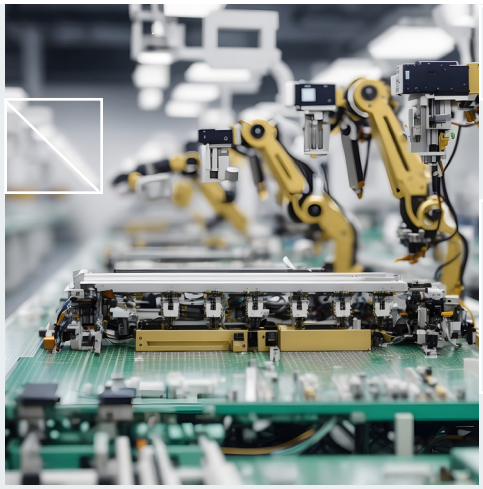


E-BOOK

FIDUCIA DEI DISPOSITIVI: PROTEGGERE IL FUTURO DELLE TECNOLOGIE SMART

digicert®

INDICE

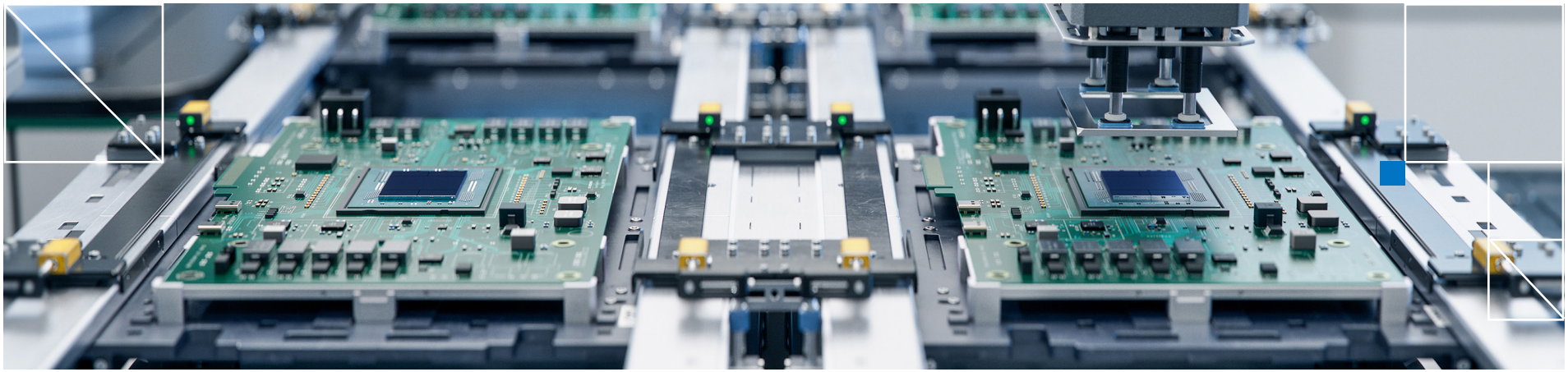
LE PROMESSE E I PERICOLI DI UN MONDO SEMPRE PIÙ CONNESSO

Ogni giorno che passa il mondo è sempre più connesso, questo offre molte opportunità ma anche grandi vulnerabilità. I rischi che incombono sul mercato dei dispositivi connessi evolvono con la stessa rapidità della tecnologia, minacciando non solo i singoli utenti ma anche l'integrità di intere reti.

Più dispositivi significa più vettori di attacco. Una singola violazione può provocare una perdita considerevole in termini di dati ed economici, minando la fiducia dei clienti e compromettendo l'operatività di aziende grandi e piccole.

E se da un lato produttori e sviluppatori sfruttano il bisogno di connettività del pubblico, dall'altro chi non presta attenzione alla sicurezza continua ad alimentare il grande business delle violazioni di dispositivi, un'industria criminale che porterà nelle tasche degli aggressori 10.000 miliardi di dollari entro il 2025.

La questione oggi non è se puoi permetterti di investire nella sicurezza dei dispositivi, ma quanto a lungo potrai permetterti di non farlo. La fiducia dei dispositivi è una necessità, non una funzionalità. Oggi hai a disposizione quattro possibilità per resistere meglio agli attacchi e distinguerti tra tanti competitor.



CAPITOLO 1

MARKETING ORIENTATO ALLA SICUREZZA

La produzione dei dispositivi connessi è sempre più orientata alla sicurezza e alla costruzione di solide difese contro una crescente gamma di minacce, che coinvolgono identità, resistenza alle manomissioni e conformità.

Implementare un'identità digitale immutabile

La fiducia dei dispositivi protegge l'identità di un dispositivo dal momento della sua creazione, assicurandone l'integrità in ogni fase del ciclo di vita. Le identità immutabili a loro volta proteggono da una serie di attacchi, garantendo una base sicura che rafforza l'intero processo di produzione.

Resistenza alla manomissione a livello di engineering

Il rischio di modifiche non autorizzate, che possono compromettere non solo i singoli dispositivi ma anche intere reti, rende essenziale un'operatività resistente alle manomissioni. Un dispositivo ha il giusto grado di fiducia quando la resistenza alle manomissioni è già integrata al suo interno tramite vari livelli di sicurezza, tra cui le ancore di fiducia hardware e i processi di avvio sicuri. Queste caratteristiche sono un deterrente per le manomissioni fisiche e proteggono l'integrità software del dispositivo, preservando la proprietà intellettuale del produttore e i dati dell'utente.

Aderire agli standard di conformità globale

La fiducia dei dispositivi rende più semplice la conformità grazie a funzioni che aiutano i produttori ad allinearsi ai protocolli di sicurezza internazionali. Ad esempio con misure come i template di conformità predefiniti in base alle normative, per evitare i rischi della non conformità.

Il marketing orientato alla sicurezza nel mondo reale

L'efficacia di queste misure di sicurezza è già visibile in contesti reali come negli esempi di seguito:

- Una società di elettronica ha utilizzato la fiducia dei dispositivi per integrare identità inalterabili nei suoi prodotti per la smart home, facendo in modo che l'origine di ogni dispositivo e gli aggiornamenti del firmware restassero autenticati e sicuri dalla produzione all'utilizzo da parte del cliente.
- Un produttore di sensori industriali ha utilizzato funzionalità antimanomissione per proteggere i suoi dispositivi che operano in infrastrutture critiche, rafforzando la resilienza dei suoi prodotti.
- La fiducia dei dispositivi ha permesso a un produttore internazionale di elettrodomestici di orientarsi nell'intricata rete di leggi sulla privacy dei dati di diverse aree geografiche mondiali. Personalizzando i profili di sicurezza per i vari mercati è stato possibile realizzare ogni dispositivo in modo conforme agli standard locali senza doverlo riprogettare, risparmiando tempo e risorse.

La fiducia dei dispositivi fornisce un framework di sicurezza completo che inizia dalla creazione di ogni dispositivo connesso. Integrando identità immutabili, garantendo la resistenza alle manomissioni e facilitando la conformità globale, la fiducia dei dispositivi non solo rafforza il processo di produzione ma migliora anche l'affidabilità dei dispositivi sul campo.

CAPITOLO 2

PRODUZIONE AGILE

L'agilità richiesta nel frenetico mondo dei dispositivi connessi rende essenziali le opzioni di deployment flessibile, che consentono ai produttori di adattarsi ai vari ambienti e requisiti in modo rapido ed efficace. La possibilità di implementare misure di sicurezza non vincolate da un approccio univoco consente di avere una postura di sicurezza su misura per ogni specifica configurazione produttiva. Questa flessibilità non riguarda solo l'adattamento ad ambienti fisici diversi, ma anche ai diversi scenari tecnologici che i produttori devono gestire.

Aderire alle diverse leggi nazionali sulla protezione dei dati

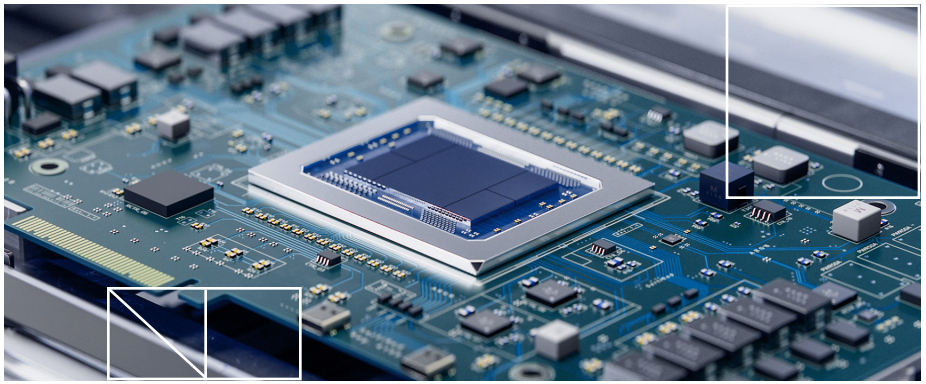
Una delle maggiori sfide per i produttori che puntano alla crescita globale è mantenere uno standard di sicurezza uniforme, rispettando al contempo le leggi nazionali sulla protezione dei dati che conoscono ampie variazioni da un luogo all'altro. Scalare le operazioni a livello transfrontaliero richiede un'attenta orchestrazione delle pratiche di sicurezza, in linea con gli obblighi di conformità di ogni area geografica e senza ostacolare la velocità e la scala dell'implementazione.

L'utilizzo di una soluzione di sicurezza che non impone una struttura rigida, ma fornisce invece gli strumenti per scalare le operazioni, offre ai produttori la possibilità di crescere globalmente senza compromettere la sicurezza dei loro dispositivi.

Adottare un approccio equilibrato per la disponibilità di risorse e memoria del dispositivo

La natura variabile delle risorse e della memoria dei dispositivi nel mondo IoT richiede una soluzione di sicurezza adattiva rispetto alle risorse. I dispositivi con potenza di elaborazione o memoria limitata possono essere un problema per un sistema di sicurezza ad alto uso di risorse, ma un sistema troppo leggero può a sua volta non offrire una protezione adeguata ai dispositivi più performanti.

Un approccio bilanciato che si adatta al profilo delle risorse di ogni dispositivo assicura invece una sicurezza ottimale senza costi superflui. Questa adattabilità è fondamentale per far sì che la sicurezza sia robusta come richiesto dai dispositivi di fascia alta, ma altrettanto semplice ed efficiente sui dispositivi più limitati.



Integrando i principi di deployment flessibile nei processi produttivi, le aziende possono gestire con sicurezza le complessità dell'attuale panorama IoT.

Produzione IoT agile nel mondo reale

I processi produttivi che integrano i principi di agilità sono risultati vincenti nelle applicazioni reali, come in questi casi:

- Un'azienda di elettronica di consumo ha usato soluzioni di sicurezza flessibili e scalabili per gestire una linea di prodotti che spazia dalle smart TV di fascia alta a gadget domestici essenziali abilitati all'IoT. La capacità di adattare le misure di sicurezza alle caratteristiche dei singoli prodotti e ai requisiti del mercato è stata essenziale per un'ottima implementazione globale dell'azienda.
- In ambito industriale, un'azienda che produce sensori per l'agricoltura intelligente ha seguito questi principi per gestire i dispositivi distribuiti in diversi continenti, ognuno con uno specifico set di requisiti relativi a condizioni ambientali e normative. L'adattabilità alle risorse di questa soluzione di sicurezza ha fatto in modo che dispositivi con capacità di elaborazione minime potessero operare in modo sicuro, anche in ambienti remoti e con risorse limitate.

Integrando i principi di deployment flessibile nei processi produttivi, le aziende possono gestire con sicurezza le complessità dell'attuale panorama IoT. L'agilità offerta da un deployment flessibile, la garanzia di una scalabilità globale e la precisione di una sicurezza che si adatta alle risorse creano insieme un ecosistema produttivo resiliente che soddisfa i requisiti attuali e anticipa le esigenze del futuro.

CAPITOLO 3

ECCELLENZA OPERATIVA

Nella produzione IoT, l'eccellenza operativa ruota intorno a un'interazione fluida tra processi automatizzati e solide misure di sicurezza. Il cuore di questa strategia operativa è la gestione automatizzata dei certificati, che sono alla base dell'identità e della sicurezza dei dispositivi IoT. Automatizzando questo ciclo di vita - dall'emissione al rinnovo alla revoca dei certificati - i produttori sono certi che le identità dei dispositivi prodotti saranno gestite con precisione e senza il rischio di errori umani.

La gestione automatizzata dei certificati si estende anche alle operazioni sul campo dei dispositivi. Dopo il deployment, i dispositivi possono ricevere aggiornamenti e patch di sicurezza da remoto, con downtime minimi e senza bisogno di interventi fisici. Le implicazioni per l'efficienza operativa sono notevoli. I dispositivi possono rimanere sul campo più a lungo, con meno necessità di richiami o aggiornamenti manuali, risparmiando così tempo e risorse.

Applicazioni reali della gestione automatizzata dei certificati

L'ubiquità della tecnologia smart fa sì che la fiducia dei dispositivi promuova l'eccellenza operativa in un'ampia gamma di contesti:

- In un progetto di smart city, ad esempio, l'uso di migliaia di sensori e dispositivi permette di raccogliere e trasmettere dati per gestire il traffico, il consumo energetico e la sicurezza pubblica. La gestione automatizzata dei certificati di questi dispositivi assicura infatti un flusso di dati sicuro e l'autenticazione dell'identità di ogni dispositivo, garantendo che le informazioni su cui si basano le decisioni critiche siano accurate e sicure.
- Nel settore sanitario, che spazia dalle apparecchiature di monitoraggio ospedaliero ai tracker sanitari indossabili, è essenziale garantire una sicurezza rigorosa e un funzionamento affidabile dei dispositivi. Automatizzando la gestione dei certificati e delle identità si possono aggiornare rapidamente i dispositivi con le credenziali di sicurezza più recenti, garantendo protezione ai dati dei pazienti e trasmettendo agli operatori sanitari fiducia nell'integrità dei dati ricevuti.
- Nelle attività di produzione, avere una gestione automatizzata della sicurezza significa avere dispositivi capaci di adattarsi ai cambiamenti nello scenario della sicurezza. La postura di sicurezza dei dispositivi sul campo si adatta all'evolvere delle minacce, riducendo al minimo le interruzioni operative. Questa adattabilità risulta essenziale per mantenere alta la fiducia dei consumatori e la reputazione dei produttori.

La gestione automatizzata del ciclo di vita dei certificati e dell'identità, integrata alle operazioni dei dispositivi IoT, rappresenta uno step fondamentale verso l'eccellenza operativa. Infatti offre più sicurezza, riduce i rischi operativi e migliora l'affidabilità complessiva degli ecosistemi IoT, in modo che possano supportare le esigenze delle infrastrutture e della società moderna.

CAPITOLO 4

PRODUZIONE A PROVA DI FUTURO

Con una sicurezza IoT in continua evoluzione, i produttori non possono focalizzarsi solo sulle problematiche attuali ma devono anticipare le sfide future.

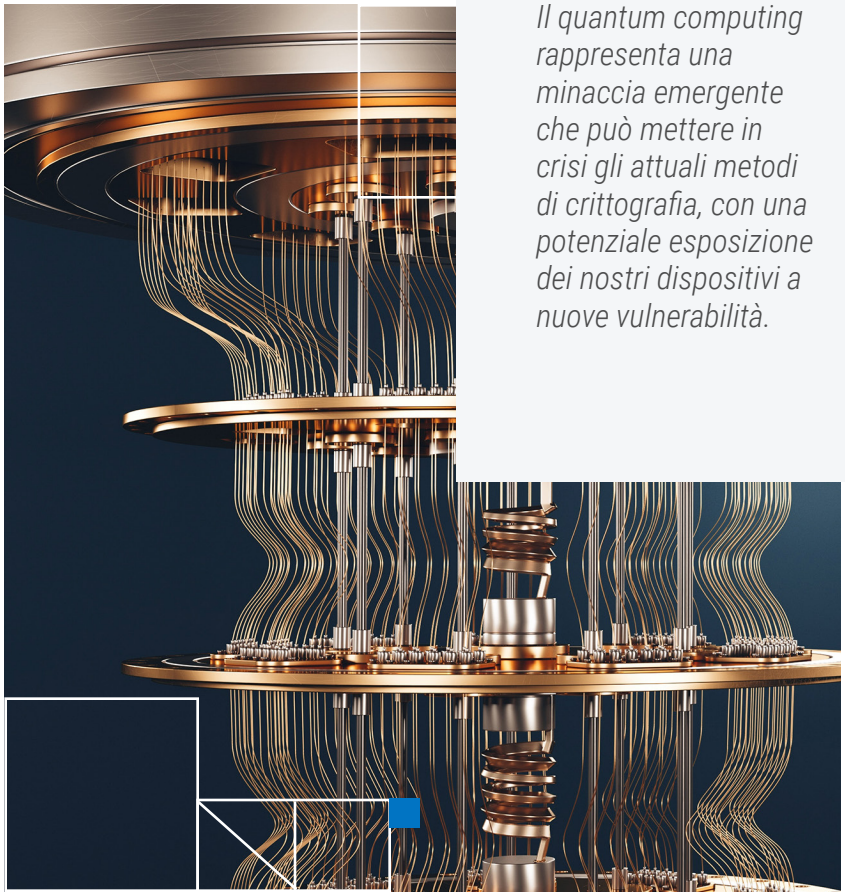
Prepararsi al quantum computing

Il quantum computing rappresenta una minaccia emergente che può mettere in crisi gli attuali metodi di crittografia, con una potenziale esposizione dei nostri dispositivi a nuove vulnerabilità. Integrando subito la crittografia post-quantistica (PQC) possiamo predisporre i dispositivi per questa eventualità, proteggendoli dalle capacità di decrittazione dei computer quantistici e garantendo l'integrità del dispositivo e la privacy dei dati a lungo termine.

Adottare le tecnologie emergenti

Tecnologie come MQTT 5.0 offrono funzioni avanzate per gestire la coda dei messaggi nella comunicazione tra dispositivi, con maggiori livelli di sicurezza, una migliore gestione dei dati e una comunicazione più efficiente tra i dispositivi. Allo stesso modo, Kubernetes, un sistema open-source che automatizza il deployment, la scalabilità e la gestione di applicazioni containerizzate, rende più agile e scalabile la gestione dei dispositivi.

Integrando MQTT 5.0, Kubernetes e altre tecnologie emergenti, i produttori possono gestire i dispositivi IoT con più efficacia, creando un'infrastruttura robusta, reattiva e adattabile al rapido avanzamento tecnologico.



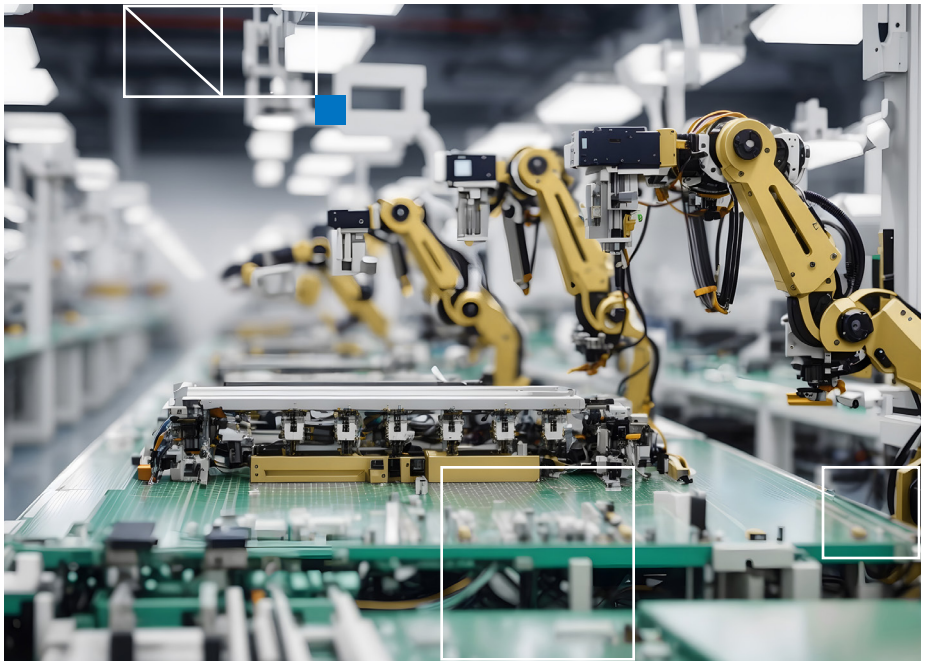
Il quantum computing rappresenta una minaccia emergente che può mettere in crisi gli attuali metodi di crittografia, con una potenziale esposizione dei nostri dispositivi a nuove vulnerabilità.

Restare al passo con le modifiche alle normative

La conformità agli standard di settore richiede un aggiornamento continuo, perché i benchmark cambiano con l'emergere di nuove minacce alla sicurezza e con l'evoluzione delle normative. Mantenersi al passo con la conformità significa non solo aderire agli standard attuali, ma anche partecipare attivamente al dialogo che dà forma alle normative.

Impegnandosi con gli enti di normazione e i gruppi di lavoro tecnici, i produttori possono conoscere prima le nuove modifiche e preparare di conseguenza i loro prodotti. Questo approccio proattivo alla conformità offre una transizione più agevole quando entrano in vigore nuovi standard, evitando costose rielaborazioni e mantenendo i prodotti all'avanguardia nelle pratiche di sicurezza.

Dal punto di vista strategico, un produttore sempre allineato ai nuovi standard si posiziona come leader, capace di soddisfare le richieste dei clienti più attenti alla sicurezza e di affrontare le complessità dei mercati globali con tanti diversi requisiti normativi. Inoltre, questo approccio indica agli stakeholder che il produttore è in grado di mantenere gli standard di sicurezza più elevati, di creare fiducia e di migliorare la reputazione del marchio.



La chiave per rendere la produzione a prova di futuro nel settore IoT

Anticipare le minacce emergenti, adottare tecnologie innovative e mantenere un approccio proattivo verso la conformità aiuta i produttori a garantire prodotti sicuri per l'uso attuale, e resistenti per le sfide di domani. Questa lungimiranza strategica è ciò che differenzia i leader dell'area IoT, e che gli consente di sviluppare prodotti sicuri, affidabili e all'avanguardia capaci di resistere alla prova del tempo e al progresso tecnologico.

CAPITOLO 5

GLI IMPATTI TANGIBILI DELLA FIDUCIA DEI DISPOSITIVI

Se un solido framework di sicurezza dei dispositivi funziona bene, i clienti scoprono dalle applicazioni reali quale sia la capacità trasformativa offerta dalla fiducia dei dispositivi. I casi di studio che seguono non solo illustrano le applicazioni pratiche di questo framework, ma evidenziano anche gli impatti aziendali misurabili, rendendo chiari i vantaggi strategici offerti da queste soluzioni.

Caso di studio n. 1

Cliente: Un produttore leader di dispositivi per la smart home

Soluzione: Implementare un framework di sicurezza su un'intera gamma di prodotti

Risultato: Il cliente ha documentato un forte calo dell'incidenza delle violazioni, con un conseguente aumento della fiducia dei consumatori che ha portato un significativo incremento della quota di mercato e un miglioramento in termini di reputazione del brand. Il produttore è stato in grado di quantificare i benefici, con un ritorno sull'investimento ben superiore alle aspettative.

Caso di studio n. 2

Cliente: Una multinazionale specializzata in dispositivi IoT industriali

Soluzione: Semplificare i processi di conformità

Risultato: Integrando una sofisticata soluzione per la sicurezza dei dispositivi, l'azienda ha semplificato i processi di conformità, ottenendo risparmi sui costi e un time-to-market più rapido per i nuovi prodotti. Il framework di sicurezza ha consentito di automatizzare gli aspetti critici di gestione della sicurezza dei dispositivi, riducendo il carico di lavoro dei team IT e diminuendo il rischio di errori umani nella gestione dei certificati.

Caso di studio n. 3

Cliente: Un grande produttore di automobili

Soluzione: Sviluppo di una soluzione di sicurezza personalizzata

Risultato: Lo sviluppo di una soluzione di sicurezza personalizzata ha consentito di creare una piattaforma per auto connessa ad alta sicurezza. Il successo di questa partnership non solo ha rafforzato l'immagine del produttore come innovatore nelle tecnologie automobilistiche, ma ha anche messo in evidenza l'impegno e l'esperienza del fornitore nell'affrontare le specifiche sfide del settore.

La capacità di dimostrare un approccio proattivo e completo alla sicurezza è importante in un'epoca in cui le violazioni dei dati e le vulnerabilità della sicurezza finiscono sulle prime pagine.

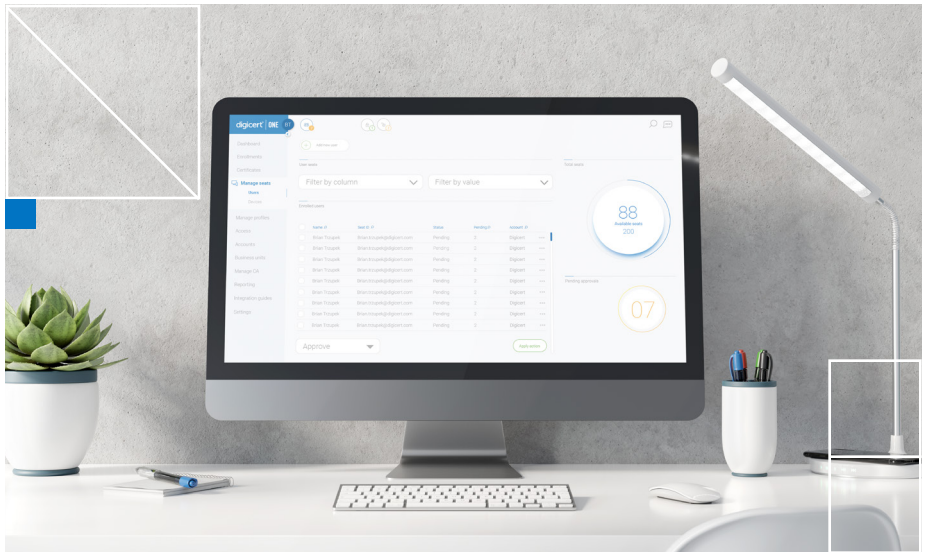
Soluzioni di sicurezza con un impatto duraturo

L'impatto commerciale delle soluzioni implementate in questi casi di studio non è solo di tipo operativo: ci sono implicazioni strategiche che riguardano il modo in cui queste aziende sono percepite nel settore. La capacità di dimostrare un approccio proattivo e completo alla sicurezza è importante in un'epoca in cui le violazioni dei dati e le vulnerabilità della sicurezza finiscono sulle prime pagine.

PROTEGGI I TUOI DISPOSITIVI PER PROTEGGERE LA TUA AZIENDA

Proteggi i tuoi dispositivi per proteggere la tua azienda

La sicurezza dei dispositivi e l'eccellenza operativa oggi muovono interessi enormi. I produttori, navigando in un contesto di sicurezza sempre più complesso, si trovano di fronte a una scelta obbligata: scegliere un atteggiamento proattivo verso la sicurezza dei dispositivi per non restare indietro.



DigiCert® IoT Trust Manager rende la fiducia dei dispositivi una realtà. Visita digicert.com/contact-us per scoprire come questa fiducia può proteggere i tuoi dispositivi, i tuoi dati e la tua azienda dalle minacce attuali e future.

Informazioni su DigiCert

DigiCert è il fornitore leader di "fiducia digitale" e consente a privati, aziende, governi e consorzi di operare online con la certezza che la loro presenza nel mondo digitale sia sicura.

DigiCert® ONE, il cuore della piattaforma di fiducia digitale, fornisce alle aziende visibilità e controllo centralizzati su un'ampia gamma di esigenze di Digital Trust, proteggendo siti web, accessi e comunicazioni aziendali, software, identità, contenuti e dispositivi. DigiCert unisce un software pluripremiato alla leadership del settore in termini di standard, supporto e operazioni, ed è il fornitore preferito delle aziende globali leader che puntano sulla fiducia digitale.