Microsoft

IoT Security in Depth:

From the Device to the Cloud

Table of Contents

1 Overview 2

2 IoT security posture foundations 3

3 Securing IoT environments holistically, from the device to the cloud 4

3.1 Device security: Building a secure device ecosystem 4

3.1.2 Enterprise-class operating systems, SDKs, and operating models 6

3.2 Connection and edge security: Providing secure connectivity and integration 7

3.2.1 Data and analytics protection at the edge 7

3.2.2 Streamlined connectivity development for secure IoT solutions 7

3.3 Cloud security: Detecting and responding to threats in the cloud 8

3.3.1 Hybrid cloud workload threat protection 9

3.3.2 Aggregation, analysis, and response 9

4 Conclusion 11

1 Overview

By forging new links between the cyberworld and the physical world, IoT creates a paradigm shift that dramatically increases the scope of security. As organizations rush to adopt IoT, novel security challenges abound, amplified by an enormous diversity of hardware, software, services, and deployment locations. In fact, while 91 percent of IoT decision-makers report plans to increase the number of their connected devices by more than 15 percent within two years, they cite security as the greatest concern for deploying IoT technologies.[1]

Threats to devices, applications, services, connections, and data must be addressed holistically across the IoT infrastructure to create a consistent security posture across IoT devices, the edge, the cloud, and the connections between all those elements. IoT leaf devices range from simple, single-function sensors and actuators to server-class systems. IoT gateways establish intelligence at the network edge, for purposes that range from performing on-site analytics to protecting vulnerable endpoints. Public and private clouds provide centralized, elastic storage and compute power as well as platform as a service (PaaS) services to scale on demand and provide resiliency in the event of failures.

Compounding the difficulty of securing the IoT environment is a lack of comprehensive IoT expertise within most organizations. Instead, there are typically separate domain experts in information technology (IT) and operational technology (OT), without overarching management to coordinate them. In fact, IoT decision-makers cite a lack of centralized management and executive awareness as the top challenges of securing IoT.[1]

That organizational complexity mirrors the complexity of the IoT infrastructure. It is challenging to integrate the diverse elements of the IoT environment and create a consistent security posture across them. At the same time, the sheer scale of many IoT deployments—including potentially millions of endpoints—creates the need to reimagine the strategic approach to securing IoT infrastructures. The importance and gravity of securing IoT infrastructures are increased because protecting critical infrastructure, lifesaving medical devices, and major economic forces is at stake.

2 IoT security posture foundations

Modeling the threats against vital resources must begin early in the process of designing and planning security measures for IoT, when flexibility exists to eliminate threats by design, rather than mitigating those threats later. Development teams should perform formal threat modeling to proactively map out how a potential attacker might exploit vulnerabilities to processes, data flows, or storage. The process of identifying threats, resolving them, and then validating those resolutions should continue indefinitely as changes are made to the IoT environment.

The rigor needed for in-depth security of an IoT environment requires involvement from parties across the design, development, and deployment of the IoT infrastructure. Roles for IoT manufacturers/integrators, as well as IoT solution developers, deployers, and operators, are examined in Security best practices for IoT.

In addition to a robust working threat model, IoT security posture draws on theoretical constructs and established best practices. The transition from traditional IT (cyber only) to IoT (cyber plus autonomous-physical) network architectures requires organizations to reevaluate their security postures and their established approaches to security strategy, such as perimeter-based measures and VPNs. In addition, hardware with the potential to be connected to IoT infrastructure should be designed according to the seven properties of secure devices best practices.

Strategic considerations for securing IoT environments

Zero-trust computing assumes a constant breach state and treats every interaction as hostile until proven otherwise. Every request must be authenticated, with least-privileged access limiting rights to resources.

Assessing Zero Trust readiness ▸

Scale and diversity addresses complexity based on devices with varying architectures and security postures—often in uncontrolled locations—as well as hybrid cloud services.

Security beyond the perimeter ▸

Trusted apps for the edge ▸

Breach detection uses machine learning to characterize normal patterns of user and system behavior, then detects anomalies that indicate potential threats.

Investigating risky users ▸

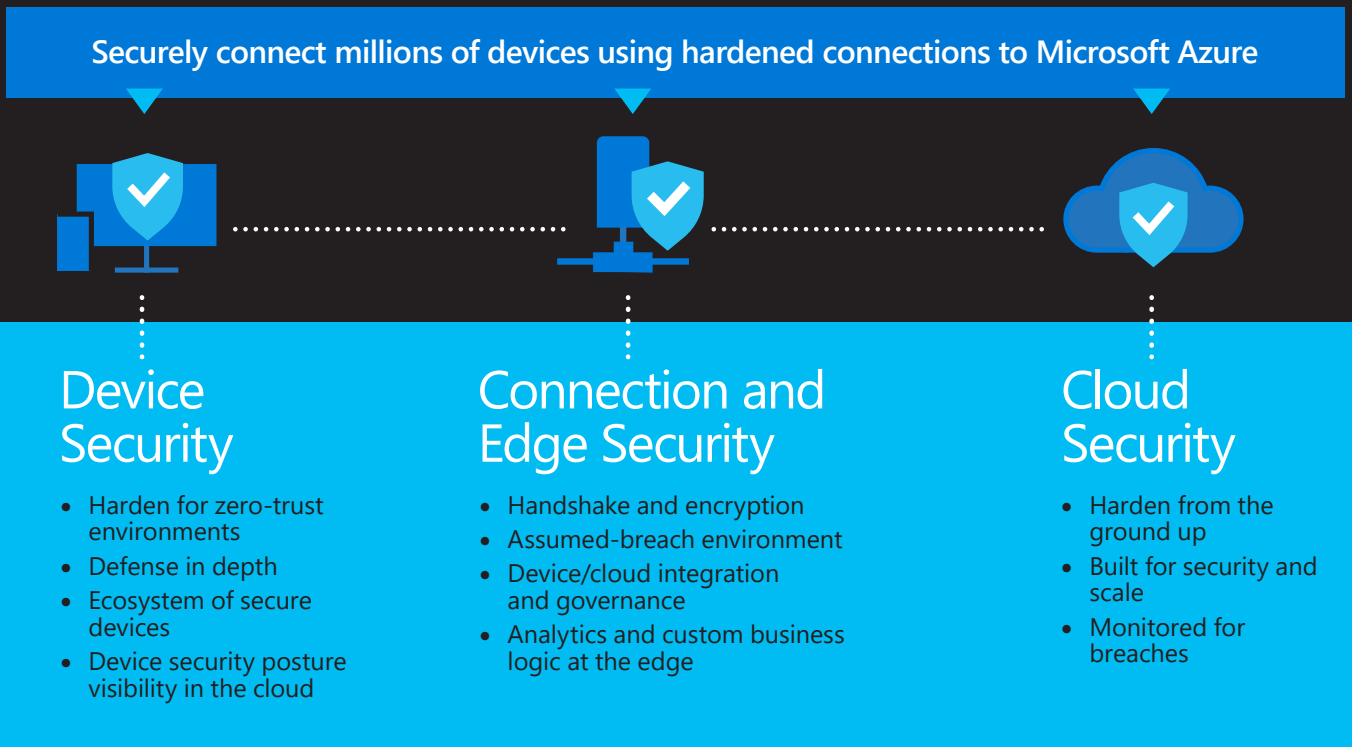
Defending IoT devices ▸

Risk management formalizes risk assessment with a structured, hierarchical framework that analyzes the gap between an organization's current security state and a desirable target state.

Determining security maturity ▸

3 Securing IoT environments holistically, from the device to the cloud

Microsoft has engaged in a range of efforts such as developing technologies, programs, partnerships, and standards initiatives that address all aspects of securing IoT infrastructure, including IoT devices, edge devices, connections, and the cloud. These technologies help secure cross-OS environments—such as Linux, Windows, Azure Sphere, and more—providing the ecosystem and deployment models organizations need as they implement IoT and secure the environment, from end to end.



3.1 Device security: Building a secure device ecosystem

Key to generating value from IoT is securely drawing on the capabilities of millions of diverse devices. The complexity of that effort is increased by the variety of devices and their widely differing levels of risk and security criticality, which require a range of security features and capabilities. For example, the risk and criticality of compromise to a smart light bulb in a retail location may be lower than that of a temperature sensor at an industrial facility.

3.1.1 Hardware-based security features and capabilities

As new classes of devices become connected—often without due attention to security—seemingly minor IoT implementations expose millions of microcontroller units (MCUs) to the internet. Compromised MCUs can be harnessed for botnet attacks, a growing concern that currently costs the average business some $400,000 per year.[2] Device manufacturers must cost-effectively build baseline security into low-cost or low-margin devices.

For more information, see [The seven properties of highly secure devices](#).

Azure Sphere provides a hardware and software device platform for the creation of secured, internet-connected devices equipped with Azure-certified MCUs manufactured and certified by Azure partners. In addition, software development kits (SDKs) enable partners to build more secure devices, including those not based on Azure Sphere. Built explicitly to enable any device to connect to it, the Azure IoT environment enables ecosystem members to design and build devices according to their specific needs and their responses to individual risks.

IoT Hub Device SDKs enable OEMs and ODMs to build apps that run on IoT devices and send telemetry to and otherwise communicate with the IoT hub. The SDKs also streamline the ability to take advantage of emerging hardware capabilities. These include trusted platform modules (TPMs), which are dedicated cryptographic co-processors, and the Device Identifier Composition Engine (DICE), which provides hardware-based cryptographic device identity, attestation, and data encryption.

Azure Sphere MCUs provide a sophisticated hardware-based root of trust for securely deploying device-specific software and updates and gathering system health and error-reporting data for troubleshooting and analysis. The same framework also supports end-customer interaction with provider networks, across devices that range from home appliances and customer electronics to vehicles, industrial equipment, and critical infrastructure.

At the ecosystem level, Microsoft fosters partnerships with hardware manufacturers to enable secure models such as embedding keys and other cryptographic information in silicon. All software elements that run on the device, other than customer-provided applications, are provided, signed, and maintained by Microsoft.

The Azure Sphere security model draws on three main elements:

Secured, connected Azure Sphere-certified MCUs. Azure Sphere specifies a silicon architecture and certification requirements, as well as the integrated Pluton security subsystem, which is implemented in silicon.

Purpose-built Azure Sphere operating system. This custom lightweight Linux-based operating system is optimized for security and built specifically to run on Azure Sphere-certified MCUs in IoT implementations.

Cloud-based Azure Sphere Security Service. This service provides certificate-based authentication, software updating, failure reporting, and remote attestation.

For additional information, see the Azure Sphere Documentation and Understand and use Azure IoT Hub SDKs.

3.1.2 Enterprise-class operating systems, SDKs, and operating models

At the low end, IoT devices may do little more than pass along discrete data; at the high end, systems might perform demanding workloads such as image identification and transcoding against multiple live data streams. Many OSs are likely to be involved. The Azure IoT environment enables providers to bring solutions to market rapidly with a coherent security model across operating systems—including Linux, Azure Sphere, Azure RTOS, and Windows.

Endpoints running various flavors of Linux benefit from Azure IoT Device SDKs supplied by Microsoft that streamline the development of secure device-level applications, as well as Azure Security Center for IoT agents that support visibility and data collection across endpoints. In the context of edge computing, the OpenEnclave SDK secures workloads within trusted execution environments—also known as enclaves—which dramatically simplify the development of trusted applications. These components are open source in multiple languages, which gives customers visibility into the code and the ability to analyze its security.

Azure RTOS provides a real-time system environment for embedded applications, highly optimized for size and performance. In addition, it carries an extensive range of safety and security certifications, increasing its suitability for regulated and critical applications.

Windows for IoT adapts the Windows OS to IoT operating models, with favorable licensing and distribution arrangements, bringing the full Windows hardware and software ecosystem to bear on fixed-purpose devices for use in industrial automation, digital signage, and kiosks, for example.

The Windows for IoT family of operating systems protects data during execution, at rest, and in motion:

Protection during execution. Windows for IoT guards against unauthorized access while data is in use by protecting the device during startup and restricting execution to known and trusted code. Secure enclaves—available across all OSs—provide isolated execution environments for further protection.

Protection at rest. Data is protected at the point of storage using full volume encryption based on BitLocker, augmented with cryptographic co-processing by the TPM.

Protection in motion. As with other OSs, Windows for IoT data is protected while being transported around the environment using transport level security (TLS) connections augmented by security tokens and/or on-device X.509 certificates.

For additional information, see the Windows for IoT documentation, Understand and use Azure IoT Hub SDKs, Azure RTOS, and Introducing Azure Security Center for IoT.

3.2 Connection and edge security: Providing secure connectivity and integration

The connections between the highly diverse and distributed devices in IoT environments require an assumed-breach mentality, because any connection can be compromised, possibly without immediate detection. Therefore, best practices call for connections to be encrypted using TLS, with identity authenticated using X.509 certificates.

3.2.1 Data and analytics protection at the edge

Moving analytics and custom business logic to the edge provides a range of advantages. Rather than passing the full data set generated at the edge to the cloud for processing, edge implementations perform those functions at or near the edge. That approach supports offline operations and reduces bandwidth requirements to the cloud service, particularly when the vast majority of data is inconsequential, such as a surveillance camera that may collect hours of video where nothing of note happens.

In such scenarios, running anomaly detection based on machine learning on captured data at the edge allows for intelligent response by discarding data, storing it locally, or sending digests and insights to the cloud. Likewise, edge processing is vital to real-time or near-real-time scenarios such as industrial IoT, where control systems cannot tolerate the transport latency of data passed back and forth to the cloud.

Azure IoT Edge, a fully managed service, supports deployment of edge implementations, backed by digital certificates of cloud workloads such as Azure services, third-party services, or your own business logic to your devices using standard containers. Processing is handled at the edge, with monitoring performed from the cloud.

Placed between endpoints and the rest of the IoT infrastructure, edge gateways powered by Azure IoT Edge provide an additional layer of in-depth security. In this context, the gateway acts as a proxy for the endpoints that provides traffic control and abstraction, shielding the IoT endpoints from direct contact with the broader network. Those benefits are broadly useful to all types of endpoint devices, particularly those that may not be manufactured to high security standards.

For additional information, see the Azure IoT Edge documentation and Set up X.509 security in your Azure IoT Hub.

3.2.2 Streamlined connectivity development for secure IoT solutions

Scalable IoT solutions depend on reliable and secure bidirectional communication between millions of IoT devices and edge gateways, to and from cloud applications. Azure IoT Hub is a PaaS that provides the message interchange for cloud integration patterns, such as device-to-cloud telemetry and cloud-based device management.

The Azure IoT Hub Device Provisioning Service enhances scalability with automated just-in-time provisioning that doesn't require human intervention. It first registers the device to establish its connection to the IoT solution then configures it according to the specific requirements of the solution it is registered to. DPS supports fully featured provisioning, including capabilities such as secure attestation, allocation policies to control assignment to IoT hubs with specific criteria, monitoring and diagnostics, and encryption for data at rest.

The open source Azure IoT SDKs accelerate the process of connecting devices to the IoT hub while also increasing overall code quality to enhance security of the underlying processes. Programming language support includes C, C#, Java, Node.js, and Python. Microsoft conducts continual, end-to-end testing to certify operation on platforms that include Linux, Windows, MBED, Arduino, .NET, and Intel Edison. Certification of hardware and software technologies together benefits the environment's overall security posture. The SDKs enable secure authentication mechanisms using SAS tokens and X.509 certificates, as well as hardware root of trust in IoT devices.

For additional information, see Understand the Azure IoT SDKs, What is Azure IoT Hub?, and Provisioning devices with Azure IoT Hub DPS.

3.3 Cloud security: Detecting and responding to threats in the cloud

The Azure cloud is hardened from the ground up and built for security and scale, enabling ease of use while also helping ensure protection against threats. Customers extend that hardening further using Azure Security Center and implement alert aggregation as well as threat analysis and response using Azure Sentinel.

Azure capabilities that complement these tools include:

Azure Key Vault, a mechanism for safeguarding secrets used by cloud applications and services, such as API keys, passwords, and certificates.

Azure Key Vault ▸

Azure Active Directory, a cloud-based identity and access-management service that supports capabilities such as single sign-on and multifactor authentication.

Azure Active Directory ▸

3.3.1 Hybrid cloud workload threat protection

Security tools must be capable of detection and analysis of threats across devices and cloud services. Similarly, security teams must be enabled to detect, prevent, and remediate attacks at every point in the IoT environment, from simple sensors and actuators to edge computers and gateways.

Azure Security Center for IoT unifies security management and threat protection across the IoT infrastructure. It provides insights about potential threats anywhere in the environment from the device to the cloud, helps prioritize the order of response to open issues, and provides remediation steps. Microsoft distills more than 6 trillion security signals per day into the Microsoft Intelligent Security Graph, one of several threat intelligence feeds consumed by Azure Secure Center for IoT to power its threat-protection function.

Agentless deployments of Azure Security Center for IoT provide low-touch setup for advanced analytics on device logs. Device agents can be installed for additional signals provided as they collect, aggregate, and analyze raw security events directly from the device. Azure Security Center for IoT, available for Azure RTOS, generates recommendations and alerts and delivers them to the customer's dedicated workspace as the basis for investigating suspicious events.

A unified view of security across the IoT environment enables security teams to hunt for threats across the environment, seeking out potential vulnerabilities such as unused open ports, unencrypted datastores, and deviations from internal security standards or established best practices. These mechanisms continually monitor the environment for potential security issues that could range from an emerging vulnerability to a certificate needing renewal. Adaptive threat-detection algorithms powered by threat intelligence and machine learning respond to malicious activity signals.

For additional information, see the Azure Security Center for IoT documentation.

3.3.2 Aggregation, analysis, and response

Security teams are inundated with massive volumes of alerts as their resources are stretched by maintenance and other routine tasks. Traditional Security Information and Event Management (SIEM) products may not adequately focus on specific threats within noisy, cloud-scale alert data. Many organizations enhance those capabilities using security orchestration automated response (SOAR) tools to enhance gathering and prioritizing data from multiple platforms.

Azure Sentinel combines SIEM and SOAR functionality to provide cloud-native, scalable visibility and insight across the security landscape. The solution collects alert data, applies threat intelligence and machine-learning-powered analytics to reveal threats, and provides one-click or automated response to specific alerts. It also provides tools based on the MITRE ATTACK framework for proactive threat hunting.

Azure Security Center for IoT offers an Azure Sentinel connector that provides onboarding of IoT data workloads into Sentinel from Azure IoT Hub-managed deployments.

A vibrant community that includes Microsoft engineers continually updates content workbooks, playbooks, and query plans for threat hunting using Azure Sentinel. Using these resources, security teams can use Azure Sentinel as a single solution for data collection, threat detection, incident investigation, and rapid response.

Implementing cloud-native SIEM and SOAR functionality based on Azure Sentinel provides the following capabilities:

Collect security data at cloud scale. The data reach of Azure Sentinel extends across users, devices, applications, and infrastructure with elastic storage volume and query requirement capacity, for unlimited scale.

Detect threats. Azure Sentinel applies analytics to incoming machine data and threat intelligence, including Microsoft Intelligent Security Graph to detect novel threats while also minimizing false positives.

Investigate threats and incidents. Machine learning algorithms sift through log data and other signals to detect patterns and anomalies at machine speed, to support threat-hunting operations at scale.

Respond automatically to incidents. Azure Sentinel helps simplify security orchestration and automate common tasks with prescribed procedures based on security playbooks.

For additional information, see the Azure Sentinel documentation and the Azure Sentinel connector for Azure Security Center for IoT.

4 Conclusion

IoT contributes significantly to digital transformation, requiring a reimagining of enterprises' security. In particular, tools and approaches, including devices, the network edge, data connections, and cloud resources, must work end to end.

Microsoft crystallizes decades of security leadership to operationalize IoT security across all OSs through tools and best practices. As organizations work to adopt and mature their IoT infrastructures, they can use these measures to assess their security needs, manage their current state, and execute a structured approach to continuously improve their security postures.

Learn more about building secure IoT deployments with Azure IoT security at azure.microsoft.com/en-us/overview/iot/security/.

[1] Base: 262 global decision-makers of IoT planning and deployments. Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, June 2019.

[2] Accenture Security. Ninth Annual Cost of Cybercrime Study. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.