Large Enterprise Healthcare Company Strengthens Security Posture with Trellix

Industry
Health Care

Size
Large Enterprise

Country
US

Customer Overview

A large enterprise healthcare organization operates in a highly regulated environment where data protection, patient privacy, and regulatory compliance are mission-critical. The organization manages large volumes of electronic health records (EHR), patient telemetry, and sensitive medical data across multiple facilities, hybrid infrastructure, and cloud environments.

As part of its digital transformation strategy, the organization expanded workloads into AWS to improve scalability, resiliency, and operational efficiency. This expansion introduced new requirements for cloud-native security visibility, centralized threat detection, and compliance monitoring aligned with healthcare regulatory frameworks such as HIPAA and regional data residency mandates.

The organization required a security architecture capable of protecting cloud and hybrid workloads while maintaining operational continuity for clinical and patient-facing systems.

Business & Technical Challenge

Before modernization, the organization relied on multiple disconnected security tools spanning endpoint, network, and threat intelligence domains. This fragmented approach limited visibility across AWS workloads and on-prem infrastructure, making it difficult to correlate threats across cloud, endpoint, and network telemetry sources. Security teams relied on manual investigation workflows that slowed incident response and increased operational overhead, as they had to manage multiple security vendors and platforms.

As AWS adoption increased, the organization required cloud-scale threat detection aligned with elastic cloud workloads, centralized visibility across AWS and hybrid environments, and integration with AWS-native telemetry sources, including cloud activity logs, identity events, and workload signals. The organization also required security analytics that could support compliance reporting and audit readiness in a highly regulated healthcare environment.

Solution Architecture

The organization implemented a Trellix security platform integrated with AWS cloud services to create a unified, cloud-aligned security architecture. Security telemetry from AWS workloads and cloud activity was centralized into Trellix Helix, enabling correlation across endpoint, network, and cloud security events. This provided a single operational view across a hybrid infrastructure common in healthcare environments.

Helix delivered centralized extended detection and response analytics across AWS and on-prem assets, while Trellix Wise provided advanced analytics and detection tuning using aggregated telemetry. Threat Intelligence capabilities enhanced proactive detection against healthcare-targeted threat campaigns. The architecture supported hybrid deployment models, allowing sensitive data processing to remain aligned with regional data residency requirements while leveraging AWS cloud analytics to improve detection speed and scalability. The architecture also supported healthcare regulatory audit requirements through centralized logging and reporting capabilities.

The Outcome

Following the implementation of Trellix solutions, the organization achieved measurable improvements aligned with AWS Cloud Value Framework pillars. Security teams gained improved cross-environment threat visibility across AWS and on-prem systems while improving detection and response speed through centralized analytics and correlation. Patient data and clinical systems protection improved through unified detection coverage.

Operational efficiency improved through the consolidation of multiple security tools into a unified platform. Investigation timelines decreased due to correlated cloud and endpoint telemetry visibility. Security operations workflows became more streamlined and easier to manage across distributed healthcare environments.

Cloud-scale analytics enabled efficient processing of large healthcare telemetry datasets while supporting distributed facility environments. Compliance and governance posture improved through centralized logging, reporting, and audit-ready security data aligned with healthcare regulatory and data residency requirements.

Strategic AWS Business Impact

The organization successfully aligned cybersecurity operations with its AWS cloud adoption strategy. The integrated security architecture enabled secure cloud expansion while maintaining strict healthcare compliance requirements. Security teams gained real-time visibility across hybrid workloads while reducing operational complexity and improving incident response timelines.

Testimonial

The addition of on-demand scanning has been a major improvement for the security team. This is a capability that has been highly requested for years, and having it available now provides much greater confidence in endpoint visibility and response readiness. The on-demand malware scanning capability within Trellix Endpoint Security (HX) makes it significantly easier to verify that scans are actively running across the environment, which directly contributes to faster and more reliable response times during investigations.

The organization is also expanding its security posture by enabling additional capabilities such as EDRF and Data Security modules. While deployment will take time due to the scale of the environment, the team is confident these enhancements will further strengthen detection coverage, improve investigation workflows, and support long-term security and compliance objectives.

Security Analyst

Large Enterprise Health Care Company

Independent research conducted by UserEvidence. Source: Survey of a Large Enterprise Health Care company. Data verified February 02, 2026.

UserEvidence

uevi.co/6468JQFZ UEID: 6468JQFZ