Modernizing Cybersecurity for Healthcare

Contents

Protecting Patients and Their Data

The Future of Healthcare: Inclusive Access Through Virtual Health

Navigating the Compliance Maze

Tomorrow's HIPAA: Proactive Security for Patient Data

A Simplified Approach to Security and Compliance

Zero Trust: A Foundation for Healthcare Security

Key Security Challenges in Healthcare

Cisco Services for PHI Security and Resilience

Cisco Integrated Security: Delivering Unified Resilience and Compliance

Cisco Security Suites: Mapping Solutions to Healthcare Compliance Controls

Getting Started with Cisco

Resources

Appendix: Cisco Security Solutions

Protecting Patients and Their Data

As a healthcare organization, you face the ongoing challenge of modernizing IT to meet evolving demands from patients, clinicians, and staff, while complying with cybersecurity frameworks and regulations. Your modernization efforts may include cloud-based Electronic Health Record systems (EHRs), secure digital environments for Protected Health Information (PHI) and medical assessments, online administrative services, and mobile apps supporting patient engagement and clinical safety. You aim to enhance patient care, operational efficiency, and PHI protection, which requires careful security governance.

This Solution Brief will help guide you through IT modernization in healthcare, emphasizing innovation and security. We explore initiatives to transform operations, improve patient and clinician experiences, and strengthen cyber defenses. Learn to streamline processes, implement security governance, and support compliance.

The Future of Care: Inclusive Access Through Virtual Health

Healthcare access is increasingly challenged by provider shortages and facility closures. Virtual health bridges the digital divide, addressing disparities for underserved populations in both remote and metropolitan areas. By delivering services via video, mobile apps, and sensors, virtual health ensures coordinated care independent of time or location.

Success requires ecosystem collaboration. Public and private sectors must align incentives, while government support for connectivity remains vital to enable inclusive care. Beyond video visits, virtual health leverages remote monitoring and asynchronous data sharing to improve clinical outcomes securely and efficiently.

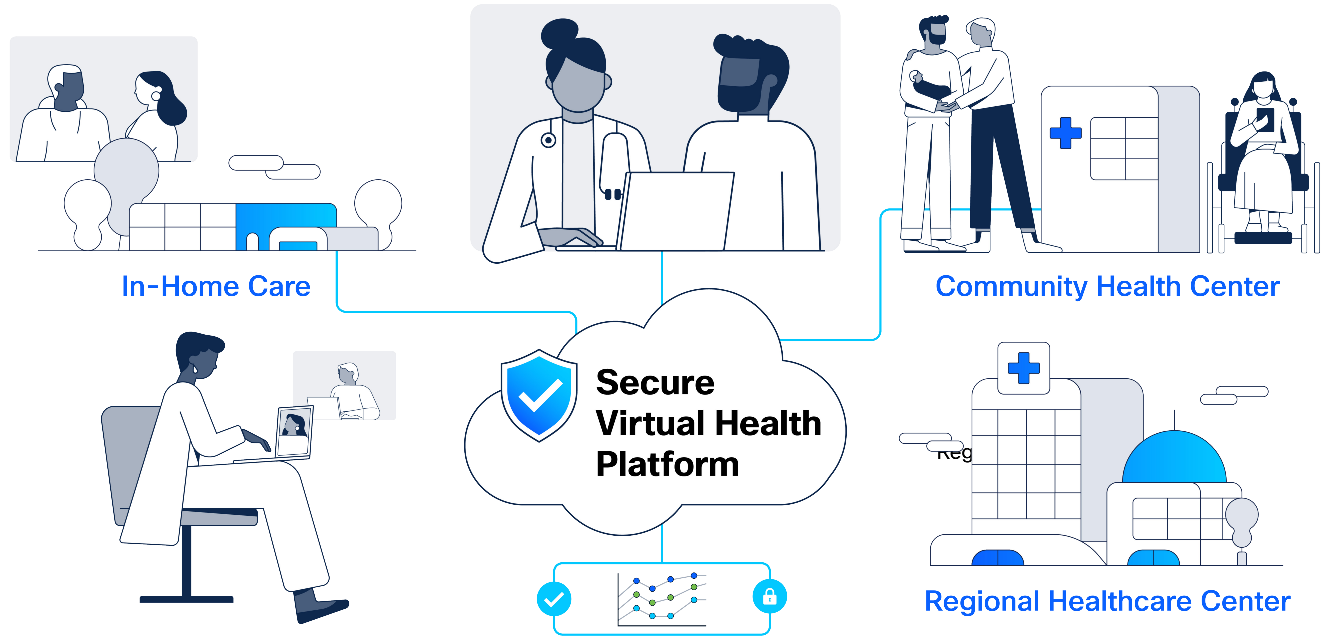
By embracing these digital solutions, healthcare organizations can:

- **Expand Equity:** Reach underserved communities regardless of geography through hybrid care models.
- **Enhance Coordination:** Use AI and analytics to support clinical decision-making and patient safety.
- **Improve Efficiency:** Streamline operations and reduce costs through automated workflows.

Secure digital solutions help providers bridge access gaps while protecting sensitive patient data.

The Digital Health Ecosystem:

Connecting Care Everywhere



In-Home Care

Community Health Center

Secure Virtual Health Platform

Regional Healthcare Center

Expand equity
Faster access
Continuity of care

Clinical confidence
AI-assisted decisions
Fewer missed appointments

Operational efficiency
Lower cost of care
Regional collaboration

NIST CSF

NIST SP 800-53

NIST SP 800-207

GDPR

ISO 27001

HIPAA

PHIPA

HITECH

CIS Benchmarks & Controls

Navigating the Compliance Maze

Healthcare organizations operate within a complex landscape of cybersecurity frameworks that collectively guide the protection of sensitive health information and ensure regulatory compliance. Core frameworks include HIPAA and HITECH, which mandate the safeguarding of PHI. These are complemented by the National Institute of Standards and Technology (NIST) frameworks–NIST Cybersecurity Framework (CSF), NIST SP 800-53, and NIST SP 800-207 (Zero Trust Architecture)–which provide structured, risk-based approaches to managing cybersecurity controls and implementing zero trust principles. Additionally, the Center for Internet Security (CIS) Benchmarks and Controls offer a prioritized set of industry-standard best practices to harden IT systems and mitigate the most common cyber attacks.

Together, these frameworks form an interconnected set of guidelines that help healthcare organizations establish a strong security posture, manage risks, and comply with legal requirements. Healthcare providers are increasingly aligning with the HHS Cybersecurity Performance Goals (CPGs). These goals provide a clear subset of high-priority security practices specifically designed to help the healthcare sector prioritize investments and improve cyber resiliency against common threats. Organizations must consider regional regulations like PHIPA for Ontario, Canada, and international standards such as GDPR and ISO 27001 when operating across borders.

Navigating numerous overlapping regulations and standards, healthcare organizations rely on these frameworks to build resilient cybersecurity strategies. Adhering to these diverse requirements safeguards sensitive data, fosters trust, and enables adaptation to evolving threats, ensuring secure and efficient healthcare delivery.

Understanding the complex regulatory landscape is the first step. To effectively navigate these requirements and safeguard patient data, proactive cybersecurity measures are essential.

Explore Security Frameworks and Certifications

Tomorrow's HIPAA: Proactive Cybersecurity for Patient Data

The healthcare cybersecurity landscape is rapidly evolving as new technologies and interconnected patient data drive ongoing updates to frameworks like HIPAA from bodies such as HHS. While specific HIPAA changes are expected, the core mission remains: protect patient privacy, ensure data integrity, and maintain system availability.

Healthcare organizations must prepare for regulatory changes that are not yet fully defined. The best approach is to proactively strengthen cybersecurity today, building a resilient foundation for future requirements. Adopting leading practices protects against threats and ensures readiness for new HIPAA mandates.

Cisco’s security architecture empowers healthcare organizations to enhance patient safety, safeguard sensitive data, and maintain continuity, no matter how regulations change.

- **Embrace Zero Trust Principles**
  Continuously verify all users, devices, and applications before granting access to PHI and critical clinical systems.

- **Strengthen Identity and Access Management**
  Implement strong multi-factor authentication (MFA) and least privilege access to protect sensitive patient data across all systems.

- **Segment Networks and Secure Medical IoT**
  Segment networks and secure medical IoT and applications to protect PHI and patient safety.

- **Enhance Threat Detection and Response**
  Use AI and threat intelligence for swift detection and automated action to minimize breach impact.

- **Secure Cloud and Hybrid Environments**
  Protect PHI with consistent policies across all cloud and on-premises environments, preventing data exfiltration.

- **Continuous Vulnerability Management**
  Proactively find and fix weaknesses to help reduce your attack surface and prioritize risks.

- **Strong Incident Response**
  Develop and test plans for fast recovery, minimizing downtime, and fulfilling breach notification requirements.

A Simplified Approach to Security and Compliance

Modernizing healthcare IT shouldn't be overwhelming. As organizations face increasing cyber threats and evolving HIPAA requirements, strategic initiatives can streamline processes while strengthening PHI protection. Key focus areas include:

- **Adopting integrated security platforms:** Consolidating tools for unified visibility and control across diverse clinical environments.
- **Automating compliance tasks:** Reducing manual effort for HIPAA reporting, audits, and policy enforcement.
- **Leveraging secure cloud solutions:** Utilizing cloud-native security for EHRs, telehealth, and other critical healthcare applications.
- **Using AI/ML for enhanced threat detection:** Proactively identifying and neutralizing threats targeting sensitive patient data.
- **Standardizing security processes and training:** Equipping clinical and administrative staff with best practices for PHI handling and cyber awareness.

Digital solutions free up resources for patient care, but true resilience starts with a clear strategy. Developing a modernization roadmap ensures security investments align with clinical goals and regulatory needs. By prioritizing intentional planning and expert guidance, healthcare organizations can simplify transformation and build a secure, compliant foundation for the future.

Zero Trust: A Foundation for Healthcare Security

In modern healthcare, trust is never assumed. A Zero Trust Architecture protects PHI by continuously verifying every interaction across the workforce, workload, and workplace.

- **Enforce Least-Privilege:** Grant only the minimum access required for clinical and administrative roles to limit the blast radius of a breach.
- **Strategic MFA:** Implement multi-factor authentication on every system that allows access to PHI, ensuring identity verification at every critical touchpoint.
- **Dynamic Access Control:** Apply real-time, risk-based policies across users, devices, and assets, extending from the edge to the data center.

To future-proof the digital workplace, Cisco integrates the Hybrid Mesh Firewall to secure the data center. This ensures consistent, resilient protection for critical workloads and patient data, regardless of where they reside.

This unified approach creates a resilient environment where clinicians can focus on care, knowing patient data is secure. It ensures that security scales seamlessly with the evolving demands of modern, digital-first medicine.

Key Security Challenges in Healthcare

Cloud and Application Security

- Data breaches in cloud-hosted EHRs/Picture Archiving and Communication System (PACS)
- Malware in patient portals or telehealth apps
- Misconfigured cloud services exposing PHI

Network Security

- Unauthorized access to hospitals networks
- Denial of service disrupting patient care systems
- Data interception on unsecured medical IoT devices

Data Center and Research Security

- Physical and insider threats to on-premises PHI
- Virtual machine escape in shared environments
- Lateral movement attacks

User and Device Security

- Phishing and malware threats targeting clinicians
- Lost medical devices and weak credentials
- Insider threats from compromised accounts

Threat Detection and Response

- Advanced Persistent Threats (APTs) targeting healthcare research
- Ransomware targeting patient systems
- Stealthy malware in clinical networks

Supply Chain and Third-Party Risk

- Vulnerabilities in partner ecosystems
- Lateral movement from compromised integrations
- Limited control over external security postures

Cisco Services for PHI Security and Resilience

Beyond technology, Cisco offers a suite of expert services tailored for healthcare. These services provide strategic guidance, hands-on support to protect PHI, optimize your security posture, ensure continuous compliance, and offer critical emergency incident response should a security incident occur.

Zero Trust Advisory

The Cisco Zero Trust Advisory Service helps you understand and visualize a secure Zero Trust future. Our security experts will help pinpoint and measure your strengths and weaknesses. They will work with you to design a roadmap to achieve your security strategy. Deliverables include a CISA-aligned Zero Trust Strategy and Analysis Report which includes a Zero Trust scorecard, strategic roadmap, and an executive summary of our findings and recommendations.

HIPAA Aligned Security Assessment FUTURE 2026

A new security assessment to help healthcare organizations (IT, Security, Applications, Biomed) to understand their current state maturity grade according to NIST 800-207 and proposed HIPAA changes, as well as help prioritize a roadmap to drive greater compliance.

Healthcare Digital Capabilities Assessment

A Healthcare Digital Capabilities Assessment evaluates an organization's digital maturity across areas such as infrastructure, security, collaboration, and digital processes. The assessment helps identify strengths, gaps, and opportunities, guiding organizations toward effective digital transformation and improved operational outcomes.

Healthcare Segmentation Advisory

Cisco's Healthcare Network Segmentation Advisory helps increase visibility, standardize policies, and prevent gaps during implementation. We empower you with expert guidance, industry best practices, and a strategy to achieve network segmentation across your organization including all connected assets - IT, IoT, IoMT, etc.

Application Microsegmentation Service

Protecting your critical applications, for instance for EHR, when on-prem or in the cloud is essential to ensure patient care and day-to-day operations. This strategy service is designed to help you successfully implement application-level segmentation policies to safeguard patient privacy, prevent unauthorized access, and reduce blast radius in the event of a breach.

HIMSS Analytics Infrastructure Adoption Model (INFRAM) Services

HIMSS INFRAM is an international, seven-stage (0-7) model for assessing infrastructure adoption and capabilities maturity. Cisco INFRAM Services enhance your business foundation by optimizing technology and infrastructure. The assessment identifies opportunities within your current investments and delivers a clear roadmap for improvement.

Talos Incident Response

Cisco Talos Incident Response (Talos IR) helps security teams efficiently prepare for and respond to cyber threats by providing expert guidance and proven best practices. Key benefits include:

- 24x7 access to Talos incident Response, ready for immediate action during critical security incidents
- Development of clear, step-by-step Incident Response (IR) playbooks tailored to specific threats and business needs
- Readiness and logging architecture assessments to identify gaps and enhance overall incident response preparedness
- Proactive threat hunting and on-demand intelligence to identify emerging threats before they affect operations
- Support for proactive security measures to strengthen overall incident readiness

Talos IR empowers organizations to respond quickly and confidently to incidents, minimizing impact and enhancing cyber resilience.

Talos Threat Intelligence

Cisco Talos is the elite threat intelligence organization at the heart of the Cisco Security portfolio. Comprised of top security experts, Talos delivers superior protection by providing unified, real-time threat data across all Cisco security products and services. This shared intelligence enables consistent, coordinated decision-making throughout the security ecosystem, ensuring comprehensive visibility and rapid response across large and diverse networks. A common operating environment powered by Talos is essential for effective cybersecurity defense and insight in today’s complex threat landscape.

Cisco Integrated Security: Delivering Unified Resilience and Compliance

To navigate the complexities of modern healthcare–from expanding medical IoT to stringent PHI compliance–organizations need more than fragmented tools; they need unified resilience. Cisco Security Cloud serves as this foundation. It is an integrated, AI-driven platform designed to help eliminate security silos and simplify management across your environment.

Rooted in zero trust, the platform secures patient data through continuous identity verification and global threat intelligence, delivering:

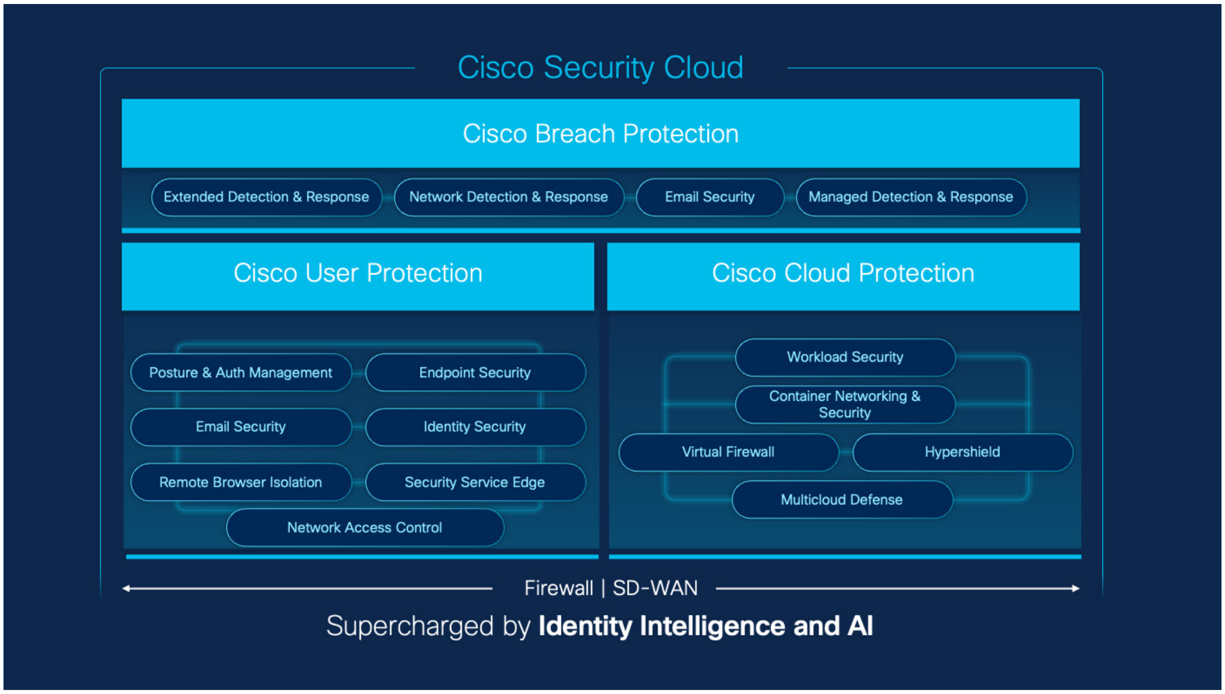
- **Better Efficacy:** AI-speed detection to protect clinical systems and devices.
- **Better Experience:** Unified workflows for overstretched IT and clinical staff.
- **Better Economics:** Reduced complexity through strategic vendor consolidation.

Cisco delivers these outcomes through four core solution suites tailored to your security maturity:

- **User Protection Suite:** Secure, frictionless access for clinicians to any application on any device.
- **Breach Protection Suite:** Accelerated threat detection and response powered by AI and global telemetry.
- **User and Breach Protection Suite:** Combines the strengths of both suites to deliver a unified platform for comprehensive workplace security.
- **Cloud Protection Suite:** Safeguard applications and data across hybrid and multicloud environments.

Together, these suites empower healthcare providers to grow with confidence, ensuring security never comes at the expense of patient care.

A Unified Foundation for Your Workload, Workforce, and Workplace Protection



Comprehensive Protection Across Workload, Workforce, and Workplace

Navigating the complexities of HIPAA, NIST, and the HHS Cybersecurity Performance Goals (CPGs) requires a direct alignment between security technology and regulatory policy. Cisco's integrated suites—Breach, User, User and Breach, and Cloud—are designed to map specifically to the essential controls required to protect patient data and maintain clinical continuity.

To provide a clear operational perspective, these capabilities are organized across the three core Zero Trust domains:

- **Workplace:** Securing the clinical environment, medical IoT, and campus networks.
- **Workforce:** Protecting the clinicians, staff, and third-party partners accessing critical systems.
- **Workload:** Safeguarding the applications and PHI data that power healthcare services.

This framework provides a complete picture of how Cisco supports regulatory compliance while strengthening patient-centered cybersecurity. While the following mappings illustrate our comprehensive coverage, the subsequent sections provide a deeper exploration into the specific products and operational benefits of each suite.

Table 1. Workload Capabilities Mapped to Breach, User, and Cloud Protection Suites, and Splunk

Key: ● Helps support

		Workload Capabilities									
	Cisco Product	Application & API Security	Encryption	Data Loss Prevention	Application Micro Segmentation	Secure DevOPs	Vulnerability Management	Threat Detection & Response	3rd Party Access	Policy Enforcement & Automation	Forensic Logging Platform
Breach Suite	XDR	●		●			●	●	●	●	●
	Secure Endpoint	●					●	●		●	●
	Email Threat Defense		●	●			●	●		●	●
	Secure Network Analytics	●	●	●				●	●	●	●
	Telemetry Broker							●	●		●
	Talos IR Threat Hunting	●				●	●	●	●		●
	Secure Malware Analytics	●						●			
User Suite	Duo	●						●	●	●	●
	Secure Access	●	●	●	●	●	●	●	●	●	●
	Identity Services Engine	●	●		●			●	●	●	●
	Secure Endpoint	●					●	●		●	●
	Secure Client	●	●	●				●	●	●	●
	Email Threat Defense		●	●			●	●		●	●
Cloud Suite	Secure Workload SaaS	●	●		●	●	●	●		●	
	Hypershield	●	●		●	●	●	●		●	●
	Isovalent Enterprise Platform	●	●		●	●	●	●		●	●
	Secure Firewall (virtual)	●	●	●	●	●	●	●	●	●	●
	Multicloud Defense	●	●	●	●	●	●		●	●	x
Splunk	Enterprise Security	●	●	●		●	●	●	●	●	●
	SOAR	●	●	●		●	●	●	●	●	
	User Behavior Analytics	●		●				●	●		●
	Attack Analyzer	●		●				●	●	●	●
	Asset & Risk Intelligence	●		●				●	●	●	●
Other	AI Defense	●	●	●		●	●	●	●	●	●

Additional information about specific Cisco products can be found in the Appendix.

Table 2. Workforce Capabilities Mapped to Breach, User, and Cloud Protection Suites, and Splunk

Key: ● Helps support

		Workforce Capabilities								
	Cisco Product	Email Security	Multi-Factor Authentication	Credential Management	Cybersecurity Training	Role-Based Access Control	Posture Assessment	Endpoint Detection & Response	Access Audit Logging	Zero Trust Access (ZTA)
Breach Suite	XDR	●						●	●	
	Secure Endpoint			●		●	●	●	●	●
	Email Threat Defense	●			●			●	●	
	Secure Network Analytics					●	●	●	●	●
	Telemetry Broker	●				●	●	●	●	●
	Talos IR Threat Hunting	●			●			●	●	
	Secure Malware Analytics	●						●		
User Suite	Duo		●	●		●	●		●	●
	Secure Access	●	●	●		●	●		●	●
	Identity Services Engine		●	●		●	●		●	●
	Secure Endpoint	●	●	●		●	●	●	●	●
	Secure Client	●	●	●		●	●	●	●	●
	Email Threat Defense	●			●			●	●	
Cloud Suite	Secure Workload SaaS		●	●		●	●	●	●	●
	Hypershield					●	●	●	●	●
	Isovalent Enterprise Platform					●			●	●
	Secure Firewall (virtual)					●			●	●
	Multicloud Defense					●			●	●
Splunk	Enterprise Security	●	●	●		●		●	●	●
	SOAR	●	●	●		●		●	●	●
	User Behavior Analytics	●	●	●		●		●	●	●
	Attack Analyzer	●		●				●		●
	Asset & Risk Intelligence			●			●	●	●	●
Other	AI Defense					●			●	●

Additional information about specific Cisco products can be found in the Appendix.

Table 3. Workplace Capabilities Mapped to Breach, User, and Cloud Protection Suites, and Splunk

Key: ● Helps support

		Workplace Capabilities					
	Cisco Product	Network Macro & Micro Segmentation	Network Telemetry & Flow Analysis	Anomaly Detection	Centralized Logging (SIEM)	Device Profiling	Network Access Controls
Breach Suite	XDR	●	●	●	●	●	●
	Secure Endpoint		●	●	●	●	●
	Email Threat Defense		●	●	●		
	Secure Network Analytics	●	●	●	●	●	●
	Telemetry Broker		●	●	●	●	
	Talos IR Threat Hunting		●	●	●	●	
	Secure Malware Analytics		●	●			
User Suite	Duo	●	●	●	●	●	●
	Secure Access	●	●	●	●	●	●
	Identity Services Engine	●	●	●	●	●	●
	Secure Endpoint	●	●	●	●	●	●
	Secure Client	●	●	●	●	●	●
	Email Threat Defense		●	●	●		
Cloud Suite	Secure Workload SaaS	●	●	●	●	●	●
	Hypershield	●	●	●	●	●	●
	Isovalent Enterprise Platform	●	●	●	●	●	●
	Secure Firewall (virtual)	●	●	●	●	●	●
	Multicloud Defense	●	●	●	●	●	●
Splunk	Enterprise Security		●	●	●	●	●
	SOAR		●	●		●	●
	User Behavior Analytics		●	●		●	
	Attack Analyzer			●			
	Asset & Risk Intelligence		●	●		●	●
Other	AI Defense	●	●	●		●	●

Additional information about specific Cisco products can be found in the Appendix.

Cisco Breach Protection Suite

The Cisco Breach Protection Suite safeguards workloads by unifying detection, investigation, and response across endpoints, email, network, identity, firewall, and cloud environments. This comprehensive suite includes Cisco XDR, Cisco Secure Email Threat Defense, Cisco Secure Endpoint, and Cisco Secure Network Analytics (SNA). Leveraging AI and threat intelligence, it offers:

- Accelerated incident response for healthcare, minimizing the impact of breaches on patient care and sensitive PHI through cross-domain visibility and automated investigations.
- Robust defense against phishing and ransomware, protecting clinicians and staff from email-borne threats that often target access to patient data and critical systems.
- Advanced endpoint protection for medical devices, clinical workstations, and mobile devices, preventing malware infections and data exfiltration across the healthcare network.
- Proactive anomaly detection across the network, identifying suspicious activities and insider threats to safeguard PHI and maintain the integrity of clinical operations.

Healthcare relies on deep partner interconnections with insurance providers, pharmacies, and clinics, which significantly expand the digital attack surface. The Cisco Breach Protection Suite helps mitigate this third-party risk through early detection and observability. By utilizing Cisco XDR and SNA, the suite identifies anomalous behavior and lateral movement originating from partner integrations. This unified visibility allows organizations to contain supply chain attacks quickly, ensuring the continuous protection of patient care and sensitive PHI.

Cisco User Protection Suite

The Cisco User Protection Suite is designed to protect the healthcare workforce by securing user access and endpoints with zero trust, safeguarding patient data and medical devices by enforcing strict identity verification and device posture checks. This suite provides essential components like Cisco Secure Email Threat Defense, Cisco Duo multi-factor authentication, Cisco Secure Endpoint, and Cisco Identity Services Engine (ISE).

It supports Zero Trust principles and seamless hybrid work by offering:

- Robust protection against email-borne threats, safeguarding clinicians and staff from phishing, ransomware, and business email compromise that often target access to PHI.
- Phishing-resistant multi-factor authentication (MFA), ensuring only verified healthcare personnel and authorized users can access sensitive systems and patient data.
- Advanced threat detection and blocking on all devices, from clinical workstations to mobile devices, preventing malware infections and data loss.
- Granular network access control, enforcing least privilege for users and devices, including medical IoT, to protect critical clinical systems and PHI.

Cisco User and Breach Protection Suite

Designed to address today's complex challenges–from expanding attack surfaces and sophisticated identity-based threats to implementing a robust zero trust strategy–the User & Breach Protection Suite seamlessly integrates essential capabilities. This includes identity protection, secure access to applications, and AI-driven Extended Detection and Response (XDR) across email, endpoints, cloud, and network.

The Suite provides unmatched, correlated visibility and insights, enabling proactive security measures and building organizational resilience. It simplifies operations, reduces alert fatigue and vendor sprawl, and accelerates your security maturity journey, leading to enhanced security outcomes and a seamless experience for both users and security teams.
With the User and Breach Protection Suite, you can:

Defend Against Identity Threats
Stop identity-based attacks with layered protection that provides actionable insights across the Cisco portfolio.

Improve Security Outcomes
Integrated products work together to defend against the evolving threat landscape, provide clear verdicts for decisive response action, and increase security maturity.

Increase Operational Efficiency
Ease operational burdens and support vendor consolidation by leveraging the Cisco ecosystem.

Cisco Cloud Protection Suite

The Cisco Cloud Protection Suite secures hybrid and multicloud environments by unifying segmentation and gateway controls. It provides visibility and access controls to protect applications and data while simplifying security operations. Protect your apps and data, gain pervasive visibility, and streamline security management across your environment. The suite combines simplicity, flexibility, and investment protection for easy adoption of Cisco Hybrid Mesh Firewall. Cloud Protection Suite Essentials offers two options-Essentials Segmentation and Essentials Gateway-to help customers achieve their security goals from ground to cloud.

Leveraging AI-driven automation, it offers:

- Segmentation for any application or environment to stop the lateral movement of attacks across the data center and cloud, ensuring that zero-trust policies are consistently enforced at the workload level.
- Kernel-level visibility and enforcement through eBPF-powered technology, providing deep insights into application behavior and high-performance security without impacting system velocity.
- Distributed exploit protection detects discovered CVEs, prioritizes risks to the business, and automatically generates compensating controls to shield against vulnerabilities until patches can be applied.
- Multicloud network security for AWS, Azure, and GCP from one interface simplifies operations, while delivering robust protection to stop inbound attacks, data exfiltration, and unauthorized movement, as well as advanced protection against zero day exploits and to block malware in encrypted traffic.

Getting Started with Cisco

Securing digital environments in healthcare is essential for patient privacy, safe care, and supporting staff. Cisco's integrated security architecture addresses healthcare's unique needs–from protecting devices and systems to helping ensure compliance with regulations like HIPAA. Our comprehensive solutions simplify challenges, boost cyber resilience, and modernize healthcare IT.

Partnering with Cisco helps healthcare organizations confidently handle evolving threats, optimize operations, and create secure care environments. Connect with our experts to develop a tailored strategy that lets clinicians focus on patients and ensures a secure digital future. For assistance, contact your Cisco Account Executive.

Resources

- Cisco in healthcare
- Cisco portfolio for healthcare
- Powering inclusive care for all
- Why Cisco for healthcare

Appendix: Cisco Security Solutions

This appendix provides a comprehensive overview of additional Cisco security products that underpin the integrated suites and services discussed in the main document. Organized by key security domains, these solutions offer granular capabilities to further strengthen your healthcare organization's cyber defenses

Network Security

Securing networks is critical to protecting patient data, research assets, and clinical operations. Cisco's network security solutions help prevent unauthorized access, detect threats in real time, and ensure safe connectivity across distributed environments.

Cisco Hybrid Mesh Firewall

Cisco Hybrid Mesh Firewall provides unified security management and consistent policy enforcement across on-premises, cloud, and hybrid environments. It combines Cisco Secure Firewall physical and virtual appliances with cloud-delivered firewalls in a single, integrated architecture, enabling centralized visibility, simplified operations, and scalable protection. With AI-driven automation, threat intelligence, and flexible deployment options, Cisco Hybrid Mesh Firewall empowers organizations to safeguard users, applications, and workloads everywhere—streamlining policy management while adapting to dynamic business needs and modern, distributed IT infrastructures.

Cisco Secure Firewall

Cisco Secure Firewall offers advanced threat protection across data center, cloud, and IoT environments with unified management. Powered by AI-driven SnortML detection, it blocks zero-day attacks and threats in encrypted traffic without decryption. Features include centralized management, intrusion prevention, application visibility, and seamless integration with Cisco XDR for accelerated incident response. The firewall family supports diverse deployment options including hardware, virtual, and cloud-native, ensuring scalable, high-performance security tailored to enterprise needs.

Cisco Identity Services Engine (ISE)

Cisco ISE is a comprehensive identity and access control platform that enforces Zero-Trust security policies across wired, wireless, and VPN networks. It provides device profiling, posture assessment, and dynamic network segmentation to ensure only authorized users and devices gain access. Cisco ISE integrates with Cisco security products to deliver contextual access control, helping organizations meet compliance requirements by reducing attack surfaces and enforcing granular access policies.

Cisco Multicloud Defense

Cisco Multicloud Defense is a cloud-native security solution that delivers centralized visibility, policy enforcement, and protection across AWS, Azure, and GCP environments. It integrates seamlessly with cloud-native architectures, enabling consistent threat prevention and workload segmentation. With automated policy controls and real-time traffic analysis, Cisco Multicloud Defense simplifies compliance and strengthens your security posture. It allows organizations to streamline operations, reduce risk, and accelerate the deployment of security across diverse multicloud infrastructures.

Cisco Security Cloud Control (formerly Defense Orchestrator)

Cisco Security Cloud Control centralizes and streamlines security management across on-premises and cloud environments, enhancing visibility and efficiency. With real-time insights, AI-powered automation, and a unified interface, it accelerates threat detection, policy enforcement, and troubleshooting. Features like natural language querying and AIOps support faster decision-making and simplify operations. Manage solutions such as Secure Firewall, Multicloud Defense, Hypershield, and more, while ensuring consistent protection and simplified scalability through cloud-assisted onboarding and continuous feature updates.

Cisco XDR

Cisco XDR unifies threat detection, investigation, and response across endpoints, networks, cloud, and applications. By correlating telemetry from Cisco and third-party sources, it provides comprehensive visibility and context to identify and prioritize threats faster. Automated playbooks streamline response, while AI-driven analytics reduce alert fatigue and simplify operations. Cisco XDR enables organizations to accelerate threat response, minimize risk, and strengthen security posture with a single, integrated platform for end-to-end cyber defense.

Device Security

The device is now the healthcare security perimeter. Cisco Device Security protects patient data and clinical uptime by validating the integrity of every endpoint—from clinician laptops to medical IoT (IoMT). By enforcing strict posture requirements, we ensure only healthy devices connect, preventing compromised hardware from disrupting care or threatening patient safety.

Cisco Secure Endpoint

Cisco Secure Endpoint delivers advanced Endpoint Detection and Response (EDR) capabilities, leveraging threat intelligence to detect, investigate, and remediate threats in real time. It integrates with Cisco Secure Client as a module, providing continuous monitoring, behavioral analysis, and automated threat containment to reduce attack surfaces and support compliance with Zero-Trust security frameworks.

Cisco Secure Client (including AnyConnect)

Cisco Secure Client delivers unified, secure access for users across any device, location, or application. Integrating VPN, Zero Trust Network Access (ZTNA), posture assessment, and robust threat defense, it enables secure connectivity to corporate resources while protecting users from modern threats. With centralized management, flexible deployment, and seamless user experience, Cisco Secure Client simplifies secure access for hybrid workforces. It supports compliance and policy enforcement, ensuring that users stay productive and protected wherever they work.

Cisco Security Connector

Cisco Security Connector is a network extension app for iOS/iPadOS devices enrolled in Cisco Meraki Systems Manager. It enables DNS-layer security via Cisco Umbrella and content filtering through Cisco Clarity, providing per-app or full-device protection. This integration enhances visibility and control over mobile endpoints, supporting secure access and compliance in hybrid work environments.

Cisco Meraki Systems Manager (SM)

Cisco Meraki Systems Manager is a cloud-based Mobile Device Management (MDM) solution that simplifies endpoint management and security across diverse device types. It integrates with Cisco XDR for unified visibility and automation, enabling administrators to deploy security applications like

Cisco Secure Client and Cisco Security Connector at scale. Systems Manager supports device posture assessment, policy enforcement, and remote configuration, helping organizations maintain compliance and secure hybrid workforces.

User Security

Identity is the gateway to patient data. Cisco User Security protects clinicians from phishing and identity-based attacks while ensuring frictionless access to critical systems. By verifying every user through zero trust, we safeguard PHI without disrupting clinical care.

Cisco Duo

Cisco Duo provides Multi-Factor Authentication (MFA) and Zero-Trust security to verify user identities and device health before granting access. It supports adaptive access policies, passwordless authentication, and risk-based authentication, and integrates with a broad range of applications and environments—including Microsoft. Duo also features Single Sign-On (SSO), device trust checks, and comprehensive reporting for compliance and auditing. It enhances protection against identity-based attacks, secures remote and hybrid workforces, and helps healthcare organizations meet compliance mandates with robust security controls.

Cisco Secure Access

Cisco Secure Access is a cloud-delivered security service edge (SSE) solution that provides seamless, secure access to applications and resources from anywhere. By combining Zero Trust Network Access (ZTNA), cloud access security broker (CASB), secure web gateway (SWG), and firewall-as-a-service (FWaaS), it protects users and data against modern threats. With unified policy management, AI-driven insights, and a frictionless user experience, Cisco Secure Access enables organizations to secure hybrid workforces and simplify security operations across distributed environments.

Cloud, Application, and Workload Security

Cloud platforms power patient care, collaboration, and medical research—but they must be secured. Cisco's cloud security protects data, applications, and users across all cloud environments—including those running critical healthcare systems like Epic—while supporting compliance and patient privacy.

Cisco Umbrella

Cisco Umbrella is a cloud-delivered security platform that provides secure internet gateway services, including DNS-layer security, secure web gateway, firewall, and Cloud Access Security Broker (CASB) functionalities. It blocks malicious domains, URLs, and IPs before a connection is established, preventing threats such as malware, phishing, and ransomware. Umbrella supports remote and distributed workforces with consistent policy enforcement and integrates threat intelligence to enhance protection and compliance with cybersecurity requirements.

Cisco AI Defense

Cisco AI Defense delivers advanced threat protection using AI and machine learning to detect, prevent, and respond to emerging cyber threats in real time. It analyzes vast telemetry data across networks, users, and cloud environments, identifying malicious activity and automating response actions. With continuous learning and adaptive defense, Cisco AI Defense enables organizations to proactively defend against sophisticated attacks and reduce risk, all while simplifying security operations and accelerating incident response.

Cisco Hypershield

Cisco Hypershield s a distributed enforcement layer, extending consistent segmentation and threat protection to workloads across hybrid and multi-cloud environments. Hypershield enforces policy at two levels. At the network layer, it extends L4 segmentation to every port on Cisco Smart Switches, enforcing policy on internal traffic at line rate. At the workload layer, the Hypershield agent uses eBPF technology to deliver deep kernel-level visibility, enabling context-aware segmentation based on identity, application, and process, well beyond what network-only controls can provide. This distributed model scales with the environment and eliminates the visibility gaps inherent in centralized architectures.

Cisco Secure Workload

Cisco Secure Workload protects applications across on-premises, cloud, and hybrid environments by providing deep visibility, AI/ML-driven policy automation, and real-time threat detection. It enables zero-trust microsegmentation to reduce attack surfaces and prevent lateral threat movement. The platform continuously monitors compliance and integrates with existing infrastructure and security tools for consistent workload protection.

Cisco Secure Email Threat Defense

Cisco Secure Email Threat Defense delivers advanced, cloud-native protection for Microsoft 365 and Google Workspace email environments. Leveraging AI and machine learning, it detects and blocks sophisticated threats such as phishing, malware, business email compromise, and ransomware. Continuous analysis, threat intelligence, and automated response capabilities stop attacks before they reach users' inboxes. With seamless integration, real-time reporting, and simplified management, Secure Email Threat Defense helps organizations safeguard sensitive data and ensure business email continuity.

Cisco Web Application and API Protection (WAAP)

Cisco WAAP safeguards web and mobile apps, APIs, and bots with advanced WAF, API security, DDoS mitigation, and client-side protection. AI-driven automation refines policies and detects threats, while the solution adapts to changes across hybrid and multicloud setups. It provides analytics and 24/7 managed support to protect applications and lower operational costs.

Analytics

Data-driven insights are key to proactive security. Cisco's analytics solutions help institutions detect threats, monitor user behavior, and optimize security operations using real-time intelligence.

Cisco Secure Malware Analytics (Threat Grid)

Cisco Secure Malware Analytics provides advanced malware sandboxing and threat intelligence for fast detection, analysis, and prioritization of threats. It integrates with Cisco Secure Endpoint and other tools, offering detailed behavioral insights and automated protection. Available as a cloud subscription or on-premises appliance, it safeguards sensitive data and accelerates incident response with rich context and global intelligence feeds.

Cisco Secure Network Analytics (SNA)

Cisco SNA offers comprehensive network visibility and real-time threat detection across on-premises and cloud environments without requiring decryption. Leveraging behavioral modeling, machine learning, and global threat intelligence, it identifies anomalies, insider threats, and encrypted malware. The agentless solution scales with organizational growth and integrates with Cisco XDR for unified threat investigation and automated response, enhancing network security posture and compliance.

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging centralizes the collection, storage, and analysis of security telemetry and logs across your network. It supports compliance, investigations, and threat hunting with detailed audit trails and actionable insights, and integrates with Cisco SNA and XDR to streamline security operations.

Cisco Telemetry Broker

Cisco Telemetry Broker is a scalable, flexible platform that collects, normalizes, and distributes telemetry data from diverse network devices and sensors. It enables real-time analytics and monitoring by feeding enriched data into security and operational tools. Supporting multiple telemetry formats and protocols, it enhances visibility and supports compliance by ensuring comprehensive data availability for security analytics.

Digital Experience Assurance

Clinical uptime depends on visibility beyond the local network. Digital Experience Assurance provides end-to-end visibility into the paths clinicians take to reach EHRs and cloud apps. It aids security by quickly distinguishing between performance issues and active cyberattacks, ensuring uninterrupted patient care.

ThousandEyes

ThousandEyes provides end-to-end path visualization for EHRs and cloud applications, aiding security by distinguishing between performance issues and active cyber attacks. By eliminating visibility blind spots, it ensures clinicians have resilient, secure access to the digital tools required for patient care.

Splunk Security

Splunk integrates with Cisco for deep visibility into security events. It enables healthcare organizations to correlate data, investigate incidents, and automate response across complex environments.

Splunk Enterprise Security

Splunk Enterprise Security unifies threat detection, alert triage, threat intelligence, investigation, response and case management in a single platform. Its powerful capabilities enable you to realize comprehensive visibility, empower accurate detection with context and fuel operational efficiency. Built on the Splunk platform powered by AI capabilities, Splunk Enterprise Security delivers analytics at scale for continuous security monitoring with cost-effective data optimization. With Splunk, you can detect what matters, investigate holistically and respond rapidly.

Splunk Security Orchestration, Automation, and Response (SOAR)

Splunk SOAR empowers security teams to automate repetitive tasks, orchestrate workflows, and accelerate incident response. By integrating with a wide range of security tools and systems, Splunk SOAR enables automated threat detection, investigation, and remediation. Its playbooks, case management, and analytics streamline security operations, helping reduce response times and improve efficiency.

Splunk Asset and Risk Intelligence

Splunk Asset and Risk Intelligence delivers continuous asset discovery and compliance monitoring to accelerate investigations and minimize risk exposure. Leveraging the rich data in Splunk, the solution provides comprehensive asset inventories, unlike the fragmented, inaccurate, and outdated information typical of traditional asset management tools.

Splunk Attack Analyzer

Splunk Attack Analyzer provides automated threat analysis and associated digital forensics of files and URLs to deliver consistent high-quality analysis of potential threats, save analysts time, and help SOCs achieve the operational efficiency needed to outpace adversaries. The solution uses proprietary technology to extract malicious content from text, images, macro source code, website content to automatically analyze credential phishing and malware threats.

Splunk User Behavior Analytics (UBA)

Splunk UBA helps organizations find know, unknown, and hidden threats across users, endpoint devices, and applications. Splunk UBA analyzes both users and entities using multi-dimensional behavior baselines, dynamic peer group analysis, and unsupervised machine learning. This allows it to rapidly detect anomalous behavior – such as compromised or misused accounts or devices, IP theft, or data exfiltration – and eliminate it.