Microsoft

Security best practices for Microsoft partners

Improve your security posture with Microsoft tools, resources, trainings, and platforms.

Version 1.2

Why security matters for you and your customers

With the rise in sophisticated cybersecurity attacks, security continues to be one of the top challenges of our digital age.

Today, anything less than comprehensive security is no security at all.

Microsoft is invested in keeping our ecosystem secure as cyberthreats rise.

The volume of password attacks has risen to an estimated 921 attacks every second—a **74% increase** in just one year.[1]

Microsoft synthesizes **43 trillion**[1] security signals daily, using sophisticated analytics to understand and protect against digital threats.

Microsoft has **8,500+** engineers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, and frontline responders across **77 countries.**[1]

1. "Microsoft Digital Defense Report 2022," Microsoft, 2022.

As the threat landscape continues to evolve—and industries transition from remote to hybrid work—you need to adopt an end-to-end **Zero Trust security model** that covers the entire technology ecosystem.

What is the Zero Trust framework?

Microsoft follows the Zero Trust framework, a highly effective security model that assumes all activity—even by trusted users—could be a breach.

Verify explicitly

Authenticate and authorize based on all available data points, including user identities, location, device health, service or workload, data classification, and anomalies.

Use least privileged access

Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Assume breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Use the Zero Trust framework to become a key security collaborator

By adopting the Zero Trust security model, you can keep your organization resilient, consistent, and responsive to attacks.

Keep your employees and business safe—anytime, anywhere, and on any device.
By applying proven Zero Trust security techniques, you can keep the data belonging to you, your business, and your employees safe from cyberattacks.

Help customers mitigate risk.
Customers value partners who can safeguard their data, close security maps, and advise on the products, services, and solutions for best-in-class security.

Stay at the forefront of digital transformation.
Partners who invest in key solutions today—and become experts on intelligent security—position themselves to be valuable resources in the years to come.

Security holds immense opportunity for partners.
Gartner expects the total addressable market in security and risk management to reach $261.9 billion in 2026.[1]

1. Gartner: "Forecast: Information Security and Risk Management, Worldwide, 2020-2026, 3Q22 Update," September 28, 2022.

Creating a safer world for all—together

Microsoft will deliver ongoing guidance and resources to help you adopt stronger protective measures.

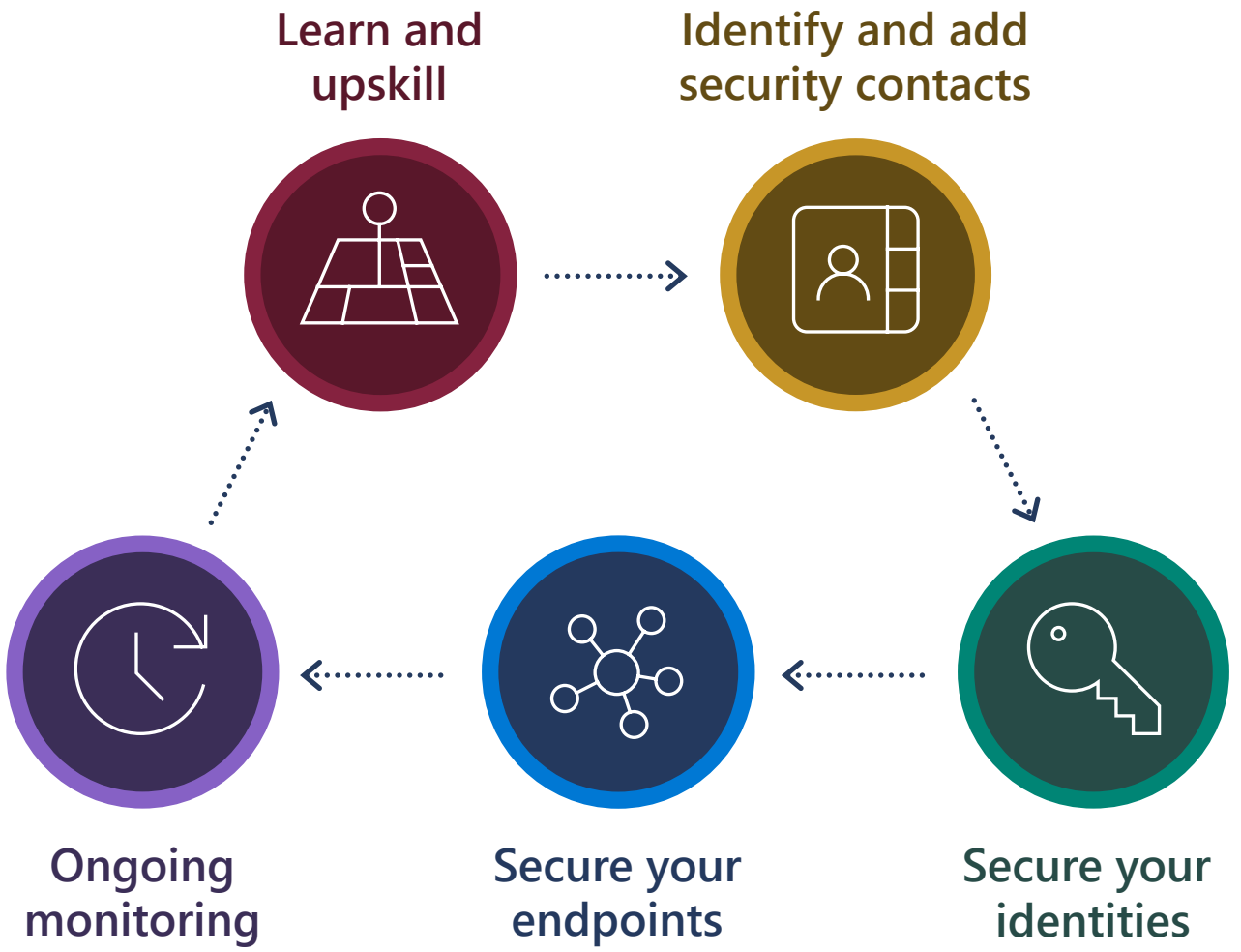
To successfully implement Zero Trust across our ecosystem, we're relying on you to take the necessary security actions.

By working together, we can better plan for shifts in the cybersecurity landscape and proactively respond to risk for years to come.

Implement a strong approach to security

With new threats constantly emerging, security must remain a top priority for your business—and tasks should be properly delegated to ensure a sustainable system.

Explore this guide for key actions and trainings that can help you implement ongoing practices and keep your security sharp.



Commit to ongoing security with these best practices

Upholding security is not a step-by-step process—it's an ongoing commitment. Keep your customers and organization safe by continually updating and investing in each aspect of your security.

Learn and upskill

Evolve with the security landscape to protect your organization and your customers. Sharpen your skills with courses designed to help you make the Zero Trust model work for you.

Identify and add security contacts

Establish an individual or group who will be accountable for security-related issues, responding quickly when notified about potential threats.

Secure your identities

Take action to enforce multifactor authentication (MFA) and remove unnecessary delegated administrative privileges.

Secure your endpoints

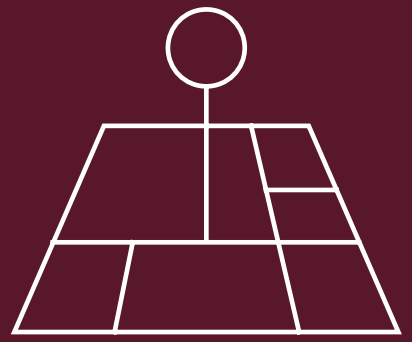
Invest in platforms that prevent, detect, investigate, and respond to advanced threats.

Ongoing monitoring

Remain engaged with your Zero Trust framework, tapping into resources that help you detect fraud and protect identities.

Learn and upskill

Tap into trainings and gain the skills you need to keep you and your customers safe.



Key role:
Security Operator/Analyst or Security Administrator

Stay up-to-date on the security landscape

Learn the best ways to implement the Zero Trust framework and deploy and sell security products and services.

Register for "Security through the Lens of Zero Trust," a course that demonstrates how to help customers easily protect their identities and networks using tools available through Microsoft Azure and Microsoft 365. This key training is available via our ongoing 2-day live webinar series or as an on-demand workshop.

Webinar view time: 2 2-hour, 30 min sessions

Register for webinar

Join on-demand workshop

Learn more about the principles of Zero Trust and the corresponding tools designed to fortify your business.

Read time: 5 min

Read the blog

Identify and add security contacts

Establish a point of contact for security information.

Key role:
Security Administrator

Security contact responsibilities and guidance

The security contact is an individual or group within your organization who will serve as the point of contact if Microsoft detects a threat. The contact must have an inbox that can be monitored constantly—we recommend using a distribution list—and respond with urgency to investigate and remedy security concerns.

Read time: 5 min

Establish a security contact

Secure your identities

Safeguard against frequent attacks with these simple tools.

Key role:
Security Administrator

Enforce multifactor authentication (MFA) for all users in tenants for you and your customers

Your identity secure score shows how aligned you are with Microsoft's security recommendations—and where you can better protect your customers and business.

Read time: 6 min

Check your score

MFA is a key component of the Azure Active Directory security defaults. Explore the benefits of these defaults and follow simple actions to enable them for your customers.

Read time: 5 min

Read the blog

Learn more about the Azure Active Directory security defaults, including deployment considerations and enforced security policies.

Read time: 8 min

Read the article

Discover how to manage Azure Active Directory roles and close commonly used avenues for cyberattacks.

Read time: 5 min

View best practices

Passwordless authentication is an effective alternative to MFA, and Microsoft offers a variety of methods to fit your customers' needs.

Read time: 9 min

Explore authentication options

Secure your identities

Complete these key processes to improve customers' security.

Key role:
Security Administrator

Remove Inactive DAP (delegated administration privileges) connections

Familiarize yourself with delegated administration privileges—how to acquire them, manage them, report their activity, and more.

Read time: 6 min

Explore the FAQ

Strengthen your customers' security by monitoring DAP and removing connections that aren't in use.

Read time: 5 min

Learn how

Transition active DAP connections to GDAP (granular delegated admin privileges)

Granular delegated administration privileges (GDAP) allow customers to partition partners' access, creating an appealing option for those who have regulatory privacy or security requirements.

Read time: 2 min

Learn more about GDAP

Create new GDAP relationships with the GDAP bulk migration tool, which allows partners to execute the DAP-GDAP transition in batches.

Read time: 10 min

Discover tool features

Secure your endpoints

Equip your devices to better prevent, detect, investigate, and respond to cyberattacks.

Key role:
Security Administrator

Use Microsoft Defender for Endpoint

Microsoft Defender for Endpoint works to stop threats, scale defenses, and evolve your security.

With components ranging from asset discovery to auto investigation, this comprehensive security solution provides essential endpoint protection.

Read time: 2 min

Learn more about Microsft Defender for Endpoint

Watch an overview video. View time: 7 min

Review the documentation for a deeper dive into its capabilities. Read time: 4 min

Compare plans to get started. Read time: 3 min

Use Azure Active Directory Conditional Access to enforce compliant devices

Create a Conditional Access policy to ensure that all devices accessing an organization's resources comply with selected security standards—such as requiring device encryption or a PIN to unlock.

For accounts with customer tenant access, Microsoft recommends a separate endpoint.

Read time: 2 min

Learn more about Conditional Access

Ongoing monitoring

Mitigate risk by upholding the Zero Trust framework.

Key role:
Security Operator/Analyst or Security Administrator

Detect fraud

Watch for suspicious activity by configuring your security notifications and monitoring customer transactions.

Configure your Azure AD Identity Protection notification emails to stay informed on at-risk users and detected risky sign-ins (in real time). Promptly investigate suspicious activity and help ensure customer safety.

Read time: 4 min

Configure notifications

Gain insight into customer transactions by viewing and exporting activity logs. By staying up-to-date on customer purchases, you may be able to better identify any actions that seem suspicious.

Read time: 2 min

Gain insight

Azure fraud detection and notification locates potential cryptocurrency mining activities in your customers' Azure subscriptions. Notifications enable you to take swift action against fraudulent behavior.

Read time: 2 min

Subscribe to fraud notifications

Ongoing monitoring

Optimize security spending and track budgets.

Key role:
Security Operator/Analyst or Security Administrator

Manage costs

Managing Azure costs is crucial to keeping security updated and sharp. Microsoft offers resources to help you monitor cost trends, detect anomalies, and track your investment in security.

Maximize your cloud environment efficiency and gain visibility into your spending with our cost optimization training module.

Training time: 51 min

Start training

Help customers manage their monthly Azure spending by creating a budget. Monitor, alter, or remove the budget as necessary, gaining crucial data to strengthen your partnership.

Read time: 3 min

Learn to create budgets

Manage nonpayment, fraud, and misuse by building practices that reduce risk and address violations of Microsoft policies. Because you are financially responsible for customers' nonpayment and fraudulent purchases, having a plan of action is essential for your business.

Read time: 2 min

Make a plan

Cost alerts notify you when a customer's spending exceeds a set amount. Types of alerts include budget, credit, and department spending quota, enabling you to keep a close eye on your customers' spending—and catch any suspicious activity.

Read time: 3 min

Turn on alerts

Continually invest in each aspect of your security

Maintaining strong security requires more than completing one task; it’s a continual practice of monitoring your—and your customers'—ecosystem. Thinking critically about security and regularly updating your knowledge and tools is the only way to remain safe in a shifting landscape.

Joining forces is the best line of defense

At Microsoft, we're committed to helping you adopt security strategies that empower you and your customers to continue achieving at the highest level.

As we invest in tools for stronger threat protection rooted in the Zero Trust framework, we rely on you to proactively strengthen your security posture.

Through our partnership, we can create a safer world.

Together, let's evolve to meet security challenges and protect people and organizations around the globe

Questions? Register for weekly open Q&A sessions with Microsoft Business Operations.

Compare available support options and choose the right plan for your business.

Need help? Submit a support request in Partner Center.

Stay secure by joining our "Security Through the Lens of Zero Trust" live webinar series or on-demand workshop.

Contact Microsoft partner technical consultants* for assistance deploying security best practices.

* Available to partners with a Microsoft Action Pack, Solutions Partner designation, or specialization.


Microsoft
Thank you

Additional resources

Continue your journey with a suite of tools designed to enhance partner security.

- GDAP bulk migration tool FAQ
- Secure customer tenants and help customers adopt MFA
- Mandating multifactor authentication (MFA) for partner tenant
- Learn about the secure application model framework
- Enable the secure application model framework
- Get the list of impacted Azure resources that have Azure fraud activities
- Security best practices for partners in the Cloud Solution Provider program

Partner checklist

Improve your security posture by completing these actions, ensuring that each action is matched with the ideal role in your organization.

Learn and upskill

- ☐ Register for the "Security through the lens of Zero Trust" webinar
- ☐ Read the "Securing the channel" blog post
- ☐ Watch the on-demand security workshops

Key role: Security Operator/Analyst or Security Administrator

Add a security contact

- ☐ Identify your organization's security contact and consider setting this up as a distribution list with multiple people who can respond quickly.
- ☐ Keep your contacts updated in Partner Center.

Key role: Security Administrator

Secure identities

- ☐ Enable phish-resistant MFA for your tenants.
- ☐ Enable phish-resistant MFA for your customer tenants.
- ☐ Review your DAP report and remove unneeded connections.
- ☐ Migrate the DAP connections you still need to GDAP.

Key role: Security Administrator

Secure endpoints

- ☐ Use secured devices to access your tenant.
- ☐ Enforce compliant devices using Azure AD Conditional Access.
- ☐ Use next-generation antivirus and endpoint detection, as well as response products such as Microsoft Defender for Endpoint.

Key role: Security Administrator

Ongoing monitoring

- ☐ Enable fraud detection and notifications.
- ☐ Set up cost management, budget limits, and related notifications on Azure subscriptions.
- ☐ Set up identity protection and configure reports and alerting.

Key role: Security Operator/Analyst and Security Administrator