UST Epic EHR cloud security assessment on Microsoft Azure

Accelerate Zero Trust and Agentic AI readiness in just four weeks

ust.com

Healthcare organizations face increasing pressure to protect critical Epic workloads from ransomware, insider threats, and cloud misconfigurations, while simultaneously modernizing infrastructure for agility and cost control. UST's Epic EHR 4-Week Security Assessment on Microsoft Azure is purpose-built to deliver intelligent, actionable security guidance in record time. Backed by our Epic expertise, Microsoft's cloud-native security model, and Agentic AI-powered agents, this engagement surfaces blind spots, identifies misalignments, and lays the foundation for autonomous, scalable protection.

UST

More than an assessment. It's a launchpad for intelligent cloud defense

Today's healthcare IT environments are overwhelmed by fragmented observability, inconsistent policy enforcement, and the rising complexity of hybrid cloud ecosystems. Many lack visibility across containerized workloads and critical DevSecOps pipelines. Breaches are growing in severity and cost, while security operations remain reactive and manually stitched together. UST delivers a modern alternative: a four-week, outcome-driven diagnostic designed to bring clarity, structure, and intelligent automation to your Epic cloud posture.

Through a tightly scoped, high-impact engagement, UST helps you move beyond checklist security audits. We deliver prioritized remediation strategies powered by intelligent agents that not only detect risk but understand its context. This accelerates resolution and enables continuous improvement.

Agentic AI and Zero Trust at the core

This engagement is grounded in UST's proprietary Agentic AI architecture and aligned with Zero Trust principles. Our UST Sentinel Mind agent performs automated detection, anomaly analysis, and root cause correlation. UST FinOps Agent adds visibility into cloud usage and security-driven cost spikes. UST Governance Agent ensures policy alignment, real-time compliance checks, and configuration hygiene across your Microsoft Azure footprint. Together, these agents enable faster time to detection, lower mean time to resolution, and long-term readiness for autonomous security operations.

We focus on security control domains most vulnerable in Epic-on-Azure environments: identity and access management, asset visibility, log and event monitoring, data protection, and workload containment.
Our maturity model evaluates your organization's posture across each domain and delivers a roadmap for Zero Trust-aligned transformation.

What to expect from the 4-week engagement

The process begins with a discovery call and security questionnaire to establish scope and priorities.
UST then conducts structured interviews with your stakeholders and telemetry reviews across key surfaces, including endpoints, identity perimeter, production workloads, and CI/CD pipelines.
Throughout the engagement, our team applies intelligent agent tools to extract telemetry, visualize dependencies, and detect behavioral anomalies.
Findings are delivered in a final report with maturity scoring, risk heatmaps, and clear, defensible remediation recommendations backed by UST and Microsoft best practices.

Built for healthcare. Designed for transformation

With more than 15 years in healthcare and over a decade of cloud transformation success, UST blends deep Epic domain expertise with intelligent engineering systems to deliver results quickly, securely, and at scale. Our healthcare security leaders, cloud architects, and AI specialists collaborate closely with client teams to reimagine security operations from reactive to resilient.

Learn how to protect what matters most while accelerating your path to intelligent cloud defense.

Since 1999, UST has driven transformation through digital solutions, platforms, engineering, R&D, products, and innovation. With 30,000+ employees, we deliver measurable value worldwide.

ust.com

Version 0101-20250910