Windows 11 Pro

Complete security playbook for the hybrid workplace

Ransomware attacks increased by 150% in 2021.[1]

Here are some of the ways a secure, future-proof IT infrastructure helps protect your business from cyberthreats:

Take a Zero-trust approach

Zero-Trust security model reduces risk by explicitly verifying data points such as user identity, location, and device health for every access request, without exception. When verified, users and devices have limited access to only necessary resources.

The Zero Trust principles are threefold:

1

First, verify explicitly. That means always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

2

Second, use least privileged access, which limits user access with just-in-time and just-enough-access, risk-based adaptive polices, and data protection to help secure both data and productivity.

3

Third, assume breach. Assume breach operates in a manner that minimizes blast radius and segments access. Verify end-to-end encryption and use analytics to gain visibility to improve threat detection and defenses.

To implement a zero-trust approach, organizations must understand its own data and where that data is housed.

Businesses should know the level of data sensitivity and potential risks of exposure to determine where zero-trust needs to be mandated. For cloud-based storage and applications, like email services and cloud data storage, establishing a zero-trust environment makes sense and is crucial to mitigate risks. Without this approach, company passwords, devices, and sensitive data are inevitably at risk to attacks.

Implement advanced authentication methods

A security breach becomes a lot more likely if user authentication methods become compromised. Unauthorized access to an employee's device often affords a potential bad actor access to an organization's entire network. Implementing a secure way of making sure users are who they say they are is essential in today's hybrid work environment. Multifactor authentication can go a long way towards creating a more secure environment. Passwords are no longer sufficient to mitigate increasingly sophisticated threats, as they are often easily compromised. Techniques like two-factor authentication, combined with the biometric capabilities readily available on many modern devices, such as Windows Hello for Business, are much more effective at protecting organizations and their networks from cyberattacks, especially when strengthened with a zero-trust security strategy.

Strengthen hardware security

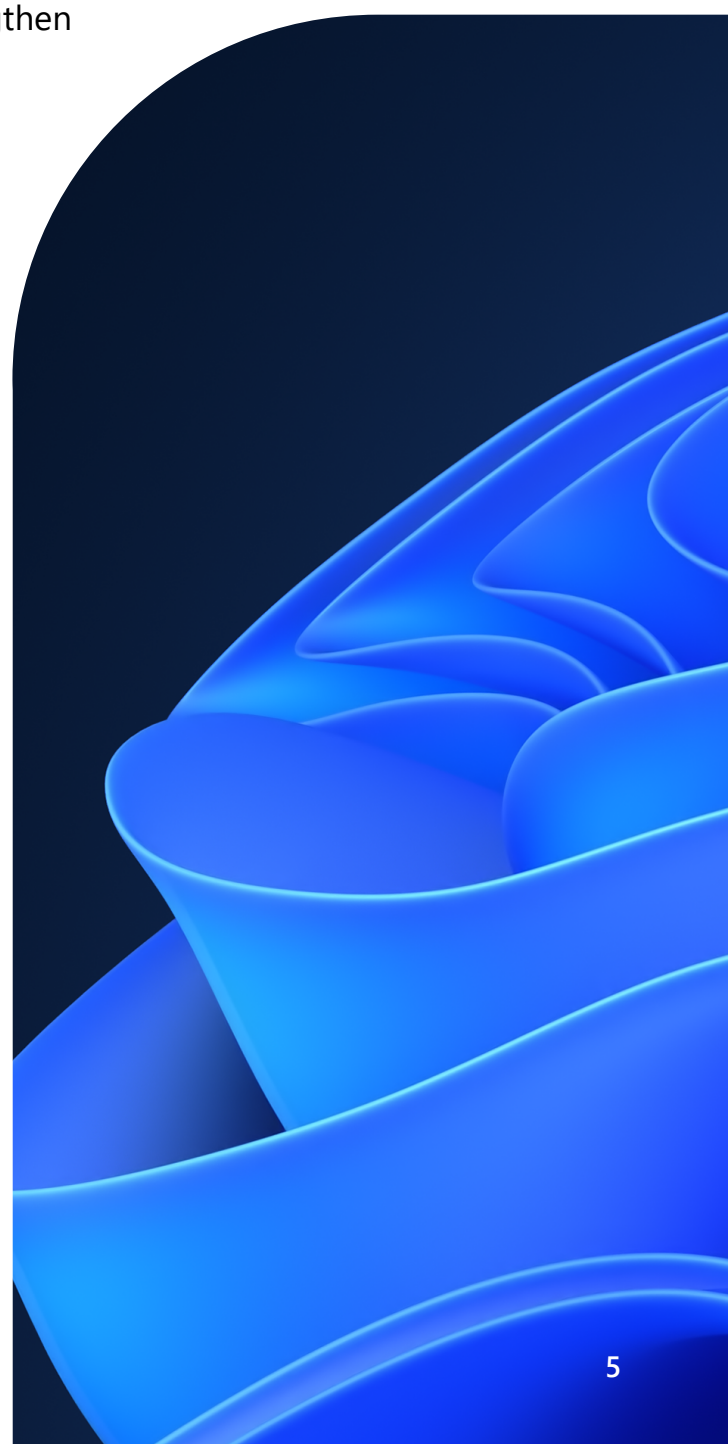
The operating system alone cannot be relied upon to protect from the wide range of tools and techniques cybercriminals can use to compromise a computer. Intruders, once inside, can deploy hard-to-remove malware into device firmware, or they can steal sensitive data and important credentials. It can be difficult to detect these intruders once they have gained access. There needs to be a strong alignment between hardware security and software-based security applications. Modern threats call for computing hardware that is secure at the chip and processor level, protecting sensitive business information right where it is stored. There are entire classes of vulnerabilities that can be negated simply by having built-in security capabilities at the hardware level.

Such capabilities can be found in all Windows 11 Secured-core PCs, for example. In addition, significant performance enhancements can be achieved when compared to deploying similar security capabilities with software alone. This increases a system's overall security posture without sacrificing system performance.

Use access controls for identity-based protection

In the cloud, administrators can control and manage identities and access from one location. For example, with Microsoft Azure Active Directory (Azure AD), they can centrally manage the identities of staff as well as configure and deploy policies for accessing applications, sites, and groups. Administrators can embed compliance requirements and any new rules can be incorporated as they arise.

Cloud-based controls increase security and strengthen compliance. Microsoft's research has found that multifactor authentication alone can block over 99.9% of account compromise attacks.[2] Conditional access allows administrators to create rules based on activity or location, which further reduces the opportunity for attackers to exploit vulnerabilities. For example, login attempts coming from outside the country or arriving at strange hours can be rejected. In addition, administrators can enable single sign-on, allowing users secure access to applications anywhere while making password management easier for IT.



Microsoft recently introduced the general availability of multicloud security support. Now businesses can onboard multicloud resources to Azure Security Center, such as Google Cloud Platform (GCP) and Amazon Web Services (AWS), as well as protect servers with Azure Defender for Servers based on Azure Arc.

Protect remote devices

The Microsoft cloud makes it easier to manage devices and applications. For example, with Microsoft Intune, device deployment can be managed securely

and remotely, while applications can easily be scaled to respond to demand. Microsoft Windows Autopilot utilizes security settings and other controls to help protect devices before an employee connects to any resources.

Secure applications

Get more protection from untrusted sources by opening files and websites in an isolated container with Windows Defender Application Guard. Cloud-first design enables easy extensibility with Microsoft 365, Microsoft Defender for Cloud, and Microsoft Defender for Endpoints.[3]

Streamline security management across diverse locations and extend security to the cloud. Help protect devices, data, apps, and identities anywhere. Deploy with confidence, knowing that 99.6% of applications are compatible with Windows 11.[4]

Automate security maintenance

Cloud-based technologies enable IT administrators to automatically apply updates, patches, and backups across systems and devices. This reduces configuration errors and limits downtime while protecting systems against new threats. Routine chores can be automated, allowing administrators time to focus on important tasks that truly require their expertise.

Keep your business secured with Windows 11 Pro devices

Transforming your organization's security posture should be a priority, and equipping your workforce with secure devices is the cornerstone for success. New Windows 11 Pro devices, combined with Microsoft 365, is built for secure hybrid work.

- Protect your employees against malware, viruses, phishing attempts, malicious links, and help keep business-critical data safe.

- Gain layers of powerful security across devices, data, identities, applications, and the cloud.

- Streamline IT with unified, cloud-based endpoint management tools including Microsoft Endpoint Manager, Azure Active Directory, and Windows Autopilot. Remotely set and enforce policies, manage applications and identities, and easily deploy business-ready devices.

- Overcome remote collaboration hurdles with a single solution that includes videoconferencing, productivity apps, file sharing, and more. Ensure your employees have secure access to critical work apps and information with a unified collaboration solution.

- For people in data-sensitive industries or business scenarios, Secured-core PCs are the most secure Windows devices, and come with all the advanced security features of Windows 11 enabled.

Significantly reduce risk from cyberattack by replacing aging PCs with new, modern devices optimized for security and hybrid work. Windows 11 Pro and Microsoft M365 brings hardware and software together for powerful, out-of-the-box protection to shield your devices, data, applications, identities, and services.

Windows 11 Pro

[1] *https//www.bloomberg.com/news/videos/2021-12-09/microsoft-fires-back-at-crowdstrike-on-cybersecurity-video*

[2] *https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/*

[3] *Sold seprately*

[4] *App Assure program data from Oct 2018 to Feb 2022. Since 2018, App Assure has worked with thousands of customers and evaluated over 1.1 million apps with a 99.6 percent app compatibility rate. To learn more, visit the App Assure website and see Windows IT Pro Blog post on App Assure*