Case Study

Enabling Proactive Cyber Defense for a Leading Healthcare Provider

Summary

A top-tier healthcare organization partnered with us to strengthen its enterprise security posture by implementing a proactive, scalable, and regulatory-compliant security framework. The goal was to ensure patient data protection, maintain service integrity, and reduce cyber risks across the IT landscape.

© Infinite Computer Solutions, 2025

Scope

- Assess enterprise-wide security risks, identify vulnerabilities, and align with healthcare compliance mandates.
- Develop cybersecurity policies, standard operating procedures, and governance models.
- Establish a layered security architecture covering network, endpoints, identity, and access.
- Deploy advanced solutions for threat detection, prevention, and rapid response.
- Build employee security awareness and establish an incident response playbook.

Challenges

- Increasing cyber threats targeting healthcare data and systems.
- Need for alignment with HIPAA and other regulatory frameworks.
- Gaps in real-time monitoring, incident response, and endpoint protection.
- Dispersed IT infrastructure and lack of centralized identity governance.
- Requirement to balance strong security controls with seamless user experience.

© Infinite Computer Solutions, 2025

Solution

- Governance Automation: Deployed ServiceNow GRC to standardize compliance tracking and risk management workflows.
- Secure Access Architecture: Implemented Cloudflare Access (SDP) for zero-trust, identity-aware application access.
- Threat Detection & Response: Enabled IBM QRadar SIEM for centralized logging, anomaly detection, and event correlation.
- Network Protection: Deployed Next-Gen Firewalls (Palo Alto) for deep packet inspection and threat prevention.
- Endpoint Defense: Rolled out Microsoft Defender EPP for integrated malware protection, behavioral analysis, and remediation.
- Identity & Access Management: Centralized IAM via Microsoft Azure AD, enforcing MFA and access control policies.
- Data Protection: Integrated Symantec DLP to monitor, classify, and protect sensitive data from unauthorized access.
- Automated Response: Established playbooks and automation for incident response and digital forensics.

Business Value

- Improved Risk Posture: Significantly reduced security gaps with continuous monitoring and early threat identification.
- Regulatory Compliance: Ensured alignment with HIPAA and healthcare-specific mandates through automated controls.
- Faster Incident Containment: Automated threat response led to faster containment, minimizing service disruption and loss.
- Enhanced Data Security: Protected critical patient data and IP from internal and external threats.
- Operational Efficiency: Enabled centralized governance and reduced manual overhead with automation and orchestration.
- Employee Awareness: Strengthened organization-wide security culture, reducing risk from insider threats.

For more information, please visit www.infinite.com