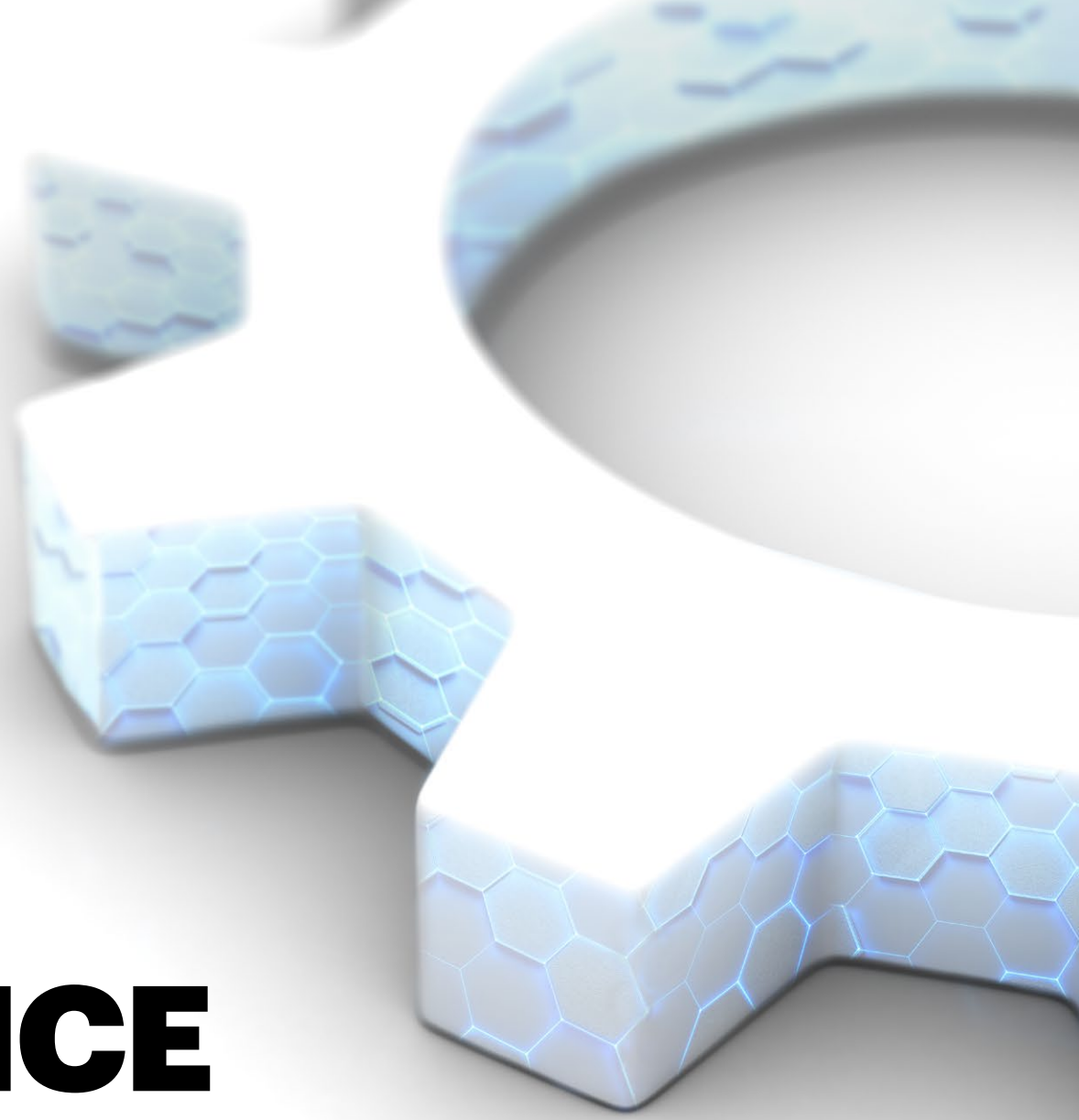
accenture



INDUSTRIAL EQUIPMENT

BUILDING CYBER RESILIENCE

A changed landscape for industrial equipment

In 2020, industrial equipment companies have shown a new agility. As COVID-19 prompted industrial equipment leaders to switch over manufacturing lines to produce life-saving equipment, many companies have been exemplary in stepping up to the operational challenges the crisis presented. From John Deere helping to build two hospitals in two weeks in Wuhan, China, to Bosch developing a rapid-testing machine for COVID-19 samples[i], industry leaders are using their businesses for the collective good. They've modified their operations with amazing speed.

We do not believe industrial equipment companies will go back to their previous ways of doing business. The partnerships, ecosystems, speed and digital capabilities that this health crisis has prompted will continue into the future. As industrial equipment increasingly becomes a web of smart, connected products and services, companies must work in new ways.

And with those new ways of doing business come new ways of securing the business in the cyber realm—ways most companies knew they needed to head toward, but are now accelerating because of the crisis. Getting the basics right is more important than ever, but companies must also approach cybersecurity differently from a macro perspective. An adaptive security approach helps make companies more cyber resilient, given the increased number of remote workers and ecosystem partners within any one business.

Our research shows three out of every four industrial equipment companies (74%) reporting the cost of staying ahead of cyber attackers is unsustainable. Finding new, cost-effective ways to keep your company secure and resilient in the cyber realm needs to happen sooner rather than later.

What is cyber resilience?

Cyber resilience means a company can continue conducting business without real interruption for any length of time. Even though adverse cyber events are unavoidable, cyber-resilient companies better anticipate, identify and contain cyber breaches than other companies. This means they can better protect critical information. Providing that protection is crucial to creating the consumer, partner and employee trust necessary to be truly competitive.

Staying the course is not an option

Industrial equipment companies report cost increases averaged across 17 components of cybersecurity.

57%

of organizations report cost increases in the last two years.

22%

of organizations report cost increases of more than 25 percent.

Security components ranked by biggest cost increases

1. Network security
2. Threat detection
3. Security monitoring
4. Cyber risk management
5. Firewalls
6. Threat intelligence
7. Application security
8. End-point detection and response
9. Incident response
10. Identity and access management
11. Vulnerability management
12. OT-related security
13. Privileged access management
14. Staffing (or People)
15. Remediation
16. Governance, risk and compliance
17. SIEM and event consoles

74%

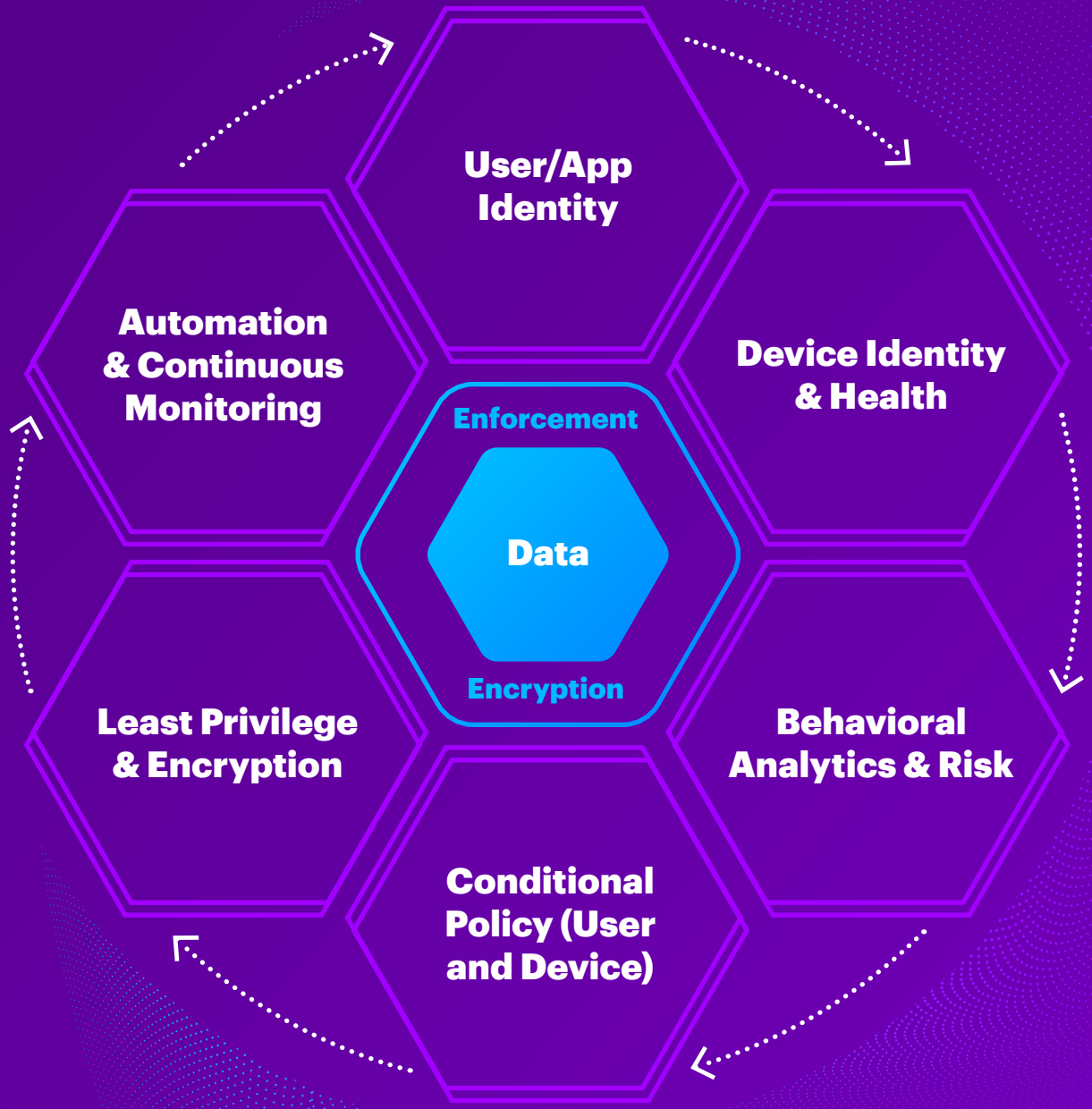
say staying ahead of attackers is a constant battle and the cost is unsustainable.

Adaptive security technologies can help.

Adaptive security: Dynamic cybersecurity for dynamic businesses

With the increasing amount of remote work generated by COVID-19 likely to continue, we expect more companies to move to adaptive security. Adaptive security is powered by analytics and automation. It enhances the security posture of any organization and is particularly effective for companies with an increasing number of system entry points. It works against opportunistic and targeted attacks, as well as trusted insiders and other insider threats.

Adaptive security means constant verification. Even if a user is inside a company's network, a company will not assume it's safe. Instead, it is provided granular user-access control as never before for authentication and verification. Unlike traditional static security approaches, adaptive security includes context-aware security access policies and controls. These shift dynamically based on the risk of every access request, and help a business detect anomalies faster and more accurately.



Cybersecurity basics matter more than ever

While some industrial equipment businesses already were transforming their cybersecurity to support new, innovative ways of doing business, COVID-19 has accelerated the move for many. Adaptivity is an important overarching approach to cybersecurity, but companies still need to get some traditional basics right to be protected.

Recent Accenture research shows 13% of industrial equipment companies are more secure in the cyber realm than their peers.[ii] These Leaders achieve significantly higher performance than their industry peers in at least three of four basic areas:

Find breaches faster

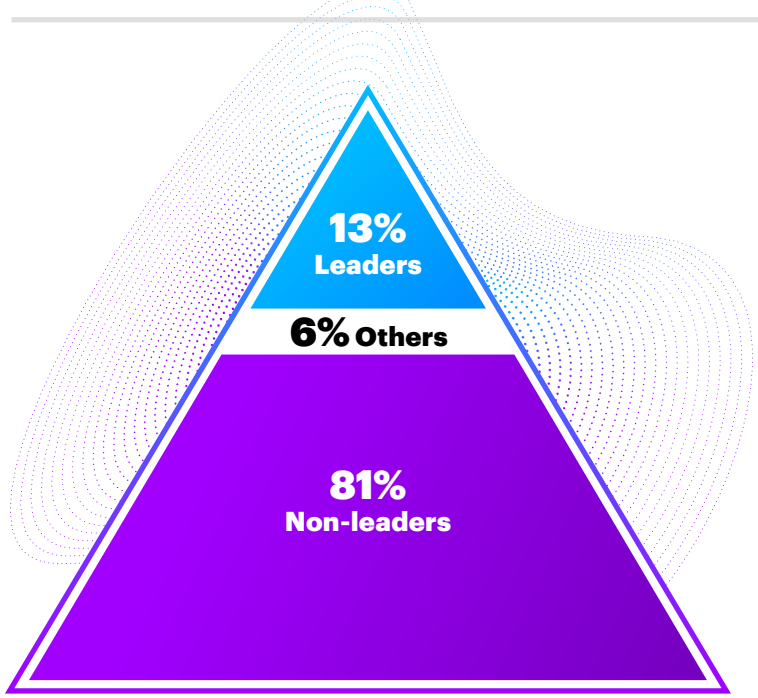
Fix breaches faster

Stop more attacks

Reduce breach impact

But Leaders aren't just achieving higher performance—they are actually more cyber resilient than their fellow industrial manufacturers, **without spending any more money.** Let's take a look at what they're doing right.

Leaders are more cyber resilient without spending more money



Leaders don't invest more. They invest differently.

The majority of industrial equipment companies (88%) are spending 20%+ of their budget on advanced technology investments.

Artificial Intelligence (AI), Next-Generation Firewall (NGF) and Risk-Based Authentication (RBA), among other advanced technologies, go a long way toward fortifying cybersecurity in today's partner-based business models. And while those partner-based business models are a boon to business, they can increase a company's risk exposure.

While survey participants did not rank Privileged Access Management (PAM) among their priority technologies, we see an increasing number of our clients utilizing it. The growing number of internal and external access points, as well as a deluge of data, make IT access a pressure point for many companies—one they are addressing as their work becomes more remote and distributed.

Cybersecurity technologies: What Leaders prioritize

Leaders' priorities	SOAR	AI	NGF	RBA	RPA	PAM
Faster incident detection	#2	#1	#3	#4		
Faster incident response	#1	#1		#4	#3	
Shorter recovery times	#1	#2		#3	#4	

AI Artificial Intelligence (Machine Learning/Natural Language Processing)

NGF Next Generation Firewall

PAM Priviledged Access Management

RBA Risk-Based Automation

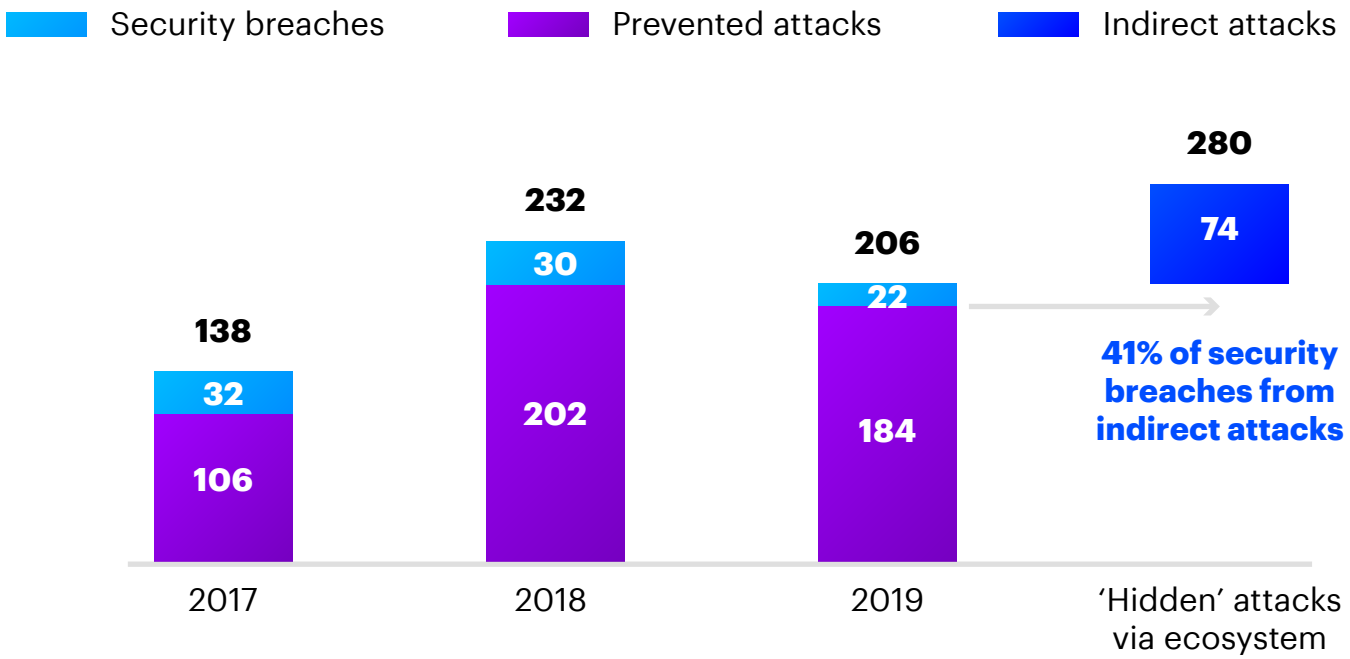
RPA Robotic Process Automation

SOAR Security, Orchestration, Automation, Response

Protecting the weakest link

Our research shows that 40% of security breaches now come from indirect attacks, meaning they are generally supply-chain-related attacks that come via an industrial equipment company's ecosystem. As business partners become more connected, particularly in the supply chain—delivering connected experiences and products utilizing the Internet of Things (IoT)--their potential entry points for cyberattacks multiply. So, while partnering is essential for the progress of business, it requires a new approach to cybersecurity and cyber resilience.

"Hidden" ecosystem attacks pose huge risk



Leaders' strengths: Speed, scale and collaboration

Speed.

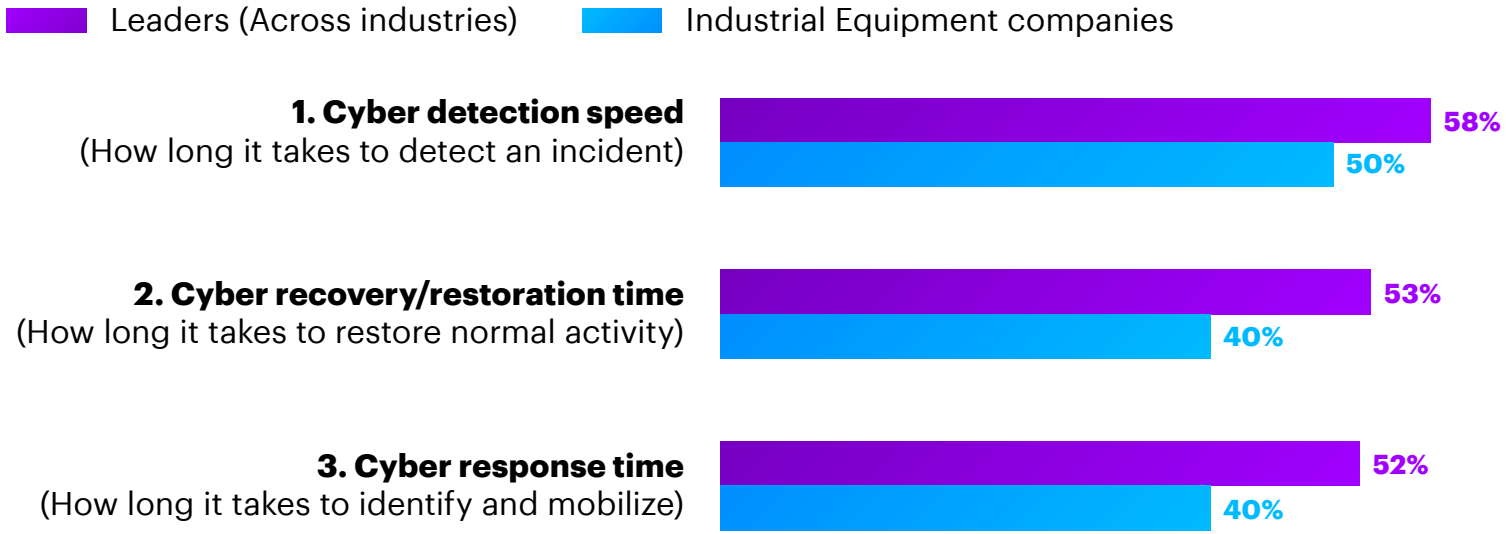
Industrial equipment cybersecurity Leaders know speed matters, but they approach speed from multiple angles: detection speed, response time, and recovery/restoration speed. All three areas are crucial to not just cybersecurity, but also to cyber resilience over the longer term. In particular, cybersecurity teams are using AI and SOAR (Security, Orchestration, Automation, Response) technologies to improve the efficiency of their operations.

Take action

Invest in the advanced digital security technologies Leaders are using, like AI and SOAR, and Risk-Based Automation.

Prioritize moving fast

Top three ways leaders measure the success of their cybersecurity program

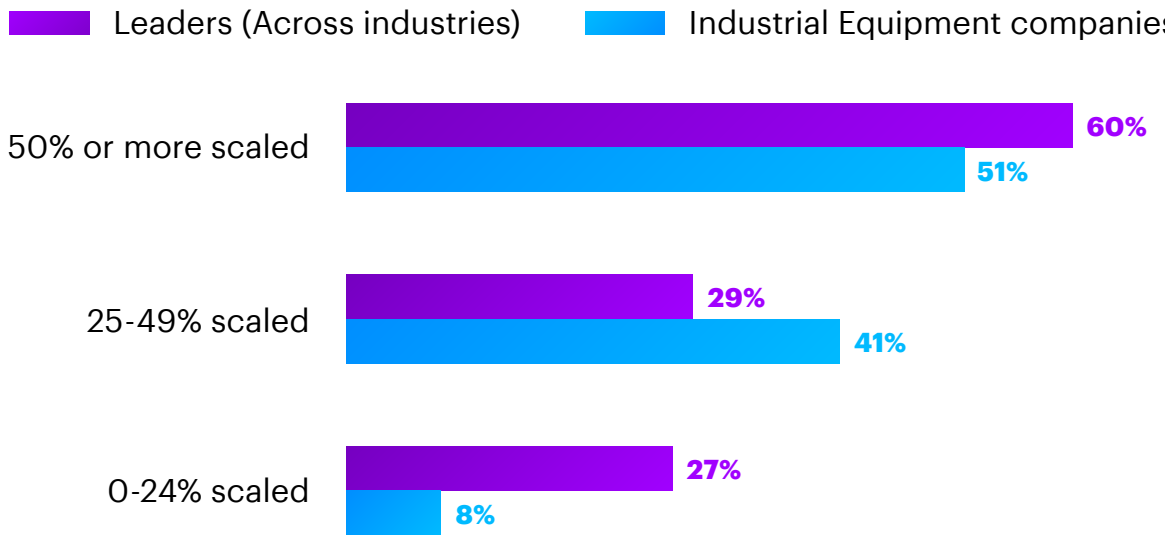


Scale.

It's no coincidence that Leaders are 4X better defending against attacks—they scale security technologies significantly more than their peers. More than half of Leaders (51%) scale half or more of their security tools throughout the enterprise, providing them a much broader base of protection. We are helping an increasing number of industrial equipment clients bring operational technology and the Internet of Things into the mix as part of these broad-based deployments.

Scale more: Leaders 4X better at defending attacks

The percentage of the security tools piloted then scaled and used throughout the enterprise



Take action

Move out of pilots and pockets of progress to broad-based deployments, centralizing control of cybersecurity.

Collaboration.

Leaders are more tapped in, not only to business partners but also to the industry security community. They more often share knowledge of threats with their ecosystem as well as the industry as a whole, and they collaborate with both more often to test cybersecurity resilience. This is essential because, with downtime for some manufacturers costing millions of dollars per day, the industry is a prime target for threats like ransomware. Shared threat intelligence goes a long way toward helping not just individual companies, but the industrial equipment industry collectively.

We find that the vast majority of cyberattacks are not new types, yet they occur again and again. The faster industrial equipment companies share these threats and collaborate with each other to stop them, the safer the entire industry will be in cyber space. Keeping quiet about a threat simply worsens the number and intensity of similar attacks across the industry.

It is no surprise, given their proactivity and collaborative practices, that Leaders are also more likely to be involved with developing cybersecurity standards for the industry.

Emphasizing collaboration does not mean Leaders take a rosy, unrealistic view of its potential risks. Secure collaboration becomes more important than ever as travel ecosystems grow. With approximately four out of 10 attacks on industrial equipment companies occurring through weak links in the supply chain—from compromises in shared IoT technology to internal weaknesses in managed service providers within the ecosystem—addressing partner vulnerabilities is a must.

Take action

Share threat information through industry cybersecurity organizations. Create cybersecurity standards for your ecosystem.

Collaborate more: Leaders 2x better at defending attacks

Main ways organizations that are best at collaborating work with partners

Cyber resilience: A journey, not a destination

Cyber resilience is not a one-and-done endeavor. Because the threat landscape is always changing, as is technology, it's a continuous process. Leaders are blazing a trail other companies can follow, with an imitable example for how it's done. They're partnering with the business side of the house to evolve cybersecurity as the business evolves.

To follow in their footsteps, industrial equipment companies need to broaden their scope with adaptive security. They'll need to look beyond the basics and into areas where the business has moved into new frontiers, requiring broader, deeper or newer types of protection:

Protect factory systems in real time

Secure adoption of cloud services will help protect industrial factory systems, as security can be updated in real time in the cloud.

Extend protection to the entire enterprise

Protections now must be built into the entire enterprise, from IT/OT network anomaly detection to vulnerability management.

Create partner cybersecurity standards

Given the number of attacks that could stem from any supplier in the ecosystem, industrial equipment companies need to monitor not only their own cybersecurity, but also ensure partners adhere to strict standards of adaptive security.

Focus on cybersecurity for connected products

Detection and response capabilities are crucial not only to protecting the products industrial manufacturers are putting into customers' hands but also the entire industrial internet of things (IIoT).

As industrial equipment companies settle into a changed landscape during and post-COVID-19, they are experimenting with many new ways of doing business. And with those new ways of doing business come new ways of securing the business in the cyber realm.

Many companies are already on the road to greater cyber resilience, but COVID-19 accelerates that journey, making it all the more important.

We're here to help.

Contacts

Daniela Altamirano
Senior Manager, Security
daniela.altamirano@accenture.com

Benjamin Janzer
Senior Manager, Security
benjamin.janzer@accenture.com

Ganesh Narayanan
Senior Manager, Security
ganesh.v.narayanan@accenture.com

Lars Zywietz
Managing Director
Industrial Equipment, Security
lars.zywietz@accenture.com

Matthias Wahrendorff
Senior Principal, Industrial Research Lead
matthias.wahrendorff@accenture.com

About Accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries—powered by the world's largest network of Advanced Technology and Intelligent Operations centers. With 513,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at **www.accenture.com**

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Visit us at **www.accenture.com/security**

About the research

Accenture Research conducted its third annual cybersecurity study with 4,644 security executives in 16 countries. We collected responses from companies with $US1B+ in revenue, across 24 industries. This report is our analysis of 425 industrial equipment executives.

References

[i] https://wasteadvantagemag.com/stepping-up-to-help-diesel-industry-leaders-innovate-during-covid-19-pandemic/
[ii] All data is from Accenture Research Cybersecurity study, unless otherwise noted.