CASE STUDY · VENAFI · CYBERARK ECOSYSTEM · PKI MODERNIZATION

Accelerating a Mature PKI Practice: From On-Premises PKI to Automated Containerized PKI

How Accutive Security partnered with a large enterprise to advance a sophisticated PKI practice from on-premises Venafi TPP to a cloud-hosted, automated certificate management platform, training 130+ operators and maintaining full operational continuity throughout.

PRE-ENGAGEMENT CLIENT SNAPSHOT

PROFILE	ENVIRONMENT	PLATFORM OPERATORS
Large financial services enterprise	Venafi TPP (on-premises), Microsoft ADCS, Sectigo and DigiCert as external CAs, AWS-hosted workloads	130+
ENGAGEMENT SCOPE	**PARTNER**	
Four stages: Health check → TLSPC migration → Platform expansion → Container-native automation	Accutive Security — certified delivery expertise in the Venafi / CyberArk ecosystem	

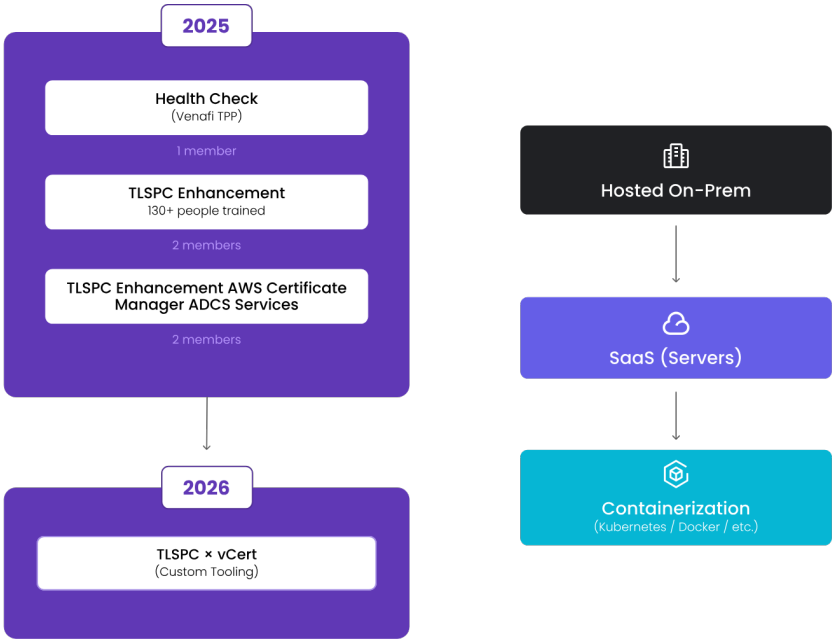
When a Production PKI Environment Outgrows Its Platform

The migration path for enterprise PKI is well established in principle. Organizations running on-premises certificate management platforms are moving to cloud-hosted machine identity platforms, extending coverage for cloud workloads in multi-CA environments, and advancing toward containerized certificate automation. What that migration looks like in practice, particularly for organizations that already operate a sophisticated, production-grade PKI environment, is less frequently documented.

The client, a large financial services organization, was not starting its PKI journey. It was operating Venafi Trust Protection Platform (TPP) across a multi-CA environment, with Microsoft ADCS and DigiCert as active CAs, AWS workloads issuing internally-trusted certificates, and over 130 trained operators managing the platform. Over time, however, the mature TPP operation had drifted out of currency and needed to

modernize without disruption.

Given the client's existing sophistication, the goal of Accutive Security's engagement was not the typical remediation or rescue operation. Rather, it was to accelerate a mature PKI practice past the limits of its existing platform and into a cloud-delivered, multi-CA, container-aware architecture, without disrupting existing operations. Accutive Security engaged across four sequential stages to deliver that outcome.



The engagement timeline alongside the industry PKI migration arc: hosted on-premises → SaaS → containerization (Kubernetes / Docker).

STEP 1

Health Check

Mapping Platform Currency Against Infrastructure Demand

When Accutive Security began its engagement with the client, their PKI environment was already mature, reflecting years of deliberate investment. However, the TPP instance had fallen behind its supported version path, a gap with cascading operational consequences:

- The outdated version blocked access to newer platform integrations.
- Known security patches remained unapplied.
- Network discovery jobs had not kept pace with infrastructure changes, creating coverage gaps that produced missed certificate renewals.
- Validation policy enforcement was inconsistent across the platform hierarchy. Some certificates carried no validation policy, while AWS certificates issued through the internal Microsoft CA were failing validation because TPP could not reach the remote endpoint.
- License utilization was diluted by accumulated inventory clutter, obscuring the platform's true operational scope.
- The PKI function put enterprise-scale risk on a single engineer.

An assigned Accutive Security engineer conducted a structured technical review spanning CA configurations, discovery job coverage, certificate validation policies, AWS certificate integration status, license utilization, and platform resilience. This analysis produced a sequenced remediation roadmap, prioritizing immediate stabilization actions first and automation maturity improvements later.

- **Immediate priorities addressed the most consequential gaps:** resolving the version currency issue, restructuring network discovery scans to eliminate scheduling overlap, troubleshooting CA import job failures affecting the Microsoft CA, and establishing platform-wide validation policies.
- **Medium-term priorities** covered trusted root imports, AWS certificate validation remediation, policy-driven renewal automation, and certificate ownership governance.

The client executed against this sequence. The stabilization work that followed created the clean operational baseline on which the TLSPC migration was built.

IMMEDIATE-PRIORITY FINDINGS	
Upgrade Venafi TPP version or migrate to SaaS platform	Restore extended support and security patching against active threat vectors
Run segmented network discovery scans	Improve operational efficiency by scheduling discovery during off-hours and avoiding scan overlap into business hours
Troubleshoot CA import jobs targeting Microsoft CA	Restore visibility, accurately reflect infrastructure consumption, and support comprehensive outage reporting
Establish platform-wide validation policies	Enable consistent discernment between trusted and untrusted certificates across the parent policy

STEP 2

Migration to TLS Protect Cloud

Transitioning 130+ Users to a Cloud-Hosted Platform

With the health check findings addressed and a stable platform baseline established, Accutive Security led the full migration from on-premises Venafi TPP to TLS Protect Cloud (TLSPC). The client had already licensed TLSPC but had not yet deployed it. Two engineers managed the implementation end-to-end, covering architecture design, platform configuration, CA integration, and go-live transition.

The migration moved the platform off a more maintenance-intensive on-premises footprint and onto a cloud-delivered platform, with enhanced visibility and automation potential.

At the conclusion of the implementation, Accutive Security delivered formal handoff training to more than 130 users. The platform was now cloud-managed, fully supported, and positioned to support the integration and automation work that would follow.

STEP 3

Platform Expansion

AWS Certificate Manager Integration, ADCS Automation, and Machine Identity Visibility

With TLSPC operational as the centralized identity security platform, the next phase extended the platform's scope across the client's infrastructure. Two engineers led a set of integrations that materially deepened machine identity coverage.

- The first integration connected AWS Certificate Manager to the TLSPC control plane, enabling cloud-native certificate issuance for AWS workloads under a centrally managed policy layer.
- The second extended the engagement beyond pure CLM into the client's Microsoft PKI operations. Accutive Security deployed new SCEP servers for ADCS and integrated them into the TLSPC fabric.

The client retains and operates ADCS in-house; Accutive Security's contribution was automating it through the SCEP layer and bringing it under consistent, policy-driven certificate management for the first time. With the integrations in place, two automation capabilities were activated that directly reduce the operational burden on the client's PKI team.

- **Certificate auto-renewal,** configured through TLSPC's automation engine, handles the renewal cycle for certificates across the environment without manual intervention, eliminating the per-certificate renewal work that had previously placed significant overhead on limited resources.
- **Push provisioning** extends this automation to the delivery layer: when a certificate is renewed, the platform automatically installs it to the target endpoint, whether NGINX, IIS, Apache, F5, or another integrated platform, without requiring manual deployment.
- **vCert-based pull provisioning,** introduced alongside push provisioning, is a complementary automation model in which workloads and applications request their own certificates on demand, rather than receiving them through centrally coordinated push delivery. Pull provisioning is well-suited to environments where certificate consumers are dynamic or distributed, and it forms the technical foundation on which the containerized automation is built.

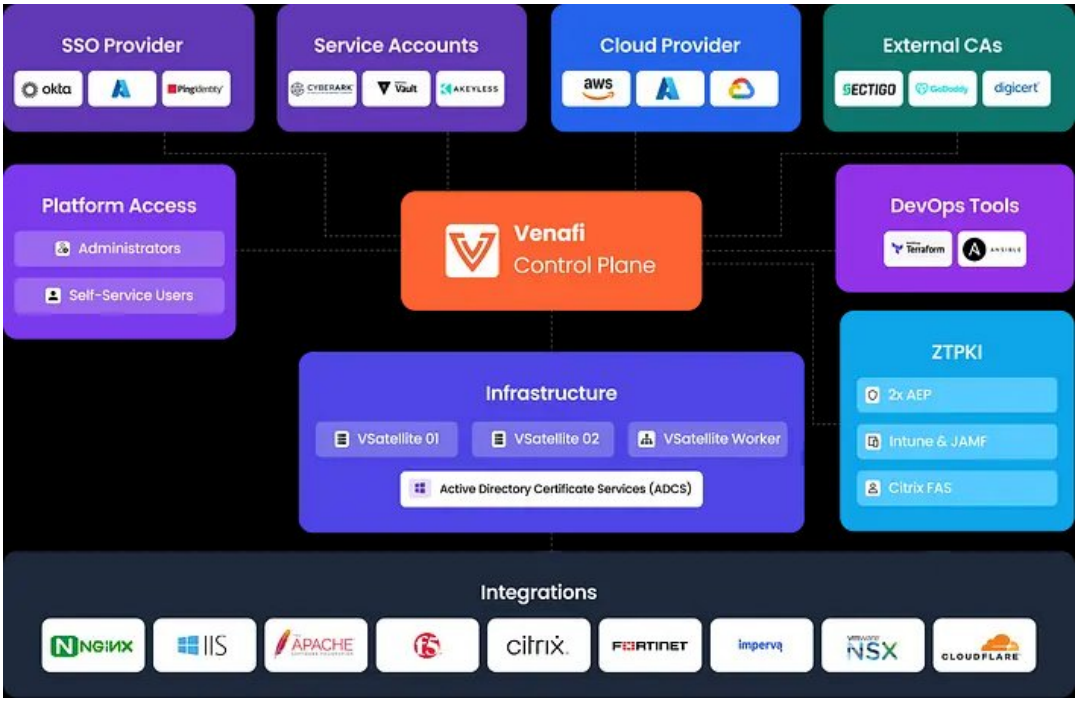
TLSPC also provides outage reporting, surfacing certificates approaching expiry, validation failures, and installation errors before they cause service disruptions. With the full certificate inventory now visible and validation policies consistently enforced across the hierarchy, these alerts reflect the actual state of the environment, giving the team accurate, actionable intelligence for outage prevention rather than reactive incident response.

The Result: An End-to-End Machine Identity Architecture

These integrations moved the client's machine identity program from a certificate management deployment to a unified machine identity fabric: one control plane governing issuance, policy, and lifecycle across both cloud and on-premises infrastructure.

The architecture now spans the full scope of the client's machine identity environment. The Venafi Control Plane (now known as Palo Alto Networks' Next Generation Trust Security) serves as the operational center, integrating across three cloud providers (AWS, Azure, and Google Cloud), three external CAs (Sectigo, DigiCert, and the internal Microsoft CA), and three SSO providers (Okta, Microsoft Entra, and Ping Identity). Service account and secrets platforms (CyberArk, HashiCorp Vault, and Akeyless) connect to the control plane for coordinated machine identity governance. DevOps tooling integrations span vCert, Terraform, and Ansible.

Two VSatellites and a VSatellite Worker bridge the control plane into Active Directory Certificate Services (ADCS). Coverage extends to two AEP infrastructure instances, Intune, JAMF, and Citrix FAS. Endpoint and platform integrations include NGINX, IIS, Apache, Citrix, Fortinet, VMware NSX, F5, Imperva, and Cloudflare. The result is an enterprise-scale machine identity fabric, not a point deployment.



The Venafi Control Plane architecture: SSO providers, service accounts, cloud providers, external CAs, DevOps tooling, VSatellite infrastructure, ZTPKI coverage, and endpoint integrations governed from a single control plane.

STEP 4

Container-Native PKI

Bringing Certificate Automation into Kubernetes Environments

The fourth phase undertook the development of a custom solution, a containerized vCert proof-of-concept, that extends certificate lifecycle management natively into Kubernetes environments. The solution uses sidecar containers to automate certificate provisioning, renewal, and rotation at the workload level, eliminating manual coordination from certificate processes in environments where containers are ephemeral and deployment cycles are continuous.

The on-premises → cloud → containerized PKI arc is the path that mature enterprises across every sector are now beginning to walk. While most are still at the planning stage, this organization is already at the leading edge.

Business Outcomes: What the Four-Stage Engagement Delivered

The PKI modernization program produced crucial outcomes that directly improve how the organization manages machine identity at enterprise scale.

Full visibility into all non-human identities

The client now has an accurate, consolidated view of every certificate in its environment across multiple CAs, cloud providers, and on-premises infrastructure through a centralized identity security platform. AWS-hosted certificates that had previously sat outside validated scope are now included. Outage reporting surfaces expiring and invalid certificates before they cause service disruptions, giving the security team actionable intelligence rather than reactive incident response. And as containerized workload coverage advances, that visibility will extend to Kubernetes workload identities as well.

Automated renewal ahead of the 47-day certificate lifecycle

Certificate renewals across the environment are now handled automatically through auto-renewal and push provisioning without manual intervention. This reduces the operational burden ahead of shrinking TLS certificate lifecycles (100 days in 2027 and 47 days by 2029). The automation foundation also supports the firm's preparation for post-quantum cryptography migration.

A foundation for secure, scalable containerized workloads

With pull provisioning introduced through vCert and the containerized proof-of-concept advancing, the client is positioned to extend the same certificate governance that covers its broader environment into Kubernetes workloads. This enables mutual TLS between services, zero-trust access controls at the workload level, and certificate issuance that keeps pace with deployment pipeline velocity.

Consistent certificate validation across the full environment

Certificate validation failures that had persisted across the platform are resolved, and policy enforcement is now applied uniformly across every certificate in the hierarchy. With consistent, policy-driven certificate management, the client is better positioned to govern issuance, policy, and lifecycle across both cloud and on-premises infrastructure.

What This Engagement Demonstrates About PKI Modernization at Enterprise Scale

The four-stage journey documented here reflects both the operational complexity of enterprise PKI modernization and the type of partner engagement that makes it achievable. Each stage built directly on the one before it:

- A structured health check that produced a sequenced remediation roadmap.
- A migration that created a cloud control plane while preserving operational continuity.
- A platform expansion that deepened both automation coverage and CA governance.
- A containerization initiative that brought certificate automation to the infrastructure layer where modern applications live.

Accutive Security delivers across all four stages, not as a handoff model where different teams own different phases, but as a continuous partner relationship built on certified delivery expertise in the Venafi/CyberArk ecosystem.

ACCUTIVE SECURITY

The Cryptography, Data Protection and Identity Security Center of Excellence

Explore what a phased PKI modernization engagement looks like for your environment.

Consult a PKI expert · accutivesecurity.com/contact-us · letstalk@accutive.com · +1.888.666.8315

CORPORATE MAILING ADDRESS

27068 La Paz Road, Suite 245
Aliso Viejo, CA 92656

ACCUTIVE SECURITY CANADA

2912 W Broadway, Suite 131
Vancouver, BC V6K 2G8

letstalk@accutive.com · +1.888.666.8315 · accutivesecurity.com