Microsoft Security

Issue 3

CISO Insider

Welcome to the third issue!

Explore

The cloud is secure; but are you managing your cloud environment securely?

A comprehensive security posture starts with visibility and ends with prioritized risk management.

Lean on Zero Trust and hygiene to tame the wildly diverse, hyper-networked environment of IoT & OT.

Letter from Rob

Welcome to our third issue in the CISO Insider **series.** I'm Rob Lefferts and I lead the Microsoft Defender and Sentinel engineering teams. We launched this series about a year ago to share insights from our discussions with some of your peers as well as from our own research and experience working on the frontlines of cybersecurity.

Our first two issues considered escalating threats such as ransomware and how security leaders are using automation and upskilling opportunities to help respond effectively to these threats amid an ongoing talent shortage. With CISOs facing even more pressure to operate efficiently in today's economic uncertainty, many are looking to optimize using cloud-based solutions and integrated managed security services. In this issue, we look at emerging security priorities as organizations shift to an increasingly cloud-centric model, bringing along everything in their digital estate from on-premises systems to IoT devices.

Executive summary

The public cloud offers the win-win-win of strong foundational security plus cost efficiency plus scalable computing, making it a key resource in a time of tightening budgets. But with this triple play comes a need to 'mind the gaps' that arise in the nexus between the public cloud and private clouds and on-premises systems. We look at what security leaders are doing to manage security in the liminal spaces between networked devices, endpoints, apps, clouds, and managed services. Finally, we look at two technologies that represent the apex of this security challenge, IoT and OT. The convergence of these two polarized technologies—one nascent and the other legacy, both introduced to the network without adequate built-in security—creates a porous edge vulnerable to attack.

Topics

Issue 3 looks at these three cloud-centric security priorities:

01 / Cloud security strategy

The cloud is secure; but are you managing your cloud environment securely?

Cloud adoption has accelerated as organizations seek new efficiencies in response to both economic constraints and a talent shortage. CISOs trust the public cloud services for their foundational security, but the cloud is only as secure as the customer's ability to manage the interface between the public cloud and private infrastructure. We look at how security leaders are closing the gap with a strong cloud security strategy—for example, by securing their cloud apps and workloads with tools like cloud posture management and the cloud-native application protection platform (CNAPP).

02 / Comprehensive posture management

A comprehensive security posture starts with visibility and ends with prioritized risk management.

With accelerated cloud adoption comes a proliferation of services, endpoints, apps, and devices. In addition to a strategy for managing the critical cloud connection points, CISOs are recognizing a need for greater visibility and coordination across their expanding digital footprint—a need for comprehensive posture management. We look at how security leaders are expanding their approach from preventing attacks (still the best defense, as long as it works) to managing risk through comprehensive posture management tools that help with inventorying assets and modeling business risk—and of course, identity and access control.

03 / IoT/OT

Lean on Zero Trust and hygiene to tame the wildly diverse, hyper-networked environment of IoT & OT.

The exponential growth in connected IoT and OT devices continues to present security challenges—especially given the difficulty of reconciling technologies that are a blend of cloud-native, third-party tools and legacy equipment retrofitted for networking. The number of global IoT devices is projected to reach 41.6 billion by 2025, creating an expanded attack surface area for attackers who use such devices as entry points for cyber-attacks. These devices tend to be targeted as points of vulnerability in a network. They may have been introduced ad hoc and connected to the IT network without clear direction from the security team; developed without foundational security by a third party; or managed inadequately by the security team due to challenges like proprietary protocols and availability requirements (OT). Learn how many IT leaders are now evolving their IoT/OT security strategy to navigate this gap-ridden edge.

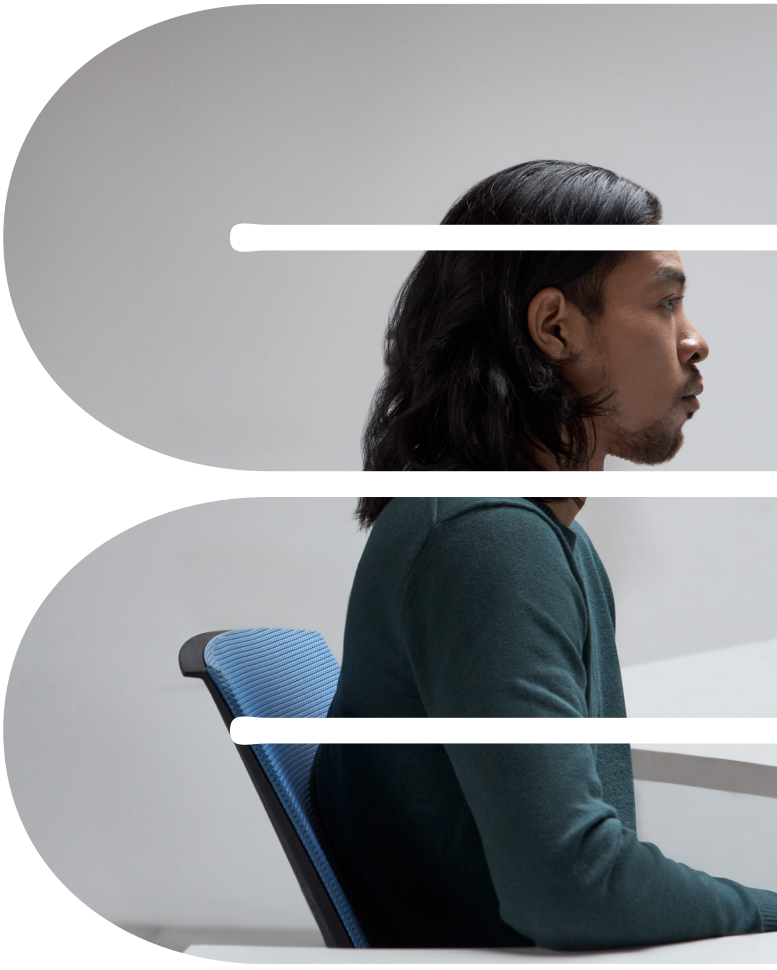
Cloud security strategy

At a time of talent shortages and tightening budgets, the cloud offers many benefits—cost efficiency, infinitely scalable resources, cutting-edge tooling, and more reliable data protection than most security leaders feel they can achieve on-premises. While CISOs used to see cloud resources as a tradeoff between greater risk exposure and greater cost efficiency, most of the security leaders we speak to today have embraced the cloud as the new normal. They trust in the strong foundational security of cloud technology: "I expect that cloud service providers have their house in order in terms of their identity and access management, their system security, and their physical security," says one CISO.

But as most security leaders recognize, cloud foundational security does not guarantee your data is secure—the protection of your data in the cloud greatly depends on how cloud services are implemented alongside on-premises systems and homegrown technology. Risk arises in the gaps between the cloud and the traditional organizational boundary, the policies, and technologies used to secure the cloud. **Misconfigurations** occur, often leaving organizations exposed and dependent on security teams to identify and close the gaps.

The cloud is secure; but are you managing your cloud environment securely?

> *"A high number of breaches are because of misconfiguration, someone inadvertently misconfiguring something, or changing something that allows the data to be leaked."*
>
> – Utilities - Water, 1,390 employees



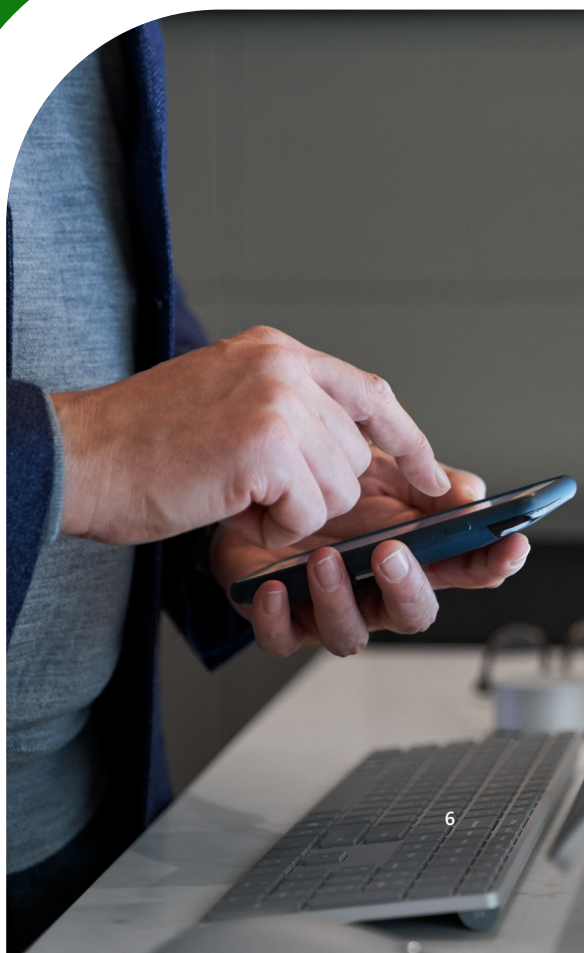
Cloud security strategy

By 2023, 75 percent of cloud security breaches will be caused by inadequate management of identities, access, and privileges, up from 50 percent in 2020 (Misconfiguration and vulnerabilities biggest risks in cloud security: Report | CSO Online). The challenge exists not in the security of the cloud itself, but in the policies and controls used to secure access. As a financial services CISO puts it, "Cloud security is very good if it is deployed correctly. The cloud itself and their components are secure. But you get into the configuration: am I writing my code properly? Am I setting up my connectors across the enterprise correctly?" Another security leader sums up the challenge: "The misconfiguration of those cloud services is what opens up the services to threat actors." As more security leaders become aware of the risks of cloud misconfiguration, the conversation around cloud security has shifted from "Is the cloud secure?" to "Am I using the cloud securely?"

What does it mean to use the cloud securely? Many of the leaders I talk to approach cloud security strategy from the ground up, tackling the human errors that expose the organization to risk such as identity breaches and misconfigurations. This is in line with our recommendations as well—**securing identities and adaptively managing their access are absolutely fundamental to any cloud security strategy.**

The cloud is secure; but are you managing your cloud environment securely?

For anyone still on the fence, maybe this will help: McAfee reported that 70 percent of exposed records—5.4 billion—were compromised due to misconfigured services and portals. Managing access through identity controls and implementing strong security hygiene can go a long way to closing the gaps.



Cloud security strategy

A robust cloud security strategy involves these best practices:

1. **Implement an end-to-end cloud-native application protection platform (CNAPP) strategy:** Managing security with fragmented tools can cause blind spots in protection and higher costs. Having an all-in-one platform that enables you to embed security from code to cloud is critical to reduce overall cloud attack surface and automate threat protection. The CNAPP strategy involves the following best practices:

   A. Prioritize security from the start in DevOps. Security can fall to the wayside in the rush to develop cloud apps. Developers have an incentive to solve a business problem quickly and may lack cloud security skills. As a result, apps can proliferate without the appropriate data authorization rules. APIs have become a prime target for hackers, as organizations often cannot keep track of them given the rate of cloud app development. Gartner identifies "API sprawl" as a growing issue, predicting that by 2025, fewer than half of enterprise APIs will be managed (Gartner). It is therefore critical to implement a DevSecOps strategy as quickly as possible.

   B. Strengthen cloud security posture and fix misconfigurations. Misconfigurations are the most common cause for cloud breaches—check out Cloud Security Alliance's top most common security group-setting misconfigurations. While leaving storage resources open to the public is the most common fear we hear, CISOs also cite other areas of neglect: disabled monitoring and logging, excessive permissions, unprotected backups, etc. Encryption is an important hedge against mismanagement—and critical to reducing the risk of ransomware. Cloud security posture management tools offer another line of defense by monitoring cloud resources for exposures and misconfigurations before a breach happens, so you can reduce attack surface proactively.

   C. Automate detection, response, and analysis of incidents. Identifying and fixing misconfigurations is great, but we also need to ensure we have the tools and processes in place to detect attacks that make it past the defense. This is where threat detection and response management tools can help.

Best practices for a strong cloud security strategy

   D. Get access management right. Multifactor authentication, single sign-on, role-based access control, permission management, and certifications help manage the two biggest risks to cloud security: the user and misconfigured digital properties. Least access is a cloud infrastructure entitlement management (CIEM) best practice. Some leaders rely on an identity access management or entitlement management solution to put active security controls in place. One financial services leader leans on the cloud access security broker (CASB) as a "key backstop" to manage the organization's SaaS services and to maintain control of their users and data. The CASB acts as an intermediary between users and cloud apps, providing visibility and enforcing governance actions through policies. backstop" to manage their SaaS services and maintain control of their users and data. The CASB acts as an intermediary between users and cloud apps, providing visibility and enforcing governance actions through policies.

A cloud-native application protection platform like that offered in Microsoft Defender for Cloud not only offers visibility across multi-cloud resources, but also provides protection at all layers of the environment while monitoring for threats and correlating alerts into incidents that integrate with your SIEM. This streamlines investigations and helps your SOC teams stay ahead of cross-platform alerts.

An ounce of prevention—closing identity and misconfiguration gaps—combined with robust tools for attack response go a long way to securing the whole cloud environment, from the corporate network to cloud services.

Comprehensive posture management

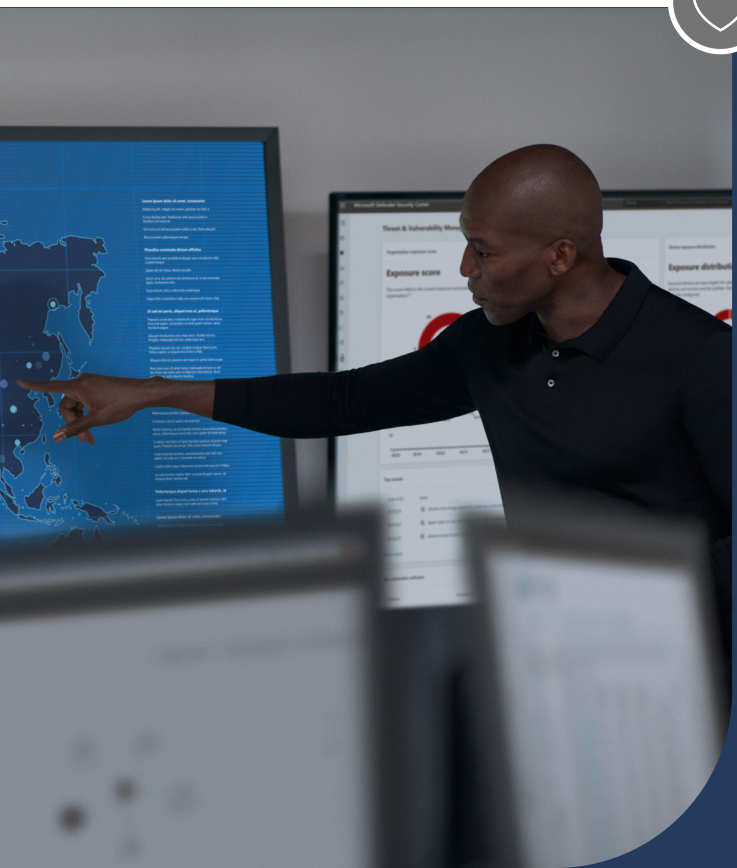
The shift to cloud-centric IT not only exposes the organization to implementation gaps, but also to a proliferating array of networked assets—devices, apps, endpoints—as well as to exposed cloud workloads. Security leaders are managing their posture in this perimeter-less environment with technologies that deliver visibility and prioritized response. These tools help organizations map an asset inventory that covers the entire attack surface, spanning managed and unmanaged devices both within and outside of the organization's network. Using these resources, CISOs are able to assess the security posture of each asset as well as its role in the business to develop a prioritized risk model.

In our conversations with security leaders, we're seeing an evolution from perimeter-based security toward a security posture-based approach that embraces a borderless ecosystem.

A comprehensive security posture starts with visibility and ends with prioritized risk management.

As one CISO puts it, "To me, the posture goes down to the identity.... We don't look at it just as the old traditional posture where the perimeter is but move that all the way down to the endpoint." (Utilities-Water, 1,390 employees). "Identity has become the new perimeter," comments a FinTech CISO, asking: "What does identity mean in this new model where there is no outside and inside?" (FinTech, 15,000 employees).

Given this porous environment, CISOs understand the urgency of comprehensive posture management—but many question whether they have the resources and digital maturity to put this vision into practice. Fortunately, through a combination of industry-proven frameworks (updated for today's needs) and security innovation, comprehensive posture management is within reach for most organizations.



"Get tooling in your cyber infrastructure that allows you to do an asset inventory. Second, look at which one of those are critical, which have the biggest risk to the organization and understand what the potential vulnerabilities are of these devices, and decide whether this is acceptable—do I need to patch or isolate it."

– Ken Malcolmson,
Executive Security Advisor, Microsoft

Comprehensive posture management

Here are some best practices and tools security leaders are using to manage their posture in an open-ended, cloud-centric environment:

1. Achieve comprehensive visibility with an asset inventory.

Visibility is the first step in holistic posture management. CISOs are asking, 'Do we even know all we have out there as a first step? Do we even have visibility before we can get to management?' A risk asset inventory includes IT assets like networks and applications, databases, servers, cloud properties, IoT properties, as well as the data and IP assets stored on this digital infrastructure. Most platforms, like Microsoft 365 or Azure, include built-in asset inventory tools that can help you get started.

2. Assess vulnerability and analyze risk.

Once an organization has a comprehensive asset inventory, it's possible to analyze risk with respect to both internal vulnerabilities and external threats. This step relies heavily on context and is unique to each organization—a reliable risk assessment depends on a strong partnership among the security, IT, and data teams. This cross-functional team leverages automated risk scoring and prioritization tools in their analysis—for example, the risk prioritization tools integrated into Azure Active Directory, Microsoft 365 Defender, and Microsoft 365. Automated risk scoring and prioritization technologies may also incorporate expert guidance for remediating the gaps as well as contextual information for effective threat response.

Best practices for comprehensive security posture management

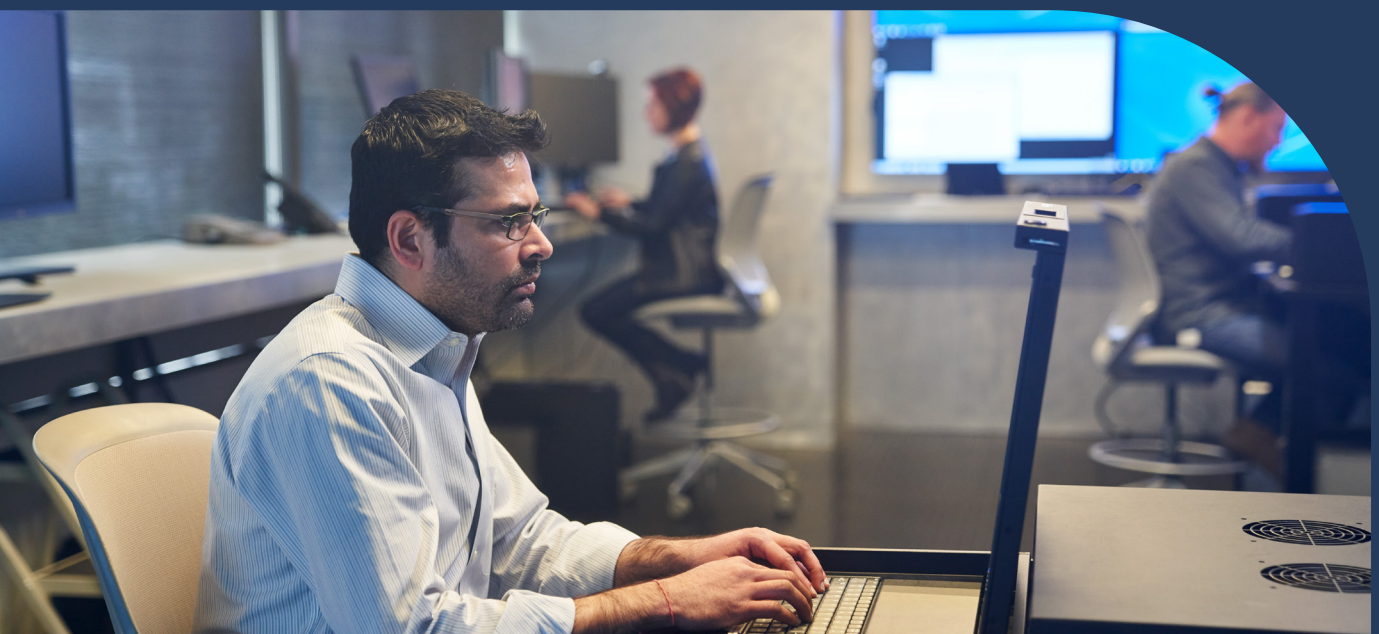
3. Prioritize risk and security needs with business risk modeling.

With a clear understanding of the risk landscape, technical teams can work with business leaders to prioritize security interventions with respect to business needs. Consider the role of each asset, its value to business, and the risk to the business if it is compromised, asking questions like, 'How sensitive is this information and what would be the impact to the business of its exposure?' or 'How mission critical are these systems—what would be the impact of downtime to the business?' Microsoft offers tools to support a comprehensive identification and prioritization of vulnerabilities according to business risk modeling, including Microsoft Secure Score, Microsoft Compliance Score, Azure Secure Score, Microsoft Defender External Attack Surface Management, and Microsoft Defender Vulnerability Management.

4. Create a posture management strategy.

An asset inventory, risk analysis, and business risk model form the basis for comprehensive posture management. This visibility and insight help the security team determine how best to allocate resources, what hardening measures need to be applied, and how to optimize the tradeoff between risk and useability for each segment of the network.

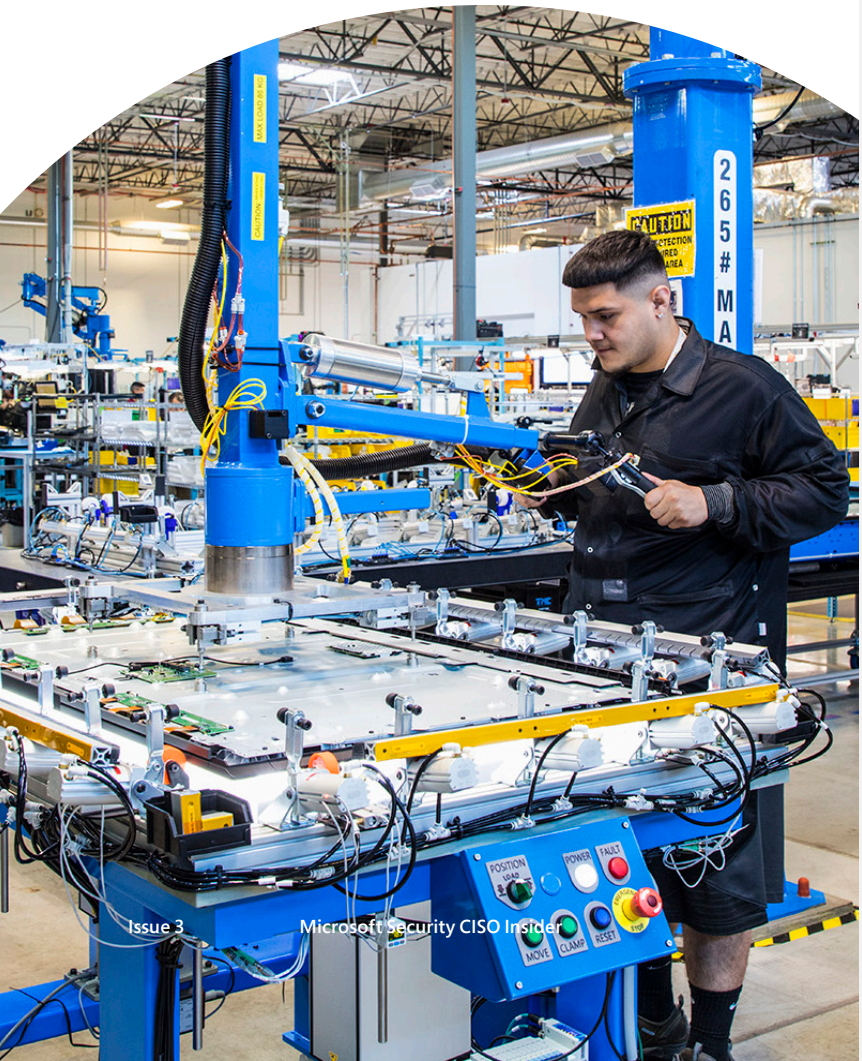
Posture management solutions offer the visibility and vulnerability analysis to help organizations understand where to focus their posture improvement efforts. With this insight, they can identify and prioritize important areas in their attack surface.



IoT and OT security

Lean on Zero Trust and hygiene to tame the wildly diverse, hyper-networked environment of IoT and OT

The two challenges we've discussed—the cloud implementation gap and the proliferation of cloud-connected devices—are creating a perfect storm of risk in IoT and OT device environments. In addition to the inherent risk of an expanded attack surface area introduced by IoT and OT devices, security leaders tell me they're trying to rationalize the convergence of nascent IoT and legacy OT strategies. IoT may be cloud native, but these devices frequently prioritize business expediency over foundational security; OT tends to be vendor-managed legacy equipment developed without modern security and introduced ad hoc onto the organization's IT network.



Here's a closer look at the state of IoT-OT risk today:

IoT and OT devices are helping organizations modernize workspaces, become more data driven, and ease demands on staff through strategic shifts like remote management and automation. The International Data Corporation (IDC) estimates there will be 41.6 billion connected IoT devices by 2025, a growth rate exceeding that of traditional IT devices.

But with this opportunity comes significant risk. Our December 2022 Cyber Signals report, The Convergence of IT and Operational Technology, looked at the risks to critical infrastructure posed by these technologies.

Key findings include:

- 75% of the most common industrial controllers in customer OT networks have unpatched, high-severity vulnerabilities
- From 2020 to 2022, there was a 78% increase in disclosures of high-severity vulnerabilities in industrial control equipment produced by popular vendors
- Many devices publicly visible on the internet are running unsupported software. For example, the outdated software Boa is still widely used in IoT devices and software development kits (SDKs).

IoT and OT security

Lean on Zero Trust and hygiene to tame the wildly diverse, hyper-networked environment of IoT and OT

IoT devices often represent the weakest link in the digital estate. Because they are not managed, updated, or patched the same way that traditional IT devices are, they can serve as a convenient gateway for attackers seeking to infiltrate the IT network. Once accessed, IoT devices are vulnerable to remote code executions. An attacker can gain control and exploit vulnerabilities to implant botnets or malware in an IoT device. At that point, the device can serve as an open door to the entire network.

> ***"Almost every attack we've seen in the last year started from initial access to an IT network that was leveraged into the OT environment."***
>
> – David Atch, Microsoft Threat Intelligence, Head of IoT/OT Security Research

Operational Technology devices pose an even more sinister risk, with many being critical to the operation of the organization. Historically offline or physically isolated from corporate IT network, OT networks are increasingly blended with IT and IoT systems. Our November 2021 study conducted with Ponemon Institute, The State of IoT/OT Cybersecurity in the Enterprise, found that over half of OT networks are now connected to corporate IT (business) networks. A similar proportion of companies—56 percent—have internet-connected devices on their OT network for scenarios like remote access.

OT connectivity exposes organizations to the risk of major disruption and downtime in the event of an attack. OT is often core to the business, providing attackers with an enticing target they can exploit to cause significant damage. The devices themselves can be easy targets, as they often involve brownfield or legacy equipment that isn't secure by design, pre-dates modern security practices, and may have proprietary protocols that elude visibility by standard IT monitoring tools. Attackers tend to exploit these technologies by discovering exposed internet-facing systems, gaining access through employee login credentials, or exploiting the access granted to third-party suppliers and contractors. Unmonitored ICS protocols are one common entry point for OT-specific attacks (Microsoft Digital Defense Report 2022).

IoT and OT security

To tackle the unique challenge of managing IoT and OT security across this blended continuum of different devices connected in different ways to the IT network, security leaders are following these best practices:

1. Achieve comprehensive device visibility.

Understanding all the assets you have in a network, how everything is interconnected, and the business risk and exposure involved at each connection point is a critical foundation for effective IoT/OT management. An IoT- and OT-aware network detection and response (NDR) solution and a SIEM like Microsoft Sentinel can also help give you deeper visibility into IoT/OT devices on your network and monitor them for anomalous behaviors such as communication with unfamiliar hosts. (For more information on managing exposed ICS protocols in OT, see "The Unique Security Risk of IOT Devices," Microsoft Security).

2. Segment networks and employ Zero Trust principles.

Wherever possible, segment networks to inhibit lateral movement in the event of an attack. IoT devices and OT networks should be air-gapped or isolated from the corporate IT network through firewalls. That said, it's also important to assume your OT and IT are converged and build Zero Trust protocols across the attack surface. Increasingly, network segmentation isn't feasible. For regulated organizations like healthcare, utilities, and manufacturing, for example, OT-IT connectivity is core to the business function—take for example, mammogram machines or smart MRIs connecting to electronic health records (EHR) systems; smart manufacturing lines or water purification requiring remote monitoring. In these cases, Zero Trust is critical.

Best practices for securing IoT and OT environments

3. Employ IoT/OT security management hygiene.

Security teams can close the gaps through some basic hygiene practices like:

- Eliminating unnecessary internet connections and open ports, restricting or denying remote access, and using VPN services
- Managing device security by applying patches and changing default passwords and ports
- Ensure ICS protocols are not directly exposed to the internet

For actionable guidance on how to achieve this level of insight and management, see "The Unique Risk of IoT/OT Devices," Microsoft Security Insider.

Actionable insights

- **Use an IoT/OT-aware network detection and response (NDR) solution and a security information and event management (SIEM)/security orchestration and response (SOAR) solution to gain deeper visibility into IoT/OT devices on your network, monitor devices for anomalous or unauthorized behaviors, such as communication with unfamiliar hosts**
- **Protect engineering stations by monitoring with endpoint detection and response (EDR) solutions**
- **Reduce the attack surface by eliminating unnecessary internet connections and open ports, restricting remote access by blocking ports, denying remote access, and using VPN services**
- **Ensure ICS protocols are not exposed directly to the internet**
- **Segment networks to limit an attacker's ability to move laterally and compromise assets after initial intrusion. IoT devices and OT networks should be isolated from corporate IT networks through firewalls**
- **Ensure devices are robust by applying patches, changing default passwords and ports**
- **Assume your OT and IT are converged and build Zero Trust protocols into your attack surface**
- **Ensure organizational alignment between OT and IT by promoting greater visibility and team integration**
- **Always follow best IoT/OT security practices based on fundamental threat intelligence**

As security leaders seize the opportunity to streamline their digital estate amid escalating threats and pressure to do more with fewer resources, the cloud is emerging as the foundation of the modern security strategy. As we have seen, the benefits of a cloud-centric approach greatly outweigh the risks—especially for organizations that employ best practices to manage their cloud environments through a robust cloud security strategy, comprehensive posture management, and specific tactics to close gaps at the IoT/OT edge.

Look to our next issue for more security analysis and insights. Thanks for reading the CISO Insider!

Learn more

Explore the latest cybersecurity insights and updates at Microsoft Security Insider.
www.microsoft.com/security-insider

All cited Microsoft research uses independent research firms to contact security professionals for both quantitative and qualitative studies, ensuring privacy protections and analytical rigor. Quotes and findings included in this document, unless specified otherwise, are a result of Microsoft research studies.