Solution Brief

VENAFI

Don’t Let Certificate Outages Impact Your Business

Unplanned digital certificate expirations can interrupt business operations and impact your bottom line

Unplanned certificate-related outages are not just inconvenient, they can be very costly. The resulting downtime can jeopardize revenue on your external commerce sites. But it can also wreak havoc on reliability and availability. Recovering from an unplanned certificate outage can be lengthy and siphons valuable IT resources from other important projects. To maximize productivity and minimize emergency downtime, you need to actively manage certificates to prevent them from expiring unexpectedly.

More Certificates Can Lead to More Outages

Widespread security initiatives like HTTPS Everywhere and an explosion of new devices that require SSL/TLS for authentication have caused an exponential increase in the number of keys and certificates your organization needs to manage and control. With Google and others pushing for shorter and shorter certificate renewal periods, you’ll be forced to step up your certificate lifecycle management. If your organization relies on more than one Certificate Authority (CA), coordinating management efforts between CA dashboards will quickly become overwhelming.

Managing the certificates that you know about is hard enough. But now free CAs make it relatively easy for anyone in your organization to request and install a certificate without contacting IT. This can result in large numbers of unknown certificates—large organizations report finding an average of 16,500 unknown keys and certificates after deploying Venafi.[1] As a result of this significant blind spot, many outages are caused by certificates that weren’t even on the IT team’s radar. Organizations need to discover these renegade certificates by maintaining complete visibility across all certificates from all CAs.

Venafi solves certificate expiration, management and security challenges for the world’s largest banks, retailers, insurers, healthcare providers and manufacturers.

[1] Source: TechValidate. TVID: 363-53E-598.

Five Steps to Proactively Prevent Certificate Outages

To eliminate your risk of outages, you need to be able to discover, track and continuously monitor all your certificates in real time across your entire enterprise network, including cloud, virtual and DevOps environments. That's more than you can do on a single CA dashboard or on a SharePoint site. Here are five steps you can take to eliminate outages in your organization:

1. **Discover all certificates.** Choose a discovery tool that lets you look across your entire extended network—including cloud and virtual instances, and CA implementations. This will help you locate every certificate that can impact the reliability and availability of your organization's critical infrastructure.
2. **Create a complete inventory.** Catalog your entire inventory of certificates and store it in a centralized repository where you can track and manage the status of all certificates. This makes it easy to rotate your certificates before they expire.
3. **Verify security compliance.** Investigate certificate properties to ensure that certificates have proper owners, attributes and configurations so all certificates fall into line with your organization's regular cadence of renewals.
4. **Continuously monitor certificates.** Conduct non-stop surveillance of all certificates so that you'll know immediately when something isn't right. This is the most efficient way to keep tabs on renewal requirements, as well as misuse.
5. **Automate renewals.** Eliminate the risk of human error by automating certificate renewals, allowing you to install, configure and validate certificates in seconds. You'll not only improve availability, you'll be able to do it in a fraction of the staff hours previously required.

Real-time Certificate Management Helps You Avoid Outages

Venafi can help you eliminate the risk of certificate outages in your business. Our industry-leading certificate and key management solution gives you full visibility and control over certificates throughout on-premises, virtual and cloud environments. Plus, Venafi allows you to automate the entire certificate lifecycle, so all your certificates comply with your organization's security policies while improving the reliability and availability of your critical business systems.

TRUSTED BY THE TOP

5 OF 5 Top U.S. Health Insurers
5 OF 5 Top U.S. Airlines
4 OF 5 Top U.S. Retailers
4 OF 5 Top U.S. Banks
4 OF 5 Top U.K. Banks
4 OF 5 Top S. African Banks
3 OF 5 Top AU Banks

ABOUT VENAFI

Venafi is the cybersecurity market leader in protecting cryptographic keys and digital certificates which every business and government depends on to deliver safe encryption, authentication and authorization. Organizations use Venafi key and certificate security to safeguard machine-to-machine connections and communications—protecting commerce, critical systems and data, and mobile and user access.

To learn more, visit www.venafi.com