E-book Series

Microsoft Security

Securely work from anywhere

Modernize your security culture
beyond traditional corporate boundaries

Flexible and hybrid work is here to stay

The shift to a hybrid workstyle has been forcing organizations to rapidly adapt. Remote employees are getting work done any way they can—using personal devices, collaborating through cloud services, and sharing data outside the corporate network perimeter. Hybrid employees work on both corporate and home networks, switching between business and personal devices.

Hybrid work requires a Zero Trust strategy across your environment

Security architectures that count on network firewalls and virtual private networks (VPNs) to isolate and restrict corporate resources are no longer enough. The reality of hybrid environments and increased cybersecurity attacks has steered the need for adopting a Zero Trust approach, which allows you to modernize your security culture beyond traditional corporate boundaries.

An effective Zero Trust architecture reduces risk across your digital estate at every opportunity by adhering to the following principles:

As employees' home networks stretch the corporate network perimeter, with different devices joining that network, security threats are both multiplying and becoming more sophisticated while attack vectors evolve.

of enterprise organizations have started moving toward a hybrid workplace.

Source: Zero Trust Adoption Report, July 2021.

Verify explicitly

Always make security decisions using all available data points, including verifying every identity, location, resource, and data classification while identifying device health and anomalies.

Use least-privilege access

Limit access with just-in-time/just-enough-access (JIT/JEA) and risk-based adaptive policies. Capture and analyze telemetry to better understand and secure your digital environment, ensuring you can discover and secure unmanaged endpoints and network devices.

Assume breach

Minimize blast radius with micro-segmentation, end-to-end encryption, continuous monitoring, and automated threat detection and response.

> A Zero Trust model is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction; asserts least-privilege access; and relies on intelligence, advanced detection, and real-time response to threats.

From cloud to edge, Zero Trust security supports hybrid work

A Zero Trust model combines policies, processes, and technology to establish trust, from cloud to edge, irrespective of where users access your network. A Zero Trust model doesn't presume any identity or device is secure on any network; the approach mandates that you verify it, and do so while continuously monitoring network, data, and application security in the office, at home, and across devices.

Here's how to move forward with a Zero Trust model:

In the office

Move all employees off the corporate network to be fully cloud/internet-first. This strengthens the "assume breach" approach and makes everyone more secure while providing a seamless and consistent experience from anywhere.

At home

Ask all employees who continue to work remotely, either full-time or part-time, to run a test of their home network to ensure it's secure.

Across devices

Whether employees are in the office or remote, every device with access to corporate resources should be managed. Protect devices against credentials compromise with essential tools like multifactor authentication (MFA) and risk assessment using Identity Protection in Microsoft Azure Active Directory, continuous access evaluation, and Microsoft Intune app-protection policies. Take advantage of a password-less experience that your employees love and IT trusts. Enforce more granular security protocols based on user actions within the app or the sensitivity level of data they're trying to access.

Zero Trust architecture helps enforce security program management

In a Zero Trust architecture, every digital estate, identity, endpoint, application, network, infrastructure, and data source requires policy enforcement. Analyzing productivity and security signals across these estates helps improve security program management by evaluating security culture, identifying areas for improvement or best practices and historical context, and enabling one-click configuration changes.

Zero Trust deployments help security teams reduce manual efforts by automating routine tasks like resource provisioning, access reviews, and attestation. You can also use machine learning and AI in threat protection tactics like security automation and orchestration, enabling your organization to build back infrastructure quickly after an attack.

How a Zero Trust approach benefits your hybrid work environment

A Zero Trust approach not only solves several security problems arising from remote and hybrid work models, it also helps create benefits such as:

Improved employee experience and productivity

A Zero Trust approach allows your employees to safely work from home, enroll new devices from anywhere, hold secure meetings, and achieve greater levels of productivity. Implementing single sign-on (SSO) and MFA, using password-less authentication, and eliminating VPN clients reduces day-to-day friction and improves the employee experience.

IT cost saving

Deploying a Zero Trust model can consolidate organizational spending on software as a service (SaaS) security solutions to support hybrid work. You can retire on-premises security solutions like identity and access (IAM), VPN, third-party antivirus, antimalware, and security information and event management (SIEM) solutions. Modernized endpoint management makes it easier for IT to set up

Move data highlight on the right up one page, change decrease in calls to decrease risk of breach >>>>

and manage devices. Implementing a Zero Trust architecture can reduce help desk calls and shorten ticket resolution times.

Increased agility and adaptation

A Zero Trust model empowers users and admins with automatic protection and security insights to execute with confidence and agility. Device health, antimalware status, and security are constantly monitored and validated. When you assume breach and provide the least-privileged access necessary, it empowers employees with the flexibility and freedom they want.

Talent retention

In a hybrid work world, embracing flexibility is critical to attracting and retaining employees. A Zero Trust approach empowers people to work productively and securely whenever, wherever, and however they want.

Robust and integrated security

By helping you establish a strong cloud posture, a Zero Trust approach provides security and visibility across applications, endpoints, networks, and users. Integrating controls and telemetry across security points enables you to apply unified policies and enforce them consistently, resulting in a more robust security posture for your organization.

Value of Zero Trust solutions from Microsoft

$7M+ in reduced spending on legacy software and infrastructure

75% faster setup for new users on devices

50% decrease in IT and help desk calls

Source: The Total Economic Impact™ Of Zero Trust Solutions from Microsoft, December 2021.

Start your journey with Zero Trust security

With a Zero Trust strategy, you can deliver on improved and modernized security while driving tangible business results.

To learn more, visit aka.ms/zerotrust