Building cyber resilient higher education institutions

Defending against and recovering from modern cyberthreats

With critical systems and sensitive personal, financial and research data at stake, higher ed institutions present a particularly enticing target for cyberattackers.

It comes as little surprise, then, that attacks against universities, colleges and community colleges have skyrocketed in recent years, their ripple effects amplified by tight budgets and small IT teams. Combine these factors with the added stress of adjusting to new remote work and remote learning realities, and higher ed must confront an exceedingly complex cyberthreat landscape. In an effort to keep all digital workloads protected and up to date, whether they sit on campus or in the homes of faculty, students or administrators, higher ed CIOs and IT teams must choose future-proof, affordable and easy-to-manage cyber protection and imaging solutions tailored to fit their unique needs.

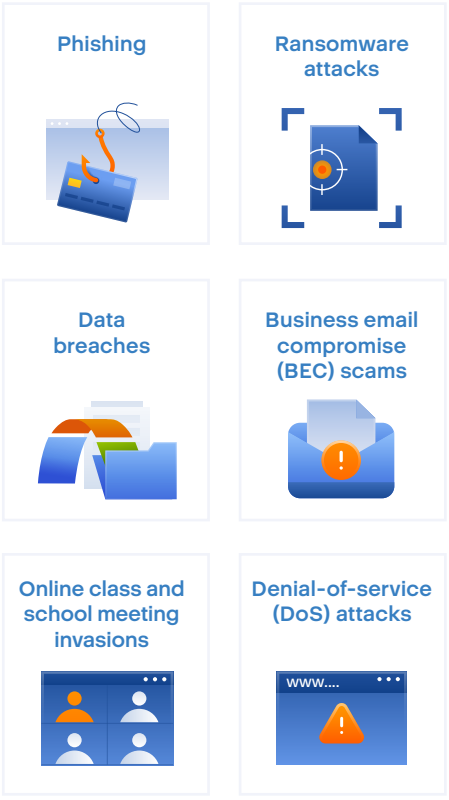
Turnkey solutions for higher ed

With ransomware threats rising, institutions need cybersecurity and backup solutions to protect vulnerable, sensitive personnel and student data. Acronis solutions enable universities and colleges with budget and IT staffing constraints to protect themselves against cyberattacks, including ransomware. Acronis helps higher ed institutions build cyber resilience with layered defenses against cyberattacks and quick recovery of systems and data from attacks that do succeed.

Comprehensive cyber protection

Trying to build cyber resilience from a patchwork of different vendors' point products can create gaps in both an institution's defenses against

How educational institutions are being attacked



and ability to recovery from cyberattacks. It is only a matter of time before cybercriminals find and exploit them. Acronis Cyber Protect provides a single platform that enables higher ed IT teams to seamlessly manage both cybersecurity and data protection, boosted by the power of machine learning (ML) and artificial intelligence (AI). With full-stack anti-malware protection and comprehensive endpoint management, Acronis Cyber Protect combats advanced cyberattacks while simplifying daily IT operations, endpoint deployments, management and reporting.

From a single console, IT teams can protect faculty, staff and students both in remote work and study environments and on campus with remote desktop, automated patch management, remote device wipe, URL filtering and protections for teleconferencing applications like Zoom, Cisco WebEx and Microsoft Teams.

System provisioning and image deployment

Acronis Snap Deploy is widely used in higher education for simple, fast provisioning of multiple laptops and desktops from a master image ("cloning"). This enables easy, error-free onboarding of incoming students, faculty and staff with new machines, and rapid resetting of systems to a pristine state in computer labs and similar educational settings at the start of each new academic period.

About Acronis

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection and endpoint management for educational institutions, managed service providers (MSPs), small and medium businesses (SMBs) and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity.

Acronis offers the most comprehensive security solution on the market with its unique ability to meet the needs of diverse and distributed IT environments. A Swiss company founded in Singapore in 2003, Acronis has 45 locations across the globe. Acronis Cyber Protect Cloud is available in 26 languages in 150 countries and is used by over 20,000 service providers and over 750,000 businesses and educational institutions. Learn more at www.acronis.com.

Key pain points

Defend against cyberattacks like ransomware

Higher ed needs to defend its data and uptime against AI-enhanced cyberthreats with its own AI-powered defense-in-depth measures, including endpoint detection and response, advanced email security and URL filtering.

Manage both campus-based and remote endpoints

Higher ed IT staffs need remote management tools they can use to monitor, configure and troubleshoot every system used by faculty, staff and students, wherever they are. This includes functions like vulnerability assessments, patching of operating systems and applications, and installation and maintenance of cybersecurity and data protection measures.

Meet data privacy and compliance requirements

Higher ed institutions are facing stricter regulatory requirements to stop cyberattacks on sensitive personal data of students, staff and faculty, protect proprietary research data, and to quickly recover systems and data from attacks that do succeed. This requires deploying modern cyber defense-in-depth measures as well as improved backup, disaster recovery and incident response regimens.