Cisco Stealthwatch for Higher Education

Increase visibility, security, and compliance

Colleges and universities face wide-ranging and complex technology and security challenges. Social-savvy millennials arrive on campus, or connect virtually, from countless devices and with unfamiliar requests. Labs and libraries connect to innovative endpoints and cloud solutions. And learning environments stretch across the globe and integrate with open and online course platforms.

Higher education IT and security teams must embrace cloud, mobile, Bring-Your-Own-Device (BYOD), and social technologies for 10,000 users or more. At the same time, they must also protect student and faculty information, secure research data, and maintain application performance. These challenges are amplified by the need for open and scalable networks to accommodate a vast range of users:

- Students, faculty members, and researchers who require extensive cloud services
- Visitors and contractors who need limited but quick access
- Medical, finance, and executive staff who deal with specific regulations

Higher education IT and security professionals face these enormous challenges with limited network tools, and thus cite information security as their number one issue.[1] Although these institutions increasingly embrace new technologies, few have the visibility to understand what is happening on their network. This lack of visibility leaves open doors for attackers to hide, steal data, and misuse organizational resources. In fact, almost one-third of higher education institutions are victims of a cybersecurity attack each year.[2]

[1] "Top 10 IT Issues, 2017: Foundations for Student Success," EDUCAUSE Review, January 17, 2017

[2] "Data Analytics, Cybersecurity Top 2017 Higher Ed Tech Trends," EdTech, January 12, 2017

Cisco Stealthwatch helps higher education institutions:

- Understand and monitor complex network traffic
- Protect student and research data
- Detect P2P and rogue guest activity
- Reduce threat response times and streamline operations
- Comply with RIAA, MPAA, DMCA, and HEOA regulations

University improves network visibility and cybersecurity

Central Michigan University faced an increase in mobile devices, file-sharing traffic, and compliance issues on its open network. The IT team needed to gain network visibility and enable automated responses to illegal file sharing. Team members also needed a way to rapidly elevate security concerns and anomalous behavior.

After deploying Cisco Stealthwatch and gaining critical visibility into internal network traffic, the IT group achieved faster incident detection, prioritization, and response. This improvement resulted in better cybersecurity decisions and reduced peer-to-peer file sharing violations, which can lead to expensive fines for colleges if not mitigated.

Network visibility and insight

Fortunately, higher education IT and security teams can address these challenges with the network visibility and analytics provided by Cisco Stealthwatch™ technology and complementary security solutions. Together, these solutions enable a "security everywhere" strategy with the network acting as a critical sensor and enforcer.

Cisco Stealthwatch gives IT and information security teams comprehensive visibility that allows them to gain real-time situational awareness of all activity on the network. Visibility is cost-effectively achieved by collecting NetFlow and other forms of telemetry data from network infrastructure devices such as routers, switches, and firewalls.

The solution records and stores NetFlow data, which includes sender and receiver IP addresses, along with the time, date, and size of every network transaction. This insight is critical for obtaining a comprehensive view of network traffic, as well as additional context such as application-level awareness.

With metadata collected directly from infrastructure devices, Cisco Stealthwatch transforms the network into a powerful security sensor. Visibility scales across campus locations without relying on expensive probes. And the solution monitors traffic from specialized network devices, in classrooms and labs, that may not be compatible with endpoint-monitoring software.

Furthermore, the Stealthwatch Cloud License allows organizations to extend visibility and threat detection to public, private, and hybrid cloud environments. By deploying a lightweight agent, the solution can collect telemetry from the network and provide insight far beyond the campus.

This visibility dramatically reduces the time from problem onset to resolution and helps ensure that faculty, students, and staff always have access to the resources they need.

Security analytics and response

In addition to providing visibility, Cisco Stealthwatch technology transforms the volumes of collected telemetry from network infrastructure into actionable intelligence through powerful security analytics. College and university security teams then use this analysis to identify and counter network attacks and compliance violations.

Because traditional security solutions rely on signatures to detect threats, they overlook persistent and targeted attacks. Cisco Stealthwatch, however, monitors and analyzes network behavior and identifies suspicious activities for investigation. With this behavioral analysis, even the most evasive and sophisticated security incidents are quickly identified.

"Stealthwatch provides a holistic view of our network rather than a specific link or part of the network. The rich functionality together with the superb customer support gives us an excellent tool for combating security issues on the network."

University of Manchester

To achieve this intelligence, the solution builds a baseline of expected behavior on each network host and triggers alarms when anomalous activity is observed. If attackers or unauthorized users gain entry and perform unexpected or prohibited activities such as Peer-to-Peer (P2P) file transfers or breach attempts, Stealthwatch identifies these threats and alerts security responders.

This rapid response allows IT teams to dedicate more time to 24x7 application performance for course registration, research systems, and classroom technologies.

Incident and compliance investigation

Cisco Stealthwatch uses NetFlow to build a historic audit trail, which investigators can leverage to quickly uncover an incident's underlying cause. If malware is detected, the operator can identify the point of infection and track its propagation within minutes.

Additionally, after observing abnormal behavior such as long data center access times, network operators can quickly distinguish between network, server, and application issues, and determine the start time and duration of the activity.

The solution's audit trails can also help identify file sharing activity that violates copyright regulations upheld by the:

- Recording Industry Association of America (RIAA)
- Motion Picture Association of America (MPAA)
- U.S. Digital Millennium Copyright Act (DMCA)

Additionally, Cisco Stealthwatch can quickly tie host and network activity to the IP, username, and systems involved to track offenders and avoid violations or lawsuits. And the solution helps colleges protect Personally Identifiable Information (PII) and comply with the following government and private industry regulations:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- Higher Education Opportunity Act (HEOA)

“Stealthwatch has delivered a strong benefit to our organization, providing a fast return on investment.”

University of Chicago

Advanced endpoint awareness with Cisco ISE

The Cisco® Identity Services Engine (ISE), a complementary security solution, helps address the challenges associated with open networks through its highly secure network access and endpoint awareness.

When Cisco Stealthwatch is integrated with Cisco ISE, additional endpoint information, such as user, device, credentials, and security policy compliance, is woven into the network audit trail. Investigators can quickly identify the person and device type responsible for suspicious traffic.

Additionally, ISE simplifies campus guest access with automatic registration and access limitations. When needed, ISE can quarantine users and devices from the network after Cisco Stealthwatch identifies a compromised endpoint, leveraging the network as a security enforcer. This capability helps prevent the spread of infection until the issue has been investigated and remediated.

When integrating Cisco ISE and Cisco TrustSec® software-defined segmentation with Cisco Stealthwatch, the combined solution dramatically reduces the network attack surface. Cisco TrustSec assigns a Security Group Tag (SGT) to each user and endpoint based on their role, such as student, faculty, or staff. Administrators can then develop and enforce dynamic and adjustable SGT-based policies to restrict users from accessing unauthorized resources without disrupting network availability.

Learn more

Together, Cisco Stealthwatch, ISE, and TrustSec can help colleges and universities institute more secure and responsive networks that better protect their valuable data from today’s advanced threats. For further details on Cisco Stealthwatch, visit https://www.cisco.com/go/stealthwatch. To learn more about how to enable your education network with Cisco, go to https://www.cisco.com/go/education.

C22-739376-00 08/17