CASE STUDY

VENAFI®

// Retail Customer Eliminates Outages and Improves Security

Executive Summary:

- **Industry:** Retail
- **IT Environment:** As a leading global retailer, the company supports online transactions with SSL/TLS encryption and authentication.
- **Business Challenges:**
  - Frequent, expensive outages.
  - Errors due to holes and manual practices in CSR process.
  - Unknown certificate ownership and accountability.
  - Complex certificate management process that is not comprehensive or scalable.
  - Lack of effective policy enforcement and compliance for key and certificate management.
- **Solution's Business Impact:**
  - Eliminated 100 percent of outages in business units using certificate automation, with an organization-wide reduction of 80 percent.
  - Reduced certificate provisioning time from days to less than one minute.
  - Enabled easier, safer certificate provisioning through automation.
  - Reduced staffing costs.
  - Achieved senior-level buy-in.

Business Profile

This company is one of the larger retailers in the U.S., with thousands of stores across the country and a strong online presence. It offers customers a wide range of consumer goods and prides itself on providing fantastic value and convenience for its customers, without sacrificing the superior customer service and support on which it built its reputation.

IT Environment

The company's IT environment supports thousands of employees, as well as its online store and mobile apps. The retailer uses TLS certificates to authenticate its online store, and because its annual revenue runs into the billions of dollars, protecting customer payment data is paramount.

Business Challenge

The retailer had been enduring persistent certificate-related outages for several years. On average, the company suffered at least one certificate-related outage every two weeks, which impacted customers and multiple stores. The company's certificate provisioning and management processes were insufficient to stop these outages from occurring, and senior management was quickly losing their patience with the company's security organization, as it had not been able to quell the problem.

The company's PKI team lacked the capability to effectively manage the hundreds of thousands of certificates in its IT ecosystem. They could track only a few thousand of those certificates, most of which resided on load balancers and were managed

manually using spreadsheets. According to the security architect who led the Venafi implementation, most of the company's outages revolved around issues with these managed certificates—an untenable situation.

IT processed managed certificate requests through a ServiceNow portal without the ability to automate any of the steps. Once a certificate signing request (CSR) was created, it would go through a complex business process. After posting, half of the PKI services team did nothing but copy and paste a CSR into a script, press "Enter," get a result and then email it. This series of steps was 100-percent manual, which meant the process was not only tedious but also prone to human error.

To make matters worse, the retailer lacked any defined service boundaries that could track how other teams across the company were provisioning certificates. As a result, the PKI team knew they needed to set boundaries that differentiated their responsibilities from those of the various application teams.

Over the years, the PKI team built some in-house automation capabilities to help with certificate provisioning and management. However, these capabilities failed to provide the necessary visibility into the company's managed certificate inventory, let alone the hundreds of thousands of other certificates that were left unmanaged.

The retailer's senior management team made it explicitly clear that the company would no longer tolerate certificate-related outages. Moreover, the CIO issued a mandate for "HTTPS Everywhere" in order to better protect the company's assets and customers. In addition to eliminating outages and scaling encryption, the PKI team immediately had to address additional certificate-related initiatives, including:

- An update of all SHA-1 certificates to SHA-2.
- The migration of SSL/TLS certificates from one certificate authority to another.

The team needed automated certificate management to meet the requirements set forth by senior management and to maintain operations and security.

Solution: Venafi

As these problems came to a head, the retailer was in the process of migrating to a new automation framework and had made a decision not to port its limited certificate automation capabilities from the homegrown solution it was using to the new framework. The PKI team quickly realized that building a certificate management solution that would protect the certificates of all their machines would be cost-prohibitive. It was also not part of their core competency.

After evaluating several vendors, including AppViewX and CSS (now Keyfactor), the PKI team chose Venafi. The PKI team felt only the Venafi solution could fully address the retailer's certificate-related challenges.

Solution's Business Impact

Outages Eliminated

Within two months of installing Venafi, the retailer's outages in business units using certificate automation were eliminated; companywide, they dropped by 80 percent. In addition, certificate-related incidents in general went down more than 70 percent because Venafi's certificate management capabilities dramatically improved Mean Time to Recovery (MTTR).

For example, Venafi quickly pinpointed the cause of a major outage affecting the retailer's critical payment infrastructure. The outage prevented the company from processing payments for one hour, costing millions of dollars. With Venafi's help, the PKI team discovered that a team issued a manual CSR with a small typo while not using Venafi's automation solution. This ultimately created the outage. Once the error was discovered and corrected, functionality was restored.

This was the first time that the PKI team did not shoulder the blame for an outage. Instead, senior executives began to focus on teams not using Venafi's certificate automation, pointing out that any team not fully on board with the Venafi solution was putting the retailer at risk.

Over 90 Percent of Operational Workload Now Automated

The retailer saw a dramatic drop in its total number of outages as a result of Venafi's advanced automation capabilities. In fact, the company successfully automated more than 90 percent of its operational certificate-related workload. For example, the provisioning of all of the managed certificates on its load balancers is now 100-percent automated, eliminating the use of spreadsheets once and for all.

By automating steps that had always been done manually, the company has eliminated human error. Venafi's ability to automate certificate requests has also diminished provisioning time from several days to less than one minute, on average.

Additionally, the retailer has had a long-standing goal of removing people from the process of building, managing and running systems. Given that the company's IT organization has placed a strong focus on building DevOps (and DevSecOps) capabilities, the company understood it needed a solution that used an application program interface (API) as a primary mechanism through which consumers of certificates could interact. The consistency brought about by Venafi's automation capabilities has provided the company with consistent actions, eradicating mishaps and risks previously caused by human error.

Automated Policy Management

By providing clear guardrails, engineers have been able to work within clear and reasonable constraints, with fewer security policy exceptions as a result. Fewer exceptions mean the PKI team can spend more time on service improvements than one-off solutions.

Moreover, engineers have been pleased that their applications are no longer being affected by certificate-related outages. They are relieved to have gained stability through the automation of certificate management, as well as the additional functionality Venafi provides.

Certificate Self-Service

This improved consistency in how certificates are managed means teams no longer have to shoehorn a one-size-fits-all security solution into their applications. It has also inspired teams to rethink the possibilities of how they manage their own certificate consumption.

As a result of using the Venafi solution, the retailer has succeeded in leveraging a vendor API framework to create a full lifecycle certificate management service. With an eye toward its internal customers and after reviewing how its engineering teams worked day to day, the company positioned its certificate self-service management as a consumable service—easy to leverage, and in the spirit of full-stack ownership. It has eliminated manual management and enhanced the retailer's service offering without the need for additional members on its team. Engineers are now empowered to solve certificate needs in the most appropriate way for their application.

From Certificate Management to Machine Identity Protection

This retailer turned to Venafi for certificate management, and Venafi delivered an automated solution that quickly showed its value. As a result, the leadership team's opinion of both Venafi and the PKI team went from being skeptical to calling them saviors—and saying as much to the company CIO. The team has made progress because Venafi's solution has helped them eliminate the problem of certificate-related outages.

In addition to certificate management, Venafi understands the need to protect cryptographic keys and digital certificates which serve as machine identities that authenticate machine-to-machine connections and communications. Machines serve all aspects of today's retail business, and machine identity protection is needed to keep critical retail systems and data safe.

Trusted by:

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

About Venafi

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

To learn more, visit venafi.com