Venafi

CASE STUDY

Retail Customer DevOps Push Aided by Automated Machine Identity Management

Executive Summary:

Industry: Retail

IT Environment: As a leading global retailer, the company supports online transactions with SSL/TLS encryption and authentication.

Business Challenges:

- DevOps teams had to rely on the PKI team for certificate issuance, which took longer than the lifespan of some machines.
- Certificate provisioning and management hobbled the speed of DevOps approaches.
- Slow processes increased the risk that security policies would be circumvented.
- The PKI team lacked visibility across machine identities in the DevOps infrastructure.

Solution's Business Impact:

- Automated certificate issuance without disrupting app development.
- Certificate provisioning times dropped from several days to less than one hour.
- Automated policy enforcement of machine identity management included in DevOps workflows.
- Integrated seamlessly with DevOps tools, including Kubernetes, Terraform and Chef.
- Provided visibility to the PKI team across different teams and environments.

Business Profile:

This company is one of the world's largest retailers, with stores across the U.S. and a strong online presence. In addition to over 250,000 employees and 2,000 stores, the retailer also has an online store and mobile apps. It offers customers a wide range of consumer goods at competitive prices and continually strives to provide excellent customer service and support.

IT Environment:

The retailer was adopting more of a DevOps culture in order to benefit from the faster and continuous approach to software development. To enable its DevOps practices, the retailer increased its dependence on cloud computing and microservices architecture.

Its IT organization had already taken steps to facilitate DevOps practices. The organization was migrating to a continuous delivery platform to automate future cloud deployments, including Amazon Web Services (AWS). A range of DevOps tools had also been deployed for its developers:

- Terraform
- NGINX
- Kubernetes
- HashiCorp Vault
- Chef
- Apache Tomcat

To help secure its many cloud instances, containers and APIs, the IT organization was also leveraging ServiceNow to manage its digital certificates.

Business Challenge:

The retailer's InfoSec department, particularly its PKI team, was struggling with certificate issuance and management in the faster DevOps infrastructure. Their manual method of provisioning and managing certificates was in direct conflict with DevOps processes. The developer and engineering teams needed security solutions that would enable—not hinder—the rapid pace of agile development, and the security team needed to ensure high security standards weren't being compromised.

Requesting certificates was a slow, frustrating process that forced DevOps engineers to reach out to the PKI team for support. The turnaround time could take as long as five days, which was longer than the lifespans of many of the retailer's virtual systems and containers.

This friction, combined with the DevOps team's lack of understanding about the importance of certificate provisioning, increased the risk of developers seeking workarounds that could potentially compromise the company's security. Because digital certificates serve as machine identities that enable authentication and encryption for the many virtual systems and containers created by DevOps, they are critical to security. If certificates are improperly issued, configured and managed, they can pose a significant risk to an organization's security.

With ad hoc issuance of certificates, the PKI team did not have visibility across machine identities in the DevOps infrastructure. This meant certificates would expire without prior knowledge, causing applications to stop working—a source of irritation for developers, executives and ultimately customers. Because this problem only promised to metastasize as the number of machines continued to increase, the retailer needed a way to properly secure the identities of all these new apps and services.

In other words, the PKI team needed to provide a solution that would give DevOps engineers a means to incorporate security, as well as easily provision and manage keys and certificates throughout the development process. This solution needed to be automated to eliminate human error and improve the speed of provisioning without hobbling the rate of development. In addition, the retailer wanted something that would integrate seamlessly into the DevOps environment so that it worked with the aforementioned tools and platforms necessary for successful development.

Finally, the solution needed to provide visibility and intelligence into the machine identities used in DevOps practices in order to manage these identities across different teams and heterogeneous environments. This would let the PKI team easily identify any imminent problems.

Solution: Venafi

The PKI team began their search to find a solution that would incorporate machine identity management into their DevOps infrastructure, improving upon their development process.

The solution would need to automate the provisioning of keys and certificates so that DevOps teams could focus on fast development without putting the retailer at risk. It also needed to be one that the PKI team could easily use both to oversee the company portfolio of hundreds of thousands of machine identities and to effectively protect them and manage their ongoing lifecycle. This included issuance, configuration, installation, renewal and revocation, among other processes.

After evaluating several vendors, including AppViewX and CSS (now Keyfactor), the PKI team chose Venafi. With Venafi, the retailer can now ensure machine identity management while providing DevOps teams with an automated solution that doesn't slow down their processes.

Solution's Business Impact:

Automation Dramatically Cuts Certificate Provisioning Time

Venafi automated the retailer's certificate management processes, enabling policy-enforced provisioning and renewal. DevOps teams no longer have to involve the PKI team to obtain or renew their certificates. As a result, the amount of time needed for DevOps teams to provision certificates has dropped from several days to less than one hour.

Venafi also allows the company to automate certificate issuance, installation and configuration of AWS Elastic Load Balancing (ELB). Now the DevOps team can initiate a new virtual system or container and begin receiving encrypted traffic within minutes. Given that AWS ELB automatically allocates incoming application traffic across a range of targets—including containers, IP addresses and Amazon EC2 instances—Venafi automation has transformed and streamlined the workflow of the retailer's DevOps teams.

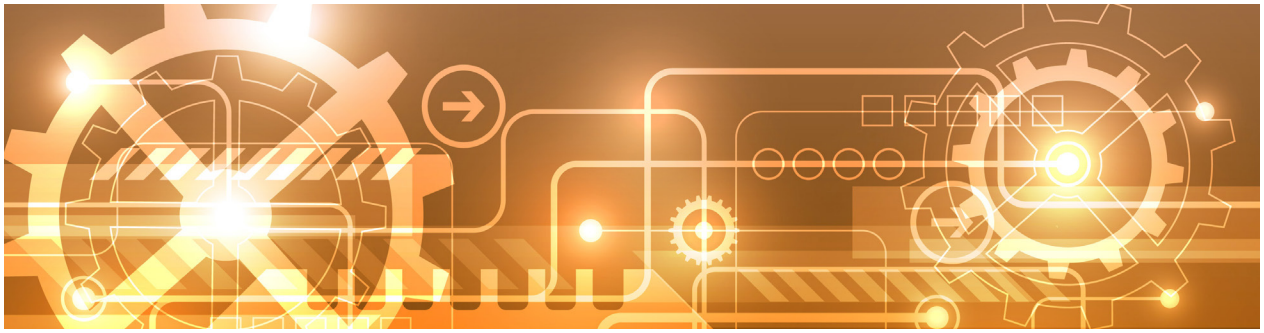
Finally, because this automation works at the speed and scale of cloud computing, DevOps teams can now jettison their reliance on manual provisioning. Additionally, the PKI team no longer has to be concerned about missing, expired or vulnerable certificates that could threaten the availability and security of the retailer's network.

Integration of Certificate Provisioning into DevOps Workflows

Venafi provides comprehensive APIs that integrate with the retailer's DevOps toolsets, ensuring that all key and certificate policy enforcement, access control, workflow processes and audit logging are part of automated build processes.

Venafi also enables the retailer to integrate at two primary points in its workflow. The Venafi Platform works seamlessly with the retailer's continuous integration/continuous delivery (CI/CD) pipeline, which is being used to automate all cloud deployments. Moreover, Venafi integrates successfully with ServiceNow for both certificate requests and to automatically open tickets when certificates are up for renewal.

And this is just the beginning. The retailer is working to further integrate the Venafi Platform into its broader DevOps ecosystem, selecting from native Venafi integrations that have over a thousand applications and common APIs.



Automated within DevOps Workflows

This retailer turned to Venafi's machine identity management solution for its DevOps teams. Venafi in turn delivered an automated solution that quickly showed its value. Now the DevOps team can simply use a credential to automatically consume the Venafi API within their DevOps workflows. The credential triggers a defined policy for the device.

Because Venafi works seamlessly within DevOps workflows, developer teams don't need to have specific knowledge about certificates or how they work. Venafi automates the process of provisioning certificates, so that developers and other teams can perform their tasks without having to consider manual provisioning of certificates. As a result, Venafi's automation has taken a great deal of stress and worry away from the PKI team.

Developers also have seen that certificates are automatically renewed in development environments, which uses certificates with very short lifespans. And these short lifespans have become irrelevant because certificates now are renewed every time an app or other service is run. The retailer's orchestration solution is set to renew certificates every several minutes. And developers can see in real time how the company's orchestration solution works with Venafi to generate a new certificate, put it in the store and then bounce the app to consume it.

Policy-Enforced Automation

With Venafi, InfoSec ensures that DevOps bakes policy enforcement into their automated build processes to achieve certificate compliance with security and audit policies. As virtual systems and containers are commissioned and decommissioned by the DevOps teams, certificates are automatically provisioned, renewed, replaced and revoked—per the firm's security policy.

Now when DevOps teams apply a specific credential, that credential automatically triggers the policy to apply the appropriate management and security actions. After implementing the actions, Venafi sends a success code indicating it has completed the certificate's provisioning and renewal and closes the ticket. If Venafi discovers an error, such as the reuse of a private key, it sends an error code that flags it, so that the PKI team may quickly respond to the situation.

When Venafi is used across a company for machine identity management, DevOps teams can integrate with the same platform that provides machine identity management for the rest of the enterprise. This enables security teams to enforce a shared set of enterprise policies for governance and oversight of machine identities while retaining the flexibility to build policy variations where needed. DevOps gets to leverage the security best practices of the PKI team—but at the speed and scale of DevOps processes.

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
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
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

Venafi is the cybersecurity market leader in machine identity management, 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**