FORTINET

REPORT

Independent Study Pinpoints Significant SCADA/ICS Security Risks

Table of Contents

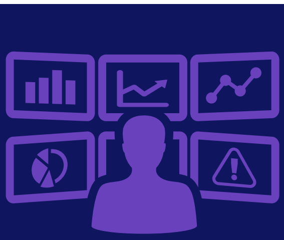
Executive Summary

Many businesses and government agencies have embraced supervisory control and data acquisition (SCADA) systems or industrial control systems (ICS) in recent years, but the technologies face major security challenges. **Nearly 6 in 10** organizations using SCADA or ICS that were surveyed by Forrester Consulting in a study commissioned by Fortinet indicate they **experienced a breach** in those systems in the past year—and many of those organizations are adding to their risk by allowing technology and other partners a high level of access into their systems. Most organizations also report **connections between their traditional IT systems and their SCADA/ICS**, introducing the potential for outside hackers to penetrate these control systems.

Despite these risks, many operators are not taking advantage of many of the security tools available to protect SCADA/ICS. About **half** of those surveyed **have not deployed secure shell (SSH) or transport layer security (TLS) traffic encryption** for their SCADA/ICS, and many do not use role-based access control for employees.

At the same time, many organizations using SCADA/ICS open up avenues of attack by allowing a host of other technologies, including global positioning system (GPS), active radio-frequency identification (RFID), and Wi-Fi devices, to connect to their networks. Meanwhile, 97% of those surveyed acknowledged security challenges because of the convergence of traditional information technology (IT) and operational technology (OT).

While the bad news is that SCADA/ICS face several threats, the good news is operators can take additional steps to protect their systems by rolling out additional security tools.



Understanding SCADA vs. ICS

ICS are often managed via SCADA systems that provide a graphical user interface for operators to observe the status of a system, receive alerts, or enter adjustments to manage processes.

The ICS market is expected to grow rapidly, reaching

$81 billion in 2021.

The attack surface is rising every year.

The SCADA market is expected to grow **6.6%** annually, reaching

$13.43 billion in 2022.

Introduction: SCADA/ICS Are Attractive Targets

In recent years, many organizations beyond electric and water utilities have deployed SCADA/ICS as they look to automate their data collection and their equipment. The technologies have become high-value targets for hackers looking to disrupt business operations, to collect ransom, or to attack rival nations' critical infrastructure.[1] Per the Forrester study, **56%** of organizations using SCADA/ICS **reported a breach** in the past year, and only 11% indicate they have never been breached.

Attackers can cause real harm. In December 2015, several regions of western Ukraine experienced power outages due to an attack on electric industrial control systems.[2] It is not confined to entities outside the United States. For example, in March 2016, hackers breached the network of an unnamed U.S. water utility, and for a short time, took control of several programmable logic controllers that govern the flow of toxic chemicals used to treat water.[3]

A major part of the problem is access to SCADA/ICS by third parties. Many organizations place a lot of trust in the security of their technology vendors and other outside organizations by giving them wide access to their internal systems. About **6 in 10** organizations surveyed by Forrester gave **either complete or high-level access** to partner or government organizations. In short, SCADA/ICS operators face serious risks, and they face several hurdles on the road to improved security.

SCADA/ICS Quicky Growing—in Depth and Breadth

The SCADA/ICS markets are growing quickly. Transparency Market Research predicts the global ICS market alone will grow from $58 billion in 2014 to $81 billion in 2021, with an annual growth rate of 4.9% between 2015 and 2021.[4] ICS have become widely used in manufacturing, at seaports, in water treatment plans, in oil pipelines, in energy companies, and in building environmental control systems.[5] SCADA, at the same time, which serve as the graphical user interface into ICS, are growing at an annual growth rate of 6.6%.[6]

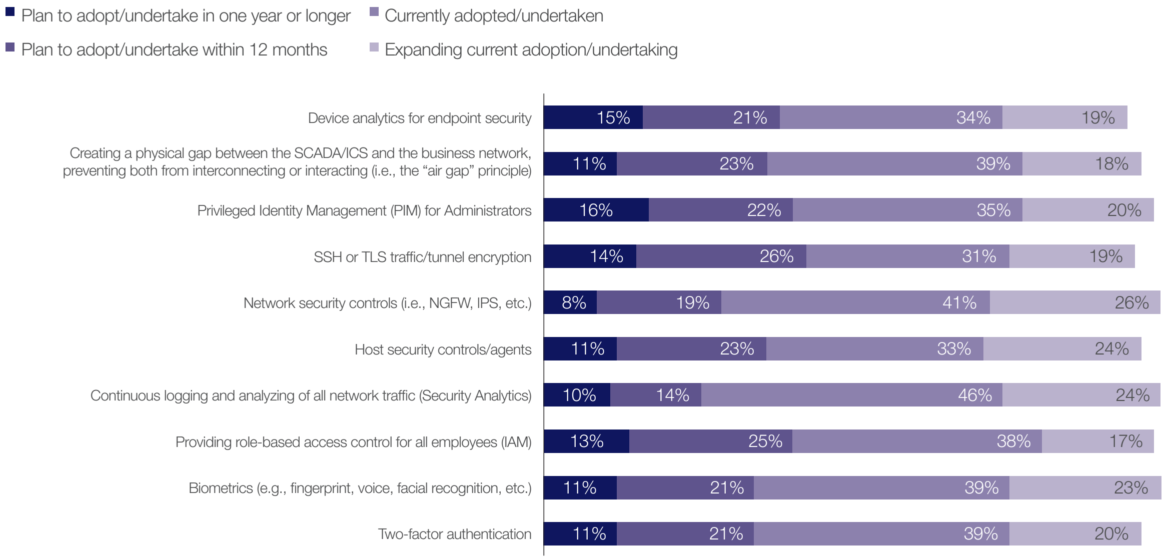
The good news is that organizations operating SCADA/ICS seem to recognize that they face risks. Many use a number of technologies and security methods to protect the systems. For example, the Forrester study found that **70%** of the organizations surveyed **continuously log and analyze all their network traffic**, 24% of which are expanding their current security analytics deployments. About **two-thirds** use some kind of **network security controls**, and **62%** use **biometric-based security controls** such as fingerprints or facial recognition.

Despite these numbers, many organizations have not deployed several other security technologies that could help protect their SCADA/ICS. Half of those surveyed have not deployed SSH or TLS traffic encryption, although more than half of that number plan to adopt one of those technologies within a year.

In addition, **45%** of respondents do not use Privileged Identity Management (PIM) for Administrators, which allows organizations to monitor high-level accounts in their IT environments. Another **45%** do not use role-based access control for employees. However, only a small percentage say they have no plans to adopt these technologies.

Most organizations currently undertake numerous measures to secure their SCADA/ICS

Question: What are your organization's plans to adopt or undertake the following measures to secure your organization's SCADA/ICS?



	Planning within 12 months or longer	Adopted or expanding adoption
Device analytics for endpoint security	36%	53%
Creating a physical gap between the SCADA/ICS and the business network, preventing both from interconnecting or interacting (i.e., the "air gap" principle)	34%	57%
Privileged Identity Management (PIM) for Administrators	38%	55%
SSH or TLS traffic/tunnel encryption	40%	50%
Network security controls (i.e., NGFW, IPS, etc.)	27%	67%
Host security controls/agents	34%	57%
Continuous logging and analyzing of all network traffic (Security Analytics)	24%	70%
Providing role-based access control for all employees (IAM)	38%	55%
Biometrics (e.g., fingerprint, voice, facial recognition, etc.)	32%	62%
Two-factor authentication	32%	59%

Base: 429 global decision-makers responsible for security of critical infrastructure, IP-level protection, IoT, and/or SCADA
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

Figure 1: Most SCADA/ICS operators continuously log and analyze network traffic, while just over half deploy device analytics for endpoint security.

Many SCADA/ICS operators ignore basic security tools.

45% do not use role-based access control.

This creates openings for insider threats.

Challenges to SCADA/ICS Security

Organizations relying on SCADA/ICS technologies appear to be worried about the use of the cloud by the vendors of those systems. In particular, organizations are concerned about employee use of personal and cloud technologies that may connect to their SCADA/ICS.

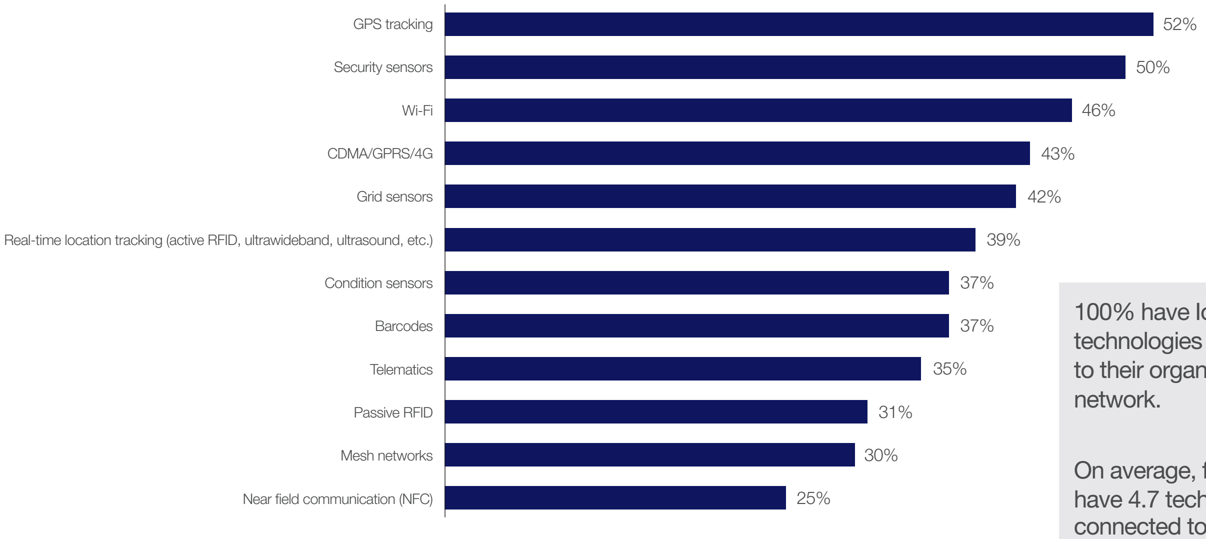
Even as organizations see several potential security risks, they may add to their problems with some of their actions. Notably, many allow a substantial number of **wireless and Internet-of-Things (IoT) technologies to connect to their networks**, which bring with them additional vulnerabilities. Every company surveyed in the Forrester study reports having some IoT or wireless technologies connected to their network, which may include connections to SCADA/ICS. The risk is definitive, with an average of 4.7 IoT technologies connected.

Wi-Fi is just as big a problem. More than **40%** of organizations have Wi-Fi devices, mobile devices, and grid sensors connected. Many of these connections lead to complications for organizations trying to manage the convergence of their IT and OT—the hardware and software that runs SCADA and ICS. In addition, nearly **three-quarters** have at least basic connections between IT and OT, a possible red flag when it comes to protecting them against malicious threats.

Concerns about IT and OT convergence vary. About **4 in 10** worry that either they or their security partners lack the expertise needed to protect their IT and OT. Another **39%** worry about leaks of sensitive data, and **one-third** are concerned about exploitation of backdoors in connected devices. Another potential problem for organizations operating SCADA/ICS is the level of access they give to technology and other partners. This access gives hackers another avenue of attack.

IoT technologies currently connected to the network

Question: Which of the following Internet of Things (IoT) technologies are currently connected to your organization's network? (Select all that apply.)



100% have IoT technologies connected to their organization's network.

On average, firms have 4.7 technologies connected to their network.

Base: 429 global decision-makers responsible for security of critical infrastructure, IP-level protection, IoT, and/or SCADA
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

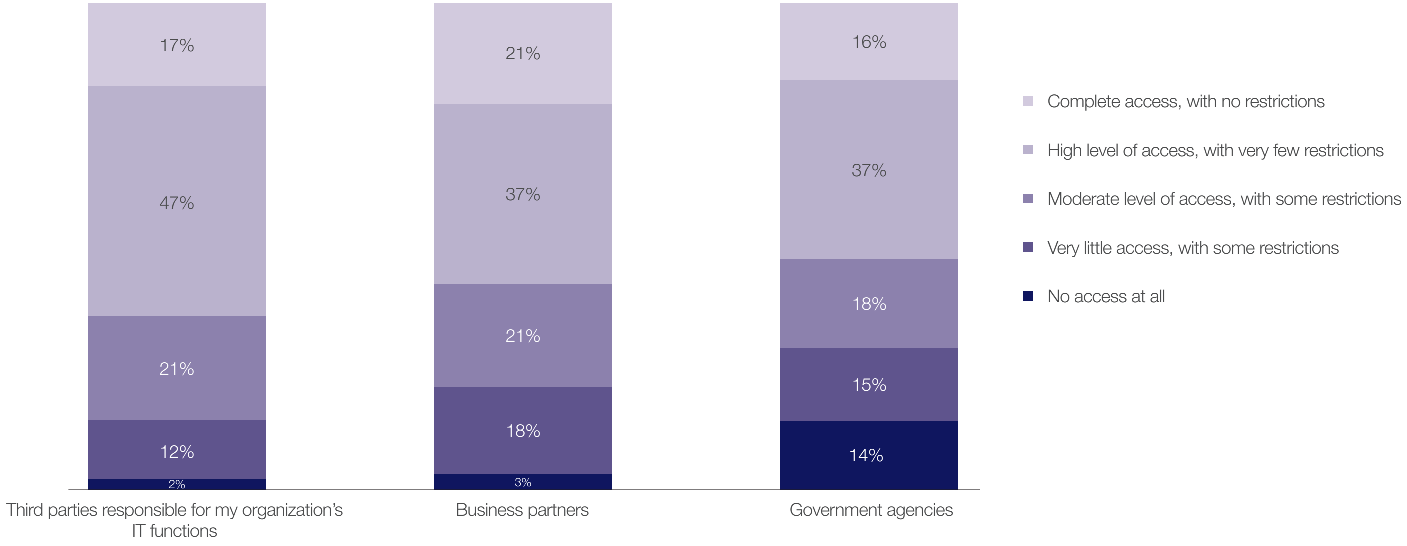
Figure 2: Most SCADA/ICS users have a large number of other technologies connected to their networks.

For example, **64%** of organizations give third-party IT vendors either complete or high-level access to their SCADA/ICS. But the problem does not start with the first level of relationships: nearly 60% give other business partners complete or high-level access, and more than **50%** give government agencies the same level of access. When it comes to industries, manufacturers are the most willing to provide complete access to outside organizations.

Adding to the potential risk is the fact that many organizations outsource some of their SCADA/ICS security. The top SCADA/ICS functions outsourced to IT vendors were wireless security, intrusion detection, network access control, and IoT security. And outsourcing is far from isolated: **56%** of the organizations surveyed outsource SCADA security to multiple vendors. In some cases, the use of multiple vendors creates a **patchwork of defenses that do not work well together.**

Most organizations grant outside parties with complete or high-level access

Question: What best describes the level of access your organization grants the following entities to its SCADA/ICS?



Base: 429 global decision-makers responsible for security of critical infrastructure, IP-level protection, IoT, and/or SCADA
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

Figure 3: Many SCADA/ICS users give technology vendors and other business partners high-level access into their systems.

Organizations running SCADA/ICS trust their partners with their systems.

64% give third-party IT vendors complete or high-level access.

Your IT vendor's vulnerability may be your own.

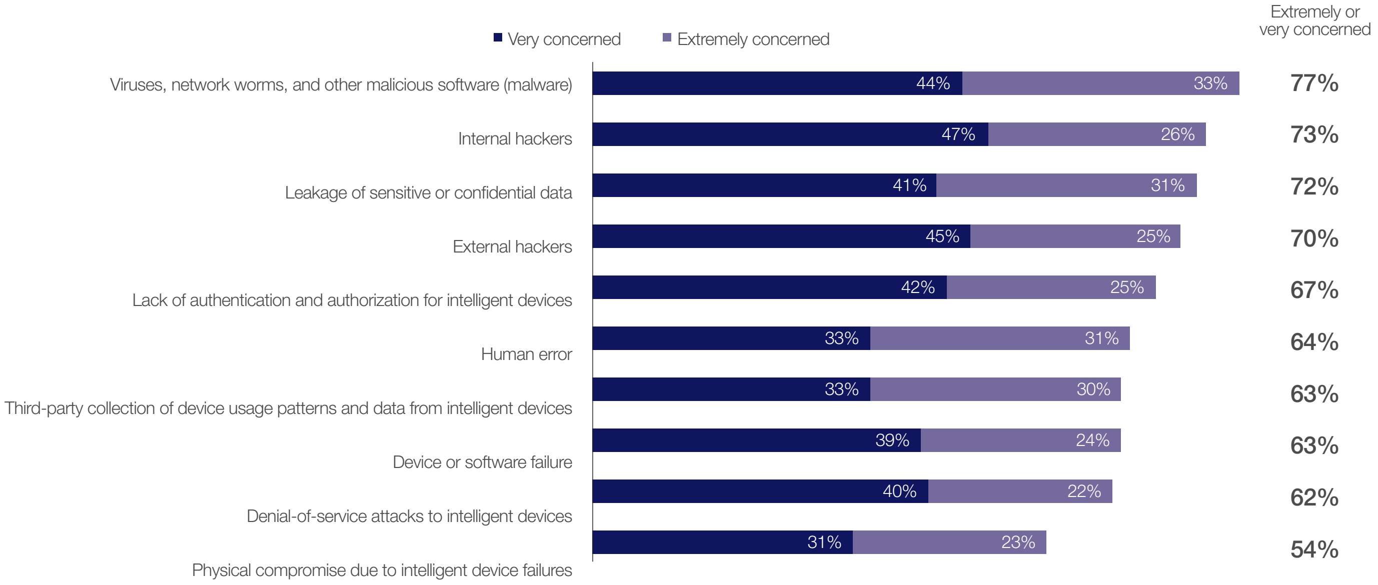
SCADA and ICS Threats

In addition to asking about internal policies, the Forrester study queried organizations operating SCADA/ICS about their most serious security threats. Operators see multiple threats from several sources, with malware and internal leaks heading up security concerns. Here, more than **three-quarters** of organizations acknowledge being very or extremely concerned about outside malware. More than **7 in 10** were very or extremely concerned about internal hackers, leakage of sensitive data, and external hackers. More than **two-thirds** are concerned about a lack of authentication or authorization for intelligent devices, and nearly two-thirds are concerned about human error and about third-party collection of data and device use patterns.

Concerns over malware and internal hackers have grown since a similar study was conducted in 2016. And while the threat landscape has evolved substantially since then and there is a heightened level of risk to SCADA/ICS, SCADA/ICS operators perceive that risks have actually diminished. For example, human error, third-party collection, and device or software failure are of smaller concern for them, though this may be due to them seeing evidence of security risks from other sources.

Security concerns range from viruses and hackers to data leaks and lack of authentication

Question: Please rate your level of concern with the following as they relate to the security of your SCADA/ICS network.



Base: 429 global decision-makers responsible for security of critical infrastructure, IP-level protection, IoT, and/or SCADA
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

Figure 4: SCADA/ICS operators are concerned about malware, internal hackers, and several other threats.

More than

70% of OT organizations

are extremely concerned about internal hackers, leakage of sensitive data, and external hackers.

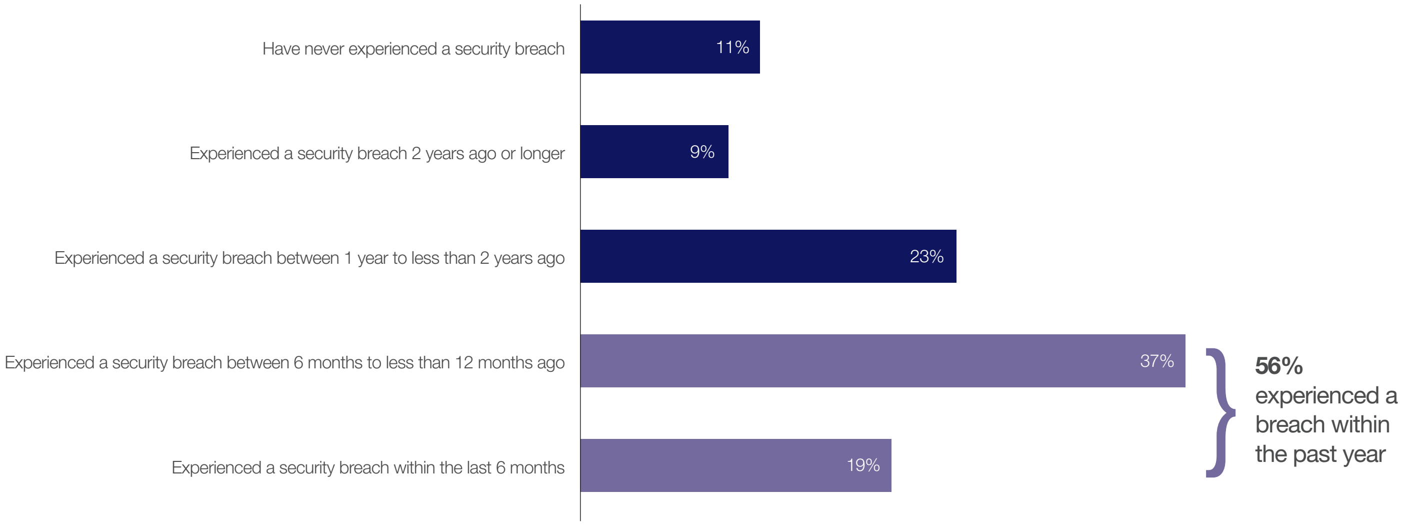
Impact of Threats

Even with many organizations deploying multiple security practices, breaches in SCADA/ICS are common. For example, **56% of respondents reported a SCADA/ICS breach** in the past year, and another **32%** have experienced a breach earlier. That leaves a small percentage that say they have never had a breach.

SCADA/ICS breaches have serious repercussions. **63%** of organizations say the safety of their employees was highly or critically impacted by a SCADA/ICS security breach. Another **58%** report major impacts to their organization's financial stability, and **63%** note a serious drag on their ability to operate at a sufficient level.

56% of organizations have experienced a SCADA/ICS security breach within the past 12 months

Question: To the best of your knowledge, has the SCADA/ICS at your organization experienced a security breach?



Base: 429 global decision-makers responsible for security of critical infrastructure, IP-level protection, IoT, and/or SCADA
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

Figure 5: Most SCADA/ICS users have experienced a systems breach in the past year.

Breaches are common in SCADA/ICS.

56% of SCADA/ICS operators reported a breach in the past year.

Breaches compromise the safety of employees and organizations' financial stability.

Recommendations on Mitigating Risks

Many organizations see several options for mitigating SCADA/ICS security. Nearly half see a full business or operational risk assessment as a top way to improve their risk posture as OT and IT systems converge. Other common approaches for mitigating risk include implanting common standards, increasing the centralization of device management, and consulting government bodies such as the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

When asked about choosing a SCADA/ICS security vendor, just over half of organizations trust technology consultants to provide reliable information. For example, SCADA/ICS vendors and partners score only slightly more than **50%** when it comes to garnering trust.

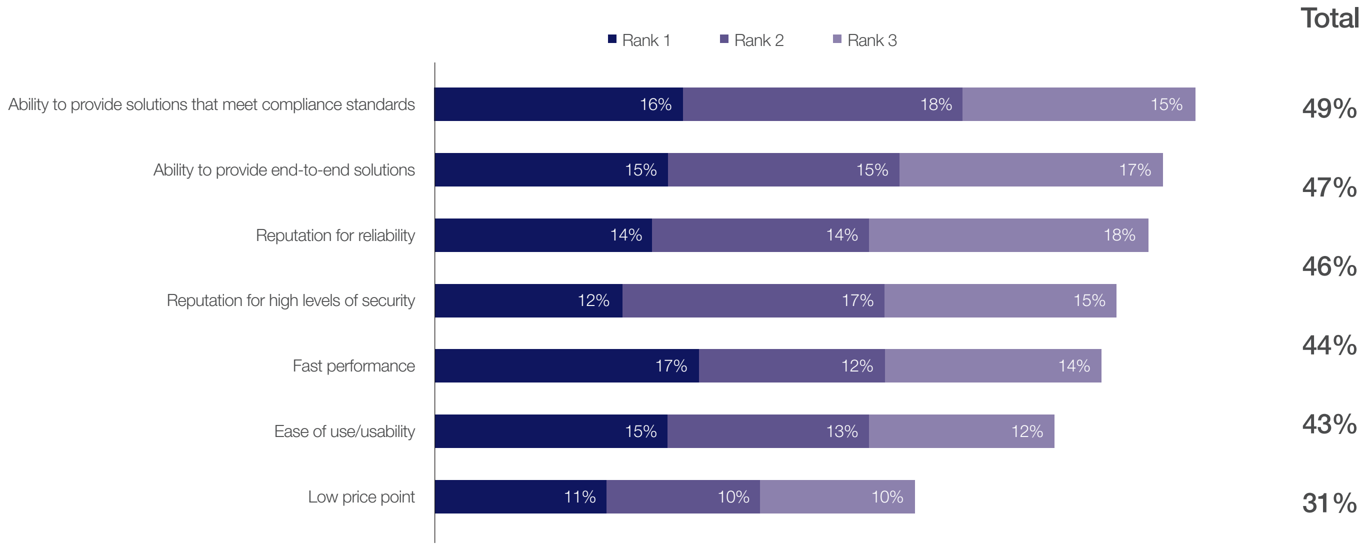
For the evaluation of security providers and technologies, organizations should consider their ability to deliver:

- Fast performance
- Ability to meet compliance standards
- Comprehensive, end-to-end solutions

Reputation for reliability and for high levels of security all scored high among organizations. Compliance with industry and security standards is a top concern, with nearly half ranking the ability to meet compliance standards as a top factor in their choice of security solutions. The ability to provide end-to-end solutions is second in the list of distinguishing factors. Interestingly, only **3 in 10** targeted low cost as a major factor.

Meeting compliance standards, providing end-to-end solutions, and reliability are most important when selecting a vendor

Question: When considering a security vendor for your SCADA/ICS, which of the following factors, if any, are the most important in your selection? (Rank the top three.)



Base: 429 global decision-makers responsible for security of critical infrastructure, IP-level protection, IoT, and/or SCADA
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

Figure 6: SCADA/ICS users have several priorities for security vendors, including the ability to meet compliance standards and the ability to provide end-to-end solutions.

The Road Ahead

Many organizations using SCADA/ICS plan to increase spending on related security technologies this year. Those not planning to add to their budgets risk getting left behind. Nearly three-quarters of organizations plan to increase IoT security spending, with 36% of them increasing spending by 5% or more. More than 7 in 10 plan to spend more on OT security, and nearly **4 in 10** plan to increase spending by at least 5%. Another **7 in 10** will spend more on OT infrastructure this year, with 37% planning a hike of 5% or more. These investments indicate an ongoing and increased commitment to OT and the security standards and controls needed to protect those systems.

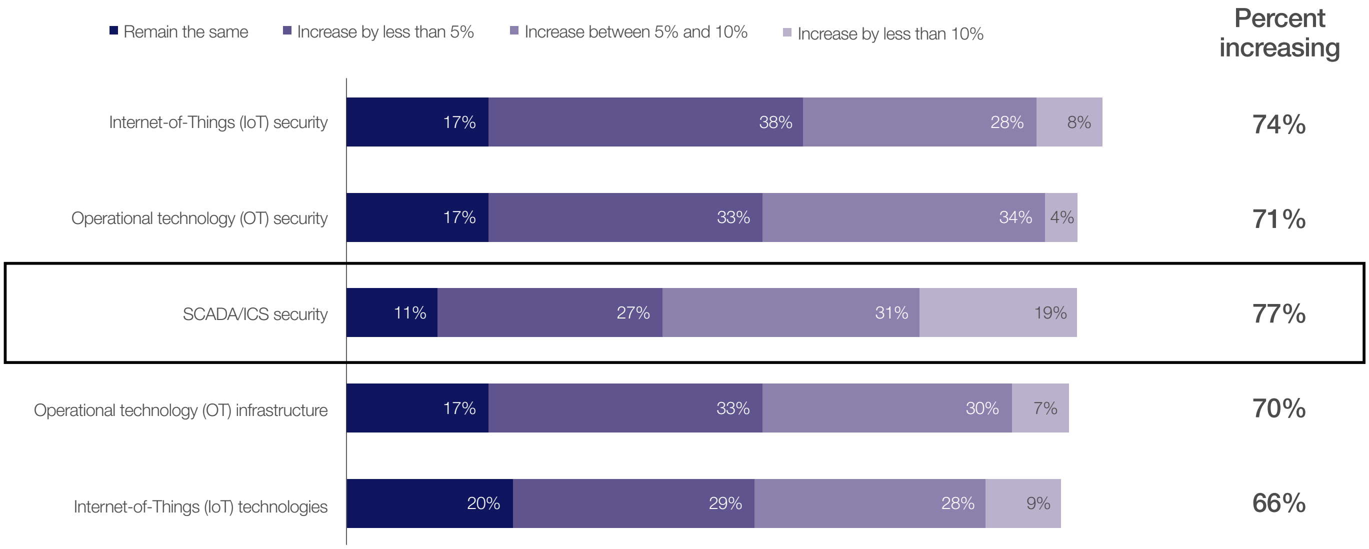
While thinking about what security measures to spend money on, SCADA/ICS operators can take several steps to protect their assets. These include:

- Segmenting networks by separating connected wireless and IoT technologies from SCADA/ICS
- Securing network infrastructure, including switches, routers, and wireless networks, through firewalls and other tools designed to protect these assets
- Applying identity and access management policies to keep outsiders out of networks and to prevent employees from accessing parts of the network they do not need to access
- Using a web application firewall (WAF) to scan and patch unprotected web applications
- Deploying endpoint protection to deliver real-time, actionable intelligence and visibility into threats

With the potential to impact the physical safety of employees or customers, security considerations for SCADA/ICS must be different than for traditional IT systems. The good news is that, by taking a multilayer approach to SCADA/ICS security, organizations can significantly improve their security footing and thereby reduce their risks.

Spending in SCADA/ICS security is increasing more than in other areas

Question: How do you expect your organization's spending in the following areas to change from 2016 to 2017?



Base: 429 global decision-makers responsible for security of critical infrastructure, IP-level protection, IoT, and/or SCADA
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

Figure 7: Many operators of SCADA/ICS plan to increase security spending in several areas in 2018.

Reference List

[1] Joe Weiss, "Industrial control systems: The holy grail of cyberwar," The Christian Science Monitor, March 24, 2017.

[2] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," WIRED, March 3, 2016.

[3] John Leyden, "Water treatment plant hacked, chemical mix changed for tap supplies," The Register, March 24, 2016.

[4] "Global Industrial Controls System Market to Grow at CAGR of 4.9% from 2015 to 2021," Transparency Market Research, September 2015.

[5] Mark Fabro, "Industrial Control Systems Cyber Security," Presentation to U.S. Department of Defense, June 7, 2017.

[6] "SCADA Market Worth 13.43 Billion USD by 2022," MarketsandMarkets, accessed April 12, 2019.

FORTINET®

www.fortinet.com

June 28, 2019 8:26 PM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2019:report-operational-technology-forrester Folder:report-operational-technology-forrester