Microsoft Surface

Securing the Way for AI

Multilayered Device Defenses

Contents

Introduction

For many businesses in today's fast-paced digital world, AI stands as a beacon of limitless potential. By unleashing new levels of imagination and productivity, companies can create innovative products and services that set their industry's benchmarks.

Furthermore, AI's capability to analyze and process massive amounts of data with precision empowers businesses to gain a deeper understanding of consumer behavior and market trends.

This enhanced perspective guides more calculated and strategic decision-making. AI isn't just a technological add-on but a transformative force that can reshape industries and shift how businesses operate and compete.

Companies aiming to unlock the power of AI must prioritize strong security measures at the device level. By adopting a comprehensive security strategy that spans the entire ecosystem, businesses can build a secure environment where AI innovation can flourish.

Establishing a secure infrastructure that covers every digital layer lets organizations drive AI advancements and data-centric innovations while maintaining the necessary vigilance to safeguard their assets.

This e-book will explore the strategies and tools for building foundational device security so you can take advantage of the benefits of AI while maintaining integrity and trust in your systems.

Chapter 1

The evolving threat landscape

Targeting the weakest link

Like predators on the hunt, cybercriminals tend to attack the weakest mark. For instance, many ransomware attacks target unmanaged or bring-your-own devices (BYOD), exploiting their generally weaker security measures and defenses. Research for the 2023 Microsoft Defense Report found that 80% to 90% of successful ransomware compromises originated through unmanaged devices.[1]

Attackers typically seek the path of least resistance to infiltrate unauthorized systems. They employ identity theft tactics ranging from conventional brute-force attacks to advanced password spraying across various countries, IP ranges, and Adversary-in-the-Middle (AiTM) attacks.

Phishing remains a regular tool in the cybercriminal arsenal. Attackers deploy both malware-based phishing to take over devices and AiTM phishing techniques to hijack identities for further illicit activities, including business email compromise.

Today, weak identity and data protections represent a welcome sign to would-be attackers. Before implementing AI, businesses must prioritize securing identities and data as a strategic measure to mitigate risks and as a critical investment in the company's long-term resilience and success.

Evolving cybercrime tactics

As organizations strive to increase cybersecurity, cybercriminals evolve to get around new defenses. Many are using the cybercrime as a service model to orchestrate widespread phishing, identity theft, and distributed denial-of-service (DDoS) attacks. At the same time, they're finding ways to get around multifactor authentication and other protective measures to carry out precise attacks.

Ransomware groups increasingly focus on manual, hands-on keyboard tactics, employing techniques that use the victim's existing environment and remote encryption methods to hide their activities. Some cybercriminals will impersonate people within the company, or compromise trusted third parties to make their activities harder to detect while they gain access to corporate systems and data.

Because AI relies on data for learning and execution, businesses must ensure sensitive information isn't exposed to malicious actors. As cybercrime tactics continue to evolve, organizations looking to use AI must also increase their security practices to protect identities and data.

Attackers target what they see as the weakest link, including passwords, outdated systems, and unmanaged devices.

57%

of devices on legacy firmware are exploitable to a high number of Common Vulnerabilities and Exposures (CVEs).[1]

25%

of operational technology devices on customer networks use unsupported operating systems, making them more susceptible to cyberattacks due to a lack of essential updates and protection against evolving threats.[1]

Endpoint attacks can affect anyone. While some individuals might be adept at recognizing common tactics like phishing emails, cybercriminals are continually refining their techniques to stay ahead of technological and security advancements.

Balancing cybersecurity and AI innovation

AI enables machines to perform tasks that normally require human intelligence, such as understanding language, recognizing images, making decisions, and learning from data. It has the potential to revolutionize different facets of business operations, including marketing, customer services, cybersecurity, inventory management, and content creation. By using AI, employees can save time and resources for creative and strategic work, while improving processes and lowering costs. However, with new technology comes new risks. As you look to implement AI in your organization and run AI processes on company devices, it's important to recognize the potential dangers.

The best approach is to develop a comprehensive strategy for device security so you can confidently embrace AI innovation without putting your systems, data, and people at risk.

Three key components of a secure device strategy:

Oversight
See where threats and vulnerabilities exist.

Control
Ensure devices are properly managed.

Protection
Prevent threats from putting data and systems at risk.

Chapter 2

Tracking risks at every device layer

To be truly effective, device security must encompass every layer—hardware, firmware, and software. Each layer is susceptible to cyberattacks that can affect the device's functionality, efficiency, and the security of the data it uses or creates.

Businesses must monitor risks across every digital layer and deploy protective strategies like encryption, authentication, authorization, timely updates, and surveillance.

These measures become even more critical in devices using AI technologies due to their heightened vulnerability to data tampering, targeted attacks, and privacy violations.

The following pages outline the device components that typically contain exploitable vulnerabilities targeted by cybercriminals—and the modern tools for defending against these attacks.

Every digital layer serves a unique purpose:

Hardware
Refers to the device's physical components, including processors, memory, sensors, and cameras.

Firmware
Provides the foundational software that manages the hardware's functions, including booting, updating, and communications.

Software
Includes the applications and programs running on the device, such as the operating system, web browsers, and AI applications.

First layer: Hardware vulnerabilities

Weak identity verification allows malicious actors to gain access

Passwords often pose security risks, primarily due to human error. When a user's password is stolen, either by phishing, malware, or physical theft, an attacker can use it to gain access to its critical hardware components, such as the processor, memory, storage, or peripherals.

Once they've gained access, attackers might install malware, ransomware, or spyware. They can steal or alter the device's data, including encryption keys or personal information, cause damage to or destroy the device's hardware or software, or take control over the device's operations or functionalities.

Password attacks have increased 10x.[1]

Non-removable SSDs increase the risk of data theft

Devices with non-removable SSDs are at an increased risk of data theft when they're decommissioned or sent off for necessary repairs. Once the device is out of the end user's sight, attackers could potentially access the data by booting the device from an external source or using malicious USB devices. Removable SSDs help provide peace of mind by ensuring that an organization's sensitive information won't be exposed when their devices change hands or are no longer in use.

Attackers are targeting the hardware supply chain

Attackers are quickly adapting to the fact that organizations are becoming more vigilant about device security. In this era of heightened awareness around hardware security, attackers are switching their focus to earlier stages in the device lifecycle, notably the supply chain.

This shift has led to increased supply chain attacks, where attackers intercept devices during transit, inserting malicious code or physical implants that act as a "back door" that they can enter through upon the device's first boot-up.

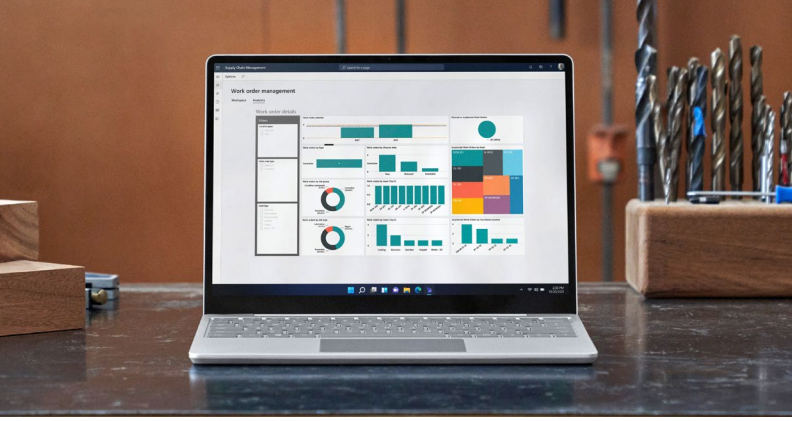
Supply chain security is a shared responsibility. Rather than trusting that every device reaches its destination untouched, organizations must properly vet their original equipment manufacturers (OEMs) and suppliers. Consider track records and security practices to make sure they're investing significantly in supply chain security and perform rigorous quality control of every device that falls under your company's purview.

Robust hardware defense for AI integration

Strong hardware security is critical for accessing AI experiences. It ensures the physical components of a device—processors, memory units, sensors—are shielded from unauthorized access and tampering to protect AI experiences at both the local level and in the cloud.

At the local level, strong security mechanisms help protect the device's integrity and privacy of AI apps and local language models. When engaging with AI systems in the cloud, you must protect the integrity of the user's identity to ensure only the right individuals are using those systems.

For both kinds of AI experiences, investing in robust hardware security measures isn't just about protecting technology—it's about safeguarding business continuity, reputation, and the trust of stakeholders.



Second layer: Firmware vulnerabilities

Legacy Basic Input Output System (BIOS) interfaces are vulnerable to pre-boot attacks

First used in 1975, BIOS is a traditional firmware that devices use to start hardware operations. Some devices still rely on legacy BIOS interfaces, posing several security vulnerabilities.

Malware developers have found ways to exploit vulnerabilities in the early stages of a device's boot process, including the system-embedded firmware and the critical moments between firmware initiation and the OS startup.

This can compromise the boot process, allowing malicious code to execute before the OS's security measures are in place.

Cameras and microphones require more granular control

In security-sensitive environments like military bases, government offices, banks, hospitals, airports, or research labs, regulatory requirements may discourage the use of cameras and microphones. In these settings, organizations need tighter control of their device firmware so they can disable cameras and microphones.

The ability to block certain functionalities serves as a safeguard against breaches, preventing the unintentional capture and transmission of sensitive information while helping organizations ensure strict regulatory compliance.

Preparing the firmware level for AI experiences

Securing a device's firmware is vital when using AI technologies. Firmware acts as the intermediary between the device's hardware and the software applications it runs—including ones that use AI. Firmware vulnerabilities can serve as gateways for cyber attackers to infiltrate and manipulate the device, leading to data breaches and unauthorized access to sensitive information.

Since firmware controls essential functions such as device booting, operation, and communication, its security is paramount for the overall protection and integrity of the endpoint. By ensuring firmware is regularly updated and protected against unauthorized modifications, businesses can prevent exploits that could undermine AI-driven operations.

This level of security is indispensable for maintaining the reliability, performance, and trustworthiness of AI experiences, especially in environments where the accuracy and confidentiality of processed data are critical.

Third layer: Operating system and software vulnerabilities

Privilege escalation amplifies the damage of an attack

An escalation of privilege attack starts with targeting a low-privilege user, then moving laterally through the system until the attacker secures access to valuable resources. This breach enables the perpetrator to undertake activities beyond their authorized scope, such as accessing confidential information, altering system configurations, installing malicious software, establishing unauthorized entry points, and manipulating data that AI experiences might use.

Lack of encryption mechanisms leaves data vulnerable

Without encryption mechanisms in place, data is left exposed and susceptible to theft, alteration, or corruption by malicious actors. This vulnerability means that data could be easily accessed by unauthorized users who manage to gain physical or remote entry to the device. Furthermore, the data is at risk of being modified or damaged by harmful software or code, including malware, ransomware, or viruses. During transmission via email, messaging, or file sharing, the data could be intercepted or leaked, posing significant privacy and security risks.

The implications of these vulnerabilities are severe for both the owner and recipient of the data. There could be a loss of confidentiality, where sensitive or personal information like passwords, financial records, health documents, or trade secrets become exposed. There is also a risk to the integrity of the data, which may turn inaccurate, incomplete, or inconsistent, which decreases its reliability and value when used by AI applications. Lastly, the availability of the data could be compromised, rendering it inaccessible, unusable, or entirely lost.

The role of software security in preserving AI reliability

Software vulnerabilities can seriously compromise the integrity and performance of AI experiences. Software security ensures that the applications and operating systems running AI applications are protected against malware, hacking attempts, and unauthorized access, which are pivotal in maintaining the data's confidentiality, integrity, and availability.

Given AI's complexity and data-driven nature, any breach in software security can lead to manipulated outputs, incorrect decision-making, and exposure of sensitive information. This affects the reliability and effectiveness of AI applications and presents substantial risks to user privacy and organizational reputation. For this reason, regular updates, patch management, and vulnerability assessments are essential for protecting software and operating systems running AI workloads.

Chapter 3

Multilayered security for the era of AI

Multilayered device security is paramount because risks exist at every layer of a device's makeup. Think of it as fortifying a castle—the more layers of defense you build around it, the harder it becomes for an attacker to breach and cause damage. However, adding AI to the mix also adds more potential weaknesses in your security framework, making comprehensive security even more essential.

Designed for the era of AI, Microsoft Surface devices integrate hardware and software security features with Microsoft Security cloud capabilities, making it more challenging for attackers to find and exploit vulnerabilities at every level. They provide hardware, firmware, and software security by using Microsoft-built components and advanced Windows security features that prevent unauthorized access, protect data, and enable faster and smarter AI applications on the device.

How do Surface devices secure every layer for AI innovation?

Hardware defenses

AI innovation relies on secure hardware to ensure that the data and algorithms used for training and inference aren't tampered with or stolen. Surface devices offer robust security starting right from the hardware layer, with Microsoft performing strict supply chain oversight to safeguard against hardware tampering.

Devices come with secure microchips, biometric authentication, and a removable SSD to protect the device from malicious attacks that would compromise the integrity and confidentiality of data and AI processes.

Firmware protections

Surface devices secure this critical layer with enhanced firmware protection and device management capabilities. Regular updates delivered via Windows Update and streamlined deployment via the Microsoft Intune admin center offer heightened control over the device's hardware, mitigating the risk of firmware-based cyberattacks.

The firmware security offered by Surface devices plays a crucial role in securely handling sensitive data, preventing attackers from hijacking cameras and microphones, and safeguarding the device against unauthorized interventions or alterations to ensure the AI applications remain intact and reliable.

Operating system and software security features

Surface devices use Windows 10 or Windows 11, which receive regular updates to incorporate the latest security advancements. These operating systems come equipped with robust defenses against a spectrum of threats, including malware, ransomware, and phishing, through integrated tools like Windows Security and Microsoft Defender.

The software and operating system security included with Surface devices facilitate the safe access, storage, and processing of vast datasets and code, which is crucial for maintaining privacy and data integrity when using AI.

Running secure AI workloads

Instead of relying solely on cloud processing for AI workloads, there's a growing interest in using the processing capabilities of local devices. Select Surface devices enable the processing of local AI workloads by integrating a neural processing unit (NPU). This specialized hardware is designed to execute AI experiences efficiently while operating independently of the CPU.

Including an NPU in Surface devices allows for advanced AI functionalities such as Windows Studio effects, which uses AI to enhance online meetings' audio and video quality. Plus, it offers enhanced security for AI workloads by allowing users to run AI models locally on the device rather than sending the data over networks or the cloud to be processed by a third-party service.

Using the NPU, Surface devices deliver quicker, smoother, and more secure AI experiences without cloud connectivity and with minimal impact on battery life.

As organizations grow more comfortable and familiar with AI, there will be an increase in hybridized AI models wherein AI operates both in the cloud and on local devices. Wherever you plan to run AI workloads, it's crucial to ensure proper oversight, control, and protection to maintain a secure and efficient digital ecosystem.

Three essential strategies for modern security

Remote device management

RDM allows for instant access to and monitoring of devices. Administrators can swiftly locate, lock, quarantine, or wipe devices in emergencies, ensuring immediate response to any security threats. It also enforces security policies and configurations across devices, performing regular updates and patches to reduce the risk of vulnerabilities and prevent potential exploits. Additionally, RDM incorporates security measures such as encryption and two-factor or multifactor authentication, which are crucial for safeguarding data and restricting access to authorized personnel.

Zero Trust security

At the core of Zero Trust security is a demand for rigorous identity verification for anyone and any device attempting to access resources on a private network. This requirement holds true regardless of the user's or device's location, whether inside or outside the network's perimeter. The model operates under the assumption that threats can exist outside and inside the network, making it essential to adopt a "Never trust, always verify" approach to security.

Security in the cloud

Surface showcases the best of what Microsoft has to offer, including its cloud security stack. For example, Microsoft Security Copilot[2] is designed to enhance the efficiency and capabilities of security professionals, ensuring swift and effective security outcomes while adhering to responsible AI principles. It offers an intuitive, natural language interface to assist in various tasks such as incident response, threat hunting, intelligence gathering, and posture management.

Seamlessly integrating with security solutions like Microsoft Defender XDR, Microsoft Sentinel, and Microsoft Intune, Security Copilot helps quickly summarize incident information, evaluate impact, advise on remedial actions, and generate comprehensive reports on security investigations and threats.

Conclusion

Comprehensive security from chip to cloud

Organizations that want to use the power of AI must prioritize comprehensive device security that extends from hardware to software. At the hardware level, this involves implementing robust protections against physical tampering and ensuring the integrity of physical components. This is crucial as hardware is the foundation upon which all software operates.

On the software side, deploying advanced security protocols, including strong encryption, access controls, and regular updates to guard against cyber threats is essential. These measures must be integrated seamlessly to create a unified defense strategy.

Microsoft Surface devices offer fortified hardware and software to create a secure environment for AI adoption. Whether you plan to use AI in the cloud or directly on your devices, Surface ensures that your data and operations remain secure at every layer. This comprehensive security coverage supports your initiatives for innovation while protecting your digital environment.

Get AI ready.

Learn more about Microsoft Surface >

Chip-to-cloud security

Multilayered security with Microsoft

Hardware

- Windows Hello for Business
- TPM 2.0
- Pluton technology
- Removable SSD

Firmware

- Microsoft UEFI
- Surface Enterprise Management Mode (SEMM)
- DFCI

OS

- HVCI/VBS
- Secure Boot by BitLocker

Cloud

- Microsoft Defender
- Surface Management Portal

[1]Microsoft Digital Defense Report, October 2023.

[2]Microsoft Security Copilot is not included as a standard feature with Surface devices. An additional license must be acquired to use this security service. For more information on obtaining the necessary licensing, contact a Microsoft representative or visit the official Microsoft website.