

Digital Transformation in Education

Smart and Secure Campus



Table of contents

Introduction	3	Benefits of Smart and Secure Campus solutions	13
Current situation	3	Quick and cost-effective	13
University vulnerability	5	Comprehensive protection	14
What can we do?	7	Focus on what matters	15
Smart and Secure Campus solutions	9	Partner ecosystem	16
End-to-end solutions	10	Real-world success	17
Seamless integration with physical security	11	Get started	22
Advanced threat intelligence	12	Sources	23

Educational institutions are under attack

Higher education accounts for **17% of all data breaches** where personal information was stolen—second only to the healthcare sector¹.

Why? A single university provides a treasure trove of high value targets for cybercriminals, with everything from students' personally identifiable information, to extremely valuable intellectual property and research data. In addition to growing cyberthreats, universities must also contend with increasing physical safety threats—78% of crimes against university students and faculty reported under the Clery Act occurred on campus². Compounding these challenges is the stress of expanding compliance issues around data privacy standards. Protecting all facets of physical and digital campus spaces in a unified, seamless way—from building access controls and cameras to data centers and endpoints—is imperative. Institutions need a comprehensive approach to security that ensures the safety and privacy of their students, devices, and data.



A high-angle photograph of several students sitting on the floor in a classroom or library setting. They are focused on their devices: one student in the foreground uses a laptop, another uses a tablet, and others are seen with smartphones. The scene is dimly lit, with the primary light source coming from the devices' screens. The students are dressed in casual attire like jeans and plaid shirts. The floor is made of light-colored wood.

Defending universities from a myriad of physical and digital threats is challenging

The damage from physical and cyber attacks is often hard to quantify, generating harm beyond those directly impacted. Educational institutions face the additional effects of damage control, remediation, and other costs, plus the immeasurable harm to the institution's reputation and the loss of student, parent, and alumni trust. Higher education institutions don't always have the resources to invest in a robust security solution. With an open environment and relatively easily accessible libraries and community centers, plus young students who may be unaware of phishing and other cyber threats, universities represent a unique physical and digital security challenge. Further confounding the problem, institutions often have more than a dozen security tools in place, but many of these tools don't interact with each other or share data, making them less effective than a comprehensive security solution.

And universities are particularly vulnerable

36% of higher education institutions are hit by a cyberattack every hour³.



13% of data breaches occurring in the first half of 2017 were related to education institutions, resulting in the compromise of around 32 million records⁴.



10% of simulated phishing e-mails sent to users in education institutions were successful, causing the recipient to click on a fraudulent link⁵.



12,700 physical attacks affected education institutions, harming more than 21,000 students and educators worldwide, from 2013 through 2017⁶.





Higher education institutions need powerful solutions to protect student, staff, and institutional data and provide a safe environment—despite constrained resources.

What can we do?

Protect data from breaches and cybercrime.

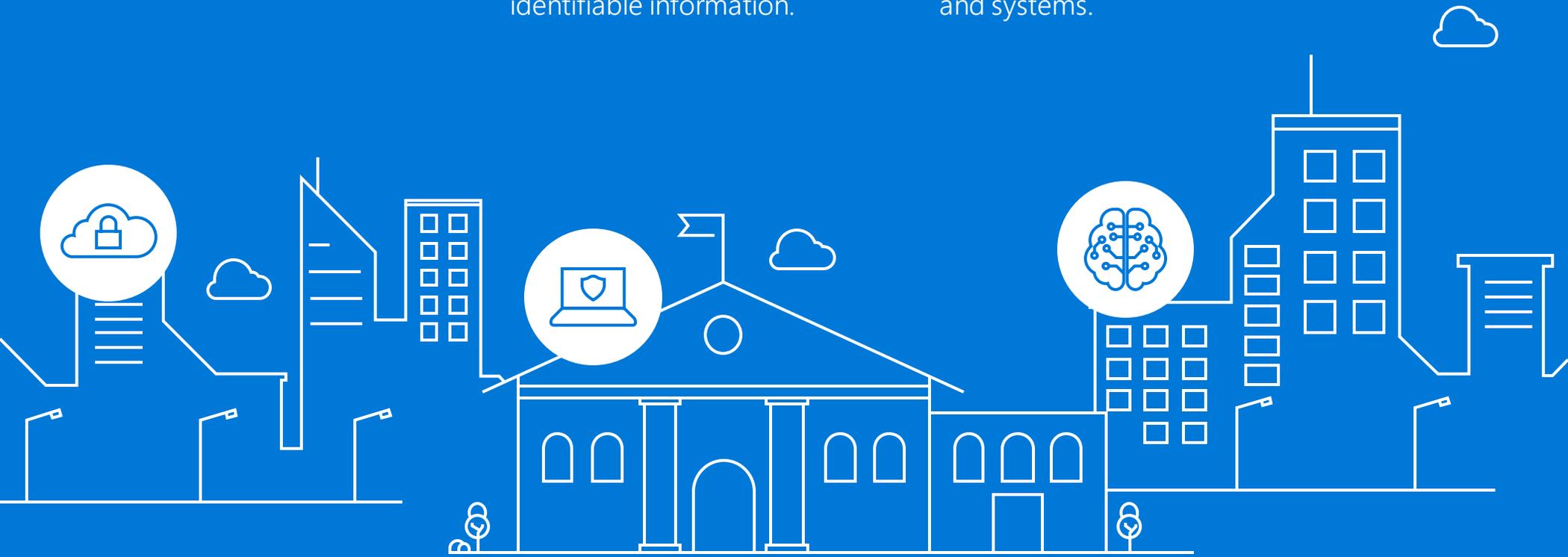
Leverage industry-leading security controls and intelligence to help protect against new and evolving cyber attacks

Ensure your students are protected from identity theft and fraud.

Establish defense in depth and remediation measures to enhance the protection of students' personally identifiable information.

Integrate cybersecurity and physical security to unify and strengthen your defenses.

Limit your exposure to all types of cyber and physical threats and extend your security across data centers, access control points, and edge devices and systems.



Ready to talk to an expert? Contact us [→](#)

Safeguard your students online and on campus

Higher education institutions need powerful security solutions to address physical and cyber security threats and reduce risk. Solutions that work smarter together maximize constrained resources and reduce the management burden on IT. Microsoft's Smart and Secure Campus solutions provide end-to-end, integrated security solutions and threat protection of identities, access control systems, and institutional data. Microsoft's Intelligent Security Graph provides industry-leading artificial intelligence and insight into threats while Microsoft 365 Threat Protection offers unparalleled scale and comprehensive defense against complex threats. Microsoft Azure Sentinel transforms security operations, enabling a birds-eye view across the institution with next-generation security information and event management. Combined with seamlessly integrated physical security on the Microsoft Azure IoT platform, institutions are empowered to protect, detect, and respond to all threats before they cause serious harm.



Microsoft's Smart and Secure Campus solutions provide:



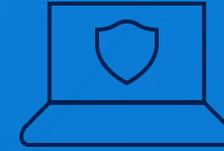
End-to-end
intelligent solutions



Seamless integration
with physical security



Advanced threat
intelligence



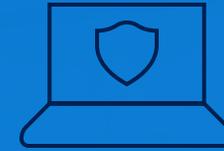
End-to-end intelligent solutions

With cybersecurity solutions from Microsoft, universities can more easily detect suspicious activity and remediate cyber threats that affect student and university data. End-to-end, integrated security helps modern higher education institutions preserve the confidentiality of information online, whether student data, intellectual property, or other sensitive information, and further reduce risk through addressing both physical security and cyber security strategies with one cloud platform. Microsoft 365 and Microsoft Azure's IoT platform provide built-in Microsoft Threat Protection and security technologies, enabling institutions to make the most of their investments, while eliminating the need for multiple point solutions. Integrated services translate to smarter investments and reduced IT burden.



Seamless integration with physical security

Microsoft's partner solutions help ensure physical safety and peace of mind on campus through detecting and preventing suspicious activity, while instantly communicating incidents across campus. Solutions leverage Microsoft Azure's next-generation Internet of Things (IoT) and Azure Digital Twins to virtually model the relationships and interactions among people, places, and devices to see what's going on in real time and ensure security across end points. Microsoft Azure Sphere IoT Security, a new solution for creating highly secure, Internet-connected microcontroller (MCU) devices, can further enhance the security resilience of the IoT devices themselves. Choose from partner solutions to enable physical access control, campus monitoring, alerting, emergency response and more.



Advanced threat intelligence

Microsoft's Threat protection is supported by one of the largest threat intelligence networks through Microsoft's Intelligent Security Graph, the foundation for all of Microsoft's security solutions. The Microsoft Intelligent Security Graph powers Microsoft Threat Protection by using industry-leading artificial intelligence and machine learning to correlate vast threat intelligence and security signals to identify and mitigate cyber threats. It obtains threat signals from each of Microsoft's services, third party threat feeds, and global footprint and blends threat signals with powerful machine learning, threat analysis from our 3500+ in-house security specialists⁷, and support from over \$1 billion in annual cybersecurity investments⁸. Additionally, Microsoft uses cloud-powered real-time attack forensics to increase protection from sophisticated and targeted phishing attacks. Automated Incident Response tools can automatically hunt for compromised accounts instead of relying on compromised users to alert you or attackers to make a mistake.

Identify and remediate cyber threats — quickly and cost-effectively

With Smart and Secure Campus solutions, institutions can automatically address threats while saving time and resources to better protect their campus



UNIVERSITY IT



89.3% Reduction in time required for investigation and remediation with Office 365 Threat Intelligence⁹.

27,168 IT hours saved annually due to improved detection and response to security threats⁹.

ROI of 186% (Three-year benefits included: avoided IT costs due to consolidation of security systems, savings from faster remediation of end user security events, reduced end user downtime, and reduced likelihood of data breach)⁹.

Microsoft provides comprehensive threat protection



Protect

Defense in depth

- Monitoring and controls
- Identity and access management
- Proper hygiene
- Security development lifecycle
- Data encryption.



Detect

Extensive signal fabric

- Cloud scale intelligence
- Machine learning
- Behavioral monitoring.



Respond

Closing the gap between discovery and action.

Benefit from unparalleled insight and protection:

450 billion

authentications processed monthly¹⁰.

1.2 billion+

devices scanned each month for threats¹⁰.

12 million

attacks prevented daily¹⁰.

90%

of security professionals surveyed agreed that Office 365's use of machine learning algorithms mitigated phishing campaigns¹¹.



Leverage Microsoft 365 Threat Protection so you can focus on your students



Reduced license costs

through security solutions consolidated onto a single platform, instead of a myriad of third-party security solutions. Save up to \$300,000 in decreased licensing costs as your institution becomes more proficient at leveraging Office 365 E5 with Threat Intelligence and decreases its reliance on other security solutions¹¹.



Significant time savings

through consolidation onto a single platform, over security operations teams managing and maintaining multiple third-party security solution software or vendors. Initially, that time is reduced by 775 hours annually, increasing to 1,000 hours by the third year as the institution continues to eliminate those third-party solutions¹¹.



Greater efficiency and effectiveness

in the investigation, monitoring, and remediation of issues through consolidation of security systems enabling you to create a "single pane of glass" for your institution's security teams.

"We're a small team, and I think the goal of getting machine learning and AI to better recognize these attacks and automate a response... I think that would certainly help us with the small staff size. We can take advantage of those machine learning/AI capabilities in order to maximize what our team is able to do."

IT SECURITY DIRECTOR, EDUCATION

And take advantage of a robust partner ecosystem

Choose from Microsoft's partner solutions that leverage the Azure platform and technology such as Azure Digital Twins and Azure Sphere IoT Security—for enabling campus safety, physical access control, alerting and emergency response, and more—to ensure safety across endpoints on campus.



ICONICS provides building automation and IoT solutions to reduce energy costs and significantly streamline facilities management. Higher education campuses realize 10-20% savings off their total energy costs by deploying ICONICS solutions.



Genetec is a global provider of IP security and access control solutions unified in a single platform, Security Center, to improve security and empower your organization through enhanced situational awareness, unified command and control, and connectivity to the cloud.



Fortinet develops and markets cybersecurity software and appliances and services such as firewalls, anti-virus etc., to help education institutions move their data to the cloud and utilize elasticity, scale, and performance of cloud-based services.



Armored Things provides intelligent end-to-end physical security solutions, leveraging predictive analytics to detect unusual activity, modern, easy-to-use tools to enhance existing safety operations, and streamline security operations across enterprises.



Real-world success

George Washington University, USA

Enhancing digital and physical security on campus with cloud-based identity and access management

Challenge

Managing different faculty, staff, and student identities in a higher education scenario is a challenge. George Washington University was looking for an efficient way to secure its data and manage the constituents who require access to institutional data outside its firewall—whether it's parents, incoming students, 275,000 alumni, or neighbors who use the library.

Solution

As part of the university's journey to the cloud, GW is rationalizing and enhancing its directory and identity management solution using Microsoft Azure Active Directory Premium P1.

Benefits

- Increased ease-of-use and security with a single platform that includes all the identity management capabilities needed for the university.
- Leveraged a single source location from Azure AD Marketplace that hosts tools and interoperable apps for simple extensibility.



"Our whole experience with Azure AD has been a boost of confidence for IT as we take steps to safeguard everyone with a comprehensive solution that supports a modern, digital environment for GW."

MARK ALBERT

Director, University Web & Identity Services
George Washington University

University of Southern Denmark

Keeping university data safe and secure

Challenge

Under increasing attack, the University of Southern Denmark (SDU) needed to find a better way to protect its valuable research data and IP from cyberattacks.

Solution

SDU adopted the Microsoft 365 Education solution, which includes the Enterprise Mobility + Security solution. They also deployed Microsoft Azure Active Directory and Microsoft Advanced Threat Analytics.

Benefits

- Reduced security workload by 60 percent with automated protection features.
- Streamlined manual security tasks, like detecting anomalies and addressing threats.
- Increased visibility into the university's IT environment.
- Empowered university's IT team to better detect and prevent threats.



"I like how Microsoft 365 capabilities work together as an ecosystem, with one window for all my security information. Tools like Windows Defender ATP are so deeply integrated... that I have better analytics and detailed forensics to strengthen our overall security profile."

BO S. DREIER
IT Security Specialist
University of Southern Denmark

University of Arizona, USA

Putting a shared cybersecurity vision into operation

Challenge

University of Arizona decided to transform its decentralized, heterogenous IT landscape and improve the institution's cybersecurity.

Solution

The university implemented a holistic security model that improved identity access management proactively and improved compliance with cybersecurity and regulatory requirements.

Benefits

- Modernized the 12-year-old on-premise Active Directory platform.
- Reduced project risk, despite the challenges of a complex and distributed university IT environment.



"Other vendors were willing to work with us and remediate our environment back to a clean state, but Microsoft offered us that, plus a next-generation security vision and architecture predicated on always being under attack, 24x7x365."

DEREK MASSETH

Chief Technology Officer
University of Arizona

London College of Business Studies, South Africa

Digitally transforming educational infrastructure and development approach

Challenge

The e-learning content builders for tertiary education and business learners at the London College of Business Studies wanted to end their reliance on unpredictable, unsecure, on-premises virtualized infrastructure.

Solution:

The university moved its secure online learning portals to the cloud via Azure, protected by a new global ID management capability—enabling educators to distribute and create new e-learning content faster.

Benefits:

- Enabled highly secure live broadcasting of digital learning content.
- Empowered the institution with a new, protected digital infrastructure enabling faster expansion at a global breadth.



"Our sites are more robust and secure, with geo-redundant and encrypted data, daily backups and the ability to restore availability."

EUGENE LONG

Software Development Manager
London College of International Business Studies

Get started

Ready to talk to an expert?
Contact us

Trial the full Microsoft Threat
Protection solution for 30 days at
aka.ms/TryMTP



Sources

1. [HUB, Higher Education – A Goldmine of Personal Data for Hackers, 2017](#)
2. [US Department of Education, Campus Safety and Security Data Analysis Cutting Tool, 2018](#)
3. [VMWare, University Challenge: Cyber Attacks in Higher Education, 2016](#)
4. [Education Data Breaches Double in First Half of 2017, Campus Technology, 2017](#)
5. [State of the Phish report, Wombat Security Technologies, 2018](#)
6. [Education under Attack, Save The Children, 2018](#)
7. [The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack, Microsoft Blogs, 2017](#)
8. [Enterprise security for our mobile-first, cloud-first world, Microsoft blogs, 2015](#)
9. [A Forrester Total Economic Impact™ Study Commissioned By Microsoft, September 2018](#)
10. [Advanced Threat Protection: an integrated cybersecurity solution, 2018](#)
11. [A Forrester Total Economic Impact™ Study Commissioned By Microsoft, September 2018](#)

