Solution guide series

Microsoft

Security: A Guide to Flexible Solutions

Explore security goals

Strengthen your security

The threat landscape is evolving and an increase in attack surfaces has caused cyber security resources to become overwhelmed with teams being overworked. As a result, your security team needs flexible solutions that provide comprehensive threat intelligence.

Meet today's challenges with solutions that are integrated across people, devices, apps, and data. Easily work across platforms with built-in experiences. And, help secure your future with AI and automation.

This guide will show you step-by-step how to help secure your organization while providing a frictionless user experience so people can get their jobs done. Each scenario has a short list of questions, recommended activities, and resources to get started.

Secure remote access

Empower remote workers to access the apps they need anywhere, anytime, with enhanced security.

Questions to consider	Recommended activities
1. Do you have a way to manage identities across all your devices and applications?	☐ Use Microsoft Azure Active Directory (Azure AD) as your universal identity platform.
2. Can your users sign on and seamlessly access all their business applications?	☐ Use single sign-on with Azure AD so employees can access resources from any app or device while working remotely.
3. Are you currently using passwords for your authentication?	☐ Employ Microsoft Azure Multi-Factor Authentication to strengthen security for remote work.
4. Can you extend security to your devices?	☐ Manage and secure corporate data in approved apps on personal devices using Azure AD and Microsoft Endpoint Manager.

Get started with these resources:

- Learn about securing your remote workers.
- Start using secure remote work solutions.

Alleviate VPN bottlenecks

Add new identity-based controls to your existing network to prevent business disruption and the reintroduction of old risks.

Questions to consider	Recommended activities
1. Are you managing the security of all the cloud applications your organization uses?	☐ Track what cloud apps your organization uses and help secure them with capabilities like single sign-on and conditional access in Microsoft Cloud App Security and Azure AD.
2. Do you support identity based conditional access?	☐ Use conditional access as part of Azure AD.
3. Are you managing the security of all the cloud applications your organization uses?	☐ Track what cloud apps your organization uses and help secure them with capabilities like single sign-on and conditional access in Microsoft Cloud App Security and Azure AD.
4. How can you move to a single sign-on solution for all of your applications in the cloud and on-premises?	☐ Secure access to your legacy apps with Azure AD App Proxy, or prebuilt integrations with networking providers and app delivery controllers.

Get started with these resources:

- Watch the Security Controls for Remote Work webinar.
- Read the Single Sign-On and Managed Access to all Applications from the Cloud white paper.
- Learn about secure remote work.

Get started with Zero Trust

Zero Trust should serve as an integrated security philosophy. It's both a journey and the foundation for secure remote work.

Questions to consider	Recommended activities
1. Do you have an identity solution that includes conditional access and analytics to improve visibility?	☐ Verify and secure each identity with strong authentication across your entire digital estate.
2. Is access only granted to cloud managed and compliant devices?	☐ Gain visibility into devices accessing the network. Ensure compliance and health status before granting access.
3. Are your on-premises apps internet-facing and cloud apps configured with single sign-on?	☐ Discover shadow IT, gate access, monitor and control user actions, and ensure appropriate in-app permissions.
4. Are your workloads monitored and alerted for abnormal behavior?	☐ Move from perimeter-based data protection to data-driven protection.
5. Do you have machine learning–based threat protection and filtering with context-based signals?	☐ Use telemetry to detect attacks and anomalies, automatically block and flag risky behavior.

Get started with these resources:

- Try the Zero Trust assessment tool.
- Get 10 tips for getting started with Zero Trust.
- Learn how to implement Zero Trust across your organization.

Protect against phishing and advanced threats

Protect your organization against sophisticated threats such as phishing and zero-day malware across domains.

Questions to consider	Recommended activities
1. Do you have security protection features built into your email service?	☐ Enable the protection features of your email service.
2. Do you have a strong authentication solution?	☐ Use Microsoft Azure Multi-Factor Authentication on all your accounts to strengthen your security.
3. Do you know how to recognize phishing attacks?	☐ Educate yourself, friends, and colleagues on how to recognize phishing attempts and report suspected encounters.
4. Is your end point protection solution complete and automated?	☐ Use Microsoft Defender Advanced Threat Protection for endpoint preventative protection, post-breach detection, automated investigation, and response.
5. Do you have an integrated threat protection solution that enables you to view all threats from a centralized view?	☐ Analyze threat data across domains, building a complete picture of each attack in a single dashboard with Microsoft Threat Protection.

Get started with these resources:

- Download the Office 365 Advanced Threat Protection e-book.
- Get a modern blueprint for endpoint protection.
- See how integrated threat protection can strengthen your security.

Protect sensitive information

The need to protect and govern data and manage risk is essential to digital transformation.

Questions to consider	Recommended activities
1. Do you know where your business-critical and sensitive data resides and what is being done with it?	☐ Use flexible and intelligent classification capabilities to help you identify your sensitive data.
2. How do you protect data consistently across your digital estate, and do it without impacting end user productivity?	☐ Protect data across a hybrid environment with a unified admin console.
3. Do you have control of this data as it travels inside and outside of your organization?	☐ Control access for unmanaged devices to enable full access, web-only access, or block access completely.
4. Are you using multiple solutions to classify, label, and protect this data?	☐ Extend the solution to third-party apps and services, giving you a truly comprehensive data protection solution.

Get started with these resources:

- Get an overview of Microsoft Information Protection and governance.
- Learn about Microsoft Information Protection announcements.
- Read the Data Protection Best Practices e-book.

Mitigate insider risks

Quickly identify and take action on critical insider risks and remediate corporate code-of-conduct policy violations across company communications.

Questions to consider	Recommended activities
1. How vulnerable is your organization to insider threats?	☐ Create your insider risk management policy and enable permissions for insider risk management and the audit log.
2. What types of insider risks are you most concerned about?	☐ The Alert dashboard lets you review potential risks including employee data theft, data leaks, and offensive language.
3. Can you timely detect code-of-conduct policy violations in company communications?	☐ Customizable communication compliance policy templates let you identify and remediate code-of-conduct policy violations.
4. Are you meeting supervision regulatory requirements across company communications?	☐ The Alert dashboard lets you review potential risks including employee data theft, data leaks, and offensive language.

Get started with these resources:

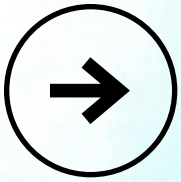
- Learn how to leverage AI and machine learning to address insider risks.
- Get started with Insider Risk Management.
- Stay up to date with our Insider Risk blog.

Increase flexibility and enhance your cybersecurity

Operational flexibility cannot be achieved without a true commitment to and investment in cybersecurity. Global organizations need to reach the state where their core operations and services won't be disrupted by geopolitical or socioeconomic events, natural disasters, and cyber events if they are to weather such events and remain strong.

Microsoft Security solutions empower your organization by offering flexibility, a seamless user experience, and integrated, best-in class protection.

If you'd like to know more about how Microsoft Security can strengthen your organization, our sales advisors are here to help.



Contact us