Microsoft Security

The New Zero Trust Guide for CISOs

Perimeter-free Security for the Age of AI-accelerated Threats

As data increasingly flows across cloud environments, networks, and external partners, traditional perimeter-based security approaches are no longer sufficient. The scale and sophistication of cyberattacks grow every month with AI as a multiplying factor for their speed, complexity, and effectiveness. With all this, CISOs and other IT leaders are finding that a Zero Trust approach is essential. It improves upon traditional perimeter-based security, offering improved security, compliance, governance, and operational agility.

But what is Zero Trust?

It's not a product, or a strategy, or even a technology. It's a philosophy—an approach to security. As its name implies, Zero Trust assumes every transaction, user, and device is a potential threat, requiring continuous authentication and verification.

Zero Trust assumes every transaction, user, and device is a potential threat, requiring continuous authentication and verification.

The "everything-is-a-threat" approach demands that any Zero Trust approach be informed by three core principles:

1. Verify explicitly.

Everything is continuously authenticated and authorized based on user identity, location, device health, service or workload, data classification, and anomalies.

2. Use least-privileged access.

User access is limited by just-in-time, and just-enough-access (JIT/JEA), risk-based adaptive policies, and data protection to help secure both data and productivity.

3. Assume a breach.

Every situation is treated as though a breach has already occurred to improve prevention and minimize cross-system access and further damage.

From those principles, Zero Trust provides a proactive defense by treating every access attempt as suspicious, regardless of its origin—even if it's contained in data that's already inside your network. This enables Zero Trust to apply a flexible approach that addresses seven key risk areas:

Identity — Use automated authentication like multifactor authentication (MFA) and single sign-on (SSO).

Data — Classify, label, and protect data across your environments at rest, in motion, and in use.

Endpoints — Manage all types of endpoints accessing your data.

Applications — Simplify and secure access to cloud and mobile apps and on-premises resources for all authorized parties.

Network — Reduce perimeter-based scalable security vulnerabilities like VPNs with improved visibility into network traffic.

Infrastructure — Automate protection and security management whether operating on-premises, in the cloud, or in a hybrid environment.

AI — Enhanced by AI, Zero Trust can accelerate and automate threat detection and response, allowing you to adapt in real time by dynamically adjusting policies and controls. Automation of these actions helps reduce IT and security workloads while improving your security posture.

Implement at your own pace

You don't have to implement Zero Trust all at once across your organization. You can implement it incrementally, starting small with high-impact areas based on your specific needs, existing resources, and threats.

Zero Trust, loads of benefits

However you plan and execute Zero Trust, you'll find that it improves many aspects of security, systems management, and user experience, including:

- A safer organization through increased security and visibility that verifies every transaction and data package
- Streamlined action on leadership decisions through centralized security controls and accelerated policy updates
- Fewer budget headaches with lower-cost and more effective security measures
- Lowered security team stress by simplifying employee and administrator experiences

Take a closer look

To find out more about Zero Trust implementation for enhanced operations and security, read our "Fundamental Guide to Zero Trust: A Leadership Approach to AI-enhanced Security." It gives you a blueprint to accelerate and launch Zero Trust with trusted Microsoft tools and solutions.

Read the e-book now