

How to Choose the Right OT Security Solution in 2025

A deep dive into the breadth and depth of functionality modern industrial and critical infrastructure operations need to mitigate risk across OT environments.

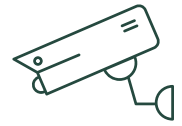




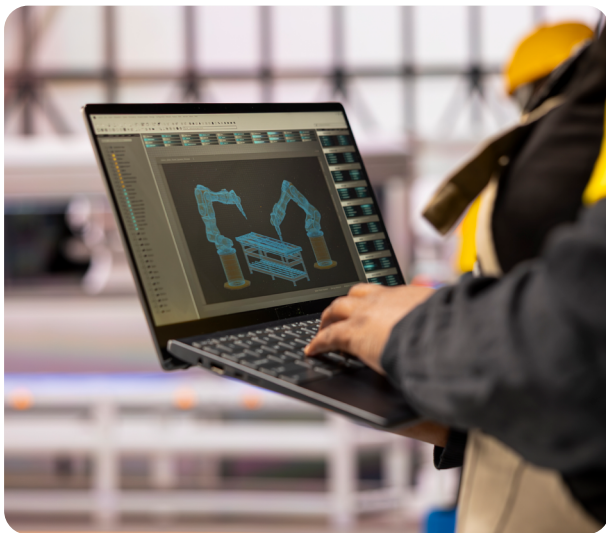
Table of Contents

How to Choose the Right OT Security Solution in 2025	1
Unlock Resilience with the Right OT Security Solution	3
How Operational Technology Breaches Occur	4
Impacts of OT Breaches	5
Riskier Systems Leave You Vulnerable	5
Disruption to Essential Services and Financial Losses	5
Reputational Damage	5
How OT Security Fits into the Industrial Cybersecurity Ecosystem	6
NIST CSF 2.0	6
The Purdue Model for ICS Security	7
The MITRE EMB3D Framework	8
Building a Secure Ecosystem in Heavy Industries: Integrations with OT Security	9
Core Components of an OT/ICS Security Solution	11
Inventory & Visibility	11
Must-Have Features for Inventory & Visibility	14
Vulnerability Prioritization	14
Must-Have Features for Vulnerability Prioritization	14
Risk Mitigation	15
Must-Have Features for Risk Mitigation	15
Threat and Response	16
Must-Have Features for Threat & Response	16
Governance, Risk and Compliance (GRC)	17
Must-Have Features for GRC	17
Checklist: How to Select an OT Security Solution	18
Why Manufacturers Choose Asimily	20
Better OT Security Leads to Better Strategic Outcomes for Manufacturing Organizations	21
About Asimily	22

Unlock Resilience with the Right OT Security Solution



Securing operational technology presents a unique challenge for most organizations. Industrial control systems (ICS) and connected equipment like water and wastewater treatment systems often run on outdated operating systems that are many years past their intended lifespan. This equipment often can't be updated easily with new software, if it's even designed to be updated in the first place.



Mitigating risk in the operational technology (OT) landscape requires unique considerations. These devices play a crucial role in manufacturing, utilities, and other heavy industries, and protecting them requires a deep understanding of the devices, how they're built, and the workflows associated with these environments.

These systems, such as assembly line robots, pipeline monitoring, and other technologies, are deployed with limited ability to remediate potential issues or even visibility from the IT side of the network. Moreover, these systems are often overly complex and rely on legacy software that is difficult to update even if one were made available. Given also a focus on high uptime, securing OT systems often takes the form of microsegmentation and air gapping to prevent attackers from reaching the machine in the first place.

Moreover, these systems regularly have extremely long lifespans. It's not uncommon for the same ICS or OT device to be used for 20 years or more. Any scans of a network may not even fully discover OT systems because they often are not connected to the internet in the same way as IT systems. This difficulty with discovering OT systems adds another layer of complexity to defending them.

Manufacturing is no stranger to resource constraints. Shutting down a production line to resolve a technology issue means that there is a direct negative impact on revenue, so often the focus is on OT uptime and quick resolutions to ensure that the final product gets out of the facility. Between raw material costs in the supply chain and trade policy shifts, manufacturing firms have a multitude of issues to contend with, even before getting into defending their OT. As the risk of cyberattacks targeted toward ICS continues to increase, the need to focus on securing these systems takes on more strategic importance as well.

The risk is ever-present, but so is the opportunity to achieve OT security and mitigate security risk for manufacturers and other heavy industries.

This guide will explore the key considerations that organizations must address to mitigate risk in their OT and ICS ecosystems. From compliance to utilization, we'll cover the functionality manufacturers require to measure and mitigate risk to their ICS technologies.

How Operational Technology Breaches Occur

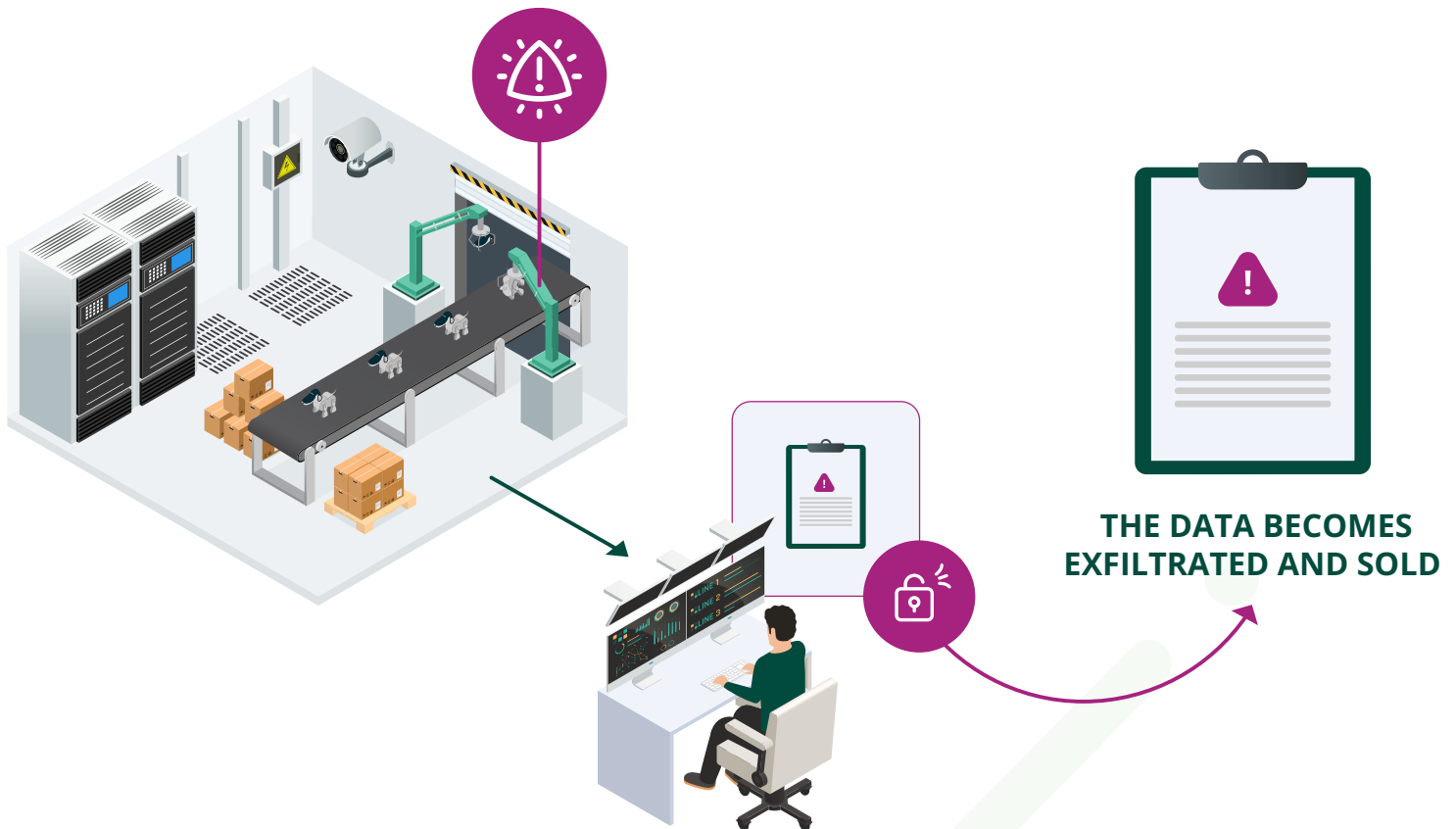


Operational technology has not historically been connected to the internet. Where they needed to be connected, there was heavy airgapping involved to enforce some natural separation from traditional IT assets like employee workstations. However, a drive toward efficiency has led to equipment like water quality monitoring systems and manufacturing equipment being connected to the internet for analysis, vendor access, maintenance, and other important functions.

There's a further issue because organizations have to balance safety and confidentiality in OT security. Given that these systems lack basic security features, essential processes such as applying patches or firmware updates can be difficult,

creating gaps that malicious actors can exploit. Yet, despite the criticality of deploying robust security measures, approximately 70% of organizations investing in OT cybersecurity encounter challenges with implementation, often due to complexities around integrating IT and OT environments.

This creates the possibility of OT systems being used as a stepping stone to access data stored in IT databases, which creates new attack pathways to defend. As the enterprise becomes more holistically connected, this becomes a serious possibility to protect against. As attackers find more hardened IT systems, their return on investment for attacking OT becomes more attractive.



Impacts of OT Breaches



The effects of OT breaches can be significant, particularly in terms of overall safety. Operational technology and industrial control systems govern critical infrastructure like power plants, water and wastewater facilities, and manufacturing facilities. If there is a breach and operations go down, the results could be catastrophic.



Riskier Systems Leave You Vulnerable

Riskier Assets Mean More Challenges: The Cybersecurity and Infrastructure Security Agency released nearly 2 dozen advisories about vulnerabilities in industrial control systems between mid-July and early August 2025. This aligns with a larger trend of threat actors targeting ICS or OT systems to breach company data.

Weaker Tech = More Issues: Because ICS and OT systems are a bigger focus for threat actors, they are starting to surface more vulnerabilities and craft more attacks targeting these systems. Organizations need to patch or keep their OT strictly protected.



Disruption to Essential Services and Financial Losses

Essential Services Disruption: Operational technology often powers critical infrastructure such as oil pipelines, water and wastewater treatment plants, or safety systems like temperature monitors. An attack on these ICS or OT systems risks disrupting vital services like water and power for communities..

Financial Losses: A cyberattack on an ICS or OT system can result in substantial losses for the company that owns the equipment. This takes the shape of paying to resume operations or, in cases like Colonial Pipeline, a massive loss to the balance sheet of the enterprise.



Reputational Damage

Negative Reputational Impacts: A successful OT breach can, and often does, result in a significant reputational impact for the organization. Many OT or ICS breaches occur within public utilities, so there isn't as much danger of customers cancelling, but the reputational damage of a breach can be severe regardless.

By highlighting these critical impacts, it becomes clear that cybersecurity in OT and ICS is not just about protecting data—it's about ensuring trust, maintaining a key level of service, and ensuring that these systems are protected.



How OT Security Fits into the Industrial Cybersecurity Ecosystem



Building an effective cybersecurity program can be confusing and complicated. It is often challenging to know where to start, especially with the complexity around OT security. Often, the most helpful tools for building a program are to map activities and protections to the compliance standards set by governing organizations. Industrial cybersecurity has had decades to generate guiding standards, models, and frameworks.. Some of these include ISA/IEC 62443, NIST SP 800-82 (part of the NIST Cybersecurity Framework (CSF)), the Purdue Model for ICS Security, and the MITRE EMB3D Framework.

These frameworks serve as the beginnings of an ICS or OT security program. They are not the only controls that security professionals must put in place, but they are a good first step.

NIST CSF 2.0

The NIST Cybersecurity Framework (CSF) Core is structured around six fundamental pillars that form the backbone of a robust cybersecurity strategy. These pillars, designed to be implemented concurrently, foster a comprehensive cybersecurity culture within organizations. Each pillar encompasses specific objectives and sub-components, tailored to address various aspects of cybersecurity. While not specific to ICS/OT, this framework can nevertheless be readily applied to these technologies. NIST SP 800-82 is specific to ICS and OT and helps tailor the more general guidance of CSF 2.0 for industrial devices.

The Six Pillars of NIST CSF

PILLAR	DESCRIPTION	NUMBER OF COMPONENTS
 Governance	This function establishes the foundation for cybersecurity risk management. It involves setting, communicating, and overseeing the organization's cybersecurity strategy, expectations, and policies.	30
 Identification	This pillar focuses on developing a clear understanding of the organization's current cybersecurity landscape and potential risks.	44
 Protection	Here, the emphasis is on implementing and maintaining appropriate safeguards to mitigate identified cybersecurity risks.	11
 Detection	Involves the timely discovery and analysis of potential cybersecurity threats and breaches.	22
 Response	This pillar outlines the necessary actions to be taken when a cybersecurity incident is detected.	13
 Recovery	Outlines the restoration of assets and operations that may have been impacted by a cybersecurity incident.	8
Total		128

These six functions are each broken down into granular and specific components, specifically outlining how organizations can create a holistic approach to cybersecurity that addresses prevention, detection, and recovery aspects. This framework provides a flexible and adaptable structure that can be tailored to meet the specific needs and risk profiles of different organizations, regardless of their size or industry.

NIST SP 800-82 (or NIST SP 800-82r3 as of 2025) provides an overview of the typical system topologies seen in ICS/ OT environments, aids in threat model development by considering common threats in these environments. Further, it addresses typical vulnerabilities and provides recommendations on safeguards and countermeasures, including a “walk-crawl-run” approach to take into account the varying levels of cybersecurity maturity across the industry (in Appendix F of the [NIST publication](#)).

The Purdue Model for ICS Security

The Purdue Model for Industrial Control System Security was initially designed as part of the Purdue Enterprise Reference Architecture (PERA), which is commonly used in computer-integrated manufacturing (CIM). The Purdue Model is leveraged most commonly in factories that are completely automated and has come to define one of the main standards in securing operational technology.

The Purdue Model is split into six zones, which contain information technology (IT) and OT systems. When implemented properly, the Purdue Model establishes an “air gap” between ICS/OT and IT systems, isolating them so an organization can enforce effective access controls without hindering business.

Zone Level	What It Covers
Level 4-5 Enterprise System Zone	This is the zone that features traditional IT systems like workstations.
Level 3.5 Demilitarized Zone (DMZ)	This zone includes security systems like firewalls and proxies, and is meant to provide separation between IT and OT. It can also be used as a way for the two layers to communicate bidirectionally.
Level 3 Manufacturing Operations Systems	This layer includes custom OT devices that run operations on the manufacturing floor, such as Manufacturing Operations Management and Data Historians.
Level 2 Control Systems Zone	Systems that supervise, monitor, and control physical processes, like SCADA software, distributed control systems, and human-machine interfaces.
Level 1 Intelligent Devices	This level includes systems that send instructions to devices in Zone 0. Programmable logic controllers and remote terminal units are common devices in this layer.
Level 0 Physical Processes	This lowest zone contains the sensors, actuators, and other machines responsible for all the physical processes, like assembly and lubrication. A lot of modern sensors communicate with monitoring software via cellular networks.

This model is on the older side, first unveiled in 1992, and often bypassed because Zone 0 sensors can communicate directly with monitoring software now. There are debates about the relevance of the Purdue Model as a result of this. However, the reality is that the model still offers a consolidated

approach for how to think about the segmentation in OT and ICS technologies. For example, the Zone terminology alone is universally understood and a simple way to characterize the “location” of a device in an industrial setting.

The MITRE EMB3D Framework

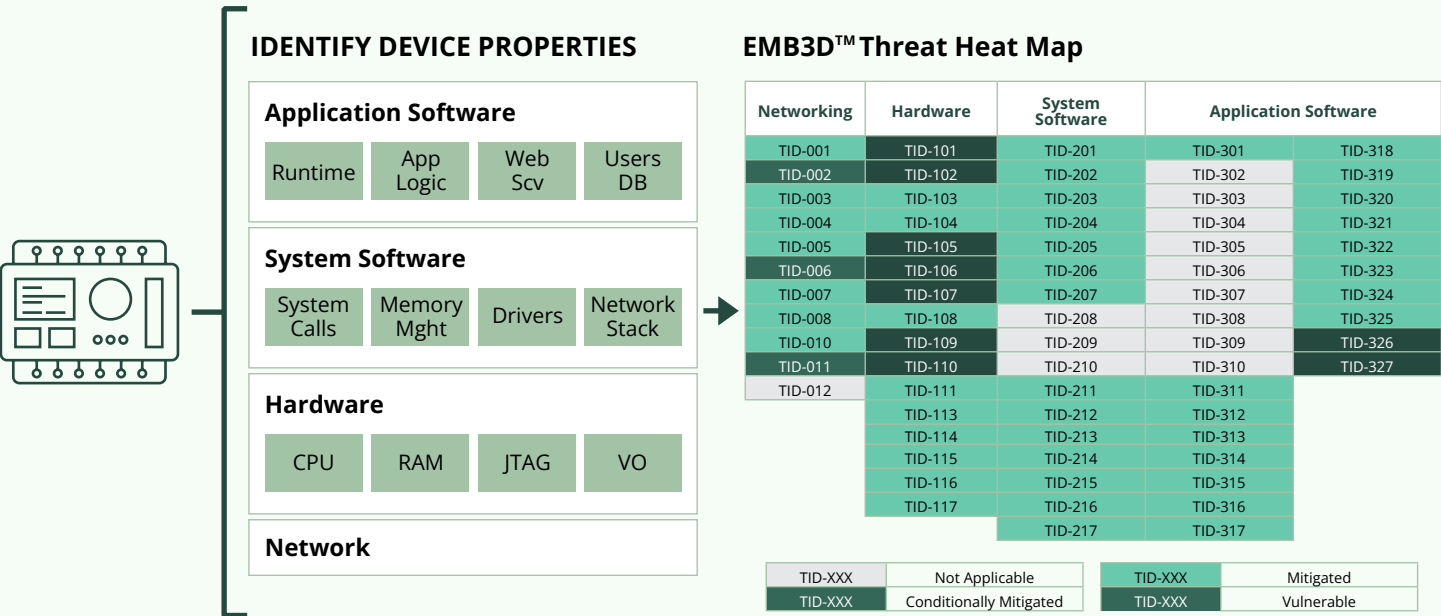
First announced in December 2023, the MITRE EMB3D Framework is a threat model specifically designed to cover embedded devices within critical infrastructure industries. The goal is to provide a shared and cultivated knowledge base of cyber threats to embedded devices, along with security mechanisms to mitigate these threats.

Within the EMB3D framework, there are three main categories to examine:

Device properties that describe a device’s hardware and software components and its capabilities, such as physical hardware, network services and protocols, software, and firmware. Each set of device properties is divided into sub-properties mapped to a set of threats. Mapping properties directly to threats means that users can identify which device is potentially vulnerable to which attack. This also empowers teams to understand which kinds of threats they may need to defend against.

EMB3D threats describe how threat actors can achieve their objective or affect a system or device. Each of the threats within MITRE EMB3D includes (i) information about the targeted technical features; (ii) the actions that must be taken, including what will happen when the threat is successful; and (iii) the vulnerabilities or weaknesses that the mechanism has to have in order for the threat to succeed. The EMB3D framework also relates to the MITRE ATT&CK Framework for ICS, which includes TTPs like changing a controller’s operating mode to evade detection and using a connection proxy to direct network traffic between systems.

Mitigation strategies and techniques for each threat. These are valid both for device owners, who can use mitigation strategies to prevent and reduce the risk of a threat, and end users who can use them to validate that devices are sufficiently protected. The mitigations define the mechanisms or technologies that can defend against the threat while also providing flexibility in how mitigations can be implemented within any unique device constraint.



Source: MITRE Corporation

Building a Secure Ecosystem in Heavy Industries: Integrations with OT Security

SOLUTION TYPE/CATEGORY	WHAT IT IS & WHAT IT SECURES	HOW OT SECURITY SOLUTION INTEGRATES/RELATES
 Network Security	Firewalls and Intrusion Detection/Prevention Systems: Implement next-generation firewalls (NGFWs) and intrusion detection/prevention systems to control network traffic and detect malicious activities. Virtual Private Networks (VPNs): Use VPNs to secure remote access for employees working off-site	OT security needs to monitor network traffic and ensure that only approved monitoring solutions are communicating. Network access control (NAC) and segmentation are key factors in strong OT security. Segmenting OT onto its own, separate networks from IT can avoid a substantial amount of potential risks.
 Vulnerability Scanners	Vulnerability Scanners: Vulnerability Scanners actively send queries to endpoints (or software agents installed on them) to get information about their state and configuration. This can be used to detect vulnerabilities.	Vulnerability scanning often isn't done in OT environments, largely because scans present the risk of disrupting operations. Scanners typically regurgitate voluminous information about <i>potential</i> exploits. Any vulnerability scanner should filter out irrelevant or non-exploitable CVEs from those results, reducing or eliminating time-consuming tasks that don't really reduce risk much. It should also enable you to configure no-scan lists to ensure devices that shouldn't be scanned aren't.
 OT Asset Management	Operational Technology Asset Management: Traditional security tools, like an Endpoint Detection & Response offering, are too invasive for many OT devices. Rather, leveraging a tool that can monitor for suspicious activity is more effective.	These asset management solutions should tie into monitoring solutions for a common inventory of all devices.
 Data Protection	Backup and Recovery: Implement regular data backup and recovery processes to protect against data loss and ransomware attacks.	OT solutions should be able to detect anomalous behavior from monitored devices, receive updates, and allow for easily made (no coding) custom rules for industry-specific and novel attack types.

SOLUTION TYPE/CATEGORY	WHAT IT IS & WHAT IT SECURES	HOW OT SECURITY SOLUTION INTEGRATES/RELATES
 Access Management Solutions	Multi-Factor Authentication (MFA): Implement MFA to add an extra layer of security for user authentication. Privileged Access Management (PAM): Control and monitor access to sensitive systems and data, following the principle of least privilege. Identity and Access Management (IAM): Use IAM solutions to manage user identities and access rights across the organization.	Access management tools can help with the IT solution monitoring OT systems. Limiting access based on permissions is crucial to ensuring data security. These should support SSO policies.
 Compliance & Risk Management Tools	Governance, Risk, and Compliance (GRC) Tools: Implement GRC solutions to manage regulatory compliance and track overall security posture.	OT tools should be able to set custom policies based on compliance and governance standards for your unique environment.
 SIEM & SOC	Security Information and Event Management (SIEM): Implement SIEM solutions to collect and analyze security data from various sources. Threat Intelligence Platforms: Use threat intelligence to stay informed about emerging threats and vulnerabilities.	OT security tools need to integrate data into your SIEM for more centralized visibility into your full technology architecture.
 CMMS, EAM & CMDB	Computerized Maintenance Management Systems (CMMS), Enterprise Asset Management (EAM), and Configuration Management Databases (CMDB) all help organizations manage, maintain, and service physical assets.	Your OT solution should sync data between the CMMS/CMDB, helping keep them up-to-date with any changes. In some cases, this can also mean automatically creating work orders for issues like anomalies and vulnerabilities.
 IPAM	IP Address Management: These tools monitor and manage a network's IP addresses.	Keep track of devices as they move across the network – this improves device classification and vulnerability assignment. This can include real-time location systems (RTLS) integrations.

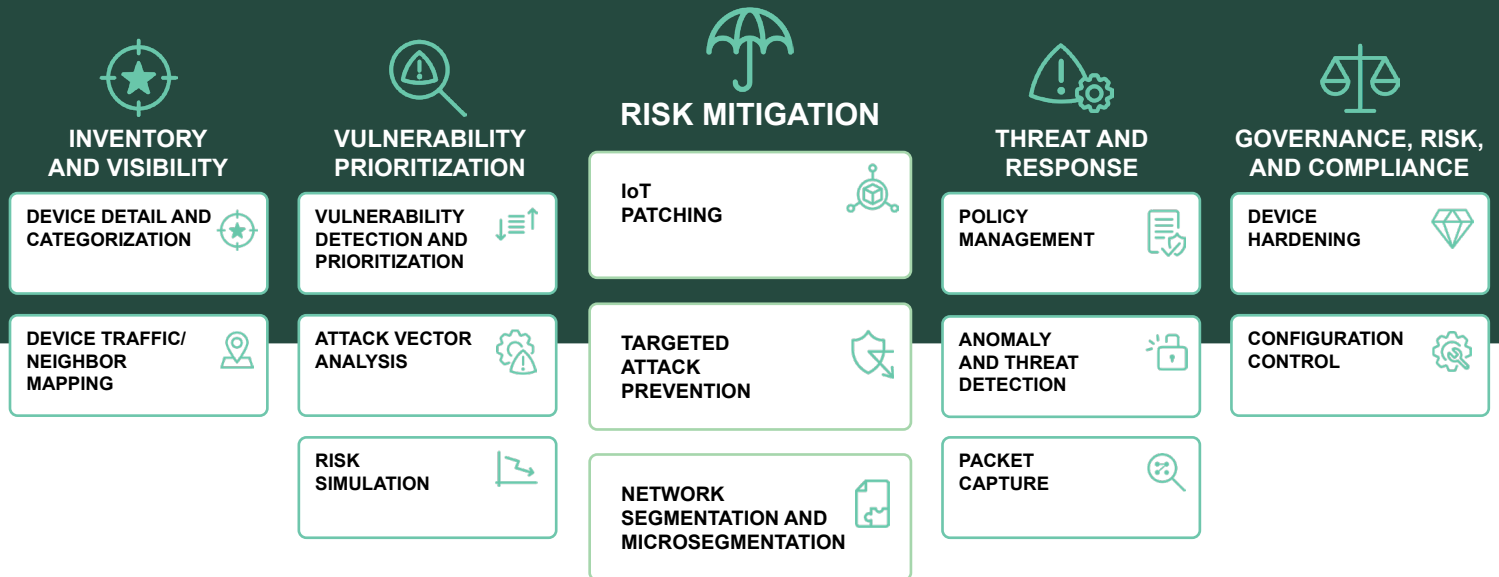
Integrations and workflow management reinforce the notion that OT security does not exist in isolation from other solutions. OT/ICS security solutions should work to create a single pane of glass for device visibility and cybersecurity.



Core Components of an OT/ICS Security Solution



The key features of an OT/ICS security solution mirror the device security lifecycle.



Inventory & Visibility

A meaningful inventory is a long, detailed, and classified list of all OT and ICS devices that includes data, including:

- ✓ Manufacturer
- ✓ Model
- ✓ Criticality Score
- ✓ Crown Jewel Identifier
- ✓ Purdue Zone | Level
- ✓ Possible Vulnerabilities
- ✓ Expected Communication Behavior
- ✓ Port Numbers
- ✓ Applications
- ✓ Hostname
- ✓ Version Number
- ✓ Operating system, firmware, and software
- ✓ Configurations



You cannot secure what you cannot see.



A comprehensive asset inventory enables you to gain insight into security posture; you can also use it to discover older technologies that should be replaced, pass audit inventory requirements, and identify how to optimize connected equipment to better serve business needs. With visibility into the various manufacturers and device types, organizations gain more valuable information crucial to mitigating risk and making technology investments to identify where potential risks might exist. Leveraging a purpose-built OT and ICS security solution provides additional context into these devices, and the network is crucial.

For OT devices, a passive analysis of network traffic without actively pinging devices is critical to mitigate the risk of service outages. Blind active scanning can cause outages and impact functionality for these devices, which results in critical insight. Many tools feed into a comprehensive asset inventory, but a purpose-built OT/ICS security solution will reference these data sources in addition to its own methods for understanding the devices on a network.

These safe methods include passive scanning and discrete protocol-based device querying for additional information. Discretion in this case means having prior knowledge of the existence of an OT and ICS device, how it communicates, and how to have it securely give a security solution information about the OT or ICS device itself.

It is possible to perform safe active scanning on OT and ICS devices, but the traditional active methods of directly engaging with the endpoint pose substantial operational risk. Instead, a more efficient method of active scanning for OT involves using specific active queries that leverage specific protocols such as CIP, Modbus, and S7Comm with special messages and instructions that return useful information.

Must-Have Features for Inventory & Visibility



Complete Device Classification and Enrichment

Asimily leverages multiple sources to build a clear picture of each device, populate its record with details such as firmware versions and serial numbers, and determine its context within the network. Asimily's deep packet inspection and protocol analyzer combine to provide organizations with better device categorization along with network context, to help mitigate risk.



AI/ML Traffic Analysis & Neighbor Mapping

Manufacturing organizations need to understand the quantity, type, and destinations of traffic to and from the device. This is especially important with remote monitoring solutions. Understanding a device's traffic in the context of the network provides crucial security insights. To help with this, Asimily leverages machine learning to analyze this traffic and build a comprehensive picture of the device and its use in your unique environment. This helps prioritize the riskiest vulnerabilities, such as ones that affect devices with significant network access compared to ones with minimal network access.



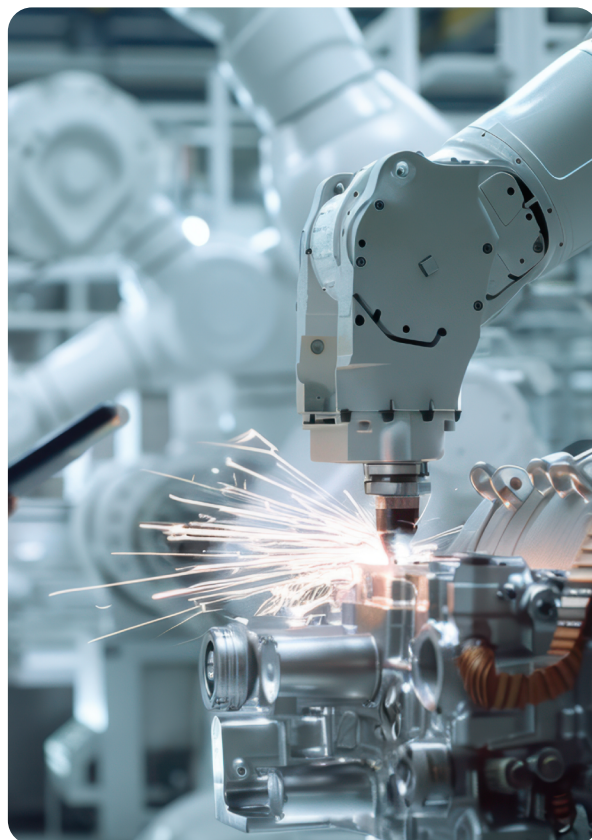
Deep Packet Inspection – Asimily’s deep packet inspection capabilities track protocol-specific information via either safe active scanning or passive scanning, leveraging the intelligence from common OT protocols. This agentless functionality ensures that organizations don’t need to have sensors installed to collect inventory information. It can also build plant-level or business-level insight, which is key for distributed operations. Deep packet inspection from Asimily thus ensures that security teams remain informed about their inventories.



Unified Inventory – By using any of the out-of-the-box software integrations with Asimily (or Asimily’s API), your entire asset inventory and/or security stack can come closer to the elusive single source of truth. Asimily can ingest from multiple sources (vulnerability scanners, SIEM, CMDB, etc.) as well as share its own information.



Device Usage Tracking – One of the benefits of a comprehensive asset inventory built on next content is that critical infrastructure companies can gain insights into utilization metrics. This can inform capital planning decisions – if a sensor in a different part of the facility is seldom used, an organization can verify this through Asimily. This ultimately can lead to greater efficiency through deferred capital expenditure spending and purchasing the best equipment for your needs.





Vulnerability Prioritization

A single repository of devices that can then be used to inform vulnerability prioritization would be transformative for manufacturing and other critical infrastructure industries. This is sorely lacking in the OT/ICS landscape, and it doesn't help that traditional scanning technologies born in the more robust IT world to identify vulnerabilities can cause service interruptions in OT/ICS environments. Purpose-built OT security solutions will typically start to show vulnerability information for each device on the network once an inventory is built.

Too often, vulnerability information in the industry stops with only the easily accessible and basic information that a vulnerability is present. Understanding which vulnerabilities are the most important gets them closed fastest, ahead of attackers. That takes contextual knowledge of what OT/ICS are doing, including the impact of their going down and the likelihood of an exploit using that vulnerability happening.

Not every vulnerability detected for each device is going to be exploitable in your network. For example, a device on your network with a 10.0 CVSS score that isn't connected to any critical systems and isn't utilized is less likely to cause a breach.

Must-Have Features for Vulnerability Prioritization



Risk Simulation – Similar to vulnerability prioritization, Asimily provides you with the ability to simulate the risk reduction benefits of a given remediation action, enabling you to map the efforts of risk remediation to the desired outcome. This is especially crucial in forecasting which resources will be needed to reduce risk to meet organizational cybersecurity goals.



Vulnerability Enrichment – Asimily examines the exploitability of a vulnerability contextually within the network. This measure involves cross-referencing multiple sources like the MITRE ATT&CK and EMB3D Frameworks, Software Bills of Materials provided by device manufacturers, CVEs, and more. By referencing these sources and analyzing them within the context of your network, **Asimily provides a prioritized list of vulnerability remediation activities ranked by impact and likelihood, empowering you to mitigate real risk with actionable advice.**





Risk Mitigation

Once a vulnerability has been prioritized, it still needs to be remediated. While all aspects of a comprehensive OT/ICS security solution should feed into holistic risk mitigation, key features make risk mitigation an actionable task for users, directly within a platform. In particular, when faced with a new vulnerability, there are 3 major ways to respond.

Must-Have Features for Risk Mitigation



Network Segmentation & Microsegmentation

– If simpler, easier, faster methods fail, then the last resort is typically network segmentation, which can aid in preventing attackers from accessing OT systems. Performing microsegmentation can be very intricate, which makes it necessary to plan for multiple possibilities. Asimily helps teams guard against exploitation in addition to vulnerabilities.

1. Based on the inventory analysis and understanding of the network, Asimily determines actual network traffic to create a baseline and visualize devices and behavior.
2. Asimily enables users to choose between manual and automated methods to deploy new network rules quickly and easily.
3. Prior to deployment, Asimily can validate planned segmentation to account for logical groupings and legitimate outliers in a manufacturing setting.



NEW FEATURE

Patching – One of the best ways to mitigate risk is by patching known vulnerabilities as they arise. While patching is notoriously challenging to manage, implement, and scale, Asimily includes patch recommendations when offering remediation guidance to users. For IoT devices in OT/ICS environments, Asimily can also directly deploy patches. Advanced features such as scheduling them to deploy during a downtime window, patching devices in bulk, and automating patching are also available. This saves time and ensures that devices have been hardened per the manufacturer's guidance.



Targeted Attack Prevention – Broad macro and microsegmentation are critical tactics for mitigating risk, but can be costly and time-consuming to implement for some organizations. Targeted segmentation from Asimily uses exploit vectors to find the simplest fix that stops an exploit (using a prioritized vulnerability) from succeeding. This requires a deep analysis of each vulnerability and finding the weak point, which most industry solutions do not do - they simply report the vulnerability is present and perhaps classify it using the MITRE ATT&CK Framework. That's not the same as finding a weak point in an exploit.

Asimily will suggest the way to stop the exploit chain while still allowing the ICS or OT environment to function normally. An example would be turning off a service that an exploit needs but the device does not, which occurs when a manufacturer allows equipment to leave their factories with unnecessary access.



Threat and Response

It's necessary to prepare for the possibility of an attack. Doing this ensures that you can shield critical OT and ICS devices against cyber attack, but only if you plan effectively. IT teams need to work with plant management on scheduling routine system evaluations to mitigate cyberattacks and reduce their impact on core functionalities, including those that involve IoT and OT. In the context of OT, there are key components that security solutions must contain in order to effectively mitigate risk in the realm of threat detection and incident response.

Must-Have Features for Treat and Response



Anomaly and Threat Detection – With Asimily's network traffic analysis, rogue behavior can be seen quickly. Users are able to identify any unusual connections or strange behaviors as they appear on the network, keeping up with constantly shifting attacker techniques from groups like Volt Typhoon or ScatteredSpider. By alerting to anomalous device behavior, Asimily helps prevent threats before they can compromise technologies.



Threat Intelligence – Integrated threat intelligence is vital for effective defense. Knowing which threat actors are running active campaigns targeting OT systems and having that information readily at hand is necessary. Asimily integrates more than 100 data sources, including VirusTotal and EPSS, ensuring that security teams are kept up to date on OT threat activity.



Policy Management – Each manufacturing organization's network is different. As a result, Asimily has developed a policy engine that empowers you to set custom device behavior rules. These rules can detect threats in the context of your network, and can alert, trigger actions, or both.



Packet Capture – If an incident were to arise, Asimily's packet capture functionality starts the data gathering needed for a successful incident handling process. It takes the traffic from any device and captures it for forensics – either automatically or manually, depending on the rules you set.



Governance, Risk and Compliance (GRC)

Manufacturing and other critical infrastructure organizations are not as highly regulated as some companies, but that does not limit the value of governance, risk, and compliance (GRC). Most of the focus remains on highly regulated industries like financial services and healthcare, but the reality is that GRC can help structure programs and enable easy audit trails while also mitigating risks and tracking controls.

Must-Have Features for GRC



Configuration Control – Configuration drift remains a major concern for fixed-function devices like OT/ICS systems. These seldom-detected changes can often open the device up to new risks. With Asimily, teams can take a snapshot of a device's known good state and set alerts if it deviates from that configuration. You can then revert the device back to the last known good state, which will restore its functionality.



Device Hardening – Device hardening is a crucial step in securing your OT system. It's easy to make the mistake of thinking that air-gapping the system is enough to protect it, but the reality is that any configuration can change for any variety of reasons. These changes, which are seldom detected, can open the device up to new security risks. Configuration snapshot is a key Asimily capability that helps keep configurations in the best possible state. The device configuration offering enables you to take a snapshot of a device's known good state and set alerts if a device deviates from that known good configuration. You can also revert the device to the known good state, restoring its functionality if the configuration is changed. This is a crucial feature as most audits require documentation of these deviations as well as the ability to revert changes back.



Reporting – The ability to provide rich reporting is vital for GRC, especially with regard to proving compliance with standards. Audit-ready reporting can be transformative for meeting regulatory requirements, and also for communicating up to the board or senior leaders in an easily digestible format. Asimily includes many types of reports for security professionals to deliver, in multiple formats. Users can leverage PDFs, PowerPoints, or other file formats to report on their activities and show their compliance with corporate policies as well as regulations.



Checklist: How to Select an OT Security Solution

Asimily OT RFP Template

	Requirement Description	 asimily	Vendor 2	Vendor 2
A.Visibility and Classification				
A1	The solution passively collects asset data using both an AI/ML analysis of network traffic patterns and comprehensive deep packet inspection, to create and maintain a classified asset inventory safely.	X		
A2	The solution ingests outside data sources to create a higher-quality asset inventory (e.g. from vulnerability scanners, CMDBs, DHCP services, SNMP, etc).	X		
A3	The solution quickly parses new device communication protocols, enabling you to easily add future manufacturers or devices to the asset management system.	X		
A4	The solution exposes devices immediately when detected – even before precise classification –to assist with Shadow IT problems – with no supplemental human analysis needed.	X		
A5	The solution can identify, capture, and monitor operating systems, applications, firmware versions, and patch levels present within the IoT and OT inventory.	X		
A6	The solution can discover and inventory serial-attached devices and understand parent-child relationships.	X		
A7	The solution supports the detection of legacy operating systems that are no longer under manufacturer support.	X		
A8	The solution accurately classifies and categorizes devices.	X		
A9	The solution does not require agents to generate inventory and classification.	X		
A10	The solution can alert when a new device is discovered.	X		
A11	The solution allows users to fully customize the way devices are grouped beyond pre-determined sets chosen by the vendor (e.g. Crown Jewels, Manufacturing Area, or Line).	X		
B.Vulnerability Mitigation A.Visibility and Classification				
B1	The solution uses the National Vulnerability Database (NVD) and manufacturer sources to find new vulnerabilities – enabling quick responses to shorten exposure should an exploit arise.	X		
B2	The solution uses the widely understood MITRE terminology for vulnerability description.	X		
B3	The solution analyzes vulnerabilities using the MITRE ATT&CK framework to identify the highest-priority vulnerabilities by eliminating lower-priority and non-exploitable vulnerabilities based on the specific context (network, configuration) of each device.	X		
B4	The solution analyzes SBOM data to enhance the vulnerability mitigation process.	X		
B5	The solution reduces or eliminates false positives both within the platform and from other vulnerability management tools – creating a source of truth for vulnerability mitigation progress.	X		
B6	The solution creates ACLs based on your unique environment to aid in zero-trust efforts and simplify the process of making networks more secure for devices.	X		
C.Vulnerability Remediation				
C1	The solution provides targeted remediation guidance by surfacing the simplest action that reduces the most risk while blocking the attack chain of a specific vulnerability – enabling organizations to reduce risk and maximize scarce remediation resources – beyond segmentation and patching.	X		
C2	The solution simplifies remediation by providing an actionable list of what to do next ranked by risk, which is based on Potential Impact and Likelihood of exploitation.	X		
C3	The solution assists in preparing for regulatory compliance to minimize exposures and financial liabilities.	X		
C4	The solution ensures no operational impacts will occur when remediation recommendations are implemented.	X		
C5	The solution supports the ability to assign remediation tasks to specific users.	X		
C6	The solution includes a Risk Simulator that shows how each mitigation effort will reduce risk overall within the context of your environment, to efficiently prioritize scarce remediation resources.	X		

	Requirement Description		Vendor 2	Vendor 2
D. Threat Detection & Incident Response				
D1	The solution analyzes devices' network traffic to detect anomalies that may indicate indicators of compromise, malicious activities, and alerts based on anomalous behavior.	X		
D2	The solution vendor offers new rules in response to new threats (e.g. zero-days).	X		
D3	The solution allows detected potential threats to trigger actions, such as quarantining or alerts to manage the response and recovery efficiently.	X		
D4	The solution enables you to create rules for anomaly detection with or without programming skills (e.g. in languages such as YAML).	X		
D5	The solution can capture packet-level traffic for any device for later forensic analysis, automatically or manually.	X		
D6	The solution enables you to retain packet-level traffic capture data in your preferred storage location. (e.g. sftp://###.###.###.###/pcaps)	X		
D7	The solution provider offers the capability to detect unauthorized traffic between IT-OT as well as external communications to protected OT areas.	X		
E. Configuration Control				
E1	The solution enables you to capture a snapshot of a device's 'known good configuration' to better recover in the event of configuration changes or ransomware attacks.	X		
E2	The solution enables you to create both bulk and automatic configuration snapshots of large numbers of devices by setting automated rules and parameters.	X		
E3	The solution regularly checks for configuration drift, alerting if a device has drifted from the preferred configuration.	X		
E4	The solution provides a configuration comparison view, showing configuration changes down to the parameter level when configuration drift occurs (including tracking additions and removals).	X		
E5	The solution provides a timeline view to assist an investigation into the causes of configuration drift.	X		
F. Risk Modeling, Reporting & Operational Efficiency				
F1	The solution generates an organizational risk score that is easy to understand and summarizes the organization's overall device risk level.	X		
F2	The solution can simulate device risk using both theoretical and actionable recommendations, enabling you to see how specific changes will immediately reduce the current risk.	X		
F3	The solution provides accurate device utilization metrics based on a custom expected usage window (e.g. during business hours vs 24/7)	X		
F4	The solution provides collaboration features to allow individual users to share context regarding device details, analyst notes, etc.	X		
F5	The solution provides a customizable user area to track assignments and ownership of workloads, devices, and tasks.	X		
F6	The solution provides access to a device location (or integration to a location solution) to assist with real-time asset location.	X		
F7	The solution supports central management for multi-location/region deployments through region tagging.	X		
F8	The solution enables custom alert suppression and alert prioritization to reduce alert fatigue/alert storms.	X		
F9	The solution can be configured to generate custom repeated alerts until the alert is addressed.	X		
F10	The solution enables you to schedule reports to be delivered to specified members of the organization via email.	X		
F11	The solution supports customizable dashboard reporting capabilities so each user can have their own preferred view of key data.	X		
F12	The solution runs on a variety of virtual or physical platforms and supports on-premise or Cloud deployments.	X		
F13	The solution includes cloud support and hosting options for the backend server in both public and private cloud environments.	X		
F14	The solution supports manual or imported/exported device tagging.	X		
G. Integrations				
G1	The solution provides a comprehensive list of integrations to allow organizations to use their preferred software stack with the workflows currently in place.	X		
G2	The solution provider can quickly add new integrations based on the organization's preferred security stack.	X		
G3	The solution offers a REST API to enable cohesion between different software components – creating efficient workflows and reports.	X		

OT Case Study: Why Manufacturers Choose Asimily

THREAT AND RESPONSE

- Set intelligent policies to thwart known exploits from spreading to additional devices
- Automate packet capture for forensic analysis of any connected device to support root cause analysis and reduce Incident Response costs

WORLD-LEADING RISK MITIGATION

- Block attacks with guidance on how to group devices in any combination to segment or micro-segment
- Recommendations to mitigate attack vectors outside of segmentation and patching
- Speed up IoT patching and password management of devices with a click of a button

Why Organizations Choose the Asimily Platform

GOVERNANCE, RISK, AND COMPLIANCE

- Prevent risk before purchasing with risk modeling and device hardening guidance
- Control configurations with snapshots of every device which can be used for recovery, including for ransomware
- Detect drift in device configurations and scroll through their timelines to detect causes

VULNERABILITY PRIORITIZATION

- Identify the top 2% riskiest devices in the environment for immediate risk reduction
- See Risk ROI for any given action before taking the time with Risk Simulator

INVENTORY AND VISIBILITY

- Gain a complete repository of IoT, OT, IoMT and IT devices while finding “unmanaged” devices
- Safely gather data on devices by using passive, protocol-based, API-based, or a combination of techniques applicable to your environment

Better OT Security Leads to Better Strategic Outcomes for Organizations



The advantages of a robust OT security strategy extend far beyond protection against cyber threats. Robust cybersecurity practices ensure that manufacturers and other heavy OT users maintain uptime and improve operational efficiency. This happens by minimizing both the downtime associated with successful attacks and by greater control over downtime from necessary cybersecurity maintenance windows. This ensures manufacturing can help service strategic goals – such as flexibility and higher customer satisfaction – while staying operationally efficient.

A comprehensive OT and ICS security approach can significantly enhance operational efficiency and ensure long-term operational health. This can extend to maintaining optimal utilization, improving machinery lifespans, and making data-driven decisions about technology investments. This level of visibility not only improves security but also streamlines procurement processes and reduces administrative costs – impacting capital expenditure for the entire organization.

CASE STUDY

Leading Food Manufacturer Selects Asimily as the Vendor of Choice to Secure OT Manufacturing Line



Leading Food Manufacturer required a solution that would:

- Passively scan their network for OT and IoT devices, resulting in no operational impacts or downtime, while providing the same level of detailed information on each device and behavior.
- Surface valuable device and vulnerability data, enabling them to address the riskiest devices and reduce risk quickly.
- Provide straightforward remediation steps for critical vulnerabilities, ensuring actionable next steps validated to reduce risk.

This leading food manufacturing organization operates eight locations in the Pacific Northwest. As a large manufacturer, any downtime for the manufacturing line can be catastrophic, resulting in a \$1M loss in restarting the line for every hour of downtime. With Asimily, the organization can seek to prevent downtime while reducing risk across their connected devices.

A truly holistic OT/ICS security strategy makes manufacturers and other critical infrastructure adopt a more proactive mindset. Instead of reacting to security incidents as they occur, this approach encourages continuous monitoring, optimization, and improvement of the entire OT/ICS ecosystem. By regulating operational behavior and maintaining stable operations, manufacturing organizations and other critical infrastructure can ensure

optimal performance and longevity of their OT/ICS technologies.

Ultimately, this proactive stance not only enhances security but also contributes to operational resilience, predictability, and long-term sustainability for OT and ICS architectures as they are increasingly under attack from adversaries.

About Asimily

Asimily provides the only complete IoT, OT, and IoMT Risk Mitigation platform. It has the depth and breadth of capability to keep all devices secure, including visibility, vulnerability prioritization, risk mitigation, threat response, and Governance, Risk, and Compliance. Asimily provides protection for the entire lifecycle of connected devices.

The company's solutions are deployed at major hospital systems globally and in the U.S., including Methodist LeBonheur Healthcare, Tufts Medicine, MemorialCare, and more.

Founded in 2017 by cybersecurity experts from Symantec and other top firms, the company has differentiated itself through its technology. Through sophisticated OT, IoT, IoMT, and more device scanning, Asimily's platform discovers and classifies all connected devices within networks (using the largest repository of device metadata and capability information on the market). Using Asimily's proprietary machine learning-based technology, Asimily predicts which OT devices are most critical and which are most likely to face a successful attack. Asimily baselines and profiles technology behavior, and detects network anomalies that could indicate a potential compromise or exhibit insecure behavior that could precipitate one. Additionally, Asimily tracks device utilization and active recalls, so organizations can ensure that assets are being allocated efficiently. Asimily helps manufacturing organizations defend their systems, improve OT device management and uptime, reduce operational expenses, and achieve compliance with relevant security standards.

www.asimily.com

