E-book Series

Microsoft Security

Rapidly modernize your security posture

Build confidence with your employees, partners, customers, and other stakeholders

Evaluating your security posture is an ongoing challenge

The security landscape is constantly changing with the rapid adoption of hybrid work, increasing ransomware attacks, and evolving regulatory oversight. Today's security leaders must balance these challenges with business needs to collaborate, innovate, and grow. With these challenges come essential questions from employees, partners, customers, and C-suite stakeholders:

- Do we have the right security strategy and controls?
- Can we measure breach risk?
- Are our security controls good enough to handle modern-day cyber risk and vulnerabilities?
- Do we have tools for timely incidence response?

Can we easily meet today's and future compliance and reporting needs? Confidence in security teams depends on the answers to these questions. The answers are also integral to your security posture, which impacts your ability to protect resources and keep your organization out of headlines that damage your business reputation, erode customer trust, and affect profitability. You need proper methods and practices Confidence in security teams depends on the answers to these questions. The answers are also integral to your security posture, which impacts your ability to protect resources and keep your organization out of headlines that damage your business reputation, erode customer trust, and affect profitability. You need proper methods and practices to reassess your security posture and constantly track results.

With a whopping 1100% increase in ransomware attacks year-over-year between July 2020 and June 2021, staying on top of attack trends—such as ransomware and supply chain threats—is more important than ever.

Source: Fortinet Ransomware Survey Shows Many Organizations Unprepared. Fortinet. 29 September 2021

Building confidence and trust with Zero Trust principles

Implementing a modern security strategy adds visibility across multiple endpoints, access decisions based on risk assessment, and automated detection and response actions. You can enable comprehensive security monitoring, risk-based access controls, and policy automation throughout your security infrastructure to focus on protecting critical assets (data) in real time within a dynamic threat environment.

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

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.

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 betters 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.

Increase effectiveness of security management with Zero Trust models

A Zero Trust strategy helps you analyze your current security posture, find gaps, and take timely action to eliminate those gaps. You can enable the integrity and privacy of data with visibility, continuous assessment, and analysis that quantifies security posture and provides recommendations and guidance for improving it.

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

Understand your current security posture

Using tool assessments like Secure Score and Compliance Score, measure the security posture of your assets against industry benchmarks and best practices. Your security team can continuously monitor security scores to instantly understand your risk and which assets are vulnerable. By getting measurable data when you add these scores to your regular reporting and security KPIs, you can demonstrate your progress.

Take advantage of visibility and analytics

Continuously observe and monitor your assets across various attack vectors, detecting leaks and pressure points that threaten your sensitive data flow. Analyzing these observations and patterns helps you to derive risk insights and predict the likelihood of a breach. With continuous analytics and tracking, you can determine the right level of access controls in real time, balancing your user experience with proper governance. Analyzing these security signals allows you to evaluate your security culture and identify areas for improvement.

Undergo risk assessment

Assess risks like configuration drift, missed software patches, and gaps in security policies. Supported by AI and automation capabilities, better visibility makes it easier to identify vulnerabilities and quickly mitigate threats to reduce risk. You can improve security posture by identifying areas for improvement based on best practices and historical context, enabling one-click configuration changes, and offering impact assessments to optimize coverage and rollouts that enhance productivity for your users.

Benefits of having a robust security posture with a Zero Trust approach

Improving your security posture through a Zero Trust architecture helps you protect against a fast-changing threat landscape and earn the trust of your stakeholders. It carries business benefits such as:

Demonstrating impact to your board of directors

With security score and analytics, you can provide clear evidence to your business leaders and support a case for changing your security strategy. Specify actions to take for improving security, the level of effort of those actions, and how these actions will affect users.

Driving innovation with partners and enriching relationships

A Zero Trust model examines security breaches that may occur during partner interactions, and unifies and consolidates security policies in house. In doing this, you're minimizing vulnerabilities created by insufficient security practices of outside vendors, while ensuring that the right users have an appropriate level of access to resources and assets. You can establish trust relationships to enable secure access for specific partners and contractors—regardless of their location, device, or network.

Increasing security team morale

Help boost your security team's confidence, so they're better able to apply Zero Trust policies across environments from a single platform, quickly identify and remediate security concerns, and reduce the complexity of security environments. In addition to improving your security posture, a Zero Trust approach enables your security team to simplify their cybersecurity strategy and retire unnecessary legacy solutions.

Enabling agile response to business scenarios

Implementing a Zero Trust architecture helps your organization to roll out policies and technologies that improve your security posture, simplify security management, and enable greater business agility to support new business scenarios. Provide your security team with automatic discoverability, centralized visibility, practical guidance, and control of assets. Empower your IT team to spend less time maintaining infrastructure and more time furthering the changing needs of the business.

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