Microsoft Security

Cyber Insurance and Security Posture Management for Education

Strengthen your security posture to improve your cyber insurance profile by implementing foundational security controls.[1]

Schools and higher education institutions are amongst the most targeted entities by cybercriminals[2], making it critical to have a strong security posture and adequate cyber insurance coverage should an incident occur. Microsoft's 2021 Digital Defense Report showed that **98% of attacks could have been prevented with basic cyber hygiene practices.**[3]

"Why is my cyber insurance more expensive and providing less overall coverage?"

Cyber insurance industry trends: One size does not fit all.

Increasing cyberthreats and increasing demand

Ransomware, supply chain, and critical infrastructure attacks are on the rise at an alarming pace, posing a greater threat to K-12 schools and higher education institutions than ever before, thus, forcing the insurance industry to raise rates[4] and provide less overall coverage.

Demand for cyber insurance is also growing, from premiums worldwide standing at $9.2 billion USD at the beginning of 2022, to a predicted $22 billion USD by 2025.[5]

Although there is much awareness surrounding these sophisticated threats, little progress has been made with respect to controlling insurance losses and costs based on proactive security posture management, resulting in increasing premiums in an ever-evolving threat landscape.

Access to security posture data is a challenge

Today's threat landscape is complicated. In order to accurately underwrite each customer, insurers need confirmation their security posture is in good standing.

Cyber insurance applications are intended to help insurers assess the security posture of a company. While that information can be useful, it typically only provides data for a snapshot in time, rather than a holistic, ongoing, security posture view.

Without accurate data regarding the ongoing security posture, insurers are left to underwrite individual risks and offer pricing and coverage terms based on general industry standards. While the underwriting process varies between insurance carriers, carriers that consider the ongoing security posture of an organization should be able to offer preferred coverage terms and pricing to entities with enhanced security controls.

"What can I do to strengthen my security posture so I can potentially qualify for better coverage terms?"

Secure more by implementing seven key cyber hygiene controls.

While there are several practices organizations can take to holistically strengthen their security posture, the following controls were selected based on industry standards as a baseline to improve the overall risk profile in the underwriting process.

1. Multifactor Authentication

- Multifactor authentication (MFA) helps prevent account compromise by securing the sign on process, adding a layer of protection beyond a username and password.
- Microsoft 365 A3 licenses can take advantage of prompted MFA for all users, including students, during certain scenarios or events that fit business requirements.
- In the A5 license, MFA provides the strongest security position and an improved user experience with the addition of risk-based Conditional Access.

» **Learn more about MFA for Microsoft 365**

2. Email Security

- Prioritizing email security is important in safeguarding internal communication and reducing cyberthreats—helping protect schools, enhance productivity, and ensure compliance with data protection laws.
- Microsoft Defender for Office 365 Plan 2, included in the Microsoft 365 A5 license, is a cloud-based email filtering service that helps protect against advanced threats to email and collaboration tools, including phishing training, business email compromise, and malware attacks. It also provides investigation, hunting, and remediation capabilities to help security teams efficiently identify, prioritize, investigate, and respond to cyberthreats.

» **Learn how to protect against threats and secure your email**

3. Data Backups

- Sensitive student data is extremely valuable. Having a thorough and frequent backup process is critical for seamless recovery and business continuity in the event of a breach.
- As a user-driven measure to ransomware protection, Windows 10/11 supports object-based backups using the OneDrive for Business tool. This setting can be enabled by the user by simply signing into their work or school account. If the endpoint is compromised by ransomware, the files and folders can be safely restored using OneDrive.
- Additionally, our partners Rubrik and Veeam leverage Azure Backup—a solution to backup and recover data from the Azure cloud—to do a complete immutable backup of critical infrastructure. Should there be a site-wide ransomware attack, your data can be safely and quickly restored.

» **Learn more about the importance of backups**

4. Privileged Access Management

- Privileged Access Management (PAM) helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources, giving visibility into who is using privileged accounts and what they are doing while logged in.
- PAM, included in the Microsoft 365 A5 license, provides another granular layer of protection and audit capabilities for privileged access to Microsoft 365 data.

» **Learn more about PAM**

5. Endpoint Detection and Response (EDR)

- Protecting endpoints is a necessary part of a strong cyber security program. Through continuous endpoint monitoring and data analysis, organizations are better equipped in understanding threats relative to their environment.
- Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
- Microsoft Defender for Endpoint Plan 1 is part of Microsoft 365 A3 license, which includes features such as Attack Surface Reduction to find attack surfaces in your environment, and Next Generation Protection—our robust antimalware and antivirus protection.
- Plan 2 is included in the Microsoft 365 A5 license, providing additional features such as Automated Investigation and Response and Endpoint Detection and Response tools to protect environments.

» **Learn more about Microsoft Defender for Endpoint**

6. Vulnerability Management

- Testing and deploying security patches to technical environments is a critical part in protecting systems, managing potential vulnerabilities, and helping prevent exploits.
- Defender Vulnerability Management is a new Microsoft 365 capability that delivers asset visibility and intelligent assessments to prioritize risks and automate fixes for vulnerabilities. Leveraging Microsoft threat intelligence, breach likelihood predictions, business contexts, and device assessments, Defender Vulnerability Management rapidly and continuously prioritizes vulnerabilities to critical assets and provides security recommendations to mitigate risk.
- Try Defender Vulnerability Management with your Microsoft 365 A3 or A5 license.

» **Learn more about Microsoft Defender Vulnerability Management**

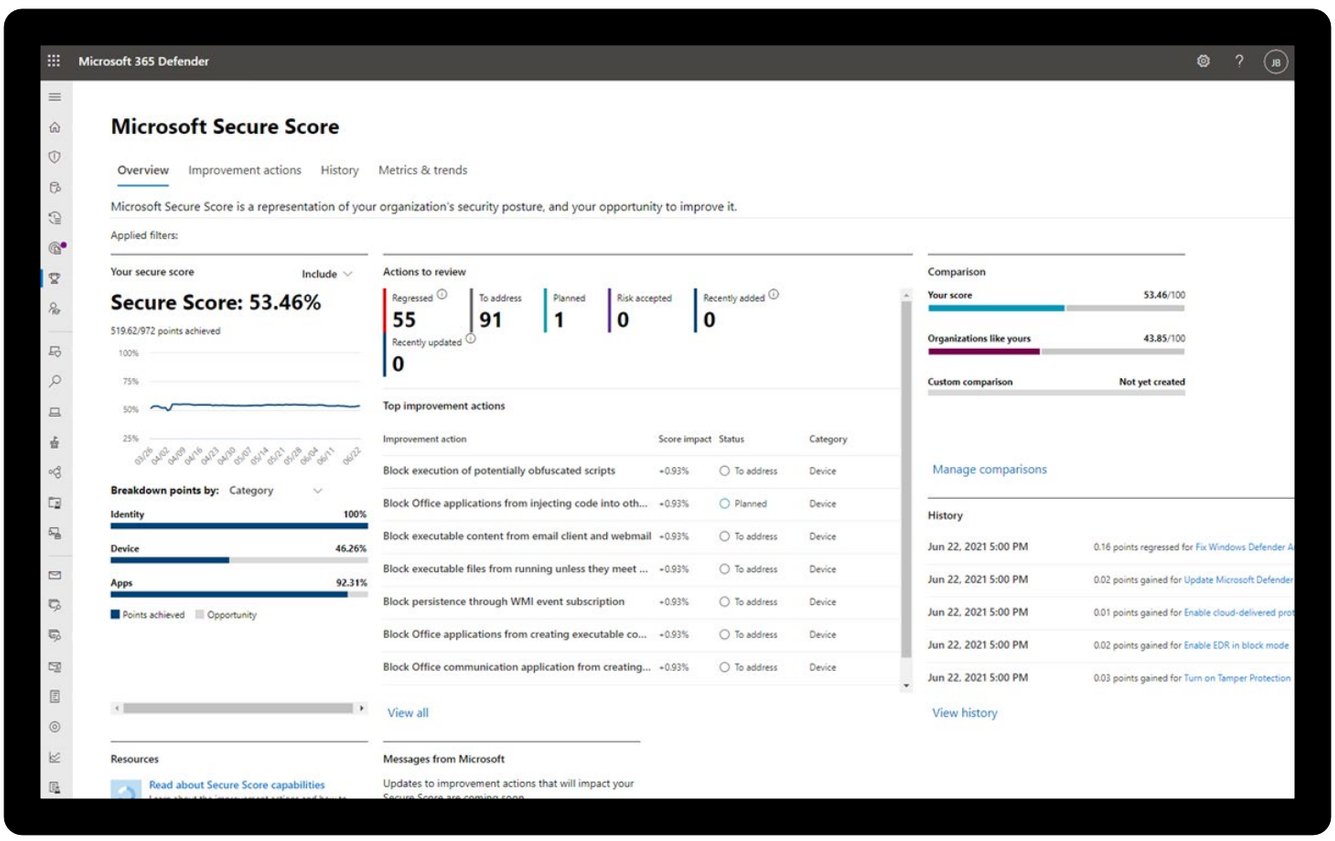
7. 24/7 Centralized Log Monitoring

- Continuous monitoring of activity and user behavior is critical to early-stage detection of suspicious activity, breach containment, and reducing the potential impact and cost of a ransomware attack.
- Microsoft Sentinel, a cloud-native SIEM/SOAR solution, uses the power of AI to provide 24/7 monitoring, user behavioral analytics, and automated response for lean security teams using a single pane of glass.
- Microsoft 365 A3 customers can utilize Sentinel's free data sources, and A5 customers can additionally take advantage of the Sentinel benefit to quickly identify potential threats and enable effective response mechanisms. Sentinel is also available to Azure customers.

» **Learn more about Microsoft Sentinel**

Having these seven basic security controls in place will bolster your defense strategy, help fulfill state and government compliance regulations, and should improve your risk profile to potentially qualify for better cyber insurance coverage terms.

You can periodically check and improve your security posture by viewing your Secure Score in the Microsoft 365 Defender dashboard to ensure you're staying on track.



Ready to get started on your journey to strengthening your security posture? Reach out to your Microsoft representative today to evaluate your Microsoft 365 A3 or A5 capabilities to help with improving your cyber insurance profile.

1 This information is provided to allow Microsoft field teams to work with partners to develop best practices to integrate Microsoft cyber security solutions to reduce risk exposure and mitigate potential losses. Microsoft and its employees are not licensed producers and therefore are not engaging in the sale, solicitation or negotiation of insurance and are NOT offering advice regarding insurance terms, conditions, premium rates or claims. Customers and partners in need of such services should be advised to consult with an appropriately licensed insurance producer, agent, broker or claims adjuster.

2 https://www.microsoft.com/en-us/wdsi/threats

3 Microsoft Digital Defense Report, October 2021,

4 https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html

5 Cyber insurance: Risks and trends 2022 | Munich Re Topics Online