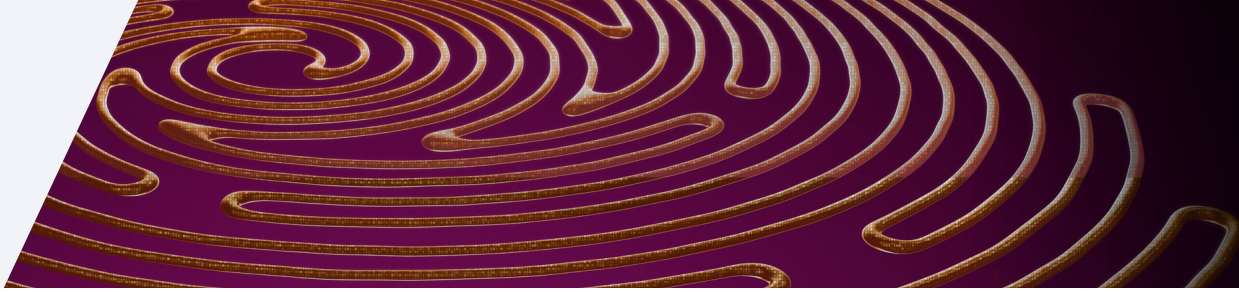
Venafi



CASE STUDY

Global Bank Eliminates Kubernetes Certificate-Based Outages with TLS Protect for Kubernetes

Business Challenge: No visibility into machine identities used across Kubernetes

This multinational bank, a longtime Venafi customer, was in the process of migrating many of their applications originally deployed using on-premise infrastructure to a multicloud infrastructure using Kubernetes. During this process, a customer-facing app suffered a certificate-related outage. This was unusual for them because they had not suffered any certificate outages since they began using Venafi to manage the machine identities of their on-premise apps.

During remediation, the customer discovered that the outage was caused by a certificate misconfiguration from a workload deployed to a Kubernetes cluster. It turned out that the development team responsible for the workload used an older version of cert-manager, the open source tool thousands of companies rely on to automate the issuance and management of TLS certificates in Kubernetes. Interestingly, this customer realized that their security team did not have visibility into any certificate usage or configuration in their Kubernetes clusters, which allowed the misconfiguration to go unnoticed.

This pointed to an organizational challenge: The security and application platform teams were not in close synchronization. The platform team assumed that the tools used by the security team were not appropriate for their usage, given that certificates are handled differently in cloud native environments. For instance, the high volume of Kubernetes workloads being deployed on faster release cycles consumed significantly greater numbers of TLS certificates than were used in traditional data centers, requiring a different machine identity management approach.

After the outage and remediation occurred, the security team met with Venafi and asked for guidance on how they could help their platform teams manage machine identities in cloud native environments to prevent future outages.

"We needed complete visibility and control of every cloud native certificate configuration in our new multicloud environment because all applications are moving to this new platform," said the vice president of security. "And if we could get the same results we saw with Venafi on premises in the cloud, it would be a huge win."

Just a year earlier, Venafi had acquired the company Jetstack. Jetstack created cert-manager, the world's leading open source certificate management solution. Previously unknown to the security team, cert-manager, with over half a billion downloads in 2021, was very well known to the platform team—offering instant credibility that a workable solution was to be had.

Solution: TLS Protect for Kubernetes

Venafi's cloud native experts met with both customer teams to demonstrate how the customer's current investment in Venafi's machine identity management solution could easily be extended to include cloud infrastructure as well. Originally called Venafi Jetstack Secure, TLS Protect for Kubernetes would provide the security team with observability, consistency and control of machine identities across the entire enterprise, whether infrastructure was on premises or in modern Kubernetes environments.

Built on top of cert-manager, TLS Protect for Kubernetes is designed specifically for enterprise usage. In addition to providing commercial support complete with SLAs, TLS Protect for Kubernetes also includes such

enterprise-ready capabilities, such as FIPS-compliant signed builds of cert-manager across the entire organization on any number of Kubernetes clusters, configuration consistency of cert-manager usage and certificate issuance, and a single dashboard for monitoring the health of all Kubernetes clusters.

In other words, TLS Protect for Kubernetes would connect platform teams that rely on cert-manager with security teams that rely on Venafi solutions to bring about reliable and secure Kubernetes environments.

"TLS Protect for Kubernetes would have been a bargain just for the on-call expertise and enterprise-level support that we could access from the team that created cert-manager," said the vice president of platform.

Added the vice president of InfoSec: "Venafi and the TLS Protect for Kubernetes team also provide best practice blueprints to maintain cloud security and compliance as we scale, as well as the ability to seamlessly extend our visibility across both classic on-premise and modern cloud infrastructure. That's the closest thing to a silver bullet I've seen in my 25 years as a security professional."

Ending certificate-related outages within Kubernetes clusters

The first task for TLS Protect for Kubernetes was to help the bank identify in-cluster certificates that could potentially trigger an outage—and the bank was surprised to find several hundred of them. With Jetstack Secure, the platform team easily revoked the offending certificates and replaced them with ones that complied with corporate security policies defined within the Venafi platform. Jetstack Secure enforced this automatically.

In addition, TLS Protect for Kubernetes automated discovery of all machine identities used within every Kubernetes cluster—including those that were previously invisible to either the security or platform teams—and immediately reported them to the security team. This gave the company a continuously updated inventory of all their certificates across their cloud native infrastructure. And to further reduce the risk of outages and other security vulnerabilities, it also helped the platform team automate cert-manager configuration across all clusters. This improved the experience for developer teams, allowing them to go even faster.

Orchestrating machine identity management within Kubernetes

The security team was pleased that TLS Protect for Kubernetes automates tasks such as centralized logging and monitoring because it gave them confidence that their cloud environments were managed at the same level as their on-premises ones. Moreover, TLS Protect for Kubernetes uses consistent, well-documented and proven processes to control the usage of keys and certificates in Kubernetes environments.

Said the vice president of security: "I love how TLS Protect for Kubernetes automates the configuration and management processes, eliminating human error. And it includes a first-class support package, which helps ensure we meet our platform uptime SLA. The TLS Protect for Kubernetes team is always a phone call or text away."

Making certificate-as-a-service truly frictionless for developers

Development teams were thrilled that they nolonger had to worry about the various aspects of certificate management that used to hobble speed of development —including requesting tokens, managing private keys and maintaining cert-manager across hundreds of clusters. Moreover, they could now procure and manage valid Venafi-approved certificates without having to worry about whether certificates adhered to policy.

Said the vice president of platform, "I'm happy knowing that the risks of outages have been greatly diminished because of cert-manager or certificate misconfiguration issues, not to mention that we are now in compliance with corporate security policy."