Best practices IoT security Microsoft Defender for IoT

9 min read

Adopting guidance from the US National Cybersecurity Strategy to secure the Internet of Things

By David Weston, Vice President, Enterprise and OS Security

August 7, 2023

Zero Trust Microsoft Defender Cryptojacking more

The recently published United States National Cybersecurity Strategy warns that many popular Internet of Things (IoT) devices are not sufficiently secure to protect against many of today's common cybersecurity threats.[1] The strategy also cautions that many of these IoT devices are difficult—or, in some cases, impossible—to patch or upgrade. A key development occurred on July 18, 2023, at the White House with the announcement of a US cybersecurity labeling program for smart devices to inform consumers in choosing products that are less vulnerable to cyberattacks.[2] This labeling program requires manufacturers to take responsibility for the security of devices, not just when they are shipped, but over their lifetime with security updates. Microsoft has a long history of building secured platforms which can provide the basis for manufacturers to create products that achieve the requirements of the cybersecurity labeling program, including Windows IoT, Azure Sphere, and Edge Secured-Core.

Microsoft's IoT security commitments

While customers are familiar with our approach to Windows PC and server security, many are unaware that Microsoft has taken similar steps to strengthen the security of business-critical systems and the networks that enclose them, including vulnerable and unmanaged IoT and OT endpoints. Microsoft often detects a wide range of threats targeting IoT devices, including sophisticated malware that enables attackers to target compromised devices using botnets[3] or compromised routers,[4] and a malicious form of cryptomining called cryptojacking.[5] This blog post details Microsoft's efforts to help partners create IoT solutions with strong security, thereby supporting initiatives outlined in the new National Cybersecurity Strategy and other US Cybersecurity and Infrastructure Security Agency (CISA) initiatives.

Developing and deploying software products that are secure by design and default is both a challenging and costly endeavor. According to recent guidance from the CISA, Secure-by-Design requires significant resources to incorporate security functions at each layer of the product development process.[6] To maximize effectiveness, this approach needs to be integrated into a product's design from the onset and cannot always be "bolted on" later.

Security by design and default is an enduring priority at Microsoft. In 2021, we committed to investing USD100 billion to advance our security solutions over five years (approximately USD20 billion per year) and today we employ more than 8,000 security professionals.[7] One result of these investments is Windows 11, our most secure version of Windows yet. At Microsoft, we have a great deal of experience around security by design and default and have strived to implement best practices into our products and programs to assist partners who combine hardware, innovative functionality, online services, and operating systems (OS) to produce and maintain IoT solutions with robust security.

Applying Zero Trust to IoT

Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network. Regardless of where the request originates or what resource it accesses, the Zero Trust model teaches us to "never trust, always verify." A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy.

Microsoft advocates for a Zero Trust approach to IoT security, based on the principle of verifying everything and trusting nothing (see Seven Properties of Highly Secure Devices). Zero Trust is also aligned with the new directives in the US National Cybersecurity Strategy and the requirements of the new US cybersecurity labeling program.

A traditional network security model often doesn't meet the security or user experience needs of modern organizations, including those that have embraced IoT in their digital transformation strategy. User and device interactions with corporate resources and services now often bypass on-premises, perimeter-based defenses. Organizations need a comprehensive security model that more effectively adapts to the complexity of the modern environment, embraces the mobile workforce, and protects their people, devices, applications, and data wherever they are.

To optimize security and minimize risk for IoT devices, a Zero Trust approach requires:

1. **Secure identity with Zero Trust:** Identities—whether they represent people, services, or IoT devices—define the Zero Trust control plane. When an identity attempts to access a resource, verify that identity with strong authentication, and ensure access is compliant and typical for that identity. Follow least privilege access principles.
2. **Secure endpoints with Zero Trust:** Once an identity has been granted access to a resource, data can flow to a variety of different endpoints—from IoT devices to smartphones, bring-your-own-device (BYOD) to partner-managed devices, and on-premises workloads to cloud-hosted servers. This diversity

creates a massive attack surface area. Monitor and enforce device health and compliance for secure access.

3. **Secure applications with Zero Trust:** Applications and APIs provide the interface by which data is consumed. They may be legacy on-premises, lifted and shifted to cloud workloads, or modern software as a service (SaaS) applications. Apply controls and technologies to discover shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, monitor for abnormal behavior, control user actions, and validate secure configuration options.
4. **Secure data with Zero Trust:** Ultimately, security teams are protecting data. Where possible, data should remain safe even if it leaves the devices, apps, infrastructure, and networks the organization controls. Classify, label, and encrypt data, and restrict access based on those attributes.
5. **Secure infrastructure with Zero Trust:** Infrastructure—whether on-premises servers, cloud-based virtual machines, containers, or micro-services—represents a critical threat vector. Assess for version, configuration, and just-in-time access to harden defense. Use telemetry to detect attacks and anomalies, automatically block and flag risky behavior, and take protective actions.
6. **Secure networks with Zero Trust:** All data is ultimately accessed over network infrastructure. Networking controls can provide critical controls to enhance visibility and help prevent attackers from moving laterally across the network. Segment networks (and do deeper in-network micro-segmentation) and deploy real-time threat protection, end-to-end encryption, monitoring, and analytics.
7. **Visibility, automation, and orchestration with Zero Trust:** In our Zero Trust guides, we define the approach to implement an end-to-end Zero Trust methodology across identities, endpoints and devices, data, apps, infrastructure, and networks. These activities increase your visibility, which gives you better data for making trust decisions. With each of these individual areas generating their own relevant alerts, we need an integrated capability to manage the resulting influx of data to better defend against threats and validate trust in a transaction.

Microsoft's Edge Secured-Core program

At Microsoft, we understand Secure-by-Design and Secure-by-Default are difficult to build and even more challenging to get right. To simplify this process, we created Edge Secured-Core, a Microsoft device certification program that codifies and operationalizes the security tenets such as secure by default and Zero Trust into a clear set of requirements. Edge Secured-Core also provides tooling and assistance to our device ecosystem partners to help them build devices that meet these security requirements. We have further customized those requirements for various platforms that manufacturers use to build devices, including Microsoft-provided operating systems Windows IoT and Microsoft Azure Sphere, and ecosystem-provided operating systems based on Linux. Edge Secured-Core devices from partners including Intel, AAEON, Lenovo, and Asus can be found in the Azure Certified Device Catalog today.

Windows IoT

Windows IoT is a platform that leverages our long history and investment in Windows security to enable more secure and reliable IoT solutions. Whether you are building devices for industrial usage, healthcare or retail sectors, or other scenarios, Windows IoT provides key capabilities to protect your devices and data from the many prevalent threats in today's digital landscape.

Windows IoT capabilities include:

- **BitLocker**, which encrypts the data stored on the device to prevent unauthorized access.
- **Secure Boot**, which verifies the integrity of the boot process and prevents malicious code from running.

- **Code integrity**, which verifies the integrity of operating system files when loaded and enforces device manufacturer policies that dictate the drivers and applications that can be loaded on the device.
- **Exploit mitigations**, which automatically applies several exploit mitigation techniques to operating system processes and apps (examples include kernel pool protection, data execution protection, and address space layout randomization).
- **Device attestation**, which proves the identity and health of the device to cloud services.

Windows IoT also offers end-to-end management and updates using the trusted Windows infrastructure, ensuring consistent and timely delivery of security patches and feature enhancements. Some versions of Windows IoT support a 10-year servicing term, allowing partners to receive updates and maintain application compatibility, reducing the risk of obsolescence and vulnerability.

Another benefit of Windows IoT is the flexibility to run containerized workflows, including Linux, on the same device. This allows partners to use existing skills and tools, thereby optimizing performance and resource utilization. Containers provide isolation and portability, enhancing the security and reliability of applications.

Defending against threats with Microsoft Azure Sphere

Microsoft Azure Sphere is a fully managed, integrated hardware, operating system, and cloud platform solution for medium- and low-power IoT devices. It offers a comprehensive approach to secure IoT devices from chip to cloud.

Azure Sphere devices combine a low-power Arm Cortex-A processor running a custom Linux-based operating system serviced by Microsoft with Arm Cortex-M processors for real-time processing and control. Device manufacturers can develop, deploy, and update their applications, while Microsoft independently provides operating system security updates and device monitoring. Additionally, Azure Sphere devices embed the Microsoft Pluton security architecture, providing a hardware-based root of trust and cryptographic engine. Pluton protects the device identity, keys, and firmware from physical and software attacks and enables secure boot and remote attestation.

Azure Sphere provides deep defense by employing multiple layers of protection to mitigate the impact of potential vulnerabilities, such as secure boot, kernel hardening, and a per-application network firewall. Azure Sphere devices communicate with a dedicated cloud service, the Azure Sphere Security Service, which attests the device is running expected and up-to-date software, performs both operating system and application updates, provides error reporting, and retrieves a Microsoft signed certificate that is renewed daily.

Similar to Windows IoT, Azure Sphere also offers a 10-year term for security fixes and operating system updates for all devices, as well as an application compatibility promise that ensures existing applications will continue to run on future operating system versions. Also, supporting CISA's secure-by-design recommendations, Azure Sphere has started enabling embedded development using Rust, a coding language designed to improve memory safety and reduce mistakes during development.[8]

Enhancing security on Linux devices

While Microsoft directly provides operating system updates for Windows IoT and Azure Sphere, Edge Secured-core provides a way of ensuring the same security tenets of secure-by-design and default principles are applicable for devices that use ecosystem-provided distributions of the Linux OS. We collaborate with Linux partner companies to ensure their distributions meet security requirements such as committing to security updates for at least five years, building in support for Secure boot, etc. Microsoft incorporates security checks to onboard operating system partners and ongoing monitoring using Microsoft security agents on these devices, thus providing confidence to customers.

Secure your IoT devices with Microsoft Defender for IoT

Next to consumers, organizations are investing in automation and smart technology to streamline operations, cyber-physical systems, once completely isolated from the network, are now converging with mainstream IT infrastructure. Microsoft Defender for IoT is a security solution that enables organizations to implement Zero Trust principles across enterprise IoT and OT devices to minimize risk and protect these mission-critical systems from threats, as their attack surface expands.[9]

Defender for IoT empowers analysts to discover, manage, and secure enterprise IoT and OT devices in their environment. With network layer monitoring, analysts get a full view of their IoT and OT device estate as well as valuable insights into device-specific details and behaviors. These insights in tandem with generated alerts help analysts protect their environment by easily identifying and prioritizing risks like unpatched systems, vulnerabilities, and anomalous behavior all from a centralized user experience.

Support for the broader IoT ecosystem

Beyond these core platforms, Microsoft provides additional programs and services to enable partners to create more secure IoT devices. For example, due to the wide range of possible configurations and hardware platforms, operating systems such as Azure RTOS place the responsibility of security more heavily on the device manufacturer. SDKs and services like Device Update for Microsoft Azure IoT Hub allow partners to add support for over-the-air software updates to their products.

Microsoft Security supports the US National Cybersecurity Strategy

Microsoft remains committed to supporting the US National Cybersecurity Strategy and helping partners effectively deliver and maintain more secure IoT solutions using powerful technology, tools, and programs designed to improve security outcomes. It is vitally important that partners focus on IoT security by prioritizing security through smart design and development practices and carefully selecting platforms and security defaults that are secure as possible to lower the cost of maintaining the security of products.

Learn more

Learn more about Microsoft Defender for IoT.

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] United States National Cybersecurity Strategy, The White House. March 2023.

[2] Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers, The White House. July 13, 2023.

[3] Microsoft research uncovers new Zerobot capabilities, Microsoft Threat Intelligence. December 21, 2022.

[4] Uncovering Trickbot's use of IoT devices in command-and-control infrastructure, Microsoft Threat Intelligence. March 16, 2022.

[5] IoT devices and Linux-based systems targeted by OpenSSH trojan campaign, Microsoft Threat Intelligence. June 23, 2023.

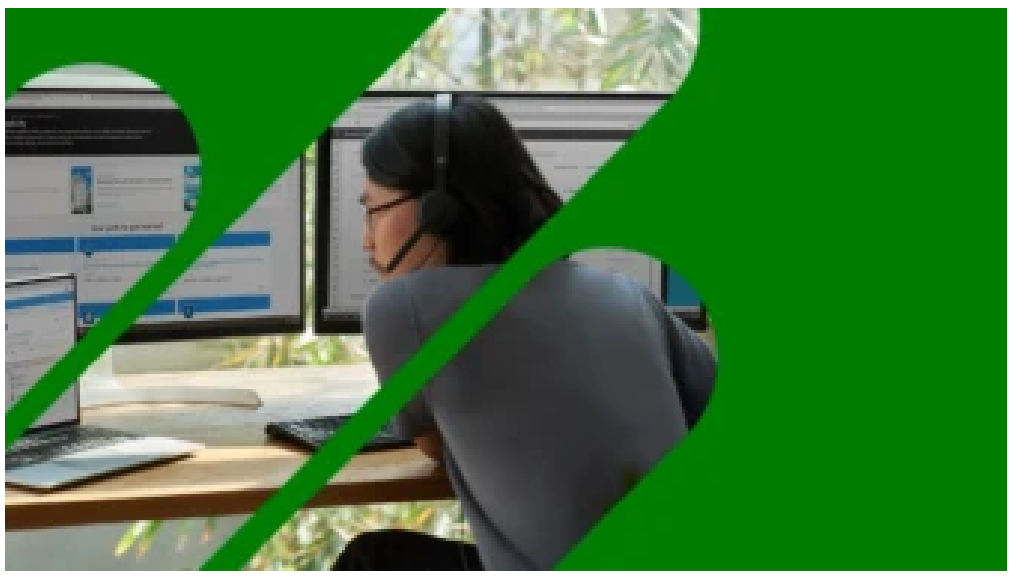
[6] Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default, CISA. April 13, 2023.

[7]Satya Nadella on Twitter. August 25, 2021.

[8]Modernizing embedded development on Azure Sphere with Rust, Akshatha Udayashankar. January 11, 2023.

[9]Learn how Microsoft strengthens IoT and OT security with Zero Trust, Michal Braverman-Blumenstyk. November 8, 2021.

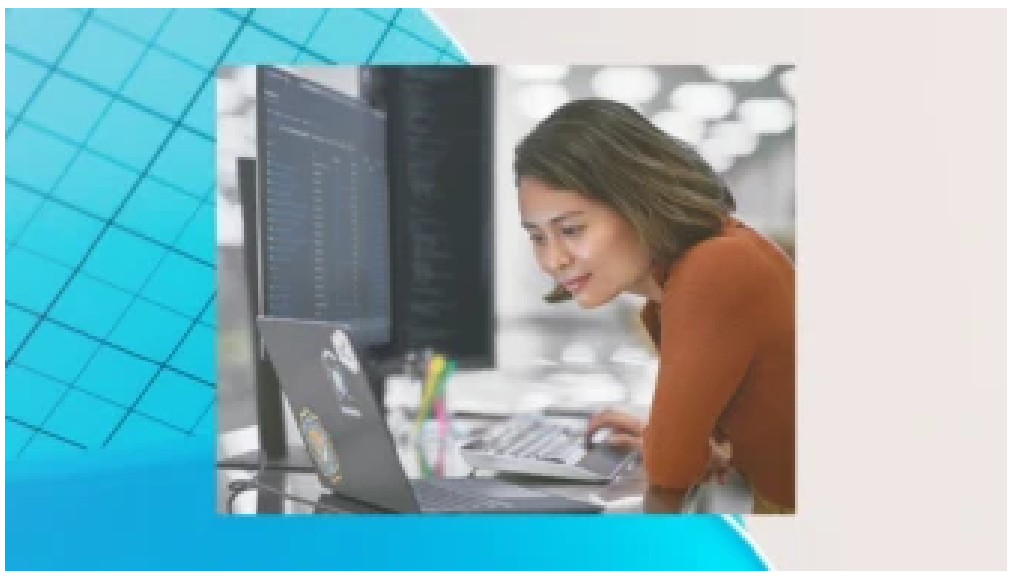
Related Posts



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.



Industry trends Microsoft Intune Jan 29 <1 minute read

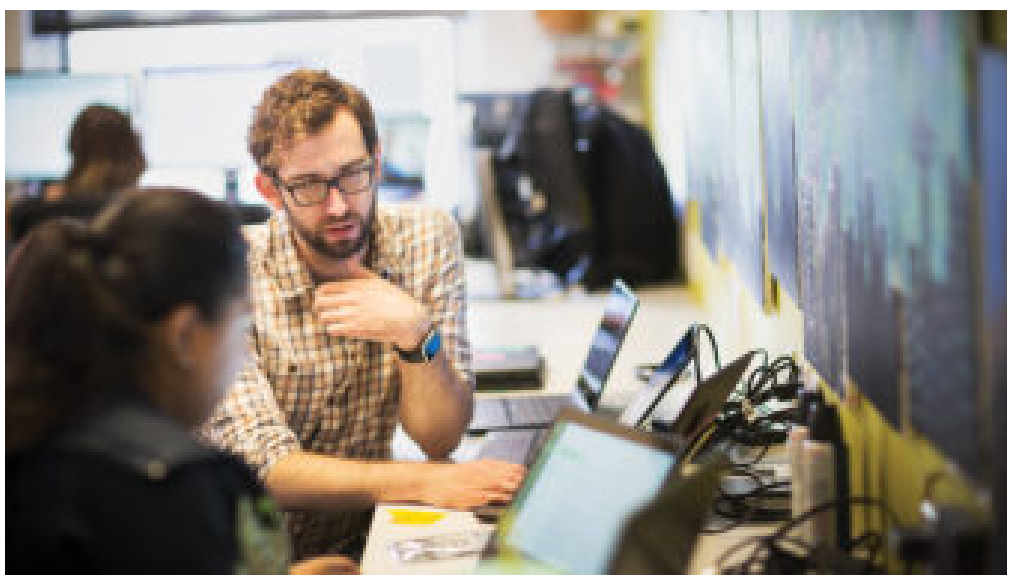
Best practices in moving to cloud native endpoint management >

This blog is the second of three that details our recommendation to adopt cloud native device management. Understand the lessons from various Intune customers in their journeys and how they achieved greater security, cost savings, and readiness for the future through their cloud transformations.

News AI and machine learning Microsoft Intune
Sep 26, 2023 6 min read

New security features in Windows 11 protect users and empower IT >

Windows 11 is designed to simplify security with features from the chip to the cloud that are on by default. Since its launch, we've seen a 58 percent reduction in security. Learn more about the new features.



Research Threat intelligence Microsoft Defender Attacker techniques, tools, and infrastructure
Jul 25, 2023 13 min read

Cryptojacking: Understanding and defending against cloud compute resource abuse >

Cloud cryptojacking, a type of cyberattack that uses computing power to mine cryptocurrency, could result in financial loss to targeted organizations due to the compute fees that can be incurred from the abuse.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

- Surface Laptop Studio 2
- Surface Laptop Go 3
- Surface Pro 9
- Surface Laptop 5
- Microsoft Copilot
- Copilot in Windows
- Explore Microsoft products
- Windows 11 apps

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
- About Microsoft
- Company news
- Privacy at Microsoft
- Investors
- Diversity and inclusion
- Accessibility
- Sustainability