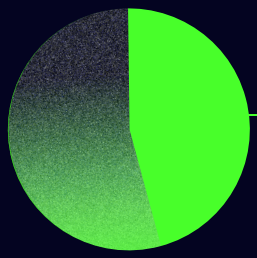
SECURING CAMPUSES: CLOSING CYBERSECURITY GAPS WITH REAL-TIME INTELLIGENCE

CENTRIPETAL

Higher education institutions aren't just schools—they are digital ecosystems, research hubs, and economic powerhouses. They store vast amounts of sensitive data, from student records to groundbreaking research, making them a prime target for cybercriminals.



66%

of institutions were hit by ransomware in 2024

A Sophos survey revealed that 66% of higher education institutions experienced ransomware attacks in 2024.

Yet, universities were built for openness and collaboration, not security. Their unrestricted networks, thousands of unmanaged devices, and critical infrastructure create a vast attack surface, unlike any other industry.

Cybercriminals know this — and they're exploiting it.

Universities are a top target:
Higher education institutions face an average of 3,574 cyberattacks per week, more than any other industry.

Financial impact:
The average cost of recovering from an attack is more than $4 million.

Disrupting research & operations:
Nation-state actors target universities for intellectual property theft, while ransomware gangs hold campus operations hostage—forcing closures and ransom payments.

Overwhelmed security teams:
University IT and security teams are drowning in alert fatigue, understaffing, and outdated defenses—forcing them into constant firefighting mode rather than preventing breaches.

A new approach is necessary to transition from reactive to proactive protection. The answer lies in operationalizing threat intelligence and applying it at the network's edge.

Gartner

According to analyst firm Gartner,

"99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year."

The intelligence to stop these attacks existed - it just wasn't applied in a preventative way. By applying intelligence at the network's edge to block known threats before attackers reach the reconnaissance stage, you can stop known attacks, drastically reduce event volume, and help under-resourced IT and security break free of fighting reactively.

WHY IS SECURING HIGHER EDUCATION INSTITUTIONS SO DIFFICULT?

Securing higher education institutions is widely regarded as one of the most challenging tasks in cybersecurity due to a unique convergence of factors.

3,574

cyberattacks attempts per week

The University Attack Surface is Massive

Higher education institutions operate in an environment designed for openness, not security, making them prime targets for cyber threats. With open networks, unmanaged devices, and critical research and administrative systems, traditional security measures struggle to keep pace. The education sector faces 3,574 cyberattacks per week—more than any other industry—putting sensitive data, operations, and institutional reputation at risk. Intelligence-powered cybersecurity provides a proactive defense by blocking known threats before they reach the network, reducing risk across every device and connection without disrupting academic collaboration.

Research & Intellectual Property Are a Goldmine for Hackers

Universities are prime targets for cybercriminals and nation-state actors due to their valuable research, financial data, and government contracts. In 2024, 66% of higher education institutions were hit by ransomware, and intellectual property theft continues to rise. Traditional security measures are not enough to protect against these evolving threats. Intelligence-powered cybersecurity provides proactive defense by blocking malicious domains, phishing attempts, and ransomware attacks in real time—preventing breaches before they happen and safeguarding critical research and data.

Openness vs. Security

Universities face the challenge of balancing openness with security as they navigate BYOD, hybrid learning, cloud adoption, and open access. Traditional security solutions force a trade-off, often restricting collaboration to enhance protection. With complex networks and expanding attack surfaces, integrating security without disruption is a growing challenge. Intelligence-powered cybersecurity eliminates this compromise by providing real-time threat protection while preserving academic openness, enabling institutions to adopt new technologies without increasing risk.

Cyber Threats Go Beyond Data

IoT-connected devices significantly expand the attack surface, making university networks more vulnerable to cyber threats. Attacks on IoT infrastructure can disable security cameras, power grids, HVAC systems, and emergency alert systems—directly impacting campus operations and safety. In early 2023, universities experienced the highest rate of DDoS attacks, crippling network access. Intelligence-powered security provides real-time protection, identifying and stopping threats before they can exploit connected systems. This proactive approach safeguards both digital and physical assets, ensuring operational continuity and student safety.

Security Teams Are Overwhelmed

University IT teams are overwhelmed by an endless stream of security alerts, staffing shortages, and the need to react rather than prevent breaches. According to EDUCAUSE, in 2024, cybersecurity remains the top IT concern for higher education, with limited resources making proactive defense even more challenging. Intelligence-driven automation reduces the burden by blocking threats before they trigger alerts, allowing security teams to focus on high-priority threats and strategic security initiatives instead of constant firefighting.

These factors collectively contribute to the burgeoning challenge of securing higher education institutions against cyber threats. Implementing comprehensive cybersecurity measures that address each of these vulnerabilities is essential to protecting the integrity and reputation of academic institutions.

TURNING COMPLEXITY INTO RESILIENCE

Higher education institutions can't afford to stay reactive. Legacy security systems aren't working, and cybercriminals are already ahead. Intelligence powered cybersecurity is the only way to shift from a reactive strategy to a proactive one—and secure entire campuses without disrupting access, collaboration, or innovation. These institutions need intelligence powered defenses that prevent attacks before they happen, adapting, in real-time — without disrupting learning and research. That's exactly what Centripetal's CleanINTERNET® delivers.

How CleanINTERNET® Makes the Job Easier:

CleanINTERNET® proactively secures campuses with intelligence powered protection, preserving openness, safeguarding critical research, and empowering security teams to focus strategically.

CleanINTERNET® specifically delivers value in four key areas:

Proactive Threat Prevention

Automatically neutralizes threats before they reach university networks by applying billions of real-time threat indicators at scale and protection from 100% of all known threats. Universities no longer have to rely solely on reactive measures.

Enhanced Security Team Efficiency

Eliminates up to 90% of noise and false positives, significantly reducing the operational burden on IT staff and freeing them to focus on strategic, high-value tasks.

Protection Without Compromising Openness

Allows universities to maintain their collaborative, open culture while effectively securing their digital environment—balancing open access with robust, proactive cybersecurity.

Comprehensive Infrastructure Protection

Defends not only critical research data and student records but also campus IoT devices.

REIMAGINING CYBERSECURITY FOR HIGHER EDUCATION

Centripetal's CleanINTERNET® is the modern, proactive cybersecurity solution explicitly designed for higher education's unique environment. CleanINTERNET® leverages real-time global threat intelligence to automatically block malicious activity at the network's edge, before it impacts campus operations.

Unlike traditional reactive solutions that rely on static firewall rules or endpoint detection after a breach occurs, CleanINTERNET® proactively prevents cyber threats by instantly recognizing and neutralizing known malicious actors and domains in real-time, drastically reducing the overall attack surface.

Why Centripetal?

Centripetal, the global leader in intelligence powered cybersecurity, is operationalizing the world's largest collection of threat intelligence, in real-time, to protect organizations from every known cyberthreat through its innovative patented technologies.

The company's CleanINTERNET® solution delivers the only proactive approach to intelligence powered cybersecurity, leveraging the latest computing technology and skilled operations intelligence analysts, at dramatically lower cost. We are experts in threat intelligence, with a team comprised of cryptologists, and security analysts from the U.S. Intelligence & Defense community who have protected the most sensitive assets in the world. Centripetal is based in Reston, VA with offices in Portsmouth, NH and Galway, Ireland.

centripetal.ai