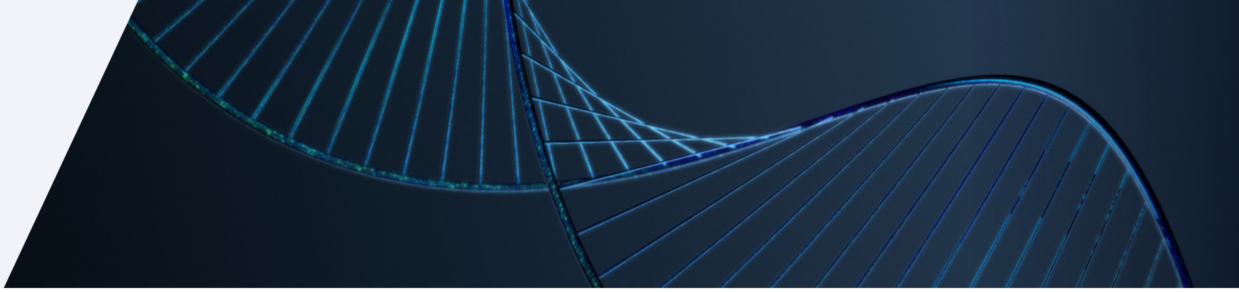

VIA VENAFI BRIEF

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

Who should read this: This VIA Venafi brief is for current and prospective Venafi customers. It should be read by CISOs, security architects and PKI directors who understand PKI and the importance of maintaining proper certificate lifecycles, but lack a certificate management plan that can be easily 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 SSL/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.

Reports from both the U.S. Government Accountability Office (GAO) on Oversight and Government Reform and U.K.'s Information Commissioner's Office (ICO) pointed to the expiration of a certificate as part of the failure at Equifax that led to the theft of data from hundreds of millions of people.[1]

Similarly, certificate-related outages were the reason why thirty million customers lost access to O2 and other UK mobile providers in late 2018, and were the cause of multiple highly publicized website and application failures, such as the LinkedIn outages of 2017 and 2019 and Microsoft Teams in 2020.[2]

Research by Venafi shows that the average Global 5000 company has thousands of TLS certificates spread throughout its infrastructure. It also found this number is increasing by 25% year over year,[3] with 95% of companies not knowing where all of their machine identities, including their TLS certificates, are being used within their networks.[4]

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 over 350 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 technology invented by Venafi that delivers the visibility, intelligence and automation necessary to stop outages.

Visibility: Venafi helps enterprises discover TLS certificates wherever they are across broad global infrastructures—whether in known network locations or across the internet's IPv4 address space—and notifies certificate owners and other stakeholders when escalation actions are needed.

Intelligence: Once machine identities are discovered, Venafi applies an organization's policies related to expiration dates, installation locations, validation of corrective actions and more to make certificate lifecycle management intelligent, efficient and easy.

Automation: Venafi automates standard machine identity tasks—from reporting and information retrieval to certificate renewal or revocation—reducing the risk of human error and the cost of labor.

Professional Services

Venafi has ready-made service offerings to assist in customer deployments.

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

New Venafi customers with a recommended **Venafi Proven Path: Foundation Level One** service offering will get assistance accelerating the first two steps of VIA Venafi.

The VIA Venafi methodology is essential in protecting the TLS certificates that connect and encrypt 350 million internet domains, over 1.5 billion sites and countless services that are critical to security and operational systems alike—from e-commerce and financial transaction systems to load balancers and traffic inspection devices.[5]

VIA Venafi uses proven experience to drive InfoSec teams to the common goal of eliminating certificate-related outages before they occur.

The 8 Critical Steps

When the following steps are applied completely, they will 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 the Venafi Platform. The InfoSec team can then create an "outage safety net" to alert critical parts of the organization about impending outages. An effective outage warning system notifies organizational leaders rather than trying to track down individual owners of certificates. It builds executive awareness of impending outages and promotes action before sites, services and applications are crippled.

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

In this step, Proven Path: VIA Venafi Direct customers can get help defining their outage safety net, identifying key teams, processes and analytics, as well as educating certificate owners about preventing outages.

2. Establish a Foundation for the Outage Prevention Solution

Install the Venafi Platform components to implement an outage prevention solution. This solution, even in its out-of-the-box state, provides the visibility, intelligence and automation your organization needs 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 platform.

Venafi works with server operations, network, InfoSec and PKI teams to implement the Venafi Platform, which includes installation, configuration and enablement of key functions and capabilities. Our experienced services and support teams provide best practices and assist in standing up the core service and its functions.

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 help 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 assists application and development teams run faster, experience fewer obstacles and achieve their goals more securely.

Because InfoSec teams cannot stop outages on their own (they often lack permissions or contextual knowledge of certificate usage to do this), Venafi provides certificate owners with security-centric knowledge and practices to facilitate their efforts. 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. At the same time, 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, our 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 Proven Path: VIA Venafi Direct service offering, to help them simplify complex projects and reduce the number of unknowns. In both cases, customers benefit from shared experiences and the knowledge of what has worked in other organizations.

This step also includes two key aspects of the overall solution: creation of an enterprisewide machine identity management policy and the detailing of workflows, signoff and exceptions. The policy for machine identities will standardize practices and take 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, and procedures for signoff and override are documented. We channel our experience to assist our customers' staff in building multifaceted, streamlined implementation plans and offer clear advice on the ways in which the Venafi Platform integrates with an organization's current tools and solutions.

5. Train the Teams Who Support the Services—and Document the Processes

While teams are designing and defining the services in Step 4, Venafi experts—through consulting services or presales advice—can help train and enable these deployment teams. The goal for Step 5 is to instruct them on becoming experts in managing certificate lifecycles as part of a broader InfoSec strategy. Venafi works with PKI and InfoSec teams to show how 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

In this step, customers gain early "wins" and build momentum for the project. 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 Platform, they become active participants in the organization's machine identity management 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 are trained on machine identities and, if necessary, on user interfaces.

Through a train-the-trainer method that is part of the Proven Path: VIA Venafi Direct service offering, Venafi can assist with the onboarding of all remaining certificate owners. Your project team will be trained in the best practices to onboard new certificate owners, including providing the necessary end user guidance and training.

8. Assess Service Effectiveness, Tune and Evaluate the Adoption Process

Once onboarded, certificate owners have a simple interface to work with, and the service informs them when they need to perform certificate lifecycle actions to prevent an outage. Owner actions are bound by the workflows or approvals defined by the organization's change management plan. Owners can perform the required actions manually or leverage the fully automated capabilities of the Venafi Platform. Actions can also be performed completely through APIs to satisfy the needs, for example, of a fast-moving DevOps team.

In the event a certificate owner does not take appropriate action within the acceptable time frame, detailed escalation paths are defined and enabled. Not only are individual alerts created, but enterprisewide visibility is provided through dashboards and reports that are configured to track organizational progress. To be proactive, future expirations can be reviewed in detail and planned for accordingly.

Venafi Professional Services can help formalize this process through the development of a "Maturity Goals and Strategy" document to track and evaluate the ongoing effectiveness of the program.

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.

Why Do Other Methods Fail to Stop Outages?

InfoSec professionals have been dealing with certificate-related system and service outages for as long as the internet has been around. There are numerous reasons manual or even semi-automated processes do not stop these outages. Chief among these is the sheer volume of certificates in many large organizations. Worse yet, is the number of certificates organizations do not even know they have. Manual processes just can't keep pace with certificate growth.

Apart from the obstacle of rapidly increasing certificate volumes, specific points of failure often create headaches for organizations not using VIA Venafi.

- **Building a spreadsheet inventory is not enough.** Network discovery may find web server certificates and load balancer certificates, but it won't locate certificates that aren't actively listening for TLS handshakes.
- **Assigning certificate ownership by requestor doesn't work.** Tracking ownership is a difficult task and may become impossible if the original requestor changes positions or leaves the company.
- **Single certificates in multiple locations lead to unexpected failures.** The same certificate may be installed in multiple locations. Yet it wouldn't be obvious that these are the same certificate.
- **Escalation capabilities are critical.** If the person being notified of an impending certificate expiration fails to act, an automated escalation path is needed.
- **Email is often seen as a burden and noise.** If staff is notified by email that a certificate is going to expire, is there assurance that the message will get through?

VIA Venafi addresses these potential failure points to eliminate the risk of certificate-related outages.

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 machine identity management, 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 Proven Path: VIA Venafi Direct service offerings.

Resources:

1. United States Government Accountability Office. Report to Congressional Requesters. Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. August 2018.
2. Ranger, Steve. ZDNet. O2 Network Outage Ends: Here's What Happened. December 7, 2018.
3. Dimensional Research sponsored by Venafi. Survey on Growth of Cryptographic Keys and Digital Certificates. 2017.
4. Research by Venafi Labs and assessments by Venafi Professional Services.
5. Tek Eye. How Many Websites Are There in The World? Last Updated: January 2019.

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**