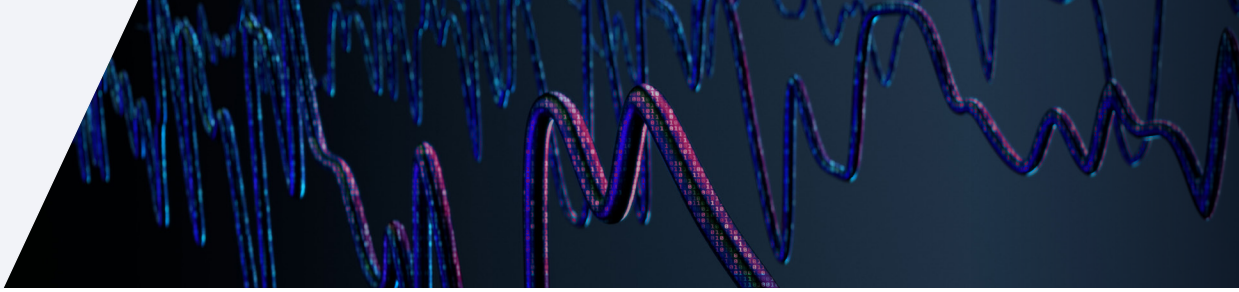
Venafi



CASE STUDY

Surescripts Moves to Decisively Reduce Risk

Company Uses Venafi to Minimize Risk in Key and Certificate Lifecycle Management While Supporting Rapid Growth

Executive Summary

surescripts

Industry: IT Services for Health Care

IT Environment: Provides secure connectivity and bi-directional exchange of health care information.

Business Challenges

- Assure trusted exchanges of confidential health information
- Improve certificate lifecycle management with customers
- Reduce risk by securing keys and certificates
- Scale keys and certificates safely to support rapid growth

Solution Business Impact

- Enables fast remediation of noncompliant keys and certificates
- Reduces risk with well-regulated, visible keys and certificates
- Simplifies ongoing monitoring with a clear baseline for "normal" activity
- Protects against trust-based attacks
- Enables secure and automated scalability

Business Profile

Surescripts provides the only nationwide network in the U.S. that lets health organizations securely share electronic clinical information. The company's customers include pharmacies, retail clinics, physician practices, hospitals, health information exchanges (HIEs), health information service providers (HISPs), pharmacies and imaging centers. Through Surescripts, these organizations easily communicate with each other through a single point of connectivity, regardless of the technology platforms they use.

IT Environment

Surescripts enables standards-based connectivity and bidirectional exchange of a broad range of health information. These services enable communications between hospitals, physicians, payers, pharmacies, labs and more. Providing services to the highly regulated healthcare industry requires ensuring privacy and limiting access where needed.

Business Challenge

Healthcare demands strict compliance with privacy regulations and the Health Insurance Portability and Accountability Act (HIPAA). This means that Surescripts must assure trust for a wide range of information types, such as referral orders, continuity of care documents, immunization notifications, visit summaries and more.

To support the confidential exchange of information, new Surescripts customers provide a certificate signing request (CSR). Surescripts then signs the CSR with its internal issuing certificate authority (CA). This enables Surescripts to create a secure connection to customers' networks, issue keys and certificates and create mutual trust files. Surescripts' IT team works directly with customers, while the security team manages the certificate lifecycle—from issuance and revocation to troubleshooting, inventory and expirations.

Surescripts also needs to ensure secure email between itself and other HISPs on behalf of customers. Surescripts generates organizational email certificates for their customers, installs them into an email platform and publishes them so that other organizations can identify trusted entities. Surescripts needed an easy way to generate S/MIME certificates and track ownership of these certificates, enabling Surescripts to notify customers when certificates must be updated.

Recently, Surescripts embarked on a major growth initiative, which meant significantly scaling their certificate inventory and processes. Instead of an average of one per week, the company expects to issue hundreds of certificates per week.

Solution: Venafi

With many more threats striking at keys and certificates, Surescripts took a hard look at their trust infrastructure and several potential solutions to help reduce risk. The Surescripts team needed a solution that would both reduce risk and increase efficiency in their key and certificate processes, while also securing and automating these processes as the company grows. A new solution also had to integrate easily with their existing multivendor PKI infrastructure. The company briefly considered cloud solution providers, but they often required that the existing infrastructure be significantly changed, which was not an option.

"We wanted a vendor with a neutral viewpoint and a solution that allowed us to be as strategic as possible," says Paul Calatayud, Chief Information Security Officer for Surescripts. "For example, we wanted open APIs, so that we could enhance interactions with our customers. We wanted the option to pull data from our Salesforce system and offer certificate self-service options through a portal. And we wanted role-based access control to strengthen policy and enforcement."

"Venafi helped us dramatically reduce risk. The Venafi platform made it much easier to put strong governance in place. Now, private keys are not issued on random servers. With Venafi, we've improved data integrity by automating much of the process. And we know what 'normal' looks like, so we can better detect anomalies when they occur."

Paul Calatayud,
Chief Information Security Officer, Surescripts

Surescripts found all of that and more with Venafi.

Solution Business Impact

Brought Fast Results in the Proof of Concept

Venafi consultants supported the Surescripts teams during a proof-of-concept pilot and implementation. In less than three weeks, the Venafi platform was making a measurable difference. The solution detected certificates and keys that did not comply with enterprise policies for attributes such as key length, hashing algorithm and validity periods. The Venafi platform also generated new compliant keys and certificates and allowed Surescripts to automate secure replacement of the vulnerable ones that were identified.

Reduced Risks in Certificate Processes

Surescripts' previous certificate issuing processes increased risk. One location sent data to a second location, which would issue certificates. Sending data back and forth between locations created potential vulnerabilities. Because the process was manual and required multiple staff to be involved, data quality issues also surfaced.

"Now that we have a huge amount of accountability and situational awareness around keys and certificates, we increased their cipher strength and beefed up our lifecycle policies to further reduce risk from trust-based attacks."

Paul Calatayud,
Chief Information Security Officer, Surescripts

"Adding to the risk was the fact that we lacked visibility into keys and certificates," says Calatayud. "We couldn't be absolutely certain who had issued them, which devices had the proper ones and we had no way to validate their cipher strength."

Now Venafi provides Surescripts with complete visibility across multiple types of encryption assets, including TLS keys and certificates, SSH keys and mobile and user certificates. It identifies key and certificate vulnerabilities, enforces enterprise policies and detects anomalies with ongoing monitoring. By deploying the Venafi Platform, Surescripts established a well-regulated, visible environment for their keys and certificates.

Provided Protection Against Trust-based Attacks

Today, Surescripts knows exactly where keys and certificates are issued and to whom, which will accelerate remediation in the event of a trust-based attack. The security team has a high trust level that certificates are compliant and known. At the same time, the Venafi Platform automates and simplifies key and certificate operations, which reduce the burden on the IT team.

Simplified Ongoing Monitoring and Maintenance

With Venafi, Surescripts established a baseline of normal certificate and key usage to simplify ongoing monitoring. And the security team was able to easily define key and certificate ownership and assign appropriate roles.

Delivered Secure and Automated Scalability

Venafi also gives Surescripts the ability to automatically scale its processes. "A growing volume of keys and certificates raised several critical concerns," says Calatayud. "Clearly we would have a much greater attack surface and higher risk. In addition, our existing solution was difficult to scale to the level we needed. Without Venafi, we would have had to add 20 staff to support the growth."

Enabling Additional Company Growth

The Venafi platform has allowed Calatayud's team to become more strategic than they had ever imagined. With the Venafi APIs, Surescripts has greatly simplified onboarding new customers. The Venafi APIs also provide flexibility to further expand their capabilities.

"We can provide the right APIs for certificate issuance while assuring transaction quality and medical-grade compliance," says Calatayud. "We hope to also create a self-service portal for customers, so that they can easily check the status of their certificates and renew them. We're just getting started."

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**