E-book Series

Microsoft Security

Minimize the impact of internal or external bad actors

Reduce the risk of security breaches while preventing attacks

Your organization's health and reputation depend on your security strategy

With the widespread adoption of cloud-based enterprise environments and the growth of the mobile workforce, data footprints exist beyond the traditional boundaries of corporate networks. Traditional approaches that focus on establishing perimeter-based security, where everyone inside the network perimeter is trusted, are no longer relevant.

If an attacker gains access to your network, they can access any data, applications system, and resource within it. They may breach your network by stealing user credentials, taking advantage of a security vulnerability, or introducing a malware infection. Such attacks can result in loss of revenue and high cyber insurance premiums, which can be a significant setback for your organization's financial health and market reputation.

To reduce the impact of a significant incident, adding defense-in-depth layers, identifying the business risk of a breach, and understanding the resulting damage to reputations and relationships are all essential.

Nearly two-thirds of organizations were breached in the past year, and it cost them an average of $2.4 million per breach.

Source: Forrester. The 2021 State of Enterprise Breaches, April 2022.

Robust security posture with a Zero Trust approach

Knowing your organization is vulnerable is the first step toward a robust security posture. Unlike outdated models, Zero Trust security assumes that security risks exist inside and outside the network. It presumes that you are constantly under attack and that a security incident can happen at any time. A Zero Trust approach insists that you be prepared with a setup that minimizes the blast radius of such an incident and creates an in-depth security layer, which reduces the extent of the damage and how fast it spreads.

To put this approach into practice, follow these three Zero Trust principles:

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.

Applying the Zero Trust principle of assume breach

The Zero Trust model moves network defenses from static, network-based perimeters to focus on users, assets, and resources. Zero Trust security requires strict verification for every user and device on the network every time before granting access to data and applications.

Segment networks to prevent lateral movement

With a Zero Trust approach, networks are divided into smaller segments for specific workloads. Ingress and egress controls help minimize the blast radius of unauthorized access to data. Implementing software-defined perimeters with increasingly granular controls limit an attacker's ability to propagate through your network and dramatically reduce a threat's lateral movement.

Use real-time threat protection to detect and respond

Implementing cloud-native filtering and protection for known threats, while further investing in automated alerting and remediation, helps reduce your average time to respond to attacks. Deploy real-time threat assessment used in access decisions, utilizing cloud intelligence and all available signals to detect and respond to access

anomalies. Use machine learning and AI in threat protection tactics like security automation and orchestration to defend your organization, so you can build back infrastructure quickly after an attack.

Use cloud-native access controls integrated with identities

Cloud-native access controls that integrate with identities are key to enforcing the least-privileged access principles. You can quickly update your detection engine with any newly identified attacks for a known web attack and ensure that each request in your network is checked against attack signatures. For unknown attacks, ensure that you observe patterns in request traffic, and that your defenses are constantly learning and updating such patterns as your traffic evolves.

Protect data with end-to-end encryption

Lastly, assuming a breach, encrypt data end to end, from data-at-rest to in-transit to data-in-use. Encrypt virtual-machine disks, storage, and data at rest; use the application gateway for in-transit data and virtual private networks for encrypted traffic. Utilize hardware-based secure enclaves to encrypt data-in-use.

Benefits of minimizing business damage with a Zero Trust approach

A Zero Trust approach solves several security problems arising from security breaches.

Demonstrate robust security and risk posture

A Zero Trust approach allows triage alerts, correlation of additional threat signals, and remediation actions. Analyzing signals helps improve your posture by evaluating your security culture and identifying areas for improvement or best practices. Any change in your network automatically triggers analysis for potential malicious activity. You gain complete visibility of all assets and resources within the networks and how they're performing, which results in a significant overall reduction in risk exposure.

Reduce blast radius within your organization

Deploying a Zero Trust model can help minimize the impact of an external or insider breach. It enhances your organization's ability to detect and respond to threats in real time and reduces the blast zone of attacks by restricting lateral movement.

Control damage to reputation

When a breach occurs and an attacker is able to access confidential data, this can bring severe impacts, like damage to brand reputation, loss of sensitive intellectual property, disruption to customers, and financial harm to your business. Zero Trust security helps to reduce the attack area by continuously assessing, monitoring, and analyzing your network, while a Zero Trust architecture helps define policies that are updated automatically when risks are identified.

Lower cyber insurance premiums

To evaluate the cost of cyber insurance, you need a better security model and architecture. By implementing Zero Trust security, you have control, visibility, and governance with real-time analysis for protecting your network and endpoints. Your security team can detect and overcome gaps in your overall security posture and prove to insurers that you have proactive strategies and systems. A Zero Trust approach also improves cyber resilience and may even help pay for itself by reducing premiums.

Increase security team morale

Zero Trust deployments reduce manual efforts for your security team by automating routine tasks like resource provisioning, access reviews, and attestation. As a result, you can empower teams with the time and telemetry they need to detect, deter, and defeat the most critical attacks and risks, both internally and externally, which in turn boosts IT and security team morale.

Zero Trust models from Microsoft reduce the risk of a data breach by

Source: The Total Economic Impact™ Of Zero Trust Solutions

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