CASE STUDY

digicert®

Technology company stops outages, consolidates PKI using DigiCert Trust Lifecycle Manager

Executive Summary

Industry: Technology
Headquarters: North America

Key business requirements:

- Stop outages caused by unknown expired digital certificates
- Centralize certificate lifecycle management (CLM) under IT security team
- Automate certificate management and enforcement of security policies at-scale
- Seamlessly migrate PKI from acquired companies into DigiCert CertCentral

Solution:

- DigiCert Trust Lifecycle Manager
- DigiCert CertCentral

Key outcomes:

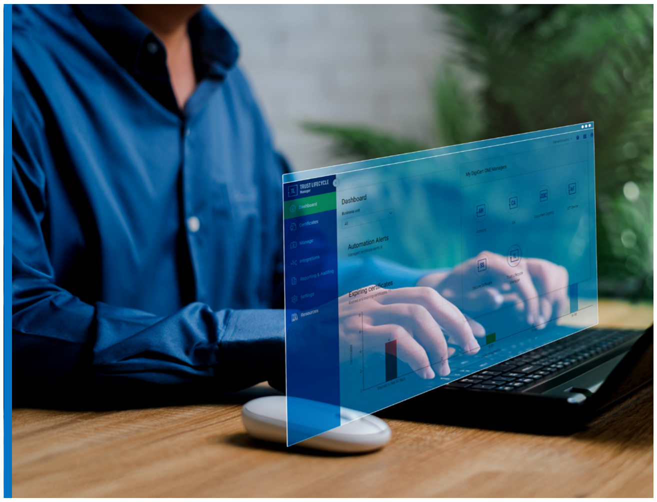
- IT security team can now discover all TLS certificates across entire enterprise, regardless of origin
- Single pane-of-glass dashboard provides unified visibility and intelligence into certificate inventory
- Templates let users easily automate complete certificate lifecycle, from issuance to renewal and revocation
- Automated security policies and parameters limit the possibility of human error, security breaches or business disruptions

Requirement

Centralize certificate management to stop outages and prevent compromise

An up-and-coming technology company was starting to see traction with their innovative platform. Over the last year, however, the company had experienced an increasing number of certificate-related outages. The latest one brought down their developer portal for several hours and led the new director of IT security to perform an internal audit to understand the root cause.

The results of the audit were concerning. While the company had a policy for managing TLS certificates, they had no way of enforcing it. As a result, they had limited visibility over the company's certificate population. The PKI administrators used DigiCert CertCentral for issuing and managing certificates from DigiCert, but other departments within the company were procuring certificates in an ad hoc fashion. The director saw procurement orders for PAYGO certificates from other certificate authorities (CAs), as well as email renewal alerts from Let's Encrypt.



> *“None of the processes were automated, and when you have to rely on people to track certificates, it’s going to lead to outages and worse.”*

“We had to piece it together because we had no way to discover certificates across the organization to figure out what was going on. There were no defined processes, and management was clearly siloed,” said the director. “People were relying on spreadsheets and alerts to manage certificates. None of the processes were automated, and when you have to rely on people to track certificates, it’s going to lead to outages and worse.”

And this situation wasn’t sustainable, particularly as the company continued to grow. In fact, they had recently acquired a smaller company that used a different primary CA from DigiCert, their approved CA, and they needed the ability to incorporate that PKI into their own without disruptions. “We needed to overhaul how we managed certificates—and we needed to find a solution that would help us do so as quickly and safely as possible,” the director said.

Solution

DigiCert Trust Lifecycle Manager provided end-to-end CLM coupled with tight CertCentral integration

There was no shortage of vendors offering certificate lifecycle management (CLM) solutions. But the company was reluctant to choose one that couldn’t promise uninterrupted integration with DigiCert. “I used a solution from another vendor at my previous company, and we had a few instances where the connectors stopped working. It was a huge headache,” the director recalled. “When we learned about Trust Lifecycle Manager, we knew that would be one less worry.”

In addition to working seamlessly with DigiCert CertCentral, Trust Lifecycle Manager was CA-agnostic, which meant it could discover and centrally manage certificates from other CAs. Even better, its automation capabilities could enforce security policies and bulk replace certificates from other CAs with ones from DigiCert. This level of crypto agility was essential both for the company’s plans to scale their business and for the inevitability of post-quantum cryptography.

Finally, the director appreciated the level of support DigiCert provided. “DigiCert’s customer support is just an email or phone call away, and it’s leagues above most everyone,” the director pointed out. “We knew we could trust them, which was critical given the urgency of our situation.”

Enabling discovery of all certificates across the enterprise

The company first used Trust Lifecycle Manager to discover all their TLS certificates. The process unearthed several surprises, including the marketing team’s use of Let’s Encrypt certificates to stand up several landing pages. The team, which wasn’t aware of any enterprise policy for procuring certificates, chose the easiest way to get their work done. “Fortunately, none of these certificates led to outages, but this is not how we want to do this going forward,” the director said with a chuckle.

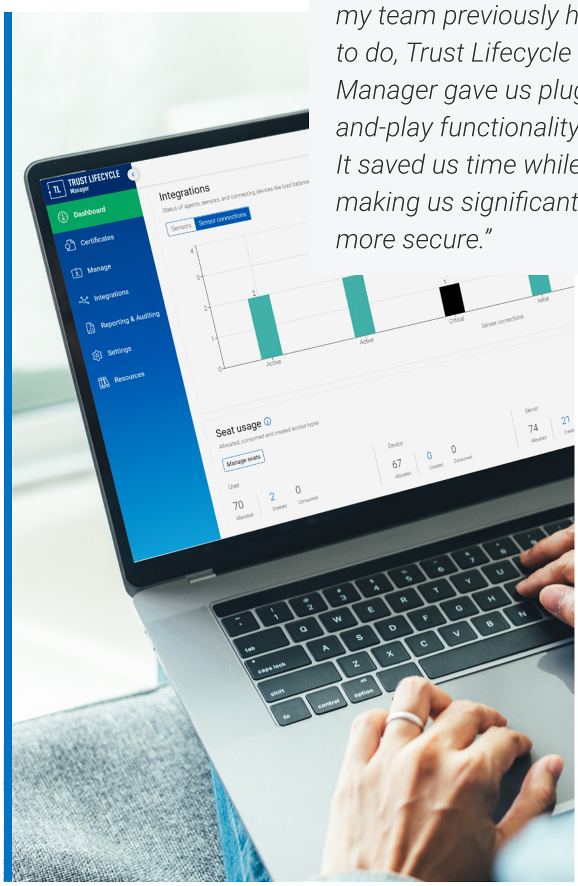
The security team also valued how Trust Lifecycle Manager’s single pane of glass view gave them complete visibility into the company’s enterprisewide certificate population. “After months of not knowing where most of our certificates were located, it was awesome to see them all in one place,” the director said. “Trust Lifecycle Manager let us slice and dice them in all sorts of ways, which meant that we now had the intelligence to prioritize and replace expiring or rogue certificates.”

Consolidating and centralizing certificate management

Once initial discovery was complete, the security team leveraged Trust Lifecycle Manager to start centralizing certificate management. First, they replaced all certificates set to expire within the next 30 days with DigiCert certificates. "Trust Lifecycle Manager and CertCentral work like peanut butter and jelly. No matter where the certificate was originally issued, we could replace it with one from DigiCert—and it took minutes instead of days," the director said.

Next, the security team used Trust Lifecycle Manager to find additional certificates that could lead to problems in the near term. They swapped out a group of wildcard certificates with individual TLS certificates issued through CertCentral and then multiple certificates with outdated encryption algorithms. "Instead of all the steps my team previously had to do, Trust Lifecycle Manager gave us plug-and-play functionality. It saved us time while making us significantly more secure," the director noted.

> *"Instead of all the steps my team previously had to do, Trust Lifecycle Manager gave us plug-and-play functionality. It saved us time while making us significantly more secure."*



Automating company's unique CLM processes

Once the company had taken care of immediate availability and PKI security concerns, they looked to automate the certificate lifecycle, from issuance and procurement to renewal and revocation. Fortunately, Trust Lifecycle Manager made it easy to automate all aspects of the lifecycle based on the company's processes rather than forcing them into using "one-size-fits-all" workflows. Using template-based Trust Lifecycle Manager Profiles, the security team could create templates that let them granularly manage certificates based on such factors as frequency of renewal and whether a certificate could be automatically renewed or required approval beforehand.

Moreover, Trust Lifecycle Manager's automation capabilities meant that the company could enforce corporate security policies. "When Trust Lifecycle Manager 'sees' a certificate that wasn't issued according to our standards, it automatically revokes it and alerts us to the issue," said the director.

As the date for completing their acquisition approached, the director sounded confident that consolidating their PKI infrastructure would be painless. "Trust Lifecycle Manager has done everything we needed and then some," the director said. "The fact that it will continue to support our network no matter which companies we might acquire or how big we grow is a game changer."

[Discover how Trust Lifecycle Manager empowers your PKI modernization journey.]