Addressing Security Risk in Higher Education

November 2020
Table of Contents

The Decentralized Campus 3
Higher Education Headaches 4
A Practical Approach to Securing Higher Education Institutions 7
Introducing SentinelOne Singularity™ XDR Platform 9
Protect Against Ransomware Attacks 10
Get Complete In-Depth Visibility 11
Secure Devices with SentinelOne Ranger 12
SentinelOne for Higher Education 13
The Decentralized Campus

Unprecedented, unpredictable, and transformational. Those are three words that can be used to describe 2020. This year has seen the evolution of traditionally brick-and-mortar industries like education move to virtual environments. As schools and the education sector shift to hybrid and digital classrooms, they also potentially become a prime target for cyber attacks.

Security leaders need to consider

- What are the new challenges in a connected classroom?
- How can schools continue to protect sensitive student data?
- How BYOD affects school’s capabilities to protect themselves?
- Higher education institutions have seen some of the largest staff scale backs in 2020. With less security analysts on staff, how can they protect themselves against cyber attacks?
Higher Education Headaches

Modern ways of learning pose unique cybersecurity and IT challenges for colleges and universities.

1. Malware Threats

Before the digital revolution, classrooms used to be strictly pencil, paper, chalkboard, and chalk environments. Now, teachers and students alike are using iPads and laptops, Smart Boards, smart notebooks, and more. With all of these devices, security leaders need to keep up with the security demands but there are simply too many to keep track of in a connected environment. The simple fact that any one of these devices can be subjected to cyber threats is one of the many things that keeps security leaders up at night.

Malware represents one of the greatest cyber threats to all organizations, including higher education. The near exponential rate at which new malware variants are released, alongside the inherent limitations of the traditional defenses, is resulting in a high risk of infection. Ransomware attacks have disrupted many education institutions like University of Utah, Michigan State University, and the University of California, to name a few.

27 institutes of higher education in the United States, Canada, and Southeast Asia were attacked recently by nation-state hackers looking for military secrets


Higher education sector may receive as many as nine times the number of cyberattacks as experienced by the average organization.

2. Challenges with BYOD (Bring Your Own Device)

Most schools provide laptops or iPads for their students, but when we look at universities and colleges, students are often tasked with carrying their own. This means that on every college campus, there are hundreds of thousands of students and professors connecting to the main network using unsecured devices. While this doesn’t seem like a large threat, it becomes a bigger problem when one considers that with one simple action, like printing a term paper in the library, that student would gain access to the enclave, network and so can any malicious threats in the student’s computer.

Security leaders are tasked with solving an unsolvable problem. Without asking every single student and administrator who connects to the school’s network to download a security solution, those devices remain a threat to the school as a whole. Access to the network isn’t the main issue, it is what happens once someone is connected that is the real threat.

3. Staffing Levels and Budget Constraints

The travel and retail industries aren’t the only ones to see budget cuts and staffing cuts as a result of the pandemic and economic downturn. For higher education, especially public colleges and universities, the plummeting enrollment rates, debts, and the unprecedented turn of 2020 have forced them to not only slash their budgets but also cut staff. Take into consideration the fact that as these campuses attempt to reopen and adjust to the new normal, they will have to invest millions of dollars in actions to prevent the spread of COVID-19.
Security leaders in higher education are now having to make do with tighter budgets and smaller staff. This means that analysts and engineers will have to take on the roles of several people if they want to get ahead.

According to a recent Boston Globe piece about the effect of COVID-19 on higher education:

“Many experts have compared this crisis to the 2008 economic crash, but it is different in one key way. This time, the institutions most damaged by the crisis will not be the elite schools whose endowments were decimated by that stock market crash but the more typical colleges that enroll the vast majority of students in this country.

With all of these challenges plaguing the higher education arena, what can CISO’s and security leaders do to keep up?
A Practical Approach to Securing Higher Education Institutions

Cybersecurity is far from easy, especially for higher education. Like healthcare, higher education involves so many connected devices with their own individual risks that it becomes nearly impossible to keep track of the threats that they each individually might pose to the institution.

Also like healthcare, higher education institutions need to be more wary than most potential breaches because of the extensive Personally identifiable information (PII) they hold on their staff and students. Let’s look at some of the strategies that higher education security leaders should take advantage of, in order to stay ahead of the threat landscape.

1. Gain Control Across Endpoints and Cloud

With all of the connected devices present on campus, it’s impossible to have eyes on all of them. Security must move to the endpoint and everywhere that the data lives and is accessed. A solution that is specifically designed for the endpoint, cloud, and IoT will protect your enclave network from threats posed by connected devices. By securing endpoints (entry points) of end-user devices, the solution becomes an umbrella helping to protect the most vulnerable asset a campus has: data. Whether it’s
unintentional or simply a bad actor attempting to find entry points in a school’s suit of armor, endpoint security that uses machine-learning and automation helps repel those attacks before they have a chance to gain access to student and staff PII.

2. **Mitigate Threats with Proactive, Real-time Detection and Response**

Detection and response is an important part of any defense strategy. Even the most robust security model will experience a breach, so planning for this inevitability is crucial. Protecting higher education endpoints in real-time can reduce and eliminate the dependency on human intervention. The benefit of this is that with the right solution, it will have a machine learning algorithm in place that learns of past, present, and future threats and block those threats immediately before they have the chance to do any real damage.

3. **Empower Security Teams with Automated Endpoint Security**

As mentioned earlier, one of the major issues that’s becoming more prevalent as the year continues is the staff cuts, especially in the tech arena for higher-education. Leaders are now having to level-up junior security analysts or ask their advanced teams to carry a heavier load in order to keep up with potential and current cyber threats. Instead of burdening security analysts with more work, look for solutions that include automated threat detection and response so that the university can react to perceived threats within seconds. With the right solution, turn every device into a sentinel that can map and enforce the enterprise IoT footprint. Using AI algorithms, devices can self-defend and ultimately heal themselves by stopping malicious threats in their tracks and remediating where they need to.
Introducing SentinelOne Singularity™ XDR Platform

SentinelOne for Higher Education
Secure your valuable student, faculty and staff data and intellectual property.

The SentinelOne Singularity XDR Platform combines next-gen prevention and EDR capabilities in a single Sentinel agent to achieve autonomous EPP at machine speed. Singularity delivers differentiated endpoint protection, endpoint detection and response, IoT security, cloud security, and IT operations capabilities - consolidating multiple existing technologies into one solution.

SentinelOne empowers universities and higher education security teams with a more efficient way to protect information assets against today’s sophisticated threats.
Protect Against Ransomware Attacks

Legacy AV and first generation EDR had their day. Modern fileless attacks require distributed intelligence that operates autonomously at the endpoint, to thwart attacks early in their progression.

+ Behavioral AI monitors the endpoint and limits the spread
+ Storyline™ technology auto-correlates events and maps to MITRE, accelerating triage
+ Patented 1-click remediation surgically removes malignant events

SentinelOne is a next level product that insures me that our endpoints are secure and my co-workers have all the freedom on the devices.

SECURITY AND RISK MANAGER
Higher Education
Get Complete In-Depth Visibility

Going beyond traditional antivirus and EDR solutions, ActiveEDR, powered by SentinelOne’s patented Storyline™ technology, allows security teams to quickly understand the story and root cause behind threat actors and autonomously respond to them.

Storyline™ automatically contextualizes all OS process relationships every second of every day and stores them for future investigations.

With SentinelOne, everyone from advanced SOC analysts to novice security teams can visualize and understand the attack storyline without spending hours recreating the storyline by hand. The SentinelOne agent is also able to automatically remediate and rollback the actions of the threats with a single button click. This technology empowers security teams to focus on the alerts that matter and leverage technology to assist in what before was limited to human mandated tasks.

+ Detect and stop advanced attacks
+ Understand the root cause and attack storyline
+ Empower your SOC team

"Must-have endpoint protection!"

Gartner peer insight:

CISO
Education, 3B - 10B USD
Secure Devices with SentinelOne Ranger

A single, compromised device on a university campus can become an adversary’s operating base for reconnaissance, lateral movement, and a breach.

SentinelOne Ranger transforms every Sentinel agent into an array of distributed network sensors, automatically and autonomously protecting the campus infrastructure from IoT attacks and compromised devices. No extra hardware. No network changes. No manual traffic analysis.

Ranger is the easy button for network visibility and control.

Just turn it on. 1-click simple.

“A superb EPP/EDR agent and a good security partner! [sic]”

INFORMATION SECURITY ENGINEER
Education, 3B - 10B USD
SentinelOne for Higher Education

Higher education institutions have a tough road ahead of them in the wake of the COVID-19 pandemic, but it can be made easier by utilizing a cybersecurity solution that is purpose built to prevent tomorrow’s threats.

**Autonomous EPP + EDR**
Real-time detection and remediation of modern attacks at the endpoint, at machine speed, and without human intervention.

**Unprecedented Visibility**
Contextualize and identify threats in real-time. Storyline™ technology reduces manual effort and automatically strings together related events in an attack storyline.

**Frictionless Threat Resolution**
Patented Storyline™ enables 1-click remediation and rollback to accelerate recovery to real-time. Storyline Active Response or STAR™ provides proactive detection and response. For threat hunters and responders, remediation is integrated as a standard EDR response.

**Simplified Experience**
One agent consolidates security functions and reduces agent count. One console unifies administration of devices and cloud workloads. Fast to deploy. Easy to manage.

**Exceptional Customer Experiences**
Customers are our #1. The proof is in our high customer satisfaction ratings and net promoter scores that rival the globe’s best companies.

**SentinelOne Vigilance**
Get answers, not alerts, with our managed detection, investigation and response service.

To learn more, speak with an expert, or request a demo, visit us at www.sentinelone.com
More Capability, Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?
Contact us

sales@sentinelone.com
+1-855-868-3733

sentinelone.com