eBook

Der Schutz des geistigen Eigentums in der Automobilindustrie

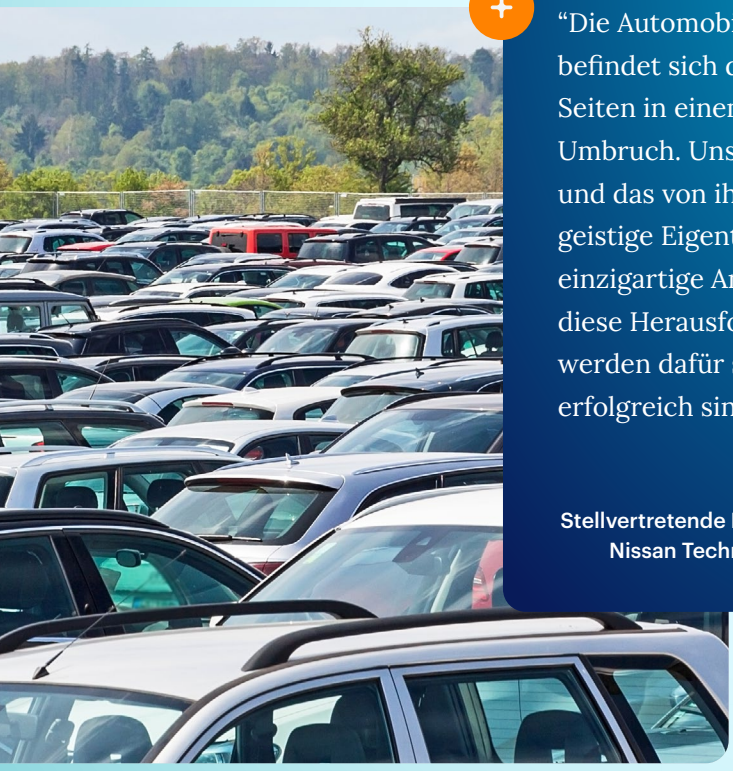
netskope

Was die Automobilindustrie antreibt

Automobilhersteller arbeiten daran, die Art und Weise, mit der ihre Kunden mit ihrer Marke und ihren Produkten interagieren, vollständig zu transformieren. Ihr Ziel ist es, die sich wandelnde Customer Journey in Bezug auf das Produkt besser zu verstehen.

Die Hersteller haben die profitablen Wachstumschancen durch die Integration digitaler Technologien in alle Geschäftsbereiche erkannt, was zu einer digitalen und datengestützten Transformation der Branche, sowie der Einführung agiler Methoden und neuer Technologien wie Blockchain und NFT geführt hat. Die Umsetzung war jedoch eine Herausforderung.

Dieser tiefgreifende Wandel betrifft alle Bereiche der Automobilindustrie und bedeutet eine Neuausrichtung der Forschung und Entwicklung, eine Bereicherung für die Produktinnovation, digitale Erlebnisse und eine Umgestaltung der Partnerschaftsmodelle und des Einzelhandels.



"Die Automobilindustrie befindet sich derzeit von allen Seiten in einem gewaltigen Umbruch. Unsere Mitarbeiter und das von ihnen geschaffene geistige Eigentum liefern einzigartige Antworten auf diese Herausforderungen und werden dafür sorgen, dass wir erfolgreich sind."

Emma Deutsch,
Stellvertretende Direktorin Testbetrieb
Nissan Technology Centre Europe

Dies sind nur einige der Herausforderungen, mit denen führende Automobilhersteller zu kämpfen haben:

1. **Radikale Fortschritte im Autodesign und das Aufkommen neuer Wettbewerber**
   Elektroautos und das Software Defined Vehicle bringen Veränderungen im gesamten automobilen Ökosystem mit sich. Von neuen Partnerschaften und Kooperationen über eine radikale Neuinvestition von F&E-Mitteln bis hin zu einer Umstellung der Fertigung von komponentenorientierten auf funktionale Strukturen und Prozesse – alles muss neu gedacht werden.

2. **Veränderungen der Kundenpräferenzen und der Kundenbindungsmodelle**
   Der Automobilsektor steht vor den gleichen Herausforderungen, die der Einzelhandel erlebte, als das Internet zur bevorzugten Einkaufsmethode wurde. Die Verlagerung der Ladenfront von einem physischen Standort zu einer digitalen Website ist nur der Anfang der Veränderungen, die für Omnichannel- und Direktkundenmodelle erforderlich sind. Abonnements und Mitgliedschaften sind Teil eines seismischen Wandels in der Beziehung zwischen Automobilmarken und Kunden.

3. **Daten als Wertbewerbsvorsprung**
   Software ist im Wesentlichen ein Organisations- und Präsentationssystem für Daten und als solches ist das Software Defined Vehicle ein Fahrzeug, das auf Daten basiert. Egal ob es sich um das Endprodukt oder um industrielle und betriebliche Prozesse handelt, Daten sind die treibende Kraft in der Automobilindustrie. Dies zeigt sich in der Verwendung von NFT und Blockchain (Ablösung von Abo-Modellen und Garantien) sowie in der umfassenden Nutzung von KI zur Weiterentwicklung des autonomen Fahrens. Im operativen Bereich bedeuten “Daten” einen Wettbewerbsvorteil – und ihr Wert nimmt weiter zu.

4. **Veränderungen in der Regulierungslandschaft**, einschließlich der intensiven globalen Konzentration auf Emissionen. Mit der zunehmenden Konzentration auf die globale Klimakrise ist die Automobilindustrie immer wieder Gegenstand neuer gesetzlicher Entscheidungen. Auf der ganzen Welt nennen Regierungen Termine für das Verbot der Zulassung neuer Verbrennungsmotoren, was zu einer intensiven Entwicklung von Batterietechnologien führt. Sogar Super- und Hyperautos werden mit kleineren Motoren entwickelt, um die Nachfrage der Verbraucher nach Geschwindigkeit mit den immer enger werdenden gesetzlichen Vorgaben in Einklang zu bringen.

5. **Globale Makroereignisse und Krisen, die sich auf Betrieb und Lieferketten auswirken**. Sei es die Corona-Pandemie, die weltweiten Unterbrechungen der Lieferketten oder der Krieg zwischen Russland und der Ukraine – all diese Krisen zwingen die Automobilindustrie, sich zu verändern und neue Lösungen für unerwartete Herausforderungen zu finden, zum Beispiel die Ermöglichung eines pandemiebezogenen Homeoffice oder die Sicherung der Lieferketten und der globalen Logistik.

Automobilhersteller bewältigen die Herausforderungen der Branche durch:

- Weiterhin starke Investitionen in Forschung und Entwicklung

  » Der Automobilsektor ist in der EU der größte Investor in F&E und gibt jährlich fast 59 Milliarden Euro aus.

- Ausbau grundlegender Lieferketten zu verbesserten Lieferkettennetzen, die alle Anlagen, Produktionsmittel, Produkte und Transportmittel umfassen, welche zur Unterstützung der Lieferkettenabläufe und des Produktflusses erforderlich sind.
- Umkehrung der globalisierten, gebündelten Produktionsinfrastruktur (die ursprünglich zur Erzielung von Einsparungen und Skaleneffekten konzipiert wurde), um komplexere internationale Grenzen zu überwinden.
- Abkehr von der Abhängigkeit von physischen Händlern und Entwicklung von Omnichannel, datengesteuerten und automatisierten Vermarktungsmodellen.

  » Mehr als 80 Prozent der Fahrzeugkäufer nutzen Online-Quellen während des Kaufentscheidungsfindung.

McKinsey (2021) rät CEOs in fortgeschrittenen Industrien (einschließlich Automobil- und Montageindustrie), strategische Maßnahmen zu ergreifen, die sich in drei Kategorien einteilen lassen:

- Wachstum mit hohem Selbstvertrauen
- Margen- und Produktivitätsverbesserung der nächsten Generation
- Entwicklung von Strategien und Organisationen für das nächste “New Normal”

Quellen

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

netskope

Die Auswirkungen auf den Datenschutz

Cloud und digitale Transformation sind wiederholt Bestandteil der empfohlenen strategischen Maßnahmen, darunter:

1. Digitale Disruption, um Go-to-Market-Ansätze voranzutreiben.
2. Digitale Analytik zur besseren Bewertung der Unternehmensleistung.
3. Einsatz digitaler Tools zur Risikominimierung und Kostensenkung.
4. Cloud-Partnerschaften zur Steigerung der Entwicklungsdynamik (Schaffung einer gezielten Cloud-Strategie).
5. Gestaltung einer Organisation, die auf Geschwindigkeit ausgelegt ist.

McKinsey skizziert auch andere Empfehlungen, die von den IT-Teams ein hohes Maß an Aufmerksamkeit erfordern, darunter Fusionen und Übernahmen sowie die Umgestaltung der globalen Präsenzen und der industriellen Lieferketten.

All diese Empfehlungen sind entweder explizit oder implizit Punkte auf der To-do-Liste des CIO und der Datenschutz ist für alle ein kritischer Erfolgsfaktor.

Sichere Navigation durch Datenbedrohungen

Laut der weltweiten PwC-Umfrage unter CEOs aus dem Jahr 2022 sind 59 Prozent der deutschen Befragten über Cyberrisiken besorgt, wobei die CEOs des produzierenden Gewerbes trotz des hohen Volumens an Cyberangriffen in diesen Sektoren ein geringeres Maß an Besorgnis über Cyberrisiken zeigen als alle anderen Sektoren (40 Prozent).

Am meisten befürchtet wurden Auswirkungen, die Cyberattacken auf die Fähigkeit der Unternehmen haben könnten, Produkte und Services zu verkaufen (62 Prozent), obwohl der Risikofaktor für die Fähigkeit zur Innovation durch Technologie und Prozesse am größten war.

> “Traditionell hat sich die Automobilindustrie immer auf Spionage als die größte Bedrohung für den Datenschutz konzentriert. Die Sicherheit in diesem Bereich musste besonders vor der breiten Einführung der Cloud unter Beweis gestellt werden. Derzeit haben es Cyberkriminelle jedoch regelmäßig mit Ransomware-Angriffen auf Automobilhersteller abgesehen, da ein plötzlicher Produktionsstopp (oder die Drohung, sehr wertvolles geistiges Eigentum zu veröffentlichen) eine unglaublich starke Motivation für die Zahlung von Lösegeld darstellt. In den letzten Monaten gab es eine Reihe hochkarätiger Ziele in der Automobilindustrie.”
>
> **Paolo Passeri,**
> **Leiter Cyber Intelligence, Netskope EMEA**

Die Automobilindustrie im Visier

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat 2021 mit seinem Branchenlagebild Automotive die Cybersicherheit in der Automobilbranche genau untersucht und die spezifischen Angriffsflächen aufgezeigt.

Ransomware-Angriffe sind größte Bedrohung der Cybersicherheit

Cyberkriminelle zielen mit der Verbreitung von Ransomware vor allem auf finanziellen Gewinn ab und nehmen daher besonders häufig Unternehmen ins Visier, die finanziell lohnenswert erscheinen – das so genannte Big Game Hunting. Das betrifft gerade auch viele Automobilhersteller und Zulieferer. Angreifer können durch die Veröffentlichung gestohlener Unternehmensdaten enormen Schaden anrichten und stellen ein hohes Risikopotenzial für die Betroffenen dar. Darüber hinaus gibt es in den Medien immer wieder Schlagzeilen über erfolgreiche Datendiebstähle, Phishing- oder DDOS-Attacken bei Unternehmen der Automobilbranche.

Produktionsanlagen sind auf Angriffe nicht vorbereitet

Dank Digitalisierung und Industrie 4.0 sind moderne Produktionsanlagen vielfach mit Sensoren ausgestattet und untereinander hochgradig vernetzt. Diese Systeme sind meist nicht in die klassischen Unternehmens- oder Zulieferernetze eingebunden und manchmal auch nicht mit dem Internet verbunden. In der Produktion kommen kaum Schutzsysteme zum Einsatz, die Angriffe erkennen. Auch Mitarbeiter sind hier selten in Cybersicherheit geschult und erwarten keine gezielte Anlagenmanipulation.

> “Da die Digitalisierung die Geschäftspraktiken im gesamten Automobil- und Mobilitätssektor weiter verändert und zu immer größeren Datenmengen führt, wird die Cybersicherheit für Händler und Einzelhändler ebenso wichtig wie für Hersteller.”
>
> **Lynda Ennis, Gründerin und Geschäftsführerin des Personalberatungsunternehmens für die Automobilindustrie, Ennis & Co**

Die Lieferketten sind eng verzahnt und verletzlich

Automobilhersteller und ihre Zulieferer sind arbeitsteilig organisiert und haben ihre Arbeits- und Produktionsabläufe sowie ihre logistischen Prozesse und IT-Systeme eng miteinander integriert. Sie teilen dabei auch sensible Informationen wie beispielsweise Konstruktionsdaten. Beeinträchtigungen in der Fertigung bei Zulieferern können sich schnell auf die Automobilhersteller auswirken. Die hohe Vernetzung in der Supply Chain zwischen den Automobilherstellern und ihren Zulieferern erhöht das Risiko für Cyberangriffe und das Schadenspotential.

Homeoffice & mobiles Arbeiten in der Cloud verändern Sicherheitsrisiken

Pandemiebedingt haben in den vergangenen Jahren auch in der Automobilbranche viele Unternehmen weltweit Arbeitsplätze aus geschützten Firmenbüros in Homeoffice Workplaces umgewandelt – eine Veränderung, die die Risiken für Cyberangriffe deutlich erhöht. Der Grund: Hybrides Arbeiten aus dem Homeoffice oder von diversen mobilen Endgeräten mit webbasiertem Zugriff auf Office-Anwendungen aus einer Private oder Public Cloud erfordert andere Sicherungskonzepte als das Arbeiten im klassischen Unternehmensnetzwerk.

Homeoffice-Arbeitsplätze brauchen aber nicht nur in technischer Hinsicht eine neue Security-Ausrichtung sondern auch grundsätzliche Regelungen – beispielsweise über den Umgang mit dienstlichen Unterlagen – und die Sensibilisierung der Mitarbeiter: für mögliche Phishing-Kampagnen, über den Umgang mit Passwörtern oder auch die Nutzung von Videokonferenz-Systemen.

Quellen

Quelle: BSI: Cyber-Sicherheit in der Automobilbranche - Branchenlagebild Automotive
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive.html

Schwachstellen im System

Ein durchschnittliches Fertigungsunternehmen (500-2000 Benutzer) verwendet

1522 Anwendungen,

98%

von denen 98 Prozent nicht von IT-Teams verwaltet werden.

113

dieser Anwendungen werden zum Hochladen, Erstellen, Freigeben oder Speichern von Daten verwendet.

Quelle der Malware-Downloads:

31% Cloud-Anwendungen

69% Internet

netskope

Die fünf wichtigsten Anwendungen für Malware-Downloads in Fertigungsunternehmen

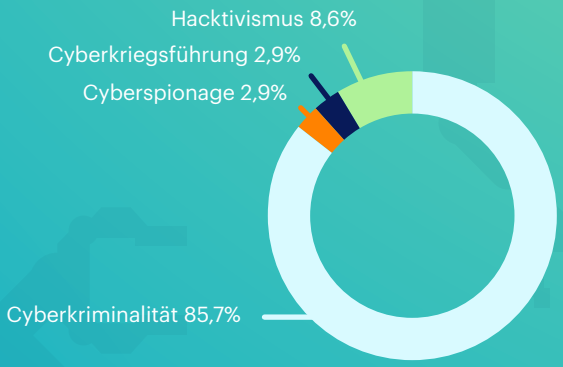
5

- Box
- Weebly
- SourceForge
- OneDrive
- Github

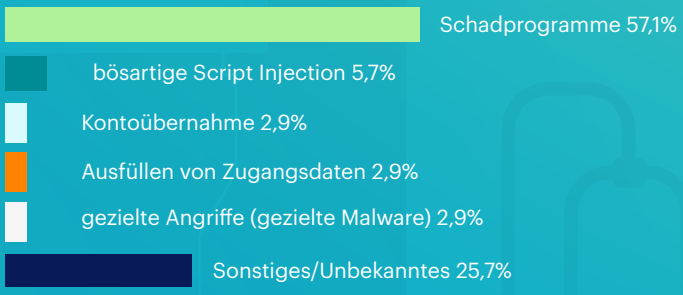
Top-App-Kategorien für Malware-Downloads

» Cloud-Speicher
» Entwicklungstools

Beweggründe für Angriffe auf Fertigungsunternehmen (Jan-Jun 2022)



Techniken, die bei Angriffen auf Fertigungsunternehmen eingesetzt werden (Jan-Jun 2022)



Datenzentrische Sicherheit

Das gute alte Rechenzentrum ist in vielen Unternehmen nicht mehr das Zentrum ihrer IT-Systeme. Immer mehr Unternehmen nutzen zusätzlich die Public-Cloud-Services der großen Hyperscaler wie AWS, Microsoft Azure oder Google Cloud sowie andere IT-Lösungen, die von ihren Anbietern als webbasierte Software-as-a-Service (SaaS) aus der Cloud bereitgestellt werden. Gleichzeitig werden diese Systeme nicht mehr nur von festen Arbeitsplätzen im Unternehmensbüro aus bedient, sondern – besonders verstärkt durch Corona-bedingtes Homeoffice in den letzten Jahren – über verschiedenste mobile Endgeräte von überall her und zu jeder Zeit. Statt aus ihrem lokalen Rechenzentrum beziehen Unternehmen nun gewünschte IT-Anwendungen und IT-Services immer mehr aus heterogenen, weltweit verteilten Cloud-Ökosystemen – mit entsprechenden Folgen für IT-Security und Datenschutz.

Der Marktanalyst Gartner hat diese Entwicklung früh erkannt und 2019 in seinem Report „The Future of Network Security Is in the Cloud" einen neuen Ansatz für Sicherheitsarchitekturen vorgestellt: Secure Access Service Edge – oder kurz: SASE.

99.5% der britischen und deutschen IT-Führungskräfte planen in den nächsten fünf Jahren Projekte zur Umgestaltung von Netzwerken und Sicherheit

62% haben diese Projekte bereits begonnen oder planen dies in den nächsten 12 Monaten

79% sehen Einsparungspotenzial durch den Einsatz von Cloud-basierter Sicherheit

Quellen

Quelle 1: Daten von Netskope Threat Labs, nur produzierende Unternehmen, 12-Monatszeitraum 1. Juli 2021 - 31. Juni 2022
Quelle 2: https://www.hackmageddon.com/
Quelle: Gartner Report, The Future of Network Security Is in the Cloud https://www.gartner.com/en/documents/3957375
Quelle: Netskope, Navigating Change, Oktober 2021
https://resources.netskope.com/ebooks/navigating-change-the-operational-impact-of-network-and-security-transformation

netskope

Was ist SASE?

SASE ist ein Cloud-basiertes Sicherheits-Framework, das notwendige Funktionen für die Implementierung von Sicherheitsdiensten zum Schutz von Remote-Mitarbeitern, Cloud-basierter Technologie, lokalen Anwendungen und Infrastrukturen bietet. SASE kombiniert dabei Netzwerksicherheitsfunktionen wie SWG, CASB, FWaaS und ZTNA mit WAN-Funktionen wie beispielsweise SDWAN, um die dynamischen Anforderungen von Unternehmen an einen sicheren IT-Zugang zu unterstützen. Diese Funktionen werden in erster Linie als Service und auf der Grundlage der Identität der Entität, des Echtzeitkontexts sowie der Sicherheits-/Compliance-Richtlinien bereitgestellt.

Sicherheit und Networking – die beiden Seiten einer SASE-Architektur

Secure Access Service Edge (SASE) vereinigt Netzwerk- und Sicherheitsservices in einer Cloud-Architektur, um Benutzer, Anwendungen und Daten überall zu schützen. Da sich Benutzer und Anwendungen nicht mehr in einem klar begrenzten, klassischem Unternehmensnetzwerk befinden, müssen auch die Sicherheitsmaßnahmen über die herkömmlichen Hardware-Appliances am Netzwerkrand hinausgehen. Stattdessen stellt SASE die notwendige Vernetzung und Sicherheit als Cloud-Dienste bereit. Richtig umgesetzt, macht ein SASE-Modell klassische Appliances und Legacy-Lösungen überflüssig. Statt den Datenverkehr zur Sicherheit an eine Appliance weiterzuleiten, verbinden sich die Benutzer mit dem SASE-Cloud-Service, um Anwendungen und Daten sicher zu nutzen, wobei die Sicherheitsrichtlinien konsequent durchgesetzt werden.

> "Viele europäische Unternehmen haben die Absicht, ihre Netz- und Sicherheitsarchitekturen umzugestalten, wissen aber noch nicht, wie sie dabei am besten vorgehen sollen. SASE ist die Lösung, die Netzwerk- und Sicherheitsdienste in einer Cloud-Architektur zusammenführt, um Benutzer, Anwendungen und Daten überall zu schützen - und bietet CIOs und CISOs eine einmalige Gelegenheit, ihre Architektur zu verändern."
>
> **Neil Thacker, CISO EMEA bei Netskope**

Kritische Anwendungsfälle für SASE in hybriden Arbeitsumgebungen

1. Sicherstellung einer stabilen Netzwerkleistung, Benutzerfreundlichkeit und Sicherheit
2. Aufrechterhaltung von Transparenz und Kontrolle in der Cloud
3. Schutz vor Cloud-fähigen SaaS- und Web-Bedrohungen
4. Verhinderung von Datenexponierung, Diebstahl und Insider-Risiken
5. Erzielung von Kosteneinsparungen und Betriebseffizienz

Die Vorteile von SASE für die Automobilindustrie

SASE bietet die notwendige Funktionalität für die Implementierung von umfassenden Sicherheits-Services, die es im Zeitalter verteilter Cloud-basierter IT und mobiler Nutzung benötigt. CIOs und Verantwortliche für IT- und Cyber-Security profitieren von folgenden Vorteilen:

Wenn die Sicherheit cloudbasiert und datenzentriert ist, sind Benutzer und Datenstandort keine einschränkenden Faktoren mehr. Benutzer und Daten können unabhängig von Standort und Zugangsgerät gesichert werden, so dass Automobilunternehmen die Vorteile der Hybridarbeit nutzen können.

Ein tiefgreifendes, kontextbezogenes Verständnis von Datentypen und -verwendung bedeutet, dass Richtlinien mit einer höheren Granularität als “Zulassen/Sperren” entworfen werden können. Das bedeutet, dass Sicherheitsteams mehr Partnerschaften, Produktivitätsanwendungen und gemeinsamen Datenaustausch zulassen können, ohne sich unangemessenen Risiken auszusetzen.

Die Sicherung der Daten und nicht der Anwendung bedeutet, dass die Sicherheitstransparenz nicht nur sanktionierte Anwendungen umfasst. Dadurch können die Geschäftsbereiche innovativ arbeiten und Produktivitätssteigerungen erzielen, ohne sich ständig durch zeitaufwändige Sicherheitsgenehmigungen kämpfen zu müssen, die Monate dauern können bevor eine Anwendung als hilfreich eingestuft wird. Außerdem wird sichergestellt, dass die Daten überall dort geschützt sind, wo sie im Rahmen des produktiven Geschäftsbetriebs übertragen werden: in der Cloud, im Internet und auf jedem Gerät.

netskope

Neben der Minderung der Kosten für Cyberangriffe und Ransomware-Attacken berichten Unternehmen auch von Einsparungen in Millionenhöhe in anderen Bereichen: SASE ermöglicht Kostenvorteile durch die Konsolidierung von Anbietern und die Integration des Technologiemanagements sowie eine erhebliche Senkung der Netzwerkkosten, da die Sicherheit inline angewendet wird und nicht alles bis zu den Geräten im Rechenzentrum zurückverfolgt werden muss.

Die Benutzererfahrung wird erheblich verbessert, unabhängig davon, wo die Mitarbeiter in einem Hybridsystem arbeiten, ohne dass der Datenverkehr aus Sicherheitsgründen zwischen verschiedenen Standorten hin- und hergeschickt werden muss.

Unternehmen haben eine viel bessere Kontrolle über die Rechtsprechung, der ihre Daten unterliegen und können die Einhaltung von Datenschutzbestimmungen besser kontrollieren.

“In den letzten zwei Jahrzehnten haben die Automobilunternehmen zunehmend wie agile Technologieunternehmen gedacht und gehandelt - mit einem starken Fokus auf Innovation und neue Technologien neben den Grundlagen der Technik.

Ein modernes Auto enthält heute Millionen von Codezeilen und Hunderte von Sensoren, die zahlreiche Daten liefern, um unsere Produkte während ihres gesamten Lebenszyklus besser analysieren und weiterentwickeln zu können. Dies ermöglicht eine kontinuierliche Entwicklung, wie z. B. Over-the-Air-Updates, die es in früheren Jahrzehnten nicht gab. Um die Privatsphäre unserer Kunden zu schützen, hat der Datenschutz für uns einen hohen Stellenwert. **Wir haben von Anfang an darauf geachtet, diesen in unserem Innovationsprozess mitzudenken**.”

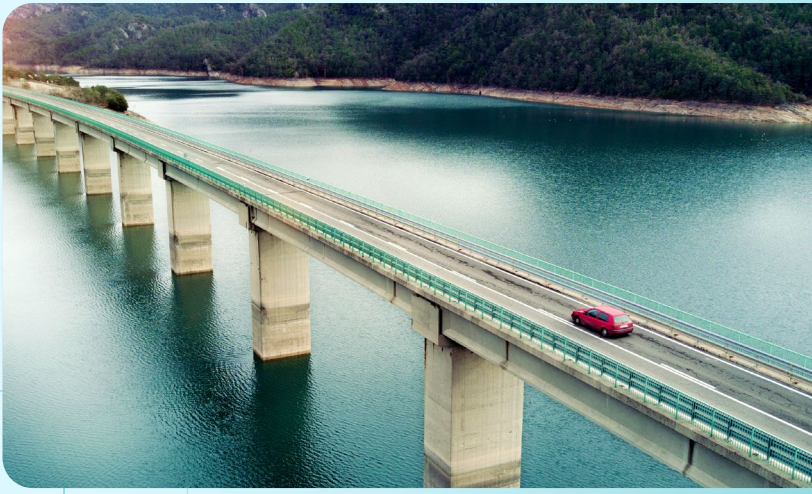
Julie David, Geschäftsführerin
PEUGEOT UK

Über Netskope

Netskope ist ein führendes Unternehmen im Bereich Secure Access Service Edge, das Cloud-, Daten- und Netzwerksicherheit neu definiert und Unternehmen dabei hilft, Zero-Trust-Prinzipien anzuwenden. Die intelligente Security Service Edge (SSE)-Plattform von Netskope ist schnell, einfach zu bedienen und schützt Menschen, Geräte und Daten, egal wo sie sich befinden. Netskope hilft Unternehmen, Risiken zu reduzieren, die Effektivität zu erhöhen und einen beispiellosen Einblick in alle Cloud-, Web- und persönlichen Anwendungsaktivitäten zu erhalten.

Tausende von Kunden, darunter mehr als 25 der Fortune-100-Unternehmen, vertrauen auf Netskope und sein leistungsstarkes NewEdge-Netzwerk, um Bedrohungen abzuschwächen und technologische, organisatorische, netzwerktechnische und regulatorische Veränderungen zu bewältigen.

Weitere Informationen über Netskope und den SASE-Ansatz finden Sie unter www.netskope.com oder per E-Mail an netskope-dach@netskope.com.




netskope