Best practices AI and machine learning Microsoft Intune
7 min read

Why endpoint management is key to securing an AI-powered future

By Steve Dispensa, Vice President of Product for Enterprise Management
Archana Devi Sunder Rajan, Partner Group Product Manager

June 26, 2023

Endpoint security

Zero Trust

Microsoft Copilot for Security

Microsoft Defender

Microsoft Defender for Endpoint

Microsoft Defender Threat Intelligence

Hybrid work

Microsoft Security Insights

The chief information security officer (CISO) agenda has a new set of priorities. Hybrid work and the resultant architecture updates, so prevalent at the beginning of the pandemic, are no longer top of mind. Instead, the thinking is focused on tackling ever more sophisticated threats and integrating Zero Trust in a more nuanced fashion through the concept of data security posture management.[1] With the coming wave of AI, this is precisely the time for organizations to review that new CISO agenda and prepare for the future. To be properly ready for AI, Zero Trust principles take on new meaning and scope. The right endpoint management strategy can help provide the broadest signal possible for AI large language models and make your organization more secure and productive for years to come.

The importance of being prepared for the AI era

The immediate challenge of securing remote employees due to the pandemic may have passed, but the CISO remains as strategic as ever, especially given challenges with resources and the notable amount of open headcount security positions. With these limited resources, the CISO already had to manage the complexities of human actor-operated ransomware and breaches, with more password attacks than ever. However, the proliferation of AI increases the complexity of potential threats for the organization multifold.

Innovations like Microsoft Security Copilot will provide a holistic view of your endpoint security and management data. Using generative AI will help bolster enterprise defenses, especially when using the data available from your endpoint manager's view of your digital estate. A holistic view of what is happening in your environment is critical to dealing properly with security threats and is optimized by receiving signals for all your endpoints. Endpoint management is no longer just mobile device management, but today is responsible for all devices, managed and unmanaged, and provides a powerful way to feed data into AI large language models.

> *Did you know? With Security Copilot, you will be able to leverage generative AI to reason over data across the Microsoft Security portfolio and in turn strengthen the security posture of your enterprise.*

How an organization designs and implements its endpoint management strategy is key to maximizing the AI opportunity for productivity and security enhancements. Both security and employee productivity are vital for any solution; one without the other is futile. The correct endpoint management implementation optimizes the future value of AI for your organization by providing the broadest signal possible to feed into your large language models.

In this blog, we want to urge all CISOs to redouble their endpoint management efforts; both to bolster security through Zero Trust and to ensure the large language models underpinning AI are as powerful as they can be by getting the best, most consistent data from a single source.

Zero Trust for the AI era

The coming AI era will increase the importance of Zero Trust, not decrease it. AI can magnify what an organization can do, so making sure that employees, devices, and data stay secure is more important than ever. And AI can be used to both defend and attack organizations, so Zero Trust deployed properly helps defenses remain as robust as possible.

Microsoft's comprehensive Zero Trust approach rests on three core principles: verify explicitly, use least-privilege access, and assume breach. Microsoft is making progress across all facets of Zero Trust; one example is our latest enhancements to Microsoft Defender Threat Intelligence. Our backgrounds are in endpoint security and multi-factor authentication, so we know how vital identity is in Zero Trust issues. For example, enabling multifactor authentication universally is step one in cutting down phishing and other account compromise attacks.

However, to further drive Zero Trust across the whole organization, you need security policies in force at the endpoint. This might mean Microsoft Defender for Endpoint being up-to-date, or having firewall policies, local drive encryption, or local boot all applied on the device. Without all the appropriate security policies in place, the identity system won't let the user in, thus strengthening enterprise security.

You can't have Zero Trust if you don't have a strongly managed endpoint. Making sure you are using the most up-to-date endpoint management now will help lay the right foundations for security in the age of AI.

Using modern endpoint management to ensure your AI models have the best data inputs

Security is not the only reason to make sure your endpoint management solution is up-to-date.

> *Did you know? You can use the analytical AI features in the Microsoft Intune Suite to detect patterns and anomalies, and analyze events on a device timeline. Identify potential security threats and vulnerabilities and take proactive steps to address them.*

The alerts and indicators that are picked up from endpoint management solutions will, if used correctly, be a key driver in how effectively your organization can harness AI. The best indicators won't just come from as many sources as possible; not just managed devices but those that are not enrolled too. For example, let's say you have built a sophisticated AI model to predict when employees are more susceptible to phishing attacks. If you're only taking data from your email system, without understanding whether those phishing emails are being opened from a smartphone or a computer, you are not analyzing the full range of the potential problem. A fuller AI model to stop phishing attacks would include the device, user, time of day, previous user behavior, and many other data sources available from endpoint management logs. AI models are only as powerful as the data you feed them. If your data is locked away in silos or there is too much noise to signal in the data, that will not set you up effectively to harness the true potential of AI. Data aggregation is, at its core, the foundation for setting yourself up for the future. But first, let's look at your data in terms of endpoint management.

Endpoint management has evolved substantially from separate solutions that tracked computer endpoints and mobile device management. The next iteration, Unified Endpoint Management (UEM), took signals from all devices—laptops, smartphones, and specialized devices. Now, increasingly, management and security are converging in the cloud, and endpoint management means keeping every device in the organization visible and secure, and ensuring every user can be as productive as possible.

Automated and predictable security is complex, and what works for one industry vertical or company size or company architecture or region or worker role may not work for others—there is no "one size fits all." As such, the more data signals you can feed your AI models from across your digital estate, the better the AI's ability to predict potential threats. And the longer you can gather the training data, the better the predictions.

This thought goes beyond core endpoint management data: other related data from products adjacent to UEM (such as from Endpoint Privilege Management, which uses the principle of least privilege to improve security, and Remote Help, which produces a data exhaust key to identify trouble spots) is also incredibly valuable to your AI model, but only useful for AI models if it is accessible, structured, and consistent with the data exhaust provided by the UEM solution so that there is a single source of truth. So, consolidating diverse endpoint tools so that there is one consistent data flow should move up your CISO agenda.

Getting prepared for the AI future now

Generative AI is garnering many headlines right now, but many other forms of AI will also add great value. For example, intelligent applications are using AI to push the boundaries in predicting which employees will be a great fit when recruiting, or when a supplier's predicted delivery date is at risk. Natural language processing helps users ask potentially complex questions the way they would typically speak, opening up analytics beyond those who know how to code a query correctly.

> *Did you know? Generative AI and analytical AI help organizations to analyze and leverage their data in new ways, helping to bridge the gap between IT and security operations teams.*

Microsoft's scale of signal intelligence gives it a powerful perspective here, as does the fact that Microsoft Intune leads the endpoint management market in terms of volume and absolute endpoint growth. We're passionate about helping our customers get ready to seize the opportunity that AI is bringing to enterprise security and society.

Now is the time to start getting prepared for AI, and modernizing your endpoint management approach is key. Even though Zero Trust may have been used for a few years now, it has increased in importance because of AI. Endpoint management can help provide data to help customize your AI models, allowing your organization to become more secure and productive faster.

Microsoft is bringing the power of AI to you, whether that's through integrating Intune with Security Copilot or improving our anomaly detection capabilities. Throughout, we are committed to advancing the principles and practice of responsible AI, which puts security and trust as central in all our AI solutions.

With industries, job descriptions, and technology advancing rapidly, the C-suite must ask how to seize the full potential of AI, while safeguarding your business, your data, and your employees. Today, there is an opportunity to lay the foundation for your organization's AI transformation, and endpoint management is a key component of that. We're thrilled to share more with you in the future as we continue this journey. We hope you'll join us.

Learn more

Learn more about the launch of the Microsoft Intune Suite.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and Twitter (@MSFTSecurity) for the latest news and updates on cybersecurity.

[1] Microsoft Security Insider.

Related Posts

A security practitioner works at a computer.

News

Endpoint security

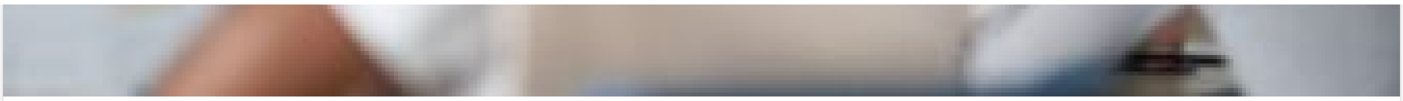
Microsoft Intune

Feb 1

8 min read

3 new ways the Microsoft Intune Suite offers security, simplification, and savings › ›

The main components of the Microsoft Intune Suite are now generally available. Read about how consolidated endpoint management adds value and functionality for security teams.



News
Analyst reports

Sep 19
3 min read

Forrester names Microsoft a Leader in the 2023 Zero Trust Platform Providers Wave™ report › ›

Microsoft is proud to be recognized as a Leader in The Forrester Wave™: Zero Trust Platform Providers, Q3 2023 report.

Best practices
Incident response
Microsoft Incident Response
Cybercrime

Jun 29
3 min read

Patch me if you can: Cyberattack Series › ›

The Microsoft Incident Response team takes swift action to help contain a ransomware attack and regain positive administrative control of the customer environment.

[Best practices](#)
[Cloud security](#)
[Microsoft Defender](#)

Jun 13
7 min read

How Microsoft and Sonrai integrate to eliminate attack paths › ›

Cloud development challenges conventional thinking about risk. Sonrai integrates with Microsoft Sentinel to monitor threats across vectors and automate responses by leveraging security orchestration, automation, and response playbooks, and Microsoft Defender for Cloud to provide visibility across the entire digital estate by identifying possible attack paths and remediating vulnerabilities.

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers