DOES YOUR CAMPUS CYBERSECURITY PASS THE TEST?

SAFEGUARD HIGHER EDUCATION ENDPOINTS
WITH HP WOLF SECURITY

At first glance, the statistics seem puzzling: Over the past two years, the industry hardest hit by cyberattacks isn't banking. Or retail. Or even government. It's education.[1]

In 2020, 44% of the world's educational institutions were targeted by ransomware,[1] with three US colleges hit by NetWalker attacks in a single week.[2] In March 2021, the FBI issued a warning to US schools about the PYSA (Protect Your System Amigo) ransomware that eventually afflicted organizations across 12 states.[3] In September 2021, Howard University lost two days of online teaching to an unnamed ransomware attack that took down the school's Wi-Fi network and sent IT teams scrambling to restore data from backups.[4]

It's clear that attacks against educational institutions are becoming more numerous, more sophisticated, and more expensive. But why are hackers coming after colleges, instead of more obviously lucrative and strategic targets? And more importantly, how can HP Wolf Security help protect your university, community college, or trade school from becoming the victim of a breach?

> "THIS IS A GROWING THREAT, AND WE STRONGLY ENCOURAGE SCHOOLS, COLLEGES, AND UNIVERSITIES TO ACT ON OUR GUIDANCE AND HELP ENSURE THEIR STUDENTS CAN CONTINUE THEIR EDUCATION UNINTERRUPTED."
>
> PAUL CHICHESTER
> Director of Operations,
> UK National Cyber Security Centre[5]

SCHOOLS ARE THE SUBJECT OF INCREASING CYBERTHREATS

5.8M
malware attacks occurred against educational institutions from mid-August to mid-September 2021[1]

80%
of education malware attacks in 2020 were ransomware attacks[6]

1,681
US schools, colleges, and universities experienced ransomware attacks in 2020[1]

US$2.7M
was the cost of an average ransomware attack for educational institutions in 2020[1]

DOES YOUR CAMPUS CYBERSECURITY PASS THE TEST?

WHY HIGHER ED IS HIGH ON THE HACKER SYLLABUS

Breaching public and even private colleges seems like an unlikely objective for a cyberattacker's malware attentions—after all, many are nonprofits. But global threat tracking shows that education is actually the most affected sector, even compared to business and professional services, retail and consumer goods, and high tech.[7]

Why? The combination of two factors makes your educational environment an appealing target: vulnerability and value.

By their very nature, institutions of higher learning are an open book of access and collaboration,[4] creating many points of entry for a cyber pathogen. And after it's inside the network, malware can enable threat actors to gain access to everything from classroom platforms to systems that contain student records and employee personnel data[8]—including personally identifiable information such as financial data, medical records, and Social Security numbers.[9] Potentially even more valuable is access to cutting-edge research data from university R&D projects worth nearly US$84 billion annually.[10, 11]

Threat actors also know that public educational institutions are more likely to comply with ransom demands,[1] which could be why they are breached more often than private institutions.[12] Even more alluring targets are schools with robust cyber insurance policies.[13]

"COLLEGE CAMPUS NETWORKS ARE NOTORIOUSLY INSECURE, IN PART BECAUSE A LOT OF DIFFERENT PEOPLE AND VISITORS NEED TO CONNECT TO THE NETWORK, AND IN PART BECAUSE UNIVERSITIES TEND TO PLACE A PREMIUM ON OPEN COLLABORATION AND ACCESS TO INFORMATION."

JOSEPHINE WOLFF
Cybersecurity professor and Future Tense contributor[4]

RANSOMWARE—THE MOST COMMON TOOL IN THE HACKER BACKPACK

Malware can take many forms, but ransomware is the most significant emerging threat in the education space—mainly scareware, screen lockers, and encrypting ransomware. But all ransomware takes the same basic approach: Gain illicit access to or control of the victim's systems and data, then either block access or threaten to disclose or sell confidential data unless an extortion payment is made.[14]

In a textbook example, when hackers attacked the University of Colorado and University of Miami, they used Clop ransomware to steal student grades and Social Security numbers, then issued a US$10 million ransom demand before posting screenshots of the stolen files on a leak site. Clop—which is typically seeded to unsuspecting users through either spam email or in combination with manipulative social engineering techniques[1]—can halt Windows processes, uninstall existing security software, and then run its own encryption routine to lock victims out of their systems and data.[15]

NetWalker—or MailTo—which hit Michigan State University, the University of California-San Francisco, and Columbia College in Chicago in the span of one week in June 2020, encrypted data and renamed files with the developer's email address and an extension made up of the victim's unique ID.[2]

Because the University of California-San Francisco data that was breached and encrypted by hackers was from the College of Medicine and described in a campus news article as "important to some of the academic work we pursue as a university serving the public good," the school negotiated a reduced ransom payout of US$1.14 million.[16]

RANSOMWARE ATTACKS ON COLLEGES

DOUBLED

BETWEEN 2019 AND 2020[13]

"THEY'RE [COLLEGES AND UNIVERSITIES] JUICY TARGETS BECAUSE THEY HAVE STUDENT DATA, THEY HAVE RESEARCH INFORMATION, AND THEY HAVE CRITICAL OPERATIONS THAT NEED TO OPERATE ON A VERY STRICT TIMELINE. THEY CAN BE EXPLOITED ON MANY FRONTS."

GILMAN LOUIE
CEO of LookingGlass[13]

THE CHALLENGES OF SECURING THE MODERN CAMPUS

As costly and disruptive as malware and ransomware attacks are for higher learning, why aren't universities and colleges doing more to defend against them? It's because the web of vulnerabilities in today's distributed campus environment is complex, and keeping an eye on every front is a lot for IT teams to manage.

THE CAMPUS IS NOW DECENTRALIZED—AND SO ARE THE THREATS

A survey of universities found that two-thirds will allow staff and employees to work remotely from anywhere for three to all days of the work week.[17] That scenario creates a lot of unsecured networks[9] and unmanaged endpoints—and cybersecurity incidents—to monitor.

EMPLOYEES ARE RETURNING TO CAMPUS WITH OUTDATED DEVICES

As staff and employee devices migrate between home and campus networks, PCs are getting out of sync with security updates. Often, these devices are not able to connect easily to centrally managed and controlled security services, network proxies, or cloud-based browser protection solutions. When they reconnect with the school network, those unpatched devices bring vulnerability, including potential access to system-level privileges that enable hackers to steal data or install malware.[1]

MORE CLOUD-BASED PLATFORMS MEAN MORE ATTACK VECTORS

From curricula and proctoring sites to video chat tools, online platforms offer convenience in the best of times and essential access in difficult ones. But they also offer cyber actors new points of attack:[1] Half of surveyed education IT leaders identified security and privacy as the biggest challenges in making the move to the cloud.[18]

NOT ALL HACKERS ARE CREATED EQUAL

When a higher ed institution is cyberattacked these days, it's unlikely by a solo hacker out to make a name for themselves with a virus or nuisance malware. It's far more likely to be by a foreign government or organized crime ring using sophisticated techniques to steal valuable research data or students' personal information.

In 2020, government agencies in the US, UK, and Canada warned officials at universities researching COVID treatments that they were being targeted not only by Russian hackers but also by hackers backed by the Chinese government.

IT TEAMS CAN'T FIGHT A BREACH THEY DON'T SEE

With more faculty devices spread across more places, your attack surface is increasing, even as your overstretched IT resources aren't. Trying to monitor all the systems, software, PCs, printers, and IoT edges accessing your network is virtually impossible without the assistance of self-managing device security. The sheer volume of alerts and the skills required to make effective use of these solutions require a dedicated team to monitor, review, and act on the thousands of alerts generated each day. By the time you know that you have a problem, you already have a BIG problem.

"CRIMINAL ORGANIZATIONS OPERATE LIKE REGULAR BUSINESSES IN THAT THEY WILL KEEP ON DOING WHATEVER THEY'VE FOUND TO WORK. THE EDUCATION SECTOR HAS PROVED TO BE PARTICULARLY PROFITABLE, SO THEY WILL KEEP TARGETING THEM OVER AND OVER AGAIN."

BRETT CALLOW
Threat analyst at Emsisoft[13]

86% OF BREACHES ARE FINANCIALLY MOTIVATED

10% ARE ESPIONAGE[8]

WHY TYPICAL ANTIVIRUS NO LONGER MAKES THE GRADE

It's not just the perpetrators of cyberattacks that have changed—so have their techniques. While higher ed institutions face run-of-the-mill viruses, Trojans, and worms every day, over the past few years IT teams have begun combating a new class of advanced threats that sail right past traditional detection-and-blocking security defenses.

Rather than trying to penetrate enterprise-level networks by targeting servers of interest directly, cybercriminals now attack endpoint devices. They know all too well that user behavior and outdated device protections are the weakest links in your network. And after they're compromised, these devices can serve as launchpads for advanced persistent threat (APT) campaigns, which can spread throughout the network, exploiting servers where valuable data can be exfiltrated or held hostage.

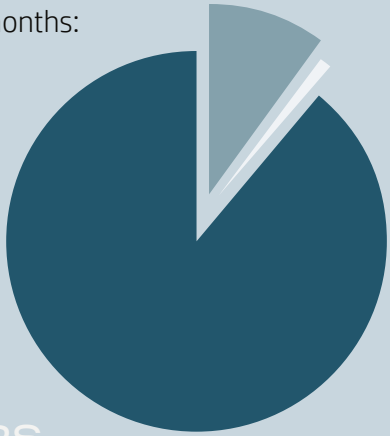
CYBERATTACKS ARE EVOLVING...

80%
OF ATTACKS ARE ZERO-DAY THREATS[19]

60%
OF ATTACKS ARE MISSED BY ANTIVIRUS PROGRAMS[19]

...BUT AWARENESS IS NOT

Most threats require human interaction to be successful. Of the threats isolated by HP Wolf Security in recent months:



89% WERE DELIVERED BY EMAIL, 11% VIA INTERNET DOWNLOADS, <1% THROUGH OTHER VECTORS

>99%

of email messages distributing malware require following links, opening documents, or accepting security warnings.[20]

ZERO TRUST IS THE ANSWER

Zero trust is a crucial tool in the fight against cyberthreats. The principle of zero trust is, as the term implies, to trust nothing at face value and to verify everything that can be verified. It leverages user and device identities, firmware and software configurations, and broader contextual information to make security and access decisions.

EDUCAUSE REVIEW: 3 CORE PRINCIPLES UNDERLYING THE CONCEPT OF ZERO TRUST IN HIGHER ED[14]

In June 2021, the higher ed IT journal EDUCAUSE Review succinctly defined the tenets of zero-trust security in its article "The Increasing Threat of Ransomware in Higher Education."

VERIFY EXPLICITLY

"Zero trust closes gaps in multifactor authentication (MFA) coverage by requiring explicit verification across the network. Instead of assuming trust based on weak assurances like network locations, zero trust uses all available data—identity, endpoint, and network data—to authenticate all access requests, no matter where they come from or what they're accessing."[14]

LEAST PRIVILEGED ACCESS (LPA)

"Zero trust makes it harder for attackers to negatively impact key systems and data by limiting users' access to the resources, devices, and environments they need. Without widespread privileges and access, attackers have fewer opportunities to move laterally within the network beyond an initial breach."[14]

ASSUME A BREACH

"As a final fail-safe, zero trust operates under the assumption that a breach has already happened or soon will. This means deploying redundant security mechanisms, collecting system telemetry, using that telemetry to detect anomalies, and—wherever possible—automating insight generation to enable near-real-time prevention, response, and remediation."[14]

DON'T TRUST; ALWAYS VERIFY—HP'S SUPERIOR APPROACH TO ZERO TRUST

HP's innovative approach to zero trust—built on 20 years of research investment at HP Labs—applies threat prevention at the source: the user who unknowingly opens the door to an attacker through seemingly innocuous activity.

By putting protection as close to the point of attack as possible—on the endpoint—you don't need to worry if the user is remote or in the office, nor do you care if the data they access is in your data center or in the cloud. Attacks are contained right on the user's computer, constraining the hacker's freedom of movement and limiting the damage they can do, while also eliminating the need for IT to perform a time-consuming remediation on the user's PC.

And because software protection that lacks hardware enforcement is always vulnerable through compromise of the operating system or underlying infrastructure, HP Wolf Pro Security applies zero trust to the entire firmware, hardware, and software stack, creating a layered threat-prevention model that is much harder to subvert.

From self-healing firmware and in-memory breach detection, to threat containment via isolation, our security reduces the attack surface, enables remote recovery from firmware attacks, and delivers protection against known and unknown threats. With the unified force of HP Wolf Pro Security Service, you get robust resiliency and built-in protection from the BIOS to the browser—even for zero-day threats.

In today's borderless threat landscape, it's easy to see why 85% of organizations say they prefer advanced IT security products with features like AI, machine learning, behavior monitoring, containerization, and micro-virtualization.[21]

DON'T PAY A RANSOM—PREVENT AND PROTECT INSTEAD

Prevention is easier (and less expensive) than recovery. The HP portfolio of hardware-enforced, endpoint-focused security services is designed to help you safeguard PCs, printers, and people, no matter what vendor or operating system—and no matter if you're a large university, community college, or local technical or trade school.

HP WOLF PRO SECURITY: THE WORLD'S MOST ADVANCED ENDPOINT SECURITY SERVICE[22]

HP Wolf Pro Security Service[23,24] provides a protection-first approach that liberates students and staff to work on university tech resources with confidence, without adding to IT's list of assignments.

PROTECTION YOU CAN TRUST

Get reinforcing layers of enterprise-grade isolation technology[25] and next-gen, AI-based anti-malware capabilities.[26] Our protection goes beyond traditional antivirus tools,[27,28] so your institution's data, user credentials, and devices stay safe.

WORRY-FREE THREAT MONITORING AND INSIGHTS

Get actionable, real-time insights on device protection status, attempted attacks, and potential threats through a single, cloud-based dashboard. Our credentialed experts[29] deliver Cybersecurity as a Service, so your in-house IT teams can shift to strategic projects instead of chasing false positives and phantom security threats.

PRODUCTIVE FACULTY AND STAFF

Defending the endpoints in your higher ed environment doesn't have to be disruptive for workers or for IT. Our transparent malware and credential protection lets employees work unrestricted using the most common applications and web browsers, without fear of compromising their data or identity—or your network.

HP SURE CLICK ENTERPRISE: ADVANCED THREAT-ISOLATION TECHNOLOGY

Cover your PC users with a virtual safety net, even when unknown threats slip past other defenses. HP Sure Click Enterprise[27] is self-managed protection that automatically isolates high-risk content and renders malware harmless.

KEEP RISKY CLICKS CONTAINED

Isolate potentially malicious content such as browser tabs, Microsoft Office files, PDFs, emails, and USBs. HP Sure Click Enterprise deploys isolation and containment with hardware-enforced micro-virtual machines (micro VMs) and advanced hypervisor technology—helping protect users and networks from malware and phishing attacks.

REMOVE BARRIERS TO PRODUCTIVITY

Protect without adding layers of hassle for employees and IT—HP Sure Click Enterprise eliminates the need for restrictive security policies and workflows. And your IT pros can be more effective with their time, thanks to simplified threat analysis that spots problems sooner and reports them on actionable dashboards.

REST EASY WITH ENTERPRISE-CLASS SERVICE AND SUPPORT

IT staff are perennially in short supply, and the move to remote and hybrid learning has pulled even more of their attention away from cybersecurity.[1] HP Sure Click Enterprise is simple to deploy and offloads the time-consuming task of threat identification, with no additional on-premises infrastructure or software purchase required.

> **"WHY IS IT THAT EXECUTIVES ARE WILLING TO PAY A $1 MILLION RANSOM TO CYBERCRIMINALS, BUT NOT WILLING TO PAY A FRACTION OF THAT TO IMPLEMENT OR MAINTAIN BACKUPS?"**
>
> IAN THORNTON-TRUMP
> CISO at Cyjax[16]

HOW HP WOLF SECURITY PROTECTS YOUR USERS AND THEIR DEVICES

Secure every potentially risky activity on your employee PCs.

- Isolate user tasks into hardware-enforced micro VMs.
- Protect high-value data and applications via virtual containers other PC processes can't touch with HP Sure Access Enterprise.[30]
- Eliminate most malware before it can infect even a single device.

A CYBER BREACH IS A HARD LESSON TO LEARN

WITH HP WOLF SECURITY, YOU DON'T HAVE TO

Cybercriminals aren't just more motivated than ever—they're also more tactically sophisticated.[31] They're a quick study on accessing your network through the weak spots in your printer and PC security.

Your school will likely face a breach at some point—it's more a matter of *when* than *if*.[8] But you can stop it in its tracks, without adding to IT's workload or disrupting learning, research, or operations. The HP Wolf Security portfolio of hardware, software, and services equals comprehensive endpoint protection and recovery resiliency—a defense that evolves with and defeats emerging education threats.

PREP FOR THE INEVITABLE TEST OF YOUR CAMPUS CYBERSECURITY—TAKE THE HP WOLF SECURITY SELF-ASSESSMENT NOW.

READY TO LEARN MORE? CONTACT AN HP WOLF SECURITY SPECIALIST.

1 Government Technology, “Cybercriminals Use Pandemic to Attack Schools and Colleges,” September 20, 2021

2 Infosecurity, “Ransomware Strikes Third US College in a Week,” June 8, 2020

3 Federal Bureau of Investigation, Cyber Division, “Increase in PYSA Ransomware Targeting Education Institutions,” March 16, 2021

4 Slate, “Howard University’s Devastating Ransomware Attack Can Teach Other Colleges a Valuable Lesson,” September 9, 2021

5 ZDNet, “Ransomware gangs have found another set of new targets: Schools and universities,” March 23, 2021

6 Verizon, “Data Breach Statistics by Industry: Educational Services,” 2020

7 Microsoft Security Intelligence, Global threat activity, accessed December 2021

8 College Consensus, “Essential Guide to Higher Education Data Breaches,” accessed December 2021

9 C ollegis Education, “Cybersecurity in Higher Ed: Understanding Vulnerabilities and Preventing Attacks” [infographic], March 31, 2021

10 NSF National Center for Science and Engineering Statistics, “Universities Report 5.7% Growth in R&D Spending in FY 2019, Reaching $84 Billion,” January 13, 2021

11 Lamar University, “Colleges and Universities Are Prime Cyber Attack Targets,” accessed December 2021

12 Insurance Business, “Data Breaches Hit Millions of School Records—Report,” July 2, 2020

13 Inside Higher Ed, “Colleges a ‘Juicy Target’ for Cyberextortion,” March 19, 2021

14 EDUCAUSE, “The Increasing Threat of Ransomware in Higher Education,” June 22, 2021

15 MSSP Alert, “University Ransomware Attacks: Hackers Hit Colorado, Miami Schools,” March 25, 2021

16 Forbes, “The University of California Pays $1 Million Ransom Following Cyber Attack”, June 29, 2020

17 EAB, “How Universities Are Planning Return-to-Work Policies and Guidelines,” June 29, 2021

18 Education Technology, “Navigating Higher Education Cloud Security in the COVID-Era,” March 7, 2021

19 Ponemon Institute 2020 State of Endpoint Security Report sponsored by Morphisec, January 2020

20 Proofpoint Human Factor Report 2019, September 2019

21 CyberEdge 2020 Cyberthreat Defense Report, March 2020

22 Based on HP’s internal analysis of isolation-backed, deep learning endpoint security services including SaaS and managed services. Most advanced based on application isolation and deep learning endpoint protection on Windows 10 PCs as of July 2020.

23 HP Security is now HP Wolf Security. Security features vary by platform

24 HP Wolf Pro Security Service is sold separately. For full system requirements

25 HP Sure Click Pro is included with HP Wolf Pro Security Service and requires Windows 10 Pro or Enterprise and Microsoft Internet Explorer, Google Chrome, Chromium, Mozilla Firefox, and new Edge are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed.

26 HP Sure Sense Pro is included with HP Wolf Pro Security Service. For system requirements

27 HP Sure Click Enterprise is available on select HP PCs and requires Windows 10. Microsoft Internet Explorer, Edge, Google Chrome, Chromium, or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed.

28 HP Sure Sense is available on select HP PCs and is not available with Windows 10 Home.

29 Security Experts available in the Proactive Security Enhanced plan only.

30 HP Sure Access Enterprise requires Windows 10 Pro or Enterprise.

31 The Hill, “Schools, colleges brace for cyberattacks as students return,” August 22, 2021