OT Security Best Practices

Published 14 September 2018 - ID G00352264 - 30 min read

By Analysts Ruggero Contu, Lawrence Orans

Increasing replacement of OT infrastructure with IT systems is opening new vulnerabilities and risks that are pushing security and risk management leaders to update security approaches and strategies. We provide guidance for securing networks and endpoints in converged IT and OT environments.

Overview

Key Challenges

- The converging of IT and OT systems, combined with increased use of IoT in industrial environments, is challenging many security practices in defining the best security architecture that aligns to transforming and modernizing environments.

- Regulatory compliance pressure is mounting, as governments around the world issue new guidelines to enhance the security of critical infrastructures. This pressure comes along with the need to keep costs down and remain competitive.

- OT and IT convergence raises new security challenges spanning across a range of new initiatives. This impacts the security of a growing range of industries.

Recommendations

Security and risk management leaders who are operating and planning in converging IT/OT environments should:

- Strengthen the security strategy with the use of a hybrid approach of traditional security technologies and specialist controls to protect OT environments.

- Review and leverage available OT security frameworks as a guidance to update cybersecurity strategy, while making sure not to ignore the coming to market of new regulations.

- Assess the impact that new digital initiatives may have on your security setup, bearing in mind that OT security challenges are impacting all industry verticals.

Strategic Planning Assumption

By 2021, 25% of asset-centric enterprises will adopt a hybrid model to secure operational technology (OT) environments with traditional security deployed alongside specialist OT security technology, up from 10% in 2018.

Introduction

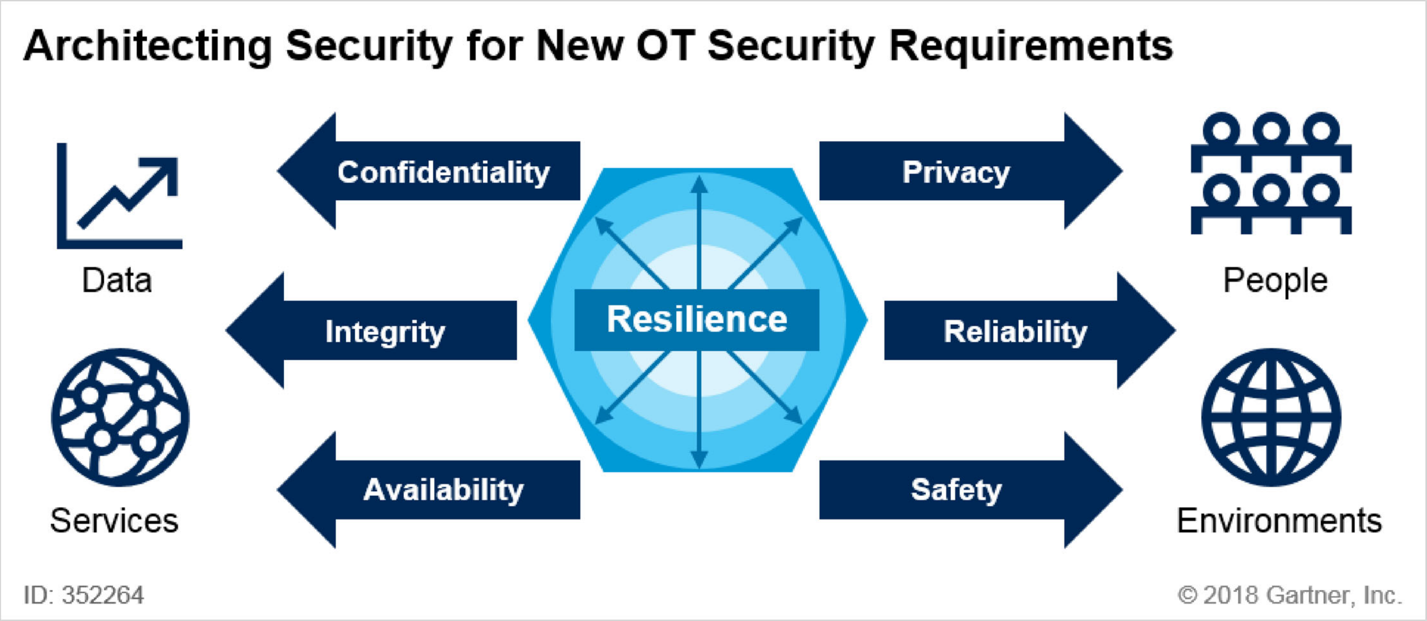
The drive to improve operations efficiency, performance and quality of services is behind the interest to leverage elements of IT infrastructures (such as Internet Protocol [IP]-based communications) within OT environments. This transformation is, in turn, introducing a commonality of security threats, across IT and OT, resulting in the demand for some form of centralized approaches to security (see Note 1). As a result of all this, security organizations from different industry verticals are facing the new challenges of having to secure increasingly converged IT and OT environments. They have the added complexity of having to cater for traditional security requirements of confidentiality, data integrity and availability along with the preservation of safety and system reliability.

This new threat scenario, along with the increasing use of the Internet of Things (IoT) in industrial environments and new regulatory frameworks, requires the implementation of new initiatives to coordinate security efforts. This is demanding the tackling of issues such as the need to improve security organization structures and cater to the shortage of specialized personnel in the area of OT security, as well as cultural issues.

An increasing number of Gartner's client interactions originate from the need to identify how to best plan a security strategy that has to extend to the new security requirements arising from IT/OT convergence.

This research note will help security and risk management (SRM) leaders, tasked with the coordination of securing these converging IT/OT environments, to develop a suitable architecture to align to the new emerging security requirements (see Figure 1). Gartner advice is to leverage traditional security controls at both network and endpoint layer, as well as specialized security tools and services developed specifically for OT requirements.

Figure 1. Architecting Security for New OT Security Requirements



Source: Gartner (September 2018)

Analysis

Maintain Your Focus on Safety and Reliability as Your Security Strategy Adapts to Converging IT and OT

The convergence of IT and OT environments is driving the need to leverage traditional IT controls and architectures to better monitor and secure critical environments, which are increasingly connected to external services. However, there remains the key requirement to preserve safety and reliability of the ever-critical OT environments.

As the U.S. NIST suggests, industrial control systems (ICS) “have many characteristics that differ from traditional IT systems, including different risks and priorities. Some of these include significant risk to the health and safety of human lives, serious damage to the environment, and financial issues such as production losses, and negative impact to a nation’s economy. ICS have different performance and reliability requirements, and also use operating systems and applications that may be considered unconventional in a typical IT network environment. Security protections must be implemented in a way that maintains system integrity during normal operations as well as during times of cyber attack.” (See “Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2,” NIST.)

SRM leaders tasked with coordinating the efforts to secure such converging environments cannot afford to disregard the highly critical requirements of safety and reliability. To achieve this, security must seek and establish collaboration and an organizational structure that involves both IT security and OT competencies. This will help align security to safety practices and regulatory requirements. SRM leaders need to revisit security processes and policies in order to extend a security strategy beyond the traditional pillars of confidentiality, integrity and availability (the CIA model), focusing on data security, but also including reliability and safety.

Key Factors Driving Interest to a Centralized and Coordinated IT/OT Security Strategy

A Wide Range of Industry Verticals Impacted by OT-IT Convergence

While OT is often related to industries such as oil and gas, energy, utilities and manufacturing, there are wider applications of OT systems across industries. With the emergence of new digital initiatives, such as smart cities, industries that traditionally haven't been focusing on OT a great deal have increased their interest toward tackling such new risks. An example comes from enterprises looking to utilize new systems to manage physical environments such as smart buildings but looking at the security implications arising from a whole set of services and data being handled by connected OT systems.

Erosion in the Value of Air Gap as a Main Approach to Securing Merging Environments

In the most extreme circumstances an air gap can be used to completely isolate two domains. This approach has been a traditional pillar for securing OT environments. The air gap technique is still heavily utilized in environments that need the highest degree of security, such as in military, intelligence organizations and the energy sector. However, due to the convergence of IT and OT, where IT systems increasingly "consume" data from OT systems, as well as the need from OT system vendors to remotely monitor their equipment, the air gap model has been increasingly compromised. The validity of the air gapping approach has been challenged even further by the opening up of different sorts of connectivity to OT networks and their components. Arguably most (if not all), controls are connected to the outside world in some way, shape or form (such as network connection, serial line or USB device).

The Stuxnet case shows the length of time isolated OT systems have been vulnerable to attacks, but there have been a number of more recent cases where highly critical systems got compromised as a result of breach of air gapping. The case of the International Space Station malware infection through a USB stick (https://www.theatlantic.com/international/archive/2013/11/russian-cosmonaut-accidentally-infected-iss-stuxnet/355150/) is one such example. In more recent times, other cases of attack to OT infrastructures circumventing isolated networks have emerged, as with the attack on the Ukraine electric grid in 2017. Recent research has also shown how security through air gap can be compromised without physical access, such as though the use of high-frequency audio exfiltration to detect digital communication. Other proof-of-concept research shows a variety of methods to circumvent air gapping, such as acoustic, thermal and light infiltration methods.

Notwithstanding this, it would be wrong to deny the value the air gap approach brings to security, particularly for more critical systems where physical isolation is needed. However, there is an increasing requirement to apply additional security measures to detect and stop eventual breaches coming from the circumvention of air gapping.

SRM leaders, when planning for air gapping, must consider the deployment of additional measures, such as device control and application control software. These measures help to stop the use of unapproved devices (such as USB keys) and the potential deployment of malicious code and its subsequent execution though physical access.

SRM leaders must also consider deployment of policies that work alongside security controls and that help mitigate risks. Such policies include restricting or blocking access to TCP and UDP ports (Ethernet/IP) or other Common Industrial Protocol-based devices, from outside the manufacturing zone.

Consider a Hybrid Architecture of Traditional Security Technologies and Specialist Controls to Protect OT Environments

Operational technology security product offerings focus mainly on OT network segmentation, OT network monitoring and OT endpoint security. The marketplace is composed of a mix of IT security providers supporting deployments to secure OT systems and specialist OT security vendors, with a high presence of startup innovative players. See the Gartner report “Market Guide for Operational Technology Security” for further information.

Finding the right balance between utilization of traditional security controls, such as firewalls, and OT specialist security tools is key. SRM leaders would need to assess the specific security requirements different OT environments would present and then decide which approach and tools to select, depending on the security requirements. This is particularly the case with the area of network security where network segmentation choices vary, as not all segmentation mechanisms offer the same assurances of trust.

Overall, the most popular approach is to rely mainly on network security and endpoint security with traditional controls, such as firewalling equipment and anti-malware (for Windows-based devices). We estimate above 90% of deployments leverage IT security controls, and the remaining part relies on security controls from OT security stand-alone providers and the security features integrated by OT system vendors. But this ratio should not be taken as a fixed reference but should vary depending on the type of data and the criticality of the systems to be secured. Some industries, such as energy (particularly nuclear power facilities) and military, are more prone to deploy high-trust approaches, such as unidirectional networks enforcing one-way traffic. The acceptance of OT security products by buyers is moderate, due to the mission-critical nature of OT environments, uneven levels of client maturity and the pace of IT/OT integration.

Securing OT Networks

Traditional security controls have great value when applied also to OT settings, particularly in this era of IT/OT convergence, but these need to be complemented in some cases by specialist controls. SRM leaders looking to address new security requirements arising from converging IT/OT must consider traditional security tools and specialist OT controls based on the different challenges faced.

As a starting point to a new converged IT/OT security initiative, there is a fundamental need to intervene at the network level, and particularly, to enforce network segmentation to better control access to critical OT systems. Enterprises are increasingly adopting network segmentation projects to protect their IT resources, particularly with OT environments, with the utilization of traditional network security equipment, such as firewalls and VPNs. But Gartner recommends also considering deploying more specialized tools, for more critical system requirements, such as OT network anomaly detection, as discussed below.

Besides network segmentation, SRM leaders looking for strategies on OT network security should also look to develop better detection and preventative measures, particularly as IT environments continue to converge with OT. Below we list some of the most popular and effective approaches and controls to secure OT environments, which SRM OT security leaders must consider.

The following traditional security controls offer critical capabilities within OT environments:

- **VPNs/firewalls** — A key value for firewalls is to enable a bidirectional communication between the IT and OT environments. Such equipment is typically used to have better control of access between IT systems and OT environments. Such equipment can be deployed both within a demilitarized zone (DMZ) to provide a more secured and regulated access between IT and OT environments and also within OT networks to achieve appropriate OT resource segregation.

  SRM leaders should achieve appropriate configuration and deployment to enable more granular customization and modifications of security policies between IT and OT. Implementation of these controls toward network segmentation should also be extended to provide finely tuned network segregation to bring more granular isolation of more critical OT assets based on better understanding and assessment of the different OT network elements.

- **Intrusion detection system (IDS)/intrusion prevention system (IPS)** — The increasing exposure of OT environments to cyberattacks is resulting in an increasing need to apply a detection strategy alongside the network segmentation function provided with firewalls. Both IDS and IPS equipment should be considered to provide situational awareness toward detecting potential attacks.

  SRM leaders must put particular attention toward the potential negative impact to critical OT network operations coming from the erroneous tagging of information or packets as malicious. The problem of false positives with IDS/IPS equipment can, at best result in the creation of needles and confusing alerts (as in the case of IDS equipment). At worst, it can result in blocking of genuine traffic (as in the case of IPS equipment), which can be very dangerous, as the blocking of a critical process may result in physical damage and/or impact to safety. These factors are among key reasons why IDS/IPS deployments in OT environments have been very slow.

  SRM leaders should consider safer ways to deploy IDS/IPS equipment within OT environments. This can be done by first deploying IDS/IPS equipment in a passive mode and after the monitoring process deciding, where appropriate, to allow active-mode deployment. The SANS institute provides some useful guidelines on how to plan the deployment of such equipment within OT environments (see "Challenges for IDS/IPS Deployment in Industrial Control Systems, SANS Institute InfoSec Reading Room 2015," SANS Institute).

- **Network access control (NAC)** — The same NAC technology that is used in many IT environments can also be implemented to improve the availability and reliability of OT networks.

  SRM leaders should particularly look at two areas where NAC that can provide most relevant value within OT environments:

  - Device profiling — Also known as "fingerprinting," NAC solutions provide visibility by identifying the device types (for example, PCs, printers and phones) that are connected to the corporate network. NAC solutions use the same profiling technology to identify the devices (for example, manufacturing components and industrial control systems) that are connected to OT networks.
  - Policy enforcement — NAC solutions can enable policy enforcement, such as blocking devices that do not authenticate to the corporate network. The same approach can be applied to OT environments, where unauthorized devices are blocked from accessing the OT network. Blocking unknown and unwanted devices will improve the reliability and availability of OT environments.

- **Deception —** With the availability of a range of products allowing for the passive monitoring of attacks through the implementation of deception technologies, there is now the opportunity to utilize such tools within OT networks. The approach with OT user cases is similar to the deployment within IP networks, where there has been an evolution in the use of honeypots toward distributed deception platforms, to detect and better understand and eventually defend from sophisticated attacks.

SRM leaders must include the deployment of specialist controls, developed specifically to cater for the critical requirements of OT systems, as part of an effective OT network security strategy. This should be part of an overarching OT security strategy that enables a defense in depth through a more granular approach. Providers of specialist OT security tools offer the advantage of being able to monitor and read specific protocols from OT system vendors (such as Schneider, Siemens and Honeywell). These providers can also provide security features that align to OT requirements while preserving reliability and safety.

However, whether looking at traditional security tools or specialist equipment, SRM leaders considering OT security controls must be cautious, as any technology that will actively scan OT systems can potentially disrupt operations. As a consequence, Gartner recommends to deploy security controls on a passive mode first and then judge where feasible to deploy active scanning tools.

Below we list some of the most popular and effective OT specialist controls to secure OT environments that SRM OT security leaders must consider:

- **OT asset discovery/monitoring** — One of the more popular specialist controls for OT environments comes from several startups that over the last five years have brought to the market OT network asset discovery capabilities, developed to be deployed with minimal impact to OT systems. As a result of concerns of potential interference with the normal operation, and resulting push-back from engineering professionals, some of these tools are deployed in a passive mode. Nevertheless, there is an increasing interest to apply different forms of active network monitoring and asset discovery in order to extrapolate more detailed endpoint and configuration data. Providers also offer OT network monitoring to support the detection of anomalies, threats and/or incidents. Some providers in this category leverage specialized threat intelligence and vulnerability assessment to support the improvement of the security baseline.

  A sample list of providers that SRM leaders must consider includes Armis, Bayshore Networks, Centri, Claroty, Cyberbit, CyberX, D&G, Darktrace, Dragos, ForeScout, Great Bay Software, Honeywell (Nextnine), Indegy, Kaspersky Lab, Lumeta, Nozomi Networks, PAS, Radiflow, SCADAfence, SecurityMatters, Sentryo, Tenable, Tripwire, Verve Industrial and 802 Secure.

- **OT vulnerability management** — A number of specialist providers make available some vulnerability management capabilities that, through an asset discovery activity, are able to correlate devices and system information with discovered vulnerabilities. However, while many legacy OT systems have limitations in applying patches, there is still the opportunity, once assets and vulnerabilities are identified, to find ways to mitigate risks through alternative measures. These measures include network segregation, replacing equipment where possible and closing down connections not needed. A number of traditional vulnerability management providers also support OT user cases; here, many vulnerability assessment vendors claim OT support for their solutions. However, when looked at in detail, in terms of scope (types of OT suppliers), coverage (manufacturers) and, most importantly, ongoing dedicated support, in many cases, there isn't a great deal of specialization.

  A sample list of providers SRM leaders must consider includes Claroty, Nozomi, PAS, Tenable and Verve Industrial.

- **Unidirectional gateways** — This technology (also sometimes defined as data diodes) has been deployed particularly with highly critical environments. Unidirectional gateways are used when there is the need to extract key information from OT environments without running the risk of opening up critical systems to unwanted and potentially malicious infiltration. They are also used in the rarer cases of sending information but preventing the inbound communication, particularly if there is the need to enforce one-way communication from an untrusted network to a trusted one, but not the other way around.

SRM leaders should consider this control to enforce unidirectional traffic if operating within an industry sector in need to secure critical infrastructures, such as nuclear power industry, energy and utilities.

A sample list of providers that SRM leaders must consider includes Advenica, BAE Systems, Deep Secure, Fibersystem, Foxit (NCC), Owl Cyber Defense and Waterfall Security.

Securing OT Endpoints

Endpoint security is the other critical area that SRM leaders, strategizing on OT, should focus on. This is particularly the case as OT-based endpoints are increasingly unable to take advantage of air gapping from IP-based systems due to converging IT/OT. This convergence is resulting in mounting exposure to IP-based attacks. (See the Gartner report “Why IIoT Security Leaders Should Worry About Cyberattacks Like WannaCry.”)

Gartner advises SRM leaders not to underestimate the new risks introduced, also because OT environments are deploying an increasing number of general-purpose endpoints, such as servers and workstations, often running Windows operating systems with internet access. As a consequence, the strategy to secure OT-based endpoints has to increasingly align with that of traditional IT environments where security controls such as anti-malware and host intrusion prevention are deployed alongside configuration management and patch management (where possible). See the Gartner report “Roadmap for Improving Endpoint Security” for detailed analysis on endpoint security.

However, Gartner advises SRM leaders to evaluate closely the specific requirements and limitations presented when looking to secure OT endpoints. Below we highlight some of the most pressing and critical aspects of an OT endpoint security strategy, aspects that need to be taken in consideration and handled alongside traditional endpoint security measures/policies:

Patch management — The specific and critical nature of the processes some endpoints support means that there has to be a targeted and well-defined patch management strategy in place. This, in some cases, means refraining from applying patching to avoid interfering with operations, as patching may be the cause of system failure. This is obviously very dangerous in OT as critical services may be compromised. The opportunity to stop OT systems from applying patching is also much more limited compared with IT, as a result of the requirement of most OT systems to keep operations running. This requirement restricts the opportunity to apply patches or system upgrades to very few occurrences in the year. The other problem SRM leaders face, in relation to patch management, is that deploying patches on an OT system may nullify the warranty of the system.

Therefore, it is sometimes key to develop an OT-specific patch management process that includes a check with the equipment vendors to address this issue before patch deployment. For more detailed analysis on this topic, see the Gartner report "Apply These Four Foundational Controls to Increase the Security of Your OT Environment."

Device control — SRM leaders should consider adding an extra layer of security for all OT endpoints, even those benefiting from physical separation through air gapping. Physical isolation is not enough, particularly for critical systems. Practical examples are available of "isolated" systems breached as a result of physical access; the Stuxnet attack is probably the better-known case. Device control tools and policies are of key importance to mitigate risks coming from local physical access. SRM leaders need to make sure that OT endpoints leverage controls, protecting from such physical access, to enable a stricter control of what type of storage devices are utilized and what type of content is deployed.

OT endpoints inventory — SRM leaders, looking at improving OT security, need to implement a strategy aimed at improving OT endpoints and systems visibility in order to better understand what needs to be protected and prioritized. A lack of proper asset management compromises any security approach and makes vulnerability management activities challenging. OT endpoint asset discovery is particularly needed with OT due to a traditional lack of full visibility of the devices and systems deployed within OT networks. This is particularly a result of the existence of legacy systems deployed over many years. The complexity and geographically dispersed nature of the OT domain further complicates the fulfillment of this process, while also increasing the need for it. As such, SRM leaders must consider an inventory strategy to include all relevant assets in need to be maintained for all OT domains in the organization. (See the Gartner report "Secure Your OT With Basic Security Hygiene.")

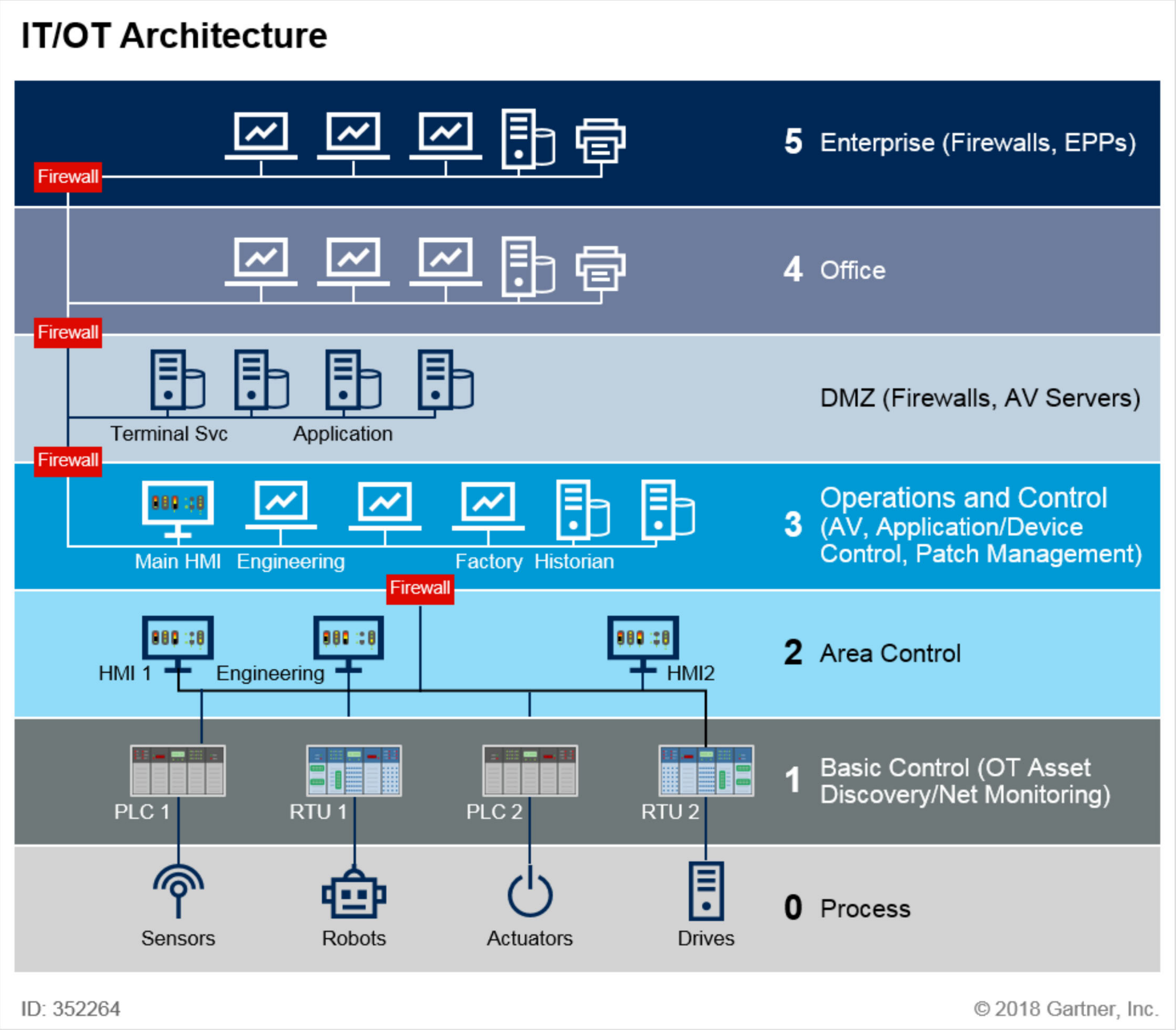
Application control — Alternative risk-mitigating measures should also be considered for OT endpoints through limiting activities of OT-based endpoints to essential tasks. SRM leaders must recognize that, compared with IT-based endpoints, OT-based endpoints are often required to fulfill much more focused tasks supporting a much more limited number of functions, processes and applications. As a result, a security strategy would benefit from restricting such endpoints only to those tasks they are deployed for, and to the applications required to enable the required processes. SRM leaders should consider application control/whitelisting and lockdown of endpoints to provide fairly straightforward, but very effective, ways to minimize risks.

Evaluate Existing Framework Models as Part of a Step-by-Step Approach to Coordinate an IT/OT/IoT Security Strategy

Reviewing and adjusting a security architecture is challenging. As a result, SRM leaders should consider and review available examples of security architectural models. There are a number of good security frameworks that can be considered as a reference model. As a starting point, Gartner would recommend looking at the Purdue model (see Figure 2). This is a very useful architectural reference framework with some of the value coming from its logical segmentation of systems into functional hierarchical areas, providing a map of the different IT and OT network zones to be secured. This model enables the identification of the most appropriate controls to be deployed across different levels. See the Gartner report “Apply These Four Foundational Controls to Increase the Security of Your OT Environment” for further analysis.

However, the approach to apply security based on such hierarchical segmentation is increasingly challenged with the impact of IIoT, where smart connected devices would communicate through communications channels outside of traditional communications protocols. Therefore, deploying a firewall to operate within IP or OT networks or at the intersection of OT and IT may not be enough.

Figure 2. The Purdue Model



AV = antivirus; EPP = endpoint protection platform

Source: Gartner (September 2018)

As a best practice, Gartner advises SRM leaders also to consider the following steps before taking strategic decisions relating to the rearchitecting of security.

First, start off with a risk-based assessment of OT environments based also on an accurate asset inventory and vulnerability assessment. The NIST Cybersecurity Framework (CSF) and the Australian government security framework offer good guidance toward a risk-based approach, particularly for critical infrastructure industries, as it caters for both IT security and OT security concerns within a single framework. This addresses both the digital and physical aspects of an organization in their approach to security (see Gartner research "Best Practices in Implementing the NIST Cybersecurity Framework").

Second, review the different security frameworks available, and upon selecting the most appropriate, create a plan of action to develop a security policy and architecture that takes into consideration the security requirements arising from converging IT and OT.

Table 1 lists some of the more popular OT security frameworks and standards along with useful architectural references and recommendations to be considered. In some cases, there may be the need to consider more than one reference as some offer architectural advice and others lay out compliance requirements.

Table 1: Sample List of More Popular Security Frameworks and Standards

Framework/Regulation ↓	Recommendations/Comments ↓
The European Parliament and the Council of the European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016	This is a regulatory framework that must be consulted by any organization operating in the European Union (EU) but also outside. It is particularly important for those industries providing vital services and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. While not providing detailed guidance on architectural recommendations, this new regulatory initiative from the EU requires the setup of minimal standards to achieve "appropriate security measures and to notify serious incidents to the relevant national authority."

Framework/Regulation ↓	Recommendations/Comments ↓
Industrial Internet Consortium, Industrial Internet of Things Volume G4: Security Framework	This is a very detailed framework SRM leaders should consider, particularly if looking to develop a security strategy that expands to broader IoT requirements. It offers detailed architectural recommendations on how to develop a security strategy aligning to IoT/OT initiatives. Taking advantage of the collaboration of Industrial Internet Consortium (IIC) members, the IIC security framework offers an in-depth cross-industry-focused security reference model.
ISACA, SCADA Cybersecurity Framework	This is a very detailed framework taking advantage of the collaboration of some of the key industry providers in the space of OT. SRM leaders looking to focus specifically to the area of OT security (rather than the broader IoT) should review this framework.
International Society of Automation, ISA/IEC 62443 (ISA-99)	The ISA-99/IEC 62443 standard should also be leveraged by SRM leaders wanting to focus specifically on OT security. This is one of the most recognized worldwide standards for security of the industrial control systems in the OT domain of organizations. The standard was created by the International Society of Automation (www.isa.org), a leading worldwide nonprofit organization. The standard offers organizations handles to improve the digital security and safety of their process and SCADA environments.

Framework/Regulation ↓	Recommendations/Comments ↓
NIST, Cybersecurity Framework	Although of relevance internationally, this framework should be reviewed by U.S.-based enterprises as some its recommendations and requirements are linked to general advice on critical infrastructure protection in the U.S. Voluntary by nature, it guides organizations to assess and treat risk without the guidance of a compliance checklist. NIST is probably the most popular framework providing guidelines for critical infrastructure protection (CIP). The NIST framework serves as taxonomy for risk management of critical infrastructure in a cybersecurity context. This is widely considered a critical basic guidance for new or existing cybersecurity risk programs, and is a legal framework for aligning IT to OT security. The CSF provides a common taxonomy and mechanism for organizations to: ▪ Describe their current cybersecurity posture ▪ Describe their target state for cybersecurity ▪ Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process ▪ Assess progress toward the target state ▪ Communicate among internal and external stakeholders about cybersecurity risk
Technical Support Working Group, Securing Your SCADA and Industrial Control Systems (Version 1.0)	SRM leaders would also benefit from this guidebook. While not offering an officially recognized standard, this is a practical set of recommendations developed to guide security practitioners with an overview of ICS security around administrative controls, architecture design and security controls.

Source: Gartner (September 2018)

Apply All Stages of an Adaptive Security Architecture to OT

As part of an overarching security strategy that aligns to new digital business requirements, there is a mounting need to adopt the concept of adaptive security also for OT security. Figure 3 shows the four stages of an adaptive security architecture.

Just as IT environments are inevitably exposed to security breaches, converging OT infrastructures are also at risk. This means that, alongside traditional preventive approaches, SRM leaders developing an OT security strategy need to start considering implementing detection, response and predictive capabilities. These capabilities will enable organizations to be faster at reacting to eventual breaches, and also to try to predict their occurrence.

The Gartner concept of adaptive security is based on the idea that preventive measures alone are not enough at a time of increasingly sophisticated targeted attacks, where the likelihood of being breached is very high for any organization. This concept also has relevance when planning to secure OT environments, particularly at a time of OT convergence with IT.

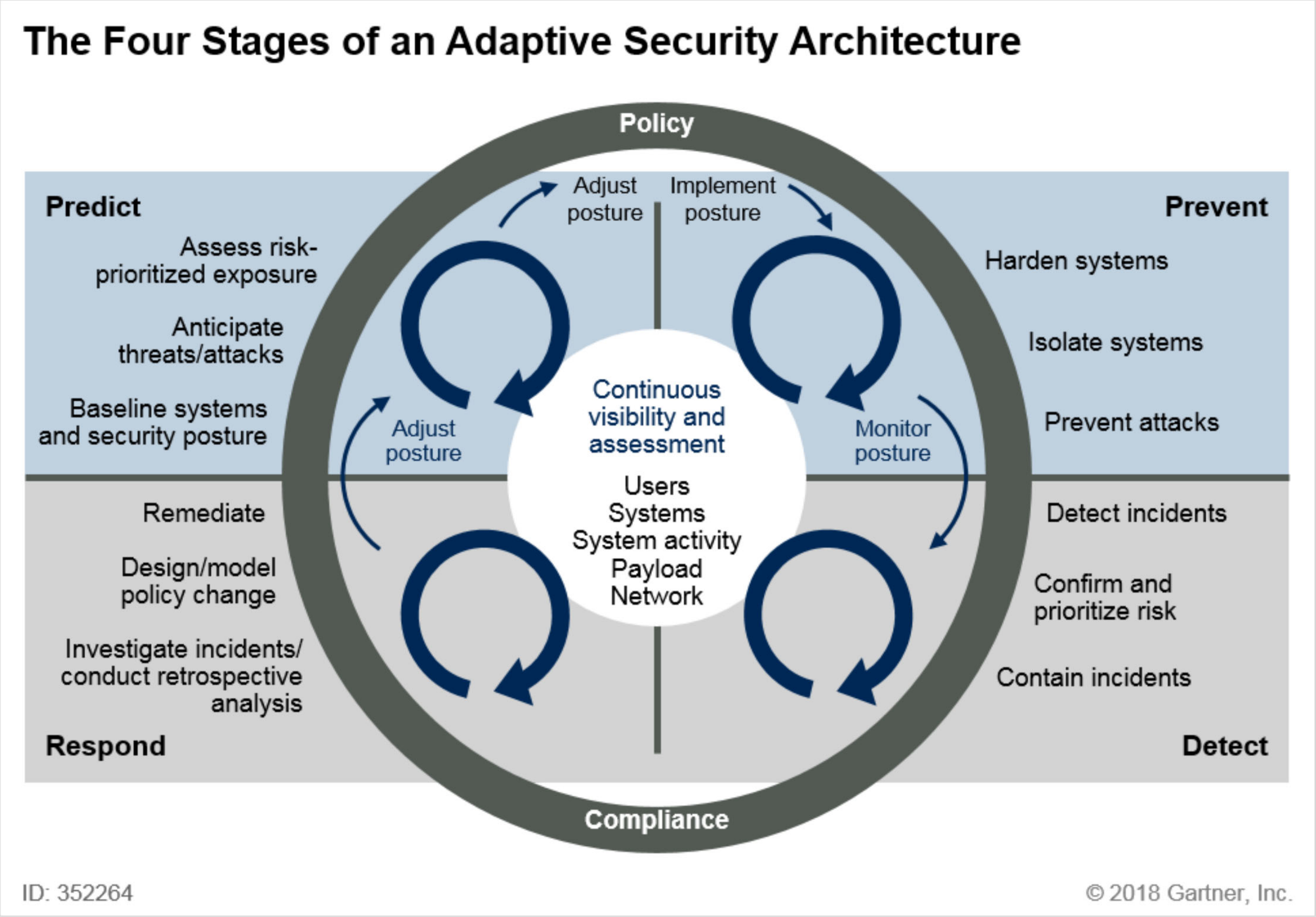
The lower maturity around the area of OT security means that organizations are focusing prevalently on preventive and detection measures, particularly around network/endpoint security and systems monitoring. These are the more mature and established markets in the area of OT security, as a confirmation of this prioritization.

Not enough is being done on the response phase. While key for organizations involved with critical infrastructure protection, planning for this area lags other aspects, and it is often conducted through the support of external service providers. External providers are used, particularly, in relation to postbreach intervention involving incident response activities, such as forensics, that can take advantage of specialist skills, an area many enterprises with OT security requirements lack.

Gartner advises SRM leaders to increase prioritization around the response phase relating to OT security incidents. This is because of the increasing likelihood of breaches as a result of the transformation taking place in many enterprises with consequent opening up of vulnerabilities. Awareness on this topic is generally growing, and we note an increasing interest from different enterprises to review the organization of their OT security operations, in some cases toward considering centralizing security operations center (SOC) activities within a converged SOC. This is often done to allow for a better coordinated and conjunct effort to monitor increasingly connected environments and also to maximize available technical and human resources. However, preparedness of enterprises remains low. As a result, we advise SRM leaders working for many of those organizations with insufficient skills and personnel resources to seek ways to improve internal competencies while relying on third parties, such as managed security service providers and consulting service practices. The focus will have to be in support of investigative and response requirements.

The anticipatory nature of the predictive phase is even more immature, particularly for OT-related environments. But there is already mounting interest in the opportunities that threat intelligence can bring to identify targeted attacks, their nature and the profile of threat actors specific to OT infrastructures. Several specialist OT security providers are now leveraging and making available threat intelligence that can be utilized to better prepare against mounting attacks and mitigate the impact of a breach through earlier detection or improvement of security setup. Enterprises with investments in threat intelligence should require their providers to add OT-related intelligence. There is also the opportunity to leverage threat intelligence from some specialist suppliers of OT network monitoring providers.

Figure 3. The Four Stages of an Adaptive Security Architecture


The Four Stages of an Adaptive Security Architecture
Policy
Compliance
Predict
Assess risk-prioritized exposure
Anticipate threats/attacks
Baseline systems and security posture
Prevent
Harden systems
Isolate systems
Prevent attacks
Respond
Remediate
Design/model policy change
Investigate incidents/ conduct retrospective analysis
Detect
Detect incidents
Confirm and prioritize risk
Contain incidents
Adjust posture
Implement posture
Adjust posture
Monitor posture
Continuous visibility and assessment
Users
Systems
System activity
Payload
Network
ID: 352264
© 2018 Gartner, Inc.

Note: The graphic is from the Gartner report
"Top 10 Strategic Technology Trends for 2017: Adaptive Security Architecture."

Source: Gartner (September 2018)

Note 1
Key Factors Driving Interest to a Centralized and Coordinated IT/OT Security Strategy

New Risks Coming From Converging IT With OT

Security awareness and prioritization arising from these converging environments has been confirmed by multiple discussions with Gartner clients, as well as specific survey data. The data points to a progression toward integrating IT best practices and aligning to the changes, resulting in:

- Initial awareness that the convergence of OT and IT products means IT-like architectures

- Wide acceptance within companies that "something needs to be done"
- Need to manage complexity
- A drive to reap rewards from connected OT systems

(See "Survey Analysis: Progressing to a Digital Business Future Through IT/OT Transformation.")

Anecdotal evidence also from conversations with Gartner clients highlights the mounting awareness and prioritization of security as a result of these merging environments and the subsequent threats posed. This growing awareness has been driven by a number of real cases of advanced persistent attacks in recent times, driving the need for a focus on converging IT/OT security issues. The publicized attack on Wolf Creek Nuclear Operating Corp. (https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html) is a recent example of attempts to compromise critical operations of nuclear power and other energy sector industries, as reported by the New York Times.

Overall, we can denote, a clear interest to leverage expertise from IT security teams to handle and coordinate OT and industrial IoT (IIoT) security requirements.

Mounting Regulatory Compliance Pressure

Traditionally, compliance has been a catalyst driver for investments in security over the years. This has also been the case for OT security-related spend. The U.S. NIST and North American Electric Reliability Corp. (NERC) CIP standards have had a very significant impact on the U.S. and global energy and utility sector in focusing on security aspects. Other industry sectors have also had an impetus to prioritize on security as a result of the Homeland Security Presidential Directive 7 (HSPD-7) of 2003, establishing U.S. policy (later known as the National Infrastructure Protection Plan, or NIPP). NIPP enhances critical infrastructure protection by establishing a framework for the department's partners to identify, prioritize and protect the critical infrastructure. Seventeen critical infrastructure sectors have been identified (see "The Impact of Critical Infrastructure Protection Standards on Security").

New CIP regulatory initiatives are being developed in other parts of the world, such as the European directive on security of network and information systems (https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive) (NIS), the Cyberspace Administration of China (CAC) draft regulations on critical infrastructure protection (https://www.dwt.com/The-Chinese-Government-Issued-Draft-Cybersecurity-Regulations-to-Protect-Critical-Information-Infrastructure-07-25-2017/) and the Australian Security of Critical Infrastructure Bill (https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1118) , bringing new examples of regulatory initiatives having an input on spend in this area.

About Careers Newsroom Policies Site Index IT Glossary Gartner Blog Network Contact Send Feedback