eBook

Protecting Intellectual Property in Automotive

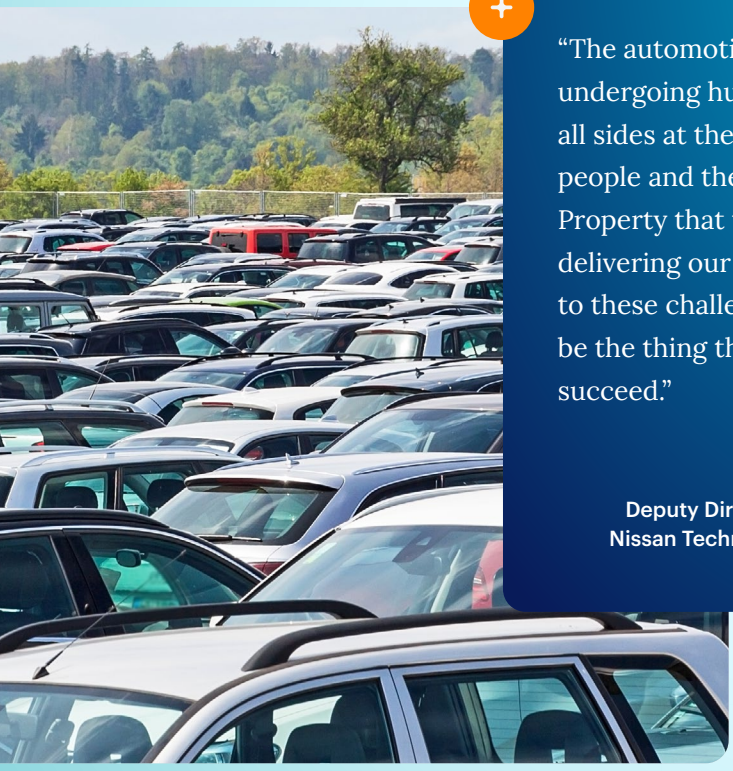
netskope

Introduction

Automotive OEMs are working to completely transform how their customers engage with their brand and products; aiming to better understand the changing customer journey in relation to the product.

Manufacturers have identified profitable growth opportunities through the integration of digital technology into all areas of the business, which has led to digital and data-led transformation, the adoption of agile methodologies, and new technology including blockchain and NFT. But execution has been challenging.

This profound change touches every part of the automotive industry; refocusing R&D, enriching product innovation and digital experiences, upending partnership models and retail.



"The automotive industry is undergoing huge upheaval from all sides at the moment. Our people and the Intellectual Property that they create, is delivering our unique answers to these challenges, and will be the thing that ensures we succeed."

Emma Deutsch,
Deputy Director Test Operations
Nissan Technology Centre Europe

These are just some of the challenges automotive leaders are wrestling:

1. **Radical advances in car design alongside the emergence of new competition**
   Electric cars and the Software Defined Vehicle bring changes throughout the automotive ecosystem. From new partnerships and collaborations, to a radical reinvestment of R&D funds, and an overhaul in manufacturing to shift from component-oriented structures and processes to functional ones; nothing escapes reinvention.

2. **Changes in customer preferences and engagement models**
   The automotive sector is going through the same challenges that faced retail when online became consumers' preferred shopping methodology. The movement of a storefront from a physical location to a digital site is only the start of the changes required for omnichannel and direct to consumer models. Subscriptions and memberships are starting to emerge as part of a seismic change in the relationship between automotive brands and customers.

3. **Data as competitive advantage**
   Software is, in essence, an organizing and presentation system for data, and as such the Software Defined Vehicle is one built from data. Whether looking at the end product, or industrial and operational processes, data is driving the automotive industry. We see this in the use of NFT and blockchain (underpinning subscription models and warranties), as well as through the industry's extensive use of AI for advances such as autonomous driving. Operationally, "data" means competitive advantage and its value only grows.

4. **Changes to the regulatory landscape**, including an intense global focus on emissions. With growing focus on the global climate crisis, the automotive industry is now continually subject to regulations. Around the world, governments are naming dates for when the registration of new combustion engines will be banned, leading to intensive development of battery technologies. Even super and hyper cars are being developed with smaller engines in an effort to balance consumer demand for speed within tightening regulatory windows.

5. **Macro global events and crises impacting operations and supply chains**. Be it the pandemic, global disruptions in supply chains or international sanctions - all these things are forcing the automotive industry to change and to find new solutions for unexpected challenges, including enabling hybrid work.

Automotive OEMs are handling the industry's challenges by:

- Continuing to invest heavily in R&D

  » The automotive sector is the EU's number one investor in R&D, spending almost €59 billion per year.

- Developing basic supply chains into improved Supply Chain Networks, that incorporate all of the facilities, means of production, products, and transportation needed to support supply chain operations and product flow.
- Reversing globalized pooled production infrastructure (which was originally designed to achieve economies and scale) in order to navigate more complex international borders.
- Moving away from a dependency on physical dealerships and developing omnichannel, data-driven, and automated go-to-market models.

  » More than 80% of vehicle buyers use online sources during the purchase-consideration period.

McKinsey (2021) advises CEOs in advanced industries (including automotive and assembly) to follow strategic actions which group into three categories:

- Secure high confidence growth
- Achieve next generation margin and productivity transformation
- Reshape strategy and organizations for the "New Normal"

Sources

The CEO agenda for companies in advanced industries
https://www.mckinsey.com/industries/advanced-electronics/our-insights/the-ceo-agenda-for-companies-in-advanced-industries
https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/a-future-beyond-brick-and-mortar-disruption-in-automotive-retail
https://www.acea.auto/figure/rd-investment-by-industry-world-region/
https://www.pwc.de/ceosurvey2022 and https://www.pwc.co.uk/issues/cyber-security-services/insights/cyber-threats-2020-report-on-global-landscape.html

The implications for data protection

Cloud and digital transformation feature repeatedly among the recommended strategic actions, including:

1. Digital disruption to drive go-to-market approaches.
2. Digital analytics to better assess company performance.
3. Using digital tools to mitigate risks and lower costs.
4. Cloud partnerships to accelerate momentum (creating a focused cloud strategy).
5. Designing an organisation built for speed.

McKinsey also outlines other recommendations requiring significant focus from IT teams, including M&A and the transformation of global footprints and industrial supply chains.

All of these recommendations are either explicitly or implicitly items for the CIO to-do list, and data protection is a critical success factor for them all.

Navigating data threats

According to the 2022 PWC global CEO survey, 49% of global CEOs are very or extremely concerned about cyber risks, but CEOs in the industrial manufacturing and automotive sectors displayed lower levels of concern about cyber risks than any other sector.

The biggest reason for concern around cyber threats was the impact it may have on the organization's ability to sell products and services (62%), with 56% also very or extremely concerned about the impact cyber risks may have on their ability to innovate through technologies and processes.

> "Traditionally, the automotive industry has focused on espionage as the major data protection threat, and the demonstration of security in this area was required ahead of the widespread adoption of cloud. However at the moment, cyber criminals are regularly targeting automotive manufacturers with ransomware attacks, because a sudden halt to production (or a threat to release highly valuable IP) is incredibly strong motivation to pay the ransom. Over the past few months we have seen a number of high-profile targets in the automotive industry."
>
> **Paolo Passeri,**
> **Cyber Intelligence Principal, Netskope EMEA**

Targeting automotive

Germany is a market with extensive automotive interests and in 2021, the German Federal Office for Information Security (BSI) specifically examined cyber risk and security in the automotive industry in detail. The subsequent report identified a number of areas of risk specific to the automotive industry:

Ransomware attacks are the biggest threat to cybersecurity
Cyber criminals primarily aim for financial gain when spreading ransomware and therefore target companies that appear to be financially worthwhile—so-called big game hunting. Automotive manufacturers and suppliers fit this "big game" profile and attackers can cause enormous damage by publishing stolen company data. There are regular media headlines about successful data theft, phishing, or DDOS attacks on companies in the automotive industry.

Production facilities are not prepared for attacks
Thanks to digitalization and Industry 4.0 efforts, modern production plants are often equipped with sensors and robots, and are highly networked. These systems are usually not integrated into the traditional company or supplier networks and are often not connected to the internet, but hardly any protection systems that detect attacks are used in production. Employees in these facilities are also rarely trained in cybersecurity and do not expect targeted system manipulation.

> “As digitization continues to transform business practices across the automotive and mobility sectors, leading to ever-increasing amounts of data, cybersecurity will become as important to dealers and retailers as it is to manufacturers.”
>
> **Lynda Ennis,**
> **Founder and CEO of automotive executive search firm,**
> **Ennis & Co**

Supply chains are closely interlinked and vulnerable
Automotive manufacturers and their suppliers are closely integrated through their work and production processes, as well as their logistical processes and IT systems. They regularly share sensitive information such as design data. Cybersecurity issues at suppliers can quickly have an impact on partnered automotive manufacturers. The high level of networking within supply chains increases both the likelihood and impact of cyber attacks and the potential for damage.

Home office, mobile working, and the cloud are changing security risks
The report acknowledged that the COVID-19 pandemic has led many automotive companies around the world to move staff out of protected workplaces and into home offices—a change that significantly increases the risk of cyber attacks. The reasons given: home office workers are using various different devices over home internet connections, accessing public cloud. New working models require new security concepts.

Source

BSI: Cyber security in the automotive industry - Automotive industry situation report
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive.html

Vulnerabilities in the system

The average manufacturing organization (500-2,000 users) uses

1522 applications

98% of which are unmanaged by IT teams.

113 of those apps are used to upload, create, share or store data.

Source of malware downloads:

31% cloud apps

69% web

netskope

Top 5 apps for malware downloads within manufacturing organizations

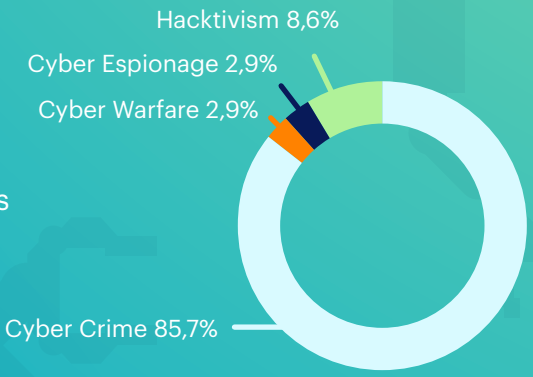
5

- Box
- Weebly
- SourceForge
- OneDrive
- Github

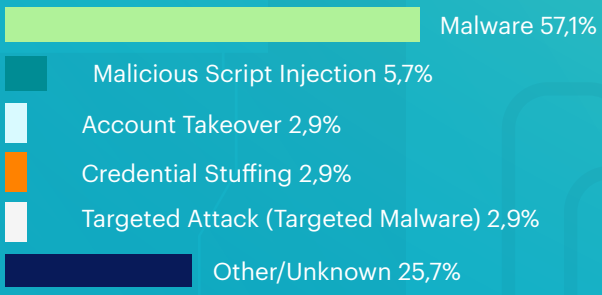
Top app categories for malware downloads

» cloud storage
» development tools

Jan-Jun 2022, motivations for attacks on manufacturing organizations



Jan-Jun 2022, techniques deployed in attacks on manufacturing organizations



Data-centric security

Today, in most companies, the data center is no longer the center of IT systems. More and more companies are using a mixture of private and public cloud services from the likes of AWS, Microsoft Azure, or Google Cloud to take advantage of significant cost savings and efficiencies.

At the same time that the centralized data center has fragmented, the workforce has broken apart too; no longer a perimeter-based office hoard, it is now a hybrid collective, working from home and across other shared locations. Work styles were already changing, but the pandemic has sped up this change and given it enough momentum that most organizations do not ever expect the workforce to fully return to the office in the way they were before.

This hybrid workforce is no longer confining their work to corporate owned and managed devices either. Personal and mobile devices are commonly being used to perform work tasks, and corporations are taking full advantage of personal home peripherals such as printers and webcams.

In this new model, you can no longer rely on the security of the data location, or the network, and you can no longer guarantee security of the user or endpoint device. New working practices and technology architectures require data-centric security; securing data wherever it goes.

Market analyst Gartner recognized this development and in 2019 presented a new approach to security architectures in its report “The Future of Network Security Is In The Cloud” in which it introduced a new concept: Secure Access Service Edge – or SASE for short.

99.5% of European IT leaders are planning network and security transformation projects in the next five years

62% have already started these projects, or plan to in the next 12 months

79% see savings potential through the use of cloud-based security

What is SASE?

SASE is a cloud-based security framework that provides all the necessary functionality and security services to protect remote workers and cloud-based technology, as well as on-premise applications and infrastructure. SASE combines network security functions such as SWG, CASB, FWaaS and ZTNA with WAN functions such as SD-WAN to support the dynamic requirements of companies for secure IT access. These capabilities are provided primarily as a service and based on entity identity, real-time context, and security/compliance policies.

Security and networking - the two sides of a SASE architecture

Secure Access Service Edge (SASE) brings together network and security services in a cloud architecture to protect users, applications, and data anywhere. With users and applications no longer residing within a well-defined, traditional corporate network, security measures must also go beyond the traditional hardware appliance at the network edge. Instead, SASE provides the necessary connectivity and security as cloud services. Done right, a SASE model eliminates the need for classic appliances and legacy solutions and uses a smaller overall number of strategic, tightly-integrated technology vendors. Instead of routing traffic to an appliance for security, users connect to the SASE cloud service to securely access applications and data, with security policies rigorously enforced.

> "Many European organizations have intentions to transform their network and security architectures, but they still don't know how best to go about it. SASE is the solution that brings together network and security services in a cloud architecture to enable the protection of data, users, applications and devices, everywhere. It provides a unique framework to help CIOs and CISOs transform their architecture effectively."
>
> **Neil Thacker, CISO EMEA at Netskope**

Critical Use Cases for SASE in hybrid work environments

1. Ensuring robust network performance, user experience, and security
2. Maintaining visibility and control in the cloud
3. Protect against cloud-enabled SaaS and web threats
4. Prevent data exposure, theft, and insider risk
5. Achieving cost savings and operational efficiencies

Sources

Netskope Threat Labs data, manufacturing organisations only, 12 month period 1st July 2021 - 31st June 2022
https://www.hackmageddon.com/
Gartner Report, The Future of Network Security Is in the Cloud https://www.gartner.com/en/documents/3957375
Netskope, Navigating Change, October 2021 https://resources.netskope.com/ebooks/navigating-change-the-operational-impact-of-network-and-security-transformation

The advantages of SASE for automotive

SASE offers the necessary functionality for the implementation of comprehensive security services that are needed in the age of distributed cloud-based IT and mobile use. CIOs, and those responsible for IT and cybersecurity, benefit from the following advantages:

When security is cloud-based and data-centric, user and data location are no longer limiting factors. Users and data can be secure regardless of location or device, allowing automotive companies to take advantage of hybrid work models.

A deep, contextual understanding of data types and usage means policies can be designed at a higher granularity than allow/block. This means security teams can allow more - partnerships, productivity apps and collaborative data sharing - without exposing the organization to undue risk.

Securing the data, not the application, means security visibility doesn't just include managed applications. This allows lines of business to innovate and achieve productivity gains without constantly struggling through time-consuming security approvals that can take months before an application is deemed useful. It also ensures that data is protected wherever it travels in the course of productive business; in the cloud, on the web, and on any device.

Aside from the mitigation of the cost of cyber attacks and ransomware costs, enterprises are reporting millions of dollars in savings from SASE as they see cost benefits through vendor consolidation and technology management integration, as well as a significant reduction in network costs as security is applied inline rather than having to trace everything back to the devices in the data center.

User experience is significantly improved, wherever hybrid work takes employees, with no obtuse networking compromises sending data traffic to and from locations just for security purposes.

Organizations have much greater control over the jurisdictions their data is subject to, and are assured greater control over privacy and data protection compliance.

"The last two decades have seen automotive companies increasingly think and act like agile tech companies–focusing heavily on innovation and new technologies alongside the fundamentals of engineering.

The modern car now contains millions of lines of code and hundreds of sensors, creating numerous data points to better analyze and develop our products throughout their ownership cycle with customers. This allows for continuous development, such as Over-the-Air updates; unheard of in decades past. **With data comes data privacy, and since the beginning we've worked to ensure we are protecting our customers' privacy and have found a successful balance between innovative product development and data protection**."

Julie David, Managing Director,
Peugeot UK

About Netskope

Netskope is a leader in Secure Access Service Edge, redefining cloud, data and network security and helping organizations apply zero trust principles. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use and protects people, devices, and data no matter where they are. Netskope helps organizations reduce risk, increase effectiveness, and gain unparalleled visibility into all cloud, web, and personal application activity.

Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to mitigate threats and address technological, organizational, network, and regulatory changes.

For more information about Netskope and the SASE approach, visit www.netskope.com or email field-sales@netskope.com.


netskope