FORESCOUT®

How We Answer the 7 Questions SRM Leaders Should Be Asking OT Security Providers

Challenges of the OT Security Selection Process

According to Gartner, by 2021, 80% of industrial IoT (IIoT) projects will have operational technology (OT)-specific security requirements, up from 40% today[1]. The diverse and complex nature of IIoT and OT security use cases can make the technology selection difficult, and unfortunately, copying IT security practices and technology will not result in a secure OT environment.

Some of the challenges security and risk management (SRM) leaders face during the OT security technology procurement process include:

1. Sensitivity of the industrial process to traditional active security methods use in IT.

2. Multisupplier/multivendor setting, requiring a third-party, independent technology that facilitates the prevention, detection and monitoring of many types of supplier equipment.

3. Lack of OT-specific RFPs due to the nascence of the OT security technology market.

4. Inflated expectations by the client and/or inflated capabilities by the vendor.

The inability of technology and service providers to meet the requirements of SRM leaders is one of the biggest obstacles to IIoT and OT security success. For SRM leaders in OT environments, it is critical to scrutinize a vendor’s infrastructure claims by testing out their APIs.

OT managers should also confirm that the technology not only detects and alerts on common CVEs, but also offers protocol compliance checks and ICS-specific threat behavioral checks. The technology should address current and future hardware needs with support for numerous OT protocols and asset discovery.

To achieve lasting success with OT cybersecurity investments, managers must ask prescriptive questions during the technology procurement process. In this eBook, we discuss the seven questions that SRM leaders should be asking during their OT security technology selection, according to Gartner, and how Forescout answers them.

By 2021, 80% of IIoT projects will have OT-specific security requirements.

Question No. 1: Is the Solution Vendor-Agnostic?

Gartner's Recommendations

- Review your equipment supplier's list of compatible technologies to ensure the security solution under consideration is scalable.
- Does the solution support your existing entire set of hardware and controllers?
- Does the solution support a broad set of additional controllers so that it will be easy for the OT security vendor to extend it and that you will be covered in the future?

How Forescout Helps

- Forescout has extensive protocol compatibility, with 100+ IT & OT protocols supported, and counting.
- We use a powerful customization framework that enables maximum flexibility and can quickly define and/or extend support for new protocols and custom network- and process-specific checks at run time.
- Our continuous improvement process helps to guarantee the coverage of needed protocols and can satisfy the most stringent requirements in terms of customization and coverage of proprietary protocols.
- Our extensive experience with all major ICS vendors and strategic agreements with ABB, Yokogawa and Honeywell help ensure that our solution can meet any hardware requirement.

Forescout has extensive protocol compatibility, with 100+ IT & OT protocols supported, and counting.

Question No. 2: Does the Solution Provide Asset Discovery to Enable Operational Continuity and System Integrity?

Gartner’s Recommendations

- Ensure the solution comes with sensors, central data visualization and analytics software.

How Forescout Helps

- Forescout uses an advanced architecture where completely passive sensors are efficiently spread out on the network. These sensors require only a copy of the network traffic to work, helping to guarantee no impact on the network.
- Rich asset inventory information and alerts about potential threats are delivered to a central visibility management platform in real time. From there, they can be escalated appropriately within the organizational ecosystem.
- By combining sensor-derived information from across the network with other data sources such as controls configuration and asset management, a comprehensive, visual and interactive model can be constructed.

- Ensure the solution passively scans and analyzes industrial network communications, provides information about industrial network assets, provides advanced anomaly detection, and alerts in real time for any threat to operational continuity and system integrity.

- Forescout provides advanced passive asset inventory & anomaly detection, alerts in real time for both cyber and operational threats and automatically assigns alerts to cases.
- Full patented DPI for IT & OT protocols, monitoring down to process values
- Fingerprinting for open and proprietary protocols alike (including ABB, Schneider Electric, Honeywell, Yokogawa, Emerson, etc.)
- Identification of nested devices, such as devices serially connected to other monitored PLCs
- The ability to detect and visually display PLC modules and their details
- Automatic fingerprinting of SEL RTAC RTUs
- Comprehensive search for indicators of incidents in network traffic and protocol messages
- Automatic threat intelligence ingestion and back-in-time threat detection
- 1,600+ threat indicators like protocol compliance checks, CVEs, and proprietary behavioral checks for cyberattacks, network issues, and operational errors
- Self-configuring network and process whitelists

Question No. 3: Does the Solution Detect and Alert on Known Common Vulnerabilities and Exposures?

Gartner’s Recommendations

- Obtain an updated list of supported, known and common OT controller and industrial control system vulnerabilities and exposures.
- Compare them with the ones listed on the ICS-CERT website, and ensure the solution not only can detect these vulnerabilities, but also can alert on them.

How Forescout Helps

- Forescout can automatically highlight devices which are missing patches and are vulnerable to vulnerabilities by matching make, model, and firmware version of the assets with the details of the patches/vulnerabilities.
- Our internal vulnerability databases are continuously updated by our analysts and sourced not only from ICS-CERT, but also from vendors themselves and other authoritative sources for even more extensive coverage.
- Users can produce a shareable report describing the current state of alerts and vulnerabilities for the monitored environments with both executive summary and a detailed analysis by accessing the Command Center and, via a drop down or menu item, select “Generate Report”.
- Applicable vulnerabilities come with a CVSS score and a Vulnerability Matching Confidence, fundamental to prioritizing vulnerability remediation.

- Determine whether the technology can ingest new signatures, threat intelligence, CVEs or other external information

- Forescout includes:
  - Comprehensive search for indicators of incidents in network traffic and protocol messages
  - Automatic threat intelligence ingestion from various internal and external feeds
  - Forensic Time Travel: After digestion of IOCs from external sources, the system can search its network logs to determine if IOCs were previously seen.
  - 1,600+ ICS-specific threat indicators like protocol compliance checks, CVEs, and proprietary behavioral checks for cyberattacks, network issues, and operational errors.
- Users can directly update their databases using the open format of the updates and/or link existing intelligence feeds.

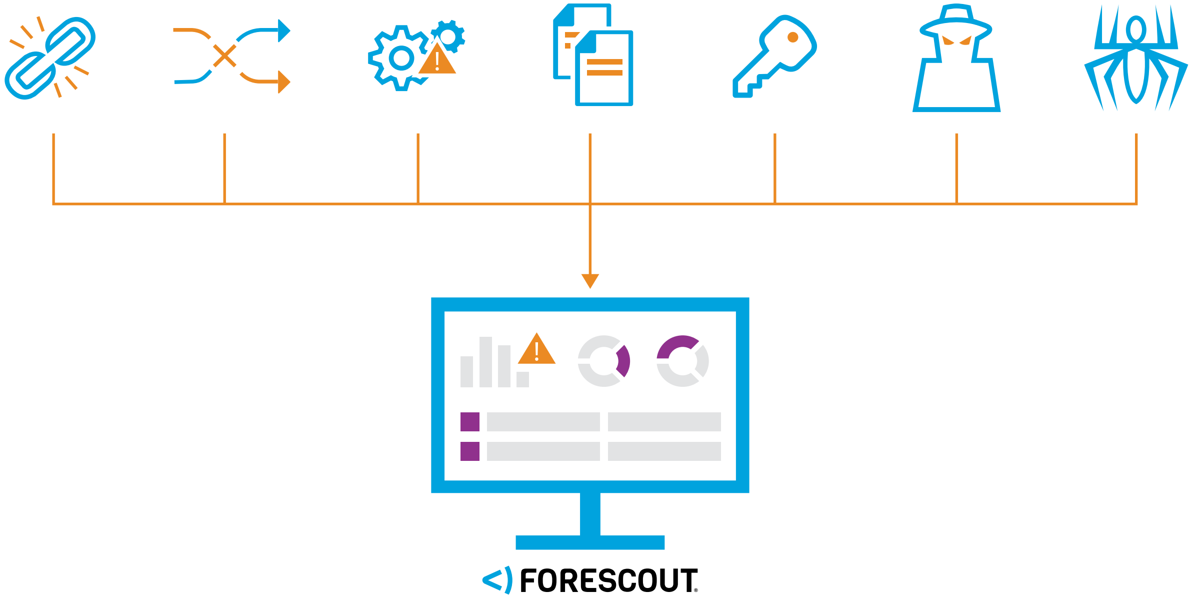
Question No. 4: Can the Solution Evolve From Mirror Mode to In-Line Security?

Gartner's Recommendations

- Disable active preventive capabilities of the OT security product, and experiment in detection only mode until you gain trust of the solution configuration.
- Before switching to active prevention mode, ensure the product neither injects extra traffic into the network nor requires extra network bandwidth to, for example, load signature updates. This situation might disrupt or slow operation of the primary control traffic, as well as impact business continuity.

How Forescout Helps

- Forescout can passively detect operational threats including network connectivity problems, device malfunction and misconfiguration, dangerous process operations, use of insecure protocols and default credentials, advanced cyberattacks, and exploit attempts. Threats detected by the sensors are delivered to a central visibility management platform in real time. From there, they can be escalated appropriately within the organizational ecosystem.
- Forescout offers an optional, non-intrusive active component that is carefully driven by the passive system to achieve additional visibility without affecting network performance.
- Forescout leverages ACL and VLAN assignment capabilities, bringing policy-based segmentation and access control to operational networks. It also offers plug-and-play integration with leading firewall vendors through Forescout Extended Modules.



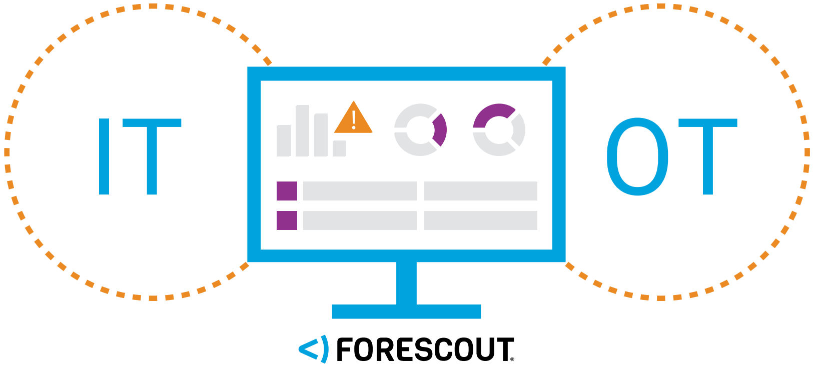
Question No. 5: Does Your Solution Provide IT Support in Addition to OT?

Gartner's Recommendations

- Favor solutions that are able to provide detection of advanced IT adversaries that evade prevention techniques and improved IT incident response/alert resolution capabilities.
- Make sure the solution supports a Cisco Express Forwarding (CEF) output or APIs to ensure integration with an IT security information and event management (SIEM) solution .

How Forescout Helps

- The Forescout platform provides end-to-end device visibility and control for both IT and OT networks.
- Integration with common enterprise systems in a matter of minutes via our built-in integration capabilities with all major SIEM solutions (including CEF, LEEF, and Splunk-specific formatting and apps)
- Integration with authentication servers to facilitate the mapping of user groups with eyeInspect (formerly SilentDefense) roles and related privileges
- Dedicated Splunk & QRadar apps
- Deployments done with all the major SIEMS on the market for some of the largest asset owners in the world
- An open REST API to easily extract information
- Event information can be exported in several other text formats



Question No. 6: Does Your Solution Support Secure IT/OT Alignment?

Gartner's Recommendations

- Understand what kind of integration and partnerships the vendor under evaluation has with other IT and OT security vendors, such as SIEM vendors, network vendors and OT suppliers.
- Determine if the product provides APIs to enable integration of OT security into the rest of the IT infrastructure.
- Make sure the product supports the security of OT-related protocols (for example, Modbus, DNP3 and CANbus) via DPI algorithms. If the product claims to do DPI on these protocols, scrutinize how comprehensive that DPI is for the protocols used in your systems. Is it just a few signatures (superficial support), or is there great depth to catch all the real-world use cases and exceptions that might come up?
- Make sure the product is able to secure the remote access on all types of OT equipment, as suppliers do regular equipment maintenance and updates, as well as reprogramming and configuration changes of PLCs.

How Forescout Helps

- We partner with industry leaders to offer built-in integration capabilities with:
  - Most major ICS vendors
  - All major security information and event management (SIEM) solutions
  - A vast range of asset management solutions
  - Majority of firewall applications available on the market
- With the Forescout platform, users enjoy unmatched visibility and control over their entire enterprise, from campus to OT.
- Forescout exposes an open REST API to easily extract information. This API is already in use by our apps (Splunk,QRadar) and by partners, and this information can be exported in several other text formats.
- Our DPI is the most comprehensive not only in terms of number of protocols (100+), but also in terms of depth of the analysis. Protocol checks are only a part of our 1,600+ threat indicators like protocol compliance checks, CVEs, and proprietary behavioral checks for cyberattacks, network issues, and operational errors.
- We detect remote logins on the network, usage of insecure passwords, configuration changes and behavioral changes of each node, reprogramming and other dangerous commands.

Users enjoy unmatched visibility and control over their entire enterprise, from campus to OT.

Question No. 7: Is the Solution Designed to Live in an OT Environment from a Hardware or Operating Environment Perspective?

Gartner's Recommendations

- Make sure the product meets your operating environment and lifetime requirements, such as, industrial temperature range and dust.
- Make sure the product has the industry certifications required for your OT network, such as Class I/Division 2 for use in hazardous environments and IEC 61850 for use in substations.

How Forescout Helps

- Forescout is completely hardware-agnostic, and can therefore satisfy any environmental requirements.

Resources

[1] 7 Questions SRM Leaders Aren't Asking OT Security Providers During Technology Selection, Saniye Alaybeyi, Gartner, 2018, https://www.forescout.com/gartner-report-7-questions-for-OT-security-providers

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com