accenture

AUTOMOTIVE CYBERSECURITY

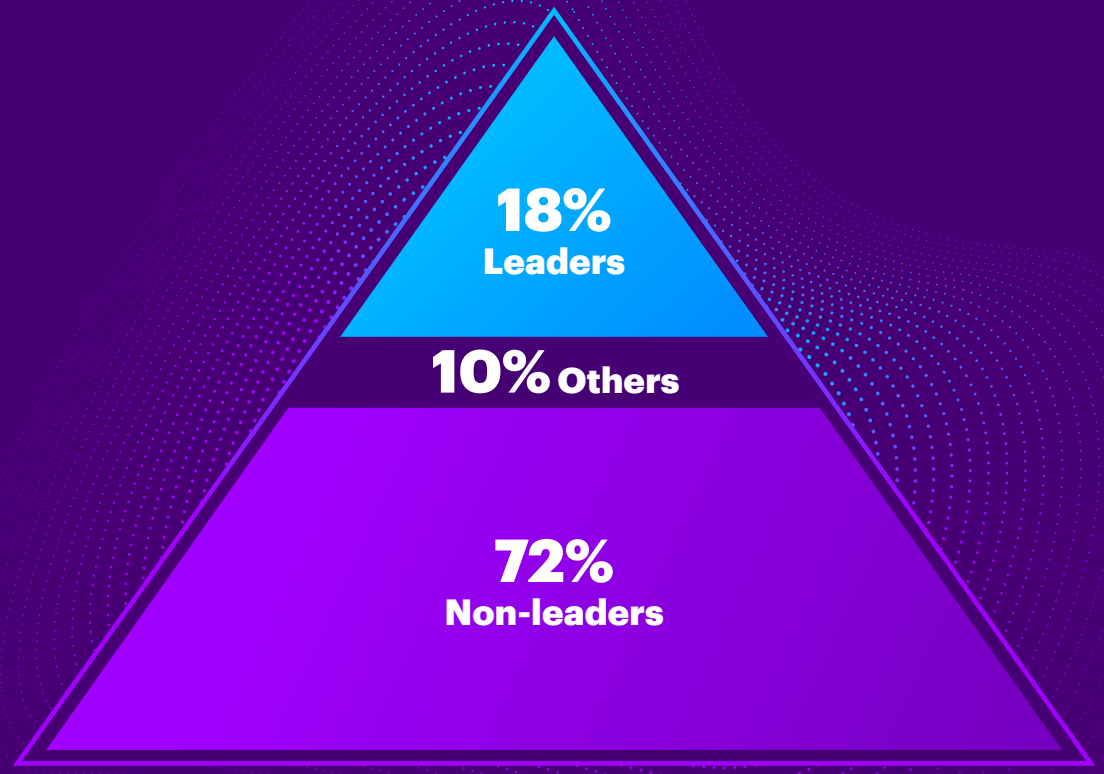
SHIFTING INTO OVERDRIVE

When an industry completely reinvents its products and its ways of doing business, it's an exciting challenge. When it does so in the middle of a pandemic, it's a heroic effort. The automotive industry has grappled with both scenarios in 2020.

Auto companies were already focused on moving to connected, clean vehicles prior to COVID-19, but have now found themselves challenged to retool and reorient to manufacture life-saving products like ventilators.

The learned agility that came from their COVID-19 efforts will likely help auto companies as they revitalize post-pandemic. And as they do, they'll need new cybersecurity measures to help them protect their new ways of doing business.

Some automotive companies were already ahead of the curve in cybersecurity, according to our most recent research. Accenture's detailed modeling of cybersecurity performance identified an elite group—just 18%[i]—that achieve significantly higher levels of performance in at least three of these categories:



Stop more attacks

4x

Leaders have nearly a fourfold advantage in stopping targeted cyberattacks.

Find breaches faster

4x

Leaders have a fourfold advantage in detection speed.

Fix breaches faster

3x

Leaders have a threefold advantage in speed of remediation.

Reduce breach impact

2x

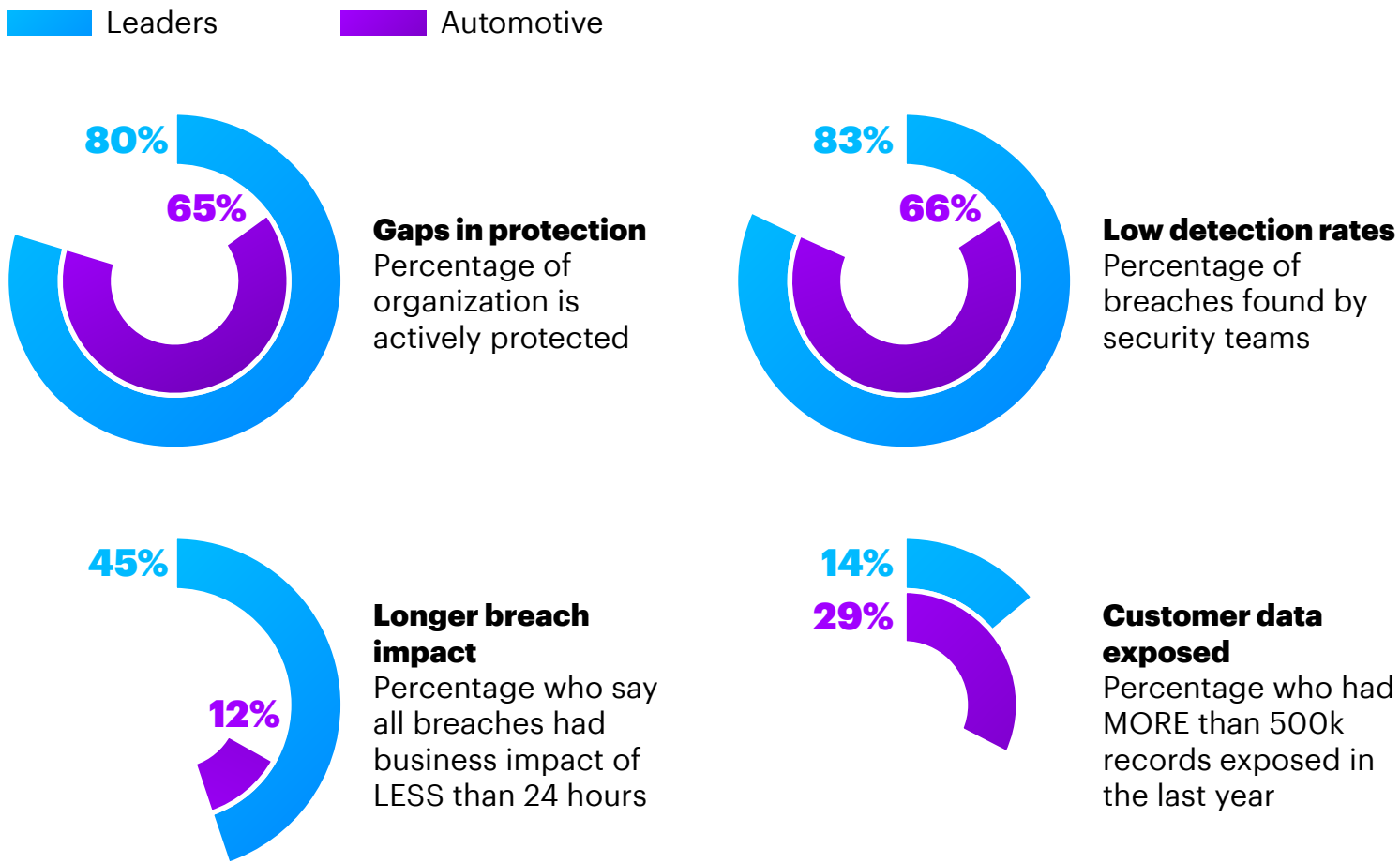
Leaders have a twofold advantage in containing damage impact.

What can other automotive companies learn from the cybersecurity Leaders in their industry? We're glad you asked.

Leaders' investments in innovation are working

While the majority of companies' security investments are failing, Leaders have a better cybersecurity track record. One of the major reasons, according to our study, is their investments in innovation. The vast majority of automotive cybersecurity leaders spend more than 20% of their cybersecurity budgets on advanced technologies—the kind that support the innovation their company is baking into their business.

Failing investments



Artificial Intelligence (AI) and Security, Orchestration, Automation, Response (SOAR) technologies top the list of advanced technologies automotive cybersecurity Leaders are investing in. But others, as you can see from the chart, are contributing to their cybersecurity ranking and success.

Leaders' priorities	SOAR	AI	NGF	RBA	RPA	PAM
Cyber detection speed	#2	#1	#3	#4	#6	#5
Cyber recovery time	#1	#2	#5	#3	#4	#6
Cyber response time	#1	#1	#5	#4	#3	#6

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

Regulating vehicle cybersecurity puts heavy responsibility on manufacturers

Currently, there are few legal regulations on cybersecurity in the automotive sector. In mid-2020, Regulations (WP.29)—a working party of the Sustainable Transport Division of the United Nations Economic Commission for Europe (UN ECE)—will change that in Europe.

As we write this cybersecurity report, the UN ECE will issue in late 2020 or early 2021 a regulation on cybersecurity in connected and autonomous vehicles. It provides uniform provisions for the approval of vehicles' cybersecurity and cybersecurity management systems (CSMS). The regulation will also cover software updates and software update management systems (SUMS).

WP.29 has many facets, but its major focus areas include:

Increased focus on secure management across entire automotive supply chain

Mandates for monitoring and incident response from the Original Equipment Manufacturer during post-production

Security certifications per vehicle type

High focus on securing and controlling data-at-rest and data-in-transit, especially when it comes to data regarding Personally Identifiable Information (PII) data.

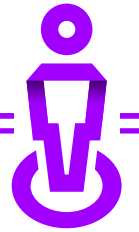
As the automotive industry moves more and more to connected cars, cybersecurity being in lockstep with the business becomes even more of an imperative.

New innovations, new challenges

Two developments open automotive manufacturers up to increasing cybersecurity challenges. The first is the more remote method of working due to COVID-19, a method that may continue for some time. And the second is the increasing business and technology partnerships automotive companies are forging as they move from producing a vehicle that is primarily of their making, to a vehicle that is a collection of software-based services and systems.

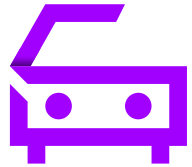
Challenge 1: More remote workers

The first challenge, **more remote workers**, is one most industries are facing. From securing personal devices and networks, to protecting collaboration technology like video-conferencing and file sharing, automotive companies will need to make some enhancements in their existing security to close gaps. It is a challenge but one where they can share solutions with thousands of companies the world over.



Challenge 2: Connected cars

The second challenge—**connected cars**—is a tougher one because it's unique to the industry. And, it relates not only to privacy and the usual security concerns, but also to a life-or-death matter—the safety of passengers and other drivers.

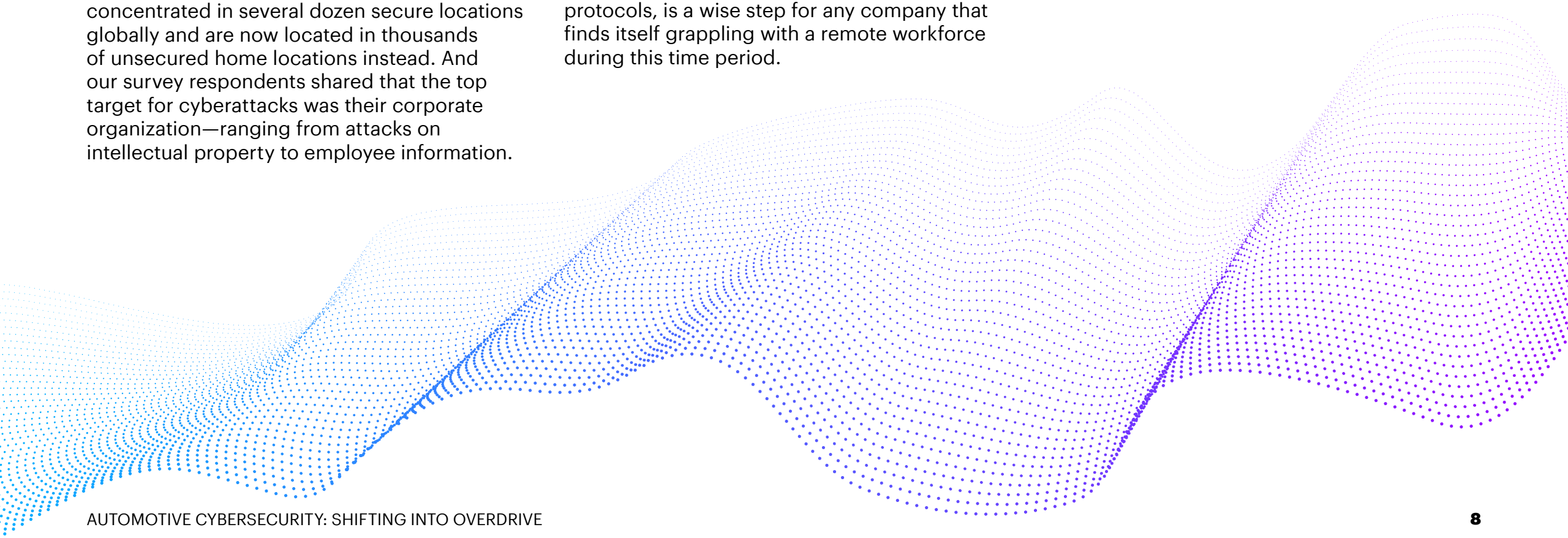


Gearing up for remote working environments

Some companies, like Accenture, were well-versed in remote working environments prior to COVID-19. But many automotive companies were still in a traditional office structure. As a result, they have been racing to accelerate their cybersecurity protections for employees—who might previously have been concentrated in several dozen secure locations globally and are now located in thousands of unsecured home locations instead. And our survey respondents shared that the top target for cyberattacks was their corporate organization—ranging from attacks on intellectual property to employee information.

Phishing by cyberespionage and cybercriminal groups, as well as nation-state-sponsored cyberthreats, are huge risks right now—particularly for companies that have not had to address at-home protection previously.

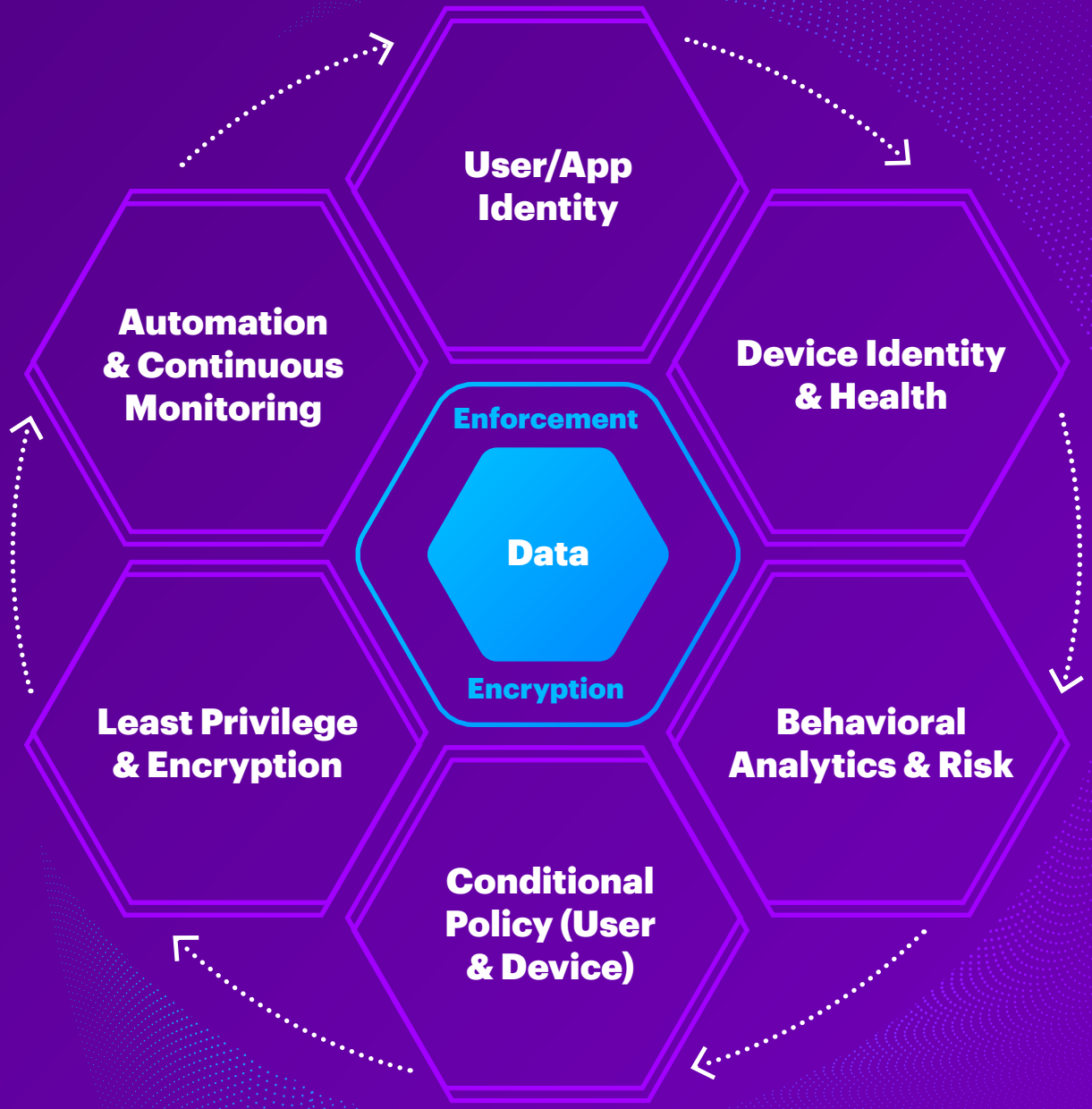
Adaptive security, based on zero-trust protocols, is a wise step for any company that finds itself grappling with a remote workforce during this time period.



Zero Trust Systems: 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 zero trust systems and adaptive security. They are powered by analytics and automation and enhance the security posture of any organization. This approach 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.

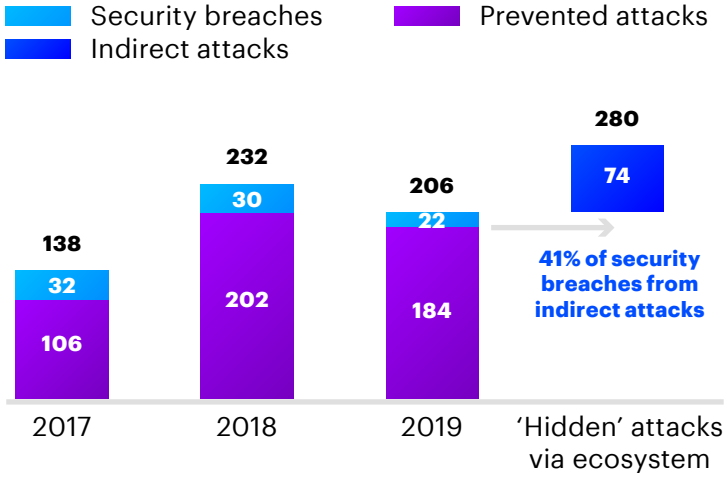
Zero trust means constant verification. Even if a user is inside a company's network, a company will not assume it's safe. Instead, it is provided granular user-access control as never before for authentication and verification. Unlike traditional static security approaches, adaptive security includes 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.



Connected car systems need to be a cyber-fortress

Cybersecurity for connected vehicles involves a continuous end-to-end chain, from the service delivery platform to mobile apps to in-vehicle telemetry. AI and machine learning to help detect unknowns and anomalies within a car's system are key—but so are advanced technologies to support the ecosystem partnership systems that created the car.

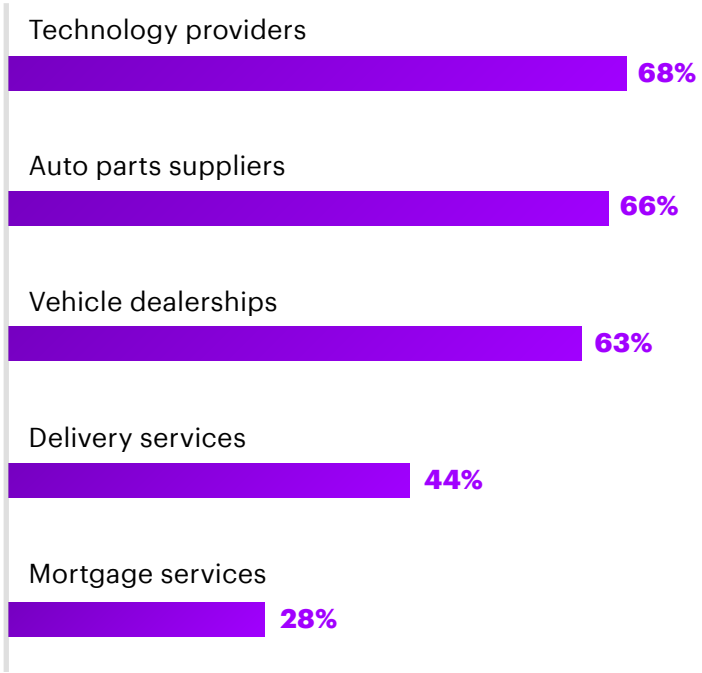
Cybercriminals target ecosystems as weak link



And our research shows that 41% of automotive company security breaches come from indirect attacks, or hidden attacks via their ecosystem.

Currently, only roughly two-thirds of automotive companies oversee the cybersecurity practices of their technology providers, auto parts providers and dealerships. Delivery and other services rank even lower. This practice leaves a huge door for cybercriminals to enter—and they are, with increasing speed and force. It's no surprise, then, that managing security over multiple stakeholders was the top challenge auto companies cited to managing cybersecurity in their industry.

For which of the following does your company oversee and monitor the cybersecurity practices as part of doing business together?



A cybersecurity strategy fit for innovation

Automotive companies need a cybersecurity foundation fit for purpose—and that purpose has changed. As manufacturers invest in emerging technologies and decouple their core architecture to allow for innovative collaboration, their cybersecurity strategy needs to change. Many are handling the basics well, but the business has moved beyond basic cybersecurity needs.

The sophistication and severity of cyberattacks is increasing at an alarming rate, significantly impacting companies across industries. The average cost of cybercrime for an organization has increased US$1.4 million to US$13.0 million.[ii]

Now more than ever, as auto companies move from vehicle manufacturing specialists to technology ecosystem specialists, their cybersecurity needs become far more complex and critical. A connected car stems from a web of interconnected companies with varying levels of cybersecurity expertise.

"The future of the industry will be characterized by partnerships that deliver more than any one company could deliver on its own."

Accenture Tech Vision

Focusing on action in a few key areas can help automotive companies advance their cybersecurity to better meet the new needs of the business:

Reassess cybersecurity using an end-to-end approach. New regulations are a bellwether for things to come, holding automotive companies responsible for secure management of areas like data at rest and data in transit. Cybersecurity in an intelligent vehicle has become a matter of life or death.

Look beyond traditional boundaries. Auto companies will more and more have to take cybersecurity standards and enforcement across the ecosystem and their own distributed operations into their hands to protect their own interests.

Take a proactive stance with regulators and shared industry intelligence. Regulators need input from automotive companies to create standards that protect consumers but are also realistic for manufacturers.

Reaching out to offer assistance and subject matter expertise helps ensure a public/private partnership for the mutual good. And industry groups like the **Automotive Information Sharing and Analysis Center** (Auto-ISAC) serve as a global information-sharing community to address vehicle cyber security risks. Auto-ISAC operates a central hub for sharing, tracking and analyzing intelligence about cyber threats, vulnerabilities and incidents related to the connected vehicle. The more companies that actively participate, the better the resources marshaled against cyber attackers.

As cars become connected products and consumers begin to clamor for the Next Big Thing that will transform their riding and driving experience, the need to protect not only those consumers, but also their own employees and business continuity, becomes paramount. The innovation so very necessary to leapfrog the auto industry to the next level brings some very serious potential risks in the cyber realm. Automotive companies that move now to anticipate and address those risks set themselves up to move into their future more rapidly—and more safely.

Contacts

Brian Irwin
Lead – Automotive, North America
Managing Director
brian.irwin@accenture.com

Alberto Meneghini
Automotive, Security
Managing Director
alberto.meneghini@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 509,000 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 responses from 100+ executives in the automotive industry.

References

[i] All data is from Accenture's Cyber Resilience research, unless otherwise noted.

[ii] "The Cost of Cybercrime," Accenture, 2019.