

HEALTHCARE

TECHNOLOGY RATIONALIZATION

# Cybersecurity tool rationalization for a multi-entity healthcare system

A large, multi-entity healthcare system had invested in security tools across identity, cloud, application, data, and operations, but years of mergers and decentralized decisions left overlapping technologies and uneven maturity. **Optiv Consulting** delivered an objective, framework-aligned portfolio analysis to rationalize the tooling without net-new spend.

SECTOR	ENVIRONMENT	REGULATED	TOOLS REVIEWED
Multi-entity healthcare	Azure, GCP, SaaS	HIPAA, PCI, SOX	125+

## THE CHALLENGE

Leadership lacked clear visibility into where tools delivered value, where gaps existed, and where consolidation could reduce risk and operational friction. They needed a defensible assessment that prioritized next steps without adding complexity.

## OUR APPROACH

- Reviewed more than 125 security tools, mapped to the CIS Critical Security Controls and MITRE ATT&CK.
- Assessed technical gaps, functional maturity shortfalls, and technology redundancies.
- Aligned findings to the client's strategic roadmap.
- Delivered phased recommendations to operationalize existing investments, improve integration and automation, and strengthen governance.

## 125+ tools

Mapped to CIS Controls and MITRE ATT&CK for real-world risk alignment

## BUSINESS RESULTS

- Gave leadership enterprise-wide clarity on effectiveness, gaps, and overlap in the security portfolio.
- Produced a risk-aligned roadmap prioritizing optimization and consolidation over new acquisition.
- Created a foundation for ROI measurement and ongoing tool lifecycle governance.