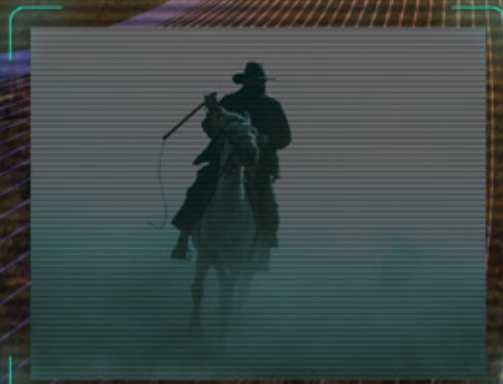
Venafi

FOR INFOSEC PROFESSIONALS

HOW TO TAME THE KUBERNETES WILD WEST

In the dusty, normally quiet town of Container Gulch, a gang of certificate outlaws is wreaking havoc in this once peaceful Kubernetes territory.

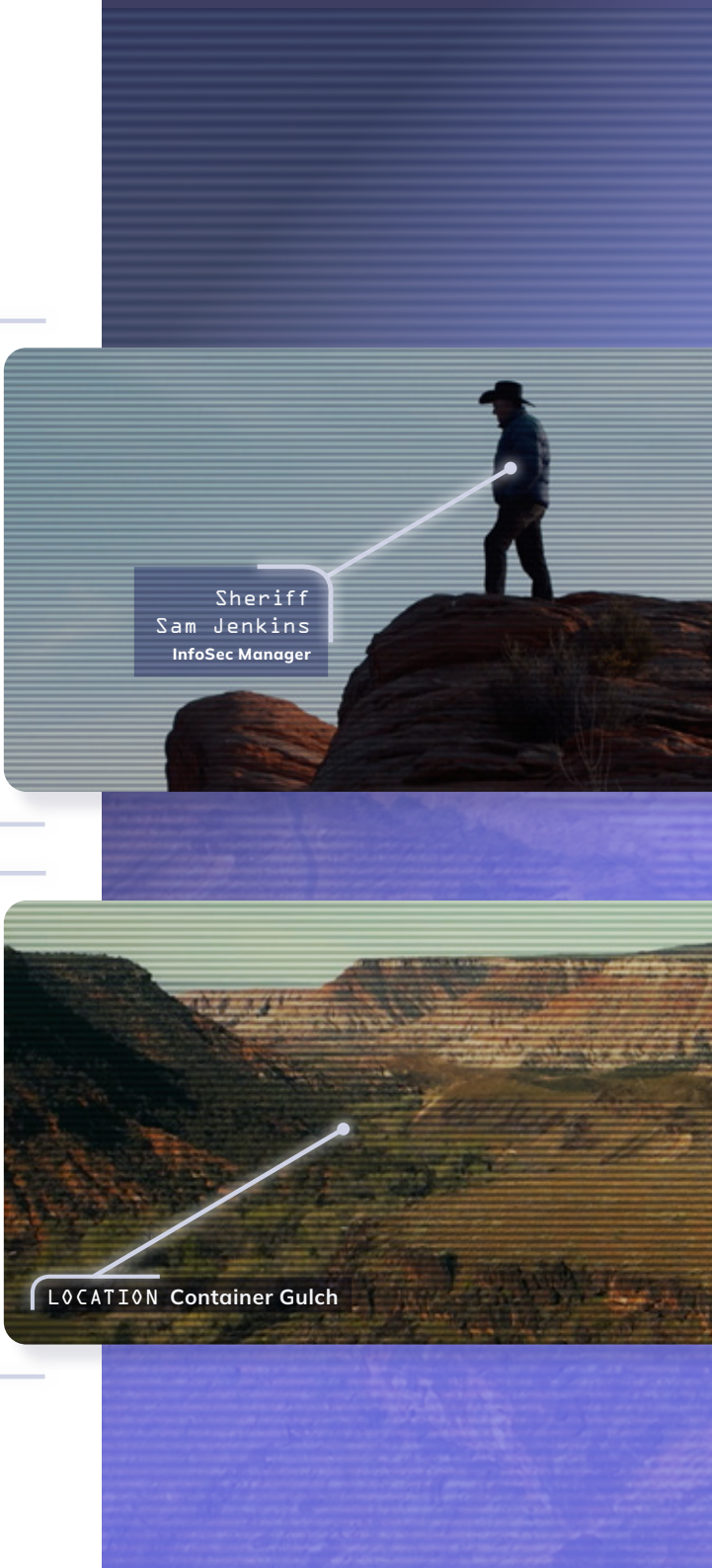


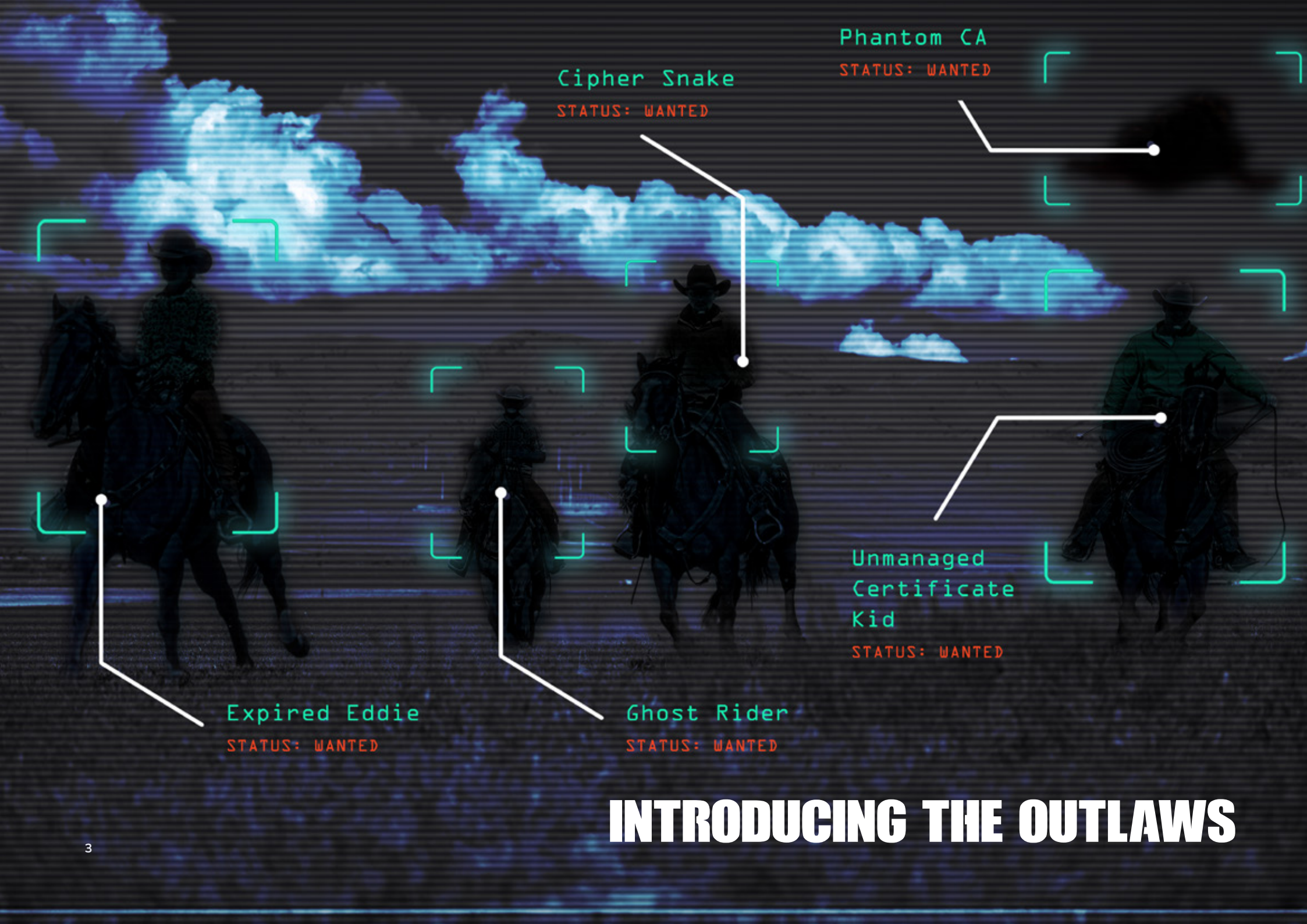
INTRODUCTION

Welcome to the container security backcountry where the TLS certificate management frontier is plagued by a notorious gang of certificate outlaws.

Follow Sheriff Sam Jenkins, InfoSec Manager, as he navigates treacherous encryption terrain across vast digital plains to apprehend these renegades and secure your Kubernetes frontier.

Join us in the heart of Kubernetes security, where only the vigilant prevail. Saddle up for an educational journey through the challenges of certificate management in the Wild West of Kubernetes.





INTRODUCING THE OUTLAWS

Weapon of Choice:

Unmanaged Certificates

Crimes:

Denial of service in a business-critical application.

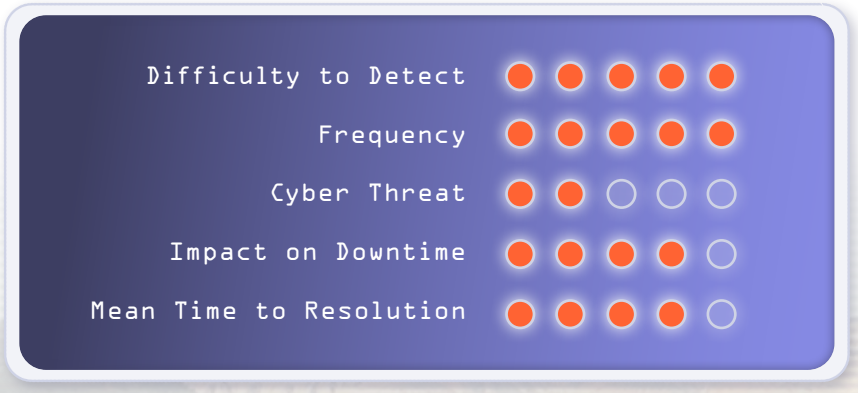
Service could be inaccessible due to an untrusted certificate.

UNMANAGED CERTIFICATE KID

In the heart of the Wild Code West, there was a lone outlaw known as the Unmanaged Certificate Kid. This self-signed scoundrel roamed the clusters, untrusted and non-compliant. Sheriff Sam knew he had to track down this renegade before chaos ensued. With a wanted poster in hand, he rode through the container canyons, determined to bring the Unmanaged Certificate Kid to justice.

CERTIFICATE VIOLATIONS

- Self-Signed
- Unmanaged
- Non-Compliant



Weapon of Choice:

Unmanaged SubCA

Crimes:

Elevation of privilege

Denial of service in a business-critical application

Decrypting captured traffic and intercepting encrypted communications

PHANTOM CA

In the shadowy corners of Kubernetes City, a mysterious figure known only as the Phantom CA operated in the dark alleys of non-compliant PKI. Sheriff Sam, a seasoned tracker, followed the elusive trail of the Phantom CA, knowing that unvalidated Certificate Authorities could bring the entire security infrastructure to its knees. The hunt for the Phantom CA led Sheriff Sam through the tangled web of certificates and keys, determined to restore order to his town.

CERTIFICATE VIOLATIONS

Non-Compliant PKI

Unvalidated Subordinate CA

Weapon of Choice:

Weak Encryption

Crimes:

Denial of service in a business-critical application

Decrypting captured traffic if cypher suite used is weak

Intercepting encrypted communications

CIPHER SNAKE

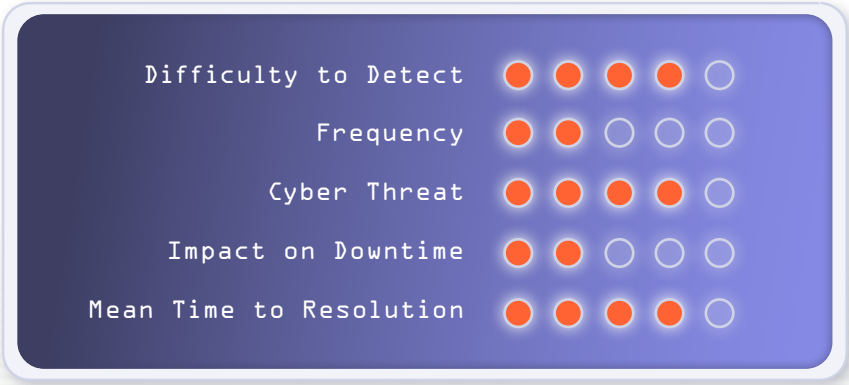
In the treacherous encryption foothills, a slithering outlaw known as Cipher Snake was causing trouble. This certificate criminal had weak ciphers, making him an easy target for malicious hackers. Sheriff Sam, with his trusty code revolver, set out to round up Cipher Snake before the vulnerabilities in the clusters could be exploited.

CERTIFICATE VIOLATIONS

Weak Encryption Standards

Easy to Hack

Non-Compliant



Weapon of Choice:

Unused Certificates

Crimes:

Spoofing application to disclose or compromise

Elevation of privilege

Denial of service in a business-critical application

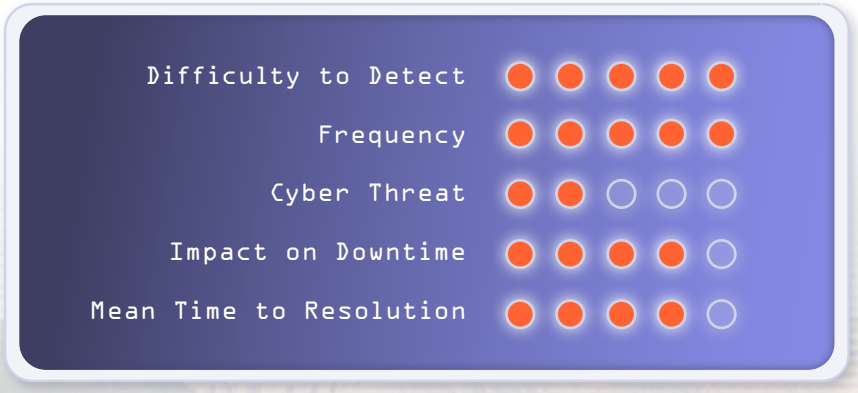
GHOST RIDER

In the vast, shadowy expanse of Kubernetes territory, a spectral presence roamed unchecked—dubbed the Ghost Rider. Not tethered to any ingress resource, this active, yet unassigned, certificate drifted like a phantom through the digital plains, a remnant of configurations past. Sheriff Sam Jenkins, ever vigilant, felt the chill of this ghostly rider's passage. Knowing well the dangers and security risks that such unused certificates posed—a hidden doorway for unwelcome visitors—he pledged to track down and exorcise this digital specter.

CERTIFICATE VIOLATIONS

No Associated Resources

Valid But Unused



Weapon of Choice:

Overly Long Expiration Dates

Crimes:

Denial of service due to longer window for attack vectors

Ability to intercept encrypted communications using compromised certificates

EXPIRED EDDIE

Out on the outskirts of Kubernetes County, there was a notorious time bandit named Expired Eddie. This certificate criminal boasted long expiry periods, making him unsafe for the entire town. Sheriff Sam, always vigilant, knew that if he didn't apprehend Eddie soon, the entire cluster would be in jeopardy of a certificate outage. The clock was ticking as Sheriff Sam pursued the time bandit across the vast Kubernetes landscape.

CERTIFICATE VIOLATIONS

Certificates With Long Expiration

Non-Compliant

CAPTURING THE OUTLAWS

By offering oversight and control over certificate issuance and policies in clusters, TLS Protect for Kubernetes ensures that none of these Outlaws can wreak havoc in Container Gulch any longer.

Unmanaged Certificate Kid

- Filters issuer types through the Venafi Control Plane to identify unmanaged certificates
- Flags self-signed certificates with warnings to highlight security risks

Phantom CA

- Eliminate unvalidated subordinate CA risks and check they are signed using only compliant PKI
- Removes unauthorized CAs so only compliant certificates are issued in clusters

Cypher Snake

- Mitigates weak encryption risks by filtering certificates based on key size to spot encryption anomalies
- Identifies and upgrades certificates with insufficient encryption to meet the correct security criteria

Ghost Rider

- Enhanced certificate discoverability to flag unused certificates
- Easily retire or delete unused certificates, bolstering cluster security

Expired Eddie

- Filter for certificates expiring after three months to prevent threats from certificates with long validity periods
- Sets issuance policies with appropriate validity, ensuring certificates match workload types

TLS Protect for Kubernetes

Acting as a vigilant sheriff in every cluster, TLS Protect for Kubernetes empowers security teams to detect certificate issues, so that they can ensure every workload runs true and trusted.

And we know that developers, akin to pioneering settlers, rapidly deploy web-facing and internal workloads with TLS and mTLS certificates quicker than a gunslinger's draw. However, with speed comes risk. When you hitch your clusters to TLS Protect for Kubernetes, it will keep a watchful eye and secure your certificates, allowing developers to focus on innovation without sweating over security.

In-Cluster Visibility

Guarantees the security and effective management of all certificates through live, in-cluster monitoring.

Automate Certificate Management

Automates TLS/mTLS management to securely issue certificates, minimize errors, and maintain up-to-date, compliant certificates.

Enforce Policy and Compliance

Enforces certificate policies within Kubernetes clusters to adhere to compliance, trust, and security standards.

Identify and Remediate Misconfigurations

Detects and rectifies misconfigured certificates, preventing vulnerabilities and potential attacker exploitation.

Multi-Cluster Management

Simplifies multi-cluster Kubernetes certificate management to ensure consistent security and mitigate the risk of drift.

Developer-Friendly Security Guardrails

Integrates security seamlessly into developer workflows, enabling secure, compliant, and efficient deployments.

Reliable, scalable and flexible machine identity management for your Kubernetes workloads.

"I love how TLS Protect for Kubernetes automates the configuration and management processes, eliminating human error. And it includes a first-class support package, which helps ensure we meet our platform uptime SLA."

Vice President of Security, Global Bank

Venafi
TLS Protect for Kubernetes

Find out more

Venafi

Venafi is the cybersecurity market leader in machine identity management, 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 venafi.com**