digicert®

Hotel Chain Withstands Cyberattack, Modernizes PKI, Using digicert® ONE

CASE STUDY

Hotel Chain Withstands Cyberattack, Modernizes PKI, Using digicert® ONE

Executive Summary

Industry: Hospitality
Headquarters: North America

Key business requirements:

- Rebuild PKI infrastructure after catastrophic cyberattack
- Restore internal systems within strict recovery time objective
- Automate user and machine certificate issuance and revocation
- Implement zero-trust access controls for secure user and device access

Solution:

- DigiCert Trust Lifecycle Manager
- DigiCert PKI Services

Key outcomes:

- Modernized PKI strengthened resilience post-attack
- Internal and customer-facing systems fully restored within 10 days
- Workforce and 50,000+ devices reconnected securely to sustain global operations
- Granular role-based access controls reduced risk of future breaches

Requirement

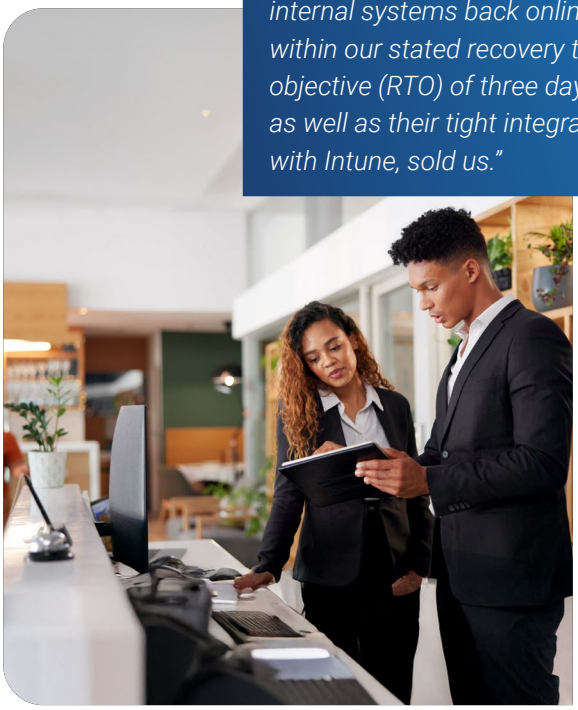
Regain digital trust after catastrophic, identity-driven cyberattack

A global hotel chain suffered a devastating cyberattack that shut down nearly all digital operations across their worldwide network. Using social engineering to bypass the company's multifactor authentication, the attackers gained full administrative access to the company's IT environment. The attackers crippled systems that powered everything from payment processing to mobile apps.

The company performed a quick assessment to determine what sensitive data had been compromised and discovered that anything related to their PKI cryptography was at risk. The security team took all their Microsoft CA (Active Directory Certificate Services) servers offline to prevent any further damage by the attackers.

However, the fallout from the attack paralyzed almost every service that had supported the chain's five-star rating. Digital key cards no longer worked, and all transactions had to be handled manually. The chain waived cancellation fees and bent over backward to aid their current guests, but given this event would cost them millions of dollars, they had to ensure this would never happen again.

"We believed our certificate management platform was sufficient—until this cyberattack exposed its limits," said the company's vice president of infrastructure security. "We needed to take a serious look at other solutions, and DigiCert® ONE offered the sort of enterprise-grade platform that could secure us at a global scale."



"Their promise to get our internal systems back online within our stated recovery time objective (RTO) of three days, as well as their tight integration with Intune, sold us."

Solution

DigiCert® ONE brought company's internal systems back online, modernized their PKI infrastructure

According to the vice president, the situation was so dire that he had to contact DigiCert using his personal email because no one in the company had access to their internal systems. Fortunately, the DigiCert team arrived at the chain's headquarters within hours of being contacted. "They gave us a quick whiteboarding of what they'd described in previous sales interactions, but this time we were listening more intently," the vice president said. "Their promise to get our internal systems back online within our stated recovery time objective (RTO) of three days, as well as their tight integration with Intune, sold us."

In addition, DigiCert promised to stand up a new private Certificate Authority (CA) complete with secure key management and other security controls that greatly improved the company's confidence in their internal PKI. "It's exactly what we needed. And they delivered all of it, fast," added the vice president.

Standing up a new internal CA in less than two days

Because the cyberattack had brought down the hotel chain's entire internal infrastructure, they needed DigiCert to modernize their PKI from the ground up. DigiCert PKI Services got cracking and quickly performed the proper key ceremonies for a root CA that would then stand up the needed Intermediate Certificate Authorities (ICAs) within the DigiCert® ONE platform. Once the new ICAs were deployed, the company could then integrate DigiCert® ONE's secure, internal PKI into their larger environment and enable them to issue new IDs that their apps could then be reconfigured to use. This was the first step in recovering the use of the mission-critical internal applications the company runs on, including email.

DigiCert was able to get this first action completed within two days. "This ability to get our ICAs production-ready with reasonable security controls took a huge burden off my team. It included key generation on an online HSM, so we didn't have to worry about that either," said the vice president.

Bringing employees and devices back online

Once the ICAs were operational, the company leveraged DigiCert Trust Lifecycle Manager to provide their workforce with the proper authentication certificates to access the internal systems. Trust Lifecycle Manager provided them with comprehensive certificate lifecycle management (CLM) tools to automate certificate issuance and revocation that were tied to user identities, ensuring that only verified, current employees could access critical systems.

Moreover, Trust Lifecycle Manager's Microsoft Intune integration got the company's 50,000+ devices back online while supporting secure device management at scale. The company could now track, renew, and automate certificates under this new infrastructure. And Trust Lifecycle Manager's AutoEnrollment CA proxy streamlined certificate issuance to support servers, users, and devices. It also automated the company's external webservers and load balancers.

"All of this leveraged our Active Directory system to ensure that the policies we already had set up for specific groups of users and devices stayed the same at minimum. Even better, Trust Lifecycle Manager, through its proxy, let us customize these parameters more granularly than we were able to do prior to DigiCert's involvement," the vice president said.

Setting up long-term resiliency for the organization

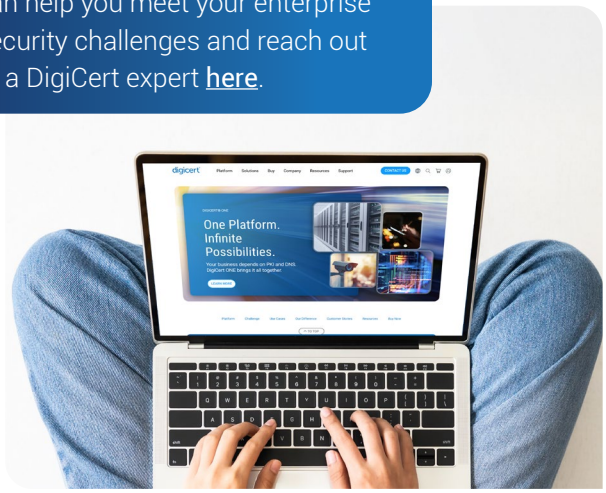
According to the vice president, it took about 10 days to get everything—internal and customer-facing—up and running again. Trust Lifecycle Manager provided transparency into the company's entire certificate population and restored the necessary TLS certificates needed to bring critical systems, including payments and reservations, back online.

DigiCert® ONE also gave the company the ability to create more granular access controls and certificate profiles based on user role, as well as detailed activity logging and audit trails tied to machine and human identities, so suspicious activity could be flagged and investigated quickly.

"In other words, the scenario that led to the attack could no longer happen because we can really fine-tune our role-based access controls and put a halt to most, if not all, of the social engineering attacks that everyone has to contend with."

Although the chain still wishes they could press rewind on the cyberattack, they were pleased that the attack brought about a companywide transformation. By replacing years of outdated systems and modernizing their PKI, the company achieved a dramatic cybersecurity upgrade. Said the vice president: "It felt like we accomplished a decade's worth of modernization in just a few months."

Learn more about how DigiCert® ONE can help you meet your enterprise security challenges and reach out to a DigiCert expert **here**.



About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert® ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at digicert.com.