QUICK GUIDE

Migrating to Zero Trust

How Venafi helps you expand your machine identity management program to support Zero Trust Maturity

Venafi®

Today's organizations need a new security model that more effectively adapts to the complexity of modern networks, embraces the hybrid workplace, and protects devices, apps and data wherever they're located.

Recent high-profile cybersecurity incidents—such as those involving **Solar Winds**, **Colonial Pipeline** and the **U.S. Office of Personnel Management (OPM)**—illustrate the dire consequences and urgent need to rethink current cybersecurity models to accelerate Zero Trust adoption.

The shift to more secure "Zero Trust architectures," in which users and machines must prove their authenticity every time they access a network service, application or data is a critical step in mitigating cybersecurity risk for digitally transforming enterprises. Zero Trust models, which require that any access request is authenticated, are particularly crucial for organizations with hybrid cloud and cloud native infrastructure because these environments typically include hundreds of thousands of applications, containers, APIs and services—in other words, machines—each of which need a unique identity to connect and communicate securely.

The shift to Zero Trust security models is so critical that in May 2021, the Biden administration issued an **Executive Order on Improving the Nation's Cybersecurity** that specifically identified the implementation of Zero Trust security as a key security goal for federal agencies. Since then, NIST and the U.S. Cybersecurity & Infrastructure Security Agency (CISA) have been working together to develop Zero Trust guidelines, recommendations and reference architectures.

CISA has developed a **Zero Trust Maturity Model** to help organizations evaluate, develop and mature Zero Trust security architectures. This model provides a set of tools to help organizations build and develop a Zero Trust security architecture that fits their unique requirements.

The CISA Zero Trust Maturity Model encompasses five pillars, as seen in Figure 1:

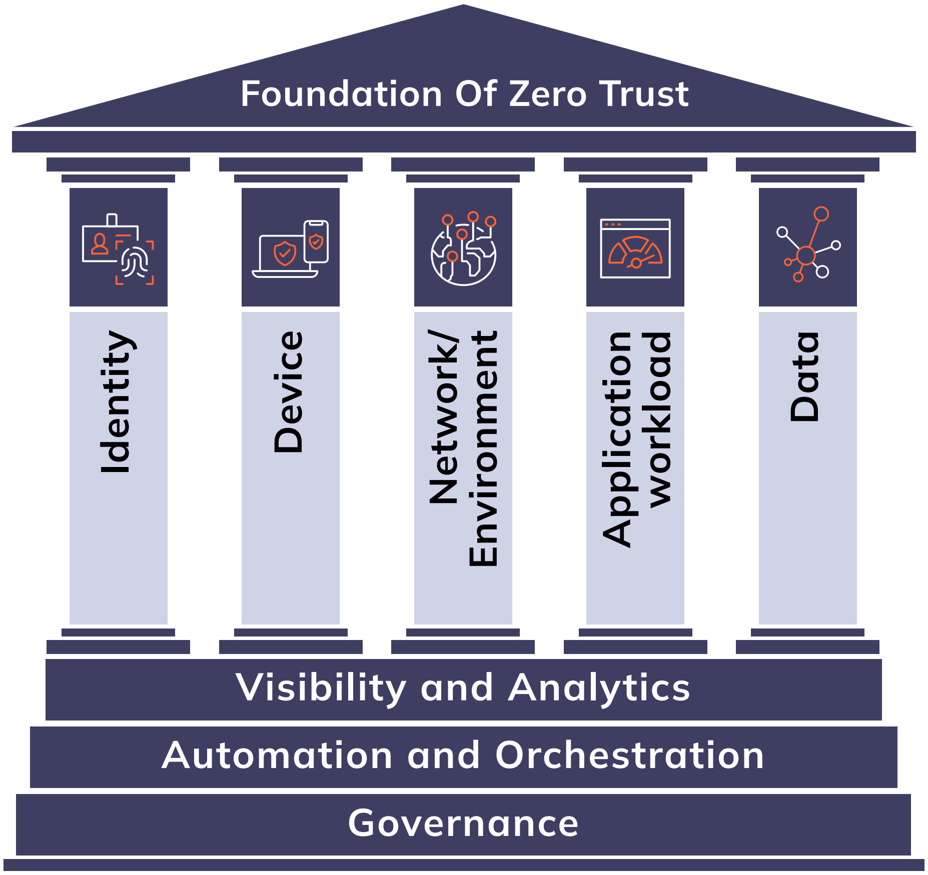

Figure 1: Foundation of Zero Trust

CISA's Zero Trust Maturity Model gives organizations a common framework and language to determine their Zero Trust maturity level, as well as give them clearcut areas to focus on in their ascent to Zero Trust Maturity. While the five pillars are clear in scope, figuring out how to achieve these goals is less obvious.

While many Zero Trust implementation guides focus on human identities, NIST states in **Special Publication 800-207: Zero Trust Architecture** that PKI (Public Key Infrastructure) is a indispensable component of Zero Trust security models. Given that the number of machine identities currently outnumber human identities at a rate of 45 to 1[1], it's evident why effective machine identity management is essential to every Zero Trust program.

Fortunately, Venafi's Trust Protection Platform covers key machine identity capabilities in each of the five pillars. The Venafi Platform can help you significantly advance the maturation of your Zero Trust security program and accelerate your organization's shift from No Trust to Zero Trust.

Venafi solutions cover key machine identity capabilities in each of the five pillars, helping you achieve your Zero Trust Maturity Model. What follows is a breakdown of these capabilities:

Pillar 1: Identity

Venafi manages the machine identities that allow machines to authenticate and communicate with one another. That includes managing the cryptography for access devices, such as Personal Identity Verification (PIV) cards and VPN tokens.

The Venafi Platform provides:

- Global visibility over your on-premise, hybrid cloud and cloud native environments
- A unified control plane that centralizes visibility and intelligence across your hybrid IT environment
- Complete lifecycle orchestration of machine identity modalities, including key and certificate management as well as tokenization
- The ability to automate end-to-end machine identity management, including thousands of proven integrations with load balancers, HSMs, DevOps tooling and a host of ecosystem partners
- Automated security controls to help you harden code signing security to protect you against malicious macros or attacks targeting software build pipelines

Pillar 2: Device

Venafi automates machine identities and secures declared infrastructure in the CI/CD pipeline, acting as a unifying tool that bridges traditional and modern device management.

The Venafi Platform provides:

- Continual monitoring and validation of the machine identity security postures of your devices
- Visibility into the types of machine identities your devices are using, such as certificates, keys and tokens
- Intelligence into the location, ownership and lifespans of your device machine identities
- Native support for integrations with other security solutions

Pillar 3: Network/Environment

Venafi helps you secure and automate machine-to-machine connections throughout your environment by managing TLS/mTLS, SSH, code signing and other protocols.

The Venafi Platform helps protect your organization's network by:

- Encrypting all machine-to-machine communication traffic to internal and external locations
- Automating alerts and triggers for expiring machine identities so that they may be replaced before they cause an outage
- Automating discovery of machine identities across networks, devices and services

Pillar 4: Application Workload

Venafi secures software development pipelines to ensure all code is legitimate and hasn't been infiltrated with malware.

The Venafi Platform provides:

- Access to centralized code signing authentication, authorization and monitoring
- Defined and enforceable enterprisewide code signing security policies, including those for application code, workflow enforcement and lifecycle orchestration
- Controls that restrict who has access to sign code, who can approve their use and when that approval expires
- Support for distributed, centralized and redundant HSM architectures
- An irrefutable log of all code signing activities for remediation and auditing purposes
- Crypto agility capabilities that quickly respond to Certificate Authority (CA) compromise or other cryptographic failures
- Machine speed for cloud environments where machine identities must be issued in seconds

Pillar 5: Data

Venafi helps your organization manage your cloud native machine identity inventory and secure your data in the cloud.

The Venafi Platform provides:

- Automated enforcement of strict machine identity access controls for machines holding valuable data
- Automated enforcement of machine-to-machine security controls for protecting your data as dictated by corporate policy and industry and government regulations

Conclusion

The journey to Zero Trust is not one-size-fits-all. While security teams recognize that Zero Trust security presents a significant improvement of traditional security models, figuring out where to start and how to develop a Zero Trust program that is right for your organization can be daunting.

Machine identity management is a great way to accelerate your Zero Trust journey; it is essential to achieving Zero Trust maturity while providing quick wins that measurably improve your risk posture.

If you are looking for help developing your Zero Trust machine identity roadmap, or if you want to accelerate your Zero Trust implementation strategies and plans, Venafi can help. We work with the largest, most security conscious organizations in the world to provide innovative machine identity management solutions that protect them from an ever-evolving threat landscape.

Evaluating the maturity of your Zero Trust initiatives? We can help. To learn more, visit **venafi.com**.

References

1. 2022 Identity Security Threat Landscape Report. CyberArk. 2022. 3-4.

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.**