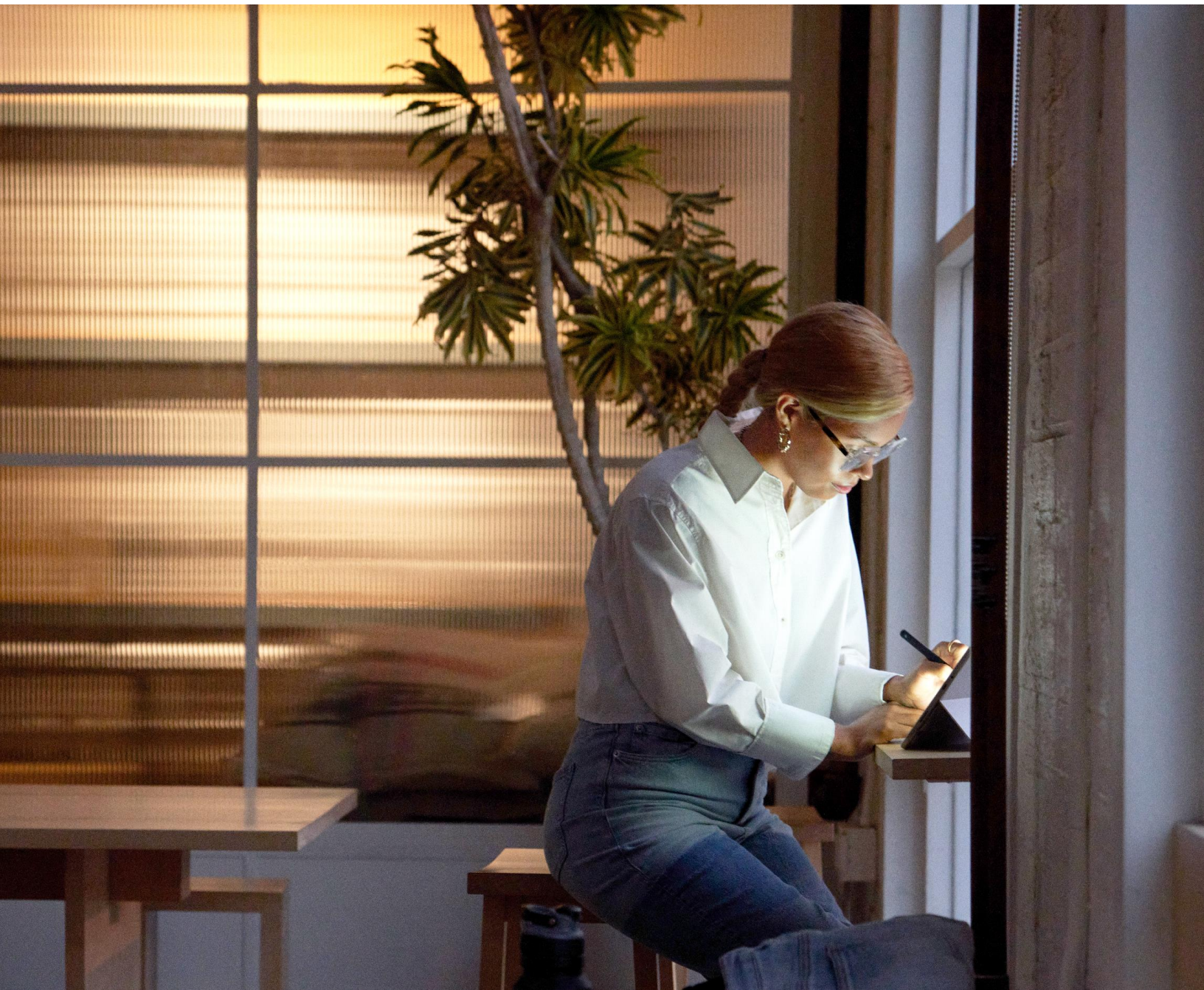
Microsoft Surface

Choose wisely: How device choice can make or break your cyber resilience plan



What does it mean to be cyber resilient?

Almost every organization today, from neighborhood coffee shops to global enterprises, depends on data, analytics, automation, and digital technologies. This reliance, coupled with a remote workforce, has increased the risk and cost of cyberattacks on a scale of impact ranging from local to global.

As these scenarios multiply in frequency and sophistication, successful security leaders now need to look beyond prevention. Cyber resilience is the ability of an organization to quickly respond and effectively recover from a negative event, minimizing the fiscal blows of security vulnerabilities. Resilience can mean the difference between losing ground or leaping forward in their recovery.

5x increase in cyberattacks against remotely managed devices between May 2021 and May 2022.[1]

$4.24 M USD was the global average cost of a data breach in 2022.[1]

[1]Microsoft, Microsoft Digital Defense Report 2022, 2022.

(cont'd) What does it mean to be cyber resilient?

How is this possible? From large enterprises to medium, small, and very small businesses, there are key principles any company can adopt to gain resilience during a crisis. It requires taking a pragmatic view of cybersecurity that assumes breaches are inevitable. In other words, it means 'assuming compromise'.

Assuming compromise is a significant departure from the traditional security mindset. Previously, IT professionals believed they could construct a secure network with a fortified perimeter, confining all business operations to the network while tightly restricting end-user devices.

However, the traditional approach overlooks the demands of modern work environments, changing business models, new technologies, and evolving security threats. To cultivate resilience, organizations require Zero Trust, a collaborative partnership between business stakeholders, IT leaders, and security professionals, and the use of advanced technology designed to enhance protection.

By 2026

50%

of C-level executives will have performance requirements related to risk built into their employment contracts.[1]

By 2025

60%

of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements.[1]

[1]Gartner Press Release, "Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23," 21 June 2022. https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

Two steps to begin building cyber resiliency

01 Implement basic measures

The majority of cyberattacks can be stopped by implementing simple practices including eliminating antiquated applications, devices, and infrastructure. Automating highly manual processes, enabling multi-factor authentication (MFA), adopting Zero Trust principles, and using modern anti-malware are also advised.

Regularly applying firmware and software updates eliminates vulnerabilities on an on-going basis. Firmware attacks represent one of the most significant risks for organizations, potentially giving bad actors unrestricted and undetected access to your network through devices from laptops to printers, routers, and more.

A key first step in building cyber resilience is auditing user endpoints to identify those containing accessible firmware.

98% of attacks can be stopped by putting in place basic hygiene measures.[1]

45% of security professionals identify email and collaboration tools as the aspect of their organization most susceptible to attacks.[2]

[1]Microsoft, Microsoft Digital Defense Report 2022, 2022.
[2]Microsoft, Cyber Resilience, 2022.

Key components of cyber resiliency

Protect and defend

All good resilience strategies begin with protecting systems, applications, and data. Grant access only to authorized users needing customer, employee, and business data. Also analyze applications and endpoint devices for vulnerabilities that may exist anywhere from chip to cloud.

Detect and inspect

As cyberattacks become more frequent and sophisticated, it becomes increasingly important to run diagnostics on devices and software, continually monitoring for anomalies. Automation can be helpful in this area, triggering system responses to certain threats, and prioritizing those that should be escalated to a team member.

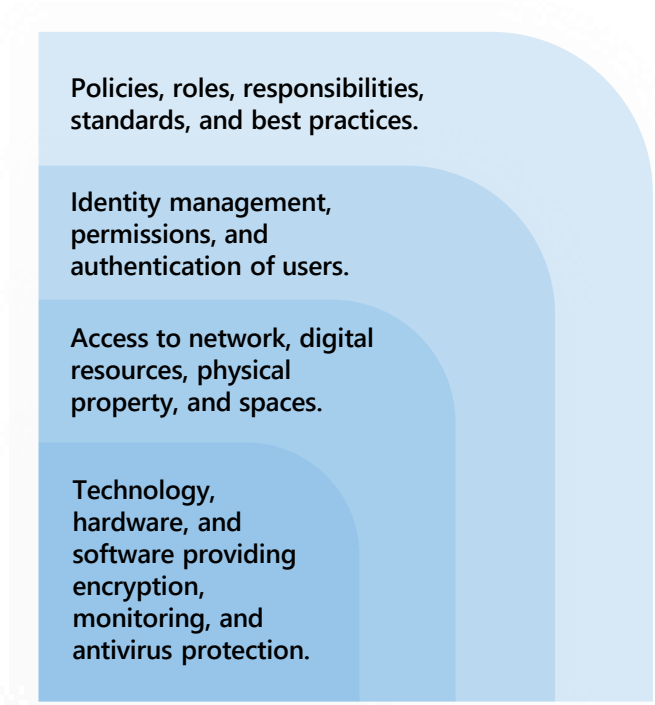
Recover

Attacks are inevitable. Accepting this reality opens the door to planning for minimal business disruption, and efficient recovery with devices designed for cyber resilience.

02 Invest in technology that withstands disruption

Security decision-makers (SDMs) are investing heavily in software security. Firewalls and data encryption, intrusion detection, and attack prevention are at the top of the list. However, neglecting to understand the vulnerability of hardware can undermine all efforts.

A typical security infrastructure is composed of several layers that work together to protect an organization's assets, data, and its operations.



Compromise at the hardware level through a physical device such as a laptop, tablet, smartphone, or IoT device flows up, compromising other layers to reach the data and networks they're intended to protect.

Partnering with technology decision-makers to choose the right device is foundational to your cyber resilience plan. Factors such as performance aligned with use, scalability, compatibility, reliability, and the security of the device itself, all come into play.

Key components of a cyber-resilient infrastructure

- Create a firmware protection plan and stay on top of firmware, UEFI, and operating system updates that can provide additional protection against emerging threats.
- Accelerate automation of manual tasks such as remote updates and device activation, leaving the IT workforce more time for high-touch activities.
- Activate a schedule to keep UEFI, firmware, and security updates current.
- Enable MFA for all end users and implement a conditional access strategy.
- Implement biometric scanning—such as Windows Hello for Business—to reduce reliance on codes, card scans, and passwords.
- Adopt devices considered to be Secured-core PCs or configure your devices to meet similar requirements.
- Reduce vulnerabilities in endpoint devices by turning off unused functionality such as Bluetooth or video cameras.

Choosing cyber resilient devices

- Research the best practices and standards for device security in your industry or sector.
- Assess your current device inventory and identify any gaps or risks in terms of functionality, age, version, or security.
- Compare different device options based on features, benefits, drawbacks, reviews, and ratings.
- Consult with experts or vendors who can provide guidance or recommendations on device selection.
- Test and evaluate the performance and security of your chosen devices before deploying them across your organization.
- Monitor and maintain your devices regularly to ensure they're functioning properly and securely.

Keep devices up-to-date

While your IT team can always test and ringfence, keeping devices up-to-date at the firmware level reduces the risk and allows IT teams to focus on resilience and growth rather than defense and repair.

Beyond firmware, attacks against remotely managed devices are on the rise. These devices include laptops, cameras, and smart conference room technology that may be exposed through open ports and can be exploited by hackers. A recent study found that 46% of IoT/OT attack types were from remote management devices.[1]

[1]Microsoft Security Insider, Unpatched and Exposed, The Unique Security Risk of IoT/OT Devices, 2022.

Choose a partner to help build a cyber resilience strategy

In a world of complex IT challenges, choosing the right IT partner can help protect businesses and prepare them to recover. A good IT partner recommends the most suitable hardware, software, and security solutions customized for the business, and reduces the need to juggle multiple vendors or solutions. A valuable IT partner has the knowledge and experience to help design and implement a comprehensive cyber resilience plan that can scale with the business. Ultimately, an IT partner should have their client's best interests in mind and work toward meeting their business goals.

With our partners, Microsoft designed Surface devices to minimize the risk of threats against firmware, operating system, and cloud applications. With Zero Trust built in from the ground up, this means security and IT decision-makers can feel confident investing resources in strategies and technologies that will prevent attacks in the future, rather than constantly defending against the onslaught of attacks aimed at them today.

Find a Microsoft partner: Authorized Microsoft Resellers – Surface for Business

How Microsoft Surface builds cyber resilience

Microsoft Surface devices are designed to facilitate basic security hygiene measures with every layer maintained by Microsoft, from the firmware to the operating system to the cloud. Surface devices, Windows 11, and Microsoft 365[1] help achieve organizational resilience with a Zero Trust approach to security and risk management that doesn't sacrifice innovation or productivity.

In designing Surface, we thought about all the ways that cyberattacks could compromise devices and users. Security is most effective when it's built into the design to address the most commonly vulnerable areas, and that's exactly what we did. As a result, Surface offers protection from chip to cloud. We designed Surface to provide peace of mind, knowing an integrated solution maintained by Microsoft protects your business. Let's dive deeper into how Microsoft Surface builds cyber resilience.

Companies that own Surface can experience up to 34% fewer security incidents, reducing time spent on security incident response.[2]

*Unique to Microsoft Surface.
**Customer Replaceable Units (CRUs) are components available for purchase through your Surface Commercial Authorized Device Reseller. Components can be replaced on-site by a skilled technician following Microsoft's Service Guide. Opening and/or repairing your device can present electric shock, fire and personal injury risks and other hazards. Use caution if undertaking do-it-yourself repairs. Device damage caused during repair will not be covered under Microsoft's Hardware Warranty or protection plans. Components will be available shortly after initial launch; timing of availability varies by component and market.
[1]Software license required for some features. Sold separately.
[2]A Business Value White Paper, commissioned by Microsoft September 2022 | Doc. #US49453722 IDC Research Study conducted from surveys and interviews between December 2021–February 2022. All respondents were IT decision-makers at large organizations (250-5000+ employees) representing organizations from the United States, Australia, India, Spain, France, United Kingdom, New Zealand, and Germany. Cost & Savings findings based on average cost and time estimates provided directly by respondents; actual costs and savings may vary based on your specific device mix and deployment. For the detailed study, click here.

Achieve cyber resilience from hardware to collaboration and the cloud

"Microsoft provides all of the services and defenses we need for ourselves and our customers on the same platform."

– NIP Group

Microsoft Surface can help solve the security gap by empowering security teams, line-of-business leaders, and workers. Designed to be secure, Surface devices combined with Windows 11 and Microsoft 365* deliver an integrated solution, with built-in layers of protection and remote device management that extend from hardware and firmware to the cloud.

Windows 11 firmly integrates hardware and software security features right out of the box, providing proactive protection and resilience against evolving threats.

*Software license required for some features. Sold separately.

"The secured PC is an attempt to establish 'the best environment in the world.' I feel that we successfully provided this environment by combining the latest technologies, including Microsoft 365, with our own technologies."

– NTT Communications Corporation

Built for security

Our security approach begins with hardware. Surface protects data through encryption as the device boots. A **Trusted Platform Module 2.0** (TPM 2.0) acts as a secure vault for storing passwords, PINs, and certificates, protecting hardware from tampering and restricting access to only authorized individuals. At every stage of the boot cycle, firmware code is inspected for authenticity to ensure the system doesn't execute any malicious code.

At startup, password-less, secure sign-in with **Windows Hello for Business** offers the highest level of biometric security with infrared camera sensors to enhance facial recognition. Biometric sign-in is the most difficult to replicate, ensuring only authorized users can access the device.

We design many Surface devices with removable SSDs[1] to provide an extra layer of protection for sensitive data stored on the device.

Microsoft is a recognized Leader in the 2022 Gartner® Magic Quadrant™ for Unified Endpoint Management Tools.[2]

Companies that use Surface experienced a 40% reduction in IT staff time related to ongoing maintenance.[3]

Designed for trust

Surface Management Portal is built into **Microsoft Intune*** providing a dedicated, centralized, cloud-based endpoint management solution. Surface Management Portal is designed to address the challenges of managing and configuring users, apps and devices at scale while Microsoft Intune* handles mobile application management (MAM) and mobile device management (MDM).

---

*Software license required for some features. Sold separately.
[1]Customer Replaceable Units (CRUs) are components available for purchase through your Surface Commercial Authorized Device Reseller. Components can be replaced on-site by a skilled technician following Microsoft's Service Guide. Opening and/or repairing your device can present electric shock, fire and personal injury risks and other hazards. Use caution if undertaking do-it-yourself repairs. Device damage caused during repair will not be covered under Microsoft's Hardware Warranty or protection plans. Components will be available shortly after initial launch; timing of availability varies by component and market.
[2]Gartner, Magic Quadrant for Unified Endpoint Management Tools, Tom Cipolla, Dan Wilson, et al., 1 August 2022. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
[3]A Business Value White Paper, commissioned by Microsoft September 2022 | Doc. #US49453722 IDC Research Study conducted from surveys and interviews between December 2021–February 2022. All respondents were IT decision-makers at large organizations (250-5000+ employees) representing organizations from the United States, Australia, India, Spain, France, United Kingdom, New Zealand, and Germany. Cost & Savings findings based on average cost and time estimates provided directly by respondents; actual costs and savings may vary based on your specific device mix and deployment. For the detailed study, click here.

Windows Update manages roll-out and update of firmware, software, and drivers. End-to-end protection ensures only approved content is installed.

The ability to manage device security remotely can mean huge time savings for your IT team, reducing the possibility of firmware or ransomware attacks, and remediating problems before they get too far.

Working alongside Microsoft Intune,* **Windows Autopilot** saves more time by streamlining secure remote deployment, preconfiguring new devices with the required security settings and policies.

"The sophistication of biometric authentication through Windows Hello facial recognition, as we have seen with Surface, is absolutely market-leading."

– Mashreq

Firmware that's locked down

Surface devices proactively block threats by eliminating a key external access point to firmware through the Unified Extensible Firmware Interface (UEFI). The Microsoft-built UEFI is accessible by Windows Update, reducing the risk of external access to the firmware.

The Microsoft UEFI together with the **Device Firmware Configuration Interface (DFCI)** allows for more granular control of firmware through Microsoft Intune.*

DFCI reduces the attack surface by disabling unnecessary hardware components and removes the dependency on the local UEFI (BIOS) password. DFCI provides the ability to lock down the boot options to prevent users from booting into another OS, and security updates running in the background provide ongoing, up-to-date protection against the latest threats.

34% fewer security incidents with Surface devices.[2]

30% less IT staff time required to deal with security incidents when using Surface devices.[2]

---

*Software license required for some features. Sold separately.
[1]Surface Go and Surface Go 2 use a third-party UEFI and do not support DFCI. For details on Microsoft protection for Surface Go and Go 2, visit https://www.microsoft.com/en-us/surface/business/surface-go-2.
[2]A Business Value White Paper, commissioned by Microsoft September 2022 | Doc. #US49453722 IDC Research Study conducted from surveys and interviews between December 2021–February 2022. All respondents were IT decision-makers at large organizations (250-5000+ employees) representing organizations from the United States, Australia, India, Spain, France, United Kingdom, New Zealand, and Germany. Cost & Savings findings based on average cost and time estimates provided directly by respondents; actual costs and savings may vary based on your specific device mix and deployment. For the detailed study, click here.

Powerful Windows 11 security enabled by default

Surface devices with Windows 11 include a new set of hardware security features enabled right out of the box. **Virtualization-based security (VBS)** and **Hypervisor-enforced Code Integrity (HVCI)**, also known as **memory integrity,** are designed to build a foundation even stronger and more resilient to attacks. VBS and HVCI work in tandem to provide better protection against common and sophisticated malware, performing sensitive security operations in an isolated environment. By checking code executions before they start, VBS and HVCI prevent malware from making its way to the system memory. If a threat gains access to system resources, the HVCI can limit and contain the malware's effects.

We ship Surface devices with Windows 11 from the factory with **security features enabled**. That helps security and business leaders normalize security-centric behaviors within your organization, satisfying the need for accountability across your teams.

Even before signing in with a variety of biometric options to avoid passwords and PINs, **Secure Boot helps** ensure firmware is as genuine as it was when it left the factory. Together, Secure Boot and Trusted Boot prevent malware and corrupted components from loading during startup.

After startup, **BitLocker** encryption helps render data inaccessible even on lost, stolen, or inappropriately decommissioned devices.

Robust cybersecurity means evolving from simply maintaining protection to being resilient against current and evolving threats. Cyber resilience is an organizational effort that demands accountability from everyone. Organizations need an integrated approach—with security built into every layer, from chip to cloud—to ensure people and data are protected wherever they work.

Want to learn more about the integrated, cyber-resilient solutions designed by Microsoft and built into Surface, Windows 11, and Microsoft 365? Contact your representative today.

Microsoft Surface

Cyber Resiliency Checklist

Questions to consider when evaluating the impact of your devices on cyber resilience

These questions and topics will help you understand where your device portfolio stands as you move deeper into security planning:

- ☐ What priority does leadership place on security when it comes to vulnerabilities in our end-user devices?
- ☐ How much budget does leadership intend to invest in device upgrades to ensure security is maintained?
- ☐ What would it cost if your security was breached?
- ☐ Do you have a complete understanding of endpoints and where they create vulnerabilities? Both quantity and quality.
- ☐ Does your company allow employees to carry or bring their own devices to connect to work?
- ☐ How many solutions do you rely on in your current security ecosystem?
- ☐ Are you using multiple device types and operating systems? Are you able to consolidate?

Talking to leaders about security

Use these conversation starters to spark discussion around security and, ultimately, decide how to make choices that support cyber resilience:

- What level of priority do we place on the security of our IP, data, and people?
- When considering security versus employee experience, which one is more important and to what extent?
- Do we have loyalties to vendors or is there opportunity to consolidate?
- Embracing a Zero Trust security model will improve our cyber resilience. What is the appetite for making this shift in security mindset?

Cyber resiliency is a team effort

For organizations to be resilient, technology decision-makers need to bring business decision-makers in all areas of the organization to the table of resilience planning.

Role	Relevancy of device choice	For consideration
Chief Financial Officer	ROI on device investment	Evaluating the Business Case of Microsoft & Total Cost of Ownership
Chief Sustainability Officer	Alignment to ESG goals	Microsoft Surface Emissions Estimator
Chief Security Officer	Integration into security ecosystem, protecting data and intellectual property	Microsoft Surface & Endpoint Security
Chief Human Resources Officer	Support of productivity, versatility, devices, and employee experience	Understanding the role of Modernized PCs in Hybrid Work Environment Optimization

Additional resources

Microsoft Security Insider

Microsoft Secure

Learn more about Zero Trust

5 Steps to Cyber Resilience

Business resilience - Cloud Adoption Framework | Microsoft Learn

The Chief Information Security Officer (CISO) Workshop - Security documentation | Microsoft Learn

Have a small business? See how Surface and security can unlock your potential.