Unifying Cybersecurity in Education

The end-to-end approach to protecting your learning environment—across any app, any cloud, and any device

Introduction

With the rise of the digital campus, cybercriminals don’t have to look very hard for new places to attack. Online courses, virtual labs, electronic student records, and the widespread use of personal devices are all opening the door to new threats. The result is that cyberattacks are growing in volume and effectiveness. Studies found that in 2019, there was a surge of ransomware attacks on universities, colleges, and school districts, with 89 notable attacks.¹

The bad news is that the academic sector is highly vulnerable, and the bad actors are taking note. Cybersecurity is the top priority for educational IT leaders according to CoSN (the Consortium for School Networking).² Many schools and campuses may be even more at risk due to overextended IT staff and limited funding.

Meanwhile, when it comes to security solutions, the complexity is higher than ever. Thousands of security vendors promise to have the silver bullet for security, and the landscape is awash with a multitude of products and agents to address different threat vectors. Security and IT teams make their decisions in silos—and with no big-picture view of the environment they’re trying to protect. It’s beyond time for a unified approach.

This white paper will explore why cybersecurity needs to be a team sport, aligning your people, processes, and technology to defend against the latest security threats. We’ll look at the key elements needed for a unified approach, and how the comprehensive security platform from VMware can help.

Security Challenges for Today’s Digital Campuses

Cybersecurity threats and high-profile data breaches are a top concern for today’s institutions, and the stakes just keep growing higher. There are more devices and apps on campuses than ever, and IT must protect the identities associated with them as well as the networks that they access. What’s more, increased collaboration between academic institutions and private or governmental partners means that you need more robust intellectual property protection—and more protection from malicious threats like ransomware.

In fact, a recent EDUCAUSE study found that 79% of institutions are concerned about the exposure of confidential or sensitive information, and for good reason. In early 2019, hackers accessed the admissions databases for three colleges—Oberlin College in Ohio, Grinnell College in Iowa, and Hamilton College in New York—and demanded thousands of dollars for stolen information.³ This type of data breach can ruin the trust of students, faculty, and staff as well as the reputation of the institution.
Meanwhile, academic institutions are faced with lots of complexity in securing their infrastructure. Disparate products, agents, and interfaces make it difficult to manage vulnerabilities. The solution sprawl can create more overhead that impacts performance. What’s more, key decisions are made by siloed IT and security teams, reacting to threats without a holistic view of the applications, data, infrastructure, and devices that they’re trying to protect. Network security is approached differently from endpoint security, which is different from cloud security, and so on.

The interesting thing is that IT and security teams are aligned on the greater goals of preventing breaches, increasing efficiency, and speeding incident resolution. The teams just don’t work together very well. According to a recent Forrester study, 77.4% of respondents said their IT and security teams currently have a negative relationship. What’s the solution?

**Strengthening Security with a Unified Approach**

To strengthen your cybersecurity posture, your entire institution needs to approach security like a team sport. It’s more important than ever to have unified visibility and control across your critical networks, workloads, and endpoints. Your busy IT and security teams need to be able to work together, using a single source of shared truth. The only way to stay ahead of ever-changing threats is with a unified platform—enabling you to zero in on vulnerabilities and mitigate them, before any damage can occur.

Following are three key tactics for building an effective security playbook.

**Tactic #1: Security needs to be built-in, not bolted on**

Too often, security is approached like a game of “whack-a-mole,” with isolated solutions being deployed in response to the latest threats. Many organizations have dozens of security solutions that require independent configuration and monitoring. This increases complexity and risk.

For maximum effectiveness, security should be built into the infrastructure you already have, creating a superior vantage point for threat detection. Your institution should be able to unite around a single platform with a holistic view—reducing the number of products, agents, and interfaces that your teams need to manage, and lowering the chances for error. This platform should help protect against lateral vulnerabilities as well as north-south threats with a “zero trust” approach, where all traffic is considered untrusted until proven otherwise. Built-in integration across control points also provides even greater control.

**Tactic #2: Security needs the context of what you’re trying to protect**

In today’s digital learning landscape, a defensive security strategy is a must. Balancing student privacy with online learning tools and BYOD policies has created high cybersecurity stakes. Your security policies are more effective if you have deep visibility into your applications and data—and what’s “normal” behavior. That way, you can detect anomalous behavior before it can become a threat.

Consider if your security solutions include real-time device assessment and remediation, endpoint detection and response, and application control capabilities that address the entire protection cycle for endpoints and workloads. Continuous diagnostics and monitoring can help you fight back against emerging threats. For added protection, your solutions should also be backed by real-time threat intelligence that suppresses intrusions before they can be deployed.

### TOP 5 CYBERSECURITY BEST PRACTICES

1. **A baseline security assessment** is critical for knowing where vulnerabilities exist, whether you opt for a baseline “Red Team” or “Purple Team” audit and/or cyber hunt exercise. Penetration tests and general audits are also recommended.

2. **Network microsegmentation** is an ideal strategy for limiting lateral movement across the network. Microsegmentation divides your data center into distinct security segments, reducing the reach of an attack if one occurs.

3. **Endpoint detection and response** technology, along with application control (whitelisting) on critical servers, can help detect and remediate advanced attacks. Overall, endpoints are the easiest attack surface for hackers.

4. **Integration of third-party threat analysis** puts your organization in an active position, rather than reactive, and goes well beyond simply responding to alerts. Trusted user communities can also help you get an edge on cybercriminals.

5. **Security training and recruitment/retention of talent** helps ensure your organization can stay protected, while also knowing how to remediate vulnerabilities.
Tactic #3: Security needs flexibility to support your unique mission

Every institution has its own unique goals, needs, and challenges. Taking a “one-size-fits-all” approach to security simply won’t work. Ideally, your institution should have flexible choices for a security stack and prevention protocols. Security solutions need to be effective for your specific workloads, endpoints, networks, clouds, and identity policies—so you can harden potential entry points and proactively immobilize threats.

Your security solutions should also prioritize ease of use and integration. This enables you to break down silos between security and IT teams, while controlling shadow IT and improving manageability. An extensive partner ecosystem is also essential for making the most of your existing security and technology investments. This way, you can accelerate your digital strategy, enable new teaching models, and deploy remote learning securely for ongoing success.

Transform Security with VMware

In a world of ever-changing threats, VMware is the right partner for protecting your institution and your students. VMware helps unify your teams with a comprehensive security portfolio, now including VMware Carbon Black. We provide you with a complete platform approach for continuous diagnostics and mitigation—delivering end-to-end visibility, protection, and system hardening across the network, data center, and endpoint hosts.

Find out how to secure your critical applications, users, and devices, backed by leading threat detection and response capabilities, and be better prepared for what’s next.

Sources

Join us online: 🌐 Leer más

LEARN MORE

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. 10/20