Case Study

High-Tech Manufacturer Saves $3.5 Million Annually with Automated Certificate Lifecycle Automation

Case Study Contents

ACCUTIVE SECURITY

1. Background

A leading high-tech manufacturer with $2 Billion in annual revenue faced numerous challenges in managing its complex certificate landscape, which included over 30 000 certificates. The company relied on certificates issued by multiple external CAs. Internal certificates were managed using Microsoft Active Directory Certificate Services (ADCS). The organization had both operational certificates used for its core manufacturing business and enterprise certificates used for other devices and servers.

Due to the nature of the organization's manufacturing business, its operational certificates were critical with outages proving very costly. With frequent enterprise certificate outages, manual processes, and limited internal resources, the company began looking for a robust certificate lifecycle management (CLM) solution with advanced automation capabilities. Additionally, the organization was looking at options for external expert support to supplement its limited internal resources

2. Overview of Challenges

1. **Complex Certificate Management**: With multiple CAs and manual management of 30 000 certificates, the company experienced inefficiencies and high risk of human error.
2. **Outages and Downtime**: Certificate-related outages occurred frequently, disrupting critical operations. The organization was suffering 4 enterprise outages per year, costing an average of $100 000 each in lost productivity. Manufacturing operational outages were more costly, leading to losses estimated at $250 000 per hour. Fortunately, these outages were less common and occurred only 1 to 2 times per year.
3. **Limited Internal Resources**: The company did not have sufficient internal staff to manage such a complex and large-scale certificate environment. Building an in-house team with the required expertise would have been costly and time-consuming.
4. **Code Signing and Encryption Integrity**: As a manufacturer of physical technology devices, ensuring the security and integrity of firmware updates was paramount. From a compliance perspective, functional HSM(s) were also required to securely perform Code Signing. The existing manual code signing process was not scalable and posed security risks.

3. Overview of Solution

To begin addressing these challenges, the client tasked Accutive Security with guiding them through an analysis of the leading certificate lifecycle management platforms. Part of this analysis involved a financial analysis of the expected return on investment of each option compared with the status quo. Accutive Security leveraged its extensive network of CLM partners and industry knowledge to obtain realistic platform pricing quotes, cost estimates for manual vs automated processes, and expected value from process automation.

Step 1: Analysis and Solution Selection

Accutive Security began the solution selection process by arranging proof of concepts of leading platforms for the client using its Accutive Security Innovation Lab. The Innovation Lab has cloud hosted instances of all major CLM platforms that can be used to build out realistic demos and proof of concepts. Once the client narrowed their search to a few potential options, Accutive Security obtained best price quotes for each platform.

To establish the projected return on investment (ROI) associated with implementing a robust CLM with

automation, Accutive Security used data on the number of client certificates as well as the volume of outages currently experienced.

- The organization's certificate infrastructure was first broken down into the operational (manufacturing) and enterprise certificate categories:
    - Operational certificates included: device and endpoint certificates (~10 000), certificates for manufacturing equipment and systems (~1500), and code signing certificates for product development (~200).
    - Enterprise certificates included: application and server certificates (~6000), user certificates (~10 000), and cloud certificates (~3000)
- Assuming that the lifecycle of each certificate takes 2 hours to manage, the annual resource hours spent on certificate management were estimated at 60 000 hours for 30 000 certificates.
- Automation generally reduces the certificate management time by 99%, from 2 to 6 hours to 1 minute or less, including end to end automation and approvals. This reduces the annual time from 60 000 hours to 300-600 hours. At an average resource cost of $80 per hour, the expenditure of manual certificate management for the client was estimated at $4.8 million per year.
- The client experienced 1 to 2 operational outages per year. They were suffering losses of $250 000 per hour of downtime for a critical operational system outage. On average, there were 3 hours of downtime per year, totaling $750 000.
- Additionally, the organization was suffering 4 enterprise outages per year averaging $100 000 each in lost productivity, overtime and other costs, for a total of $400 000 per year. The cost per outage was highly variable depending on the impacted system, application, or server.

The client was estimated to have approximately $6 million in avoidable costs due to its current certificate lifecycle management processes that could be eliminated through automation.

Through the analysis, the client realized that a solution with more limited automation capabilities would result in significantly reduced cost savings. Ultimately, they opted for Venafi, a market leader with advanced automation capabilities, for their CLM and PKI.

Step 2: Implementing CLM and PKI

The next step was implementing the Venafi CLM and PKI platforms to provide visibility and control over the lifecycle of certificates, from issuance to renewal and revocation. The Venafi platforms were implemented according to Accutive Security's Proven Path Foundation implementation.

- **Venafi CLM**: The Venafi CLM provides complete visibility and observability across the certificate landscape, ensuring that all certificates are effectively managed. With visibility and role-based access control (RBAC) in place, teams were able to issue and manage their own certificates, drastically reducing administrative overhead.
- **Venafi PKI**: Replaced the internal ADCS with Venafi PKI to enhance automation and scalability, with the futureproofing for secure management of the organization's growing number of machine identities. Venafi PKI provided a centralized framework for secure communication across the network.
- **Code Signing**: The firmware was code signed and the signature of the code was embedded into the device. Additionally, the firmware debug log was encrypted by the public key and only accessible by the private key stored on the HSM. This python-based tool utilized libraries such as PKCS11 and CBOR2 to successfully store the signature back onto the source file.

Step 3: Continuous Automation

After successfully implementing Venafi CLM and PKI, Accutive Security partnered with the client to implement continuous automation of their entire certificate lifecycle. This process aimed to reduce operational demands,

minimize human intervention, and improve overall efficiency, particularly given the company's limited internal resources. The automation was executed using Venafi Smart Automation with a key focus on outage prevention.

Key Components of Continuous Automation:

1. **Automation with ACME**

Over the first year, Accutive Security's Professional Services team worked closely with the client to fully automate the entire lifecycle of their certificates, from issuance and renewal to monitoring and revocation. A key component of the automation strategy was the use of the Automatic Certificate Management Environment (ACME) protocol. This protocol allowed certificates to be automatically requested, issued, renewed, and revoked without human intervention. ACME enabled the Venafi platform to communicate directly with Mobile Device Management (MDM) tools such as JAMF and Intune, ensuring that certificates were provisioned and renewed automatically for all users and devices. By automating this process, ACME reduced the typical manual tasks involved in certificate management from hours to minutes, ensuring that certificates stayed active.

- Issuance and Renewal: Using the ACME protocol, certificates were automatically requested from approved CAs whenever they were needed. ACME eliminated the manual process of generating Certificate Signing Requests (CSRs) and manually submitting them to a CA. For renewals, the Venafi platform automatically generates a CSR that is submitted for signing. The resulting certificate is marked as the Active version and the certificate is provisioned to an IIS certificate store.
- Continuous Monitoring and Revocation: The ACME protocol also enabled the system to monitor certificates continuously. If any certificate needed to be revoked or replaced due to a change in the environment or a security issue, the process was executed automatically without human intervention.
- Nginx and IIS Automation: Venafi certificate automation for Nginx and IIS streamlines the process of managing SSL/TLS certificates, reducing manual effort, and minimizing the risk of expired or misconfigured certificates. By integrating Venafi's CLM, Accutive Security automated the issuance, renewal, and revocation of certificates for both Nginx and IIS web servers. This ensured continuous, secure communication by automatically updating certificates without human intervention.

2. **Expert Resources**

Accutive Security provided the client with a dedicated team of onshore, Venafi-certified experts. These experts were supplemented by the client's internal resources, conducting day-to-day operations, including automating certificate requests, managing reporting, and ensuring compliance with security standards. The Accutive Security resources also provided proactive monitoring of the certificate environment to prevent errors and disruptions.

These expert resources guided the client through the continuous automation process to ensure that certificates were automatically renewed before expiration, preventing the outages that had previously plagued the company. Once the certificate lifecycle was automated, manual management was no longer required; however, there was still a need to perform maintenance, monitor the certificate lifecycle, and optimize the platforms. Continuous improvements were made to the automation framework, which helped gradually reduce the number of outages. Within a year, the company experienced only one minor outage (compared to the frequent major outages prior to automation). This outage cost the client **$20 000**—a net reduction of about 98% in outage related costs over the course of the year.

3. **Enhanced Self-Service Portal**

To further alleviate the strain on the internal team, Accutive implemented a self-service portal. This portal allowed individual business units within the company to request, renew, and manage their own certificates. By decentralizing some of the more routine certificate management tasks, the client was able to free up internal

resources and significantly reduce the time spent on administrative work. The portal utilized role-based access control (RBAC) to ensure the right level of access while maintaining security.

4. Proactive Management and Continuous Optimization

Accutive Security's services team continuously optimized the Venafi platforms in accordance with best practices for certificate lifecycle management. This included ongoing enhancements to automation processes, ensuring scalability as the client's business needs evolved. Through proactive monitoring and regular health checks, the Accutive Security team ensured that the platform ran smoothly, allowing the client to scale its business without worrying about certificate-related bottlenecks, or an increased risk of outages.

4. Client Outcomes: Operational Efficiencies and Cost Savings

By implementing automated CLM and partnering with Accutive Security for expert management, the company achieved the following:

- Net reduction in 30 000 labor hours for certificate management:
    - Although automation will ultimately produce a 90-95% reduction in certificate management hours, the actual realized reduction was closer to 50%. It is expected that the labor hours dedicated to CLM within the organization will decline substantially in future years now that the automation infrastructure is complete. The total labor savings were approximately $2.4 million in the first year, expected to increase to ~$4 million in the next fiscal year.
    - The overall reduction in labor hours was significantly less than the potential amount for two reasons:
        - Firstly, the organization wanted to maintain close oversight for 12 months to ensure that the automation was functioning properly.
        - Secondly, this calculation includes the hours and costs the client invested in continual automation and platform optimization.
- Avoided $1.1 million in outage costs annually: By achieving a near zero-outage environment through automated certificate renewals and proactive monitoring, the client was able to reduce their outage costs by 98%.

Total ROI: With $2.4 million saved in labor costs and $1.1 million saved in avoided outages, the company realized a total annual ROI of $3.5 million. The annual ROI expected to increase to $5 million for the next fiscal year.

5. Key Takeaways

This case study illustrates the critical impact that automation and expert management can have on large-scale certificate lifecycle management:

1. **Increased Efficiency**: Automating certificate management saved 30 000 staff hours annually (expected to increase to a 50 000 hour reduction within 12 months) allowing the company to focus on strategic initiatives instead of manual maintenance.
2. **Outage Prevention**: Leveraging Accutive Security's expert resources to automate certificate renewals reduced certificate-related outages by 98%, saving $1.1 million annually.
3. **Ongoing Optimization**: Accutive Security's expert resources ensured that the company's Venafi platforms were continuously optimized and managed by onshore certified experts, allowing the business to scale without needing to invest in additional internal resources.

By automating its certificate lifecycle management processes and leveraging managed services, the company was able to reduce operational costs while enhancing the reliability and security of its business-critical systems. The total ROI of the certificate automation program for this high-tech manufacturing organization was $3.5 million.

About Accutive Security

We are the Data Protection, Cryptography and Identity and Access Management (IAM) Center of Excellence.

Cryptography and Data Protection: We are focused on Public Key Infrastructure (PKI), Key Management, Hardware Security Modules (HSM), Certificate Lifecycle Management (CLM), Machine Identity Security, Secrets Management, Code Signing, Data Discovery and Masking, Test Data Management (TDM), and encryption and tokenization across applications, databases, file systems, and storage. Accutive Security is one of Venafi's leading partners and is certified to provide services on all platforms.

Identity and Access Management (IAM): Our specializations include Passwordless authentication, Privileged Access Management (PAM), Identity Governance and Administration (IGA), FIDO2 authentication, Certificate-based authentication, Identity management, Online Fraud detection, Multi-factor Authentication (MFA), Password & Session management, Risk-Based Authentication (RBA), User Behavior Analytics (UBA), Single Sign-On (SSO), Smartcards, and YubiKeys.

CONTACT INFORMATION

27068 La Paz Road, Suite 245 Aliso Viejo, CA 92656

Toll Free 888.666.8315

Contact Us

www.accutivesecurity.com

Accutive Security is a Data Protection, Cryptography and Identity and Access Management (IAM) center of excellence, delivering robust, cutting-edge cybersecurity solutions to our diverse array of clients, which ranges from fast service restaurant conglomerates to top 5 U.S. banks.

Our test data management platform, Accutive Data Discovery + Masking, is a cutting-edge solution for data discovery, masking, subsetting and automation.