INDUSTRIAL DEFENDER®

OT Cybersecurity Solutions Buyer's Guide

TODAY'S OPERATIONAL TECHNOLOGY LANDSCAPE

Operational technology (OT) refers to the process control or industrial control systems (ICS), that run factories, electric power generation and delivery, oil and gas production and delivery, shipping/logistics, etc. This technology embodies the fusion of computers with highly specialized sensors and devices that control processes in the physical world. These systems power our critical infrastructure, which is more than just roads and highways. It is the physical and virtual backbone that we all depend on for everyday life.

The threat of cyberattacks for OT systems grows every year, and examples of these attacks becoming reality have made quite a few headlines recently. Whatever is driving your intent to purchase an OT cybersecurity solution, here are six trends to keep an eye on:

1. Ransomware and nation-state attacks are on the rise.

The news headlines this year have been all about ransomware, which is just thieves stealing money with technology, rather than guns. The Colonial Pipeline and JBS Food Processing attacks were a wake-up call that cyberattacks can affect people in very direct ways – gas stations were shut down and processing plants were halted. We have been given notice that attackers can poison your water, cut off your energy supply and stop food production.

For tips on how to prevent and recover from ransomware in OT environments, you can check out this blog post:

Using the NIST CSF Security Controls to Prevent and Recover from Ransomware ➤

2. Critical vulnerabilities affecting OT continue to increase.

In the first half of 2021, 637 vulnerabilities affecting OT systems were disclosed, versus 449 in the second half of 2020. The majority of these were considered both critical and easy to exploit. Staying on top of new vulnerabilities in operational technology (OT) environments is particularly challenging to execute well because of the large number of disparate assets and software data collection limitations. If you do not have an accurate, detailed software inventory, you can't make sound mitigation decisions, and your vulnerability management effort will be ineffective.

For more tips on managing vulnerabilities in OT systems, check out this blog post:

How to Overcome Vulnerability & Patch Management Challenges in Your OT Environment ➤

3. IT-OT collaboration is accelerating.

Rather than focusing on "IT/OT convergence", many critical infrastructure companies are beginning to understand that OT technologies are already connected to IT systems. That ship has sailed. Now, we need to deal with managing the risks that have come from that, which means doubling down on a cross-functional, collaborative approach to cybersecurity. Many organizations are now choosing to share data from OT-specific cybersecurity tools with enterprise teams through a SIEM or ITSM integration to give full visibility to both functions. We see evidence of increasing IT/OT collaboration in the fact that OT cybersecurity budgets in many organizations are now a shared effort between the CISO and OT teams.

For tips on how to ask your CISO for OT cybersecurity budget, check out this blog post:

How to Ask Your CISO for OT Cybersecurity Budget ➤

4. Software Bills of Material (SBOMs) are catching on.

The complex software supply chain is creating massive vulnerability management challenges. When a vulnerability is disclosed, you don't always immediately know whether your inventory is affected by it, since every system that uses that software as a sub-component isn't always listed on a public advisory. A commonly proposed solution to this problem is widespread use of software bills of material (SBOMs), which list out all the software inside of an application.

The challenge right now for making SBOMs useful is the lack of a common software nomenclature to tag software uniformly, which makes interpreting them and comparing them with current inventories a very manual task. There are also security concerns, as an SBOM provides a lot of data on how to hack into a system. There are new vendors in the market who are addressing some of these challenges and will hopefully help to make SBOMs more useful and secure in the future.

For more information on using SBOMs to manage your software supply chain risk, check out this webinar:

What's Hiding in Your Software? How SBOMs Reduce Supply Chain Risk ➤

5. Skilled OT cybersecurity professionals are in short supply.

It's estimated that 3.5 million global cybersecurity jobs remained open in 2021. When you focus in specifically on OT security, the outlook is even worse, since these individuals need to not only understand cybersecurity in the traditional sense, but also how to manage complex control system architectures. This talent shortage is a major concern for critical infrastructure companies, especially when considering new cybersecurity tools for industrial control systems. Many mid-size organizations are now looking to outsource some of the cybersecurity workload to MSSPs or other vendors.

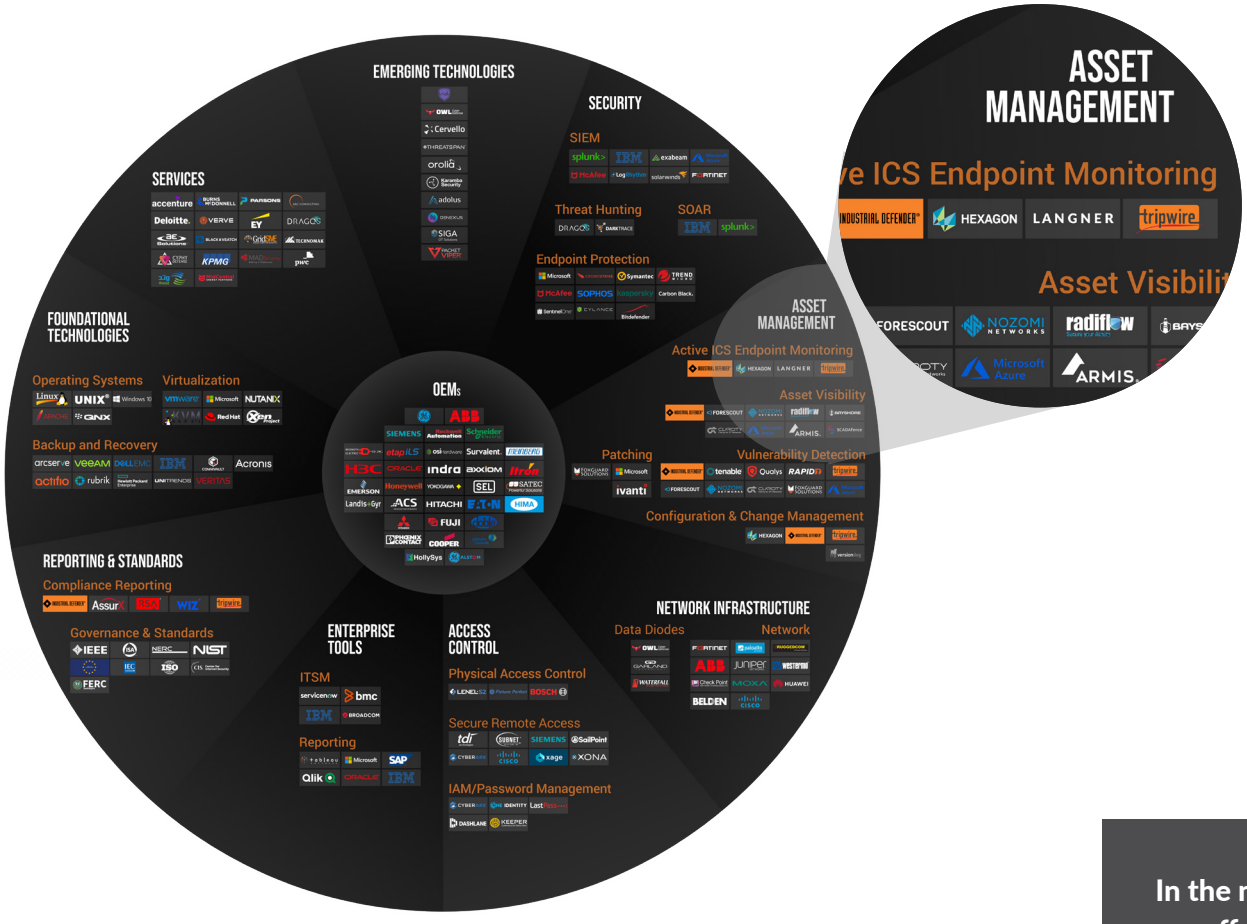
To learn how we are helping our customers tackle the talent shortage, check out our CopilOT service offering:

Industrial Defender CopilOT Service™ ➤

6. The OT vendor landscape is increasingly complicated.

Many end users must work with dozens of vendors to manage their OT systems, and at every point there can be different rules of engagement with each vendor. There are many critical components involved when trying to make control systems secure and compliant, and figuring out where these vendors overlap, or where they need to be connected is always a challenge. For this reason, we are still very much in the early days for ICS security.

To help security practitioners understand what and who is in their OT environments, we created our DefenderSphere.



This visual aid can help you better understand your complex industrial control system vendor landscape:

DefenderSphere – ICS Vendors ➤

In the next section, we offer tips on what to look for in an OT cybersecurity solution to help inform your search.

7 QUALITIES TO LOOK FOR IN AN OT CYBERSECURITY SOLUTION

1. Comprehensive Asset Identification Methods

It's important to understand how a solution discovers assets in your OT systems. Active methods include things like OT-specific agents and native polling of devices. The biggest advantages of these methods are being able to control the frequency of data refreshes and the depth of device data that they can provide. Often active is the only way to specifically obtain certain data values on-demand, like software, patches and users.

Passive methods, on the other hand, rely upon reading network traffic and strategic locations across the OT network. Instead of generating network traffic, this method listens to an OT network to extrapolate network pathing and devices. While less effective at generating data on things like software and patches, passive solutions have the advantage of near real-time monitoring for events happening within the network.

Sometimes an OT device does not lend itself to active or passive collection. It may be an asset that is not network connected, or even being monitored by a propriety closed OEM system. As a last resort, some devices may require manual data collection. Ensure that the solution can work with these types of situations.

For maximum asset visibility coverage, choose a vendor who offers you active, passive, offline and integration-based data collection methods, including:

Agents

Pros:

- The most comprehensive data collection – identify anything
- Easy to manage centrally
- No credentials required

Cons:

- Requires installation and resources on the endpoint

Agentless/Native Querying

Pros:

- Second most comprehensive data collection method
- Leverages the same collection methods created by the device vendor
- Can be done from a centralized data collector

Cons:

- Requires routable connections to device and credentials

Network Monitoring

Pros:

- Quick to deploy if the infrastructure supports it
- Quickly find unknown IP based assets
- Threat intel

Cons:

- Requires a SPAN/TAP/Mirror Port in the target network
- Limited data and only from assets talking using plain text data
- May require multiple sensors
- Not comprehensive enough for a compliance program or vulnerability analysis

Offline Collection/Manual Import

Pros:

- Safe for sensitive devices
- A wide variety of formats supported

Cons:

- Requires manual effort
- Can get quickly out of date

Integration with Existing Asset Management Systems

Pros:

- Leverages your existing investment in asset management
- Safe for sensitive devices

Cons:

- No coverage for security events
- Data collection may not be adequate or real-time

2. Robust Asset Management Capabilities

A comprehensive OT security solution should offer asset management features to manage configuration information, check software inventory against known exploits, identify critical missing OEM-approved patches, manage asset lifecycles, flag and log anomalous device activity and provide recovery services that can mitigate exploit damage.

True asset management is usually only achievable if a solution offers active data collection methods due to the level of device detail needed to execute it effectively.

A good OT cybersecurity solution should provide:

3. Authentic OT Vulnerability Management

Vulnerability management is particularly challenging to execute well in operational technology (OT) environments because of the large number of disparate assets. Industrial control systems operate continuously, so actively identifying vulnerabilities is rarely an option. A good OT cybersecurity solution should offer specialized data collection methods, including passive, agentless or native agents, to collect all the software and patch data for a particular endpoint and compare that against vulnerability feeds, such as NIST's NVD or even private OEM feeds.

Most vulnerability management solutions that are IT-focused fail to incorporate these specialized requirements. As a result, it is important to verify that the cybersecurity solution you're evaluating can handle the sensitivity of OT systems.

Look for a solution that offers:

- **A complete software inventory**
- **SBOM data ingestion**
- **NVD and ICS-CERT info from the UI**
- **Prioritization of open vulnerabilities**
- **Access to private OEM vulnerability feeds**

4. Integrated Patch Management Capabilities

An efficient OT patch management program begins with comprehensive, automated asset inventory data collection, real-time vulnerability monitoring, and vendor-approved patch data. This will let your team visualize precisely which assets are missing vendor-approved patches or have open vulnerabilities published in vendor feeds to make smarter patching and mitigation decisions.

Using integrations with industrial patching services, a good OT cybersecurity solution should be able to deliver patch data directly into the UI, including:

- **Visualizations of which assets are missing patches**
- **A security rating for each patch**
- **Information from private OEM patch feeds**

5. Monitoring of a Variety of Events and Changes

To get the most complete threat detection coverage, you should have more than just one detection method in place. Monitoring both the network and your OT endpoints detects suspicious activity in multiple ways, which can act as a type of fail-safe mechanism.

A comprehensive OT cybersecurity solution should not only be able to passively monitor the network, but also offer endpoint monitoring using multiple methods, such as OT-specific agents or native querying. There are certain events and changes a solution should monitor for that are critical to detect during a compromise, including:

- **Network intrusions**
- **Configuration changes**
- **Removable media events**
- **Hardware monitoring**
- **Log monitoring, including application logs**

6. Complete Incident Response Support

Work on and practice incident response and recovery plans that address how to maintain business continuity and/or bring your systems back online. If the worst happens and you are compromised, your OT cybersecurity solution should offer critical data that you need to get back online quickly and also determine where the compromise was initiated, and whether it is completely gone from your systems. You'll need a solution that gives you access to and secure storage for:

- **Event logs**
- **Access logs**
- **Configuration changes**

7. Well-Established Integrations & Reporting

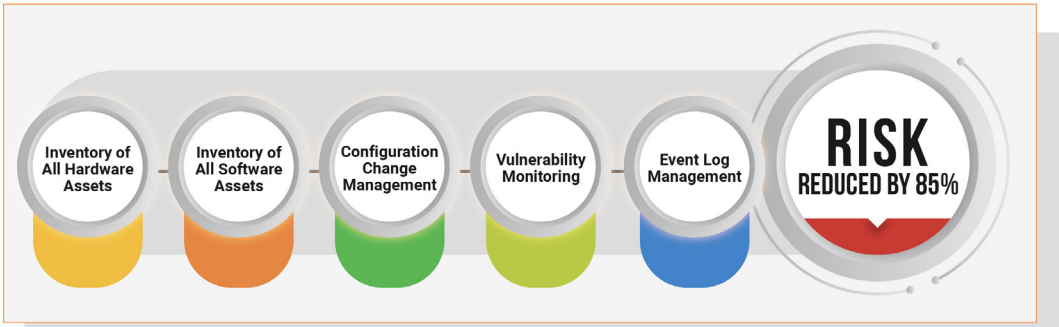
What good is all that OT asset and security data if you can't share it? Look for a solution that offers robust, API-enabled integrations with a variety of enterprise platforms to support close collaboration between enterprise and OT teams. It should also offer built-in compliance reports for commonly used standards to make regulatory audits or internal benchmarking of your cybersecurity program easy.

Choose a solution that has proven integrations with enterprise systems such as:

- **SIEM/SOAR solutions**
- **Risk analytics tools**
- **Enterprise reporting tools**
- **ITSM platforms**

OT CYBERSECURITY BEST PRACTICES

Building an effective OT security program starts with applying these five basic, foundational security controls.



Just by applying these controls in your OT environment, it's estimated that you can reduce your cyber risk by 85%. Only once you have this foundation in place can you move on to more advanced use cases to cover the other 15%, like SOAR, threat hunting and information sharing. A good way to benchmark your security program is to use a standard or framework to measure yourself against, like the NIST Cybersecurity Framework, ISA/IEC 62443 or the CIS Controls.

CHOOSING THE RIGHT OT CYBERSECURITY SOLUTION

Choosing the right OT cybersecurity solution will help you build the foundation to protect your critical operations from today's escalating cyberthreats. To learn more about how Industrial Defender can help you on your cybersecurity maturity journey, at whatever stage you might be at, schedule a time to chat with one of our OT security experts **here.**

THE INDUSTRIAL DEFENDER DIFFERENCE

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. Their specialized solution is tailored to complex industrial control system environments by engineers with decades of hands-on OT experience. Easy integrations into the broader security and enterprise ecosystem empower IT teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks. Learn more at **www.industrialdefender.com**.

SCHEDULE A DEMO

FOR MORE INFORMATION

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com
225 Foxborough Blvd, Foxborough, MA 02035
industrialdefender.com