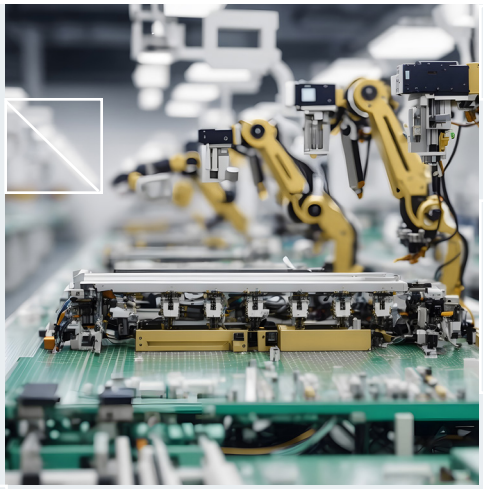


E-BOOK

VERTRAUEN IN GERÄTE: SICHERHEIT FÜR DIE ZUKUNFT VON SMART-TECHNOLOGIE SCHAFFEN

digicert®

INHALT

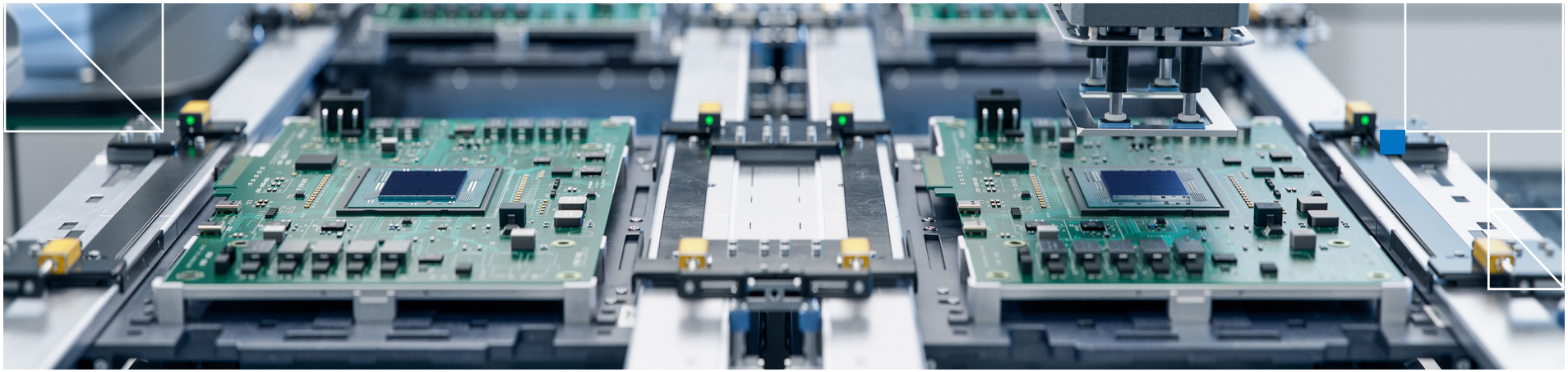
EINE ZUNEHMEND VERNETZTE WELT – CHANCE ODER RISIKO?

Jeden Tag wächst die Welt stärker zusammen. Diese Vernetzung ist reich an Chancen – bringt aber auch neue Angriffsflächen hervor. Die Gefahren, die den Markt vernetzter Geräte bedrohen, entwickeln sich ebenso schnell wie die Technologie selbst und bedrohen damit nicht nur einzelne Nutzer, sondern die Integrität ganzer Netzwerke.

Eine größere Anzahl von Geräten bedeutet auch mehr Angriffspunkte. Schon ein Angriff allein kann zum verheerenden Verlust von Daten führen und hohen finanziellen Schaden anrichten, worunter auch das Kundenvertrauen leidet. Solche Vorfälle erschüttern große wie kleine Unternehmen in ihren Grundfesten.

Hersteller und Entwickler profitieren von diesem Hunger nach vernetzten Geräten, doch jene, die die Gerätesicherheit vernachlässigen, bieten damit auch den Nährboden für Angriffe – ein lohnendes Geschäftsmodell, das bis 2025 schätzungsweise 10 Billionen US-Dollar in die Kassen von Cyberkriminellen spülen dürfte.

Die Frage ist deshalb nicht, ob Sie es sich leisten können, nicht in die Gerätesicherheit zu investieren, sondern wie lange. Vertrauen in Geräte ist eine Notwendigkeit, keine Option. Es gibt vier Wege, wie dieses Vertrauen in Geräte im Kampf gegen Angreifer helfen kann – und wie Sie sich damit von Mitbewerbern abheben können.



KAPITEL 1

SICHERHEITSORIENTIERTES MARKETING

Die Hersteller vernetzter Geräte rücken das Thema Sicherheit zunehmend in den Vordergrund, denn sie haben erkannt, dass ein robuster Schutzwall, unter anderem bestehend aus Identitätsprüfung, Manipulationsschutz und Compliance (Konformität), gegen das wachsende Bedrohungsspektrum nötig ist.

Implementierung einer unveränderlichen digitalen Identität

Das Konzept „Device Trust", also Vertrauen in Geräte, schützt die Identität eines Geräts ab dem Zeitpunkt seiner Herstellung und sorgt so dafür, dass die Geräte-Integrität in jeder Phase des Lebenszyklus gewahrt bleibt. Unveränderliche Identitäten schützen vor einer Reihe von Angriffen und schaffen eine sichere Grundlage für den gesamten Fertigungsprozess.

Integrierter Manipulationsschutz

Welche Bedeutung manipulationssichere Prozesse haben, wird noch deutlicher, bedenkt man das Risiko nicht autorisierter Veränderungen, die nicht nur einzelne Geräte, sondern ganze Netzwerke beeinträchtigen können. Mit Device Trust wird der Manipulationsschutz über mehrere Sicherheitsebenen direkt bei der Entwicklung in die Geräte integriert, darunter Trust Anchors für Hardware und sichere Bootverfahren. Diese Merkmale dienen als Abschreckung für physische Manipulation und schützen die Software-Integrität des Geräts sowie das geistige Eigentum des Herstellers und die Nutzerdaten.

Einhaltung globaler Compliance-Standards

Auch komplexe Compliance-Vorgaben sind mit Device Trust kein Problem, denn durch die integrierten Features hilft es Herstellern, internationale Sicherheitsprotokolle einzuhalten (z. B. mithilfe vordefinierter, regelkonformer Compliance-Vorlagen). So können Hersteller die üblichen Fallstricke umgehen und riskieren keine Compliance-Verstöße.

Sicherheitsorientiertes Marketing in der Praxis

Dass sich diese Sicherheitsmaßnahmen in der Praxis auszahlen, sehen wir bereits an Anwendungen wie diesen:

- Ein Elektronikunternehmen integriert unveränderliche Identitäten in seine Smarthome-Produkte und sorgt so dafür, dass der Ursprung und die Firmware-Updates jedes Geräts authentifiziert und sicher bleiben – von der Fertigung bis zur Nutzung durch Kunden.
- Ein Hersteller industrieller Sensoren nutzt manipulationssichere Features zum Schutz seiner Geräte in kritischen Infrastrukturumgebungen und stärkt so die Resilienz seiner Produkte.
- Dank Device Trust ist ein internationaler Hersteller von Haushaltsgeräten in der Lage, sicher durch die verschlungenen Datenschutzgesetze verschiedener Länder zu navigieren. Durch die Anpassung der Sicherheitsprofile für verschiedene Märkte entspricht jedes Gerät den lokalen Normen, ohne komplett neu entwickelt werden zu müssen. Das spart Zeit und Aufwand.

Device Trust bietet einen umfassenden Sicherheitsrahmen und beginnt bereits in der Entwicklungsphase eines vernetzten Geräts. Durch die Integration unveränderlicher Identitäten, Manipulationsschutz und die globale Unterstützung von Compliance-Vorgaben festigt Device Trust nicht nur den Herstellungsprozess, sondern stärkt auch die Vertrauenswürdigkeit von Geräten bei Anwendern.

KAPITEL 2

AGILE FERTIGUNG

Flexible Bereitstellungsoptionen sind ein wesentlicher Stützpfeiler, denn in der schnelllebigen Welt vernetzter Geräte ist Agilität unverzichtbar. So können sich Hersteller schnell und effektiv an unterschiedliche Umgebungen und Anforderungen anpassen. Durch maßgeschneiderte Sicherheitsmaßnahmen, die nicht in ein „Einheitsgrößen-Korsett“ geschnürt sind, kann das Sicherheitsniveau individuell auf jede Fertigungsumgebung zugeschnitten werden. Dabei geht es nicht nur um die Anpassung an unterschiedliche physische Umgebungen, sondern auch an die vielfältige Technologielandschaft, mit der sich Hersteller konfrontiert sehen.

Einhaltung regional unterschiedlicher Datenschutzgesetze

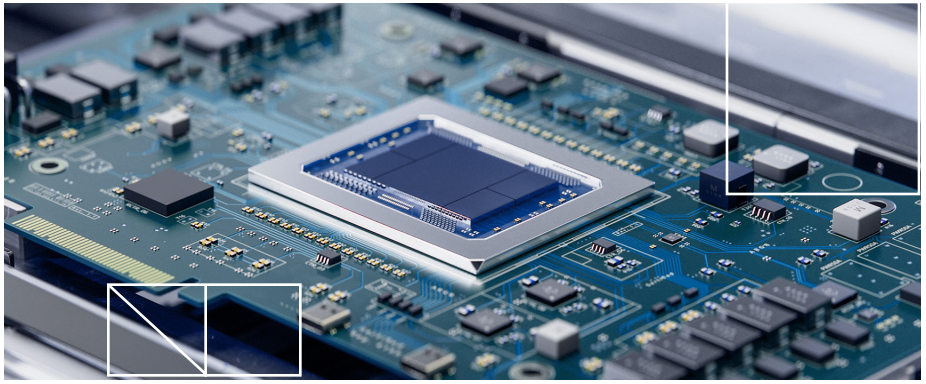
Eine der größten Herausforderungen für Hersteller, die weltweit expandieren möchten, ist es, vor dem Hintergrund vielfältiger, von Region zu Region unterschiedlicher Datenschutzgesetze einen einheitlichen Sicherheitsstandard zu gewährleisten. Die grenzüberschreitende Ausweitung des Geschäftsbetriebs erfordert eine minutiöse Orchestrierung der Sicherheitsmaßnahmen, die den spezifischen Compliance-Vorgaben der Region entsprechen, ohne die Geschwindigkeit oder den Maßstab der Bereitstellung zu beeinträchtigen.

Mit einer Sicherheitslösung, die keinen starren Rahmen vorgibt, sondern Tools zur Skalierung des Betriebs bietet, können Hersteller ihre globale Präsenz ausbauen, ohne die Sicherheit ihrer Geräte zu gefährden.

Die Verfügbarkeit von Geräteressourcen und Arbeitsspeicher im Gleichgewicht

Die schwankende Verfügbarkeit von Geräteressourcen und Arbeitsspeicher im IoT-Bereich erfordert eine Sicherheitslösung, die sich flexibel an die Ressourcen anpasst. Geräte mit begrenzter Verarbeitungsleistung oder knappem Arbeitsspeicher können sich für ressourcenintensive Sicherheitssysteme als echtes Problem erweisen. Ein zu stark abgespecktes Sicherheitssystem hingegen bietet möglicherweise nicht hinreichend Schutz für leistungsstärkere Geräte.

Ein ausgewogener Ansatz, der das Ressourcenprofil jedes Geräts berücksichtigt, gewährleistet ein optimales Sicherheitsniveau ohne unnötigen Ballast. Diese Anpassungsfähigkeit garantiert, dass das Sicherheitssystem robust genug für High-End-Geräte, aber schlank und effizient genug für leistungsschwächere Geräte ist.



Wenn Unternehmen Prinzipien der flexiblen Bereitstellung in ihre Fertigungsprozesse integrieren, können sie auch die komplexesten Vorgaben der modernen IoT-Landschaft zuverlässig bewältigen.

Agile IoT-Fertigung in der Praxis

Anwendungsbeispiele aus der Praxis bestätigen den Erfolg bei Fertigungsprozessen, die diesen Prinzipien folgen:

- Ein Anbieter von Unterhaltungselektronik nutzt flexible und skalierbare Sicherheitslösungen für die Verwaltung seiner breiten Produktpalette, die von High-End-Smart-Fernsehern bis hin zu einfachen IoT-fähigen Haushaltsgeräten reicht. Da sich die Sicherheitsmaßnahmen an das Leistungsspektrum der einzelnen Produkte und an die Marktanforderungen anpassen lassen, kann das Unternehmen seine globale Präsenz erfolgreich ausbauen.
- Ein Hersteller von Sensoren für Smart Farming (Landwirtschaft 4.0) nutzt diese Prinzipien zur Verwaltung von Geräten, die auf verschiedenen Kontinenten unter unterschiedlichen Umweltbedingungen bereitgestellt werden und für die jeweils andere Vorschriften gelten. Die ressourcenorientierte Sicherheitslösung gewährleistet, dass auch Geräte mit minimaler Rechenleistung sicher betrieben werden können, selbst in entlegenen Umgebungen und in Regionen mit begrenzten Ressourcen.

Wenn Unternehmen Prinzipien der flexiblen Bereitstellung in ihre Fertigungsprozesse integrieren, können sie auch die komplexesten Vorgaben der modernen IoT-Landschaft zuverlässig bewältigen. Die dank flexiblen Bereitstellungsoptionen mögliche Agilität, die Gewissheit einer globalen Skalierbarkeit und die Präzision eines ressourcenorientierten Sicherheitsansatzes sorgen für eine resiliente Fertigungsumgebung, die aktuelle wie zukünftige Anforderungen erfüllen kann.

KAPITEL 3

BETRIEBLICHE EXZELLENZ

Bei der IoT-Fertigung hängt die betriebliche Exzellenz stark von einem nahtlosen Zusammenspiel zwischen automatisierten Prozessen und robusten Sicherheitsmechanismen ab. Im Zentrum dieser betrieblichen Strategie steht die automatisierte Verwaltung der Zertifikate, die als Fundament der Geräte-Identität und -sicherheit im IoT-Bereich dienen. Durch die Automatisierung dieses Lebenszyklus – von der Ausstellung und Verlängerung bis hin zum Widerruf der Zertifikate – können Hersteller sicherstellen, dass die Identitäten der von ihnen gefertigten Geräte sorgfältig und ohne das Risiko menschlichen Irrtums verwaltet werden.

Diese automatisierte Zertifikatsverwaltung reicht bis hin zum Betrieb der Geräte in der Praxis. Nach der Bereitstellung werden aus der Ferne Updates und Sicherheitspatches auf die Geräte gespielt, ohne dass manuelle Eingriffe nötig sind. Auch die Ausfallzeiten werden so minimiert. Die Vorteile für die betriebliche Effizienz sind also enorm. Geräte bleiben so länger im Einsatz und es sind weniger Rückrufe oder manuelle Updates nötig. Das spart Zeit und Ressourcen.

Praxisanwendungen einer automatisierten Zertifikatsverwaltung

Angesichts allgegenwärtiger Smart-Technologie kann Device Trust die betriebliche Exzellenz in zahlreichen Anwendungsbereichen fördern:

- Bei einer Smart-City-Initiative erfassen und übermitteln Tausende Sensoren und Geräte Daten, um den Verkehr und den Energieverbrauch zu steuern und die öffentliche Sicherheit zu gewährleisten. Ist die automatisierte Zertifikatsverwaltung in die Geräte integriert, werden die Daten sicher übertragen und die Identität jedes Geräts wird authentifiziert. Damit können sich die Nutzer der Daten sicher sein, dass sie eine präzise, fundierte Entscheidungsgrundlage haben.
- Im Gesundheitswesen reicht das Spektrum an Geräten von stationären Überwachungsgeräten bis hin zu tragbaren Geräten, die die Gesundheitswerte der Nutzer aufzeichnen. Die Automatisierung bei der Zertifikats- und Identitätsverwaltung ermöglicht die rasche Aktualisierung mit den neuesten Zugangsdaten, um Patientendaten zu schützen und dafür zu sorgen, dass Gesundheitsdienstleister auf die Integrität der erhaltenen Daten vertrauen können.
- Bei Fertigungsprozessen sorgt das automatisierte Sicherheitsmanagement für Geräte, die sich an die dynamische Sicherheitslandschaft anpassen können. So kann sich das Sicherheitsniveau von im Einsatz befindlichen Geräten parallel zu neu aufkommenden Bedrohungen weiterentwickeln, ohne den Geschäftsbetrieb merklich zu stören. Diese Anpassungsfähigkeit ist entscheidend, um das Vertrauen der Kunden und den Ruf der Hersteller zu wahren.

Mit der Integration der automatisierten Lebenszyklusverwaltung von Zertifikaten und der Identitätsprüfung in den Betrieb von IoT-Geräten kommt die betriebliche Exzellenz einen deutlichen Schritt voran. Geräte werden sicherer, betriebliche Risiken sinken und die allgemeine Zuverlässigkeit von IoT-Ökosystemen steigt. Damit sind die Geräte für die Anforderungen einer modernen Infrastruktur und Gesellschaft gewappnet.

KAPITEL 4

ZUKUNFTSSICHERE FERTIGUNG

Die IoT-Sicherheitslandschaft verändert sich kontinuierlich. Deshalb genügt es nicht, wenn sich Hersteller nur auf die aktuellen Bedrohungen konzentrieren – sie müssen sich auch auf zukünftige Herausforderungen vorbereiten.

Vorbereitung auf das Quantenzeitalter

Quantencomputer könnten zukünftig zur Bedrohung werden, da die konventionellen Verschlüsselungsmethoden dann wohl nicht mehr genügen. Aktuelle Geräte werden dadurch wieder angreifbar. Die strategische Integration der Post-Quanten-Kryptografie (PQC) bereitet die Geräte auf diese Möglichkeit vor. Sie soll sie vor den Entschlüsselungsfähigkeiten von Quantencomputern schützen und für eine langfristige Geräte-Integrität und den Schutz der Daten sorgen.

Einführung neu entwickelter Technologien

Technologien wie MQTT 5.0 bieten verbesserte Funktionen wie Message Queuing bei der Gerätekommunikation, die ein höheres Maß an Sicherheit, eine verbesserte Datenverarbeitung und eine effizientere Kommunikation zwischen den Geräten ermöglichen. Ähnlich dazu sorgt Kubernetes – das Open-Source-System für die Automatisierung der Bereitstellung, Skalierung und Verwaltung von containerbasierten Anwendungen – für eine agile und skalierbare Geräteverwaltung.

Mit der Integration von MQTT 5.0, Kubernetes und anderen aufstrebenden Technologien können Hersteller ihre IoT-Geräte effektiver verwalten und dafür sorgen, dass die Infrastruktur robust und reaktionsschnell ist und sich an den rasanten Wandel des technischen Fortschritts anpassen kann.

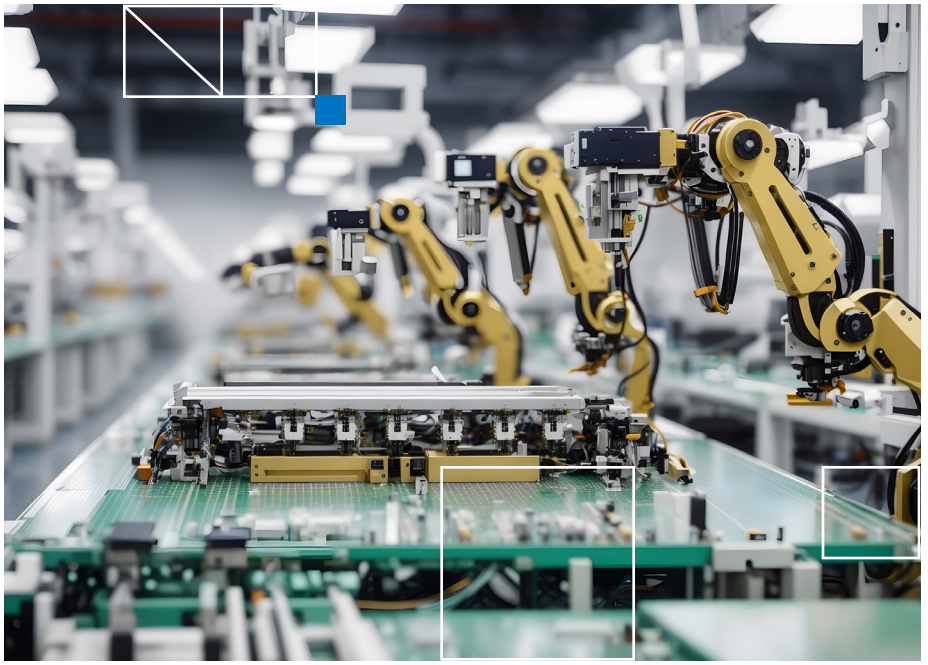
Quantencomputer könnten zukünftig zur Bedrohung werden, da die konventionellen Verschlüsselungsmethoden dann wohl nicht mehr genügen. Aktuelle Geräte werden dadurch wieder angreifbar.

Behördlichen Vorgaben einen Schritt voraus sein

Branchenspezifische Standards unterliegen einem ständigen Wandel, was deren Einhaltung erschwert. Mit neu aufkommenden Sicherheitsbedrohungen verändern sich auch die zugehörigen Sicherheitsvorschriften und Benchmarks. Wer in Compliance-Fragen einen Schritt voraus bleiben möchte, muss also nicht nur die aktuell gültigen Standards einhalten, sondern auch aktiv an deren Gestaltung mitwirken.

Durch die Mitarbeit bei Normungsausschüssen und technischen Arbeitsgruppen erhalten Hersteller Einblicke in zukünftige Änderungen und können ihre Produkte dementsprechend anpassen. Dieser proaktive Compliance-Ansatz ermöglicht einen reibungslosen Übergang, wenn die neuen Standards in Kraft treten. Außerdem lassen sich so kostspielige Überarbeitungen vermeiden. Die Produkte sind damit immer auf dem neuesten Stand der Sicherheit.

Auch strategisch bringt die Anpassung an sich wandelnde Standards Vorteile für Hersteller, die sich damit in diesem Bereich als branchenführend positionieren können. Das signalisiert sicherheitsbewussten Kunden, dass ein Hersteller ihre Anforderungen erfüllen kann und dafür gerüstet ist, die Komplexität globaler Märkte mit unterschiedlichen rechtlichen Anforderungen zu bewältigen. Den Stakeholdern wiederum signalisiert es, dass sich der Hersteller zur Einhaltung höchster Sicherheitsstandards verpflichtet hat, was Vertrauen schafft und das Marken-Image stärkt.



Der Schlüssel zu zukunftsfähiger Fertigung im IoT-Bereich

Die Produkte von Herstellern, die aufkeimende Bedrohungen antizipieren, innovative Technologien einführen und einen proaktiven Compliance-Ansatz verfolgen, sind nicht nur nach heutigem Maßstab sicher, sondern auch für zukünftige Herausforderungen gewappnet. Durch diese strategische Weitsicht heben sich die führenden IoT-Unternehmen vom Rest der Masse ab und können sichere, zuverlässige und modernste Produkte liefern, die die Zeiten – und technologischen Herausforderungen – überdauern werden.

KAPITEL 5

VERTRAUEN IN GERÄTE – DIE SPÜRBAREN AUSWIRKUNGEN

Woran ließen sich die Erfolge eines robusten Sicherheits-Frameworks besser ablesen als an Erfahrungsberichten von Kunden, die selbst Zeuge der transformativen Kraft von Device Trust geworden sind. Die folgenden Fallstudien zeigen nicht nur die praktischen Anwendungsmöglichkeiten eines solchen Frameworks auf, sondern unterstreichen auch die messbaren und strategischen Vorteile für Unternehmen.

Fallstudie 1

Kunde: Ein führender Hersteller von Smarthome-Geräten

Lösung: Implementierung eines Sicherheits-Frameworks für eine komplette Produktreihe

Ergebnis: Der Kunde verzeichnete einen deutlichen Rückgang von Sicherheitsverletzungen und einen gleichzeitigen Anstieg des Kundenvertrauens. Dies zeigte sich durch einen signifikanten Anstieg des Marktanteils und ein stärkeres Marken-Image. Der Hersteller war in der Lage, die Vorteile zu beziffern, und die verzeichnete Kapitalrendite überstieg bei Weitem die ursprünglichen Erwartungen.

Fallstudie 2

Kunde: Ein multinationales Unternehmen, spezialisiert auf industrielle IoT-Geräte

Lösung: Effizientere Compliance-Prozesse

Ergebnis: Durch die Integration einer ausgefeilten Gerätesicherheitslösung konnte das Unternehmen seine Compliance-Prozesse optimieren und damit Kosten senken. Auch die Markteinführungszeit für neue Produkte verkürzte sich. Das Sicherheits-Framework ermöglichte es dem Unternehmen, entscheidende Aspekte des Gerätesicherheitsmanagements zu automatisieren, was die IT-Teams entlastete und das Risiko menschlicher Fehler bei der Zertifikatsverwaltung senkte.

Fallstudie 3

Kunde: Ein großer Automobilhersteller

Lösung: Entwicklung einer kundenspezifischen Sicherheitslösung

Ergebnis: Die Entwicklung einer kundenspezifischen Sicherheitslösung führte zu einer hochsicheren Plattform für vernetzte Fahrzeuge. Der Erfolg dieser Zusammenarbeit zementierte nicht nur die Position des Herstellers als Innovator für Fahrzeugtechnologie, sondern bewies auch das Engagement und Know-how des Anbieters hinsichtlich der besonderen Herausforderungen dieser Branche.

Die Fähigkeit, einen proaktiven und umfassenden Sicherheitsansatz demonstrieren zu können, ist in einer Zeit, in der Datenlecks und Sicherheitslücken schnell zur Schlagzeile werden, von unschätzbarem Wert.

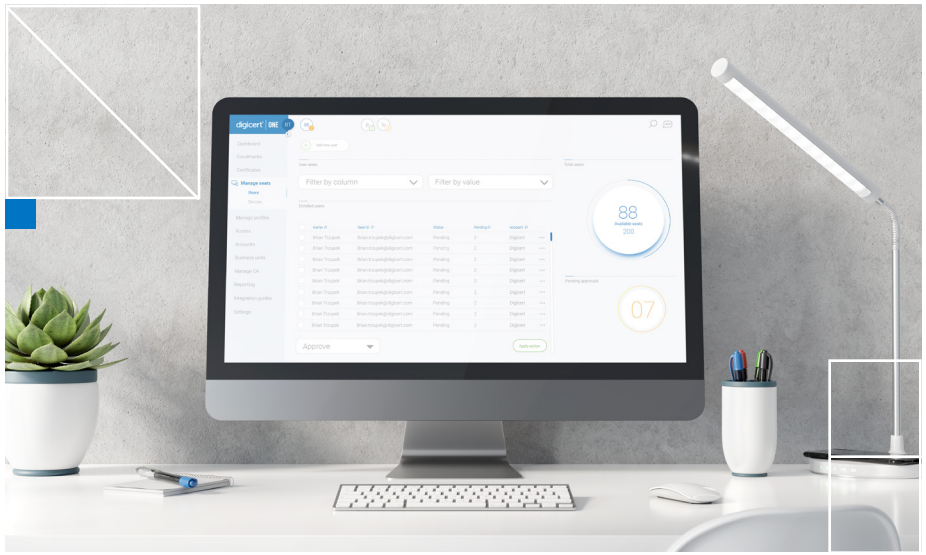
Sicherheitslösungen mit anhaltendem Effekt

Die Vorteile der Lösungen, die in diesen Fallstudien implementiert wurden, beschränken sich nicht nur auf den Geschäftsbetrieb, sondern sind auch strategisch relevant, da sie sich auf die Wahrnehmung dieser Unternehmen in der Branche auswirken. Die Fähigkeit, einen proaktiven und umfassenden Sicherheitsansatz demonstrieren zu können, ist in einer Zeit, in der Datenlecks und Sicherheitslücken schnell zur Schlagzeile werden, von unschätzbarem Wert.

GERÄTESCHUTZ BEDEUTET UNTERNEHMENSSCHUTZ

Geräteschutz bedeutet Unternehmensschutz

Die Anforderungen an die Gerätesicherheit und die betriebliche Exzellenz waren noch nie so hoch wie heute. Wenn Hersteller sich in einer solch komplexen Sicherheitslandschaft zurechtfinden möchten, ist die Wahl klar: Sie müssen das Thema Gerätesicherheit proaktiv angehen, denn sonst verlieren sie den Anschluss.



Mit DigiCert® IoT Trust Manager rückt Device Trust in greifbare Nähe. Unter digicert.com/de/contact-us erfahren Sie mehr darüber, wie Sie Ihre Geräte, Ihre Daten und nicht zuletzt Ihr gesamtes Unternehmen mit Device Trust vor aktuellen und zukünftigen Bedrohungen schützen.

Über DigiCert

Als führender Anbieter digitaler Vertrauenslösungen sorgt DigiCert dafür, dass Einzelpersonen, Unternehmen, Behörden und Gremien digitalen Interaktionen in dem Wissen vertrauen können, dass ihre digitale Infrastruktur und ihre Anbindung an eine Welt voller Online-Transaktionen sicher und geschützt sind.

DigiCert® ONE, das Fundament für digitale Vertrauensdienste, bietet Unternehmen eine zentrale Anlaufstelle für Einblicke und die Kontrolle über eine Vielzahl von digitalen Anwendungsbereichen, in der das Vertrauen eine wichtige Rolle spielt. Dazu gehören der sichere Zugriff auf Unternehmenssysteme, sichere Business-Kommunikation sowie der Schutz von Websites, Software, Identitäten, Inhalten und Geräten. Wir bei DigiCert bieten nicht nur preisgekrönte Softwarelösungen an, sondern haben uns nicht zuletzt auch durch unsere branchenweite Führungsrolle bei Standards, Support und Betrieb als bevorzugter Anbieter bei Unternehmen auf der ganzen Welt einen Namen gemacht, die Vertrauen für sich arbeiten lassen.