Solution Overview

Cisco Self-Defending Network for Education

At today’s colleges and universities, network applications have become an integral component of the academic environment and the institutional mission. Wired and wireless network connectivity, digital libraries, and increasingly, IP Communications and IP-based distance learning are now considered basic utilities, and must be just as reliable as a light switch or water faucet. But protecting network applications against constantly evolving threats – especially within an open academic network environment – presents major challenges. As a core component of the Cisco® Campus Secure program, Cisco Self-Defending Network for Education provides tools to better identify and mitigate network attacks, consolidate volumes of event data into a meaningful plan of action, and allow administrators to more proactively and effectively respond to security threats.

Challenge

College and university networks are complex, distributed environments that must serve a variety of stakeholders, often with widely different needs. Network challenges include:

- **Fundamental vulnerabilities** – IT administrators are hard pressed to ensure the security and availability of critical network applications while maintaining the open, unfettered learning environment that academic institutions require.
- **Evolving network attacks** – The tools to create and propagate network attacks have become more sophisticated and widespread, and are increasingly accessible to malicious parties both on and off campus. Propagation times are also shrinking. While network security personnel used to have days or hours to respond to new threats, today that window has shrunk to minutes or seconds.
- **Growing threats** – A recent survey conducted by The Chronicle of Higher Education and Gartner, Inc. revealed that nearly all respondents had experienced virus and worm attacks in the past year, and 73 percent said those attacks are accelerating. Fifty-three percent of respondents reported that attackers had tried to cripple campus networks, and 41 percent reported that hackers had succeeded in penetrating their systems.
- **Lack of resources to devote to network security** – In another recent survey of academic institutions by Emery University, 80 percent of respondents agreed that network security policies were very important, but only half were enacting measures to stem the tide of security breaches. Staffing and budgeting were cited as the main issues preventing further action.
- **Incomplete security systems** – Even a network with the strongest, most up-to-date antivirus software is not protected from “day zero” threats that attack campus networks before antivirus vendors have identified them.
- **Inherent complexity** – In an education network with hundreds of devices and thousands of active users at a given time, simply identifying malicious activity – much less mapping the path of an attack across compromised assets – can be extremely difficult. If the network contains security devices from multiple vendors, accurately identifying, correlating, visualizing, prioritizing, and responding to attacks in progress can be even more challenging.
- **Substantial potential costs resulting from a network attack** – If a security breach results in the compromise of thousands of user records, the notification effort alone can be a massive and costly undertaking. Stricter government regulations and privacy mandates also increase an institution’s legal exposure. Most importantly, a serious security breach can compromise student and faculty productivity, and tarnish an institution’s reputation.
Solution

Faced with these issues, many colleges and universities are searching for more comprehensive, proactive methods to protect academic networks. Cisco Self-Defending Network for Education (ATDEN) provides a suite of tools and services that tightly collaborate with the embedded security in Cisco network devices, and deliver the intelligence and functionality administrators need to protect education networks.

The Cisco ATDEN solution focuses on two critical areas of education security: timely identification and mitigation of security threats, and integration of security services into the network architecture itself. This strategy is based on two core technologies:

- **Cisco Security, Monitoring, Analysis, and Response System (MARS) appliances**, which provide comprehensive security monitoring and threat mitigation.
- **Cisco ASA 5500 Series Adaptive Security Appliances**, which combine firewall, intrusion prevention, application security, network antivirus, and VPN technology into a single device.

Cisco MARS Appliances

Cisco MARS appliances efficiently aggregate and synthesize the massive amounts of network and security data typically generated in an education network, and use sophisticated event correlation and validation intelligence to help administrators appropriately identify and respond to threats.

Cisco MARS:

- Automatically discovers the topology of the network, and uses this awareness to scan network devices for anomalous behavior and protect against day-zero attacks
- Tightly integrates and collaborates with security services embedded within Cisco network routers and switches to closely monitor network behavior
- Uses intuitive, drill-down topology maps to help administrators better visualize and respond to security events
- Provides tools to prevent, contain, or stop an attack in real time
- Supports rule creation, threat notification, and incident investigation processes, as well as a host of security posture and trend reports, tailored specifically for education networks
- Allows even administrators who are not security specialists to easily separate genuine attacks from false positives
- Allows administrators to classify false positives from a single, centralized platform, eliminating the need to fine tune individual appliances and services throughout the network
- Supports data collection and analysis from Cisco and non-Cisco devices alike, providing more comprehensive monitoring

Cisco MARS appliances are available in four sizes, depending on the security event processing power an institution requires.
Cisco ASA 5500 Series Adaptive Security Appliances

Past virus attacks such as the Slammer and Blaster worm attacks demonstrated how vulnerable educational institutions were to network attacks, and made many institutions recognize the importance of protecting the entire infrastructure, instead of just the network edge. Faced with such threats, today’s college and university networks incorporate a variety of security services, including:

- Firewall
- Virtual private network (VPN)
- Antivirus
- Web security
- Application security
- Intrusion detection and prevention
- Authentication
- Host-based security

Previously, colleges and universities had to rely on standalone solutions for each of these services (often from multiple vendors), which increased network complexity and demanded substantial human and financial resources. Today, colleges and universities are increasingly turning to converged network security solutions, in which all of these services can be delivered with a single, integrated platform.

The Cisco ASA 5500 Series combines world-class firewall features, IP security (IPSec) and Secure Socket Layer (SSL) VPN capabilities, and industry-leading intrusion prevention system (IPS) services with a centrally managed, user-friendly graphical user interface (GUI). The result is easier setup and management of security solutions, and more effective protection of education networks based on sophisticated, field-proven security technologies.

Like Cisco MARS, several sizes of Cisco ASA 5500 Series appliances are available, depending on the performance required.

For more information about Cisco MARS and Cisco ASA 5500 Series appliances, see the white paper “Self-Defending Network for Education Networks” at http://www.cisco.com/go/campussecure/.

Business Benefits

Cisco ASA 5500 Series and Cisco MARS appliances individually offer many intelligent tools to better identify and mitigate network attacks. When combined as part of the Cisco ATDEN solution, they provide a powerful, versatile, and highly manageable platform for delivering virtually any security function anywhere in the network.

The Cisco Self-Defending Network for Education solution provides:

- More comprehensive, effective network protection through intelligent reporting and analysis and robust threat detection and mitigation tools ideally suited for college and university networks
- Protection against both known and unknown threats, helping safeguard confidential data and ensure network availability
• **Lower total cost of ownership (TCO)** by reducing the number of devices in the network and allowing all security services to be managed and monitored from a single, unified platform

• **Simplified management** though a centralized, user-friendly GUI that allows even IT administrators who are not security specialists to manage and provision network-wide security services

### Why Cisco?

Founded by two Stanford University graduates, Cisco Systems® has maintained strong relationships with the world’s leading academic institutions. Working with Cisco, colleges and universities can:

• Employ end-to-end security to protect the campus network

• Rely on proven technologies, as well as partnerships with security industry leaders, to build a self-defending network

• Benefit from close collaboration among IP networking and security services, and tight integration with data, voice, video, storage, and wireless infrastructures

• Integrate and expand on security services within deployed Cisco routers, switches, and security appliances to reduce network TCO and deliver a greater return on investment

• Access the highest-rated service and support in the industry

• Realize long-term investment protection through a commitment from Cisco Systems to the Campus Secure program and its component technologies

### Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help to protect the network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of the institution. For more information about Cisco Services, see:


### For More Information

For more information about the Cisco Self-Defending Network for Education Solution, visit [http://www.cisco.com/go/campussecure/](http://www.cisco.com/go/campussecure/) or contact your local account representative.