Machine Identity Protection Reduces Security Risks at Machine Speed and Scale

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

Venafi at a Glance

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

Protecting machine identity types, including SSL/TLS, SSH, IoT and mobile, the Venafi Platform delivers the machine identity intelligence necessary 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 innovative solutions for the world's most demanding, security-conscious Global 5000 organizations.

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 life cycle automation
- Improves governance with enhanced audit responsiveness

Venafi protects machine identities, which all organizations 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 most organizations rely upon.

Businesses spend over $8 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. And as the number of machines increases, so do these risks.

Effective machine identity protection must start with machine identity intelligence founded on global visibility and risk analytics. This intelligence must then be applied to fast and coordinated actions driven by a set of enterprise policies and controls. With intelligence-driven automation, actions quickly remediate machine identity weaknesses. The result is improved cybersecurity, reduced risk and support for regulatory, legal and operational requirements.

> *“Venafi is a very reputable company with a unique product offering that solves significant operational and security use cases. [We’re faced with] the emerging realization that certificate and key management is the next battleground for privileged access.”*
>
> *Chief Information Security Officer, Large Chain Retailer*
>
> *Source: TechValidate TVID: 521-843-BE2*

Machine Identities in Enterprises

Organizations 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, organizations must be able to quickly determine the appropriate level of trust for all machine identities connected to their organization that reside inside and outside the boundaries of their network.

Security Risks

The vast majority of organizations (95%) don’t know how many machine identities are in use in their networks or where they reside. Cyber criminals know most organizations have limited visibility, policy enforcement and remediation of machine identities, which makes certificates and keys easy, high-value targets. And as the number of machines explodes, so does the machine identity attack surface.

Enterprises rely on tens of thousands of keys and certificates as the basis of machine identities for their websites, virtual machines, mobile devices, applications and cloud services. These machine identities need to be protected to secure machine-to-machine communication and authentication to keep communications safe and private and establish trust between connecting systems.

By using the keys and certificates that serve as machine identities in their attacks, cyber criminals hijack the chain of trust these digital assets provide.

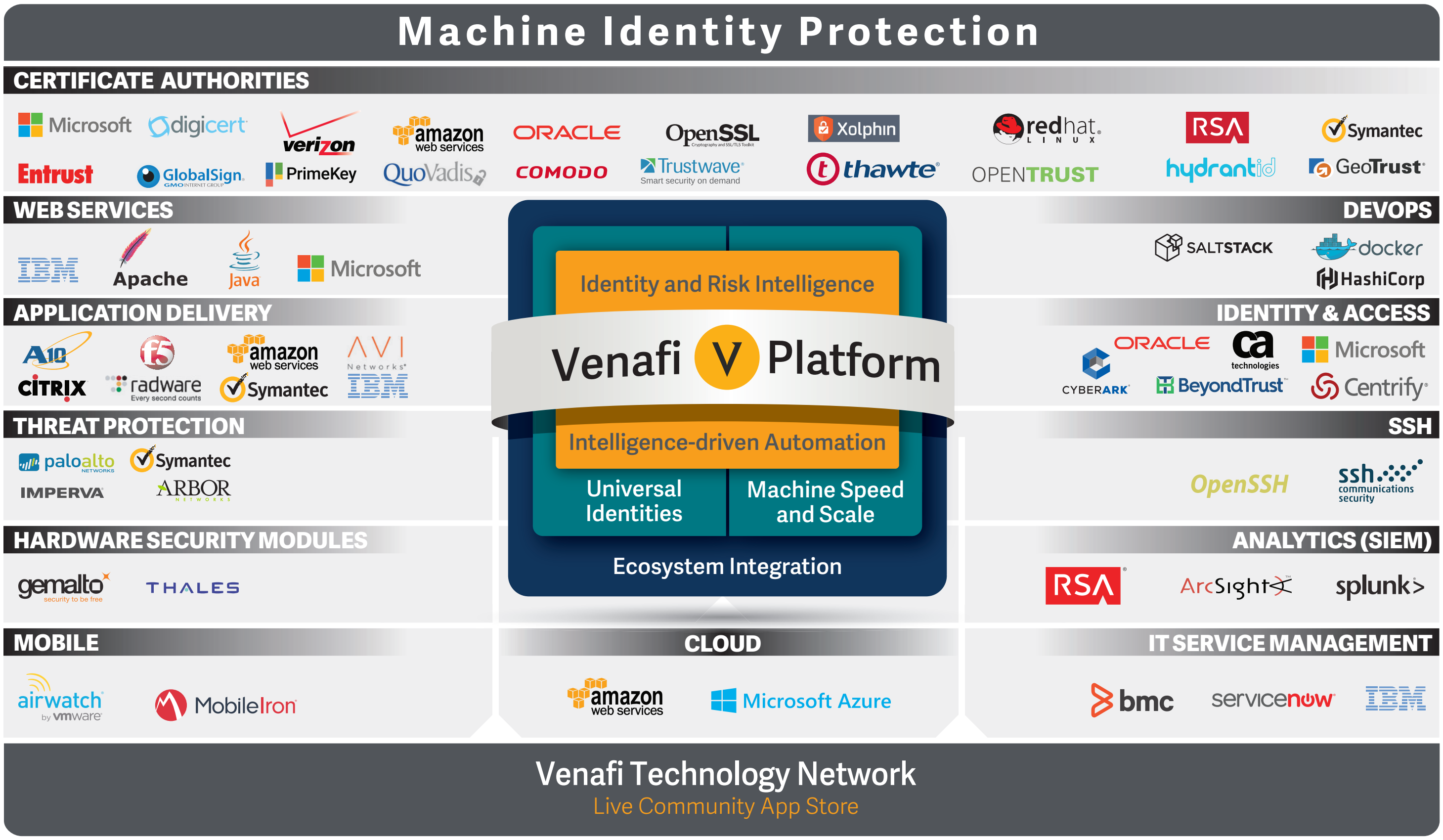
Cyber criminals use compromised or forged keys and certificates to break into private, encrypted tunnels where they can eavesdrop on digital communications. They also use keys and certificates to create their own encrypted tunnels on enterprise networks to hide their malicious activities, install malware and remove sensitive data.

Most cyber security technologies can’t see what is happening inside encrypted tunnels. Instead, they blindly trust machine identities established by keys and certificates, allowing encrypted tunnels with malicious traffic to remain hidden. 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 global visibility, organizations often experience unplanned certificate-related outages. The resulting downtime can jeopardize revenue, impede availability and lower customer satisfaction. Recovering from an unplanned certificate outage can be lengthy and siphons valuable IT resources from other business-critical projects. To maximize productivity and minimize downtime of vital business services, organizations need to be proactive in their management of certificates to prevent them from expiring unexpectedly.

It’s time to invest in machine identity protection designed to manage the volume, velocity and variety of machine identities.



Identity and Risk Intelligence

Venafi combats security and availability risks by providing intelligence and visibility into all aspects of machine identities across the global extended enterprise. This is paired with prioritized risk and reputation scoring, delivering an automated way to identify and quantify the machine identities at greatest risk.

Global Intelligence & Visibility

Comprehensive visibility into all machine identities includes those on internal and external infrastructures, the Internet and virtual, cloud and IoT infrastructures.

With Venafi, enterprises can find and track all machine identity characteristics and changes, providing the intelligence needed to proactively identify weaknesses that increase security and operational risks, regardless of the location of the machine identity or the issuing certificate authority (CA).

Risk & Reputation Scoring

External and internal certificate risk assessments allow organizations to be proactive in the identification of their security risk posture and prioritize remediation. Automating risk identification is the only approach that allows enterprises to manage the volume, variety and velocity of continuous change in machine identities.

Rogue certificate usage across the Internet is identified with a global certificate reputation service. The Venafi Platform flags certificates used to spoof, or impersonate, websites of reputable businesses no matter where they appear on the Internet, preventing potential brand damage by malicious sites.

Intelligence-driven Automation

Venafi puts machine identity intelligence into action. Intelligence-driven automation is the orchestration of rapid, corrective actions that improve security and availability, as well as reduce risks to reputation. These actions automate machine identity provisioning and remediate vulnerabilities and weaknesses at machine speed and scale.

Orchestration & Governance

Orchestration and governance align a business's need for security and availability with automated workflows and policies that govern machine identities.

Orchestration automates every phase of the machine identity life cycle, including generation, distribution, replacement, rotation and retirement, as well as compliance with all policy mandates. Together, automation and out-of-the-box integrations deliver automated certificate provisioning and continuous policy enforcement.

Remediation & Validation

Automated remediation corrects errors and weaknesses in machine identities at machine speed and scale. With Venafi, organizations 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. Validation certifies that remediation actions have been performed correctly according to specified security policies.

Partner Ecosystem

With hundreds of out-of-the-box third-party applications and certificate authority (CA) integrations, organizations can fully automate the life cycle of all machine identities within their network ecosystem. This improves operational efficiencies, availability and reliability of critical infrastructure.

Next Steps

Over half of enterprises manually track keys and certificates, and another quarter use homegrown solutions.[3] These methods don't scale or provide the automation and remediation needed to secure today's enterprises.

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

References

1. MarketsandMarkets.com. Identity & Access Management Market by Component, Organization Size, Deployment Type, Vertical, and Region - Global Forecast to 2021 February 2017. Report Code: TC 3138.
2. A10 Networks. Infographic. Malicious Traffic Hides Behind Encryption. 2016.
3. TechValidate TVID: 44E-47C-483.

> *"Venafi helped us automate a very complex task in a reliable way. Venafi is basically the only player in the market, serving a very real need."*
>
> *Engineering Director,*
> *Global 500 Banking Company*
>
> *Source: TechValidate TVID: 17B-396-F9B*

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
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