Case Study

National Insurer Reduces Outage Costs by 99% Through Automation

Case Study Contents

ACCUTIVE SECURITY

1. Background

A major national property and casualty insurer with $7 Billion in annual revenue was grappling with significant operational inefficiencies due to a lack of internal expertise and dedicated resources for managing its digital certificates. With over 15 000 certificates spread across operational and enterprise systems, the insurer's reliance on non-expert staff and manual processes led to frequent outages, operational disruptions, and increased security risks.

The certificates in question were crucial for ensuring secure communication, protecting sensitive client data, and complying with stringent industry regulations such as PCI-DSS, GLBA, HIPAA and NAIC. Unfortunately, the lack of a streamlined certificate management process led to 3 certificate-related outages per month, including frequent impacts on insured and broker facing systems. These outages were estimated to cost the company between $5 000 and $100 000 each.

In addition to the outages, the company faced rising concerns over compliance, given the potential risk of expired certificates leaving critical systems vulnerable to data breaches or non-compliance, which could significantly impact customer trust and regulatory standing. The insurer urgently needed advanced public key infrastructure (PKI) and certificate lifecycle management (CLM) solutions to automate their certificate management, reduce risks, and free up internal resources.

2. Overview of Challenges

1. **Complex and Fragmented Certificate Management**: Managing 15 000 certificates manually, including certificates from multiple external Certificate Authorities (CAs), was cumbersome. The insurance company's IT team was stretched thin, and without a centralized certificate management solution, they were frequently dealing with missed renewals and expired certificates. Certificates were distributed across various systems such as internal applications, cloud services, employee authentication systems, and client-facing platforms.
2. **Frequent Outages and Downtime**: The insurer experienced an average of 37 outages per year, most of which were caused by missed renewals and delayed issuance. Each outage had a cumulative impact on business operations, delaying critical internal processes and creating bottlenecks in customer-facing services. Over the course of a year, the total outage-related losses amounted to approximately $1.8 million.
3. **Security and Compliance Concerns**: Insurance companies are highly regulated, and certificates play a key role in meeting compliance requirements such as SOX, PCI-DSS, GLBA, and HIPAA. Expired certificates led to outages and also left the client vulnerable to breaches and non-compliance penalties.
4. **Limited Internal Resources and Expertise**: The IT team was not equipped with the specialized knowledge needed to effectively manage certificate lifecycles at this scale. This led to a reactive approach to certificate management, with renewals often handled last-minute or even after expiration, resulting in a high risk of human error. Without internal domain expertise, the organization was unable to optimize their processes and begin automating. With increasing certificate volumes, the insurer quickly found itself in a vicious cycle where higher certificate volumes meant that more and more certificates were being managed by non-experts.

3. Overview of Solution

To tackle these challenges, Accutive Security was engaged to analyze the company's existing certificate infrastructure, recommend a solution to automate and streamline certificate management, and implement the solution. The client needed a comprehensive PKI and CLM solution that prevented or eliminated outages, reduced the burden on its operational teams, and addressed security and compliance concerns.

Step 1: Analysis and Solution Selection

Accutive Security began with a detailed and analysis review of the client's certificate landscape. After a detailed review, the organization's certificates were cataloged and categorized into two distinct groups:

Operational Certificates (~4,000):
- Certificates securing internal devices, endpoints, and insurance infrastructure systems.
- Included certificates used for secure data transfers between internal applications, servers, and security monitoring systems.

- **Enterprise Certificates** (~11,000):
  - Certificates used for securing external-facing services such as client and broker portals, cloud services, and APIs.
  - Certificates for employee authentication, such as VPN access and email encryption (S/MIME), and cloud services supporting hybrid infrastructure.

Assuming the lifecycle of each certificate takes 2 hours to manage, the annual resource hours spent on certificate management were estimated at 30 000 hours for 15 000 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 15 000 hours to 150-300 hours. At an average resource cost of $80 per hour, the expenditure of manual certificate management for the client was estimated at $2.4 million per year.
- In the previous year, the client experienced 25 operational outages and 12 enterprise outages. The cost per outage was highly variable on the impacted system, application, or server, but averaged out to approximately $20 000 per outage. In the previous fiscal year, the total outage related costs were estimated at $740 000.

The client was estimated to have approximately $3.1 million in avoidable costs due to its current certificate lifecycle management processes that could be eliminated through automation.

Next, Accutive Security guided the client through 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. Based on their needs, the client opted for a leading CLM and PKI with a plan for continuous automation.

Step 2: Implementing CLM and PKI

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

- **CLM**: The 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.
- **PKI**: Replaced the internal ADCS with advanced PKI to enhance automation and scalability, with the futureproofing for secure management of the organization's growing number of machine identities. The PKI provided a centralized framework for secure communication across the network.

Step 3: Continuous Automation

After successfully implementing the 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 a proven automation methodology 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 CLM and PKI 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 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: 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 the 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, 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 insurer experienced only 4 minor outages (compared to the frequent major outages prior to automation). These outages cost the client only **$8 000**—a net reduction of about 99% 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 CLM and PKI 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 23 500 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 80%. 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 million in the first year.
  - The overall reduction in labor hours was reduced because the organization wanted to maintain oversight and continue with manual reviews of critical certificates, such as those for broker and customer facing applications. Additionally, this calculation includes the hours and costs the client invested in continual automation and platform optimization.
- Avoided $730 000 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 99%.

Total ROI: With $2 million saved in labor costs and $730 000 saved in avoided outages, the company realized a total annual ROI of $2.7 million.

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 23 500 staff hours allowing the company to focus on strategic initiatives instead of manual maintenance and administration.
2. **Outage Prevention**: Leveraging Accutive Security's expert resources to automate certificate renewals reduced certificate-related outages by 99%, saving $730 000 annually.
3. **Ongoing Optimization**: Accutive Security's expert resources ensured that the insurer's 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 insurer 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 insurer was $2.7 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 a leading delivery partner for Venafi and Keyfactor with certification 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.