Protecting and Enabling the Digital Classroom

Cyber Security and Secure Information Access for Education

A technological revolution is underway in education, transforming how it is organized, delivered, and experienced by students and teachers alike. The ultimate goal is to make education richer, improve student outcomes, and enhance the lives of instructors, allowing them to be more effective.

However, with this transition come significant challenges. Delivering innovative education services online leverages immense amounts of students' personal, as well as university proprietary, data. A staggering number of personal devices are now connecting to campus networks to access material and collaborate with teachers and students. In addition, the education sector is leveraging the cloud more quickly than other industries, as digital content and curriculum relies heavily on cloud adoption.

In this complex and evolving environment, IT must protect the network and data against malware and secure the integrity of the institute's systems, even in the cloud. This includes effectively managing and controlling access, while simultaneously providing a consistently good experience for campus users.

Increasingly sophisticated Advanced Persistent Threats (APTs) are continuously threatening to steal students' identities and other critical information. To protect against incursions, advanced security tools that detect and block stealthy and continuous hacking processes before they present a significant risk to the network are needed.

SECURE INFORMATION ACCESS AND CYBER SECURITY BEST PRACTICES FOR EDUCATION

Understanding security best practices and adopting a combination of security technology solutions and policies at all levels of the organization can effectively protect the infrastructure and its data. The following best practices help ensure that systems and people are legitimate and authorized to access the school's systems and information and protect the school's systems and data.

User Authentication

User authentication employs identity verification to ensure that the person accessing the data is who they claim they are and has access authority. Access protocols should be based on two-factor authentication that requires the system to have digital certificates to validate someone's legitimacy. Systems can do this by requiring users to have two or three different credentials, including a PIN or password, plus biometric identification or a security fob, for example.

Cloud-based services can help with access control by issuing, renewing, and revoking digital certificates that can be used to power strong authentication, encryption, and digital signing applications. An administrator can configure and monitor a tool like this from any modern web browser. For schools that require external students to access systems, a third-party authentication source can provide the second factor in proving an identity using a public credential repository for authentication along with two-factor authentication, for added protection.

Encryption

In the event of a data breach, educational institutions that have data on desktops, laptops, and removable storage devices encrypted in line with regulations will not be subject to penalties. Advanced data and file encryption for these computers and devices can provide scalable, enterprise-wide security that prevents unauthorized access by combining powerful encryption with strong access control.

Secure Endpoints and the Infrastructure

Network security alone isn't going to solve the problem. Adversaries are targeting all control points from the gateway to email to the endpoint. Organizations must know exactly where sensitive data resides, including all servers and end-points, and then secure those

points. Security practices should employ a layered data loss prevention methodology that focuses on protecting the infrastructure, the data center, and all endpoints. In addition to data loss prevention (DLP), education IT teams should consider intrusion detection and prevention services (IDS/IPS) and access control systems.

Single Point of Control

Maintaining a single, secure access point to cloud applications and services is increasingly important as curriculum and educational resources are digitized and moved to the cloud. A cloud-based data loss prevention (DLP) solution can identify specific information that needs to be protected—and then help make decisions on how to secure that information. In addition, organizations should make sure the data stored in the cloud is encrypted.

Anti-malware

Even secure data can be subject to malware or virus attacks. Therefore, it's imperative that antivirus monitoring be implemented. This provides preventative intelligence that can thwart phishing, watering hole, and other potentially dangerous attacks that often lead to a breach.

eDiscovery

With these safeguards in place, a breach is less likely, however, a security program should also include an eDiscovery component. In the event of a breach, eDiscovery auditing makes it easy for IT and legal professionals to classify and retrieve pertinent emails and general files.

Managed Security Services

Schools can take their security controls to the cloud, reducing both risk and costs, by leveraging a third-party managed security service. These services aggregate and correlate system logs, stretching to help incident responders identify malicious activities and allowing the institution to successfully protect against Advanced Persistent Threats (APTs) as well. A managed security service correlates alerts and intelligence across a range of security technologies to deliver more comprehensive attack prevention. When security technologies work together, the complex fight against advanced threats becomes a manageable function that delivers stronger protection and more value to the organization.

SYMANTEC SECURE INFORMATION ACCESS AND CYBER SECURITY SOLUTIONS FOR EDUCATION

Schools must invest in information security and management today so they can realize the exciting educational future of tomorrow. Symantec helps IT manage and protect data and secure the infrastructure, so that educators can focus on using technology to improve student performance and support learning. Created specifically with the needs of primary and secondary institutions in mind, Symantec helps ensure highly-available and secure access to resources and protection from security risks. Solution options provide immediate cost savings through a new licensing program based on Full Time Employees (FTEs) rather than per-device models, in accordance with the education budgeting process. Symantec's powerful arsenal of data loss prevention, file sharing, encryption, and authentication solutions keeps the focus on personalized learning rather than information security.

More Information

Visit our website

go.symantec.com/education

To speak with a Product Specialist in the U.S.

1 (800) 745 6054

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 billion. To learn more go to *www.symantec.com* or connect with Symantec at: *go.symantec.com/socialmedia*.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com