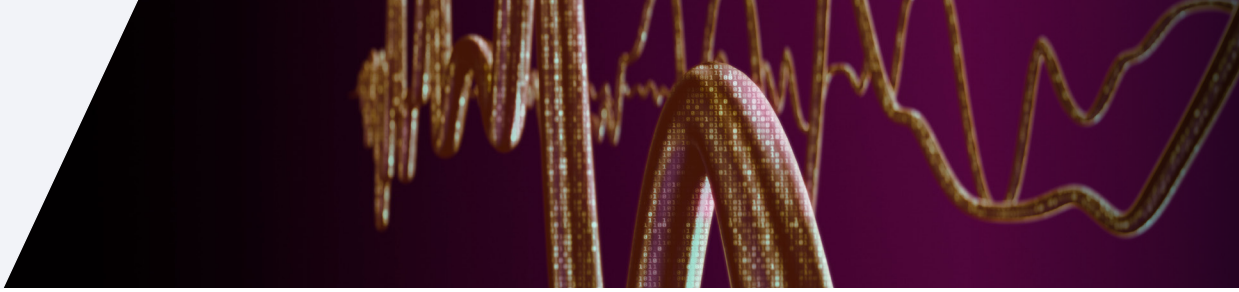
Venafi



CASE STUDY

Leading Energy Company Improves Security and Empowers Its Business

Uses Venafi Key and Certificate Security to Protect Its PKI

Executive Summary

Industry: Energy

IT Environment: Multiple data centers secure 10,000+ employees, partner access and customer web portals.

Business Challenges

- Secure SSL/TLS certificates for web services
- Protect certificates for mobile devices, multi-factor authentication and other projects
- Attain visibility into certificate location, strength and compliance
- Manage risk and protect against trust-based attacks
- Solution Business Impact
- Delivered "push button" results
- Offered a complete, detailed inventory of keys and certificates
- Enabled prioritization based on the level of risk and value of the asset
- Remediated systems impacted by the Heartbleed vulnerability
- Protected against other trust-based attacks

Business Profile

This energy delivery company transports, generates and distributes energy using an oil and liquid transportation system, a large natural gas distribution system and renewable energy. With operations across North America and the critical nature of energy supplies, the company has a first-class security team dedicated to protecting its digital and physical assets.

IT Environment

Today, the company's network supports 10,000+ employees with 8,000 mobile users. The network also secures access by alliance partners and customer web portals that enable billing and payment services. With a large geographical footprint, the company maintains multiple data centers across North America. The security team uses Public Key Infrastructure (PKI) to support these projects and services and secure the company's business across the continent.

Business Challenge

The company's security team was going to rely more heavily on PKI to secure their web services and they had projects on the roadmap, such as multifactor authentication (MFA) based on certificates. The security team also planned to use PKI to secure VPN access and mobile devices.

The prospect of expanding their reliance on keys and certificates without visibility and protection for these assets was a huge concern. The team was manually managing approximately 50 digital certificates, but they also knew that there were many more keys and certificates issued "out there" in their infrastructure. What they did not know was where each certificate was located, who had signed them or the strength of the cryptography used.

"We knew that we couldn't manually manage thousands of keys and certificates, and we knew that we needed a better way to ensure that they were correctly configured and compliant with our security policy," said the Senior IT Risk Management Analyst. "Without the ability to monitor keys and certificates, we had a huge amount of unmanaged risk."

Also, with a leap in trust-based attacks, the team knew that it needed to increase its security for keys and certificates. "What was considered secure two or three years ago isn't at all secure in today's world," said the senior analyst.

Solution: Venafi

As they were wrestling with these challenges, several team members attended a Gartner event where Venafi had been named as a Gartner "Cool Vendor." Curious, they sought additional information and immediately saw the value in Venafi key and certificate security. The company purchased the full Venafi product portfolio, which secures keys and certificates for SSL/TLS, SSH and mobile devices.

"Keys and certificates are a mix of low risk and the 'crown jewels.' One of the most interesting Venafi benefits is the ability to use the scan results to easily scope things in and scope things out and identify the critical points. Venafi was able to quickly and specifically show us the risk level and we found about 500 certificates were high-risk."

Senior IT Risk Management Analyst
Energy Company

"Venafi sold itself," said the senior analyst. "Its quality was amazing and the Venafi team's expertise and passion for security was obvious."

Solution Business Impact

Immediate Results

The company initiated a proof of concept. With a couple of conference calls and a demo over the phone, the company's security team began to use the Venafi platform and saw immediate results.

"When you demo the Venafi push button certificate issuance and deployment, voila there it is. It's a very powerful demonstration showing the gains you can get from this product," said the senior analyst. "The solution functioned as advertised right out of the gate. It was a perfect fit for our environment."

Central Visibility and Security

Using the Venafi platform, the security team created a complete key and certificate inventory. "Whether you like it or not, people are using keys and certificates on your network. They just are," said the senior analyst. "What's important is do you know where keys and certificates are being used, are they managed and are they conforming to policy?"

With the results of the Venafi assessment, the security team went from manually managing 50 certificates to discovering over 2500 keys and certificates on their network.

Reduced Risk

With Venafi key and certificate discovery, not only did the security team get a complete inventory, they were also able to prioritize the risk associated to each of those assets.

The company's security team quickly secured their most critical keys and certificates. Now with Venafi, they can correlate their security efforts to the level of risk and value of the asset.

Heartbleed Remediation

When Heartbleed erupted, the company used the Venafi platform and discovered several additional vulnerabilities beyond those discovered by their vulnerability scanners.

"We use several vulnerability scanners, but they are a broad tool and don't necessarily identify key and certificate vulnerabilities," said the senior analyst.

"Because of its focus, the Venafi platform helped us identify vulnerabilities that were specific to keys and certificates that were undetected by our other scanners. And even if hundreds of systems are affected, after the systems are patched, Venafi can complete the remediation by replacing keys and certificates with the push of a button."

"By securing our keys and certificates with Venafi, PKI has gone from being a burdensome, mysterious, black-box environment to being tools that we use at the forefront of our security. The Venafi solution empowered our business from day one."

Senior IT Risk Management Analyst
Energy Company

Protection against Trust-based Attacks

Venafi has become an integral part of the company's security ecosystem, protecting the company against trust-based attacks. The security team uses the Venafi platform to ensure that high-risk systems are secure using strong cryptography. The security team also uses Venafi to ensure that the certificates on each system are the ones that were originally issued. Certificate mismatches are a good indication that the system has been compromised, for example, with a man-in-the-middle (MITM) attack. Any mismatch is flagged, and the PKI team can immediately take action with Venafi.

Empowering the Business

With Venafi, the security team has been able to identify the high-risk SSL/TLS certificates and focus their efforts where they will have the most impact. The security team is also using Venafi to secure its mobile certificates. Today, businesses need to support multiple certificates per user. This growth is unsustainable using manual processes. But with Venafi the security team has easily and securely scaled its use of keys and certificates.

"We've been able to automatically issue certificates for our mobile devices. This has enabled all sorts of new functionality by interfacing our mobile devices with other devices," said the senior analyst.

Next Steps

To date, the company has focused on securing its most critical SSL/TLS keys and certificates. Soon, all 1,000 SSL/TLS certificates and 8,000 mobile certificates will also be inventoried and protected. The next step is to secure all SSH keys.

The security team also plans to leverage the extensive API driver integration offered by Venafi to enable the Venafi platform to integrate with other security appliances. Ultimately, the team wants to feed the Venafi intelligence to their overall security dashboard and supply their operations center with security metrics. Then when a sensitive event occurs, information would be sent and escalated in the operations center, allowing for more efficient remediation efforts.

"The Venafi team is a group of passionate, responsive and focused people," he said. "I can't say enough about how positive our relationship has been. The solution does what they say it will do, and it does it well. Period."

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**