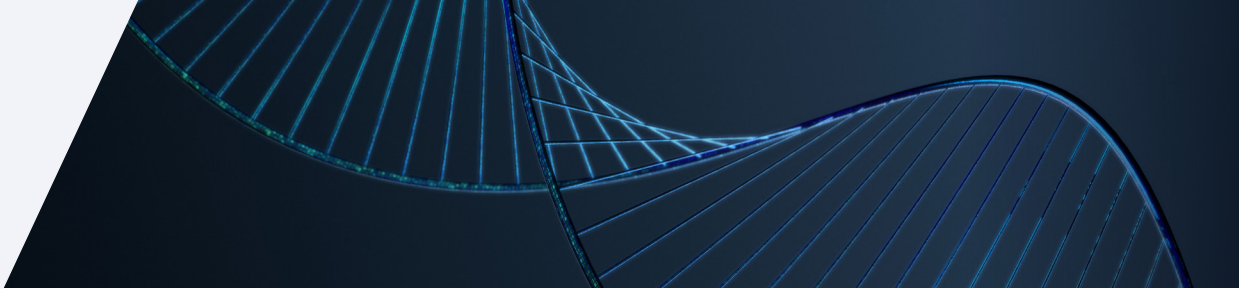
Venafi



VIA VENAFI BRIEF

VIA Venafi: 8 Steps to Stopping Certificate-Related Outages

A roadmap to building, maintaining and scaling a solution that eliminates certificate-related outages across your enterprise

VIA Venafi

Who should read this: This VIA Venafi brief is for current and prospective Venafi customers. It should be read by CISOs, security architects and security directors who understand PKI and the importance of maintaining proper machine identity management lifecycles but lack a management plan that can easily be followed. The guidance in this brief will enable their teams to stop certificate-related outages.

As organizations race toward digital transformation, the reliance on secure machine-to-machine communications has caused an exponential increase in the number of TLS certificates organizations need to manage and protect. With InfoSec teams struggling to extend necessary certificate management and security, certificate-related outages are on the rise. When sites, services and applications fail due to expired or misconfigured certificates, these failures cause time-consuming, expensive and even job-threatening challenges.

The Challenge

Certificate-related outages are becoming increasingly common in our digital economy, and their impact is often substantial.

Research[1] sponsored by Venafi in early 2022 shows that the average organization has hundreds of thousands of certificates in use. Across companies of all sizes, the average number of machine identities per organization at the end of 2021 was nearly 250,000 and was estimated to increase by 42% per year.

Outages that occur when TLS certificates are not renewed are common. According to the study:

- 83% of organizations suffered a certificate-related outage during the last 12 months
- 26% of the CIOs whose organizations experienced outages said these outages impacted business-critical systems.

Of the companies that reported outages:

- 80% had a minimum of three outages per year
- 55% had 12 or more outages per year
- 25% had weekly outages (52+) per year

Organizations need a proven plan to combat these challenges. That includes an experience-born blueprint that helps them navigate the complex people, processes and technology issues connected with outages due to expired or misconfigured certificates. In addition, they need a roadmap to their desired, transformed end state: dynamic, outage-free certificate management across their organization.

VIA Venafi: The Venafi Way

Venafi has helped hundreds of global customers eliminate site and service outages that result from certificate expirations and misconfigurations. The approach, which is based on a deep understanding of all the components needed to achieve this outcome, is VIA Venafi, the Venafi Way.

VIA Venafi is founded on Venafi TLS Protect, part of Venafi Control Plane for Machine Identities. TLS Protect delivers the observability, consistency, reliability and freedom of choice organizations need to protect themselves from certificate-related outages. With Venafi TLS Protect, organizations can:

- Discover and monitor all TLS keys and certificates
- Define and enforce security policies with ease
- Reduce downtime with a fast, automated service that scales
- Implement in the data center or cloud, depending on needs

Professional Services: VIA Venafi Direct

While organizations can implement VIA Venafi on their own, Venafi has ready-made service offerings to assist in customer deployments.

VIA Venafi Direct service offering is designed to help shorten time-to-value and assure completion of an outage prevention project. A Venafi program manager along with seasoned delivery consultants work together with your project team to develop and deploy a machine identity management program based on VIA Venafi's critical steps.

Along with leveraging Venafi TLS Protect, VIA Venafi aligns people and process and uses proven experience to drive InfoSec and application teams to the common goal of eliminating TLS certificate-related outages.

The 8 Critical Steps

When the following steps are applied completely, they prevent certificate-related outages in your organization:

1. Establish an outage safety net

If your organization has been hit by certificate-related outages, the first thing to do is "stop the bleeding." Unfortunately, certificate owners frequently don't understand the certificate renewal process and can be caught unprepared by sudden outages. Although InfoSec teams cannot stop outages by themselves, they can identify certificates that are about to expire by using Venafi TLS Protect. The InfoSec team can then create an "outage safety net" process to alert critical parts of the organization about impending outages. An effective outage safety net notifies organizational leaders who can influence immediate action rather than trying to track down individual owners of certificates. It builds executive awareness of looming outages and promotes heightened responsiveness across the organization before sites, services and applications are crippled.

With VIA Venafi Direct, Venafi Professional Services can help you establish this important outage safety net faster. The Venafi team has years of experience deploying Venafi TLS Protect and deep know-how about certificate discovery. Venafi can also help as you identify key teams, processes and analytics throughout your organization—and start educating certificate owners about preventing outages.

2. Establish a foundation for the outage prevention solution

Providing a centralized system that's configured to help certificate owners maintain the lifecycle of their certificate inventory is a critical component in preventing outages. Venafi TLS Protect provides key features and functionality that, when configured correctly, enable automated processes to help streamline the management of certificates. This solution provides the observability, consistency and reliability organizations need to prevent certificate-related outages. This step, while initially focused on preventing outages, also provides the long-term technology foundation for a comprehensive machine identity management control plane.

3. Align the organization around a service-based approach

Obtaining agreement across an organization's silos is not an easy task but Venafi has assisted hundreds of customers in navigating this terrain and has applied this experience to drive agreement across teams. Not only does Venafi help teams gain organizational agreement to build a service, but it also helps demonstrate how the service enables application and development teams to run faster, experience fewer obstacles and achieve their goals more securely.

InfoSec teams cannot stop outages on their own. They often lack permissions or contextual knowledge of how certificates are consumed on a given server or application. Venafi provides certificate owners with security-centric knowledge and practices to facilitate their efforts. Combined with these processes, Venafi provides an application-focused workflow that streamlines and simplifies the request process, all while ensuring industry security practice is enforced.

Resulting from this work, an understanding of policies, roles and responsibilities works in tandem with out-of-the-box capabilities and a broad ecosystem of integration partners to help certificate owners easily solve certificate-related issues themselves. Simultaneously, the InfoSec team gains a centralized platform to implement controls as well as visibility across machine identity types.

4. Define and design the services

Once organizational consensus is obtained, organizations need to assemble a team to build service offerings. In this effort, Venafi customers benefit from the practical, real-world knowledge we've accrued from working with hundreds of integrations teams. In addition, they can enlist the aid of the Venafi Professional Services team, through the VIA Venafi Direct service offering, to help them simplify complex projects and remove unknowns. In both cases, customers benefit from shared experiences and the knowledge of what has worked in other organizations.

The Venafi team brings lessons learned from hundreds of customers to simplify the complexity of the program while reducing unknowns.

This step also includes two key aspects of the overall solution: creation of an enterprisewide machine identity protection policy and the detailing of workflows, signoff and exceptions. The policy for machine identities standardizes practices and takes the guesswork out of the myriad of questions that must be answered, including:

- Which certificate authorities have been approved by the organization?
- What are the required configurations for certificates and keys?
- What parameters should be defined for key lengths, algorithms and expiration dates?

In designing workflows, the service is integrated with other systems like ticketing and ITSM solutions, where automated procedures for signoff and override are documented.

In designing the service for VIA Venafi Direct customers, Venafi Professional Services focuses on two key aspects of the overall program:

- Creation of an enterprise-wide machine identity protection policy to support the program
- Detailed documentation of workflows, signoffs and exceptions needed to drive the program

We channel our experience to assist our customers' staff in building multifaceted, streamlined implementation plans and offer clear advice on the ways in which Venafi TLS Protect integrates with an organization's current tools and solutions.

5. Train the teams that support the services—and document the processes

While teams are designing and defining the services in Step 4, it's time to start training the teams who support the services. Venafi experts—through consulting services or presales advice—can help train and enable these deployment teams so they become experts in managing certificate lifecycles as part of a broader InfoSec strategy.

Part of this training is implementing a process to onboard a certificate owner team; set up corresponding policies, folders and workflows; and enable messages and notifications. This often includes product and process training based on existing Venafi education programs and classes, as well as tools the team can use to educate and inform their internal stakeholders and customers.

6. Recruit, train and onboard early adoption teams for initial rollout

Gaining early "wins" and building momentum for the project is critical to its success. The Venafi team helps an organization identify and onboard early adopters of the certificate service that provides high value to the business, such as customer-facing services or online apps, or teams that have a high concentration of systems requiring TLS certificates. These often consist of some of the most critical systems, applications and data sets, including F5, NetScaler, DataPower and IIS groups. By onboarding these teams first, Venafi helps customers eliminate the risk of the costliest outages, build awareness across the organization and validate documented processes.

7. Expand adoption: Onboard certificate owners for enterprise rollout

Now it's time to enable broad adoption of the Venafi service by all application and network teams. As new groups are brought into the service, which is built on the Venafi Control Plane, they become active participants in the organization's machine identity protection strategy. The owners and managers of TLS certificates sometimes become aware of the service through ongoing communication about the organization's machine identity management goals. Occasionally, awareness comes in response to an outage or because of a "near miss" brought to light by the outage early warning system (see Step 1 above).

In this step, all certificate owners must be trained on machine identities and, if necessary, on user interfaces.

For VIA Venafi Direct customers, Venafi Professional Services educates InfoSec teams on best practices associated with defining a repeatable onboarding process to create a single platform for managing machine identities. Using a "train-the-trainer" method, the Venafi program manager assists the customer team with the onboarding of remaining certificate owners. The customer project team becomes empowered and trained in onboarding best practices for certificate owners, including providing the necessary end user-guidance and training. Additionally, Venafi Professional Services assists with the full onboarding of up to five (5) technology integrations in support of the five teams that manage the integrated platforms.

8. Assess service effectiveness, tune and evaluate the adoption process

Human error is a fact of life. Once certificate owners have taken a proactive role in managing machine identities and preventing certificate-related outages, the system can validate their work and ensure the appropriate steps have been followed. This includes the daily validation of all installed certificates and ensuring that renewed certificates are configured and operating correctly.

This step avoids many of the outages caused by fast-moving staff or those still unfamiliar with certificate-related best practices and acts as a fail-safe for many automated actions. It also checks the configuration of the end-entity certificate and validates the end-to-end certificate chain to ensure the correct certificate is both installed and effective. As an outcome of this step, the InfoSec team becomes armed with the operational processes necessary to identify potential issues before they become a problem, as well as the procedures needed to efficiently resolve them.

For VIA Venafi Direct customers, at the onset of the project, the Venafi Professional Services team works with the customer to develop a program high-level project plan. This document is used during the rollout phase of the project by the Venafi program manager with the assistance of the customer's project team to perform periodic evaluations of the overall effectiveness of the program.

Next Steps

The VIA Venafi No Outage Guarantee

Imagine a world where you will not only never again experience a site or service outage caused by an expired certificate but where "never" is guaranteed. At Venafi, we're so sure that customers who follow our guidance will not encounter a certificate-related outage, we guarantee it. Read about our "VIA Venafi No Outage Guarantee." **venafi.com/solutions/VIA/no-outages**

The VIA Venafi Review

Venafi has helped hundreds of customers stop their certificate-related outages. This is a critical step on the way to achieving an even larger goal: trusted machine identities across the enterprise that are protected against security risks of any kind. But whether your goal is simply to stop certificate-related outages or embark on an enterprisewide program for protecting machine identities, we know the process isn't easy. Our VIA Venafi Review provides an assessment of a customer's progress along these 8 Steps, with actionable advice and prescriptive suggestions.

For many customers, a VIA Venafi Review is a recommendation in their Customer Success Plan, a joint plan by Venafi and the customer, that identifies specific steps to take for each upcoming quarter to mature their machine identity management program.

Contact your account team for more information on the No Outages Guarantee, VIA Venafi Review or VIA Venafi Direct service offering.

Resources:

1. Venafi-sponsored study by market research firm Coleman Parkes Research of 1,000 CIOs from six regions: United States, United Kingdom, France, DACH (Germany, Austria, Switzerland), Benelux (Belgium, Netherlands, Luxembourg) and Australasia (Australia, New Zealand). 2022

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 identity management for machines. From the ground to the cloud, Venafi solutions automate the lifecycle of identities for all types of machines—from physical devices to software applications, APIs and containers. With more than 30 patents, Venafi delivers innovative solutions for the most demanding, security-conscious organizations in the world. **To learn more, visit venafi.com.**