



Microsoft Education Security Toolkit

Secure IT, simplified for
every classroom and campus



Welcome Letter

At Microsoft, we understand that schools and institutions operate in some of the most targeted and complex digital environments. As cyberattacks grow in frequency and sophistication, cybersecurity has become mission-critical—not just for protecting sensitive student data, research, and intellectual property, but for ensuring the continuity of teaching, learning, and institutional operations.

Our commitment is to empower educational organizations to build secure, resilient, and trusted digital ecosystems that cultivate academic success without compromise.

Our vision for security on campus is anchored in simplicity, scale, and intelligence:

- We deliver simplified management with one integrated tech stack—designed to reduce incidents and safeguard learning and research environments.
- We bring AI-powered security solutions to help support data protection, compliance, and management at machine speed and scale.
- We help schools and institutions scale Security Operations (SecOps) with automation and integrated tools, while investing in the next generation of cyber-defenders through Student Security Operations Centers (SOCs) and skilling pathways.

These pillars form a resilient, adaptive security foundation that protects institutions of every size—empowering safe, innovative learning environments.

Education leaders recognize the need for timely, strategic action to protect learning environments, strengthen digital resilience, and prepare for the future of AI-powered education. This moment presents a powerful opportunity: institutions are safeguarding their campus and shaping the future of cybersecurity. By involving students in security operations and providing hands-on experience with AI-driven tools, education is evolving from reactive to proactive leadership and digital resilience.

Schools and institutions around the world are already leading the way:

- [Singapore Management University](#) adopted Microsoft’s Zero Trust framework Security Copilot, reducing response times, easing security team workload, and enabling faster, more confident IT decision-making.
- [Oregon State University](#) pioneered a student-staffed SOC with Microsoft Sentinel and Defender, providing hands-on cybersecurity experience while strengthening threat detection and response capabilities.
- [New York City Public Schools](#) manages 750,000 LTE-enabled student devices using Microsoft Intune, ensuring secure, scalable, and efficient device management across the largest school district in the U.S.

Microsoft’s unified security platform —built on Microsoft 365 —integrates Security Copilot, Sentinel, Defender XDR, Intune, Entra ID, and Purview, into a single, AI-powered system. This approach helps institutions secure devices, protect data, manage compliance, and respond to threats faster from a unified dashboard.

One of the most exciting developments is the rise of student-led SOC’s. It’s a powerful way to turn learners into cyber-defenders while creating meaningful career pathways.

Security is no longer just a line of defense—it’s a catalyst for innovation. With Microsoft’s trusted solutions, institutions can confidently adopt AI, enable secure remote learning, support global research, and protect what matters most: student data and educational integrity.

At Microsoft, we believe security is about more than protection—it’s about enabling what’s possible. Together, we can create secure, inclusive environments where learning thrives, research advances, and every student can explore technology with confidence.



Matt Jubelirer
General Manager,
Microsoft Education

Contents

Overview

- 5 [Microsoft Secure Future Initiative](#)
- 9 [Navigating this Security Toolkit](#)
- 11 [Empowering safer learning with Microsoft security tools](#)

Tools

- 13 [Microsoft Security tools](#)

Customer Impact Stories

- 16 [Securing Learning Environments: K-12 Campus Impact Stories](#)
- 20 [Higher Education Security Innovation in Practice](#)
- 24 [More Customer Security Stories](#)

Planning

- 29 [Strategic planning for safer learning environments](#)
- 31 [Assess current your campus security posture](#)
- 34 [Security governance and policies](#)
- 36 [Technology security strategy](#)
- 38 [Organizational readiness](#)
- 40 [Financial and strategic justification](#)

Implementation

- 43 [K-12 Scenarios for Implementation](#)
- 47 [Higher education scenarios for implementation](#)

Research

- 52 [Microsoft security in education: From deployment to campus impact](#)
- 54 [Data and analytics](#)
- 56 [Academic and industry findings](#)
- 58 [Glossary of terms](#)
- 59 [Next steps checklist](#)

Overview

In this section

[Microsoft Secure Future Initiative](#)

[Navigating this Security Toolkit](#)

[Empowering safer learning with Microsoft security tools](#)



Microsoft Secure Future Initiative

Microsoft helps educational organizations stay ahead of evolving cyberthreats with a purpose-built cybersecurity platform that safeguards sensitive student, educator, and staff data. Our trusted, cloud-first solution is designed to reduce IT complexity while helping schools consolidate tools, streamline security operations, and simplify procurement.

With integrated, AI-powered threat detection and response, schools and institutions can improve visibility, accelerate remediation, and reduce manual workloads—freeing IT teams to focus on enabling learning. Built on global security standards and grounded in zero trust principles, Microsoft 365 platform assumes breach and verifies explicitly, ensuring a resilient defense that adapts to the needs of each campus environment.

Every layer of our approach is guided by the Secure Future Initiative (SFI)

- **Secure by Design:** Security comes first when designing any product or service. SFI's UX Toolkit helps reduce user-targeted attacks by improving default security features and reducing friction. It has been adopted by product teams across Windows, Azure, and Defender.
- **Secure by Default:** Security protections are enabled and enforced by default, require no extra effort, and are not optional. Microsoft 365 Copilot Control System (CCS), Windows Smart App Control, and enforced MFA for Azure and Microsoft Entra ID show how security settings are enabled and maintained.
- **Secure Operations:** Security controls and monitoring will be improved to meet current and future threats. With automated detection, fraud prevention, and integrated policy enforcement, SFI reinforces Secure Operations with real-world effectiveness.

Enable secure learning environments

Microsoft is committed to helping institutions create safe, secure, and inclusive learning environments to protect student data, minimize cyber threats, and simplify IT management.

- **Device hardening and identity protection:** Strengthen environments with Windows 11's built-in features, enforcing identity protection through Entra ID, and modernizing systems with solutions like Intune and Defender XDR.
- **Endpoint and app protection:** Safeguard student devices, help enforce compliance, and protect access to apps across the cloud and endpoints with Intune and Defender for Cloud Apps.
- **Operating system protections:** Use Windows 11's built-in security features like Smart App Control, virtualization-based security, and kernel-mode protections to establish a secure foundation for learning environments.
- **Hardware-based safeguards:** Foster device integrity with hardware features like TPM 2.0 and the Microsoft Pluton security processor that protect data and support secure boot and encryption.

"Microsoft runs on trust, and trust must be earned and maintained. Our pledge to our customers and our community is to prioritize your cyber-safety above all else."

— Charlie Bell,
EVP, Security at Microsoft

Explore the [Windows Security Book](#) to learn how Microsoft helps education institutions create secure, trusted learning environments. Discover best practices, tools, and strategies to strengthen security and support student safety at scale.

Common challenges in K–12 and Higher Education

Identity security

K-12	HIGHER EDUCATION	MICROSOFT SOLUTION
Device flexibility: Secure MFA for 1:1 or shared devices Mixed environments: Personal student devices and shared classroom computers Age considerations: Age-appropriate authentication for all grade levels	High user turnover: Constant enrollment and graduation External partners: Guests, vendors, researchers Multiple departments: Separate schools and colleges Alumni access: Ongoing graduate connections Complex credentials: Managing all logins and permissions	Entra ID • Certificate-based authorization • Conditional access policy • External identities • FIDO 2 key • Multi-tenant organizations • Temporary access pass • User/Group lifecycle policies • Verified credentials • Windows Hello School Data Sync (SDS)

Data security and compliance

K-12	HIGHER EDUCATION	MICROSOFT SOLUTION
Student data protection: Protect student data as a legal duty Multi-country compliance: Helps meet compliance in multiple countries	Sensitive data protection: Protect sensitive research, health, admissions, financial data Multi-country compliance: Helps meet compliance in multiple countries Insider threat prevention: Prevent insider threats	Purview • DLP • Information barriers • Information protection • Insider threat protection Security Copilot

Compliance requirements

K-12	HIGHER EDUCATION	MICROSOFT SOLUTION
Regulatory compliance: Helps meet FERPA, HIPAA, GDPR, EU AI Act, and data retention requirements	Regulatory compliance: Helps meet FERPA, HIPAA, Title IX, GBLA, GDPR, and EU AI Act requirements	Entra ID • Audit and reporting Security Copilot Purview • Communication compliance • DLP • eDiscovery • Information barriers • Information protection • Records management

Security management

K-12	HIGHER EDUCATION	MICROSOFT SOLUTION
Resource constraints: Manage limited technical resources and staffing Attack response: Respond to high volume of cyberattacks Insurance requirements: Meet cyber insurance coverage requirements	Decentralized IT: Manage decentralized IT environments Budget limitations: Address limited budget and security expertise Student programs: Implement student SOC programs	Defender XDR Security Copilot Sentinel

Device security

K-12	HIGHER EDUCATION	MICROSOFT SOLUTION
Device access: Provide secure access for 1:1 and shared devices District compliance: Support device compliance across large districts Threat protection: Protect against malware and unauthorized access	Personal device access: Provide secure access for personal devices Breach prevention: Prevent data breaches and malware Compliance requirements: Helps meet device compliance requirements	Defender for Endpoint • EDR policies • Network protection • Web content filtering Entra ID • Conditional access with device compliance • Internet access and private access • Web content filtering Intune • App protection policies • Device compliance policy Purview • DLP for data sharing

App security

K-12	HIGHER EDUCATION	MICROSOFT SOLUTION
M365 deployment: Deploy secure M365 apps for students Policy management: Manage platform and app security policies Threat protection: Protect against phishing and malware in apps	Multi-cloud environments: Run secure multi-cloud and multi-platform environments Hybrid security: Manage on-premises and cloud app security Identity federation: Support federated and multi-tenant identities	Defender • Defender for Cloud apps • Defender for Identity • Defender for Office 365 Purview • SharePoint policies Entra ID • Federated identity • Multi-tenant organizations • Group and Teams policies Sentinel

AI security

K-12	HIGHER EDUCATION	MICROSOFT SOLUTION
Safe AI access: Empower students with safe AI access Misuse prevention: Address concerns over AI misuse and information access Communication protection: Protect communications and sensitive data with AI tools	Advanced threat defense: Defend against complex and scalable AI-driven attacks Insider threat prevention: Prevent insiders from exploiting AI for data access Expanded access security: Strengthen data security as AI expands access	Copilot • Enterprise data protection • Safety and security settings Defender XDR • Threat monitoring Sentinel Purview • Communication compliance • DLP policy • Information barriers • Information protection • Insider threat protection • Security Copilot

Navigating this Security Toolkit

The Microsoft Education Security Toolkit helps education leaders across schools, institutions, local and regional departments, and ministries of education to simplify and secure their IT environments while enabling safe and innovative learning experiences. By leveraging a single, integrated Microsoft security stack, AI-powered threat detection, and zero trust principles, schools and institutions can reduce IT complexity, accelerate incident response, and safeguard students, faculty, and research.

Organized into five sections—[Overview](#), [Customer Experiences](#), [Plan](#), [Implement](#), and [Impact](#)—you can easily explore frameworks, guidelines, real-world examples, and proven strategies using the navigation tabs on the right-hand side of the toolkit, guiding you from understanding the security landscape through successful implementation.



Using Microsoft 365 Copilot

Microsoft 365 Copilot serves as your AI assistant—helping you navigate security documentation and explore capabilities through natural language prompts. Ask Copilot to explain unfamiliar security concepts, break down complex implementation steps into manageable phases, or identify tools and resources tailored to your environment. Whether you're a security expert or just getting started, Microsoft 365 Copilot helps you navigate documentation with clarity and confidence.

Choose the right starting point

Navigate directly to the sections most relevant to your current needs:

- **New to education security?** Start with the **Overview section** to understand Microsoft's security vision and why security matters now more than ever.
- **Building your institution's case?** Explore the **Customer Stories section** to see how peer institutions are achieving real results with Microsoft solutions.
- **Developing your strategy?** Use the **Plan section's** frameworks for identifying gaps and aligning security with your institutional goals.
- **Deploying solutions?** The **Implement section** provides detailed guidance on Microsoft security solutions and best practices.
- **Looking ahead?** Visit the **Research section** for the latest Microsoft insights, industry findings, and academic research on education security.

This toolkit serves as both a comprehensive guide and a practical workbook. Use its assessment templates, checklists, and frameworks to build a program that protects your institution while enabling innovation. Security is more than just protection—it is about empowering your institution to confidently embrace digital transformation, AI adoption, and the innovative teaching methods that define modern education.

Exploring customer experiences

Learn how schools and institutions have successfully strengthened their security posture with Microsoft. From Onslow County Schools balancing security with learning access to Oregon State University building a student-led Security Operations Center, these experiences offer actionable insights to inform your own security journey. Consider them as you explore implementation strategies, address common challenges, and demonstrate value to stakeholders.

Get started with security assessments

Throughout this Security Toolkit, you'll find practical exercises and assessment prompts to evaluate your school or institution's security posture. These tools support you in identifying gaps, prioritizing improvements, and building a roadmap for comprehensive protection. Begin by reviewing your current device and app management coverage, data protection capabilities across cloud and on-premises environments, and compliance with local, federal, and global privacy regulations.



[Copilot Prompt](#)

Act as a security administrator for a **[K–12/Higher Ed]** institution. Identify the top most common, classify each by severity and NIST CSF category, and recommend the specific Microsoft tools that address each gap. Summarize your recommendations in a table and list what additional information you need from me to refine the assessment.

TIP

Share items like Secure Score results, recent incidents, or high-risk systems. Concrete signals help Copilot generate gap analysis based on your real environment instead of generic assumptions.

Empowering safer learning with Microsoft security tools

Cybersecurity in education is about more than protection, it's about enabling safe, resilient learning. Schools and institutions operate in uniquely valuable and vulnerable environments, where personal data, research, and digital tools intersect daily. As digital learning expands, so do the challenges—and the opportunities to strengthen trust, access, and institutional resilience.

Microsoft Security helps schools and institutions stay ahead with an integrated security stack built for education, grounded in zero trust and secure-by-design principles. Our AI-powered solutions simplify management, support scalable operations, and prepare teams for the future. Security is a strategic priority that protects learning, empowers staff, and builds trust across the education community.

Real impact across education

How schools and institutions are turning security into opportunity.

- **Strategic enabler:** Use security to accelerate digital learning, advance equity, and support workforce development.
- **Trust builder:** Strengthen confidence across student access, alumni engagement, and institutional reputation.
- **Operations simplifier:** Minimize disruptions and automate response with integrated tools and intuitive dashboards.
- **Career launcher:** Prepare students for cybersecurity careers through hands-on experience and student SOC's.
- **Growth enabler:** Scale protection across teaching, learning, and research environments with flexible, cloud-first solutions.
- **Resilience driver:** Build institutional readiness with secure-by-default, secure-by-design solutions grounded in Zero Trust.
- **Innovation catalyst:** Empower educators and IT teams to adopt new technologies with confidence, backed by built-in compliance and security.

Tools

In this section

[Microsoft Security tools](#)



Microsoft Security tools

Navigating security solutions for education

Microsoft offers a comprehensive security tools tailored to the needs of educational organizations. To help you quickly grasp the purpose of each tool and how it fits into your workflow, we've provided clear summaries and thoughtfully curated tools within each category.

Whether you're securing student devices, navigating compliance requirements, or equipping your team for tomorrow's cybersecurity challenges, Microsoft's integrated approach delivers adaptable, cost-effective protection built for the needs of education.



Windows 11 Security

Provide students, faculty, and staff with comprehensive security protection from chip-to-cloud with hardware-backed safeguards that defend against threats.

FEATURES

- Secured-core PC protection
- Windows Hello passwordless authentication
- BitLocker encryption
- Microsoft Defender Antivirus (built-in)
- Smart App Control
- Copilot+ PC on-device AI security



Microsoft Security Copilot

Protect your institution at the speed and scale of AI with a generative AI-powered assistant for daily operations in security and IT.

FEATURES

Additional Security Copilot agents work across Defender, Entra, Purview, Intune, Sentinel, and third-party security tools.



Microsoft Defender

Detect and respond to attacks against your devices, identities, apps, email, and clouds with leading extended detection and response (XDR) products.

FEATURES

- Defender XDR
- Defender for Office 365
- Defender for Endpoint
- Defender for Identity
- Defender for Cloud Apps



Microsoft Purview

Safeguard data wherever it lives with a collection of unified information protection, governance, and compliance products.

FEATURES

- Information Protection
- Data Loss Prevention
- Insider Risk Management
- Communication Compliance
- Information Barriers
- Data Governance: Data Map and Unified Catalog
- eDiscovery
- Data Lifecycle Management
- Compliance Manager
- Data Security Posture Management (DSPM) for AI



Microsoft Entra

Verify every identity and access request across your clouds, platforms, and devices with a collection of identity and access products. Available as part of Entra Suite for Education.

FEATURES

- Entra ID
- Conditional Access
- ID Protection
- External ID
- ID Governance
- Privileged Identity Management
- Entra Domain Services
- Verified ID



Microsoft Intune

Strengthen device security and enable seamless work experiences with endpoint management products.

FEATURES

- Intune for Education
- Windows Autopilot
- Mobile Application Management (MAM)
- Device Compliance
- Endpoint Privilege Management



Microsoft Sentinel

Get unmatched visibility into threats with a security information and event management (SIEM) solution that includes a unified data lake for cost-effective long-term retention and advanced analytics.



Microsoft Priva

Respect student and staff privacy with proactive risk mitigation and compliance management that helps schools meet FERPA, GDPR, and other privacy requirements.

FEATURES

- Privacy Risk Management
- Subject Rights Requests

Customer Impact Stories

In this section

[Securing Learning Environments: K-12 Campus Impact Stories](#)

[Higher Education Security Innovation in Practice](#)

[More Customer Security Stories](#)



Securing Learning Environments: K-12 Campus Impact Stories

Whether managing hundreds of thousands of devices, balancing security with educational access, or protecting sensitive data with limited IT resources, K-12 districts face complex security challenges. See how three leading schools have transformed their approach to security with Microsoft solutions.





New York City Public Schools



NYC Public Schools used Microsoft Intune to manage 750,000+ devices across 1,800 schools in a matter of days.

Challenge

When COVID-19 shifted learning online, New York City Public Schools faced an extraordinary challenge: deploying and managing devices for over 750,000 students in days rather than months.

NYC Public Schools chose Microsoft Intune for its cross-platform capabilities and cost-effectiveness, as it was already included with their Microsoft 365 Education licenses. The district deployed 550,000 LTE-enabled iPads and 200,000 Chromebooks, prioritizing students in temporary housing and those without internet access. Working closely with Microsoft's Intune team, they compressed a six-month implementation into mere days, with daily—sometimes hourly—support during critical deployment phases.

Impact

The impact was immediate and lasting. Intune provided centralized management across all device types, eliminated the need for physical software distribution, and enabled silent, transparent updates that minimized disruption to learning.

Today, NYC Public Schools continues to use Intune to automate deployments, support digital assessments citywide and monitor device health and security—modernizing IT operations while keeping learning alive for students.

"We initiated the largest rollout of the most LTE-enabled devices in the shortest amount of time in history. Every minute spent waiting for a device to work is lost teaching time. Intune allows us to manage everything silently and transparently, providing a single pane of glass to understand hundreds of thousands of assets."

—Alexander Horwatt

Executive Director of Technology Innovation
NYC Public Schools

Key questions

- How could rapid device deployment capabilities, like NYC PS's pandemic response, prepare your district for unexpected disruptions?
- What impact would centralizing management of diverse device platforms have on your IT team's efficiency and security posture?
- How might ensuring every student has connected devices, regardless of circumstances, advance your district's equity goals?

Microsoft tools

- [Microsoft 365 Education](#)
- [Microsoft Intune](#)
- [Windows Autopilot](#)

[→ Read the full case study](#)



Onslow County Schools



Onslow balanced security and access with Microsoft Intune Endpoint Privilege Management.

Challenge

Onslow County Schools, the 11th largest district in North Carolina, needed to give students and educators access to essential educational software—including secure exam browsers and design software—without compromising security. As Chief Technology Officer Jeff Pittman explains, “Microsoft technology is the fabric of our entire organization,” but the district needed to maintain strict security while enabling innovation.

Impact

By deploying Microsoft Intune Endpoint Privilege Management (EPM) across 14,000 devices for grades 6-12, Onslow upgraded its security posture and enhanced its educational outcomes. The solution allows students and educators to run approved applications without administrative access, maintaining least privileged security principles. Since implementation, the district has nearly tripled its Microsoft Secure Score.

The impact extends beyond security. Educators now receive new software access within 30 minutes versus the previous 48-hour wait. With seamless cloud management through Azure, Onslow’s IT team can support devices on or off the network, ensuring continuous learning without sacrificing security.

“Using EPM to run the anti-cheating browser has helped us improve academic outcomes so that students have a more focused, secure, and equitable testing environment.”

—Tiffany Rhodes,
Educator
Onslow County Schools

Key questions

- How could balancing security with educational access, like Onslow’s EPM approach, address your district’s competing priorities?
- What impact would reducing software deployment time from 48 hours to 30 minutes have on your teaching staff’s effectiveness?
- How might tripling your security score while improving educational outcomes transform your district’s technology strategy?

Microsoft tools

- [Azure](#)
- [Microsoft Defender for Identity](#)
- [Windows Autopilot](#)
- [Microsoft Intune](#)
- Microsoft Intune Suite
- Microsoft Intune Endpoint Privilege Management

[➔ Read the full case study](#)



Westminster School

Westminster School leverages Microsoft Defender Experts to safeguard student and staff data across their campus.

Challenge

Westminster School, faced growing cybersecurity challenges with a lean IT staff protecting sensitive data for 1,350 students and 550 staff members. The team managed three to four security incidents each week, contended with excessive false-positive alerts, and carried the critical responsibility of safeguarding visa information, medical details, and personal data.

Westminster became the first school in Australia to adopt Microsoft Defender Experts for XDR. Head of IT Chris Rowtcliff describes the service as “an extension of our own team.” The managed service provides end-to-end security protection with human-led expertise, reducing alert noise “nearly down to zero” while ensuring every genuine threat is fully investigated.

Impact

This partnership quickly proved its value. When a student accidentally clicked a malware link, Defender Experts blocked the threat and traced it to another student. This insight allowed the school to respond with educational support rather than limiting the action to technical remediation.

The impact extends beyond threat response. The team now remediates almost 100% of action items, benefits from weekly expert check-ins, and contributes to Microsoft’s product development through collaborative feedback. With advanced tools and trusted expertise, the school has created a safer environment while building resilience against future threats.

“I can’t overstate the peace of mind that Defender Experts for XDR has brought us. We feel so much less overwhelmed knowing the school and the students are safe.”

—Chris Rowtcliff,
Head of IT
Westminster School

Key questions

- How could managed security services like Defender Experts for XDR help your small IT team focus on strategic initiatives rather than alert fatigue?
- What value would “experts on demand” bring to your school’s ability to learn from incidents and prevent future threats?
- How might reducing security noise to “nearly zero” transform your IT team’s effectiveness and wellbeing?

Microsoft tool

- [Microsoft Defender](#)

[→ Read the full case study](#)

Higher Education Security Innovation in Practice

From protecting sensitive research data to securing global student populations, higher education institutions face unique security challenges that demand innovative solutions. Discover how three leading universities have transformed their security posture while advancing their educational missions.





Oregon State University



Oregon State University implemented Microsoft Sentinel and Defender to protect research data, improving detection speed from weeks to minutes.

Challenge

In 2021, a major cybersecurity incident threatened OSU's vital research data and underscored the urgent need to protect their reputation as a R1 research institution. Chief Information Security Officer David McMorries notes, "We want to have an environment where science, learning, and research can be done safely in a cyber environment."

Impact

OSU implemented Sentinel and Defender with Microsoft 365 Education licensing, to make SOC their security foundation. With Microsoft engineering support, they achieved five years of security maturity in two years. Thousands of incidents were reduced to about 30 daily, with detection times improving from weeks to minutes. Sentinel became their "revolutionary" single pane for threat response.

OSU also integrated Microsoft Security Copilot to empower their student-staffed SOC. Student analysts use AI to help write advanced queries and automate processes, gaining critical workforce skills while protecting research. This dual mission—securing research while educating future cybersecurity professionals—exemplifies OSU's commitment to protection and education.

"Microsoft Copilot for Security will be a tremendous teaching tool for the students that work in OSU's SOC."

—Emily Longman

Security Operations Center
Manager Oregon State University

Key questions

- How could student-staffed security operations, enhanced by AI tools like Copilot for Security, address both your security needs and workforce development goals?
- What impact would reducing incident detection time from weeks to minutes have on protecting your sensitive research and student data?
- How might achieving "five years of maturity in two years" transform your institution's ability to balance open collaboration with robust security?

Microsoft tools

- [Microsoft Sentinel](#)
- [Microsoft Defender](#)
- [Microsoft Security Copilot](#)
- [Microsoft Entra ID](#)
- [Microsoft 365 Education](#)

[→ Read the full case study](#)



RMIT University



RMIT University deployed Microsoft Entra Verified ID for instant digital credentials serving 95,000 students globally.

Challenge

RMIT University, serving 95,000 students across 230 countries, recognized the need to upgrade student credentialing in an increasingly digital world. As Enterprise Architect Ajay Radhakrishnan explains, they focused on “missed opportunities” in identity technology while emphasizing lifelong learning connections. The challenge: creating secure, verifiable credentials that comply with global data protection laws while reducing the 14-day wait for physical ID cards.

RMIT’s Blockchain Innovation Hub partnered with Microsoft to implement Entra Verified ID, developing three use cases: student access to library and campus discounts, alumni transcripts for employment, and verifiable training certifications.

Impact

The pilot proof-of-value showed that credentials could be issued in seconds instead of 14 days. Students now control their own digital credentials through mobile devices, accessing everything from library services to future employment verification through a single QR code. The solution builds on RMIT’s existing Azure AD infrastructure and supporting open standards for interoperability with other partners in the future.

“The COVID-19 pandemic really accelerated that need because we didn’t want students to come to campus to pick up their ID cards. We used Microsoft Entra Verified ID to digitize the process and gain a lot of efficiencies.”

—[Michael Fairbairn](#),
Associate Director at
the Blockchain Innovation Hub
RMIT University

Key questions

- How could instant, blockchain-verified credentials transform your institution’s student experience from enrollment through alumni engagement?
- What operational efficiencies might emerge from eliminating physical ID cards while enhancing security and compliance across global jurisdictions?
- How might student-controlled, portable credentials that connect to broader ecosystems create value beyond traditional campus boundaries?

Microsoft tools

- [Microsoft Entra ID](#)
- Microsoft Entra Verified ID

[→ Read the full case study](#)



University of Venda



South Africa’s University of Venda migrated to Azure, achieving 99% uptime for 15,000 students.

Challenge

University of Venda (Univen), serving 15,000 students in South Africa, faced significant infrastructure challenges. Scattered on-premises servers caused frequent downtime while six-month procurement cycles hindered growth. As CIO Sam Khoza explains, their mission was to “support the university’s strategy through modern technologies” to produce globally competitive graduates.

Impact

Univen migrated 18 core systems to Microsoft Azure with Microsoft Unified Support. The migration included their document management system, HR and finance platforms, and Moodle LMS. The results were immediate. Availability rose to 99%, with zero reports of system inaccessibility even during peak exam periods.

Univen became one of the first universities in Africa to use Security Copilot with Sentinel, Defender, and Purview. Khoza notes, “As a pioneer university in Africa to implement Microsoft Security Copilot, we are leading the way in AI-powered security. It’s given us faster threat detection, smarter responses, and greater confidence.” The partnership with Microsoft Unified Support provided technology and built internal capabilities, empowering the ICT team to handle complex tasks and drive innovation.

“What used to require half a year to provision can now be easily completed on Azure within a matter of hours.”

—Vusani Nengovhela
Server Engineer
University of Venda

Key questions

- How could reducing infrastructure provisioning from six months to hours transform your institution’s ability to respond to educational needs?
- What impact would 99% service availability have on your students’ learning experience and staff productivity?
- How might becoming a regional pioneer in AI-powered security position your institution as a technology leader while protecting critical data?

Microsoft tools

- [Microsoft 365 for Education](#)
- [Azure](#)
- [Microsoft Sentinel](#)
- [Microsoft Security Copilot](#)
- [Microsoft Defender](#)
- [Microsoft Purview](#)
- [Exchange Online](#)

[➔ Read the full case study](#)

More Customer Security Stories





Memphis-Shelby County Schools

K-12 | 214 campuses | 110,000 students

Solution

Built custom data tools with Power Apps & Power Automate to create custom data gathering and reporting tools that address their diverse operational needs and saved costs on new software adoptions.

Tools

Azure SQL · Power Apps · Power Automate · Dataverse · Power BI · Power Pages

[→ Read full story](#)



Newington College

K-12 | 3 campuses | 3,200 students

Solution

Newington College partnered with Microsoft Education and Quorum to implement comprehensive cybersecurity solutions including Quorum's Cyber One MDR, Microsoft 365, and Intune following a security incident that highlighted their need for enhanced education technology protection and management.

Tools

Azure · Microsoft 365 Education · Microsoft Defender for Endpoint · Microsoft Defender for Identity · Microsoft Intune · Microsoft Sentinel · Microsoft Defender for Cloud

[→ Read full story](#)



New York City Department of Education

K-12 | 1,600 campuses | 920,000 students

Solution

When New York City's 1.2 million students faced pandemic-driven school closures and reopenings, the Department of Education rapidly deployed a cloud-based remote learning platform on Azure Synapse Analytics, achieving high performance, streamlined management, and enterprise-grade security.

Tools

Azure · Azure Virtual Desktop · Azure Blob Storage · Azure Data Lake Storage · Azure Synapse Analytics · Microsoft 365 Education · Microsoft Teams · Microsoft Purview · Power BI · Windows 11

[→ Read full story](#)



Orange Unified School District

K-12 | 42 campuses | 26,000 students

Solution

Orange Unified School District successfully deployed 30,000 devices to students and staff using Microsoft 365 Education and Windows PCs, enabling their small IT team to streamline management, strengthen security, and enrich the learning environment for future student success.

Tools

Microsoft 365 Education · Microsoft Entra ID · Microsoft Defender for Endpoint · Microsoft Intune · Windows Autopilot · Windows 11

[→ Read full story](#)



Wichita Public Schools

K-12 | 90 campuses | 47,000 students

Solution

Wichita Public Schools, serving nearly 50,000 students and 5,600 educators, is exploring Microsoft 365 Copilot with data protection to deliver more personalized and diverse learning experiences tailored to individual student needs.

Tools

Azure · Microsoft 365 Education · Microsoft Teams · Office 365 · Windows 11

[➔ Read full story](#)



Babson College

Higher Education | 2 campuses | 3,700 students

Solution

Babson College modernized its outdated infrastructure by implementing Microsoft 365 Copilot, Azure AI, and Microsoft 365 Education to develop predictive models for identifying at-risk students, create AI-powered learning tools like a mathbot for STEM courses, and prepare students with AI skills for their careers.

Tools

Power BI · Microsoft 365 Education · Microsoft 365 Copilot · Azure OpenAI

[➔ Read full story](#)



Howard University

Higher Education | 1 campus | 11,000 students

Solution

Howard University, a historically Black institution, overcame a 2021 ransomware attack to double its security score within a year by migrating to Microsoft Azure and partnering with Cloudforce, demonstrating how resource-constrained universities can strengthen security, increase efficiency, and reduce costs through strategic cloud adoption.

Tools

Azure · Azure Virtual Desktop · Microsoft Entra ID

[➔ Read full story](#)



Rowan University

Higher Education | 6 campuses | 23,000 students

Solution

Rowan University modernized its IT infrastructure with Microsoft Azure's cloud-smart strategy, resulting in enhanced accessibility, reliability, and security while giving professors up to 50% more instructional time, with plans to expand into AI technologies.

Tools

Azure · Microsoft 365 Education · Microsoft Intune · Microsoft Sentinel

[➔ Read full story](#)



University of Illinois Urbana-Champaign

Higher Education | 1 campus | 56,000 students

Solution

The University of Illinois Urbana-Champaign successfully migrated 350,000 user identities to Microsoft Entra ID in one weekend using a people-centric approach, offering valuable lessons for other organizations facing similar identity management challenges.

Tools

Microsoft Entra ID

[→ Read full story](#)



University of Washington

Higher Education | 3 campuses | 52,000 students

Solution

The University of Washington's Information School migrated its cybersecurity course labs to Azure Lab Services, transforming costly on-premises equipment into flexible virtual machines that simplified access, reduced administrative overhead, and better supported student learning objectives.

Tools

Azure · Azure Lab Services · Azure Compute

[→ Read full story](#)

Planning

In this section

[Strategic planning for safer learning environments](#)

[Assess current your campus security posture](#)

[Security governance and policies](#)

[Technology security strategy](#)

[Organizational readiness](#)

[Financial and strategic justification](#)



Strategic planning for safer learning environments

Securing your campus starts with a plan

School IT and security teams are more than technology guardians—they're essential partners for shaping safe, resilient learning environments and advancing your school's mission. Security leaders not only protect devices and data, but the future of every student and educator they support.

This planning guide provides a structured approach to building a comprehensive security strategy tailored for education. Before implementing Microsoft Security tools and programs, it helps you align your goals, assess your environment, and prioritize what matters most. Whether you're managing IT for a single K-12 school or a leading security for a multi-campus higher education institution with complex research needs, this guide equips you to lay a solid base for effective, scalable cybersecurity.



Copilot Prompt

Here is the link to our latest security strategy [insert link].

Create a communication plan and message templates explaining our new security strategy to teachers and staff. Include versions for educators, school leaders, and IT, along with FAQs addressing common concerns.

TIP

Describe staff sentiment—whether they feel overwhelmed, cautious, or curious. Copilot can adjust tone and messaging to address real concerns and encourage adoption.

Chart your course to safe learning

K-12 districts prioritize straightforward, high-impact security. Microsoft 365 A3 provides a strong foundation with essential security protections like multi-factor authentication (MFA), [Defender for Endpoint Plan 1](#), and [Intune](#) for device management. These tools help secure student learning while keeping IT operations manageable.

Defender for Endpoint Plan 1 is included in Microsoft 365 A3 for Faculty licenses but not in Student Use Benefit subscriptions. For student devices, consider additional licensing or alternative protections based on your security requirements and budget.

Microsoft 365 A5 introduces advanced capabilities for threat detection, compliance management, and AI governance, helping schools stay ahead of evolving risks. Explore the full [feature comparison](#) to find the right fit for your learning environment.

Higher education institutions face unique challenges—from safeguarding sensitive research to managing sprawling multi-campus networks and meeting rigorous regulatory standards. They require a comprehensive security framework that scales across diverse environments and adapts to complex governance needs. Microsoft’s advanced security offerings support this with integrated tools for identity protection, data loss prevention, and secure collaboration—designed to meet the demands of education.



Copilot Prompt

Compare Microsoft 365 A3 or A5 license security features for our **[K–12/Higher Ed]** environment, focusing on security, compliance, AI governance, and device management. Based on our priorities, recommend which plan fits best and why. Present results in a decision matrix and list key criteria leaders should consider.

TIP

Describe staff sentiment. Copilot can adjust tone and messaging to address real concerns and encourage adoption.



Copilot Prompt

Create a 30/60/90-day phased rollout plan for phishing-resistant MFA, starting with administrative accounts. Include prerequisites, change management steps, training needs, and risks. Identify which user groups require exceptions or pilot testing.

TIP

Tell Copilot which user groups often struggle with sign-ins or device access. This helps shape an MFA rollout that minimizes classroom disruption and supports groups needing extra help.

High-impact first steps while you plan

ENABLE PHISHING-RESISTANT MFA:

Activate multi-factor authentication for all users using [Microsoft Entra ID](#). Phishing-resistant methods like passkeys (FIDO2), Windows Hello for Business, and certificate-based authentication provide the strongest protection against credential theft. You can block more than [99.9% of account compromise attacks](#) by enabling multi-factor authentication across your accounts.

PLAN FOR MFA DEPLOYMENT

Consider a phased approach that starts with administrative accounts and high-risk users, then expands institution-wide. While MFA provides exceptional security benefits, implementing phishing-resistant authentication across an educational institution requires careful planning. Microsoft provides [comprehensive deployment guidance](#) to support your rollout.

ACTIVATE MICROSOFT DEFENDER

Use [Microsoft Defender](#) and the [Microsoft Secure Score](#) posture assessment as your baseline for ongoing improvements.

Assess current your campus security posture

You can't protect what you don't know you have.

The first step in planning a comprehensive security program is understanding where your organization currently stands. This lets you discover new opportunities to enhance your educational mission through better protection, streamlined compliance, and operational efficiency.

Use Microsoft's integrated security solutions to assess your readiness, prioritize your investments, and deliver immediate value.

Build on Windows 11 security foundations

Your security strategy starts at the device level. [Windows 11](#) delivers chip-to-cloud security with built-in protections:

- **Defend with hardware-backed security:** [Use Trusted Platform Module \(TPM\) 2.0](#) and [secured-core PC](#) protection to defend against firmware attacks and credential theft.
- **Enable passwordless authentication:** Implement [Windows Hello for Business](#) with biometrics or PIN—especially valuable for K-12 students.
- **Protect applications and data:** Deploy [Smart App Control](#) to block malicious applications while [BitLocker](#) encrypts drives.

Organizations using Windows 11 report a [62% reduction in security incidents](#). This secure foundation integrates seamlessly with [Microsoft Intune](#) and [Defender for Endpoint](#).



Protect AI innovation with built-in safeguards

Microsoft provides layered AI security protections.

[Copilot+ PCs](#): Include secured-core protection and [Microsoft Pluton](#) security processor. Neural processing units (NPUs) enable local AI processing, keeping sensitive data on-device rather than in the cloud for enhanced privacy.

[Microsoft 365 Copilot](#): Enterprise-grade security works automatically:

- **Respect existing permissions:** Maintain your institution's access controls and sensitivity labels.
- **Block harmful content:** Filter adult content, violence, hate speech, and prevent prompt injection attacks.
- **Honor encryption policies:** Apply [Microsoft Purview](#) encryption and DLP policies automatically.
- **Keep data in your tenant:** Store prompts and responses within your environment. Your data is [never used to train models](#).
- **Provide audit trails:** Track all Copilot interactions through Microsoft Purview to monitor for FERPA and COPPA compliance.

These protections enable confident AI adoption while maintaining strong security and child safety standards.

Recognize common threats

Educational institutions face a range of cybersecurity threats that can disrupt learning and compromise sensitive data. These include ransomware attacks that lock down systems, phishing attempts targeting staff and students, insider threats from compromised accounts or misused access, and nation-state attacks that target research and infrastructure.

Understanding these risks helps your team align strategies with the realities of your environment so you can protect what matters.

Reflect on security priorities

Use the table to reflect on your environment and find strengths you can build on. Start your assessment by considering these key questions.

ASK	INSIGHTS
What matters most in your environment?	Start with your most valuable assets. It could be student information systems, research data, financial records, and learning management platforms. These systems drive your mission and deserve prioritized protection.
Who needs access?	Map your user groups such as students, faculty, staff, administrators, and external users. Each group has different needs and risk profiles.
What’s working well?	Document existing security measures, successful policies, and user behaviors that already support positive security practices. Build on your strengths as you get started.

Emphasize compliance and regulatory readiness

Schools with strong regulatory compliance build community trust and confidence. Higher education institutions depend on compliance to advance priorities like medical and research programs. With the rapid adoption of AI tools in education, institutions also need proactive governance for emerging technologies.

[Microsoft Purview Compliance Manager](#) turns regulatory complexity into automated workflows. Your team can use pre-built templates instead of starting from scratch. This helps you address:

- K-12 regulations like FERPA for student records, COPPA for younger students, and other regulatory requirements.
- Higher education focuses on things like GDPR for international student data, HIPAA readiness for medical programs, and grant compliance protections.

Advance AI governance for educational innovation

[Microsoft Purview Data Security Posture Management \(DSPM\) for AI](#) provides visibility and control over how sensitive educational data interacts with AI systems like Microsoft 365 Copilot and third-party tools. DSPM for AI helps institutions monitor data sharing in AI prompts, apply automated protection policies, keep audit trails, and detect risky behaviors before compliance incidents occur.



Copilot Prompt

Create a FERPA and COPPA compliance checklist, mapping each requirement to relevant Purview tools (DLP, Information Protection, Insider Risk, eDiscovery).

TIP

Share previous audit findings or known compliance gaps. Copilot can then focus the FERPA/COPPA checklist on the areas where your district has the most risk.

Build forward

Your measurement-driven assessment creates the foundation for strategic security planning that supports your educational mission. Clear metrics help show progress and guide ongoing improvements.

- [Microsoft Secure Score](#): Measure your organization's security posture as a percentage, showing progress on completing recommended security actions across your Microsoft 365 environment.
- [Microsoft Purview Compliance Manager](#): Assess and manage compliance with a points-based scoring system that tracks your progress on improvement actions across regulations like FERPA and GDPR.

By understanding your current posture, you set the stage for a security strategy that empowers your institution.



Copilot Prompt

Analyze how we can leverage Microsoft Secure Score in Microsoft 365 to strengthen our security posture and implement a Zero Trust approach. Provide five high-impact actions that will improve our Secure Score this semester. Prioritize these actions by effort vs. impact and identify any dependencies that must be addressed first.

TIP

Share your top security goals—like protecting student data or reducing incident response time—so Copilot can prioritize Secure Score actions that directly support those goals.

Security governance and policies

Effective governance transforms security from reactive to strategic. The right frameworks streamline operations, build community trust, and align with your institution’s specific requirements.

The [National Institute of Standards and Technology \(NIST\) Cybersecurity Framework](#) provides voluntary guidance that many educational institutions adopt for practical implementation pathways and risk management. For institutions with [Microsoft Security Copilot](#) provisioned, AI-powered policy mapping can help analyze your current policies against NIST categories and prioritize focus areas.

Higher education institutions with research and medical programs may also require [ISO 27001](#) certification. This internationally recognized information security management standard supports comprehensive data protection, risk management, and compliance practices required for sensitive research environments.

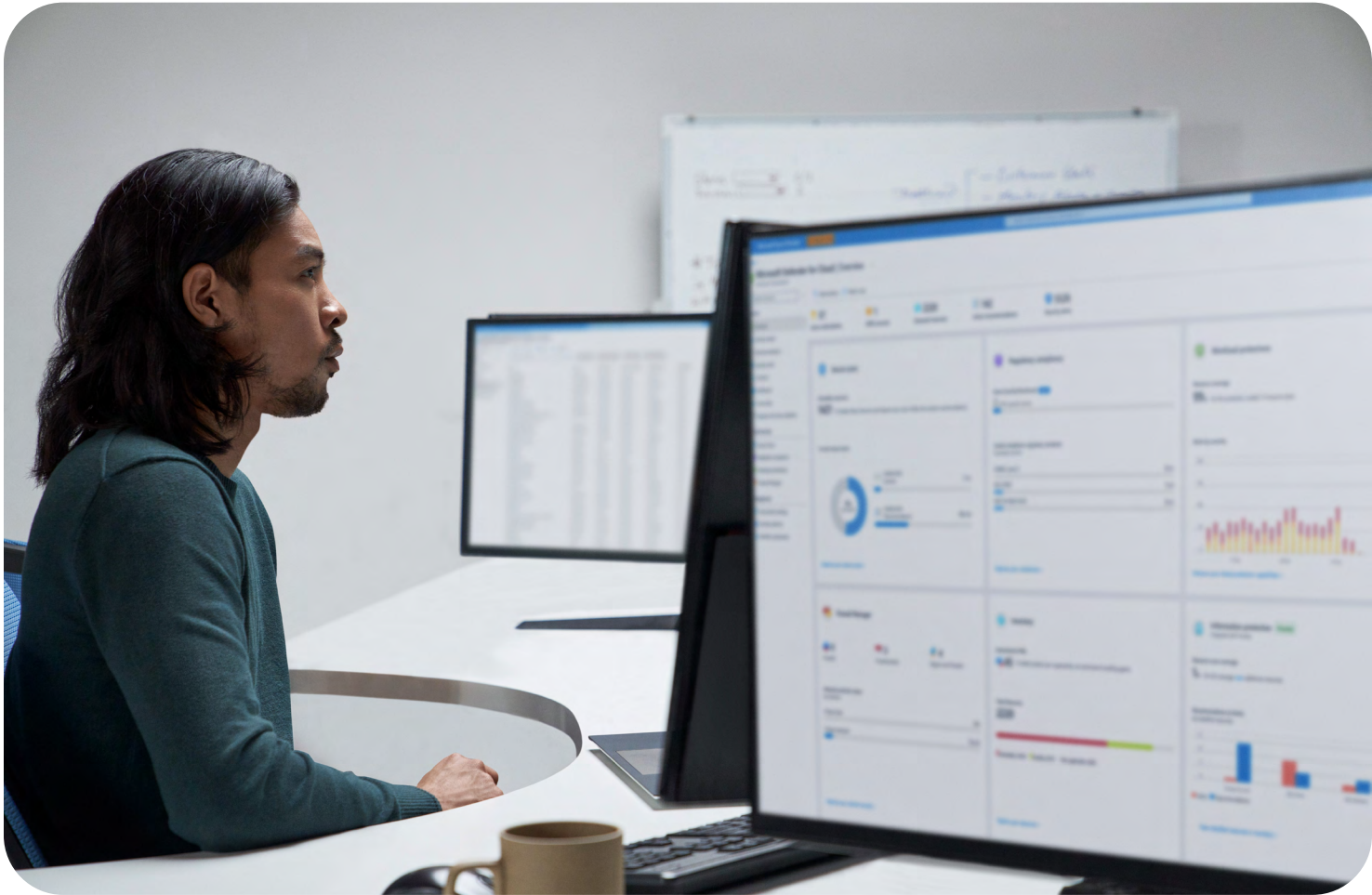


Copilot Prompt

Map out access requirements for all user groups (students, faculty, substitutes, researchers, contractors) and generate recommended Conditional Access policies using Entra ID. Provide this in a policy matrix with risk levels.

TIP

Describe seasonal or temporary access needs—substitutes, contractors, student teachers, visiting researchers—so Copilot can design dynamic access policies.



Simplify user access management

[Microsoft Entra ID](#) handles the complexity of educational environments where user needs change rapidly. Your conditional access policies should reflect academic realities including temporary users, seasonal access needs, and collaboration requirements that change with each semester. Use this table to map out user access policies that reflect your academic environment.

K-12 USERS	BOTH	HIGHER EDUCATION USERS
Students	Faculty and educators	Researchers
Substitutes	Staff	Graduate students
Volunteers	Administrators	Industry partners
Parent and guardian access	IT Personnel	
	Guest users	
	Contractors	

Incident response in action: Ransomware during finals week

During finals week, a suspicious file encryption activity triggers alerts across your institution’s network:

1. **Detect the threat:** [Microsoft Defender XDR](#) identifies the ransomware signature while [Microsoft Entra ID Protection](#) flags unusual admin login attempts from an external IP address.

2. **Respond automatically:** Within minutes, [Microsoft Sentinel](#) playbooks isolate affected devices through [Microsoft Defender for Endpoint](#), disable the compromised admin account via [Microsoft Entra ID](#), and send [Teams](#) notifications to your IT staff and superintendent.

3. **Recover with guidance:** For institutions with [Microsoft Security Copilot](#) provisioned, AI-powered analysis provides attack pattern insights and remediation recommendations, while [Microsoft Purview](#) documents everything for insurance claims and regulatory reporting.
4. **Prevent future attacks:** [Microsoft Defender for Office 365](#) proactively blocks ransomware-laden emails and malicious attachments before they reach users, while [safe attachments and safe links](#) features provide additional layers of protection against phishing campaigns that often precede ransomware attacks.

5. **Result:** Classes continue uninterrupted while your automated systems contain the threat and guide recovery efforts.

Proactive incident response planning helps your institution maintain continuity and protect learning, even during critical times like finals week.

Technology security strategy

Technology decisions are an opportunity to strengthen security and support learning from day one. By partnering with Microsoft and using built-in security features, educational institutions can create environments where protection and productivity go together.

Streamline and secure

Use [Microsoft 365 A3 for Education](#) to provide essential security features and productivity tools, helping districts optimize resources and protection from the start.

- [Microsoft Defender for Endpoint](#): Deploy advanced threat protection with Defender for Endpoint Plan 1 included in Faculty A3 licensing, providing essential endpoint security designed for educational device environments. Note: Student Use Benefit subscriptions require additional licensing for Defender for Endpoint.
- [Microsoft 365 Education](#) storage: Implement cloud-first storage with built-in FERPA compliance, data residency protections, automatic backup, and predictable operating costs.
- [Microsoft Intune for Education](#): Simplify device management designed for classroom environments without disrupting learning workflows.
- [Microsoft Purview Data Security Posture Management](#) (DSPM) for AI: Deploy foundational AI monitoring to gain visibility into AI usage patterns and help protect student data from inappropriate sharing.



Build comprehensive, research-ready security

For higher education institutions with more complex needs, a comprehensive approach helps support robust protection and compliance. Use [Microsoft 365 A5 for Education](#) to enable advanced security, analytics, and compliance capabilities, supporting complex research environments and multi-campus operations.

- Zero Trust foundation: Establish essential security framework before deploying advanced AI tools like [Microsoft 365 Copilot](#) and [Security Copilot](#).
- Hybrid infrastructure strategy: Balance cloud collaboration with on-premises research systems for regulatory compliance, data sovereignty, and intellectual property protection.
- [Microsoft Sentinel](#): Configure AI-powered Security Information and Event Management (SIEM) for enterprise-scale threat detection across multiple campuses and research networks.
- [Microsoft Purview](#): Implement comprehensive data governance for grant compliance, international research collaboration, and automated regulatory reporting.
- [Microsoft Purview DSPM for AI](#): Configure advanced AI governance with detailed analytics, policy enforcement, and compliance controls to support secure research operations.

Plan your cloud migration and data residency strategy using Microsoft’s proven [Cloud adoption framework](#).



Copilot Prompt

Provide a step-by-step plan to deploy Microsoft Intune across a multi-campus district, including Autopilot setup, compliance policies, enrollment options for shared vs. 1:1 devices, and a recommended pilot sequence. Return recommendations in checklist form.

TIP

Provide details about your device mix, network limits, and whether devices are shared or 1:1. This lets Copilot tailor Intune enrollment and policy recommendations to your environment.

Organizational readiness

Cybersecurity skilling is an essential part of any mature program. Building organizational readiness empowers your institution to deliver maximum value through skilled personnel, engaged users, and strong cyber hygiene that support your mission.



[Copilot Prompt](#)

Outline the steps to launch a student SOC program, including required Microsoft tools (Sentinel, Defender XDR, Security Copilot), curriculum resources, faculty sponsorship, student roles, and a 12-week implementation timeline.

TIP

Provide your available talent pool (e.g., cybersecurity club, STEM academy, work-study students) and estimated supervision hours. Copilot can then design a program aligned to your capacity and student skill level.

Advance through readiness stages

Microsoft provides resources that help members throughout your campus develop and refine cybersecurity knowledge and skills. Follow these implementation stages:

- 1. Foundation building: Introduce Microsoft Learn and Microsoft Education cybersecurity awareness programs institution wide.
- 2. Engagement expansion: Implement student cybersecurity programs and establish on-going security culture and skilling plans.
- 3. Advanced capabilities: Launch student Security Operations Center (SOC) programs using the Microsoft Student SOC Toolkit, which provides structured learning modules with hands-on experience in Microsoft Defender XDR, Sentinel, and Security Copilot.

Use the table to identify the most relevant resources and skilling pathways for your team.

These resources help every member of your institution contribute to a secure, resilient learning environment.

READINESS FOCUS	FOUNDATION BUILDING	EXPANSION AND ADVANCED SKILLING
K-12 IT staff Security essentials for IT administrators and automated threat response	Microsoft Learn Security hub Microsoft Certified: Security, compliance, and identity fundamentals Describe the core features of Microsoft Security Copilot	Design solutions that align with security best practices and priorities Enhance security operations by using Microsoft Security Copilot
Higher education IT staff Advanced SecOps with AI augmentation and enterprise-scale threat hunting	Microsoft Learn Security hub Configure your Microsoft Sentinel environment Enhance security operations by using Microsoft Security Copilot	Microsoft Certified: Security, compliance, and identity fundamentals Microsoft Security Operations Analyst
Faculty, staff, and administrators Classroom cybersecurity, safe technology practices, and research data protection	Build cybersecurity resilience in K-12 classrooms with Microsoft tools What is Cybersecurity? Azure for Researchers part 1: Introduction to Cloud Computing	Teach cybersecurity concepts with Minecraft Education Boost K-12 school cybersecurity leadership with Microsoft tools Azure for Researchers part 2: Cloud Security and Cost Management
K-12 students Digital citizenship; safe AI exploration	K-12 cybersecurity conversation guide and infographic Minecraft cyber & digital citizenship	Security Fundamentals (SC-900) Classroom toolkit: Unlocking generative AI safely and responsibly
Higher education students Career readiness and hands-on security experience	Microsoft Student Security Operations Center Toolkit Microsoft Learn Student Hub student certifications	Microsoft Certified: Security, Compliance, and Identity Fundamentals Microsoft Cybersecurity Scholarship Program

Financial and strategic justification

Investing in Microsoft security solutions helps educational institutions achieve measurable returns, improve resources, and strengthen compliance.

Forrester Total Economic Impact studies commissioned by Microsoft examined the security ROI for K-12 and higher education institutions using Microsoft 365 Education A5:

- [Composite K-12 organization](#): 118% ROI with \$4.22 million in three-year benefits compared to \$1.94 million costs.
- [Composite higher education institution](#): 128% ROI with \$7.28 million benefits compared to \$3.19 million costs.
- [Projected Microsoft Security Copilot ROI](#): 99-348% with a projected net present value of \$500,000 to \$1.8 million.

Explore the strategic value table to learn how strategic investments in security deliver tangible benefits for your institution.

INVESTMENT FOCUS	QUANTIFIED BENEFITS	FINANCIAL AND OPERATIONAL IMPACT
AI-powered security operations	• Security Copilot provides 23-47% SecOps productivity gains • Enhances breach prevention with accelerated threat response	Achieves a return on investment (ROI) of 99-348% across various industries.
Security and compliance	• 15% reduction in significant breaches • 29% lower breach remediation costs	Savings: \$972,800 for K-12 and \$1.2 million for higher education institutions.
Vendor consolidation	• 30% reduction in security license costs • Simplifies management by consolidating to a single vendor	Savings: \$1.1 million for K-12 and \$1.7 million for higher education institutions.
Staffing efficiency	• Avoids major IT security team expansion • Provides a crucial advantage in a competitive talent market • Mitigates hiring and retention challenges	Savings: \$545,700 in K-12 and \$1.1 million in higher education institutions. Maximizes current staffing efficiency to drastically reduce team expansion.
Productivity gains	• Saves 15 minutes per employee • Enhances security user experiences and system availability • Enhances breach prevention with accelerated threat response	Savings: \$1.7 million in K-12 and \$3.3 million for higher education institutions. • 23-47% productivity gains in SecOps with Security Copilot • ROI 99-348% across industries

Optimize licenses

Select the Microsoft 365 Education plan that’s right for your organization. Consider factors like your current security risk, team capacity, and available resources.

- **A3 foundation approach:** Start with essential security that uses existing Microsoft investments, starting with MFA and adding security layers gradually.
- **A5 comprehensive approach:** Deploy advanced security, compliance, and analytics with enterprise threat protection and compliance tools that support multi-campus operations and total cost of ownership optimization.



[Copilot Prompt](#)

Evaluate our current security vendors and create a consolidation map showing which tools can be replaced by the Microsoft security stack. Include projected savings, integration benefits, and a phased migration plan.

[Provide a link or upload a document listing all existing security vendors, along with enabled apps and features.]

TIP

Provide your current vendor list and note tools that are expensive or hard to maintain. Copilot can prioritize consolidation that delivers the biggest savings and efficiency gains.

Budget planning and justification

Your team also needs to consider your deployment timeline, how much your institution can save through ROI, and if there are additional resources available to help offset costs.

- **Phased approach:** Start with foundation deployment (A3 baseline), expand strategically (A5 upgrades), then optimize across the institution.
- **Budget calculation framework:** Calculate risk mitigation value, add operational efficiency gains, and include strategic capability development for comprehensive ROI justification.
- **Cost avoidance:** Prevent security incidents that average [\\$4.44 million per breach](#) in 2025; automate compliance to help reduce development costs; and combine infrastructure to achieve ROI of 118-128% as demonstrated in education-specific studies.
- **Education-specific funding opportunities:** Explore grant applications and industry partnerships that support security program investments while demonstrating regulatory compliance for FERPA, COPPA, and GDPR requirements.

Implementation

In this section

[K-12 Scenarios for Implementation](#)

[Higher education scenarios for implementation](#)



K-12 Scenarios for Implementation

Identity Security

Technology access models—whether shared or 1:1—introduce unique challenges for IT teams.

Summary of the challenge

For **1:1 device programs**, students often struggle with multi-factor authentication (MFA). Whether it’s a forgotten password, delayed prompts, or the need for secondary devices, these barriers can disrupt learning and create frustration.

In **shared environments**—such as labs, carts, or libraries—traditional MFA becomes impractical. With dozens of students rotating through the same machines in short sessions, repeated sign-ins create bottlenecks that slow down instruction and strain IT resources.

Microsoft solutions in action

Microsoft tools offer flexible sign-in options that help protect student data without disrupting learning:

1:1 DEVICES

CHALLENGE	MICROSOFT TOOL	OUTCOME IN PRACTICE
Students forget passwords or struggle with MFA on personal devices.	Windows Hello for Business: Allow users to sign in to their Windows devices using biometric data, or a PIN, instead of a traditional password.	Enables secure sign-in using fingerprint, facial recognition, or PIN, reducing login friction and minimizing phishing risks.
A student forgets credentials right before class or exams.	Entra ID Temporary Access Pass (TAP): Provide a time-limited passcode that can be configured for single use or multiple sign-ins.	Allows educators or IT staff to issue secure, time-limited credentials, keeping learning on track without delays.
Educators and students juggle multiple apps and logins daily.	Entra ID Federated Identity: Offer access to Microsoft Entra protected resources without needing to manage secrets.	Delivers seamless single sign-on across apps, reducing login fatigue and keeping classes moving smoothly.

SHARED DEVICES

CHALLENGE	MICROSOFT TOOL	OUTCOME IN PRACTICE
Shared devices (labs, carts, libraries) require quick access, but traditional MFA slows sign-ins.	Entra ID FIDO2 Keys: Authenticate without entering a username or password.	Enables tap-and-go access with portable security keys, eliminating the need for personal phones and keeping sessions productive.
District IT needs to validate users and devices across a large environment.	Entra ID Certificate-Based Authentication: Require users to authenticate directly by using X.509 certificates authenticated in Microsoft Entra ID.	Scales secure sign-ins using public key infrastructure (PKI), reducing help desk volume and strengthening compliance across shared environments.
District leaders must protect sensitive data without disrupting learning.	Conditional Access Policies: Protect institutional assets by requiring users to complete an action to gain access.	Dynamically adjust access based on role, risk level, and device compliance, balancing protection with usability.

Get started

Districts can take a confident, phased approach to strengthening identity security. By starting with pilot classrooms, schools and institutions can explore Microsoft Entra ID solutions using step-by-step setup guides to refine what works best and scale successful strategies district-wide—all while keeping learning uninterrupted.

EXPLORE MICROSOFT ENTRA ID SOLUTIONS

Review step-by-step setup guides, pilot in a classroom setting, then scale district wide.

[→ Learn more](#)

Takeaway

From a student signing in with a fingerprint to a district leader securing thousands of accounts, Microsoft identity solutions balance protection with simplicity. By combining Windows Hello, Entra ID tools, and flexible access policies, schools can safeguard data while keeping the focus on learning.



Data security and compliance

Schools access and store personally identifiable information (PII) that needs to be protected to keep students safe and comply with regulations.

Summary of the challenge

Cybercriminals target schools to infiltrate systems and extract sensitive data. Without strong cybersecurity protections, threat actors can gain access to data and prevent schools from using systems until a ransom is paid.

System operators often receive **data requests from vendors** that ask for access to sensitive data about students. When these requests circumvent established procedures like communicating with a central office leader, data can be shared that would otherwise be denied.

Educators need access to **PII like academic and behavioral records** to write individualized education plans (IEPs) and draft grading reports. Providing just enough access without granting universal access is challenging when schools store so much information.

Ensuring educators and staff don't disclose **private data like photos or videos of students** can be problematic when families sign media permission forms that restrict how their child's likeness may be used.

Microsoft solutions in action

Microsoft offers security tools that protect data without disrupting teaching or operations:

CHALLENGE	MICROSOFT TOOL	OUTCOME IN PRACTICE
A SIS operator receives a request to share student data from a vendor that doesn't need access to provide services.	Purview Information Barriers: Restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive.	Communication and collaboration with the vendor are restricted, preventing data sharing and maintaining existing data protections.
A SPED educator needs access to a specific student's academic and behavioral data to write an IEP but shouldn't have schoolwide access to every student profile.	Purview Information Protection: Discover, classify, and protect sensitive information wherever it lives or travels.	IT professionals classify and label the data to ensure the educator can access what's appropriate for the role without granting universal access to all student data.
A principal shares photos from a recent school event on social media that contain smiling faces of students, educators, and families.	Purview Data Loss Prevention: Prevent internal users from inappropriately sharing sensitive data with people who shouldn't have it.	Unauthorized sharing, use, or transfer of sensitive information such as photos is restricted to maintain privacy for all user groups.

Here’s how to implement a solution

To get started with Microsoft Purview, begin by identifying your district’s most sensitive data types and the staff roles that require access. Then review Purview’s core capabilities and apply appropriate sharing restrictions and data labels.

EXPLORE MICROSOFT SOLUTIONS

Learn how to identify data risks, manage compliance, and prevent data loss across your entire infrastructure.

 [Explore Microsoft Purview](#)

Real-world example: Prince William County Public Schools

In Virginia, Prince William County Public Schools administrators took steps to help create safer digital experiences for students using district-issued mobile devices and laptops. The district adopted Microsoft Purview products to unobtrusively identify cyberbullying and harassment, gaining insights into harmful or inappropriate content shared by students. This enabled the division to detect FERPA and CIPA violations and, most importantly, respond quickly when an incident arose or students needed support.

Learn how Prince William County Public Schools used the Purview family of products to maintain compliance with federal regulations and provide safer digital experiences for students.

 [Read their story](#)

Takeaway

Microsoft Purview helps schools safeguard sensitive data by setting clear boundaries on access and sharing, helping support compliance with privacy regulations. With features like Information Barriers, Information Protection, and Data Loss Prevention, IT teams can prevent unauthorized disclosures while still enabling educators and administrators to access the information they need.

Higher education scenarios for implementation

Data security

Institutions face unique data security challenges because of sensitive research, health data, financial records, admissions information, and PII that’s stored, accessed, and used.

Summary of the challenge

Grant-funded research requires collaboration and communication with other institutions. Staff need to share confidential data between authorized groups and prevent leaking data.

Leadership teams often **distribute files with strategic guidance** that shouldn’t be shared with other groups. Controlling access to sensitive information is critical.

IT professionals assess infrastructure for risks and vulnerabilities. When incidents like an internal data breach occur, CTOs need security teams to **analyze what happened and prevent future incidents**—while managing other critical tasks.

Microsoft solutions in action

Microsoft offers security solutions that protect data without disrupting research, teaching, or operations:

CHALLENGE	MICROSOFT TOOL	OUTCOME IN PRACTICE
A faculty member conducting sensitive research needs to exchange information with another university while preventing public sharing.	Purview Information Barriers: Restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive.	Communication about sensitive research is restricted to authorized groups, preventing data sharing and maintaining existing data protection.
A provost distributes a Board of Visitors memo to deans that shouldn’t be shared with faculty or staff.	Purview Information Protection: Discover, classify, and protect sensitive information wherever it lives or travels.	The memo is classified and labeled to help ensure that only deans can open and read the file.
A newly hired adjunct instructor posts PDF instructions to a Teams channel that shows students how to sign into a faculty-only database.	Purview Data Loss Prevention: Prevent internal users from inappropriately sharing sensitive data with people who shouldn't have it.	The instructor’s activity triggers alerts, prompting adjustments to policies that block access to the PDF and similar data types moving forward.
A CTO tasks IT professionals to identify systemwide vulnerabilities after a staff member inadvertently shares strategic plans with the media.	Purview Insider Risk Management: Minimize internal risks by detecting, investigating, and acting on malicious and inadvertent activities in your institution.	IT professionals detect and address unauthorized data disclosures, following policies to prevent similar incidents campuswide.
A student working for the university’s Security Operations Center (SOC) needs to monitor campuswide threats while IT staff participate in an all-day departmental retreat.	Security Copilot: Protect your institution at the speed and scale of AI with a generative AI-powered assistant for daily operations in security and IT.	The student uses AI-powered assistance to analyze signals from Microsoft Defender to detect anomalies across systems, leveraging step-by-step instructions to contain threats while IT staff are away.

Here’s how to implement a solution

To get started with Microsoft Purview, begin by identifying your university’s most sensitive data types and the faculty roles that require access. Then review Purview’s core capabilities and apply appropriate sharing restrictions and data labels.

EXPLORE MICROSOFT SOLUTIONS

Learn how to identify data risks, manage compliance, and prevent data loss across your entire infrastructure.

[➔ Explore Microsoft Purview](#)

Discover how to catch what others miss, respond faster to threats, and strengthen team expertise with AI assistance.

[➔ Learn about Security Copilot](#)

Real-world example: Oregon State University

As a part of their commitment to innovative security, administrators at Oregon State University adopted Security Copilot to deepen their cybersecurity posture after an incident. Security Copilot enabled IT professionals to automate threat detection and response processes, allowing analysts to focus on high-value tasks and complex investigations. This led to faster incident resolution, reduced operational costs, and enhanced protection of sensitive research and student data.

Learn how Security Copilot helped Oregon State University address vulnerabilities and implement a more proactive security stance campuswide.

[➔ Read their story](#)

Takeaway

Higher education institutions must protect sensitive research, limit data sharing, and secure privileged data while enabling secure collaboration among authorized users. Microsoft Purview and Security Copilot empower universities to manage access, prevent data leaks, and quickly respond to emerging risks without disrupting teaching or research.



Copilot Prompt

Draft an implementation plan for Insider Risk Management in our institution, including policy templates for data leaks, risky user behavior, and research data handling. Provide guidance for faculty, staff, and graduate assistants on responsible data management.

TIP

Describe past accidental disclosures or recurring risky behaviors (e.g., sharing PDFs via personal email). Copilot can use these patterns to shape more relevant insider risk policies.

Data compliance

Universities must adhere to data privacy, data retention, and data governance requirements outlined in federal regulations like [FERPA](#), [HIPPA](#), and [GDPR](#) to receive funding and contracts.

Summary of the challenge

Former employees sometimes **retain access to internal systems** after leaving an institution. Universities must see that access to sensitive data is revoked to prevent unauthorized disclosures that could lead to legal exposure and reputational harm.

Faculty occasionally use institutional email to **share personal or political views** with students. Universities need clear boundaries around official communication to avoid public controversies while respecting academic freedom.

Research teams often **collaborate with international partners on complex projects**. Sharing classified technical data without proper authorization could violate federal regulations and jeopardize future funding opportunities.

Microsoft solutions in action

Microsoft offers compliance solutions that help institutions adhere to regulatory requirements:

CHALLENGE	MICROSOFT TOOL	OUTCOME IN PRACTICE
A college health center integrates a third-party telehealth platform without verifying HIPAA compliance, resulting in unauthorized access to student health records.	Purview Compliance Manager: Automatically assess and manage compliance across your multi-cloud environment.	Centrally defined enforcement policies catch the noncompliant platform before access to health records is granted.
A financial aid officer mistakenly sends a report containing student loan and grant details to an unauthorized internal department, triggering an investigation.	Purview Insider Risk Management: Minimize internal risks by detecting, investigating, and acting on malicious and inadvertent activities in your institution.	Automated policies detect when financial aid data is shared with unauthorized recipients and trigger alerts or restrict access to prevent further non-compliant disclosures.
A professor sends politically charged remarks to students via email, which are later leaked and spark media attention.	Purview Communication Compliance: Minimize communication risks by helping you detect, capture, and act on potentially inappropriate messages in your organization.	Political statements in messages are automatically detected and flagged before being sent, enabling early intervention that limits reputational damage.
A university receives an audit notice from the Department of Education regarding its handling of financial aid disbursements to students.	Purview Records Management: Manage regulatory, legal, and business-critical records.	All financial aid data is labeled as records with retention periods that align with regulations, ensuring data remains available for audits and investigations.
Sensitive biomedical research data is accessed and leaked by a former employee who retained access to internal systems after leaving the institution.	Purview Information Protection: Discover, classify, and protect sensitive information wherever it lives or travels.	Research data is automatically labeled and encrypted according to policies, ensuring non-affiliated individuals are blocked from accessing institutional data.
A university health center employee accesses and shares a student’s mental health records with a professor without the student’s consent.	Purview Data Loss Prevention: Prevent internal users from inappropriately sharing sensitive data with people who shouldn't have it.	IT professionals set up automated policies to prevent unauthorized sharing of mental health records by email or chat, helping support HIPAA compliance.
A research team working on a defense technology project shares sensitive technical data via SharePoint with international collaborators, triggering a potential unauthorized export.	Purview Information Barriers: Restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive.	Policies are configured to restrict file sharing or links to files for international organizations, preventing exports of highly sensitive data.
An IT administrator mistakenly assigns expensive software licenses to unauthorized users, breaching procurement policies and licensing agreements.	Purview Audit: Respond to security events, forensic investigations, internal investigations, and compliance obligations.	Audit logs indicate who assigned the licenses, when it happened, and whether it violated policies, enabling corrective action and documentation for compliance requirements.



Here’s how to implement a solution

Universities don’t need to implement every Purview solution at once. Start by identifying key data sources and compliance priorities. Then use Purview’s built-in templates and scanning tools to assess risk and gradually expand coverage across departments.

EXPLORE MICROSOFT SOLUTIONS

Learn how to identify data risks, manage compliance, and prevent data loss across your entire infrastructure.

[→ Explore Microsoft Purview](#)

Takeaway

Maintaining data compliance requires universities to proactively manage who can access and share sensitive institutional data. Leveraging Microsoft Purview helps institutions protect privacy, prevent data leaks, and help ensure accountability across complex academic environments.



Copilot Prompt

Create a post-implementation reporting framework for our security tools (Defender, Purview, Sentinel, Entra ID). Include monthly KPIs, dashboards for leadership, improvement milestones, and metrics tied to compliance or audit readiness.

TIP

Tell Copilot which metrics your leadership values most—uptime, compliance, incident reduction, or audit outcomes. It will tune the reporting framework to those priorities.

Research

See how schools and institutions are protecting students, staff, and data with Microsoft security—leveraging AI-powered threat detection, Zero Trust strategies, and connected tools that simplify IT and strengthen resilience.

In this section

- [Microsoft security in education: From deployment to campus impact](#)
- [Data and analytics](#)
- [Academic and industry findings](#)
- [Glossary of terms](#)
- [Next steps checklist](#)



Microsoft security in education: From deployment to campus impact

Explore practical guidance on deployment, usage, and best practices for Microsoft Security solutions.

Achieve regulatory compliance with confidence: Streamline your compliance journey and prepare for future changes with Zero Trust

Microsoft, 2025

Learn how educational organizations can stay ahead of shifting compliance demands using integrated security, compliance, and identity solutions from Microsoft. Adopt a Zero Trust strategy that continuously verifies access, protects sensitive data, and unifies security tools across your educational organization. This modern approach simplifies regulatory compliance by replacing fragmented legacy systems with integrated solutions that offer better visibility, control, and resilience.

[Go to resource](#)

The decision-maker’s guide to comprehensive security: Key strategies for protecting your organization today

Microsoft, 2025

Unify security by adopting Microsoft’s comprehensive, integrated approach built on the Zero Trust framework that continuously verifies access across users, devices, data, and applications. This strategy simplifies operations, reduces risk, and maximizes the value of your security investments by consolidating tools and streamlining protection across your digital environment.

[Go to resource](#)

Rapidly modernize your security posture: Use a Zero Trust framework to build confidence with your employees, partners, customers, and other stakeholders

Microsoft, 2025

Explore how to strengthen security posture by aligning leadership around a shared strategy, prioritizing risks, and systematically applying Zero Trust principles to improve defenses. This eBook helps organizations confidently respond to threats, enhance overall security posture, and ensure progress is measurable and communicated effectively to decision-makers.

[Go to resource](#)

Safeguard your most sensitive data: Protect your critical assets with Zero Trust security framework

Microsoft, 2025

Discover how to implement a Zero Trust strategy to identify, classify, and protect sensitive data across all environments—cloud, on-premises, and mobile—using automated labeling, encryption, and access controls. This eBook helps strengthen security, reduce insider and external threats, and ensure compliance while enabling seamless collaboration and productivity.

[Go to resource](#)

**Securely work from anywhere:
Strengthen security with a Zero
Trust approach**

Microsoft, 2025

Provide secure remote and hybrid work experiences by adopting a Zero Trust framework that verifies every access request, protects endpoints, and enforces strong identity controls. This reduces the risk of cyberattacks, supports flexible work environments, and ensures data and device security without compromising productivity.

[Go to resource](#)

SOC for students: Implementation guide

Microsoft, 2025

Learn how SOC's strengthen workforce readiness and institutional security by providing practical experience, industry certifications, and alignment with strategies like Zero Trust.

[Go to resource](#)

**AI security and Zero Trust: Agile security
for agile business**

Microsoft, 2024

Protect data, applications, and infrastructure by implementing a Zero Trust security framework that verifies access and limits privileges in AI systems. A Zero Trust approach to AI systems enhances data privacy and ensures regulatory compliance, so organizations can innovate with AI.

[Go to resource](#)

**Common attacks and how Microsoft
capabilities for Zero Trust can protect
your organization**

Microsoft, 2024

Understand how cybercriminals initiate identity, device, and network attacks in unsecured systems, and learn how Microsoft Security solutions and a Zero Trust approach protect data, endpoints, and critical infrastructure.

[Go to resource](#)

**Cyber Signals Issue 8 | Education
under siege: How cybercriminals target
our schools**

Microsoft, 2024

Discover how open digital environments, widespread use of personal devices, and limited security resources are leading to cyberattacks on K-12 schools and higher education institutions. By adopting proactive strategies like Zero Trust and enhancing visibility and control across networks and devices, schools and institutions can better safeguard sensitive data and reduce the risk of disruption from increasingly sophisticated threats.

[Go to resource](#)

**The fundamental guide to Zero
Trust: A leadership approach to
AI-enhanced security**

Microsoft, 2024

Learn how to strengthen enterprise security by applying Microsoft's Zero Trust architecture, which organizes protection across identities, data, apps, endpoints, networks, infrastructure, and AI using adaptive access and continuous threat assessment. This structured approach reduces risk, improves compliance, and enables secure innovation while simplifying deployment and management across the organization.

[Go to resource](#)

Microsoft Digital Defense Report 2024

Microsoft, 2024

Explore the evolving threat landscape, ways to strategically address cybersecurity, and the new security challenges that come with AI adoption. This report includes data and statistics from Microsoft Threat Intelligence that analyzes over 78 trillion security signals each day.

[Go to resource](#)

Data and analytics

Discover how Microsoft Security solutions provide quantifiable benefits to schools and institutions.

The Forrester Wave: Zero Trust Platforms, Q3 2025

Forrester, 2025

Learn how Microsoft’s strategic roadmap, product capabilities, and customer feedback make Microsoft a Leader in Zero Trust Platform Providers according to Forrester. This report highlights Microsoft efforts to strengthen identity management across core security products as well as bring AI-enhanced protection to organizations with Microsoft Security Copilot.

[Go to resource](#)

The Total Economic Impact of Microsoft Sentinel

Forrester, 2024

Discover the advantages of modernizing security operations by replacing outdated systems with Microsoft Sentinel, a cloud-based platform that uses AI and automation to detect and respond to threats faster and more efficiently. This Forrester study found a 234% return on investment, with significant cost savings, reduced false positives, and improved team productivity—making Sentinel a strategic tool for education leaders seeking scalable, secure, and cost-effective cybersecurity solutions

[Go to resource](#)

New technology: The projected Total Economic Impact of Microsoft Security Copilot

Forrester, 2024

Understand how Microsoft Security Copilot delivers measurable improvements in security operations by using generative AI to streamline threat detection, investigation, and response. The study found a 46% average productivity gain for SecOps tasks, cost efficiencies from SecOps centralization, and a projected ROI of 348%, highlighting the importance of integrating AI-driven tools like Microsoft’s Security Copilot into cybersecurity strategies to enhance protection while addressing workforce shortages.

[Go to resource](#)

The Total Economic Impact of Microsoft Security

Forrester, 2023

Read how Microsoft Security improves cybersecurity efficiency and risk reduction through SIEM, compliance, and identity management solutions. The study found a 72% reduction in the likelihood of a breach, a 25% reduction in licensing and consumption costs, and a 50% increase in efficiency for IT and security teams.

[Go to resource](#)

The Total Economic Impact of Microsoft SIEM and XDR

Forrester, 2022

Discover how Microsoft SIEM and XDR solutions reduce threat response time, improve visibility, and help organizations consolidate vendors. The study found a 65% reduction in time spent investigating threats, an 88% reduction in response time, and nearly \$1.6 million in annual savings by consolidating vendors and management.

[Go to resource](#)

Academic and industry findings

Learn about the importance of robust security, compliance, and privacy protection in K-12 and higher education classrooms.

Implementing a Zero Trust architecture: High-level document

National Institute of Standards and Technology (NIST), 2024

Learn how to implement a Zero Trust architecture (ZTA) that enables secure, authorized access to enterprise resources across on-premises and multi-cloud environments. This architecture enables a hybrid workforce to access resources from anywhere, at any time, from any device in support of the organization’s mission. Discover how to implement ZTA consistent with the concepts and principles outlined in NIST Special Publication (SP) 800-207, Zero Trust Architecture.

[Go to resource](#)

The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology (NIST), 2024

Discover how to manage cybersecurity risks with the NIST Cybersecurity Framework (CSF) 2.0. The CSF provides a taxonomy of high-level cybersecurity standards and outcomes that can be used by schools and institutions to better understand, assess, prioritize, and communicate cybersecurity efforts.

[Go to resource](#)

2024 Educause Horizon Report: Cybersecurity and privacy edition

Educause, 2024

Explore ways higher education institutions can strengthen cybersecurity and privacy amid rapid technological and geopolitical change. The report emphasizes the importance of adopting frameworks like Zero Trust, offering security awareness training, and enhancing risk management to protect institutional data and student privacy.

[Go to resource](#)

First annual generative AI study: Business rewards vs. security risks

Information Security Media Group (ISMG), 2023

Gain valuable insights into the dual perspectives of leaders and chief information security officers (CISOs) on generative AI – its opportunities, risks, and implications. This study provides a comprehensive snapshot of perspectives from these key roles across different industries and sectors.

[Go to resource](#)

Protecting our future: Partnering to safeguard K-12 organizations from cybersecurity threats

Cybersecurity and Infrastructure Security Agency (CISA), 2023

Understand the cybersecurity risks facing elementary and secondary schools and how to apply recommendations that protect people and data. The report’s key findings include implementing high impact cybersecurity protocols, elevating security as a top priority in schools, and collaborating with local, regional, and national agencies to reduce risk.

[Go to resource](#)

Implementing phishing-resistant MFA

Cybersecurity and Infrastructure Security Agency (CISA), 2022

Learn about the importance of using multifactor authentication (MFA) to reduce the risk of cybercriminals using compromised credentials to gain access to data, networks, and information systems. Follow guidance on how to implement phishing-resistant MFA and a Zero Trust approach to security.

[Go to resource](#)

Cybersecurity incident planning for institutes of higher education

U.S. Department of Education, ND

Improve security posture through risk management best practices that align with the NIST CSF for higher education institutions. Learn about the importance of having an incident response plan in place to limit damage to networks, expedite mitigation, and enhance law enforcement’s ability to identify and apprehend perpetrators.

[Go to resource](#)

Glossary of terms

Review common terminology that’s used when discussing cybersecurity in education. For additional terms and definitions, visit the National Initiative for Cybersecurity Careers and Studies.

Access: The ability and means to communicate or interact with a system, use system resources to handle information, gain knowledge about the information in the system, or to control system components and functions

Authentication: The process of verifying the identity or other attributes of a user, process, or device

Backdoor: Any method by which authorized or unauthorized users bypass normal security measures and gain high level user access (aka root access) on a computer system, network, or software application

Breach: Any substantial loss of confidentiality, integrity, or availability of an information system or a serious impact to the safety or resilience of operational systems that is caused by unauthorized use

Distributed Denial-of-Service (DDoS): A cybercrime that occurs when an attacker floods a target with internet traffic to prevent users from accessing connected online services and sites

Encryption: The process of converting data into a form that isn’t easily understood by unauthorized people

Firewall: A device or software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized

Incident response: Any activities that address the short-term, direct effects of an incident including short-term recovery

Incident response plan: A set of predetermined and documented procedures to detect and respond to a cyber incident

Insider threat: Refers to the risk that someone with authorized access or knowledge of an organization's resources could use it to cause harm

Malware: Software that compromises the operation of a system by performing an unauthorized function or process

Mitigation: The use of one or more security measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences

Multifactor Authentication (MFA): A process of confirming the identity of a user (authentication) using more than one verification method like a password, PIN, fingerprint, or facial recognition

Passkeys: A form of multifactor authentication that uses public key cryptography in combination with biometrics like fingerprint and facial recognition or a device PIN to verify an account owner’s identity

Passwordless: An authentication method in which a user can sign into a computer system without entering a password or any other knowledge-based secret

Phishing: A cyberattack used to steal or damage sensitive data by deceiving people into revealing personal information like passwords or personally identifiable information (PII)

Privacy: The assurance that the confidentiality of, and access to, certain information about an entity is protected

Ransomware: A type of malware or phishing cyber security attack that destroys or encrypts files and folders on a computer, server, or device so that a cybercriminal can extort money to unlock encrypted data

Red team: A group authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s cybersecurity posture

Resilience: The ability to operate under adverse conditions while maintaining essential operational capabilities and recover operations in a timely manner

Risk: The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability

Risk assessment: The process of identifying, estimating, and prioritizing risks to operations, assets, or individuals

SecOps (security operations): A methodology that IT managers implement to enhance the connection, collaboration and communication between IT security and IT operations teams

SIEM (security information and event management): A security solution that helps organizations detect threats before they disrupt operations

Social engineering: The use of deception and psychological tricks, persuasion, and exploitation to deceive users into making mistakes resulting in accidentally revealing sensitive information and data

Spam: The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages

Threat: Any event or circumstance that can adversely impact operations, assets, or individuals through unauthorized access, destruction, disclosure, modification, or denial of service

Threat actors (cybercriminals): Individuals or groups that engage in harmful digital activities with the aim to compromise systems, steal data, or disrupt services

Vulnerability: A weakness in a security system, security procedures, internal controls, or implementation that can be exploited or triggered by a threat

XDR (extended detection and response):
An approach to cybersecurity that integrates detection, investigation, and response capabilities across a wider range of domains, including an organization’s endpoints, hybrid identities, cloud applications and workloads, email, and data stores

Zero Trust: An approach to cybersecurity that assumes everything is a threat; Zero Trust follows three principles: Verify explicitly, use least-privileged access, and assume a breach

Next steps checklist

- ☐ Review research on Zero Trust and identify how your institution can apply the three principles across identities, endpoints, apps, infrastructure, data, and networks.
- ☐ Share the quantifiable benefits of Microsoft Security solutions with IT professionals, financial decision-makers, and leaders.
- ☐ Explore recommendations and guidelines from agencies like CISA, NIST, and the U.S. Department of Education.



Microsoft and the Microsoft logo are trademarks of Microsoft or its subsidiaries. Other names and brands may be claimed as the property of others.

Copyright © 2026 Microsoft | 1.0