networks.

Leveraging Forescout's integrated IT/OT platform, network operators can gain complete visibility and classification of all devices in ICS networks, mitigate cyber and operational risk with comprehensive vulnerability and threat detection. In addition, they save time and money with policies for automating security controls across IT and OT networks.

Forescout's advanced alert aggregation and risk scoring models provide relevant and actionable intelligence to the SIEM or the SOC analyst for faster and more effective mitigation workflows.

OFFERINGS:

Continuous OT/ICS device discovery, classification, risk assessment and compliance monitoring. **In-depth visibility** of all IP-connected devices across campus, data center, and cloud networks.

Enforcement and automated **policy-based controls** to proactively reduce the attack surface and rapidly respond to incidents.

Dynamic network segmentation across the extended enterprise.

https://www.forescout.com/
salesdev@forescout.com
+1 866 377 8771

Honeywell

Honeywell Forge for Cybersecurity provides industrial cybersecurity software and services that help protect critical infrastructures and adopt measures to strengthen IIoT technologies. It improves cybersecurity performance, at a single site or across multiple sites, by increasing visibility into vulnerabilities and threats.

OFFERINGS:

Honeywell Forge Cybersecurity Platform: It enables safer movement of data from one site to another and uses operations data to strengthen endpoint and network security, allowing for improved cybersecurity compliance. The platform also delivers a scalable software solution to better address cybersecurity pain points in OT (operational technology) environments.

Secure Remote Access: Increase cybersecurity by connecting through a securely controlled single pipe to IT or OT assets for service delivery, troubleshooting, or remote operations. It also simplifies access to cross-vendor assets and centralizes control over remote access sessions enterprise-wide.

Secure Media Exchange (SMX): It decreases cybersecurity risk and limits operational disruptions from advanced USB-borne threats in a multi-vendor environment. This patented enterprise solution provides visibility and management of removable media.

www.honeywell.com
info@honeywell.com
+1 (877) 841-2840

FORTINET

Fortinet secures SMBs, mid-size and largest enterprises, service providers, and government organizations globally. It delivers intelligent, seamless protection across the expanding attack surface and the power to take on increasing performance requirements of the borderless network.

The Fortinet Security Fabric segments the entire network — from the IoT and industrial IoT to the cloud — to provide superior protection against sophisticated threats.

OFFERINGS:

FortiOS 7.0: The latest version of Fortinet's security operating system powers the Security Fabric, helping customers reduce and manage the attack surface, prevent advanced threats, and reduce complexity.

FortiGate next-generation Firewalls: are powered by purpose-built security processing units (SPUs), including the latest NP7 (Network Processor 7). They enable security-driven networking and are ideal network firewalls for hybrid and hyper-scale data centers.

Fortinet Network Security enables complete visibility and provides automated threat protection across the entire attack surface.

Multi-Cloud Security: Fortinet Multi-Cloud Solutions enables secure applications and connectivity from the data center to the cloud and provides necessary visibility and control across various cloud infrastructures.

Secure Access: There is no slowing the growth of network-connected wireless devices and mobile applications. It also ensures secure application and device access and management without compromising performance.

Security Operations: Fortinet Security Operations solutions deliver advanced threat intelligence to detect, prevent, and respond to sophisticated malware. It also helps achieve compliance and improve overall security awareness.

Network Operations: Fortinet's solution implements a security strategy that prioritizes automation-driven network operations to help prevent network breaches and provides an integrated security architecture to unify siloed environments.

APIs: Partner-developed integration using Fabric APIs to provide a range of pre-validated solutions from IoT to the cloud-ready for development.

https://www.fortinet.com/
chatlevig@fortinet.com
+1 (612) 554-1242

GARLAND TECHNOLOGY

See every bit, byte, and packet®

Garland Technology is a vendor of critical infrastructure visibility solutions for operational technology (OT), enterprise, service providers, and government agencies worldwide. The company believes that secure network visibility should be an easy and seamless experience.

Since 2011, Garland Technology has worked with OT customers to identify their unique challenges and requirements for critical infrastructure environments. As a result, they deliver reliable Network test access points (TAPs), Data Diode, Network Packet Broker, and cloud visibility solutions that deliver packet visibility, while ensuring secure connectivity is needed. In addition, the company provides complete network visibility that enables data centers to address IT challenges and gain complete network visibility.

OFFERINGS:

Network TAPs: Provide ICS security tools with complete packet visibility because users cannot secure what they cannot see. It helps to:
- Eliminate blind spots and improve tool performance.
- Accommodate media and speed conversion.
- Rugged and reliable packet visibility for extreme environments

Data Diode TAPs: Maintain network integrity for industrial network monitoring without exposing additional risk. It delivers:
- Physical hardware separation guarantees unidirectional traffic between network segments
- Complete secure and invisible; no IP address, no MAC address; cannot be hacked.

Network Packet Brokers: Offers flexible network traffic optimization to:
- Streamline network complexity through traffic aggregation
- Optimize network traffic with filtering, load balancing, deduplication, packet slicing and more.

Cloud Visibility: Provides packet visibility for security tools in virtual environments to offer:
- Virtual traffic mirroring vTAP
- Easy to use secure air gap platform.

https://www.garlandtechnology.com/
sales@garlandtechnology.com
+1 (716) 242-8500

Irdeto

Irdeto is a vendor of digital platform security, protecting platforms and applications for video entertainment, video games, connected transport, connected health, and IoT-connected industries.

Headquartered in the Netherlands, Irdeto's software security technology and cyberservices protect more than six billion devices and applications. In addition, the company delivers software security that protects devices and applications against tampering, hacking, and IP theft.

OFFERINGS:

Secure Environment: Complements perimeter security for edge devices in untrusted environments. It safeguards critical files and data and prevents hackers from adding malicious code, modifying executables and scripts and reverse engineering.

Cloakware Software Protection: This is a suite of advanced cybersecurity technologies, libraries, and tools that protect critical digital assets, such as keys, code and data. Cloakware provides application protection, white-box cryptography, and functional integrity verification.

Trusted Telemetry: Provides near real-time detection of hacker activity on ICS (industrial control devices) devices for timely containment of threats and produces secured forensic logs for post event analysis on air-gapped devices.

https://irdeto.com/
+31 23 556 2000

IXden

IIXDen leverages proprietary behavioral and mathematical algorithms, statistical analysis, machine learning, and AI to model the behavior of various industrial physical systems, thereby attaining a better understanding of the device data, software and hardware. The company commercializes its product in water, energy, oil and gas, and smart buildings with large multinational companies in the US and EMEA.

OFFERINGS:

Sensor Data Health for IoT devices: IXDen uses IoT device security and authentication to detect security threats and abnormal behavior. To detect even the slightest anomaly in the sensor data, IXDen implements IoT techniques to help to enhance cybersecurity with sensor data health for IoT devices.

IXDen Grade: This product serves as an overall system reliability measurement, reflecting the level of confidence the customer can put into the data provided by the sensors. If any sensor or device is malfunctioning, broken, or tampered with, the score will immediately drop, and the cause can be identified and fixed leveraging drill-down analytics.

https://www.ixden.com/
info@ixden.com

IBM Security

IBM is a cloud platform and cognitive solutions company. Within the security segment, the company offers IBM Security, an integrated portfolio of enterprise security products and services. In addition, the unit delivers a portfolio of OT (operational technology) security solutions that help industrial, asset-intensive environments monitor and secure networks, protect endpoints, and provide cybersecurity services.

The portfolio is supported by X-Force research and development that provides security intelligence to help companies holistically protect their people, infrastructures, data and applications. It delivers solutions for various requirements, including identity and access management, database security, application development, risk management, endpoint management and network security. Its security professionals monitor and analyze security issues from various sources, providing threat intelligence content as the foundation of the IBM Security portfolio.

OFFERINGS:

OT security strategy, risk and compliance: Clients can evaluate existing security governance against business requirements, including PCI, security, identity and IT regulatory compliance.

IBM QRadar: This helps clients gain actionable insights, identify the top threats and reduce the total alert volume. The IBM QRadar Security Intelligence Platform offers automated analytics for detection and investigation and search-based threat hunting tools designed to analyze and sort through a range of logs, events, and network flows.

X-Force Red ICS testing: Clients can build and test industrial control system attack scenarios to disrupt the attack chain.

IBM X-Force Exchange is a cloud-based threat intelligence sharing platform enabling users to rapidly research the latest security threats, aggregate actionable intelligence, and collaborate with peers.

https://www.ibm.com
info@ibm.com
+1 (800) 426-4968

SOPHIC powered by Israel Electric

IECyber (IEC) is Israel Electric's cyber entrepreneurship and business development division. IEC has developed its own unique cyber management solutions to protect critical infrastructure and industries. It uses a cyber defense and resilience suite that integrates technologies with people skills and behaviors. This line of tools and services provides decision-makers with a realistic and practical cyber picture that helps enhance an organization's defense and resilience.

OFFERINGS:

The **Sophic Suite** includes cyber defense and cyber resilience solutions based on vast, real life daily experience gained in a challenging geopolitical environment with the sole purpose of protecting one of the leading critical infrastructure companies and Israel's only vertically integrated electricity supplier.

Sophic Access was developed to be the missing highly secured, protected channel to remotely support and maintain the 'Crown Jewels' systems of a company/ utility. It allows complete control over sessions and activities with maximum visibility and audibility for all activities. It delivers isolated and controlled access for secure remote vendors, investigates and troubleshoots security/operational incidents, and provides secure access to applications and interfaces based on limited privileges.

Sophic Info allows secure file sanitation and transfers for worldwide SCADA critical infrastructure operators.

Sophic Zone is a "must-have" operational platform for critical infrastructure operators. It allows customers to test OT cyber sturdiness, in addition to emulating, simulating, and validating operational technology and processes.

https://www.iecyber.co.il/
sophic@iecyber.co.il
+972 72 3434588

INDUSTRIAL DEFENDER®

Since 2006, Industrial Defender has been solving the challenge of safely collecting, monitoring, and managing OT asset data at scale while providing cross-functional teams with a unified view of security. Its specialized solution is tailored to complex industrial control system environments by engineers with decades of hands-on operational technology (OT) experience.

Industrial Defender's offerings deliver easy integrations into the broader security and enterprise ecosystem, empowering IT teams with the same visibility, access, and situational awareness they're accustomed to on corporate networks. In addition, the company secures some of the largest critical control system deployments to protect the availability and safety of these systems, simplify standards and regulatory requirements, and unite OT and IT teams.

OFFERINGS:

Industrial Defender's OT cyber risk management platform, **the Automation Systems Manager,** delivers asset visibility and management, endpoint and network anomaly detection, vulnerability management, compliance reporting, and enhanced IT and OT collaboration.

Industrial Defender ASM collects, monitors and manages ICS asset data at scale, providing the essential foundation to apply ICS security controls effectively. It delivers a unified view of control systems cybersecurity, operations, and compliance management.

Building Defender helps to detect and prevent cyberattacks on building management systems (BMS). Building Defender uses sensors to analyze systems, devices and network traffic using BMS protocols, such as BACnet and Modbus.

The **RTAP solution** delivers a secure SCADA solution to manage the automation challenges of the critical infrastructure. In addition, the RTAP real-time object database offers the ability to reuse or clone system components, saving considerable time and investment in system development, expansion and maintenance.

https://www.industrialdefender.com/
info@industrialdefender.com
+1 (877) 943-3363

Kaspersky

Kaspersky Industrial CyberSecurity works to secure ICS (industrial control systems) and critical infrastructure. The company's security portfolio includes endpoint protection and several specialized security solutions and services to fight hackers and evolving digital threats.

Kaspersky Industrial Cybersecurity includes a portfolio of products and services designed to provide holistic protection for every industrial layer, including Supervisory Control and Data Acquisition (SCADA) servers, Human-Machine Interface (HMI), engineering workstations, programmable logic controllers (PLCs), network connections, and people.

OFFERINGS:

Specifically built to meet an organization's industrial-level cybersecurity needs, KICS for Nodes is designed to protect industrial operator panels, workstations, and servers. At the same time, KICS for Networks provides industrial network security monitoring.

KICS for Networks is an OT Network Monitoring and Visibility product which is a platform delivered as software or virtual appliance, passively connected to ICS networks.

KICS for Nodes is an OT Endpoint Security product delivered as software for Windows and Linux based machines.

Kaspersky Security Center is a centralized security management platform.

https://ics.kaspersky.com/
info@kaspersky.com
+1 (866) 328-5700

Karamba Security

Karamba Security has developed a suite of software products and services that enable IoT device manufacturers to protect their products, including third-party modules, without changing R&D or supply-chain processes without changing the device hardware architecture.

The company's solutions are licensed to protect over 12 million devices across a customer base that includes Alpine, AP Systems, DENSO, Hitachi, Hyundai, Seagate, Solar Edge, Stanley and Zebra.

The solutions' cover the entire lifecycle:

- Automatic analysis of the binaries and third-party modules' security posture.
- Automatically generated Software Bill of Materials and compliance to IEC 62443 standard.
- Automatically and seamlessly applied runtime controls to prevent cyberattacks deterministically.
- Real-time visibility and alerts on attack attempts.

OFFERINGS:

Karamba's Product Suite For Embedded Security Lifecycle provides software integrity and authentication needed in performance-challenged environments.

Karamba VCode can help manufacturers identify, prioritize, and mitigate security gaps in the software image before their devices leave the factory floor.

https://www.karambasecurity.com/
contact@karambasecurity.com
+972 50 313 5003

Medigate

Medigate aims to secure the clinical environment to provide a security strategy and coordinated approach. As IT, OT, IoT and physical systems converge, the threat of cyber attackers exploiting vulnerabilities across new and old infrastructure increases. Therefore, its focus is on protecting every connected device in the hospital environment.

The Brooklyn, New York-based company understands that the healthcare network requires detailed knowledge of every medical device, their proprietary protocols, and a comprehensive understanding of medical workflows.

OFFERINGS:

The **Medigate platform** understands medical device protocols, existing and potential cyber threats, as well as expected device behavior. It also meticulously analyzes device and network communication and medical workflow patterns to accurately detect anomalous behavior and identify threats in real-time with minimal false positives.

Utilizing a medical device signature database developed by Medigate Research Labs, it can fingerprint each device with deep packet inspection (DPI) techniques, allowing dynamic inventory management and facilitating advanced detection and prevention capabilities.

https://www.medigate.io/
+1 (855) 908-0775

Microsoft (CyberX)

CyberX delivers an industrial cybersecurity platform that works towards defending critical national infrastructure. The company's technology solutions work in real environments to address real and immediate threats, providing enterprise-grade cybersecurity for defending critical infrastructure in any environment.

OFFERINGS:

The **CyberX platform** delivers insights about IoT/ICS assets, vulnerabilities, and threats without relying on rules or signatures, specialized skills, or prior knowledge of the environment. Instead, its IoT/ICS-aware comes with deeply embedded knowledge of IoT and ICS protocols, devices, vulnerabilities, applications and their behaviors.

The platform's holistic approach reduces complexity with a single unified platform for asset management, risk and vulnerability management, and threat monitoring with incident response. It integrates with existing SOC workflows and IT security stacks, including SIEMs, SOAR, ticketing, CMDB, firewalls, NAC, and privileged access management solutions.

The platform is heterogeneous, and OT vendor-agnostic comes with broad support for diverse IoT/ICS protocols and control system equipment from all IoT/ICS vendors.

https://cyberx-labs.com/
support@cyberx-labs.com

Mocana

Mocana helps device operators bridge the adoption challenge between device vendors and service providers and enables digital transformation with the emerging 5G network, edge cloud and SD-WAN.

The company protects content delivery supply chain and device lifecycle for tamper-resistance from manufacture to end of life, with root-of-trust and chain-of-trust anchors. It also measures the device for sustained integrity and trustworthiness of operations and data to power AI/ML analytics.

OFFERINGS:

The **Mocana TrustCenter** operations platform provides a tamper-resistant and scalable workflow for transferring ownership and lifecycle management of devices fully integrated with authentication and certification services.

Mocana TrustEdge is a comprehensive software solution for IoT device protection. Distributed as pre-compiled binaries, TrustEdge works seamlessly with TrustCenter to provide embedded perimeter controls, authenticated and automated key management for network traffic encryption.

The **Mocana TrustCore** development platform empowers application developers with a simple set of APIs to leverage data privacy and protection controls for safety, security, and compliance without extensive re-engineering.

https://www.mocana.com/
sales@mocana.com
+1 415-617-0055

Mission Secure

Mission Secure provides OT/ICS/IIoT cybersecurity products and services to stop OT threats. The company's security platform delivers network visibility and threat detection, network segmentation, policy enforcement, and operational health monitoring of key assets. The company offers a suite of services to help customers through the life cycle of their OT security program, from risk assessments, planning, managed services, and incident response.

Mission Secure serves defense, critical infrastructure, and process industries, including chemicals, manufacturing, maritime, oil & gas, power, smart cities, and building management systems.

OFFERINGS:

OT Cyber Risk Assessments (Onsite and Remote): Get a clear understanding of your OT cybersecurity strengths and weaknesses based on onsite inspections, network monitoring, data capture/analysis, and passive penetration testing. Assessments include documented findings and recommendations.

OT Cyber Planning: Develop OT cybersecurity plans and a roadmap based on assessment findings and recommendations.

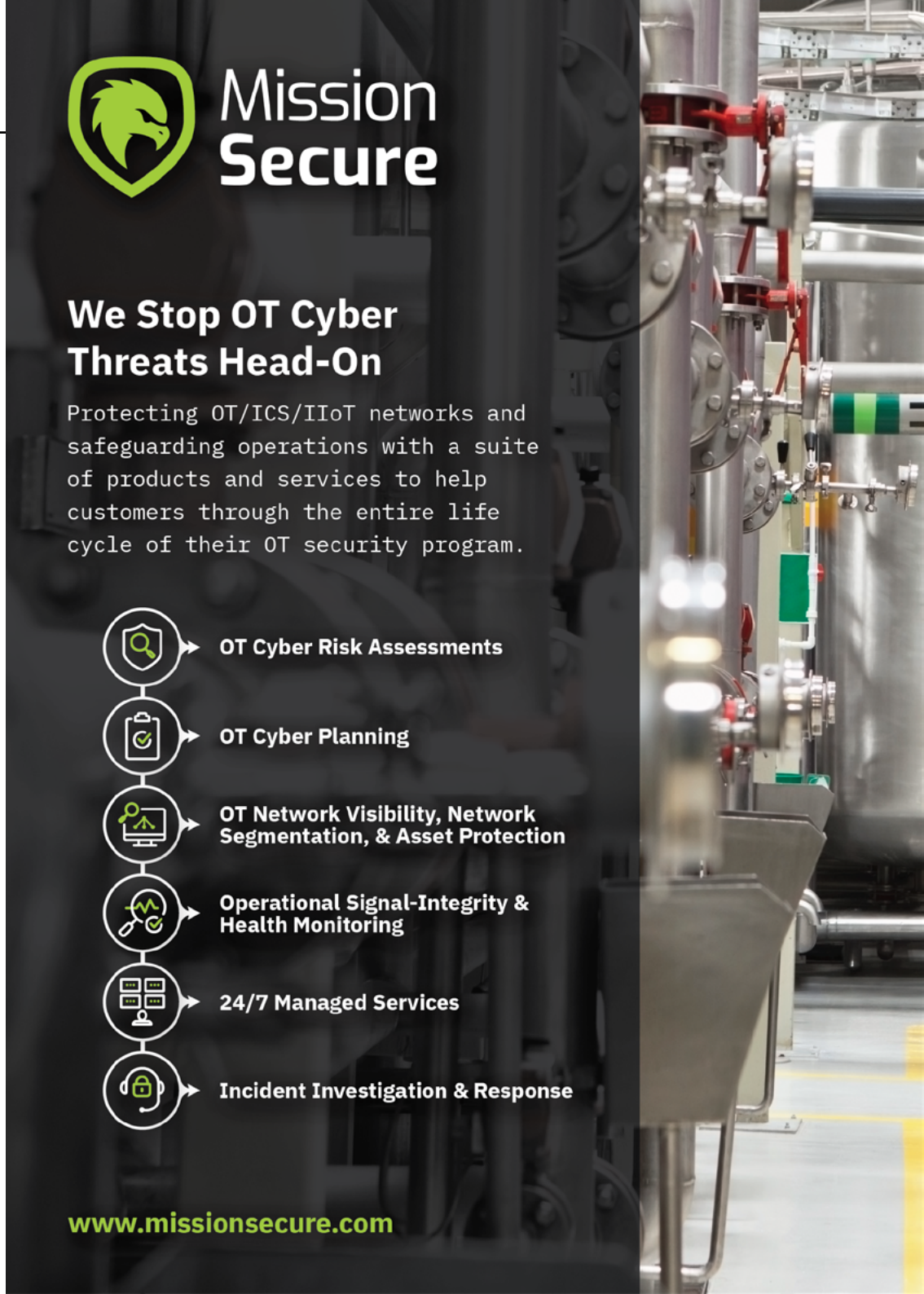
OT Network Visibility, Network Segmentation, and Asset Protection: Patented OT cybersecurity platform providing detailed asset and network visibility that is also used to enable passive threat detection or active policy enforcement and threat prevention.

Operational Signal-Integrity and Health Monitoring: Patented data integrity and operational health monitoring of key assets for possible cyber or failure events that may disrupt operations or threaten safety.

24/7 Managed Services: A 24x7 OT security team to monitor and protect OT networks. IT and OT expertise to manage cybersecurity programs or augment existing team(s).

Incident Investigation and Response: A 24/7 OT security team with the experience and expertise to investigate, eliminate, and recover from security incidents.

www.missionsecure.com
www.missionsecure.com/contact
+1 434 284 8071



NTT

NTT's Intelligent Cybersecurity services help clients create a digital business that is "Secured by Design". With enhanced threat intelligence, NTT can predict, detect and respond to cyber threats while supporting business innovation and managing risk. NTT has a global Security Operations Centers (SOC) network and over 2,000 security experts to provide solutions and services.

As digitization drives the convergence of IT and OT infrastructure, new and IT-based threats can now be seen in OT networks. Using a 'Secured by Design' methodology, NTT's solutions secure both IT and OT infrastructure. NTT's OT security solutions help clients secure the OT networks every step of the digital journey – from planning and design to implementation to live operations and monitoring and life cycle maintenance.

OFFERINGS:

Cybersecurity Advisory Services: NTT has a dedicated team of OT cybersecurity consultants globally. These advisory services help bridge the IT-OT gap, performing both rapid and detailed OT Cybersecurity assessments and an IT-OT converged review.

IT-OT Threat Monitoring & Response: This is a 24x7 SOC-delivered service that monitors and responds to IT and OT network threats. As a result, clients can focus on their core business, while NTT manages technology evaluation, procurement, and maintenance.

IT-OT Managed Security Services: 24x7 SOC-delivered service that covers a client's end-to-end cybersecurity operation. This includes SecOps, cybersecurity monitoring, device management, and ongoing improvement.

Global Technology Services: Delivered by NTT's technical experts, the services deliver in depth design workshops, supply industry best-of-breed technology, and deploy solutions globally.

https://hello.global.ntt/en-us/solutions/cybersecurity/secure-ot
zhanwei.chan@global.ntt

NanoLock Security

NanoLock Security provides zero-trust, device-level protection for IoT, OT, and connected devices. Its lifetime protection and management secure connected devices against persistent cyberattacks by outsiders, insiders and supply chain attackers.

OFFERINGS:

NanoLock MoT (Management of Things) is a cloud-based or on-premise management platform that provides device protection activation, cross-vendor, device-level monitoring, version management, and enforcement to ensure secured updates for further threat intelligence.

NanoLock solution secures connected devices during the **vulnerable Over-The-Air (OTA)** / remote firmware updates, using a proprietary and secure protocol for device-server communication.

NanoLock embedded gatekeeper is agnostic to the CPU and OS, applicable to any connected device - legacy or new. As a result, the NanoLock gatekeeper is ideal for all IoT and connected devices with minimal energy, memory, and processing requirements.

NanoLock **device-level protection and management** serves a range of IoT-connected devices, including smart meters, industrial machines, data concentrators, and smart lighting, across industries and applications.

https://www.nanolocksecurity.com/
yanirl@nanolocksec.com, Refaelas@nanolocksec.com
+972 505 791 846

Nozomi Networks

Nozomi Networks accelerates digital transformation by protecting critical infrastructure, industrial and government organizations from cyber threats. Headquartered in California, Nozomi delivers real-time security monitoring for ICS (industrial control systems) and improves resilience for industrial operations. In addition, it delivers OT visibility, threat detection, and insight to thousands of the most significant critical infrastructure and industrial sites around the world.

OFFERINGS:

Vantage: The product leverages the power and simplicity of software as a service (SaaS) to deliver improved security and visibility across OT, IoT, and IT networks. It also accelerates digital transformation for large and complex distributed networks.

Guardian: It delivers visibility, security, and monitoring of OT, IoT, IT, edge, and cloud assets. Guardian sensors send data to Vantage for consolidated security management anywhere, anytime from the cloud.

Central Management Console (CMC): The CMC product makes it easy to monitor and manage cybersecurity across distributed industrial sites. The single console provides consolidated access to data from all Guardian deployments in the field or on the plant floor.

https://www.nozominetworks.com/
info@nozominetworks.com
+1 (800) 314-6114

OPSWAT

OPSWAT provides solutions for critical infrastructure protection, with its primary goal of eliminating malware and zero-day attacks. Additionally, OPSWAT focuses on threat prevention and process creation for secure data transfer and safe device access.

The overall product solution by OPSWAT is categorized into two sets – MetaDefender for threat prevention, and MetaAccess for cloud access control and endpoint compliance.

OFFERINGS:

Advanced Threat Prevention Platform: A cybersecurity platform for preventing and detecting cybersecurity threats on multiple data channels.

MetaDefender Core: An advanced threat prevention development platform. MetaDefender Drive: Inspects devices before they enter a facility or its network.

MetaDefender Email Gateway Security: Examines every email and attachment, scanning and addressing malicious content before it's delivered.

MetaDefender ICAP Server: A network security platform.

MetaDefender Kiosk: Acts as a digital security guard. It inspects all media for malware, vulnerabilities, and sensitive data.

MetaDefender Vault: A secure file storage and retrieval solution that protects critical files.

https://www.opswat.com/
techpartners@opswat.com
+1 (415) 590-7300

Ordr

Ordr provides complete visibility and security over every connected device - from traditional IT devices to IoT, IoMT (Internet of Medical Things) and OT.

Headquartered in California, Ordr provides one common platform for security, networking, and device owners. The company enables a complete IoT device security lifecycle — from discovery and profiling of devices and risks to the automated response. It also offers role-based access controls and custom views for every stakeholder.

OFFERINGS:

The Ordr Systems Control Engine (SCE) uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. As a result, Ordr delivers real-time asset inventory, addresses risk and compliance, and accelerates IT initiatives.

Ordr also automates security, from dynamically generating segmentation policies that enable only «sanctioned» device communications, triggering appropriate quarantine, scanning, blocking policies for every class of device directly through the organization's network security infrastructure.

https://ordr.net/
info@ordr.net
+1 (833) 673-7999

OTORIO

OTORIO delivers OT (operational technology) security and digital risk management solutions that enable reliable, safe and efficient industrial digitalization. In addition, the company empowers 'secured-by-design' rollouts of industry 4.0 initiatives by making cybersecurity an integral part of the operational life cycle.

By simplifying complex IT/OT security processes, OTORIO ensures industrial control systems security, with continuous management and remediation of digital and cyber risks based on their business impact, safety, reliability and productivity.

OFFERINGS:

RAM² Security Orchestration: RAM² is a patent-pending Security Orchestration, Automation and Response (SOAR) platform for OT security and digital risk management. It seamlessly integrates information from diverse operational and security systems.

remOT: The platform offers advanced secure remote and privileged access management capabilities for the digitized industrial sector. Built from the ground-up for operational networks, remOT secures every link of the supply chain's connectivity to industrial assets to eliminate risks caused by unauthorized or malicious access.

http://www.otorio.com/
info@otorio.com
+972 545 223 813

Owl Cyber

Owl Cyber Defense provides data diode cybersecurity technology for one-way data transfers and assured network security against malware and ransomware. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl delivers one way data transfer products to meet various operational needs, from entry-level to enterprises.

Certified by the U.S. government, independent testing authorities, and international standards bodies, Owl technologies and services help secure the network edge and enable controlled unidirectional and bidirectional data transfers.

OFFERINGS:

Cross-Domain Solutions deliver accredited and validated hardware-enforced cross-domain data transfer products and advanced filtering based on Owl's data diode technology.

Data Diode products deliver comprehensive, hardware-enforced data diode cybersecurity products for commercial and industrial use to offer seamless data availability and unhackable security.

Embedded Cybersecurity Modules for equipment manufacturers.

Data Diode Card Kits comprises two Owl Communication Cards, one that sends and the other that receives, and a fiber optic able.

https://owlcyberdefense.com/
+1 (203) 894-9342

radiflow

Radiflow develops industrial cybersecurity solutions for critical business operations. It offers solutions for ICS/SCADA networks that empower users to maintain visibility and control of their OT (operational technology) networks.

OFFERINGS:

Radiflow's solution suite for OT networks provides multi-layered cyber-protection, adaptable to each user's topology and operational characteristics.

Cyber Industrial Automated Risk Analysis (CIARA) platform meets best practices around risk modeling and management using the ISA/IEC 62443 series of standards. It is a fully automated tool for asset data collection, data-driven analysis, and transparent risk metrics calculation, including risk scoring per zone and business process based on business impact.

The platform responds to the growing digitization of the production floor (Industry 4.0), leading to the rising tide of cyber threats. At the same time, risk assessment processes remain manual tasks that fail to address the full scope of the issue.

The **iSID Industrial Threat Detection system** is server-based software that analyzes all OT network traffic through a mirrored stream to generate and display a network topology model, which serves as a baseline for detecting exceptions on the network.

The **iSAP Smart Probe** is a cost-effective solution that enables the data collection from sub-networks to a central iSID server making it ideal for extensive chemical facilities with multiple primary DCS networks and secondary SCADA/PLC networks.

Ruggedized Secure Gateways provide DPI-firewalled access to production processes, with configurable access rights for different stakeholders. In addition, the Gateways' authentication proxy authenticates each user and restricts the user's access based on role or predefined tasks.

https://radiflow.com/
sales_NA@radiflow.com
+1 (302) 547-6839

Palo Alto Networks

Palo Alto Networks is shaping the cloud-centric future with technology that transforms the way people and organizations operate. The company addresses security challenges with continuous innovation that seizes breakthroughs in artificial intelligence, analytics, automation, and orchestration.

By delivering an integrated platform and empowering a growing ecosystem of partners, Palo Alto is at the forefront of protecting organizations across clouds, networks, and mobile devices. The company offers firewalls that identify and control applications, scan content to stop threats and prevent data leakage.

OFFERINGS:

Next-Generation Firewalls: Provides complete visibility everywhere, along with precise policy control.

Network Security Management: Offers easy-to-implement and centralized management features to gain insight into network-wide traffic and threats and administer firewalls everywhere.

Security Operating Platform: Prevents cyber-attacks across IT and OT infrastructure. The platform allows clients to safely modernize and integrate ICS/SCADA infrastructure and exceed security-related compliance requirements.

https://www.paloaltonetworks.com/
mops@paloaltonetworks.com
+1 (408) 738-7799

PAS

PAS, part of Hexagon, delivers software solutions that prevent, detect and remediate cyber threats. It also reduces process safety risks, optimizes profitability, and enables trusted data for decision-making.

OFFERINGS:

The **OT / ICS Cyber Integrity** identifies configuration changes against established baselines, provides continuous vulnerability management with patch level assessments, and identifies cybersecurity risks to both IT and OT/ICS endpoints. It also enables workflows and documentation for vulnerability remediations and compliance with NIST, ISA/IEC 62443, NERC-CIP, ISO27001/2, the NIS Directive, and other regulations.

Automation Asset Management: PAS Integrity aggregates, organizes and contextualizes highly complex data from disparate, proprietary industrial automation systems to help plant personnel maximize productivity, ensure reliability, and proactively identify and address potential safety incidents.

It also aggregates and organizes OT configuration data, ensures configuration consistency (from level 3 to 0), and enriches data lakes.

Operations Management / Process Safety: PAS PlantState Integrity analyzes data from disparate sources to provide critical safety and production information that improves operator situation awareness.

https://www.pas.com/
+1 (281) 286-6565

Red Trident

Red Trident is a vendor-agnostic technology company focused on improving client's operational efficiency. It offers products and services for process control systems, industrial networking, medical, governmental, and other market verticals to create easy to deploy, maintain, and improve over the lifecycle of assets.

OFFERINGS:

Cyber-ECP: The Cyber-ECP appliance is a small form factor, a DIN rail mounted device that is simple to connect to the network as plugging in a laptop. It is a linear chain of security controls, with each control reducing the attack surface an adversary would have to attack an environment.

Each control in the chain was specifically picked based on the various Tactics, Techniques, and Procedures (TTPs) adversaries use to breach an environment and the most effective way to detect and protect against these TTPs.

Red Trident Access Solution (RTAS): This is a series of products that helps eliminate travel time to remote assets, limit employee exposure to dangerous situations, reduce connectivity and operator log-in time compared to traditional RDP. It also simplifies the operator's workflow setup and management is painless.

https://redtridentinc.com/
sales@redtridentinc.com
+1 (832) 493-1153

Rhebo

Rhebo delivers offerings that help with the cybersecurity and operational stability of the ICS (industrial control systems) and IoT infrastructure in industrial, energy, and water companies.

Using its industrial network monitoring solution, the Leipzig, Germany-based company can monitor all communication within the ICS and reliably report any attacks and vulnerabilities, as well as technical error states.

OFFERINGS:

The **Rhebo Industry 4.0 Stability and Security Audit** provides a fast and comprehensive risk analysis of the Industrial Automation & Control System (IACS). With the OT security audit, users assess all IACS assets, properties, connections, communication patterns, and hidden threats.

Rhebo Industrial Protector reliably protects OT against disruption by cyber attacks, malware, technical error states and manipulation. It uses deep packet inspection technology to analyze and evaluate any communication within the network boundaries down to the content level.

Rhebo IoT Device Protection is a dedicated IoT monitoring solution that protects connected, critical IoT devices from cyber attacks, manipulation and technical error states.

https://rhebo.com/en/
info@rhebo.com
+49-341-3937900

Sapien Cyber

Sapien Cyber offers cybersecurity solutions for the OT (operational technology) environments and associated IT technology. The Australian company protects infrastructure from cyber incursions and their impact on business continuity, reputation, and financial loss.

While traditional Security Information and Event Management (SIEM) solutions provide intelligence on occupant activities, the Sapien Vulnerability Management, Threat Management and managed Security Operations Centre (SOC) offerings comes with a continuous assessment of weaknesses and defensive readiness, in addition to actionable intelligence on any threat to the network.

OFFERINGS:

Vulnerability Management System: It provides the ability to understand the hardware and software vulnerabilities within the organization's network, delivering an in-depth vulnerability assessment of the hardware and software running on devices.

Threat Management System: It offers automated detection of security threats and vulnerabilities, including an analytical tool to perform an investigation on these as well as network incidents and asset inventory. It also enables the company to provide clients ongoing security posture assessment that ensures optimal security hygiene.

https://www.sapiencyber.com.au/
info@sapiencyber.com.au

SASA Software

Sasa Software provides advanced network security solutions for OT/ICS, healthcare and critical infrastructure networks. The company delivers its line of GateScanner Content Disarm and Reconstruction (CDR) that prevents advanced and undetectable file-based attacks by leveraging optimized multi-AV scanning with nextGen detection and transforming files into a neutralized copy using proprietary file reconstruction.

It offers dedicated OT and ICS security solutions, including portable (USB) media security, network segmentation, and an offering for scanning OT computing appliances.

OFFERINGS:

GateScanner Kiosk: Prevents media and file-based attacks from portable devices using a highly secure appliance, enabling NERC CIP 003-7 compliance and internal policies.

GateScanner Desktop: Prevents file-based attacks from portable devices at the user's desktop.

GateScanner Appliance Security: Enables a Multi-AV, full HDD scan of OT computing appliances.

GateScanner Security Dome: Multi-route content security uses document uploads, file sharing, browser downloads, file-sync automation, and browser-based portable media security, storing files in a secure and encrypted vault.

https://www.sasa-software.com/
info@sasa-software.com
Israel HQ: +972-4-8679959 US: +1 (973) 422-8112 Singapore: +65-6210-2354

SecurityGate.io

SecurityGate.io is a Software as a Service (SaaS) risk management platform for industrial cybersecurity. The company's software provides complete visibility into how an organization's cybersecurity strategies are performing, with insights on where to make adjustments to strengthen operational resilience.

The platform is built to manage security controls covering people, processes and technology, across OT and IT environments. Agile SaaS workflows and reporting automation speed up the entire lifecycle of risk management activities.

Organizations across critical infrastructure sectors using SecurityGate.io report:

- The time it takes to perform out-of-the-box and custom, framework-based cyber assessments are cut in half or more.
- Risk management and security practitioners complete remediation projects faster, resulting in their risk programs achieving milestone goals sooner.
- Company leaders can consistently measure and track cyber program effectiveness across the organization and benchmark performance improvement metrics from one facility to another.

OFFERINGS:

Agile SaaS Workflows & Reporting Automation: Assessments, remediations, validations, risk registry, auditing, supplier risk analysis, and more digitized to provide insights sooner for faster program improvements.

Open API & Pre-Built Integrations: Data can be programmatically pulled from the platform for custom reporting and GRC integration. In addition, pre-built integrations with various GRC and cybersecurity products make it easy to bring insights together into one pane of glass.

Consultant & MSSP Partner Program: SecurityGate.io visualizes the value driven by the partner and reduces the effort it takes to achieve client goals. Our partners see improved engagement margins and accelerated growth of revenue with more projects.

www.securitygate.io
info@securitygate.io
+1 (832) 463-1702

SCADAfence

SCADAfence secures OT networks in manufacturing, building management, and critical infrastructure industries. The company secures industrial operations to increase production automation, IT/OT connectivity, and IIoT complexity. With SCADAfence, companies can operate securely, reliably, and efficiently as they go through the digital transformation journey.

OFFERINGS:

The **SCADAfence Platform** is a continuous OT network monitoring platform that provides visibility, risk management, governance and threat detection.

The **SCADAfence Governance Portal** increases readiness and compliance for organizational policies and regulations, provides accurate auditing based on real traffic data, and enables end to-end management of the compliance process across the organization.

SCADAfence IoT Security delivers proactive management of IoT devices for the ongoing reduction of the attack surface. It also uses AI-based technology that includes on-site automated learning for threat detection and prevention. In addition, its multi-layer vulnerability management provides IoT configurations, firmware/software versions (CVEs) and network vulnerabilities.

SCADAfence OT Remote Access Security helps manage unmanaged remote access connections.

https://www.scadafence.com/
info@scadafence.com
+1 (646) 475-2173

Sepio Systems

Sepio Systems empowers organizations to create, enforce device policies, and block unapproved and rogue hardware. First, the company calculates a digital fingerprint from the electrical characteristics of the device. Then, it compares it with known fingerprints, automatically providing information on the vendor name and product name, using physical layer fingerprinting technology and machine learning.

OFFERINGS:

The **Sepio HAC-1 platform** uses a novel algorithm, a combination of physical layer fingerprinting modules coupled with a machine learning module, further augmented by a threat intelligence database.

The platform is designed to discover all devices operating over network and USB interfaces. It provides visibility, control, and mitigation to zero-trust, insider threat, bring-your-own-device (BYOD), IT, OT, and IoT security programs. Its hardware fingerprinting technology discovers all managed, unmanaged, and hidden devices otherwise invisible to all other security tools.

https://sepio.systems/
+1 (240) 421-0669

txOne networks

TXOne Networks provides cybersecurity solutions purpose-built for the industrial control systems (ICS) environment, focusing on maximizing availability and output while preventing disruption.

Ideal for the needs of critical infrastructure, manufacturing, and other OT work sites, TXone's software and appliances secure networks and endpoints while accommodating productivity of both vulnerable legacy systems and modernized assets. In addition, solutions from TXOne Networks place a high priority on keeping the operation running.

OFFERINGS:

ICS Network Defense: TXOne Networks' Edge series focuses on increasing visibility and ease of defense with intention-focused network segmentation, virtual patching, and protocol sensitive design to allow granular control of traffic.

ICS Endpoint Protection: TXOne StellarEnforce uses a trust list to simplify and lockdown fixed-use systems, while StellarProtect uses an ICS inventory, machine learning, and process filtration to provide flexible defenses while maintaining the output and versatility of modernized assets. Both can be managed from the centralized StellarOne management console.

ICS Security Inspection: Trend Micro Portable Security 3 TXOne Edition is a handheld USB device that plugs into mobile assets for fast scanning and creates logs and an inventory of every asset scanned. It can set up a checkpoint for devices that enter the worksite premises or scan sensitive, air-gapped assets that can't connect to the internet.

OT Defense Console delivers centralized continuous monitoring of OT cyber threats with a secure, distributed industrial network support for uninterrupted production line operation.

https://www.txone-networks.com/en-global
contact@txone-networks.com
+886-2-2378-9666

tenable

Tenable is a cyber exposure company that delivers offerings to understand and reduce cyber risk. It provides users with a view of every asset across the attack surface, from cloud environments to operational technologies, infrastructure to containers, and remote workers to modern web apps with the company's vulnerability management sensors. Its machine learning powered predictions reduce remediation efforts by enabling users to focus on the risks that matter most.

As the creator of Nessus, Tenable delivers a platform that sees and secures any digital asset on any computing platform. New types of connected devices and compute platforms, from cloud to IoT, have exploded the cyberattack surface. Used by over 30,000 organizations, Nessus is a widely deployed security gold standard for vulnerability assessment.

OFFERINGS:

Tenable.ot (powered by Indegy) protects industrial networks from cyber threats, malicious insiders and human error. It provides industrial and critical infrastructure operations with the visibility, security and control needed to ensure ongoing, safe facility operation while reducing overall risk.

Tenable.ep fully integrates capabilities as part of one comprehensive solution for ultimate efficiency. It is a comprehensive, unified vulnerability management platform for the risk based revolution. It eliminates blind spots across the attack surface, including traditional IT assets, cloud services, operational technologies (OT), modern web apps, and remote workforce.

Managed in the cloud and powered by Nessus technology, **Tenable.io** provides comprehensive vulnerability coverage with the ability to predict which security issues to remediate first. In addition, it provides a complete end-to-end vulnerability management solution.

https://www.tenable.com

TOSIBOX®

Vendor of connectivity and cybersecurity, Tosibox has innovated the way ecosystems can connect, co-exist and collaborate in a single operational technology (OT) network infrastructure. Starting as easy as a single remote access solution through managed infrastructure, have been designed and applied for use by engineers for a ground 'up' approach while meeting IT and security standards.

Single infrastructure architecture for vendors to operate and control their assets, while the facility owner has peace of mind that their risk is mitigated and under control. This is accomplished through authorized, zero trust access between users (both internal and external), servers (both virtual machine and on-premise) and the edge.

Patented automated ecosystems are then created, allowing for smart layer integration and a common IT and OT environment. In addition, the automatic process allows for a streamlined and efficient data operation for users who need access to perform their daily functions from any location.

OFFERINGS:

TOSIBOX Lock 210 is an industrial router that serves as an endpoint for secure remote connections in OT networks.

TOSIBOX Lock 250 is an industrial router with integrated WiFi as a connectivity method or access point for wireless devices on-site.

TOSIBOX Lock 500 is a high-end connectivity device that brings various possibilities for customers to manage their operations and build new IoT solutions. It is ideal for demanding industrial environments and opens up new security and office networking sectors.

www.tosibox.com
mark.dilchert@tosibox.com
+61 424 445 395

Siga OT Solutions

SIGA provides operational technology (OT) cybersecurity, protocol-agnostic solutions based on Level 0 raw electrical conditioning monitoring. The Siga technology provides remote OT monitoring, anomaly detection and cybersecurity solutions for commercial, industrial, critical infrastructure, ICS and SCADA systems.

The Siga solution represents a paradigm shift in how early warning OT process anomaly detection systems operate – combining electrical signal-based advanced analytics, artificial intelligence, and machine learning.

Siga provides an OT anomaly detection solution that uses real-time monitoring of the raw electric signals. By directly monitoring these signals instead of data packets, the company can better bring visibility into the physical processes to support intelligent, real-time, business-critical decision-making.

OFFERINGS:

Higher resolution and better visibility of OT processes.

- Complete out-of-band solution, enabling cyber-resilient remote monitoring.
- AI anomaly detection engine for OT process resilience.
- Independent data archive for forensics and recovery.
- Autonomous solution, enabling the simplest, fastest and cost-effective implementation.

https://sigasec.com/
ilan.s@sigasec.com
+972 503 273 092

Tempered Networks

Tempered offers secure connectivity for vital infrastructure, industrial control systems, and the industrial Internet of Things (IIoT). The company recently announced it had built a purpose-built IIoT cybersecurity platform, enabling organizations to secure IIoT networks without the manual and financial overhead of firewalls, VLANs, ACLs (Access Control Lists), and VPNs (Virtual Private Networks).

Tempered Networks' solutions are used by a range of sectors, including water, energy, petroleum, manufacturing, and other industries.

OFFERINGS:

The **Airwall** solution makes it easy to create and maintain hyper-secure networks across complex infrastructure anywhere, including IT/OT/ICS/SCADA, remote and in the cloud. Delivering network segmentation and secure remote access, Airwall is a zero-trust software-defined perimeter that provides multi-factor authentication, comes micro-segmented, encrypted end-to-end, and is impervious to lateral movement.

Airwall Teams allows users to build truly private system-to-system networks that span public, private, cloud, and mobile networks, with just a few clicks using an intuitive graphical interface.

http://tempered.io
info@tempered.io
+1 (206) 452-5500

TrapX

TrapX provides an automated security grid for adaptive deception and defense that intercepts real-time threats while providing the actionable intelligence to block attackers. The company captures zero-day malware in its virtualized sensor network of honeypots and next-generation malware traps before the malware can inflict significant damage to customers' data centers or cloud deployments.

OFFERINGS:

The **Deception platform** delivers comprehensive protection, full visibility-at-scale, and MITRE ATT&CK integration for enhanced incident response and active defense. In addition, the company provides lightweight, touch-less technology offering non-disruptive support for an array of systems and devices, including IT, OT, IoT, SCADA, ICS, and SWIFT.

The **TrapX Flex** is a Deception as a Service (DaaS) solution that reduces remote worker risk with end-to-end visibility and control for security operations – from endpoints to the cloud and critical corporate assets. It also delivers fast time-to-value, including a hosted solution with 24×7 monitoring, analysis, and response services configured for remote worker environments.

https://www.trapx.com/
info@trapx.com
+1 (855) 249-4453

Tripwire

Tripwire protects organizations from damaging cyberattacks, keeping pace with changing technology complexities to defend against ever-evolving threats. In addition, the company helps organizations build solid foundations for security, compliance and operational excellence.

OFFERINGS:

Tripwire Enterprise is a security configuration management (SCM) suite that provides fully integrated solutions for policy, file integrity, and remediation management. The suite lets security, compliance, and operations teams achieve a foundational level of security across the enterprise, including on-premise, cloud and industrial assets.

Tripwire Industrial Visibility provides ICS operators with total clarity into the devices and activity on their network. It uses deep packet inspection, change management, event logging, and threat detection to help keep sensitive assets out of the reach of intruders.

Tripwire Device Profiler is a vulnerability scan engine appliance that can discover and profile every IP-enabled device on the network to determine the applications, services, operating systems, protocols, and vulnerabilities that may put an asset at risk.

https://www.tripwire.com/
+1 (503) 276-7500

Vdoo

Vdoo is a vendor of complex and increasingly critical product security space. With Vdoo, organizations can identify, prioritize, and mitigate various security issues. Founded in 2017 by a team of cybersecurity entrepreneurs and product security experts, Vdoo is now a global company with offices in Israel, the US, Germany, Singapore, Japan, with customers spread across various industries.

OFFERINGS:

The **Vdoo device security platform** is an automated platform that provides end-to-end product security. It helps development and security teams reduce time and effort while ensuring optimal product security. The platform addresses a diverse variety of security risks, including supply chain threats, configuration risks, standards compliance, and zero-day vulnerabilities.

The platform automates software security tasks throughout the product lifecycle, ensuring that findings are prioritized, communicated, and mitigated. In addition, its vertical-agnostic platform serves product security stakeholders and developers in a variety of industries, helping them reduce cybersecurity risks while creating new business opportunities.

https://www.vdoo.com/
info@vdoo.com, sgoldstein@vdoo.com
+972-76-5303021

Veracity

Veracity delivers a resilient, secure industrial network that provides an on-premises, centralized configuration, control, and monitoring solution that tracks all connected devices and their communications.

OFFERINGS:

The **Veracity Industrial SDN** network provides dynamic traffic control via the ability to enable or disable multiple traffic rules at a time. Upon installation, all traffic and devices are denied by default, and all attempted and seen communications between device pairs are displayed in the UI (user interface) by protocol.

Veracity's Controller is designed for operational and engineering efficiency with a logical workflow-based approach to network configuration, orchestration, security and resilience. It massively reduces the complexity of the network by repurposing the switch infrastructure to ensure communication between devices is determined by the system's design.

Veracity Net-Optix product helps protect infrastructure networks, as the growing presence of cyberattacks and the lack of protection for industrial networks and infrastructure systems at large is of growing concern. The company has designed Net-Optix to simplify and streamline the process of maintaining and updating security systems for infrastructure networks.

https://veracity.io/
info@veracity.io
+1 (888) 383-2397

Verve Industrial

Verve Industrial is an industrial control systems (ICS) cybersecurity company that partners with clients to bridge IT/OT security challenges in industrial environments across utilities (power, oil and gas, water), manufacturing, healthcare, and building controls.

OFFERINGS:

It provides secure ICS bringing together services with the **Verve Security Center (VSC),** a vendor-agnostic OT endpoint management platform. VSC begins with the industry's deepest asset inventory using a unique architecture going directly to the endpoint rather than relying on network traffic.

This provides a 360-degree risk view of each asset, including vulnerabilities, full patch status, AV and other protection elements, users & accounts and configurations. It also includes a comprehensive OT SIEM that identifies anomalous and risky endpoint behavior rather than only relying on network detections.

Perhaps the most important function is VSC's ability to take remediating actions directly from the platform, resulting in a comprehensive asset risk perspective, lowest TCO, and fastest time to remediate.

https://verveindustrial.com/
mganzer@verveindustrial.com
+1 (847) 287-6600

Waterfall

Waterfall Security delivers industrial cybersecurity offerings to protect critical industrial networks that revolutionize how industries protect physical assets and industrial processes from cyber attacks. The company's patented, unidirectional products enable safe IT/OT integration, remote monitoring and diagnostics, cloud connectivity, and tamper-proof forensics without the vulnerabilities that always accompany firewalled connectivity.

OFFERINGS:

Unidirectional Security Gateways create an impassable, physical barrier eliminating the possibility of external online attacks from reaching the industrial environment. Additionally, real-time access to information from the industrial site is made available through the product, enabling IT/OT integration, operational visibility by headquarters, vendor monitoring, industrial cloud services, and many other advanced and critical business needs.

Unidirectional CloudConnect acts as an industrial IoT gateway, collecting data from industrial sources, such as historians, industrial control systems, OPC servers, and industrial devices, then converting that data into a unified, cloud-friendly format. The CloudConnect then transmits the unified data securely out of the site and publishes it into the industrial cloud.

https://waterfall-security.com/
info@waterfall-security.com
+(972)3-9003700

Xage Security

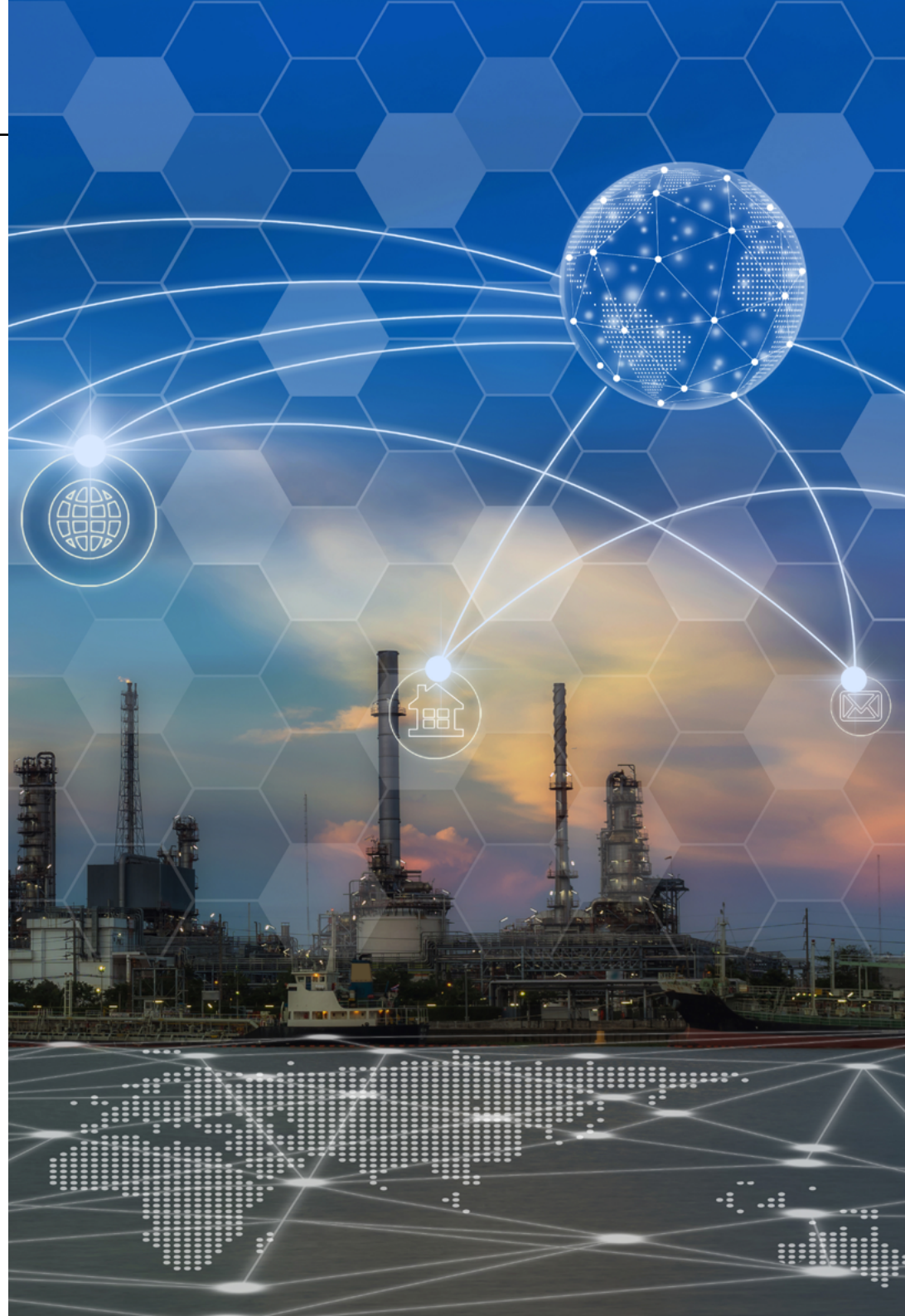
We are Security and IoT experts who created security products and industrial automation solutions used by global 1,000 companies. Using our experience enabling high growth markets, we deliver the only truly decentralized platform for protecting the Industrial Internet of Things. Xage delivers zero-trust identity and access management, securing existing systems and data while protecting on-site and remote-first digital transformation. The company offers operation-wide single sign-on and access that remains secure even in a network compromise. The Xage Fabric delivers comprehensive security for industrial and real-world operations. It protects every element, new or legacy, secures every interaction, local or remote, and enables dynamic data security for OT, IT and cloud.

OFFERINGS:

Xage provides the zero-trust solutions to cyber-harden operations and underpin transformational change, including:

- Identity and Access Management
- Zero Trust Remote Access
- Dynamic Data Security
- Device Lifecycle Management

https://xage.com/
hello@xage.com
+1 (650) 234-0400



TAKEPOINT RESEARCH

ABOUT TAKEPOINT

We empower our clients with actionable, incisive research to make even the toughest decisions a little easier. Collaboration is at the heart of our model and our mission is simply to deliver expert insight that has tangible value for your company.

Industrial Cyber

ABOUT INDUSTRIAL CYBER

Industrial Cyber is a publication dedicated to providing news and features on everything happening in Industrial Cybersecurity. It is a valuable meeting place for Industrial Cybersecurity professionals and cybersecurity experts, cybersecurity vendors and industry influencers, who learn from one another and shape the future of this dynamic and critically important market.

For more information on vendors and services providers, check out our Vendor Directory