BISHOPFOX

CASE STUDY

THE RIGHT DOSE: A HEALTH TECH PROVIDER PUTS IT'S SYSTEMS TO THE TEST

CUSTOMER SNAPSHOT

INDUSTRY	Healthcare – Technology
CUSTOMER	A leading healthcare technology enterprise serving hospitals, clinics, long-term care homes, and specialty organizations nationwide.
SERVICES PROVIDED	Continuous Security Testing, Architecture Security Assessment

CUSTOMER OVERVIEW

A healthcare technology leader was transforming its software and systems (once deployed on-premises at hospitals and healthcare facilities) to a subscription-based SaaS model, with a new cloud platform to centralize its product management. Along the way, it expanded its service offerings and acquired new web properties and product portals. As the company evolved and grew, its security needed to keep pace.

The new cloud platform was the most consequential piece of that growth; the kind of architectural leap that unlocks real product value: centralized management, faster updates, better visibility. It also meant taking on an entirely new category of risk. It would centralize management across every customer, alongside a new generation of connected hardware built to run on it, and for the first time, sensitive customer and patient data would live in a shared, multi-tenant environment.

At the same time, the external footprint kept expanding, added to over time, maintained at different points by different teams, none of it fully knowable through any single review.

The company sought a security partner deep enough to validate the architecture of what it was building, and persistent enough to keep pace with everything already out there.

THE CHALLENGE

The company's security team understood the stakes of getting the new platform right: insufficient isolation in a shared, multi-tenant environment could allow the compromise of one application component to affect data belonging to multiple customers. Because the platform was designed around zero-trust principles, the team needed to evaluate whether its access controls and permissions would limit the impact if any single component was compromised.

There was a hardware dimension too. The new connected devices would be deployed into customer environments the company didn't control, meaning the devices themselves needed to establish trustworthy identity even in physical settings where tampering was a real possibility. And because this new device architecture was expected to serve as the template for future connected products, getting the provisioning model right the first time mattered well beyond this one product line.

A single deep review, however thorough, would only ever capture a moment in time, and the company's footprint kept shifting. The company also needed ongoing testing across its growing collection of web properties and product portals to maintain a current, actionable view of external risk as the business evolved.

SECURITY CHALLENGES

- **Multi-Tenant Data Isolation:** Validate that a compromise in one part of the new cloud platform couldn't cascade into exposure of sensitive data belonging to other customers.
- **Zero-Trust Verification:** Confirm that the platform's zero-trust design would actually contain a security failure or insider compromise as intended, rather than assume it on paper.
- **Device Identity at the Edge:** Ensure each cloud-connected device could be provisioned and authenticated securely once deployed into physical environments outside the company's direct control.
- **A Moving Perimeter:** Maintain continuous visibility over a diverse, growing set of external-facing systems, spanning multiple product lines and brands, rather than relying on periodic, one-off snapshots.

THE SOLUTION

The company brought in Bishop Fox to meet the moment. Rather than a conventional penetration test, Bishop Fox conducted an architecture-level security assessment: a structured review of the design itself, working directly with the product and engineering teams who built it.

Bishop Fox's assessment team reviewed documentation, interviewed the subject matter experts and engineers behind the platform, and interacted with test and production environments to validated that selected parts of the implementation matched the intended design. Cloud components were evaluated against the AWS Well-Architected Framework; web application components were evaluated against the OWASP Application Security Verification Standard. Particular attention went to the Kubernetes permissions model underlying the platform's multi-tenancy and cryptographic root-of-trust process used to provision each physical device.

That depth of review addressed only half the challenge. The partnership expanded to include a continuous security testing program covering the company’s broader external environment. Where the architecture assessment went deep on one platform, continuous testing program helped strengthen security more broadly. The program provided ongoing visibility into assets across the company’s changing attack surface and identified any vulnerabilities and emerging threats impacting those assets. Because Bishop Fox experts validated ownership of every asset, and verified and prioritized the impact of all their findings, the customer’s security team could focus on fixing any issues before they could be exploited.

GOALS OF THE ENGAGMENT

- Review the design and initial implementation of the new multi-tenant cloud platform against healthcare-grade security requirements.
- Assess the connected device's provisioning and authentication architecture for resilience against physical tampering.
- Validate the platform's zero-trust assumptions under a simulated compromise scenario.
- Find newly introduced weaknesses across a broad, evolving external footprint before they could be exploited.

THE OUTCOME

Together, the architecture assessment and the continuous security testing program gave the company confidence in the security of its next-generation platform and an up-to-date, actionable understanding of its external attack surface exposure. The architecture assessment confirmed that the cloud platform and connected-device architecture were fundamentally well designed and aligned with established security practices for multi-tenant healthcare environments, while identifying one high-priority architectural issue the customer was able to address before it could become a larger concern.

KEY RESULTS

- **Surfaced a Multi-Tenant Blast-Radius Gap:** Bishop Fox identified an overly permissive IAM role assigned to the application workload that could allow a compromised component retrieve database credentials across all tenant environments. Existing compensating controls limited the practical impact, but the finding gave the engineering team a concrete, prioritized case for a SPIFFE-based workload identity model already on their roadmap, scoping credential access to each tenant individually.

- **Validated the Device Root-of-Trust Architecture:** Bishop Fox hardware-level review [JC3] confirmed that the platform's TPM-backed provisioning process securely established unique device identity before deployment, with no material issues identified. This gave the engineering team confidence in an architecture that will serve as the template for every connected product built on it going forward.

- **Delivered Continuous Visibility Across a Constantly Evolving Attack Surface:** The continuous security testing program identified issues as they emerged, including reflected cross-site scripting, outdated third-party software, exposed services, and legacy SSH and TLS configurations. Each cycle paired current visibility into the company’s external exposure with clear remediation guidance and follow-up testing to confirm corrective actions.

CONCLUSION

Building a secure healthcare platform requires more than validating today's environment. It requires confidence that the architecture is sound, that critical design decisions hold up under scrutiny, and that security keeps pace as the business evolves.

By combining an architecture security assessment with continuous security testing, the company gained both perspectives. Bishop Fox helped validate foundational design decisions before they became difficult to change, identify targeted opportunities to further strengthen the platform, and maintain ongoing visibility across an expanding external attack surface.

The result is a security program that supports innovation with confidence, allowing the company to continue modernizing its products while better protecting the healthcare organizations and patients that depend on them.