BYOD Security Challenges in Education: Protect the Network, Information, and Students

BYOD Security Challenges in Education:
Protect the Network, Information, and Students

What You Will Learn

The influx of personal smartphones and tablets on campus, and the resulting data deluge, imposes a new set of security challenges. This white paper, intended for IT and network security specialists in schools and higher education, explains the security precautions needed on bring-your-own-device (BYOD) campuses:

- Protecting the network from malware and intrusion
- Controlling access to private information such as grades, tests, or payroll records
- Preventing illegal music and video sharing
- In K–12, complying with regulations such as the Children's Internet Protection Act (CIPA)
- Accomplishing all of this without adding to the IT team's workload

Cisco provides a comprehensive security architecture for campuses, helping schools take advantage of the mobile learning trend and BYOD to let students "learn your way.

Controlling Security When You Don't Own the Device

The boom in personal smartphones, tablets, and laptops on campus complicates cybersecurity. When schools owned all laptops and PCs connecting to the campus network, the IT team could install security software, such as antivirus clients, on the devices themselves. Access control, too, was relatively simple, because the IT team could provide access to the appropriate resources depending on whether the school-owned device was used by students, teachers, administrators, researchers, and so on.

But this device-centric approach to security comes up short in a BYOD world, where campus users expect to connect from anywhere, using any device. Keeping security software up-to-date on students' and employees' personal devices is not feasible, even if smartphones' battery life were not an issue. The more effective approach to mobile security is enforcing security policy in the network. Network-based enforcement makes the device and connection method (wired, wireless, or VPN) irrelevant.

In BYOD environments, the network needs the intelligence to:

- Automate enforcement of access policy, based on the context, including who is making the request, when, how they are accessing the network (wired, wireless, or VPN), and with what device. An elementary school's access policy might state that teachers, but not students, can access content sites such as YouTube. A university's access policy might give researchers access to certain applications or files from campus but not from home.
- Automatically detect and mitigate web-based threats, which can lead to security breaches or degrade wireless network performance.
- Make sure that private information, such as grades, tests, and salary information, is not compromised if a personal device is lost or stolen.
- Minimize management overhead by unifying policy definition on all networks, and providing ready visibility into the activity of all devices currently connected to the campus network.
- Protect the IT infrastructure, whether it's physical, virtualized or in the cloud.

Cisco Security Solutions for BYOD in Schools and Higher Education

Schools, colleges, and universities can address these BYOD security challenges by implementing the Cisco® BYOD Smart Solution, Cisco Virtualization Experience Infrastructure (Cisco VXI™) Smart Solution, or both.

Cisco BYOD Smart Solution

The Cisco BYOD Smart Solution is a holistic approach to effectively managing and controlling access while providing a consistently good experience for campus users. The solution includes Cisco validated designs, professional services, and the capabilities described in the following paragraphs.

Automated Enforcement of Access Policy

Knowing the identity of the person and the device accessing the network is the foundation for a BYOD security strategy. Until recently, campuses needed one solution for authentication, another for assessing the security posture of school-owned devices, and yet another for policy enforcement.

The Cisco Identity Services Engine (ISE) addresses all of these requirements in a single platform. It continually gathers real-time information from the network and devices, including iOS and Android smartphones and tablets, PCs, Macs, printers, fax machines, gaming platforms, wireless IP phones, and more. Then it uses the information to control access based on campus policy. For example, a policy might stipulate that only high school students can use iPads, or that faculty can access certain services only from campus.

The flexibility of the Cisco ISE is especially valuable in BYOD environments because the IT team can easily refine policy as the program matures. Some districts begin with BYOD for the higher grades, later allowing it for younger students. Some start by providing web access only, later adding learning applications.

You can even create policies for specific individuals. For example, a school IT team might restrict or block access to all services for a student who tries to hack into school databases or repeatedly attempts to access blocked sites on the school network as well as the Internet. Schools can offer access to web-based testing during a two-hour window. Or, a university might selectively grant access to certain systems to individual faculty members, researchers, and administrators, allowing them to work from anywhere.

Cisco ISE also minimizes the IT effort required to provide guest wireless access for visitors, such as parents, board members, guest lecturers, and so on. Many educational institutions want to limit guest access to browsing and checking email, and to keep guests off the network used for student information systems and other internal systems. Cisco ISE can automatically register guests, restricting traffic to a guest VLAN that provides Internet access only. This relieves the campus IT team from having to issue passwords.

Bowdoin College Upgrades Wireless Network to Support Influx of Personal Devices

Located near Portland, Maine, Bowdoin College enrolls 1730 students. Students, faculty, and staff have enjoyed wireless connectivity since 2004. The IT team expected students to return from winter break in January 2012 with double the number of devices. In anticipation, the college upgraded its Cisco wireless network to expand coverage across the 95-building campus, support a wider variety of devices, increase security, and improve the experience by mitigating sources of interference.

To increase performance as well as capacity, Bowdoin College implemented Cisco Aironet® 3600 Series Access Points, which provide up to 30 percent faster performance than other access points. Built-in Cisco CleanAir® technology scans the entire Wi-Fi spectrum for interference and security threats. Cisco Identity Services Engine (ISE) authenticates campus guests and grants them temporary wireless access. And Cisco Prime™ products minimize management overhead because the college IT staff can manage the wired and wireless networks from a single interface.

Secure VPN Access for Faculty and Staff Working Remotely

Faculty and staff who want to work with their personal devices from off campus can download the Cisco AnyConnect® Secure Mobility Client. The client software is available for different devices and operating systems, including iOS and Android, and enforces campus security policy for voice, video, data, and applications. Simple, always-on connectivity simplifies the experience for faculty and staff, and the IT team only needs to support one client, minimizing management overhead.

Web Security

Many of today's threats spread when people visit websites. Therefore, campuses with a BYOD policy need a solution for URL filtering, malicious code detection and filtering, and application controls for popular web-based applications.

Educational institutions can choose from several Cisco web security solutions that work at the network level to block access to malicious websites:

- Cisco ASA CX Context-Aware Firewall is best for educational institutions that want full firewall capabilities as well as controls for web, Skype, peer-to-peer, and voice traffic.
- Cisco Web Security Appliance is best for schools that want a dedicated web-security gateway with the most comprehensive web content filtering, for Children's Internet Protection Act (CIPA) compliance. The Cisco Web Security Appliance also provides anti-malware protection and data loss prevention.
- Cisco Cloud Web Security service is best for institutions that do not want to purchase and support a web-security device, or that have many mobile users. You can use Cisco AnyConnect Secure Mobility Client in conjunction with Cisco Cloud Web Security to automatically assess the safe status of a device when the user logs in, and then block malicious sites during the session.

Compared to other web security solutions, Cisco solutions have an advantage in blocking websites that are not yet reported as being malicious. One reason is that they all connect to the Cisco Security Intelligence Operations (SIO) service, which calculates a reputation score for websites by considering years of operation, ownership country, history of ownership, and more (see sidebar). Websites or web-page objects that receive negative scores are blocked. Other methods that Cisco solutions use to prevent web-based threats include blocking attempts by the site to install malware; warning campus users when they click a link to a website that looks suspicious; and enforcing common-sense policies such as blocking transfer of files over a certain size, often audio or video files.

Protection from Even the Newest Malicious Websites

Cisco Security Intelligence Operations (SIO) protects campus networks and keeps IT teams informed about emerging threats that could take down the network or enable hackers to retrieve confidential information. Educational institutions that implement Cisco web security solutions for their BYOD programs benefit from Cisco's US$100 million investment in the SIO, which funded:

- Cisco SensorBase: This threat-monitoring network captures threat telemetry from more than 700,000 Cisco sensors deployed globally, monitoring 35 percent of the world's email and web traffic. This live data is combined with a historical database of more than 40,000 vulnerabilities.
- Cisco Threat Operations Center: Five hundred security analysts conduct research on emerging threats 24 hours a day, every day, from offices throughout the United States as well as Australia, China, India, Israel, Ukraine, and United Kingdom.
- Dynamic updates: Updates are delivered to the school's Cisco security devices within a few minutes, often hours before other solutions, protecting the network against the latest threats.

Cisco Secure Wireless Infrastructure

The basis of a successful BYOD program is providing an excellent user experience while minimizing risk for the educational institution. Cisco Aironet 3600 Series Access Points enable students, teacher, and staff to connect from any device, even those with weak wireless signals, at a greater distance from the access point and with up to 30 percent faster performance than any other access point. Cisco Prime Network Control System (NCS) and Cisco identity Services Engine (ISE) support Cisco Aironet 3600 Series Access Points. Unified policy and access control in Cisco ISE and converged wired and wireless management in Cisco Prime Network Control System (NCS), together with Cisco wireless LAN infrastructure, simplify and help secure the mobile experience.

Cisco provides a suite of integrated tools that schools, colleges and universities can use to manage and enforce wireless security policies (Table 1).

Table 1 Cisco Solutions for Enforcing Wireless Security Policies

Security Capability	Cisco Solution
User authentication, encryption, and access control	Cisco Identity Services Engine (ISE)
Detection and containment of unauthorized wireless access points that well-meaning teachers or students have set up, most of which do not provide adequate security controls	Cisco CleanAir technology, embedded in Cisco Aironet wireless access points
Monitoring and detection of wireless network anomalies, unauthorized access, and radio-frequency (RF) attacks	Cisco Adaptive Wireless Intrusion Prevention System
Automated wireless security vulnerability assessment	Cisco Wireless Control System (WCS)

Enhanced CIPA Compliance for K-12

While Google, Bing, YouTube, Flickr, and other search popular search engines and content-sharing sites provide a safe-search option to block adult content from results, savvy students can easily turn off the option on personal devices. Schools can transfer control of the safe-search option from students to administrators by selecting the safe-search option on Cisco web security solutions.

Low Management Overhead

Campus IT staff can centrally manage all wireless infrastructure, including Cisco wireless LAN controllers and Cisco Aironet wireless access points, using Cisco Prime NCS. Having a single management interface minimizes management overhead, simplifies troubleshooting, and accelerates awareness of security issues.

Cisco VXI Smart Solution, Protecting Data Even If a Device Is Lost

To lower desktop TCO while also increasing data security, some educational institutions are replacing some or all physical desktops with virtual desktops that campus users can access over the network from any device, including personal tablets or laptops. Files are physically stored not on the device, but in the campus data center. This means a lost device does not lead to exposure of sensitive information such as student records or research results.

The Cisco VXI Smart Solution is an end-to-end solution for desktop virtualization and collaboration. Its unique advantage in BYOD environments is the ability to deliver not just virtual desktops, but a unified education workspace that also provides access to campus voice and video services on mobile devices.

Why Cisco?

Schools, colleges, and university's that use Cisco security solutions in their BYOD program gain the advantages of working with a leader in wireless as well as security technologies:

- In Gartner's Magic Quadrant for wired and wireless LAN access infrastructure, Cisco ranks first both for completeness of vision and ability to execute. [1]
- Validated designs and comprehensive services for planning, design, implementation, and optimization help educational institutions quickly introduce or scale their BYOD programs. More than 300 trained and certified channel partners are available worldwide.
- Cisco security architecture takes advantage of existing Cisco switches and routers. For example, if a student attempts to browse from a tablet, the Cisco ISE can detect whether the device is school-owned or personal, and communicate this information to switches and routers so that they can enforce the appropriate access policy.

Cisco VXI Smart Solution in Action

Volunteer State Community College, Gallatin, Tennessee

At Volunteer State Community College, in Gallatin, Tennessee, students previously had to come to campus to work with lab applications. Now the college hosts lab applications on Cisco VXI, and students can access the applications on personal devices. This is helping us make sure that online students get the same learning experience as onsite learners.

Utica City School District, Utica City, New York

Utica City School District implemented Cisco VXI to push lesson plans and online classroom materials to any mobile device connected to the district network. Students in the district can use several hundred netbooks to date for secure wireless access to learning materials. In one elementary school, students can use netbooks to connect to their virtual workspace during class.

For More Information

- To learn more about Cisco security solutions for schools, visit: www.cisco.com/web/strategy/education/SafeSecure_RiskSchools.html
- To learn more about Cisco solutions for education, visit www.cisco.com/go/education.
- To read the full case study on Bowdoin College, visit: www.cisco.com/en/US/prod/collateral/wireless/c36_702836_00_bowdoin_college_cs_v1a.pdf
- To read the case study on Utica City School District, visit: www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/utica_cs.pdf
- To read the case study on Volunteer State Community College, visit: www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps556/case_study_c36-717074.pdf

[1] Gartner, Magic Quadrant for the Wired and Wireless LAN Infrastructure, June 12, 2012, http://www.gartner.com/technology/reprints.do?id=1-1AX7YJQ&ct=120614&st=sb

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**