

CASE STUDY

From On-Prem TPP to the Cloud in Two Weeks

A Machine Identity Modernization Case Study

INDUSTRY

Healthcare supply and logistics

REGION

U.S. Central

ANNUAL REVENUE

\$1B to \$10B

PLATFORM

Venafi TPP to cloud control plane

~2 wks

POC duration, end to end

4

Integrations delivered in POC

3 of 4

Integrations completed on first attempt

~50%

F5 certificate footprint reduced

At a Glance

OUTCOME	RESULT
POC duration	Approximately two weeks, end to end
Integrations delivered in POC	4 (IIS, F5, Okta, Azure Cloud and Azure Key Vault)
Integrations completed on first attempt	3 of 4 first-try, 4th's blockers resolved in-lab
Competing CLM POC status at completion	Still in an earlier phase after roughly 1.5 to 2 months
F5 certificate footprint reduced	~50% (approximately 800 certificates down to 400)
Compliance logging	Custom Splunk forwarding for all platform logs
Current engagement model	Embedded Hypercare team with badged access

01

Client Background

The client, with annual revenue in the \$1B to \$10B range, is a healthcare supply and logistics organization operating in the U.S. Central Region. Certificate operations sit directly in the path of clinical and distribution systems, so availability and auditability are not negotiable.

The client had been running [Venafi Trust Protection Platform](#) on premises for years. The platform worked, but the operating model had become the problem. Daily administration of TPP consumed a disproportionate amount of the team's time. The upgrades were manual and disruptive, and module based licensing for Trust Authority and TrustForce made the cost of expanding coverage difficult to justify.

Migrating to the cloud control plane addressed all four concerns at once: unlimited certificate discovery, a more predictable cost-effective profile, no more hands-on upgrade cycles, and continued product investment from the vendor.

The client was also parallelly evaluating a [competing CLM vendor](#), with that proof of concept (POC) already underway when Accutiv Security was brought in.

02

Why the Client Changed Partners

While the client's previous implementation partner was capable on paper, they did not bring the technical depth the team needed once the work moved past planning. In the client's own framing, they were looking for hands-on engineering expertise rather than paper pushers.

Hands-on engineering expertise rather than paper pushers.

WHAT THE CLIENT WAS LOOKING FOR IN A PARTNER

That was the clinching factor. A cloud migration of a machine identity platform touches Active Directory, load balancers, cloud key stores, identity providers, and every application team that consumes a certificate. It needs people who successfully built those integrations prior and who can troubleshoot them without escalating every question back to the vendor.

Machine Identity Health Check

Accutiv Security opened the engagement with a [machine identity health check](#) rather than skipping to implementation. The assessment reviewed the existing TPP estate, discovery coverage, integration inventory, access model, and operational practices.

The health check surfaced a set of concrete challenging opportunities across three areas: strengthening the security posture of the machine identity stack, improving platform adoption among certificate owners, and closing operational gaps that had been absorbing the team’s time. Those findings became the input to the POC scope, so the team tested the things that actually mattered to the client rather than a generic feature checklist.

POC Scope and Architecture

The POC phase ran for approximately two weeks and covered four integrations within a single Active Directory domain:

Microsoft IIS Machine integration for certificate discovery and provisioning	F5 Machine integration for discovery and provisioning
Okta SSO provider, enabling MFA for platform access and role-based access control scoped to certificate owners	Azure Cloud and Azure Key Vault Discovery of existing keys and certificates and provisioning of new ones

Supporting infrastructure included two vSatellites and a vSatellite worker (the worker component has since been deprecated in the platform). The control plane was connected to a public certificate authority for externally facing certificates and to Microsoft Active Directory Certificate Services (ADCS) for internal issuance and automation.

Administrative configuration was part of the same two-week window: scheduled expiration reporting, alerting, and approval rules that trigger manual review for specific certificate templates and applications. The POC closed with a knowledge transfer session so the client’s team could operate what had been built.

POC Results

Three of the four integrations, Okta, F5, and Azure Key Vault, along with the public CA connection, were completed on the first attempt with no obstacles.

The IIS integration was the exception. The team hit two product level defects rather than configuration or knowledge gaps. Instead of running discovery live with the client, Accutiv Security reproduced the client's environment in its innovation lab. The team then isolated the behavior, identified a viable workaround, and implemented the most secure available path. The client saw a working integration, not a troubleshooting session.

FOR CONTEXT ON PACE

The competing CLM vendor's POC had been running for approximately 1.5 to 2 months before the Venafi POC started, and was still working through an earlier phase of its own agent deployment when the Venafi POC finished. Both vendors were solving real problems in a complex environment. The difference the client pointed to was preparation, specifically that integrations had been validated in a lab before they were attempted in production.

The Innovation Lab Advantage

Accutiv Security maintains an [Innovation Lab](#) that mirrors common enterprise machine identity stacks. Every integration and endpoint in this engagement cycle was pre-tested there before a client facing session was scheduled.

The practical value showed up twice. First, it compressed the POC timeline, because the team already knew how each integration behaved before touching the client's environment. Second, when the IIS defects surfaced, the lab became the place to replicate the client's exact configuration and work the problem, which kept the client's engineers out of open-ended live debugging.

The broader point applies to any CLM deployment: hands-on validation in a representative environment beats reliance on vendor documentation or architectural theory. While documentation describes the intended path only, a lab brings the idea to life.

Hypercare Outcomes

The engagement cycle did not end at go-live. Accutive Security's team has been badged into the client with company email identities and direct platform access, operating as an [embedded extension of the client's machine identity function](#) rather than an outside vendor filing tickets.

Outcomes delivered during Accutive Security Hypercare to date:

- **Cloud migration of key TPP capabilities.**
Core features the client relied on in on-prem TPP now run in the cloud Control Plane.
- **F5 integration optimization with a ~50% license reduction.**
Rationalizing certificate usage across F5 brought the certificate count down from roughly 800 to 400, with a corresponding reduction in F5 license consumption.
- **Custom Splunk integration for compliance.**
All platform logs are forwarded to Splunk, supporting the audit and retention expectations that apply in healthcare and financial services environments.
- **Kubernetes cert-manager deployment.**
Certificate issuance and deployment now extend into the client's [Kubernetes workloads](#), completed most recently in the engagement.
- **Expanded team enablement.**
Additional client team members have been trained on the platform, widening internal ownership beyond the original administrators.

Support escalation is part of the model as well. When a vendor support request is needed, Accutive Security helps draft it and escalates through [direct vendor relationships](#), which keeps the client out of standard support queues on time sensitive issues.

Identified Future Opportunity

The client currently issues internal certificates through ADCS and has not yet moved to a [hosted PKI model](#). Migrating internal issuance to ZTPKI is an identified next step within the Hypercare relationship, and would further shrink the on-prem infrastructure the team maintains.

Why It Worked

Three things separated this engagement from the alternative the client was evaluating:

01 Assessment before implementation.

The health check meant the POC tested the client's real gaps, not a generic demo path.

02 Lab validation before client exposure.

Integrations were proven in a representative environment first, so client sessions demonstrated working capability instead of live troubleshooting.

03 An embedded operating model.

Badged access and ongoing enablement turned a project into a working relationship, which is where the F5, Splunk, and Kubernetes wins came from.



CASE STUDY | MACHINE IDENTITY MODERNIZATION