

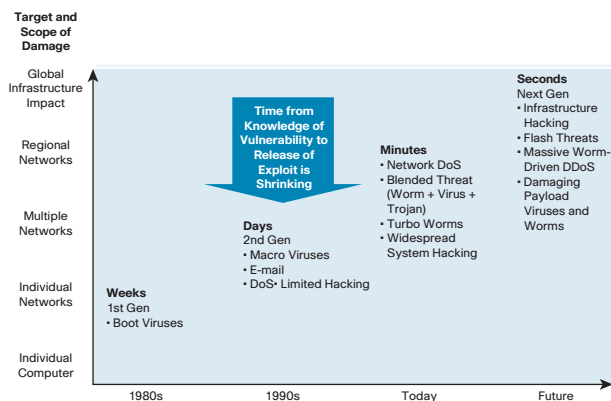
## Adaptive Threat Defense for Education

### Why Deploy Network Security?

Network applications have become tightly integrated into the core missions of today's educational institutions. Computer connectivity, digital libraries, and increasingly, IP Communications and IP-based distance learning are now considered basic utilities and must be just as reliable. But how can an institution protect critical applications while also providing an open, unfettered learning environment?

As a core component of the Cisco® Campus Secure program, Cisco Adaptive Threat Defense for Education provides timely identification and mitigation of security threats while allowing administrators to consolidate volumes of security event data into meaningful diagnostic information. With Cisco Adaptive Threat Defense for Education, network protection services closely collaborate with the embedded security in Cisco network devices, and allow administrators to more proactively and efficiently respond to security threats.

Figure 1. Security Issues in Education Continue



### Overcoming Obstacles

Today's college and university networks are distributed, complex environments that must serve stakeholders with widely different needs. This creates a number of challenges:

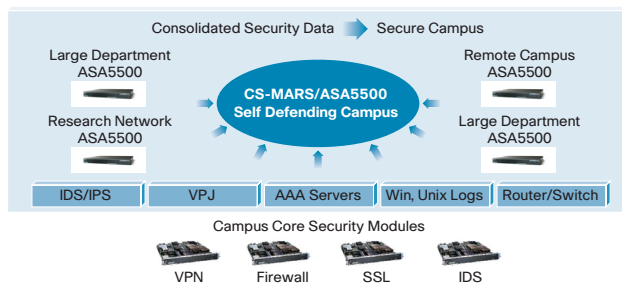
- The inherent openness of higher education networks creates an above average need for security.
- Network attacks have become more sophisticated, and the tools to create and propagate them more widespread.
- Propagation times are shrinking rapidly, from days or hours a few years ago to minutes or seconds today.
- According to a recent survey,\* nearly all institutions experienced virus/worm attacks last year, and 53 percent of those surveyed reported someone had tried to cripple campus networks. 73 percent say attacks are accelerating.

### Cisco Adaptive Threat Defense

With thousands of active IP flows in a college or university network, identifying and mapping an attack—much less correlating, prioritizing, and mitigating one in progress—can be very difficult. Cisco Adaptive Threat Defense for Education consolidates the multiple security services on network devices and employs mutual awareness among those services, allowing more unified, efficient network defense. The key components of the solution are:

- Cisco MARS (Mitigation and Response System) appliances, which provide comprehensive monitoring and threat mitigation.
- Cisco ASA (Adaptive Security Appliance) 5500 integrated security appliances, which combine intrusion prevention, application security, firewall, network antivirus, and VPN in a single device.

Figure 2. Consolidation of All Security Event Data



Cisco MARS appliances:

- Aggregate, correlate, and synthesize security event data from throughout the network, including devices from vendors other than Cisco.
- Intelligently scan data to identify anomalous network and application behavior, and help thwart even “day-zero” attacks
- Provide tools to prevent, contain, or halt attacks in real time, as well as accurately map and visualize an attack in progress
- Support institution-specific rule creation, event notification, and security posture and trend reporting

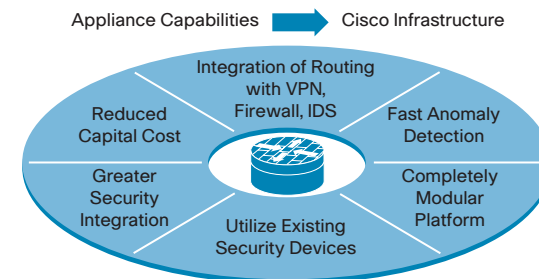
Cisco ASA 5500 appliances:

- Allow administrators to configure and manage world-class firewall features, VPN capabilities, and industry-leading intrusion prevention services via a straightforward graphical user interface
- Reduce complexity and total cost of ownership (TCO) of campus networks by converging multiple security services and devices into a single, comprehensive solution

### What are the Benefits of Cisco Adaptive Threat Defense?

- Robust security threat detection and mitigation ideally suited for open college and university networks
- Comprehensive reporting and analysis of security events
- Exceptional breadth and depth in campus network defense, supporting the needs of both Security Operations and Network Operations staff
- Flexible deployment and management of security services on existing routers, switches, and security appliances
- Protect against both known and unknown threats, helping safeguard confidential data and ensure network availability

Figure 3. Integrated Security Infrastructures for Self-Defending Education Networks



### Why Cisco?

Begun by two Stanford University graduates, Cisco Systems® has maintained strong relationships with the world's leading 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

\*Source: *Chronicle of Higher Education and Gartner, Inc., 2004*