Modernizing Cybersecurity for Universities

Contents

Student Success is Your Mission

As a higher education institution, you face the ongoing challenge of modernizing IT to meet evolving demands from students, faculty, and staff while complying with cybersecurity frameworks and regulations. Your modernization efforts may include cloud-based learning platforms, secure research environments, digital student services, and mobile apps. You aim to enhance learning experiences, operational efficiency, and data protection, but this requires careful consideration of security governance.

This Solution Brief was designed to guide you through IT modernization in higher education, emphasizing both innovation and security. We explore initiatives to transform your operations, improve student and faculty experiences, and strengthen cyber defenses. Learn to streamline processes, implement security governance frameworks, and support compliance requirements.

The Future of Higher Education: Connected, Secure, and Inclusive

The imperative for digital transformation in your higher education institution has never been more pressing. As you face increasing student expectations, expanding academic and research demands, and resource constraints, technology offers the key to revolutionizing your operations and learning environments.

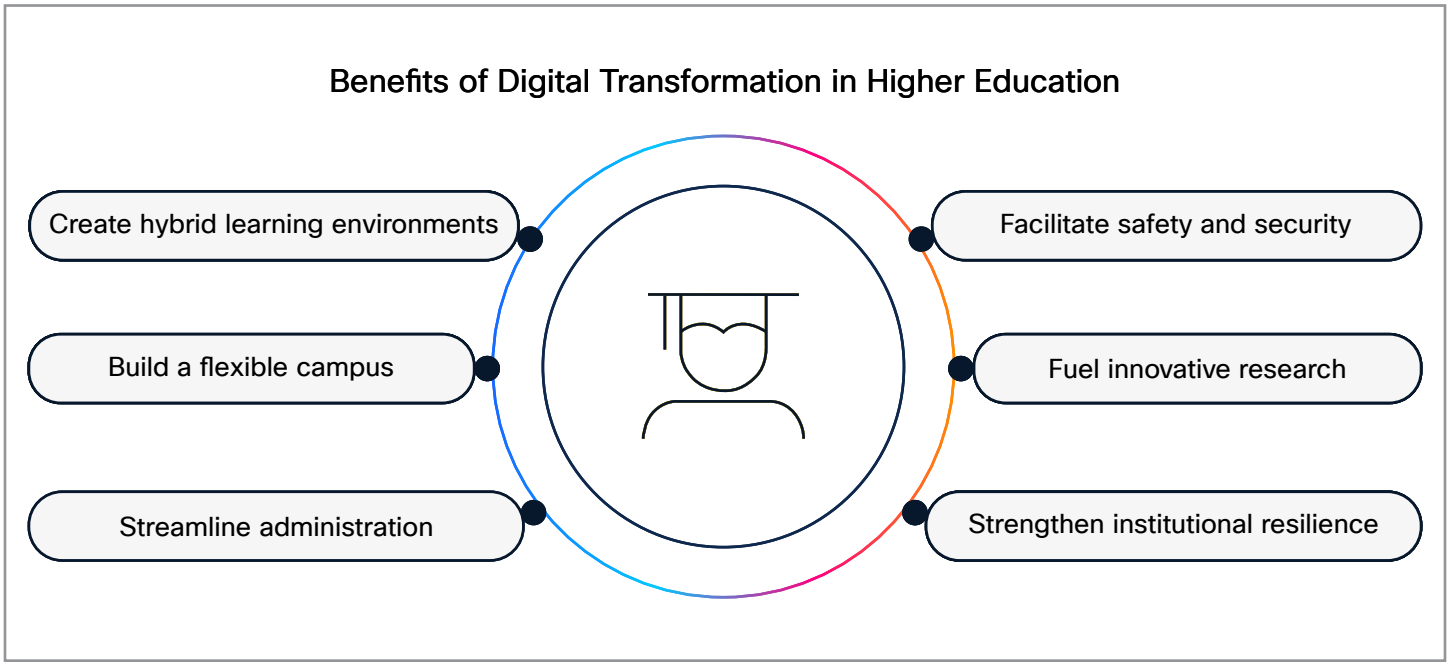
By embracing digital transformation, colleges and universities can:

- **Improve student services** with personalized digital experiences.
- **Use analytics and AI** to support academic planning and success.
- **Streamline operations** and reduce costs through automation.
- **Increase transparency** with better reporting and open data.
- **Promote inclusion** by ensuring access to digital tools.

However, modernization also presents challenges:

- **Cybersecurity threats** like phishing and ransomware.
- **Collaboration hurdles** across departments and systems.
- **Cultural resistance** to change and innovation.

With strategic planning and secure digital solutions, higher education institutions can modernize confidently—supporting student success while protecting critical data.



NIST CSF | NIST SP 800-171 | Educause | CMMC | NIS2 | ISO 27001

Navigating the Compliance Maze

As a higher education institution, adhering to key compliance standards and regulatory requirements is crucial. This helps improve student data protection, maintain institutional trust, and facilitate interoperability, and also reduces legal and security risks while promoting transparency and accountability.

Frameworks like National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), Educause, Cybersecurity Maturity Model Certification (CMMC), and Network and Information Security (NIS2) provide important guidelines, helping your systems meet security, privacy, and operational requirements. These frameworks can help build student and faculty trust, protect sensitive data, streamline security assessments, and support cloud-first academic strategies.

If your institution operates across international borders or engages in global research, you may need to address cross-regional compliance challenges by understanding and adhering to the local laws in each jurisdiction where you conduct activities. Cybersecurity requirements can vary significantly between countries, and practices acceptable in one region may not be permissible in another. You'll need to consider regulations on data transfers and protection, such as the EU General Data Protection Regulation (GDPR), Family Educational Rights and Privacy Act (FERPA), and global governance policies. Prioritizing cross-border cybersecurity compliance mitigates risks, fosters collaboration, and supports secure, efficient service delivery across academic and research networks.

Explore Security Frameworks and Certifications

Building Blocks for Modernization

Modernizing education means rethinking how institutions deliver learning, protect data, and support students in a digital-first world. These pillars form the foundation:

- **Zero Trust Architecture:** Secures your environment by continuously verifying users, devices, and applications.
- **AI-Enhanced Operations:** Boosts personalization and efficiency across classrooms and campuses.
- **Cloud-First Infrastructure:** Scales access to digital tools and reduces IT complexity.
- **Cyber Resilience:** Helps you withstand and recover from cyber threats with minimal disruption.
- **Incident Response and Recovery:** Enables fast, coordinated action when security events occur.
- **Digital Equity and Accessibility:** Expands access to technology and inclusive learning for all students.

A Simplified Approach to Security and Compliance

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

- Adoption of integrated security platforms.
- Automation of compliance tasks.
- Leveraging cloud-based solutions with built-in security.
- Using AI/ML to enhance threat detection.
- Standardizing processes and training for security.

By optimizing operations with digital solutions, institutions can free up resources to focus on student success, research, and innovation. These focus areas help simplify transformation, strengthen security, and support compliance with confidence.

Zero Trust: A Foundation for Campus Security

In today's education environments, trust must be earned—not assumed. With students, faculty, and staff accessing resources from multiple devices and locations, education institutions must adopt a "Zero Trust Architecture"—a model that assumes attackers are always present and continuously evolving.

Cisco's Zero Trust approach helps institutions:

- **Establish trust** through multi-factor authentication and device posture assessments.
- **Continuously verify trust** by monitoring user behavior and adjusting access dynamically.
- **Enforce trust-based access** using least privilege principles and secure workload communications.

This architecture ensures that:

- People are who they say they are.
- Devices are monitored for vulnerabilities.
- Access is tightly controlled and revoked when risk is detected.

By integrating Zero Trust principles into your cybersecurity strategy, institutions can protect sensitive data, reduce lateral movement, and support compliance with regulations like FERPA, Children's Online Privacy Protection Act (COPPA), and GDPR—building a resilient foundation for learning and operations.

Establish Trust

- Multi-factor authentication
- Device posture and vulnerabilities

Continuously Verify Trust

- Risk behavior monitoring
- Dynamic trust level changes

Enforce Trust-Based Access

- Least privilege authorization
- Workload communications

Key Security Challenges in Higher Education IT

Cloud and Application Security

- Data breaches in cloud-hosted environments
- Malware in third-party education apps
- Misconfigured cloud services

Network Security

- Unauthorized access to campus networks
- Denial of service disrupting online learning
- Data interception on unsecured systems

Data Center and Research Security

- Physical and insider threats to infrastructure
- Virtual machine escape in shared environments
- Lateral movement in research networks

User and Device Security

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

Threat Detection and Response

- Advanced Persistent Threats (APTs) and zero-day exploits
- Ransomware targeting student systems
- Stealthy malware and lateral movement

See the Cisco Security portfolio.

Unified Security for Modern Campuses

Educational institutions require a security strategy that spans diverse environments—from classrooms and labs to cloud platforms and remote devices. Cisco and Splunk together offer a powerful, integrated approach to campus cybersecurity, combining deep visibility, advanced analytics, and automated threat response.

This partnership empowers universities and colleges to:

- **Detect and respond to threats faster** with real-time insights across networks, users, and applications.
- **Simplify compliance** with frameworks like NIST, International Organization for Standardization (ISO) 27001, and FERPA.
- **Unify physical and digital security** through smart cameras, sensors, and endpoint protection.
- **Optimize operations** with scalable, cloud-managed solutions tailored to academic environments.

As you explore the following product categories—from network and user security to analytics and extended services—you'll see how Cisco and Splunk help institutions build a secure, resilient foundation for learning and innovation.

Platform and Suites

Cisco's platform and suites enhance cyber resilience by delivering integrated security tailored to higher education needs. They help reduce risk, improve threat response, and ensure compliance, enabling institutions to protect critical assets and maintain a strong security posture.

Cisco Security Cloud

Cisco Security Cloud is a cloud-native platform that unifies security management and operations across Cisco's security portfolio. It provides:

- Centralized visibility and control for threat detection and response.
- AI-driven analytics and automation to streamline security workflows.
- Integration with Cisco security suites for comprehensive protection.
- Support for compliance frameworks through consistent policy enforcement.

This platform enhances operational efficiency and compliance posture by consolidating security tools and intelligence.

Cisco Breach Protection Suite

Cisco Breach Protection Suite delivers unified detection, prevention, and response across email, endpoints, network, and cloud environments. Leveraging AI and threat intelligence, it accelerates incident response and mitigates advanced threats like ransomware and data exfiltration. Key features include:

- Integrated Cisco Extended Detection and Response (XDR) for cross-domain telemetry and automated investigations.
- Cisco Secure Email Threat Defense to block phishing and malware.
- Cisco Secure Endpoint for advanced endpoint protection.
- Cisco Secure Network Analytics for anomaly detection.

This suite helps schools maintain compliance by enhancing threat visibility and response efficiency.

Cisco Cloud Protection Suite

Designed for hybrid and multicloud environments, the Cloud Protection Suite provides critical controls to prevent lateral movement and protects applications and data. Key capabilities include:

- Micro-segmentation and centralized policy management.
- Zero Trust enforcement across data center and cloud workloads.
- Protection against zero-day exploits and malware in encrypted traffic.
- Automation to reduce misconfigurations and maintain business velocity.

This suite supports compliance by securing complex cloud infrastructures and preventing data exfiltration.

Cisco User Protection Suite

The User Protection Suite secures user access and data with comprehensive defenses against phishing, malware, and credential compromise. It supports Zero-Trust principles and seamless hybrid work by providing:

- Secure Email Threat Defense to block malicious emails.
- Duo multi-factor authentication for phishing-resistant access.
- Secure Endpoint to detect and block malware on devices.
- Cisco Identity Services Engine (ISE) for network access control.

This suite aids compliance with privacy regulations and strengthens user-centric security.

Network Security

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

Cisco Secure Firewall

Cisco Secure Firewall offers advanced threat protection across data center, cloud, campus, 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 Security Cloud Control (formerly Defense Orchestrator)

Cisco Security Cloud Control provides centralized, AI-driven management and policy orchestration across Cisco and third-party firewalls. It delivers intelligent, intent-based policy enforcement that adapts dynamically to network changes, simplifying firewall administration and enhancing security posture. This unified platform enables consistent policy application, real-time visibility, and streamlined workflows, supporting compliance through automated policy optimization and multi-vendor integration.

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. 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 secures complex hybrid and multicloud environments with unified, SaaS-based security management. It offers multidirectional protection—ingress, egress, and east-west—across Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI), and private clouds. Key features include continuous asset discovery, tag-based dynamic policy management, automation, and orchestration to reduce operational complexity. This solution prevents lateral movement, data exfiltration, and inbound threats, ensuring consistent security policies and compliance across diverse cloud infrastructures.

Cisco Extended Detection and Response (XDR)

Cisco XDR integrates telemetry from endpoints, networks, cloud, and applications to provide comprehensive threat detection and automated response. Leveraging AI and threat intelligence, Cisco XDR accelerates incident investigation and remediation by correlating alerts and orchestrating workflows. It enhances security operations efficiency and supports compliance by delivering unified visibility and faster threat mitigation.

Cisco Hybrid Mesh Firewall

Cisco Hybrid Mesh Firewall is a multi-deployment firewall platform with centralized cloud-based management designed for hybrid environments. It integrates hardware, virtual, and cloud-native firewalls into a unified security fabric, supporting Zero-rust segmentation, micro-segmentation, and advanced threat protection including IoT and DNS-based attacks. The solution offers AI-driven policy automation, seamless integration with Continuous Integration/ Continuous Delivery (CI/CD) pipelines, and consistent enforcement across data center, cloud, campus, and factory environments, helping organizations reduce attack surfaces and maintain compliance.

Device Security

With thousands of devices connecting to campus networks, endpoint protection is essential. Cisco's device security tools safeguard laptops, mobile devices, and lab equipment from malware, data loss, and unauthorized use.

Cisco Secure Client (including AnyConnect)

Cisco Secure Client is a unified endpoint agent built on the Cisco AnyConnect® framework, integrating Cisco Secure Endpoint and offering optional cloud management via Cisco XDR. It provides seamless, always-on VPN connectivity with intelligent tunneling protocols optimized for performance and security. The client supports endpoint posture assessment and

remediation in conjunction with Cisco ISE, enabling policy-driven access control. Additional features include built-in web security, malware defense with Cisco Umbrella integration, network visibility, and support for IEEE 802.1X and MACsec for secure network access. Cloud management simplifies deployment and updates across diverse devices.

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 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

Students, faculty, and staff are frequent targets of phishing and credential theft. Cisco's identity and access solutions ensure secure authentication, enforce least privilege, and reduce insider risk.

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 integrates with a broad range of applications and environments, including Microsoft. Duo enhances protection against identity-based attacks, secures remote and hybrid workforces, and helps organizations meet compliance mandates with continuous identity verification and risk-based access control.

Cisco Secure Email Threat Defense

Cisco Secure Email Threat Defense offers advanced protection against email-borne threats such as phishing, ransomware, and business email compromise. Leveraging AI-driven threat detection and intelligence, it provides real-time threat analysis, rapid remediation, and data loss prevention with end-to-end encryption. The solution supports cloud, on-premises, or hybrid deployments, helping organizations secure email communications and comply with cybersecurity requirements.

Cisco Secure Access

Cisco Secure Access delivers granular, policy-driven network access control that integrates with identity and device posture systems. It enables secure, zero-trust access to applications and network resources by continuously validating user and device trustworthiness. The solution supports hybrid environments and third-party integrations, helping organizations enforce consistent security policies and meet compliance standards.

Cisco Secure Web Appliance

Cisco Secure Web Appliance provides comprehensive web security by blocking access to malicious websites, filtering content, and preventing data loss. It integrates with threat intelligence to detect and block web-based threats in real time. The appliance supports flexible deployment options and centralized management, enabling organizations to protect users and data while aligning with cybersecurity compliance requirements.

Cloud Security

Cloud platforms power learning, collaboration, and research—but they must be secured. Cisco's cloud security offerings protect data, applications, and users across public, private, and hybrid cloud environments.

Cisco AI Defense

Cisco AI Defense is an end-to-end security solution designed to protect enterprises developing and using AI applications. It provides comprehensive visibility into AI assets, detects vulnerabilities and threats such as prompt injections and denial of service, and enforces real-time guardrails to safeguard AI models and applications. The solution also manages access to third-party AI tools, preventing data leakage and unauthorized use. Cisco AI Defense integrates network-level insights, advanced threat intelligence, and aligns with AI security standards including NIST and MITRE ATLAS to help organizations innovate securely in the AI era.

Cisco Attack Surface Management

Cisco Attack Surface Management continuously discovers and monitors an organization's external digital footprint to identify vulnerabilities and misconfigurations before attackers can exploit them. It provides real-time visibility into exposed assets, prioritizes risks based on threat intelligence, and offers actionable insights to reduce the attack surface. This proactive approach helps organizations maintain compliance with cybersecurity mandates by addressing external risks and improving overall security posture.

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.

Application Security

Educational apps and platforms are central to learning and operations. Cisco's application security tools protect against vulnerabilities, ensure secure development, and monitor for malicious activity.

Cisco Hypershield

Cisco Hypershield is an AI-native, distributed security architecture that embeds robust protection directly into the fabric of your university's IT infrastructure—across networks, servers, and cloud environments. Designed for the most demanding academic and research workloads, it integrates security and networking to automate policy enforcement and infrastructure upgrades. With kernel-level visibility and adaptive segmentation, Hypershield provides granular protection for sensitive research data, intellectual property, and critical learning platforms. This ensures rapid, autonomous, and trusted security at scale, simplifying management while safeguarding your institution's most valuable assets.

Cisco Secure Workload

Cisco Secure Workload is a hybrid-cloud workload protection platform that secures compute instances across on-premises data centers and public clouds, including virtual machines, bare-metal servers, and containers. It leverages machine learning and behavioral analysis to enable Zero Trust micro-segmentation, reducing attack surfaces and preventing lateral movement. The platform automates policy lifecycle management, continuously monitors compliance, and integrates with Cisco Secure Firewall and Identity Services Engine for enhanced contextual visibility and enforcement. Available as SaaS or on-premises appliance, it supports scalable, multi-cloud environments with comprehensive telemetry and AI-driven threat detection.

Cisco Web Application and API Protection (WAAP)

Cisco WAAP provides comprehensive protection for web and mobile applications, APIs, and bot management. It delivers state-of-the-art Web Application Firewall (WAF), API security, Layer 7 Distributed Denial of Service (DDoS) mitigation, and client-side protection. The solution uses AI-powered automation to refine security policies, detect threats, and reduce false positives. It adapts seamlessly to application changes across hybrid and multicloud environments, ensuring consistent security and compliance. Cisco WAAP also offers advanced analytics and 24/7 managed support to reduce operational costs while protecting critical applications and data.

Physical Security

Campus safety is a critical component of cybersecurity in higher education. Cisco Meraki's cloud-managed smart cameras and environmental sensors provide real-time visibility, intelligent alerts, and seamless integration with IT systems—helping institutions protect students, staff, and infrastructure while supporting compliance and operational continuity.

Cisco Meraki Smart Cameras

Meraki smart cameras deliver intelligent video surveillance with built-in analytics and secure cloud management. They help universities monitor campus activity, detect anomalies, and respond to incidents quickly—without the need for separate storage or software. Ideal for classrooms, dorms, labs, and public spaces.

Cisco Meraki Environmental Sensors

Meraki MT sensors monitor temperature, humidity, air quality, water leaks, and access points. They help protect IT infrastructure, maintain healthy learning environments, and prevent costly disruptions in classrooms, labs, and data centers.

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 delivers advanced malware sandboxing and threat intelligence, enabling rapid detection, analysis, and prioritization of malware threats. It integrates seamlessly with Cisco Secure Endpoint and other security tools, providing detailed behavioral insights and automated malware protection. Available as a cloud subscription or on-premises appliance, it ensures sensitive data remains secure while accelerating incident response and threat hunting through rich context and global threat 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 business 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 provides centralized collection, storage, and analysis of security telemetry and logs from across the network and security infrastructure. It supports compliance monitoring, forensic investigations, and threat hunting by delivering detailed audit trails and actionable insights. This solution integrates with Cisco SNA and Cisco XDR to streamline security operations and incident response.

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.

Splunk Security

Splunk integrates with Cisco to provide deep visibility into security events. It enables higher education institutions to correlate data, investigate incidents, and automate response across complex environments.

Splunk Platform

The Splunk Platform serves as the foundational solution for collecting, indexing, and analyzing machine data from diverse sources. It enables real-time monitoring, alerting, and customizable dashboards, providing scalable architecture and granular role-based access controls. This platform supports unified data visibility, audit readiness, and operational transparency, making it suitable for a wide range of IT and security use cases.

Splunk Asset and Risk Intelligence

Splunk Asset and Risk Intelligence discovers and inventories assets and identities across complex networks, continuously monitoring their activity to identify vulnerabilities and security risks. It provides comprehensive asset visibility and risk scoring, enabling proactive risk management and prioritization of remediation efforts. The tool helps maintain accurate asset records and control over the attack surface.

Splunk Enterprise Security (ES)

Splunk ES is a cloud-based Security Information and Event Management (SIEM) solution delivering prebuilt content and advanced analytics to detect, investigate, and respond to threats in real time. It facilitates rapid identification of malicious activities and anomalous behaviors, supports root-cause analysis, incident response, continuous monitoring, and compliance reporting.

Splunk Attack Analyzer

Splunk Attack Analyzer is a cloud-based application that maps intricate attack chains to identify credential phishing and malware threats. It automates investigation workflows to minimize manual effort, delivering actionable insights into the progression of attacks. Its automation and orchestration capabilities accelerate incident response, enhance threat detection, and strengthen overall security posture.

Splunk User Behavior Analytics (UBA)

Splunk UBA uses advanced analytics to identify insider threats and anomalous user behaviors by analyzing patterns and deviations. It integrates behavioral analytics into security monitoring to detect potential insider risks and unauthorized activities, improving overall security governance.

Splunk SOAR

Splunk Security Orchestration, Automation, and Response (SOAR) automates security operations workflows, integrates threat intelligence, and orchestrates response actions to improve incident response efficiency. This SaaS solution reduces response times, minimizes human error, and ensures consistent application of security policies through automation, enabling rapid threat mitigation and continuous security operations.

Extended Security Solutions

Advanced threats require advanced defenses. Cisco's extended offerings—including vulnerability management, Talos threat intelligence, incident response services, and consulting—help institutions strengthen resilience, respond to attacks, and align with cybersecurity frameworks.

Cisco Vulnerability Management

Cisco Vulnerability Management provides a proactive approach to identifying, assessing, and mitigating security weaknesses across networks and devices. It continuously scans for vulnerabilities and prioritizes remediation based on real-world threat intelligence, helping organizations reduce risk. The solution offers automated scanning to detect security gaps in hardware, software, and configurations, comprehensive reporting with actionable insights and compliance tracking, and integration with the Cisco Security Portfolio to enhance overall security posture by correlating vulnerability data with threat intelligence and incident response.

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.

Talos Incident Response

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

- Development of clear, step-by-step Incident Response (IR) playbooks tailored to specific threats and business needs.
- Expert analysis to ensure playbooks align with organizational processes and current threat intelligence.
- Streamlined workflows that reduce response time and improve mitigation effectiveness.
- Support for proactive security measures to strengthen overall incident readiness.

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

Cisco Services

Cisco Services provide expert guidance and hands-on assistance to help colleges and universities modernize and secure their infrastructure in alignment with strategic goals and compliance requirements. Key services offered include:

- **Program Management and Architectural Governance:** Overseeing cybersecurity initiatives to ensure alignment with institutional goals, regulatory requirements, and educational mandates.
- **Lifecycle Management and IT Optimization:** Assisting in the evolution and optimization of IT infrastructure to support secure, compliant operations.
- **Strategy Development and Technology Adoption Roadmaps:** Helping organizations plan and implement cloud adoption, Zero Trust architectures, and multifactor authentication.
- **Infrastructure Evolution Across Architectures:** Supporting modernization efforts including network modernization and enhanced detection, investigation, and response capabilities.
- **Packaged Services:** Providing pre-defined service bundles to accelerate deployment and adoption of Cisco security solutions, ensuring rapid time-to-value.
- **Support Services:** Offering ongoing hardware, software, and solution support with 24/7 access to technical experts, software updates, and threat intelligence to maintain security posture and compliance.

Cisco Partner Managed Services

Higher education institutions face growing complexity in securing digital learning environments, research infrastructure, and campus operations. Cisco's Partner Managed Services offer a scalable, expert-driven approach to cybersecurity—helping universities and colleges strengthen protection, streamline operations, and meet compliance requirements without overburdening internal teams.

Through trusted Cisco partners, institutions gain access to:

- 24/7 monitoring and threat detection across networks, endpoints, and cloud environments.
- Integrated security solutions including Cisco Umbrella, Duo, Secure Endpoint, and Firepower.
- Expert guidance and assessments to help align with frameworks like NIST, CMMC, and ISO 27001.
- Physical and cyber protection through unified video surveillance, access control, and incident response.

Whether you're securing student data, enabling hybrid learning, or protecting research assets, Cisco's partner ecosystem delivers the expertise and technology to help you stay ahead of threats and focused on your mission.

FIND A CISCO PARTNER

On-Premises Security

Despite increasing cloud adoption, the on-premises campus network remains a critical foundation for higher education. The reliance on local connections for students, faculty, and a growing array of IoT devices, coupled with ever-increasing bandwidth and remote access demands, underscores the persistent need for robust on-premises security.

Securing this environment means preventing unauthorized access, diligently monitoring activity, and rapidly remediating sophisticated threats—even those originating from legitimate but compromised users or devices. Cisco offers a comprehensive suite of on-premises security solutions that provide the granular control, deep visibility, and advanced threat protection essential for your physical infrastructure, local networks, and connected devices, seamlessly complementing your overall security posture.

Cisco's on-premises security solutions focus on blocking and controlling traffic as close to the source as possible within campus networks. These solutions reduce latency and provide immediate enforcement of security policies tailored to the institution's network environment.

Cisco Security Products Available for On-Premises Deployment

Network Security

- Cisco Secure Firewall: Available as hardware, virtual, and cloud-native deployments.
- Cisco Identity Services Engine (ISE): Typically deployed as a physical or virtual appliance on-premises.
- Cisco Hybrid Mesh Firewall: Integrates hardware and virtual firewalls into a unified security fabric, allowing on-premises deployment.

User Security

- Cisco Secure Email Threat Defense: Supports on-premises, cloud, or hybrid deployments.
- Cisco Secure Web Appliance: Typically deployed as a physical or virtual appliance on-premises.

Application Security

- Cisco Hypershield: Designed to embed security into every software component across networks and servers, allowing deployment within on-premises data centers and infrastructure.
- Cisco Secure Workload: Available as a SaaS offering or an on-premises appliance.

Physical Security

- Cisco Meraki Smart Cameras: These are physical devices deployed on-premises, with cloud management.
- Cisco Meraki Environmental Sensors: These are physical devices deployed on-premises, with cloud management.

Analytics

- Cisco Secure Malware Analytics (Threat Grid): Available as a cloud subscription or an on-premises appliance.
- Cisco Secure Network Analytics (SNA): Typically deployed as virtual or physical appliances on-premises.
- Cisco Security Analytics and Logging: Provides centralized collection, storage, and analysis of security telemetry and logs, often deployed on-premises.
- Cisco Telemetry Broker: A scalable platform that can be deployed as a virtual appliance on-premises.

Splunk Security

- Splunk Platform: The foundational Splunk solution can be deployed entirely on-premises.
- Splunk Asset and Risk Intelligence: As part of the Splunk Platform, it can be deployed on-premises.
- Splunk User Behavior Analytics (UBA): Often integrates with on-premises Splunk deployments.

Get Started with Cisco

Securing your digital environment is not just a necessity; it's the foundation for fostering innovation, protecting sensitive data, and ensuring student success. Cisco provides a proven, integrated security architecture, anchored by the unified management of Cisco Security Cloud Control and industry-leading Talos threat intelligence. This powerful architecture empowers higher education institutions to maximize existing investments, accelerate secure modernization efforts, and operationalize Zero Trust principles at scale.

By leveraging advanced automation, continuous risk assessment, and deep integration across your campus and cloud environments, Cisco enables:

- **Comprehensive, real-time visibility and automated threat detection** across all assets and domains, enhancing situational awareness and security posture.
- **Continuous, risk-informed operations** that adapt dynamically to academic and research needs, ensuring resilient defense against evolving threats.
- **Streamlined risk management processes** that reduce operational burden and accelerate compliance with critical higher education regulations and frameworks (e.g., FERPA, GDPR, NIST).
- **Scalable, future-proof defense capabilities** built on open standards and aligned with best practices for securing diverse university environments.
- **Maximized return on existing investments** through seamless integration and extension of current Cisco security licenses.

Complementing this, Splunk's data-driven analytics platform seamlessly integrates with the Cisco Security portfolio. This powerful combination provides extensive threat intelligence and advanced analytics, significantly enhancing visibility and control across users, devices, networks, and applications within your institution. Together, Cisco and Splunk enable cross-pillar Zero Trust capabilities—including identity verification, least privilege access, continuous trust verification, and AI/ML-powered threat detection and response.

This integrated approach cultivates robust security resilience by facilitating unified, automated, and adaptive security operations. It improves the experience for both users and IT operators, while consistently meeting the stringent compliance and security requirements inherent to higher education. With Cisco and Splunk, your institution can confidently navigate digital transformation, safeguarding its mission of education and research.

Resources

- Cisco in Education
- Solutions for Higher Education
- Tour a Smart School
- Facilitate Safety and Security in Education
- Cisco SAFE Guides for Campus and Branch

C99-5495879-00 10/25