WHITE PAPER

Unmasking the Hidden:

The Paramount Importance of Visibility in Securing Machine Identities & Neutralizing Threats in Kubernetes

Venafi®

Introduction

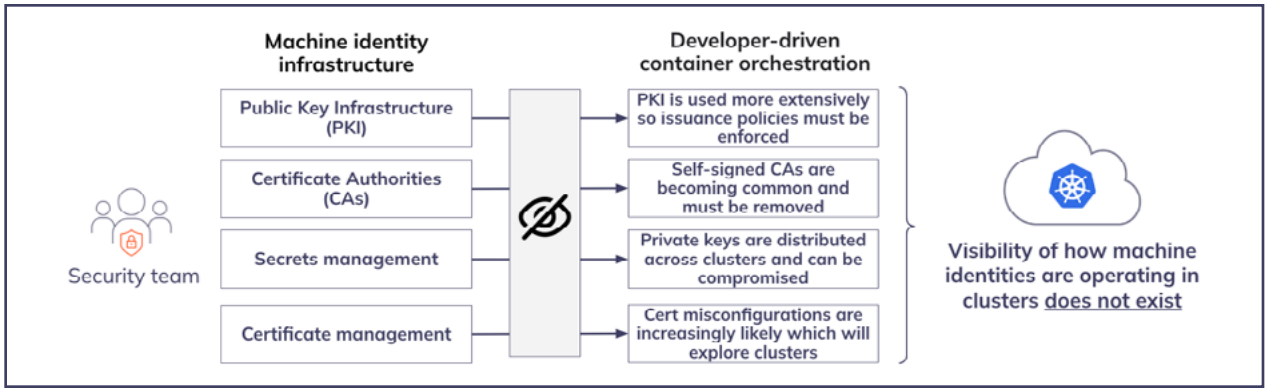
In an increasingly digital world, cybersecurity is of paramount importance, especially as organizations rapidly adopt Kubernetes for their application infrastructure. Venafi is a leading cybersecurity company that has established many groundbreaking partnerships with global enterprises to protect their machine identities and ensure secure communication within data center environments. Over the past three years, in particular, we have seen the vast majority of our customers accelerate their plans for Kubernetes cloud adoption and this is happening right across the board, across every industry sector. At the same time, we have seen the emergence of specific threat vectors that specifically target an organization's machine identity infrastructure. This brief is written to help cybersecurity teams understand and mitigate the principal factors that can lead to vulnerabilities being exposed in cloud native environments and delves into the critical need for visibility to safeguard machine identities and mitigate threats to applications hosted in Kubernetes clusters.

Navigating the Security Minefield in Kubernetes

Widespread Kubernetes adoption has created an open playing field for increased security risks, necessitating vigilance from Infosec teams. There are many examples from recent security research projects which report the increasing incidence of vulnerabilities and threats faced by applications hosted on Kubernetes. The key challenges for InfoSec teams is to know which aspects of Kubernetes threat prevention they should focus on as a priority and which commercial partnerships are best placed to help them manage and mitigate these threats. This paper will show how committing budget expenditure to threat prevention for machine identity infrastructure in Kubernetes will help organizations see immediate improvements in their cybersecurity operation. The premise for this is very straightforward: security teams do not have the critical visibility needed to stop particular types of threats from attacking their machine identity infrastructure in Kubernetes environments. These attacks leverage vulnerabilities that are currently not visible to security teams and can compromise internal development processes in order to issue rogue digital certificates and steal private keys to access Kubernetes clusters.

The Blind Spots: Machine Identities in Kubernetes

The security landscape in Kubernetes differs significantly from that of traditional data center environments. Developer-driven orchestration often does not include input from security teams and thus challenges their ability to enforce policies and deliver proper security measures. As a result, security teams lack the visibility and control over machine identities in Kubernetes that they enjoy in data center environments.



A well-managed machine identity infrastructure is critical for protecting application workloads, containers, pods, clusters in Kubernetes. Critical to the success of this infrastructure is the ability to ensure that only validated enterprise PKI is used to enforce TLS encryption for application workloads; only authorized and trusted Certificate Authorities (CAs) can issue certificates for developer teams; all private keys or secrets are properly secured, rotated and protected; and if using a service mesh, that all mesh workloads are observable and using mTLS encryption. Without full visibility of all machine identity activity across all workload contexts, vulnerabilities are certain to appear.

Visibility in Action: Machine Identity Threat Scenarios

The disparity between traditional data center security and Kubernetes security lies in the visibility and control security teams can apply to each. In Kubernetes, certificates are issued at significantly higher volumes, making auditing and monitoring challenging for security teams. This lack of visibility into machine identities in Kubernetes exposes organizations to severe security breaches. Visibility is the first step to preventing security threats. But what are the security threats that are unique to Kubernetes, why are they especially relevant for machine identities, and how can they be prevented from exploiting the application data within clusters?

The following three critical threat scenarios underscore the importance of visibility and how machine identities can be compromised to allow cybercriminals to access application data.

Protect every public ingress endpoint across multiple Kubernetes clusters	**Denial of service in a business critical application** A policy violation in the way a certificate has been issued has exposed the cluster to the outside world.
Stop rogue CAs operating within production infrastructure using self-signed certificates	**Elevation of privilege** Compromised machine identities are issued using a rogue trust root to move within and between clusters.
Prevent man-in-the-middle attacks from capturing private keys in a service mesh	**Intercept or spoofed data communication** Private keys captured and secrets intercepted so trust has been compromised across the complete mesh solution.

Venafi Expertise in Machine Identity Management

Venafi is an established and trusted cybersecurity company and has partnered with security teams across the Global 5000 sector. Our TLS Protect solution has been instrumental in securing machine identities in data center environments for well over a decade. And now in cloud native environments, machine identities, including digital certificates and cryptographic keys, serve as the foundation of secure communication within Kubernetes clusters. Ensuring the authenticity and confidentiality of these identities and how they are mapped to application workloads is crucial to maintaining a robust and modern security posture. Kubernetes adoption has surged across virtually all industries, creating both opportunities and

challenges. We recognize the new urgency to protect machine identities in the Kubernetes environment. Venafi is the creator and principal maintainer of the cert-manager open source project which is the cloud native ecosystem's de facto solution for Kubernetes machine identity management. As the cybersecurity landscape evolves, the unique nature of Kubernetes will demand a fresh perspective on security practices and Venafi is committed to helping our customers adapt and confront these new challenges.

Visibility of Critical Machine Identity Data

In the age of cloud and Kubernetes, cyber threats continuously evolve, it has become increasingly attractive for cybercriminals to target machine identities for exploitation. To mitigate this rapidly growing vulnerability, security teams need visibility of machine identities in Kubernetes clusters is to enforce security policies, minimize the opportunities for rogue behavior and thwart potential threats.

Real-time Information and Rapid Response

Real-time information on machine identity status empowers security teams to respond swiftly to policy violations and potential threats. Centralized control over certificate issuance ensures consistency and prevents vulnerabilities from unauthorized practices such as unauthorized self-signed CAs being created and used in clusters.

Integration with Venafi TLS Protect

Venafi TLS Protect for Kubernetes seamlessly integrates with the existing Venafi TLS Protect solution for data center and cloud instances, extending globally consistent security policies to Kubernetes environments. A centralized approach adapts enterprise wide security policies for Kubernetes workloads, correlating machine identities with specific workloads.

The NIST Cybersecurity Framework for Mitigation Controls

Venafi TLS Protect for Kubernetes aligns with the NIST Cybersecurity Framework, a structured approach to managing and improving cybersecurity processes. Applying this framework ensures that machine identity infrastructure is well-equipped to prevent specific threat vectors.

NIST CYBERSECURITY FRAMEWORK	Prevent threat vectors with malicious intent	Stop unintentional outages and vulnerabilities from shadow IT
Identify	Ensure observability of all machine identities and their workload context.	Locate self-signed CAs and assess the potential risk and associated threats.
Protect	Enforce centralized issuance policy for cert-manager configurations.	Use "secretless" authentication for developer team access to cert-manager
Detect	Alert on discovery of misused certs (wrong address space, etc).	Alert suspicious activity for cert verification failures or unvalidated CAs.
Recover	Automatically revoke and reissue misconfigured certificates.	Remove unvalidated self-signed CAs and replace with trusted certificates.
Respond	Implement developer guardrails and improve security audit process.	Identify all critical infrastructure and restore services with new certificates.

The NIST Framework aids organizations in identifying and mitigating security gaps. Key questions related to machine identity security help gauge an organization's vulnerability to attacks targeting Kubernetes:

By mapping Venafi TLS Protect for Kubernetes to the NIST Framework, organizations can ensure mitigation controls are in place to counter the cyber threats that target machine identities to gain unauthorized access to the cluster. In addition, the framework can help security teams build protection from unintentional threats, such as the inadvertent use of insecure self-signed CAs by developer teams.

Conclusion and Collaboration

In the face of evolving cyber threats, securing machine identities in Kubernetes is paramount. Venafi TLS Protect for Kubernetes offers a comprehensive solution, aligning with the NIST Cybersecurity Framework to ensure robust protection. Collaboration between Venafi and your security team can empower your organization to anticipate and mitigate threats effectively, safeguarding your Kubernetes environments.

To explore the unique security solution provided by Venafi TLS Protect for Kubernetes, and to enhance your security operation, we invite you to engage with our team. Together, we can ensure critical visibility of machine identities and bolster your defense against cybersecurity attacks in Kubernetes.

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.**