"Marcus"

Chief Information Officer at a Regional Health System

The Pain Point: Compliance & Vendor Lock-in

We didn't just save money. We bought ourselves an insurance policy against future vendor strategy shifts."

THE SITUATION

Following a rigorous 2025 security audit, Marcus's team was tasked with implementing enterprise-wide MFA and advanced SSL encryption. While these features were technically available through his legacy middleware vendor, the only path to acquire them required a mandatory transition to a purely commercial licensing tier. This would have forced the hospital to pay for high-cost, bundled support packages they didn't need, significantly inflating long-term OpEx and creating total vendor lock-in. Marcus needed a way to secure his environment without being forced into an inflexible, "all-or-nothing" commercial contract.

THE BRIDGELINK DECISION

Marcus didn't choose BridgeLink because it was "free"; he chose it because it was secure and flexible. He needed a platform that offered enterprise-grade MFA, SSL encryption, and Git-based audit trails through an unbundled model, allowing him to maintain the technical freedom of open source.

THE OUTCOME

Risk Mitigated

His team upgraded to BridgeLink and immediately cleared their CVE security audit by resolving critical vulnerabilities that were unpatched in his legacy version.

Strategic Control

By relying on the Technical Advisory Board (TAB) for governance rather than a single vendor's financial strategy, Marcus restored his board's confidence in their long-term infrastructure.

BridgeLink
Powered by Innovar Healthcare

www.innovarhealthcare.com/bridgelink