Machine Identity Protection for Federal Agencies Reduces Security Risks at Machine Speed and Scale

Prevent rogue keys and certificates from triggering outages or granting unauthorized access

Venafi at a Glance

Venafi has achieved Common Criteria Certification.

As the cybersecurity market leader in machine identity protection, Venafi secures connections and communications for machines.

Protecting machine identity types, such as SSL/TLS, SSH, IoT and mobile, the Venafi Platform delivers the machine identity intelligence needed to automatically safeguard the flow of information to trusted machines and prevent communication with untrusted ones—all at machine speed and scale.

With over 30 machine-identity-related patents, Venafi delivers a federal security-ready platform that provides agency-wide visibility, security, operational efficiency and compliance.

Benefits:

- Delivers fast and frictionless certificate acquisition and orchestration
- Strengthens security with continuous risk identification and mitigation
- Accelerates time to value with certificate-as-a-service
- Eliminates certificate-related outages with certificate lifecycle automation
- Improves governance with enhanced audit responsiveness

Venafi protects machine identities, which all federal agencies rely on to keep communications between machines secure and private.

Machine identities are established using digital certificates and cryptographic keys for machine-to-machine identity and access management. However, the explosive growth in machines—devices, applications, cloud workloads, virtual machines and containers—has outstripped the manual and homegrown management tools used by federal agencies.

The private sector spends over $7 billion dollars each year on identity and access management.[1] But nearly all of this is spent on protecting the user names and passwords people use for authentication; almost none of it goes towards protecting machine identities. The security gap around machine identities opens the door to a wide range of threats from outages to breaches, and increases risks to availability, integrity and security.

Federal agencies are both consumers and providers of machine identities. They must be able to rapidly and securely issue machine identities as new machines are spun up and deployed. In addition, they must be able to quickly determine the appropriate level of trust for all machine identities connected to their agency that reside inside and outside the boundaries of their network.

Machine identities need to be protected to secure machine-to-machine communication and authentication, keep communications safe and private and establish trust between connecting systems.

Security Risks

Cyber criminals, malicious insiders and nation-state hackers know most agencies have limited visibility, policy enforcement and remediation of machine identities, which makes certificates and keys easy, high-value targets. Cyber criminals use compromised or forged keys and certificates to break into private, encrypted tunnels where they can eavesdrop on digital communications. As we learned with Snowden and WikiLeaks, hackers can also use keys and certificates to create their own encrypted tunnels on federal networks to hide their malicious activities, install malware and remove sensitive data.

Using keys and certificates has proven to be an effective attack method, and, today, nearly half of all cyber attacks use malware hidden in encrypted traffic to evade detection.[2]

Availability Risks

Without network-wide visibility, agencies often experience unplanned, certificate-related outages. Agencies need to be proactive in their management of certificates to prevent them from expiring unexpectedly.

Machine Identity Intelligence

Venafi combats security and availability risks by providing intelligence and visibility into all aspects of machine identities across the extended network, regardless of the location of the machine identity or the issuing Certificate Authority (CA). This is paired with prioritized risk and reputation scoring to deliver an automated way to identify, quantify and prioritize the machine identities at greatest risk.

Automated, Intelligent Action

Every phase of the machine identity lifecycle can be automated, including generation, distribution, replacement, rotation and retirement, as well as compliance with all policy mandates. Each agency's need for security and availability is aligned with automated workflows and policies. Together, automation and out-of-the-box integrations deliver automated certificate provisioning and continuous policy enforcement.

Automated remediation corrects errors and weaknesses in machine identities at machine speed and scale. With Venafi, agencies can replace certificates in seconds or remediate thousands of certificates in just hours in the event of a CA compromise or the discovery of new security vulnerabilities.

Partner Ecosystem

With hundreds of out-of-the-box third-party applications and Certificate Authority (CA) integrations, agencies can fully automate the lifecycle of all machine identities within their network ecosystem. This improves operational efficiencies, availability and reliability of critical infrastructure.

The Venafi Platform has achieved Common Criteria Certification, validated by the U.S. Federal Government approved Common Criteria Test Laboratories and the National Information Assurance Partnership (NIAP).

Are you leaving your machine identities unprotected? Learn what Venafi can do for you. Visit www.venafi.com or contact us at www.venafi.com/contact-us.

TRUSTED BY THE TOP

3 OF THE TOP Civilian Agencies and the DoD
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
4 OF 5 Top AU Banks

ABOUT VENAFI

Venafi is the cybersecurity market leader in machine identity protection, 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 www.venafi.com

References

1. MarketsandMarkets.com. Identity and Access Management Market by Component (Provisioning, Directory Services, Password Management, SSO, & Audit, Compliance, and Governance), by Organization Size, by Deployment, by Vertical, and by Region - Global Forecast to 2020. March 2016.
2. A10 Networks. Infographic. Malicious Traffic Hides Behind Encryption. 2016.