

**INDEPENDENT STUDY
PINPOINTS SIGNIFICANT SCADA /
ICS CYBERSECURITY RISKS**

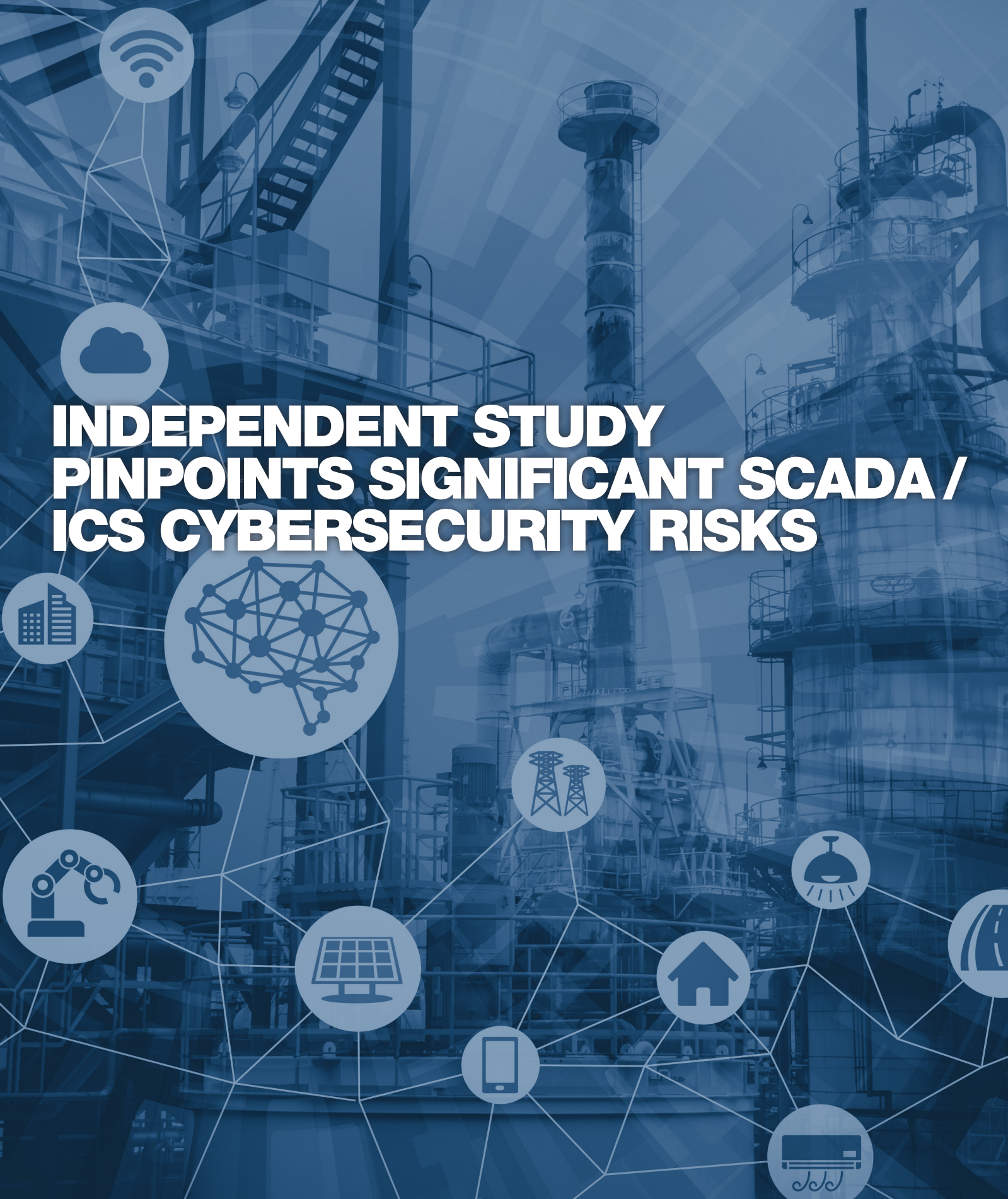










TABLE OF CONTENTS

	Executive Summary	3
	Introduction: SCADA/ICS Are Attractive Targets	4
	SCADA/ICS Quickly Growing—in Depth and Breadth	5
	Challenges to SCADA/ICS Security	7
	SCADA and ICS Threats	9
	Impact of Threats	10
	Recommendations on Mitigating Risks	11
	The Road Ahead	12

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 aren't taking advantage of many of the security tools available to protect SCADA/ICS. About **half** of those surveyed **haven't deployed Secure Shell (SSH) or Transport Layer Security (TLS) traffic encryption** for their SCADA/ICS, and many don't 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 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.

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 isn't 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.



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.

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

² Kim Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid," Wired.com, March 3, 2016.

³ John Leyden, "Water Treatment Plan Hacked, Chemical Mix Changed for Tap Supplies," TheRegister.co, March 24, 2016.

SCADA/ICS QUICKLY 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 plants, 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.

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.

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

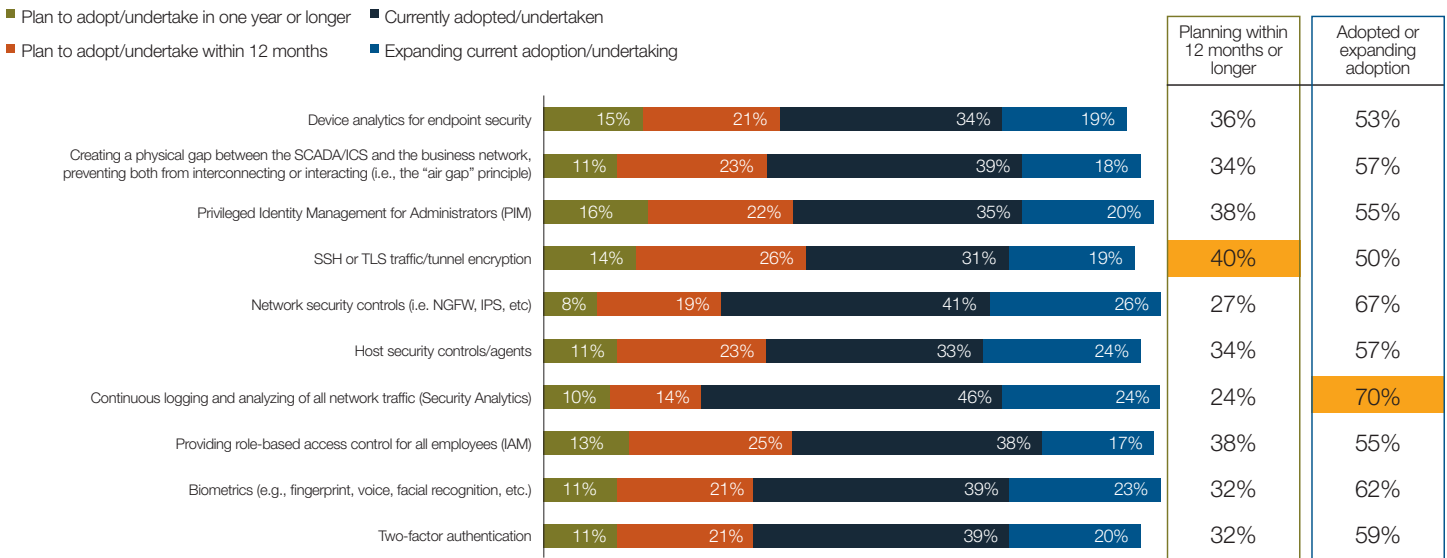
⁵ Mark Fabro, "Industrial Control Systems Cyber Security," Presentation to U.S. Department of Defense, June 7, 2017.

⁶ "SCADA Market Worth 13.43 Billion USD by 2022," Markets and Markets, accessed April 12, 2018.

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

MOST ORGANIZATIONS CURRENTLY UNDERTAKE NUMEROUS MEASURES TO SECURE THEIR SCADA/ICS

Q1- What are your organization's plans to adopt or undertake the following measures to secure your organization's 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

MOST SCADA/ICS OPERATORS CONTINUOUSLY LOG AND ANALYZE NETWORK TRAFFIC, WHILE JUST OVER HALF DEPLOY DEVICE ANALYTICS FOR ENDPOINT SECURITY.

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

Many SCADA/ICS operators ignore basic security tools.

45% don't use role-based access control.

This creates openings for insider threats.

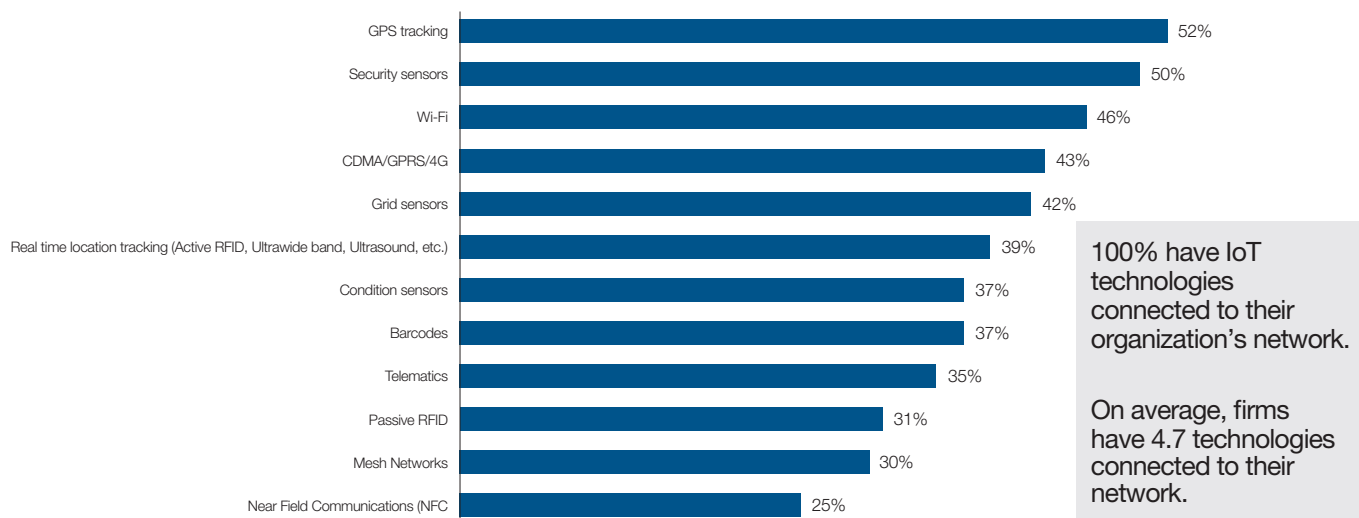
CHALLENGES TO SCADA/ICS SECURITY

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 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.

IoT TECHNOLOGIES CURRENTLY CONNECTED TO THE NETWORK

Q13 - Which of the following Internet of Things (IoT) technologies are currently connected to your organization's network? (Select all that apply.)



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

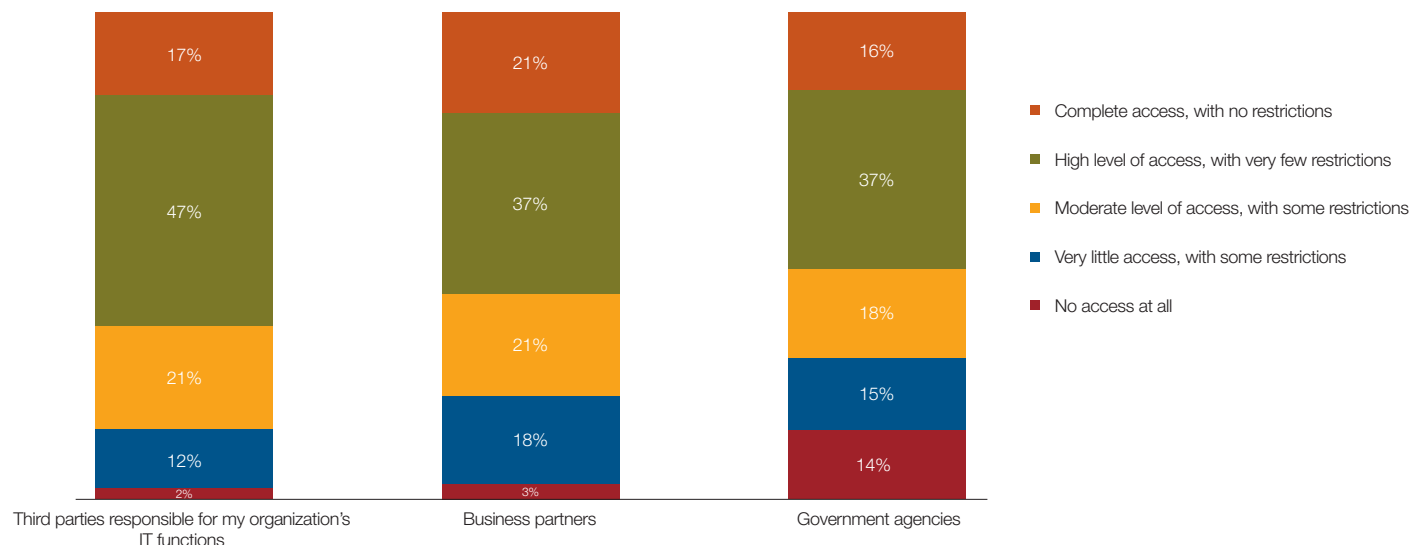
MOST SCADA/ICS USERS HAVE A LARGE NUMBER OF OTHER TECHNOLOGIES CONNECTED TO THEIR NETWORKS.

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 information technologies (IT) and their operational technologies (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 back doors 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.

MOST ORGANIZATIONS GRANT OUTSIDE PARTIES WITH COMPLETE OR HIGH LEVEL ACCESS

Q3-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

MANY SCADA/ICS USERS GIVE TECHNOLOGY VENDORS AND OTHER BUSINESS PARTNERS HIGH-LEVEL ACCESS INTO THEIR SYSTEMS.

For example, **64%** of organizations give third-party IT vendors either complete or high-level access to their SCADA/ICS. But the problem doesn't 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 don't work well together.**

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

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

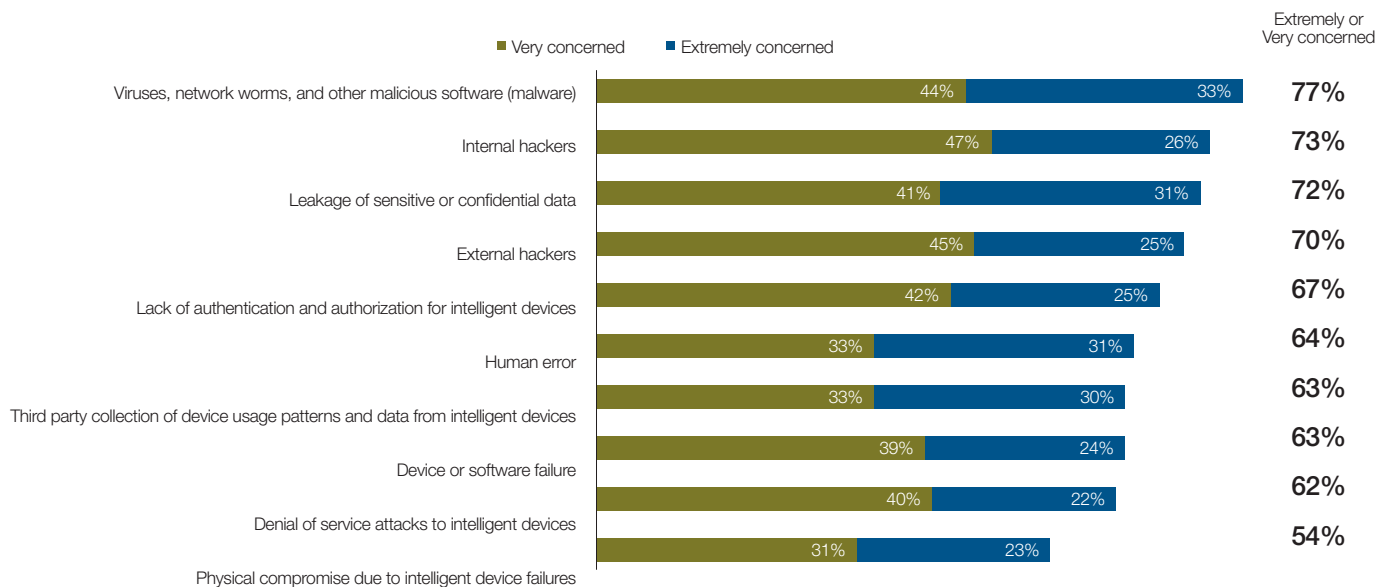
Your IT vendor's vulnerability may be your own.

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.

SECURITY CONCERNS RANGE FROM VIRUSES AND HACKERS TO DATA LEAKS AND LACK OF AUTHENTICATION

Q7- 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

SCADA/ICS OPERATORS ARE CONCERNED ABOUT MALWARE, INTERNAL HACKERS, AND SEVERAL OTHER THREATS.

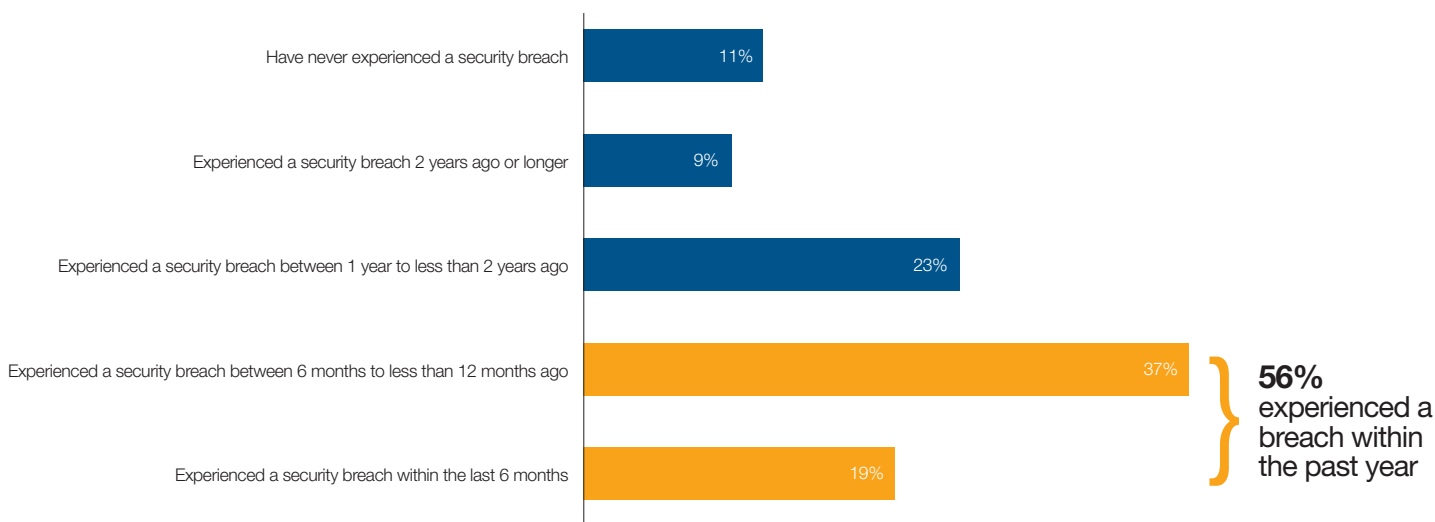
Concerns over malware and internal hackers have grown since a similar study was conducted in 2016. And while the threat landscape has evolved substantially since then and there is a heightened level of risk to SCADA/ICS, SCADA/ICS operators perceive that risks have actually diminished. For example, human 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.

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've never had a breach.

56% OF ORGANIZATIONS HAVE EXPERIENCED A SCADA/ICS SECURITY BREACH WITHIN THE PAST 12 MONTHS

Q8-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

MOST SCADA/ICS USERS HAVE EXPERIENCED A SYSTEMS BREACH IN THE PAST YEAR.

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.

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.

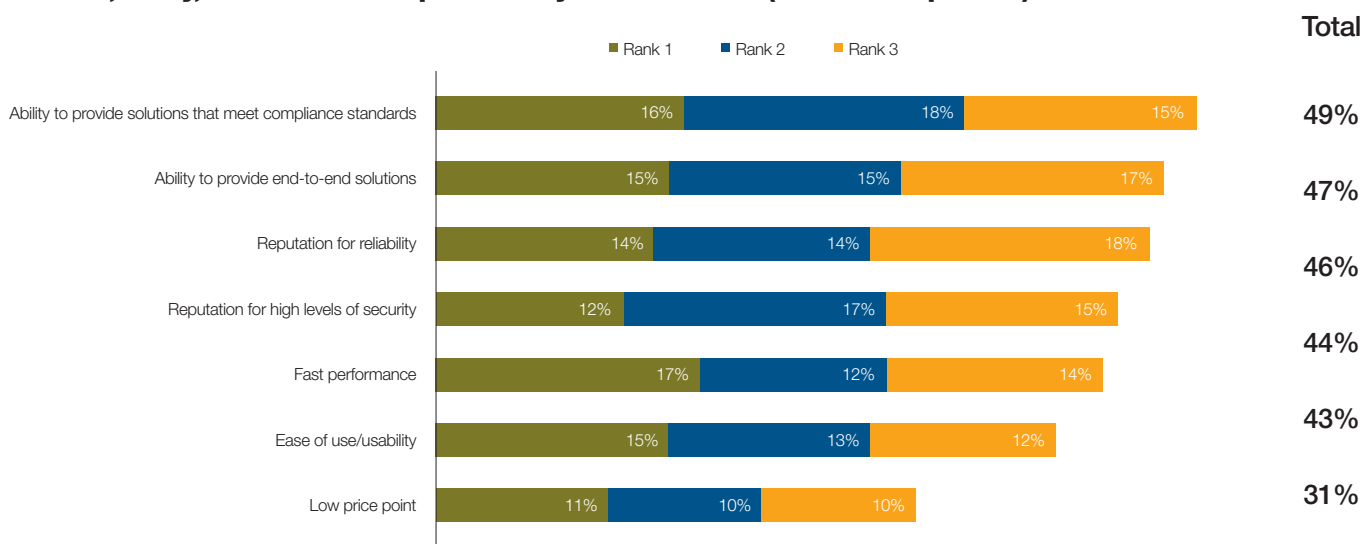
For the evaluation of security providers and technologies, organizations should consider their ability to deliver:

- 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

Q20-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

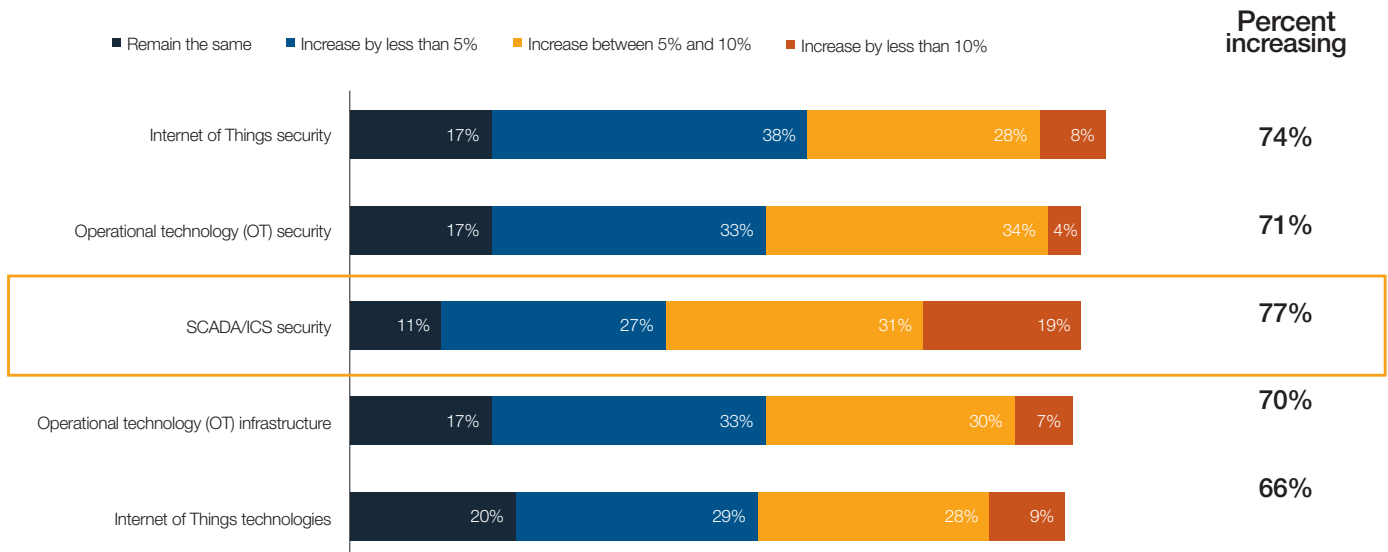
SCADA/ICS USERS HAVE SEVERAL PRIORITIES FOR SECURITY VENDORS, INCLUDING THE ABILITY TO MEET COMPLIANCE STANDARDS AND THE ABILITY TO PROVIDE END-TO-END SOLUTIONS.

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.

SPENDING IN SCADA/ICS SECURITY IS INCREASING MORE THAN IN OTHER AREAS

Q20-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

MANY OPERATORS OF SCADA/ICS PLAN TO INCREASE SECURITY SPENDING IN SEVERAL AREAS IN 2018.

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 don't 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.



GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990