Defending universities from physical and digital threats is increasingly challenging.

Institutions of higher education face a constant deluge of cyberattacks. With the current and unprecedented health crisis moving colleges and universities to online learning around the world, the challenge is even greater. **Institutions now must ensure the safety and privacy of students and staff from wherever they’re learning and working**, whether that’s on-campus or at home.

This has compounded the complexity of security and privacy management for university IT teams. Now, more than ever, **universities must keep everyone secure as they’re working and learning from a range of different locations**. Since many are on personal devices and distributed networks that have varying levels of protection and security, these endpoints and devices are becoming new targets for malicious attacks.

In addition, for institutions opening campus or taking a hybrid learning approach, managing the number of people on campus has taken on greater importance. Not only do universities have to protect students and staff from harm, but **they must also take the necessary action to keep their community healthy during the COVID-19 pandemic**. Public health guidelines like social distancing must be enforced, and in the case of an outbreak, swift action must be taken to minimize its impact.
Higher education continues to be a predominant target

**Education accounted for 62% of malicious attacks** tracked by Microsoft Intelligence in September—the most affected industry by 600%.

**Why?** A single university provides a treasure trove of high value targets for cybercriminals, with everything from students’ personally identifiable information (PII), to extremely valuable intellectual property. Remote and hybrid learning compounds these challenges by increasing the risk of attack.

Beyond 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 campus.

Protecting all facets of physical and digital campus spaces in a 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 of their students, devices, and data both at home and on campus.

---

1View the full report by visiting Microsoft Security Threat Intelligence
Maintaining security and safety both online and on campus is a difficult task.

1.3M identities have been exposed as the result of cyberattacks on higher-ed institutions in 2019³

44% of institutions have admitted to suffering a compromise involving a mobile device in 2019⁴

60% of US colleges are limiting the number of on-campus visitors due to the COVID-19 pandemic⁵

Only 42% of higher education leaders say their lockdown hardware is fast enough to protect against threats⁶
Institutions need an integrated cloud platform to bolster digital and physical safety

**Optimize insights**
Leverage a wide breadth of intelligence to build a holistic security picture that provides prioritized, high-quality insights that enable your teams to take quick action. Microsoft’s cloud platform, uses and correlates data from all the solutions to create a holistic picture of your security needs and posture.

**Automate investigation**
With high-quality insights, your institution can unlock automated processes at the workload level to streamline and hasten threat identification and remediation at scale. This automation helps your platform act like a member of your team—which is especially important with cybersecurity teams traditionally being understaffed.

**Consolidate vendors**
A single platform helps you better defend multiple areas of your institution and close vulnerabilities that come from stitching together multiple point solutions. You can also save time and stress on your IT teams by not making them identify, purchase, install, and maintain all of the solutions from multiple vendors.
Partner with an industry leader committed to maximizing security for your students and faculty

• Microsoft has invested more than $15 billion on our cloud infrastructure and invests more than $1 billion each year on cybersecurity.

• Microsoft has unique visibility into an evolving threat landscape due to our hyper-scaled cloud footprint of more than 200 cloud services, over 100 datacenters, millions of devices, and over a billion customers around the globe.

• This visibility of billions of threat signals helps Microsoft provide unmatched threat and security intelligence to customers.

• Microsoft employs a team of over 3,500 cybersecurity experts around the world to provide all our customers with 24/7 protection.

• Along with threat intelligence, Microsoft products and solutions deliver over a thousand security and privacy controls to our customers, who can use them to find the protection that’s right for them.

• All of this has helped Microsoft become recognized as an industry leader in security. In fact, Gartner has named Microsoft as a leader in five different security magic quadrants over the past year.
While meeting the compliance standards your institution requires

Microsoft **conforms to a broad set** of international, country-specific, and industry-specific compliance standards—more than any other cloud provider.

Microsoft tests their solutions with rigorous third-party audits to ensure adherence to **strict security controls**.

Microsoft compliance standards help ensure **data confidentiality, integrity, and availability**.

<table>
<thead>
<tr>
<th>ISO 27001</th>
<th>ISO 27018</th>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
<th>Content Delivery and Security Association</th>
<th>FIPS 140-2</th>
<th>HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>FERPA</td>
<td>Cloud Control Matrix</td>
<td>European Union Model Clauses</td>
<td>BITS Shared Assessments</td>
<td>ENISA-IAF</td>
<td>FedRAMP JAB P-ATO</td>
<td>United Kingdom G-Cloud</td>
<td>GDPR</td>
</tr>
</tbody>
</table>
Microsoft’s security technology keeps you protected so you can focus on what matters

Streamline security and identity management of students and faculty
The identity capabilities of our technology make it easy for you to enable students and faculty to get the data they need while preventing unauthorized access attempts and identity theft.

Protect student and faculty data, at home and on campus
With Microsoft, you can empower everyone to collaborate with confidence knowing that data, research, and work is protected, no matter where they are in the world.

Defend institutional assets from cybercrime
Our solutions help you safeguard sensitive, high-value campus systems and effectively respond to increasingly complex cyberattacks on your institution.

Maximize physical campus safety and health for the entire community
Promote the wellbeing and security of everyone on campus while accelerating emergency response times to potential health and safety threats.
Streamline security and identity management of students and staff

Identity management is key to any university’s security posture. Without robust identity and security management capabilities, it would be impossible for university teams to confirm that their students and faculty are who they say they are when engaging online.

To start bolstering identity management, solutions such as Microsoft Azure Active Directory and Multi-Factor Authentication can help by providing single sign-on and multi-factor authentication capabilities for all students, staff, and faculty.

Microsoft Intune for Education enables institutions to proactively apply and manage identity access policies on the devices and apps your students and faculty use every day, all from a single location.

With Windows Autopilot, IT teams can take a zero-touch approach to device provisioning, deployment, and retirement, helping reduce the time and infrastructure required to maintain the device while ensuring groups can stay socially distant when managing devices.
Protect student and faculty data at home and on campus

With remote learning, institutions now have to secure devices working on networks around the world. This distribution increases the risk of an attack or breach on any institution, especially as data is continually being shared between students and faculty.

Solutions like Microsoft Defender for Office 365 leverage industry-leading AI and automation to protect institutions from advanced threats in emails, links, and collaboration tools.

For network security, Microsoft Defender Advanced Threat Protection is designed to help detect and respond to advanced network threats using a combination of endpoint behavioral sensors, cloud security analytics, and industry-leading threat intelligence.

With Microsoft Cloud App Security and Azure Information Protection, institutions gain visibility and control over data as it traverses, enabling them to detect risky behavior, track document access and prevent data leakage or misuse.
Defend institutional assets from cybercrime

Many universities have high-value, sensitive data that’s critical to protect from potential threats or breaches. These assets, whether they’re research, IP, or sensitive personal information—are sought after by hackers and malicious actors, making higher education institutions prime targets for attack.

Tools like Microsoft Secure Score and Azure Security Center can help universities understand their current security posture and how to improve it through reporting of different metrics and KPIs.

Azure Sentinel makes threat detection and response smarter and faster by collecting and analyzing data from all users, devices, and applications. With Sentinel’s cleaner pane of glass that delivers only high-quality, prioritized alerts, IT teams can detect previously uncovered threats and minimize false positives, saving time and preventing them from being overloaded.
Maximize physical campus safety and health for the entire community

Along with digital security and safety, institutions have always had to take measures to **bolster physical campus safety for their entire community**. With the COVID pandemic, institutions also need a way to **ensure the proper hygienic and health measures are taken** by everyone on campus.

With solutions like Azure Active Directory and Azure Digital Twin, institutions **can control access to and create models of physical locations** across campus.

For universities using IoT technology, Azure Sphere, CyberX, and Azure Sentinel provide multiple layers of protect to **protect those physical devices and equipment from hackers** and other malicious actors.

To help detect and manage potential COVID outbreaks, instructions are **creating no-code tools through Power Platform to track and respond to pandemic concerns**.

Many also use Microsoft 365’s Communication Compliance features to **detect threatening language between students and prevent suicidal behavior**, by monitoring for specific sentiments and keywords that would indicate these types of behaviors.
Find the right security suite for your needs

Whether you want baseline, free protection from M365 A1 security, or best-in-class, comprehensive extended detection and response (XDR) with M365 A5 security, Microsoft has you covered.

<table>
<thead>
<tr>
<th>Microsoft 365 A1 security</th>
<th>Microsoft 365 A3 security</th>
<th>Microsoft 365 A5 security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic security to protect essential productivity apps – at no cost to your institution</td>
<td>Advanced security and compliance with streamlined management to protect students, faculty, and staff</td>
<td>Best-in-class intelligent security and analytics to automate and maximize protection for your institution</td>
</tr>
</tbody>
</table>

Leverage essential device, identity, and access management, including conditional access and granular policy controls. to start on your journey to a zero trust, safe and secure campus.

**Everything in A1 plus:**
- Intune for Education
- Azure Active Directory (AAD) Free
- Data Loss Prevention
- Office 365 Rights Management
- Microsoft Intune
- Azure Active Directory Premium Plan 1
- Azure Information Protection Premium Plan 1
- Microsoft Advanced Threat Analytics
- Windows E3 Pro

**Everything in A3 plus:**
- Microsoft Intune
- Azure Active Directory Premium Plan 1
- Azure Information Protection Premium Plan 1
- Microsoft Advanced Threat Analytics
- Windows E3 Pro

**Everything in A5 plus:**
- Azure Active Directory Premium Plan 2
- Azure Information Protection Premium Plan 2
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Cloud App Security
- Microsoft Defender for Office 365
- Office 365 E5

Protecting users, their work, and the productivity tools that enable inclusive, effective teaching and better learning outcomes
And add cutting-edge cloud security for further protection

In addition to the primary M365 security licenses, Microsoft offers additional cloud security to extend your protection.

### Azure Sentinel

See and stop threats before they cause harm, with cloud and AI-powered security information and event management (SIEM) reinvented for the modern campus

- **Collect data at cloud scale**—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds
- **Detect previously uncovered threats and minimize false positives** using analytics and unparalleled threat intelligence from Microsoft
- **Investigate threats with AI and hunt suspicious activities at scale**, tapping into decades of cybersecurity work at Microsoft
- **Respond to incidents rapidly** with built-in orchestration and automation of tasks
- **Reduce noise from legitimate events** with built-in machine learning and knowledge based on analyzing trillions of signals daily – accelerating proactive threat hunting
- **View a prioritized list of alerts**, get correlated analysis of thousands of security events within seconds, and **visualize the entire scope of every attack**.
- **Simplify security operations and speed up threat response** with integrated automation and orchestration of common tasks and workflows
- **Automatically scale to meet your needs**, and only pay for the resources you use.

### Azure Defender

Bring powerful extended detection and response (XDR) to the cloud, protecting hybrid cloud workloads across campus against advanced threats

- **Identify threats across IaaS (infrastructure as a service) and PaaS (platform as a service)** using advanced analytics.
- **Use built-in behavioral analytics and ML to detect attacks and zero-day exploits**.
- **Monitor networks, machines, and cloud services** for known attack patterns and post-breach activity.
- **Connect to existing tools and processes** like Azure Sentinel and other SIEM systems or integrate partner security solutions.
- **Detect unusual attempts to access storage accounts and malware uploads** and scan container images for vulnerabilities.
- **Assess application vulnerabilities in virtual machines** with built-in vulnerability assessment.
- **Manage security across all your server workloads** running on premises, in Azure, and on other cloud platforms, **in one console**.
- **Protect IoT solutions** with real-time monitoring and analysis of security events.
Start maximizing your institution’s security now

Microsoft 365 makes it easy for you to start bolstering protection for your institution right away while building a stronger security posture over time.

### First 30 Days

**Powerful quick wins**

- Take note of your current Secure Score
- Turn on audit logging for Office 365
- Configure Microsoft 365 for increased security
- Review dashboards and reports in the Microsoft 365 security center
- Connect Microsoft 365 to Microsoft Cloud App Security
- Enable Azure Active Directory Identity Protection
- Review example information protection recommendations
- Turn on Microsoft 365 compliance center
- Engage with FastTrack
- Use App Discovery to identify applications in use
- Turn on Azure Sentinel

### First 90 Days

**Enhanced protections**

- Check Secure Score for recommended actions for your environment
- Review dashboards and reports in the Microsoft 365 Security Center and Cloud App Security
- Identify and implement software updates
- Check Compliance Manger to review status for regulations
- Implement enhanced protection for admin accounts
- Enable and enforce MFA and conditional access for all users
- Adapt and implement information protection policies
- Use data loss prevention policies in Microsoft 365
- Use Cloud App Security with Microsoft 365 for advanced alerting features

### Beyond

**Build on previous security measures**

- Plan next actions using Secure Score
- Review dashboards and reports in the Microsoft 365 Security Center and Cloud App Security
- Identify and implement software updates
- Integrate eDiscovery into your legal and threat response
- Implement Secure Privileged Access for identity components on-premises
- Use Cloud App and Azure AD Identity Protection Security to monitor for insider threats
- Refine information protection policies and operational processes
Create custom solutions with little to no technical experience needed

Microsoft’s Power Platform suite enables you to address challenges and streamline processes across your institution through low-to-no-code apps, bots, and the automation of manual tasks.

Below are a few examples of how some higher-education institutions are using the Power Platform today to enhance safety and security needs for their communities.

**Upstate Medical University**
- Using Power Apps, the Upstate Medical University created an online coronavirus assessment bot that enables users to assess their symptoms and determine whether they need to seek testing.
- With the tool, the university was able to provide quick and accurate information to over 8,000 users in its first week of deployment.

**Purdue University**
- Purdue University created a Higher Education Crisis Financial Impact Tracker with Power Apps. Purdue researchers were able to access the application through Teams and input information on research initiatives and how they’ve been affected.
- Now, with over 1,100 faculty members using the tool, Purdue was able to glean a clear picture of how COVID affected their research programs.

Check out this blog to learn more about how institutions are using Power Platform to tackle their safety and security challenges.
Microsoft has a broad ecosystem of security partners to help meet your institution’s needs.

Commvault is a recognized global leader in enterprise backup, recovery, and data management across any hybrid environment.

Circadence created Project Ares, which enables institutions to provide a framework for cybersecurity degrees and acts as an extension for cybersecurity courses and labs.

Project Edison is a safety and alert notification system that keeps people situationally aware and in contact with each other using a centralized communication hub.

SysCloud creates premier machine learning analytics software for cloud security and backup. SysCloud enables you to automate the restoration process for your Office 365 files.

Genetec is a global provider of IP video surveillance, access control and license plate recognition solutions unified in a single platform, called Security Center.

Gaggle is a suite of online software that provides deep insight and analytics on incidents when students use school-provided communication and collaboration tools.
Durham University made learning from home simpler and more secure for students and faculty

When COVID started to spread, Durham University had to rapidly transition to remote work and learning for their staff and students. To help lessen IT dependence on on-premises systems, the university partnered with Microsoft to realize the following benefits.

- **Simplified access to institutional assets and tools** with single sign-on capabilities to on-premises and SaaS applications using Azure Active Directory

- **Reduced the risk of compromised student and faculty accounts** using Microsoft Azure Multi-Factor Authentication

- Eased IT’s workload by **implementing self-service password reset functionality** for students and faculty

“By migrating to Azure AD, we’ve moved the responsibility of high availability to Microsoft, who, let’s face it, are scaled to do a better job than we could. Our services are much more resilient.”

CRAIG CHURCHWARD
Technical Specialist
Keiser University provided a secure environment for students and faculty—safeguarding sensitive information remotely

When COVID struck, Keiser University, in Florida, had to temporarily close 21 campuses to keep students and faculty healthy. To support all of those who were attending and holding classes remotely, Keiser turned to Microsoft to realize the following outcomes.

- **Prevented sensitive information from being downloaded and saved** to local drives using Windows Virtual Desktop and Azure Active Directory

- **Detected potential threats and issued alerts** with Microsoft Cloud App Security, Azure Advanced Threat Protection, and Azure Sentinel

- Established Azure Information Protections rules and labels to **automatically encrypt PII, credit card numbers, and other sensitive information**

"Knowing we could control how Keiser University data is used on faculty and staff devices, and disconnect inactive sessions, helps us sleep better at night."

ANDREW LEE
Vice Chancellor of Information Technology
The University of Southern Denmark revamped their security infrastructure to prevent cyberattacks.

At any time, the University of Southern Denmark (SDU) has many sophisticated, and sensitive research programs happening on campus. To help protect these critical assets, SDU partnered with Microsoft to reach new heights in security.

- **Improved detection of brute force, password spray, and other types of attacks** on with activity logging through Microsoft Advanced Threat Analytics

- **Automated threat investigation and remediation** with Windows Defender Advanced Threat Protection

- **Applied risk-based conditional access controls** to better secure institutional applications using Azure Active Directory Privileged Identity Management

“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 ... I have better analytics and detailed forensics to strengthen our overall security profile.”

BO S. DREIER
IT Security Specialist
George Washington University

George Washington University enhanced digital and physical security on campus with cloud technology.

George Washington University wanted to find a way to enhance both digital and physical security on-campus with cloud technology. To do so, they leveraged Azure Active Directory to bolster security for their community in the following ways.

- **Managed student access and detected suspicious activity** in physical buildings on campus.
- Implemented dynamic, role-based access policies to **easily adjust student and faculty access to apps and data** as needed.
- Provided students, staff, parents, and alumni with multifactorial authentication for access to email and data storage, helping lower the risk of them becoming vectors for attacks or threats.

“It is important that our students have clean data and can move around the campus freely, but also that they feel safe.”

MARK ALBERT
Director of Web and Identity Services
Next steps

Now, if you’re ready to get started and learn more, there’s a few next steps you can take.

➔ Schedule a security deep dive at aka.ms/EngageSSC

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

➔ Get started with a 31-day free trial of Azure Sentinel

➔ Accelerate deployment, migration, and adoption of Microsoft 365 with FastTrack

➔ Learn more about global threats by visiting Microsoft Security Intelligence

➔ Learn more about our partners:
  ➔ Syscloud
  ➔ Genetec
  ➔ Commvault
  ➔ Project Edison (see it in action)
  ➔ Gaggle
Sources

1. Microsoft Security Threat Intelligence, 2020
2. US Department of Education, Campus Safety and Security Data Analysis Cutting Tool, 2018
3. Infosec, Phishing in academic environments, 2019
4. Verizon, Public sector spotlight: Mobile security index, 2020
5. Campus Safety, Pandemic forcing campuses to make big access control changes, 2020
6. My Tech Decisions, Campuses are making changes to access control due to coronavirus, 2020