CASE STUDY

digicert

DIGICERT TRUST LIFECYCLE MANAGER AUTOMATES SECURE CERTIFICATE MANAGEMENT ACROSS DIVERSE WORKLOADS

Executive Summary

Company name: DigiCert
Industry: Technology
Headquarters: Lehi, UT

Key business requirements:

- Effectively manage digital certificates on company's virtual machines (VMs)
- Streamline the many steps needed to provision and install certificates on diverse workloads
- Automate all parts of certificate lifecycle management (CLM)

Solution:

- DigiCert Trust Lifecycle Manager

Key benefits:

- Configuration templates enable SRE team to leverage DigiCert Trust Lifecycle Manager's autoenrollment functionality, shortening certificate provisioning and installation from hours to a few minutes
- Automation streamlines management of certificates, reducing likelihood of certificate-related outages and business disruptions caused by errors or expiration
- Out-of-the-box integrations with third-party platforms, clouds, and devices provide end-to-end certificate lifecycle management that dramatically lowers IT burden as business scales

Requirement

Effectively manage host security and availability across distributed IT environment

DigiCert's SRE (site reliability engineering) team is responsible for ensuring the continuous uptime and performance of DigiCert's global IT infrastructure. To securely maintain this level of availability, the SRE team must manage the digital certificates contained on the thousands of virtual machines (VMs) that support the company's data centers in the U.S., Europe, and Japan.

But managing all these certificates was becoming an increasingly challenging task as more certificates were being used as identities for the workloads on these VMs, said Binh Nguyen, Vice President of Engineering at DigiCert. "Managing certificates has always been challenging, but as we started using more and more certificates, it's almost impossible to maintain awareness of them without help," Nguyen said. "Provisioning and installing a single certificate could take hours because so many steps were involved."

"DigiCert Trust Lifecycle Manager has transformed the way we manage certificates. We've become so much more efficient while at the same time making our infrastructure so much more protected."
—Binh Nguyen, VP of Engineering, DigiCert

In the past, certificate enrollment was an onerous, time-consuming affair. After a certificate signing request (CSR) was approved and a certificate issued, the team would need to manually download the certificate and then install it onto its target host, a multistep process that varied depending on the target. Then they'd have to test the certificate. "You'd have to repeat the steps for every certificate, and the risk of human error got greater with each step," said Nguyen. "We needed ways to automate these processes because we're no more immune to an outage from an expired certificate than any other company using PKI to secure their infrastructure."

Solution

DigiCert Trust Lifecycle Manager transformed certificate lifecycle management (CLM) on VMs

For Nguyen's part, DigiCert Trust Lifecycle Manager couldn't arrive too soon. Trust Lifecycle Manager provided visibility into all the certificates used to secure the thousands of VMs and the workloads they supported. It offered ways to streamline the diverse processes involved in managing certificate lifecycles. In addition, it came with a wealth of automation capabilities tightly coupled within its processes designed to expedite certificate procurement and prevent expiring or misconfigured certificates from triggering an outage.

"DigiCert Trust Lifecycle Manager has transformed the way we manage certificates. We've become so much more efficient while at the same time making our infrastructure so much more protected," Nguyen said.

Simplifying autoenrollment using profiles

The first thing the SRE team needed to do was to streamline autoenrollment of certificates from the initial CSR to installation and testing. DigiCert Trust Lifecycle Manager simplified complex processes by providing configuration templates, known as "profiles," that offered predefined rules for issuing, installing, and managing digital certificates. Because Trust Lifecycle Manager comes with many common profiles, such as those that perform autoenrollment for web servers, Nguyen's team found the process of setting them up especially easy. "We were able to set up a profile for our ACME agent that lets us monitor our target system from a single pane of glass. Now the agent does all the necessary steps to renew expiring certificates without us having to be involved," Nguyen said.

Users could also create profiles using DigiCert Trust Lifecycle Manager's easy-to-follow templates that didn't require specialized PKI knowledge. Trust Lifecycle Manager enabled Nguyen's team to build profiles using templates that supply preset configurations defining certificate properties, including type, validity, and trust hierarchy, to enforce the necessary configurations for the use case.

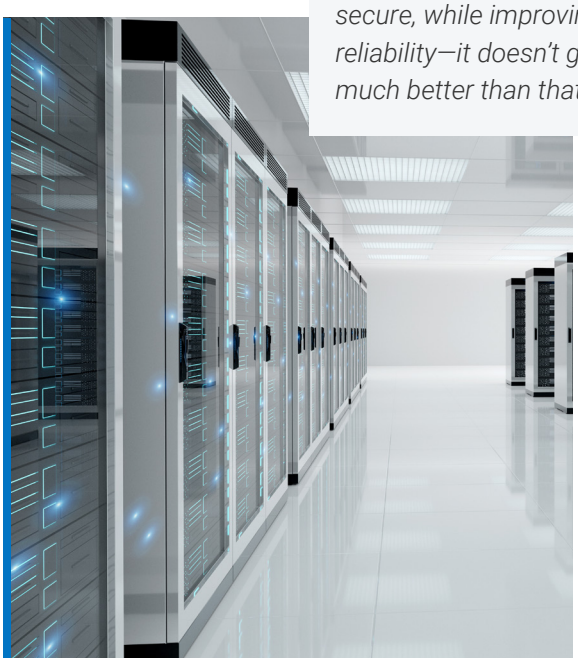
DigiCert Trust Lifecycle Manager could even configure certificate lifespans. Said Nguyen: "You don't need a high level of PKI expertise to configure these actions because Trust Lifecycle Manager handles all of it from CSR to installation and replacement. These processes, which used to take hours for us to complete, now take only a few minutes because Trust Lifecycle Manager automates all of them."

Automating CLM from discovery to renewal

In addition to profiles, DigiCert Trust Lifecycle Manager has a built-in automation architecture that enabled Nguyen's team to automate all aspects of certificate lifecycle management (CLM). Nguyen emphasized how Trust Lifecycle Manager's automated discovery capabilities have transformed the way his team manages certificates. "It's taken a huge burden off my team because they no longer have to worry about tracking all our certificates on the VMs," Nguyen said. "It not only finds and inventories certificates regardless of where they were originally issued, it also tells us who owns them, when they're going to expire, and if they adhere to our security policies."

Even better, DigiCert Trust Lifecycle Manager automation architecture enabled Nguyen's team to build automation workflows that triggered specific actions without requiring human intervention. For example, Nguyen's team built a workflow that automatically revoked any certificate that was misconfigured, contained vulnerabilities, or was issued by an unapproved CA. The workflow then replaced the certificate with an approved one from CertCentral or DigiCert ONE CA Manager, depending on the type of certificate it was replacing.

"To be faster and more secure, while improving reliability—it doesn't get much better than that."



Seamlessly integrating with third-party network devices and workloads

Finally, DigiCert Trust Lifecycle Manager integrated seamlessly with diverse workloads that the company's VMs supported, including load balancers and web servers. Through its sensors and agents, Trust Lifecycle Manager reliably managed the certificates on these network devices without requiring additional scripts or other processes that could increase complexity and problems for the SRE team. "It's great to know that our Apache servers won't accidentally go down because of a certificate we didn't know about," Nguyen said.

Nguyen also appreciated the ease with which DigiCert Trust Lifecycle Manager could manage and automate all the certificates that are used as machine identities on the many applications and microservices the company's web servers and load balancers support. "Every one of these pieces needs a certificate to authenticate themselves in order to work together with the other pieces. The complexity is overwhelming when you consider it—but with Trust Lifecycle Manager, we no longer have to," Nguyen said.

Nguyen's team has already started to roll out DigiCert Trust Lifecycle Manager to manage certificates in their cloud instances. In addition to its robust CLM and managed PKI capabilities, Trust Lifecycle Manager can also dynamically create ICAs (Intermediate Certificate Authorities) that can be spun up as needed. "Trust Lifecycle Manager gives us the agility we need so our infrastructure stays secure as we continue to scale," Nguyen said. "To be faster and more secure, while improving reliability—it doesn't get much better than that."

Get started today with DigiCert® Trust Lifecycle Manager by contacting us here.