GUIDE

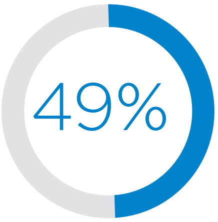
# How to stay a step ahead of cybersecurity threats in higher education

Spectrum ENTERPRISE

## Higher education faces some of the greatest cybersecurity challenges of any sector.

Colleges and universities manage a vast array of digital assets — reports, photos, videos, recordings, curriculum, brochures, research data and methodologies and other material — *and* a huge amount of highly valuable personal data. Access to relevant information must be easy for students, faculty, staff, alumni, donors and the broader community, while ensuring only authorized access to sensitive data.

Although higher education IT leaders rank cybersecurity as their top priority,[1] 30 percent of colleges and universities say their cybersecurity team is not well equipped for protecting an evolving security perimeter.[2] Keeping up with threats and attacks is challenging due to competition for cybersecurity staff and tight budgets.



percentage of institutions that had to shut down their DNS server or service because of an attack in 2020.[9]

The attack surface has never been larger. Network-connected mobile devices, applications and Internet of Things (IoT) technology are integral to higher education communication and collaboration. These unsecure, easily-corrupted devices access the network and make it vulnerable to threats. A demand for always-on, anywhere network access and the challenges of blending online and offline learning also create security issues. The collaboration in higher education research, which fuels innovation, adds to the vulnerabilities IT teams must protect.

Hackers exploit these vulnerabilities by using increasingly sophisticated technologies and evolving approaches. Eighty-six percent of observed colleges and universities have been targeted recently by botnet attacks[3] — and two in five institutions say cybersecurity has become even more important in the last year.[4]

Attackers are drawn to the higher education sector because of the huge amount of personally identifiable information (PII) available on students, faculty and others. Threats are different and more prevalent than in the past, creating a new threat profile.

- **18,471:** Number of distributed denial of service (DDoS) attacks at colleges, universities and professional schools in the second half of 2020.[5]

- **100 percent:** The increase in ransomware attacks against universities from 2019 to 2020.[6]

- **49 percent:** The percentage of institutions that had to shut down their DNS server or service because of an attack in 2020.[7]

- **24.5 million:** Number of educational records compromised in U.S. data breaches since 2005.[8]

## Tracking evolving threats

Although the profile of threats is concerning, you can protect your institution from attacks that come from a wide range of attack vectors. Understanding current and emerging types of threats can help you put the right protection in place.

**DDoS attack:** Attacks have been increasing in size, duration, sophistication and frequency. Recent DDoS attacks often involve transmission control protocol (TCP) amplification, which increases the number of both targets and affected networks. There were more than 10 million DDoS attacks worldwide in 2020, up 20 percent from 2019 — and for as little as $7 anyone can purchase a DDoS-for-hire service.[10]

**Malware, including viruses, worms and adware:** Colleges and universities regularly report that incidents involving the worm Conficker, first identified in 2008, are still a major concern. Microsoft's Global Threat Activity tracker detected 5.8 million malware incidents in the education sector in August 2021 alone, making it the No. 1 most targeted industry.[11]

**AI-empowered phishing and bots:** Phishing has evolved to include artificial intelligence (AI)-generated audio and video files that can make crime difficult to detect. An estimated two-thirds of colleges and universities lack basic email security configurations, leaving them especially vulnerable to phishing attacks.[12]

**Unsecured endpoint devices:** Student and staff use of mobile and IoT technology creates entryways for cybercriminals — from campus vending machines to "smart" doorbells on dorm rooms. Without the right network firewall, a VPN tunnel and threat management, these tools can create a network entry point. It takes five minutes for hackers to find and potentially compromise a new IoT device online, compared with 266 days for organizations to find and fix a security breach.[13]

From "smart" doorbells on dorm rooms to vending machines, the use of mobile and IoT technology creates entryways for cybercriminals.

**Ransomware:** Today's advanced strains of ransomware encrypt data on a network or lock users out of their devices. WannaCry and Petya have been particularly damaging to the higher education community.

**Data breaches:** Student and staff PII — including names, Social Security numbers, dates of birth, addresses, telephone numbers, salary data and financial aid information — have been compromised at numerous universities. Since 2005, U.S. educational institutions have experienced more than 1,300 data breaches overall.[14]

## University attacks: how they might have been prevented

Stories of higher education data breaches help paint a clear picture of the evolving threat. Read these examples and see how institutions might have thwarted an attack.

### Large state university

**Type of breach:** A series of massive DDoS Mirai botnet attacks over the span of a couple of years flooded the university's network with internet traffic.

**What was lost:** A central server that maintained a portal used by students and faculty was taken offline for several consecutive periods.

**How the breach could have been prevented or minimized:** Careful monitoring of Internet traffic could have detected the attacks. During the attacks, a DDoS solution could have resulted in blocking only certain IP addresses, allowing clean traffic to pass and productivity to be maintained or restored.

### Medium-sized public university

**Type of breach:** Data violation from a phishing attack.

**What was lost:** 636 student records and family records containing PII.

**How the breach could have been prevented or minimized:** Use of a next-generation firewall could have helped block the attack and warned university security personnel to act sooner. Intrusion detection services, in concert with strong client authentication, could have protected critical data.

### Small private university

**Type of breach:** An unauthorized person accessed email accounts of current employees resulting in a data breach.

**What was lost:** Employees' PII — including Social Security numbers, addresses, phone numbers, names of family members and salary information — was exposed.

**How the breach could have been prevented or minimized:** A managed firewall service could have blocked and protected confidential information from those not authorized to access the network.

Widespread, coordinated network protection coverage can help protect against cyber threats.

## Finding the right protection

Continually keeping ahead of cybersecurity threats to your network requires comprehensive and coordinated coverage. That includes firewalls, unified threat management (UTM), DDoS protection and the support of a network services provider to deliver managed service solutions.

When evaluating a provider and their services, here are some questions to ask to help you find the best protection possible:

- What protection do you provide against volumetric attacks?
- Do you have a means of letting us continue to work productively after a DDoS attack on the parts of the network that were not affected?
- How can you protect us from malware, phishing and other common higher education cyberattacks?
- Do you provide UTM? What protection does that provide?
- Can your firewall protect traffic between our various sites as well?
- Is a next-generation firewall part of what you offer? What does it provide?
- Do you have an integrated solution that includes firewall, UTM and internet service to simplify protection?

- We have campus-wide WiFi and multiple sites. How will you ensure they're all protected?
- What type of support is available on nights, weekends and holidays?

## Comprehensive coverage and support

Widespread, coordinated network protection coverage can keep you one step ahead of evolving and growing higher education network threats. When you choose security as a managed service, you are supported from design through implementation and provided with ongoing support. Discover how Spectrum Enterprise is uniquely qualified to protect your institution's network.

**Learn more**

1. "2020 Top IT Issues," EDUCAUSE, 2020.
2. "QuickPoll Results: The Cybersecurity Workforce," EDUCAUSE, 2021
3. "2021 Cybersecurity in Higher Education Report," BlueVoyant, 2020.
4. "Cybersecurity in higher education: going from `no' to `know,'" Edscoop, 2021.
5. "NETSCOUT Threat Intelligence Report: Findings from 2H 2020," NETSCOUT, 2020.
6. "2021 Cybersecurity in Higher Education Report," BlueVoyant, 2020.
7. "2021 Global DNS Threat Report: Elevating Network Security with DNS," IDC, 2021.
8. "US schools leaked 24.5 million records in 1,327 data breaches since 2005," CompariTech, 2020.
9. Ibid.
10. "NETSCOUT Threat Intelligence Report: Findings from 2H 2020," NETSCOUT, 2020.
11. "Microsoft global threat activity tracker," Microsoft, Sept. 2021.
12. "2021 Cybersecurity in Higher Education Report," BlueVoyant, 2020.
13. "NETSCOUT Threat Intelligence Report: Findings from 2H 2020," NETSCOUT, 2020.
14. "US schools leaked 24.5 million records in 1,327 data breaches since 2005," CompariTech, 2020.

### About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary.
Restrictions may apply. Subject to change without notice.