Microsoft Security

The Comprehensive Playbook for Implementing Zero Trust Security

Contents

Who this is for

IT and business leaders looking to secure their IT environments using a Zero Trust framework. This guide presents a comprehensive explanation of the Microsoft Zero Trust framework, along with specific steps to take in any or all of the six key areas of organizational security strategy.

Why Zero Trust?

Proliferating data and devices, growth in hybrid work, and increasingly sophisticated attacks reduce the effectiveness of perimeter-based IT security. IT professionals manage an enormous variety of technologies. Businesses commonly use a mix of cloud and on-premises infrastructure, platforms, and software. They may have multiple cloud providers and systems. Employees work on personal devices and can easily access cloud apps and services. Data exists in more places than ever before, which makes it more valuable, but also more vulnerable.

In response, many organizations, including Microsoft, are adopting a **Zero Trust** security framework. Zero Trust is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to threats:

- Verify explicitly: Always authenticate and authorize based on all available data points, including user identity, 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.

Modern threat protection is a critical component of all three areas, enabling organizations to detect attacks and anomalies, automatically block and flag risky behavior, take protective actions, and manage the growing influx of threat data.

How easily an organization can adopt these principles varies depending on its individual security challenges, needs, and capabilities. In other words, the journey to Zero Trust is unique to your business.

To help you get there faster, Microsoft has developed a flexible Zero Trust framework to guide adoption. It provides comprehensive guidance covering the six key risk areas addressed by Zero Trust:

Identity

Automate risk detection and remediation and secure access to resources with strong authentication across the entire digital estate.

Data

Classify, label, and protect data across cloud and on-premises environments to help prevent inappropriate sharing and reduce insider risks.

Endpoints

Defend the larger attack surface created by the growing number and diversity of endpoints using a flexible, integrated approach to management.

Applications

Maintain highly secure employee access to cloud and mobile apps, as well as remote access to on-premises enterprise apps.

Network

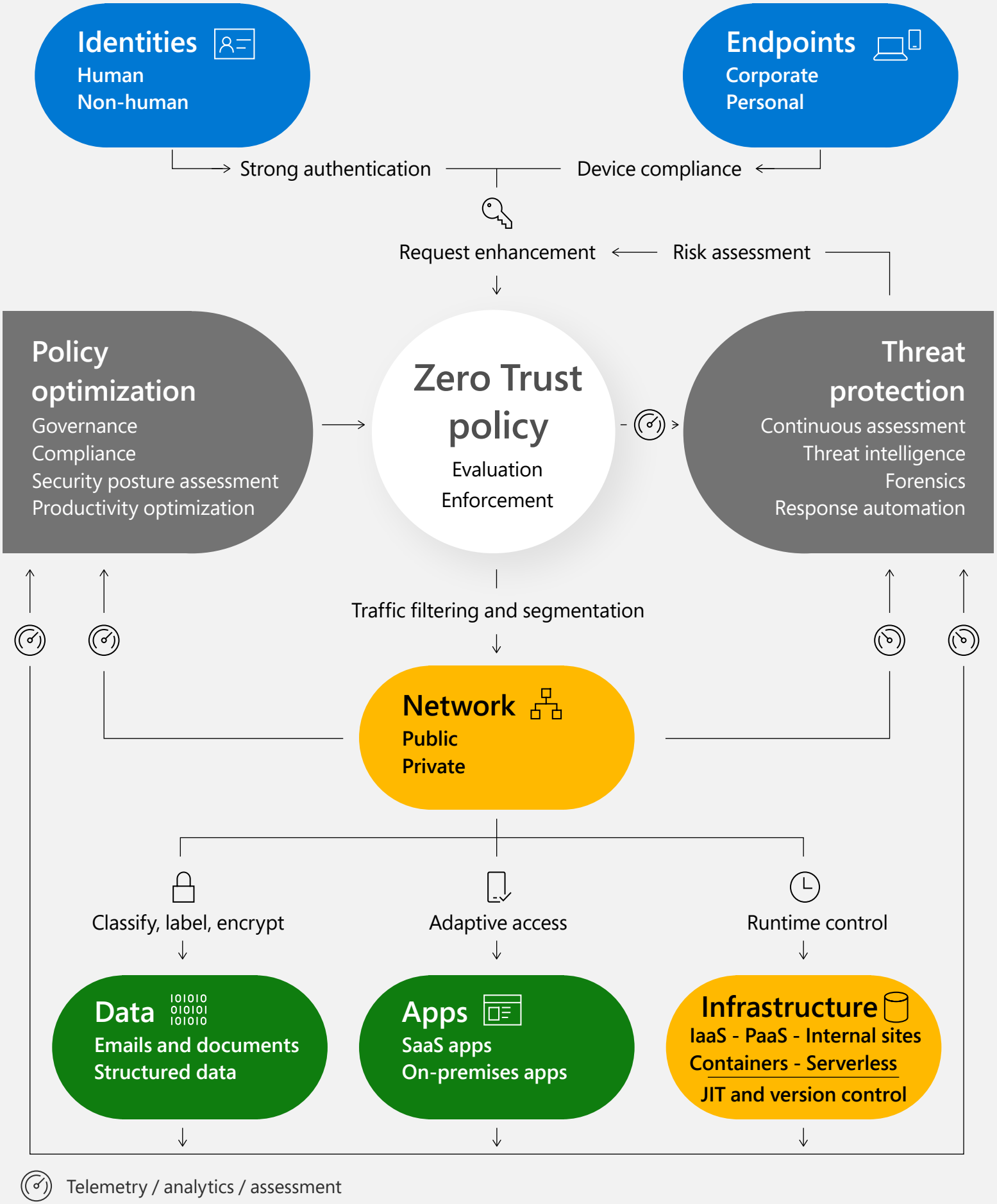
Reduce perimeter-based security vulnerabilities, including the need for VPNs, and improve scalability of security solutions for environments where the cloud is increasingly the center of IT services.

Infrastructure

Protect hybrid infrastructure, including on-premises IT and cloud environments, with more efficient and automated management.

By adopting a Zero Trust framework in one or all of these areas, you can effectively modernize your security technology and processes, and start to maximize protection in the face of modern threats. However, each organization will have different priorities depending on its current capabilities and the level of risk represented by a given security area. This guide makes it easy for you to get a broad overview of Zero Trust, as well as detailed information and actionable steps for your areas of focus.

Microsoft Zero Trust architecture



Zero Trust fundamentals

Identity

Cloud applications and the growth of hybrid work have redefined the security perimeter. Corporate applications and data are also moving from on-premises to hybrid and cloud environments. Many organizations rely on older identity and access management, built for a world with a clear line between what's inside and what's outside the network.

These systems make it difficult for people to access the apps and data they need and create security gaps by granting excessive privileges to trusted users. A Zero Trust framework, incorporating cloud-based identity solutions such as multi-factor authentication and single sign-on (SSO) across the environment, is better suited to the modern workplace.

Identity Controls for a Zero Trust framework

Implement multi-factor authentication

Multi-factor authentication helps protect your apps by requiring users to confirm their identity using a second source of validation, such as a phone or token, before access is granted.

- Tools such as Microsoft Azure Active Directory (Azure AD) enable multi-factor authentication for free.
- Azure Active Directory (Azure AD) Multi-Factor Authentication (MFA) helps safeguard access to data and apps, providing another layer of security by using a second form of authentication. Organizations can enable multi-factor authentication with Conditional Access to make the solution fit their specific needs.

Enable passwordless authentication

Passwordless authentication methods provide a simpler and more secure authentication experience across the web and mobile devices. These methods allow users to authenticate easily and securely without requiring a password.

- If you have AAD, you can enable tools like the Microsoft Authenticator app so that users can sign into any Azure AD account without using a password. Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology.
- Start with a low-risk group and explain the benefits of eliminating passwords. Deploy MFA with a passwordless authentication option until people are comfortable with it and then start replacing passwords and dependencies on passwords in the background.
- Implement single sign-on (SSO). This removes the need to manage multiple credentials for the same person and delivers a better user experience with fewer sign-in prompts.

- Microsoft Azure Active Directory (Azure AD) provides an SSO experience to popular software as a service (SaaS) apps, on-premises apps, and custom-built apps that reside on any cloud for any user type and any identity.
- When you plan your SSO deployment with your apps in Azure AD, consider these questions:
  - What are the administrative roles required for managing the application?
  - Does the certificate need to be renewed?
  - Who needs to be notified of changes related to the implementation of SSO?
  - What licenses are needed to ensure effective management of the application?
  - Are shared user accounts used to access the application?

» Enforce access controls with adaptive, risk-based policies

Move beyond simple access/block decisions and tailor decisions based on risk appetite—such as allowing access, blocking, limiting access, or requiring additional proofs like multi-factor authentication.

- Conditional Access in Azure AD enables you to enforce fine-tuned adaptive access controls, such as requiring multi-factor authentication based upon user context, device, location, and session risk information.
- You'll need a working Azure AD tenant with Azure AD Premium or trial license enabled. If needed, you can create one with Conditional Access administrator privileges for free.
- Create a non-administrator user with a password you know and create a group that the non-administrator user is a member of in Azure Active Directory.
- Fine-tune your Conditional Access policies, by asking questions about who should access your resources, what resources they should access, and under what conditions. Policies can be designed to grant access, or to block access. Be sure to ask specific questions about what your policy is trying to achieve.
- Document the answers to questions for each policy before building them out and deploy them in phases in the production environment. First apply a policy to a small set of users in a test environment and verify if the policy behaves as expected.

Block legacy authentication

One of the most common attack vectors for malicious actors is to use stolen or replayed credentials against legacy protocols, such as SMTP, that can't use modern security challenges.

- Legacy authentication protocols like POP, SMTP, IMAP, and MAPI can't enforce MFA, making them preferred entry points for adversaries attacking your organization.
- While rolling out legacy authentication blocking protection, we recommend a phased approach, rather than disabling it for all users all at once. Before you can block legacy authentication in your directory, you need to first understand if your users have apps that use legacy authentication and how it affects your overall directory.
- The easiest way to block legacy authentication across your entire organization is by configuring a Conditional Access policy that applies specifically to legacy authentication clients and blocks access.
- Even if your organization isn't ready to block legacy authentication across the entire organization, you should ensure that sign-ins using legacy authentication aren't bypassing policies that require grant controls such as requiring multifactor authentication or compliant/hybrid Azure AD joined devices.

Automate risk detection and remediation

Real-time risk assessments can help protect against identity compromise at the time of login and during sessions.

- Azure Identity Protection delivers real-time continuous detection, automated remediation, and connected intelligence to investigate risky users and sign-ins to address potential vulnerabilities.
- Data from Identity Protection can be exported to other tools for archive and further investigation and correlation. The Microsoft Graph-based APIs allow organizations to collect this data for further processing, such as with their SIEM solution.
- Enable Identity Protection to get started. Bring in user session data from Microsoft Defender for Cloud Apps to enrich Azure AD with possible risky user behavior after they were authenticated.

Enrich your Identity and Access Management (IAM) solution with more data

The more data you feed your IAM solution, the more you can improve your security posture with granular access decisions and better visibility into users accessing corporate resources.

- Azure Active Directory (Azure AD), Microsoft Defender for Cloud Apps, and Microsoft Defender for Endpoint work together to provide enriched signal processing for better decision making.
- Configure Conditional Access in Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps.

Improve your identity security posture

The identity secure score in Azure AD helps you assess your identity security posture by analyzing how well your environment aligns with Microsoft best-practice recommendations for security.

- The identity secure score is available in all editions of Azure AD. Organizations can access their identity secure score from the **Azure portal > Azure Active Directory > Security > Identity Secure Score**.
- To see your score history, visit the Microsoft 365 Defender portal and review your overall Microsoft Secure Score. You can review changes to your overall secure score be clicking on View History. Choose a specific date to see which controls were enabled for that day and what points you earned for each one.

Learn more about solutions for Zero Trust identity

Multi-factor authentication

Conditional Access

Passwordless authentication

Conditional Access administrator privileges

Microsoft Defender for Cloud Apps

Microsoft Defender for On-Premises Identity Security

Microsoft Defender for Endpoint

Microsoft 365 Defender portal

Find out more about securing Identity with Zero Trust

Zero Trust fundamentals

Endpoints

The modern enterprise has an incredible diversity of endpoints accessing data, but not all these endpoints are managed or even owned by the organization, leading to different device configurations and software patch levels. This creates a massive attack surface.

An end-to-end Zero Trust framework can help you improve endpoint security so you can enable more secure hybrid work and take advantage of device-dependent strategies such as IoT and edge computing.

Endpoint protection involves monitoring and protecting endpoints against cyberthreats. Protected endpoints include desktops, laptops, smartphones, tablet computers, and other devices. Organizations need a comprehensive solution that enables discovery of all endpoints and even network devices, such as routers. Plus, vulnerability management, endpoint protection, and endpoint detection and response (EDR).

Essentials of Zero Trust for endpoints

Register devices with your identity provider

To monitor security and risk across multiple endpoints used by any one person, you need visibility in all devices and access points that may be accessing your resources.

- You can register devices with Microsoft Azure Active Directory (Azure AD) to provide visibility into which devices are accessing your network, as well as the ability to use device health and status information in access decisions.
- Device identities are a prerequisite for scenarios like device-based Conditional Access policies and Mobile Device Management with Microsoft Endpoint Manager.

Enroll devices in Mobile Device Management for internal users

Once data access is granted, being able to control what the user does with your corporate data is critical to mitigating risk.

- Microsoft Endpoint Manager enables endpoint provisioning, configuration, automatic updates, device wipe, and other remote actions.
- You can ensure device and app compliance to control data flow outside trusted mobile apps and devices through mobile app management (MAM) and mobile device management (MDM) policies and set up mobile device management for all internal users.

Ensure compliance before granting access

Once you have identity for all the endpoints accessing corporate resources—and before access is granted—ensure that they meet the minimum security requirements set by your organization.

- Microsoft Endpoint Manager can help you set compliance rules to ensure that devices meet minimum-security requirements before access is granted.
- You can ensure device and app compliance to control data flow outside trusted mobile apps and devices through mobile app management (MAM) and mobile device management (MDM) policies.

Enable access for unmanaged devices as needed

Enabling your employees to access appropriate resources from unmanaged devices can be critical to maintaining productivity. However, it's still imperative to protect your data.

- Microsoft Intune Mobile Application Management lets you publish, push, configure, secure, monitor, and update mobile apps for your users, ensuring they have access to the apps they need to do their work.
- To configure access for unmanaged devices, Intune app protection encrypts "corporate" data before it is shared outside the app. You can validate this by attempting to open the "corporate" file outside of the managed app. The file should be encrypted and unable to be opened outside the managed app.

Enroll devices in Mobile Device Management for external users

Enrolling devices from external users (such as contractors, vendors, partners, etc.) into your MDM solution is a great way to help protect your data and ensure users have the access they need to do their work.

- Microsoft Endpoint Manager provides endpoint provisioning, configuration, automatic updates, device wipe, and other remote actions.
- Mobile Device Management with Intune helps you secure endpoints for external users or otherwise unmanaged devices.

Enforce data loss prevention policies on your devices

Once data access is granted, controlling what the user can do with your data is critical. For example, if a user accesses a document with a corporate identity, mechanisms should be in place to prevent saving that document in an unprotected location or sharing it with a consumer communication or chat app.

- Intune app protection policies help protect data with or without enrolling devices in a device management solution by restricting access to company resources and keep data within the purview of your IT department.
- App protection policies can be configured for apps that run on devices that are enrolled in Microsoft Intune or enrolled in a third-party mobile device management (MDM) solution (these are typically corporate owned).
- App protection policies can also be configured for apps that run on devices not enrolled in any mobile device management solution. (These devices are typically employee-owned devices that aren't managed or enrolled through Intune or other MDM solutions).

Enable real-time device risk evaluation

Once you've enrolled devices with your identity provider, you can bring that signal into your access decisions to allow only safe and compliant devices access.

- Through integration with Azure AD, Microsoft Endpoint Manager enables you to enforce more granular access decisions and fine-tune the Conditional Access policies based on your organization's risk appetite. For example, you can exclude certain device platforms from accessing specific apps.

Learn more about Endpoint Security

Configure and manage device identity in Azure AD

Microsoft Endpoint Manager

Mobile Device Management in Intune

Intune app protection policies

Conditional Access policies

Find out more about securing Endpoints with Zero Trust

Zero Trust fundamentals

Network

We are no longer in an era of clearly defined network specific to a certain location. Instead of a contained and defined network to secure, there is a vast portfolio of devices and networks, all linked by the cloud. Securing this portfolio is challenging for many enterprises, who often have few network security perimeters and a flat, open network, along with minimal threat protection and unencrypted internal traffic.

Adopting a Zero Trust security framework is the key to overcoming these limitations. Instead of believing everything behind the corporate firewall is safe, an end-to-end Zero Trust framework assumes breaches are inevitable. That means you must verify each request as if it originates from an uncontrolled network.

In the Zero Trust framework, there are three key objectives when it comes to securing your network:

- Be ready to handle attacks before they happen.
- Minimize the extent of the damage and how fast it spreads.
- Increase the difficulty of compromising your cloud footprint.

Preventing data breaches and other network security threats is about hardened network protection. Without proper security protocols, your business is at high risk for advanced attacks.

Zero Trust is a framework that assumes a complex network's security is always at risk to external and internal threats. A Zero Trust architecture assumes that every connection and endpoint is considered a threat. The framework protects against these threats, whether external or internal.

Essentials of Zero Trust for networks

Use a cloud workload protection solution

Having a comprehensive view across all your cloud workloads is critical to keeping your resources safe in a highly distributed environment.

- Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers and provides advanced threat protection across your hybrid workloads.
- With the Azure Security Center, you can identify and track vulnerabilities, harden resources and services with the Azure Security Benchmark, and detect and resolve threats to resources, workloads, and services.
- The central feature that enables you to achieve those goals is secure score. Azure Security Center continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.

Assign app identity

Assigning an app identity is critical to securing communication between different services.

- Azure supports managed identity from Azure Active Directory, making it easy access other Azure AD-protected resources such as Azure Key Vault used to store secrets and credentials.
- Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Applications may use the managed identity to obtain Azure AD tokens. For example, an application may use a managed identity to access resources like Azure Key Vault, where developers can store credentials in a secure manner, or to access storage accounts.
- You can use managed identities to authenticate to any resource that supports Azure Active Directory authentication including your own applications. You don't need to manage credentials. Credentials are not even accessible to you and managed identities can be used without any additional cost.

Segment user and resource access

Segmenting access for each workload helps prevent network-based breaches.

- Microsoft Azure offers many ways to segment workloads to manage user and resource access. Within Azure, you can isolate resources at the subscription level with Virtual networks (VNets), VNet peering rules, Network Security Groups (NSGs), Application Security Groups (ASGs), and Azure Firewalls. You can create an Azure Virtual Network to help your Azure resources communicate together securely.
- Choose the right network segmentation approach for your organization. Common patterns include:
  - Single Virtual Network: In this pattern, all the components of your workload or, in some cases, your entire IT footprint is put inside a single virtual network. This pattern is possible if you're operating solely in a single region since a virtual network can't span multiple regions.
  - Multiple Virtual Networks with peering: This pattern is an extension of the previous pattern where you have multiple virtual networks with potential peering connections. You might opt for this pattern to group applications into separate virtual networks or if you need presence in multiple Azure regions.
  - Multiple Virtual Networks in a hub-and-spoke model: This pattern is a more advanced virtual network organization where you choose a virtual network in a given region as the hub for all the other virtual networks in that region. The connectivity between the hub virtual network and its spokes of other virtual networks is achieved by using Azure virtual network peering. All traffic passes through the hub virtual network, and it can act as a gateway to other hubs in different regions.

Implement threat detection tools

Preventing, detecting, investigating, and responding to advanced threats across your hybrid infrastructure will help improve your security posture.

- Microsoft Defender for Endpoint Advanced Threat Protection is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
- Defender for Endpoint uses a combination of technology including endpoint behavioral sensors, cloud security analytics, and threat intelligence.
- Built-in threat and vulnerability management uses a risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations.

Deploy a Security Information and Event Management solution

As the value of digital information continues to increase, so do the number and sophistication of attacks. Security Information and Event Management (SIEM) solutions provide a central way to mitigate threats across the entire estate.

- Microsoft Sentinel is a cloud-native SIEM and security orchestration automated response (SOAR) solution that will allow your Security Operations Center (SOC) to work from a single pane of glass to monitor security events across your enterprise.
- Microsoft Sentinel aggregates data from all sources, including users, applications, servers, and devices running on-premises or in any cloud, letting you reason over millions of records in a few seconds. It includes built-in connectors for easy onboarding of popular security solutions. Collect data from any source with support for open standard formats like CEF and Syslog.
- Microsoft Sentinel integrates with many enterprise tools, including best-of-breed security products, homegrown tools, and other systems like ServiceNow. It provides an extensible architecture to support custom collectors through REST API and advanced queries. It enables you to bring your own insights, tailored detections, machine learning models, and threat intelligence.

Implement behavioral analytics

When you create new infrastructure, you need to ensure that you also establish rules for monitoring and raising alerts. This is key for identifying when a resource is displaying unexpected behavior.

- Microsoft Defender for Identity enables signal collection to identify, detect, and investigate advanced threats, compromised identity, and malicious insider actions directed at your organization.
- Microsoft Defender for Identity helps eliminate on-premises vulnerabilities to prevent attacks before they happen, helps security operations teams use their time effectively by understanding the greatest threats, and prioritize information to focus on actual threats, not false signals.

Set up automated investigations

Security operations teams face challenges in addressing the multitude of alerts that arise from the never-ending flow of threats. Implementing a solution with automated investigation and remediation (AIR) capabilities can help your security operations team address threats more efficiently and effectively.

- Microsoft Defender for Endpoint Advanced Threat Protection includes automated investigation and remediation capabilities, which can significantly reduce alert volume, allowing security operations to focus on more sophisticated threats and other high-value initiatives.
- The technology in automated investigation uses various inspection algorithms and is based on processes that are used by security analysts. AIR capabilities are designed to examine alerts and take immediate action to resolve breaches. AIR capabilities significantly reduce alert volume, allowing security operations to focus on more sophisticated threats and other high-value initiatives.
- All remediation actions, whether pending or completed, are tracked in the Action center. The Action center is where pending actions are approved (or rejected) and completed actions can be undone if needed.

Govern access to privileged resources

Personnel should use administrative access sparingly. When users require administrative functions, they should receive temporary administrative access, based on the principle of just-in-time network access.

- Privileged Identity Management (PIM) in Azure AD enables you to discover, restrict, and monitor access rights for privileged identity. PIM can help ensure your admin accounts stay secure by limiting access to critical operations using just-in-time, time-bound, and role-based access control.
- Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources.
- With PIM, organizations can give users just-in-time privileged access to Azure and Azure AD resources and can oversee what those users are doing with their privileged access.

Learn more about solutions for a Zero Trust network

Azure Security Center

Managed identities

Azure Virtual Network

Microsoft Defender for Endpoint Advanced Threat Protection

Microsoft Sentinel

Microsoft Defender for Identity

Automated investigations

Privileged Identity Management (PIM)

Find out more about securing Networks with Zero Trust

Zero Trust fundamentals

Data

With more people working outside the office and the growth in cloud apps and analytics, organizations need new tools for protecting data as it travels beyond perimeters of control. Zero Trust enables you to protect data at rest and in flight even when it leaves the endpoints, apps, infrastructure, and network that make up your organization's own IT infrastructure.

To ensure protection and restrict data access to authorized users, data should be inventoried, classified, labeled, and, where appropriate, encrypted. This requires you to know what data you have, protect it from unauthorized access and loss, and continuously monitor sensitive information for policy violations and risky behavior.

According to the 2021 Cost of a Data Breach report, organizations that have not deployed a Zero Trust program faced data breach costs averaging $5.04 million. Those that were Zero Trust "mature" saw those costs decrease by $1.76 million. Even those firms in the "early stage" of deployment had $660,000 less of a burden. In short, Zero Trust can mitigate the impact of a breach.

Essentials of Zero Trust for data

» Define a classification taxonomy

Defining the right label taxonomy and protection policies is the most critical step in any data protection strategy, so start with creating a labeling strategy that reflects your organization's sensitivity requirements for information.

- You can evaluate and then tag content in your organization in order to control where it goes, protect it no matter where it is and to ensure that it is preserved and deleted according to your organization's needs. You do this through the application of sensitivity labels, retention labels, and sensitive information type classification.
- Data classification will scan your sensitive content and labeled content before you create any policies. This is called zero change management. This lets you see the impact that all the retention and sensitivity labels are having in your environment and empower you to start assessing your protection and governance policy needs.
- Sensitivity labels from the Microsoft Information Protection solution let you classify and protect your organization's data, while making sure that user productivity and their ability to collaborate isn't hindered.

Govern access decisions based on sensitivity

The more sensitive the data, the greater the protection control and enforcement needed. Similarly, the controls should also be commensurate with the nature of the risks associated with how and from where the data is accessed. Some sensitive data needs protection by policies that enforce encryption to ensure only authorized users can access the data.

- Microsoft Information Protection offers a flexible set of protection controls based on data sensitivity and risk.
- You can configure and manage policies and view analytics across your on-premises environment, Microsoft 365 apps and services, third-party cloud services, and devices—all from a single console. You can also accurately identify sensitive information across your enterprise with comprehensive classification capabilities, including machine learning, and consistently extend protection and governance to popular third-party apps and services with SDK and connectors.
- Azure Purview provides a unified data governance service that builds on Microsoft Information Protection. You can create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. This helps data consumers find valuable, trustworthy data.

Implement a robust data classification and labeling strategy

Enterprises have vast amounts of data that can be challenging to label and classify. Using machine learning for smarter, automated classification can help reduce the burden on end users and lead to a more consistent labeling experience.

- Microsoft 365 provides three ways to classify content, including manually, automated pattern matching, and Trainable classifiers. Trainable classifiers are well-suited to content that isn't easily identified by manual or automated pattern matching methods. You can use it to identify items for application of Office sensitivity labels, Communications compliance policies, and retention label policies.
- For on-premises file repositories and sites based on SharePoint 2013 or later, Azure Information Protection (AIP) scanner can help discover, classify, label, and protect sensitive information. The AIP scanner can inspect any files that Windows can index. If you've configured sensitivity labels to apply automatic classification, the scanner can label discovered files to apply that classification, and optionally apply or remove protection.
- Configure the scanner to use enforce mode and automatically classify, label, and protect files with sensitive data.

Govern access decisions based on policy

Move beyond simple access/block decisions and tailor access decisions for your data based on risk appetite—such as allowing access, blocking, limiting access, or requiring additional proofs like multi-factor authentication.

- Conditional Access in Azure AD enables you to enforce fine-tuned adaptive access controls, such as requiring multi-factor authentication, based upon user context, device, location, and session risk information to control what a specific user can access, and how and when they have access.
- Control Access enforces controls to specific apps or actions, secures remote access to on-premises web apps, and restricts access to approved, modern authentication-capable client apps.
- Microsoft Defender for Cloud Apps lets you apply Azure Information Protection classification labels automatically, with or without protection, to files as a file policy governance action. You can also investigate files by filtering for the applied classification label within the Defender for Cloud Apps portal. Using classifications enables greater visibility and control of your sensitive data in the cloud.

Enforce access and usage rights to data shared outside company boundaries

To properly mitigate risk without negatively impacting productivity, you need to control and secure email, documents, and sensitive data you share outside your company.

- Azure Information Protection helps secure email, documents, and sensitive data inside and outside your company walls. From easy classification to embedded labels and permissions, always enhance data protection with Azure Information Protection, no matter where it's stored or who it's shared with.
- Deployment guides will help you understand how to each solution features complement each, best practices based on the CxE teams experience with customer roadblocks, considerations to take and research before starting your deployment, and offer resources links to additional readings and topics to gain a deeper understanding and an appendix for additional information on licensing.
- App Discovery policies make it easier to keep track of the significant discovered applications in your organization to help you manage these applications efficiently. Create policies to receive alerts when detecting new apps that are identified as either risky, non-compliant, trending, or high-volume.

Implement data loss prevention policies

To comply with business standards and industry regulations, organizations must protect sensitive information and prevent its inadvertent disclosure. Sensitive information can include financial data or personally identifiable information such as credit card numbers, social security numbers, or health records.

- Use a range of data loss prevention policies (DLP) in Microsoft 365 to identify, monitor, and automatically protect sensitive items across services such as Teams, SharePoint, and OneDrive, Office apps such as Word, Excel, and PowerPoint, Windows 10 endpoints, third-party cloud apps, on-premises file shares.
- You can tune your rules by adjusting the instance count and match accuracy to make it harder or easier for content to match the rules. Each sensitive information type used in a rule has both an instance count and match accuracy.

Learn more about solutions for Zero Trust data security

Data classification

Sensitivity labels

Microsoft Information Protection

Automated pattern matching

Trainable classifiers

Azure Information Protection (AIP) scanner

Labeling deployment guidance

Conditional Access in Azure AD

Integrate Azure Information Protection

Protection and Compliance Deployment Acceleration Guides

DLP policies

Find out more about securing Data with Zero Trust

Zero Trust fundamentals

Applications

To get the full benefit of cloud apps and services, organizations must simultaneously simplify access and maintain control. A Zero Trust framework helps you do both.

Using a Zero Trust framework, your organization can help ensure that apps, and the data they contain, are protected by:

- Applying controls and technologies to discover Shadow IT.
- Ensuring appropriate in-app permissions.
- Limiting access based on real-time analytics.
- Monitoring for abnormal behavior.
- Controlling user actions.
- Validating secure configuration options.

With applications now consumed from the cloud and mobile devices, the application attack surface has expanded considerably. Therefore, implementing Zero Trust for applications requires modern threat detection capabilities that cover applications across various devices and locations, including the cloud.

Essentials of Zero Trust application security

Enforce policy-based access control for your applications

Move beyond simple access/block decisions and tailor decisions based on risk appetite—such as allowing access, blocking, limiting access, or requiring additional proofs like multi-factor authentication.

- Conditional Access in Azure AD enables you to enforce fine-tuned adaptive access controls, such as requiring multi-factor authentication, based upon user context, device, location, and session risk information.
- With Conditional Access, organizations can restrict access to approved (modern authentication-capable) client apps with Intune app protection policies. For older client apps that may not support app protection policies, administrators can restrict access to approved client apps.

Enforce policy-based session controls

Stopping breaches and leaks in real time before employees intentionally or inadvertently put data and organizations at risk is key to mitigating risk after access is granted. It's also critical for businesses to enable employees to securely use their own devices.

- Microsoft Defender for Cloud Apps integrates with Azure Active Directory (Azure AD) Conditional Access so you can configure apps to work with Conditional Access App Control. Microsoft Defender for Cloud Apps allows you to selectively enforce access and session controls on your organization's apps based on any condition, such as preventing data exfiltration, protecting on download, preventing uploads, blocking malware, and more.
- Microsoft Defender for Cloud Apps session policies enable real-time session-level monitoring, affording you granular visibility into cloud apps and the ability to take different actions depending on the policy you set for a user session. Instead of allowing or blocking access completely, with session control you can allow access while monitoring the session and/or limit specific session activities using the reverse proxy capabilities of Conditional Access App Control.

Connect your business applications to your cloud application security broker (CASB)

Visibility across apps and platforms is critical for performing governance actions, such as quarantining files or suspending users, as well as mitigating any flagged risk.

- Apps connected to Microsoft Defender for Cloud Apps get instant, out-of-the-box protection with built-in anomaly detection. Microsoft Defender for Cloud Apps uses entity and user behavioral analytics (UEBA) and machine learning to detect unusual behavior and identify threats.
- Once an app is connected using one or more of these methods, you get instant out-of-the-box protection with our built-in anomaly detection engine. Additionally, you gain deep visibility into the app's user and device activities, control over data shared by the app, and can build detection policies with governance to mitigate any risky activities or sensitive-data sharing by the app.
- Defender for Cloud Apps supports multiple instances of the same connected app. For example, if you have more than one instance of Salesforce (one for sales, one for marketing) you can connect both to Defender for Cloud Apps. You can manage the different instances from the same console to create granular policies and deeper investigation. This support applies only to API-connected apps, not to Cloud Discovered apps or Proxy connected apps.

Provide remote access to on-premises applications through an app proxy

Providing users with secure remote access to internal apps running on an on-premises server is critical to maintaining productivity today.

- Azure AD Application Proxy provides secure remote access to on-premises web apps without a VPN or dual-homed servers and firewall rules. It enables users to access web apps through SSO while enabling IT to configure Conditional Access policies for fine-tuned access control.
- The Azure AD Application Proxy feature can be implemented by IT professionals who want to publish on-premises web applications externally. Remote users who need access to internal apps can then access them in a secure manner.
- Azure AD keeps track of users who need to access web apps published on-premises and in the cloud. It provides a central management point for those apps. While not required, it's recommended you also enable Azure AD Conditional Access. By defining conditions for how users authenticate and gain access, you further ensure the right people have access to applications.

Discover and manage shadow IT in your network

The total number of apps accessed by employees in the average enterprise exceeds 1,500, with fewer than 15 percent managed by IT. As remote work becomes a reality, it's no longer enough to apply access policies only to your network appliances.

- Microsoft Defender for Cloud Apps can help you discover which apps are being used, explore the risk of these apps, configure policies to identify new risky apps being used, and unsanction these apps to block them natively using your proxy or firewall appliance.
- Integrating Defender for Cloud Apps with Microsoft Defender for Endpoint gives you the ability to use Cloud Discovery beyond your corporate network or secure web gateways. With the combined user and device information, you can identify risky users or devices, see what apps they are using, and investigate further in the Defender for Endpoint portal.
- Cloud Discovery analyzes traffic logs collected by Defender for Endpoint and assesses identified apps against the cloud app catalog to provide compliance and security information. By configuring Cloud Discovery, you gain visibility into cloud use, Shadow IT, and continuous monitoring of the unsanctioned apps being used by your users.
- App Discovery policies make it easier to keep track of the significant discovered applications in your organization to help you manage these applications efficiently. Create policies to receive alerts when detecting new apps that are identified as either risky, non-compliant, trending, or high-volume.
- Defender for Cloud Apps provides you with the ability to investigate and monitor the app permissions your users granted. You can use this information to identify a potentially suspicious app and, if you determine that it is risky, you can ban access to it.

Minimize virtual machine access

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

- Lock down inbound traffic to your Azure Virtual Machines with Azure Security Center's JIT virtual machine (VM) access feature to reduce your exposure to attacks while providing easy access when you need to connect to a VM.
- With JIT, you can lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed. When you enable just-in-time VM access, you can select the ports on the VM where inbound traffic will be blocked. Defender for Cloud ensures "deny all inbound traffic" rules exist for your selected ports in the network security group (NSG) and Azure Firewall rules. These rules restrict access to your Azure VMs' management ports and defend them from attack.

Learn more Zero Trust security for Applications

Conditional Access in Azure AD

Configuring Conditional Access

Microsoft Defender for Cloud Apps

Apps connected to Microsoft Defender for Cloud Apps

Azure AD Application Proxy

Defender for Cloud Apps Best Practices

Find out more about securing Applications with Zero Trust

Zero Trust fundamentals

Infrastructure

IT infrastructure includes a diverse range of technologies, including hardware, virtual machines, software, microservices, networking, and more.

Many organizations struggle to protect this environment because they manually manage permissions across environments and lack effective configuration management of virtual machines and servers. Implementing an end-to-end Zero Trust framework makes it easier for you to:

- Ensure software and services are up to date.
- Manage configurations.
- Prevent, detect, and mitigate attacks.
- Identify and block risky behavior.

Because networks are subject to continuous and increasingly sophisticated attacks, it is especially important to protect your network infrastructure with security solutions that intelligently recognize known and unknown threats and adapt to prevent them in real time.

Essentials of Zero Trust infrastructure

Use a cloud workload protection solution

Having a comprehensive view across all your cloud workloads is critical to keeping your resources safe in a highly distributed environment.

- Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers and provides advanced threat protection across your hybrid workloads.
- With the Azure Security Center, you can identify and track vulnerabilities, harden resources and services with the Azure Security Benchmark, and detect and resolve threats to resources, workloads, and services.
- The central feature that enables you to achieve those goals is Secure Score. Azure Security Center continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.

Assign app identity

Assigning an app identity is critical to securing communication between different services.

- Azure supports managed identity from Azure Active Directory, making it easy access other Azure AD-protected resources such as Azure Key Vault used to store secrets and credentials.
- Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Applications may use the managed identity to obtain Azure AD tokens. For example, an application may use a managed identity to access resources like Azure Key Vault, where developers can store credentials in a secure manner, or to access storage accounts.
- You can use managed identities to authenticate to any resource that supports Azure Active Directory authentication including your own applications. You don't need to manage credentials. Credentials are not even accessible to you and managed identities can be used without any additional cost.

Segment user and resource access

Segmenting access for each workload helps prevent network-based breaches.

- Microsoft Azure offers many ways to segment workloads to manage user and resource access. Within Azure, you can isolate resources at the subscription level with Virtual networks (VNets), VNet peering rules, Network Security Groups (NSGs), Application Security Groups (ASGs), and Azure Firewalls. You can create an Azure Virtual Network to help your Azure resources communicate together securely.
- Choose the right network segmentation approach for your organization. Common patterns include:
  - Single Virtual Network: In this pattern, all the components of your workload or, in some cases, your entire IT footprint is put inside a single virtual network. This pattern is possible if you're operating solely in a single region since a virtual network can't span multiple regions.
  - Multiple Virtual Networks with peering: This pattern is an extension of the previous pattern where you have multiple virtual networks with potential peering connections. You might opt for this pattern to group applications into separate virtual networks or if you need presence in multiple Azure regions.
  - Multiple Virtual Networks in a hub-and-spoke model: This pattern is a more advanced virtual network organization where you choose a virtual network in a given region as the hub for all the other virtual networks in that region. The connectivity between the hub virtual network and its spokes of other virtual networks is achieved by using Azure virtual network peering. All traffic passes through the hub virtual network, and it can act as a gateway to other hubs in different regions.

Implement threat detection tools

Preventing, detecting, investigating, and responding to advanced threats across your hybrid infrastructure will help improve your security posture.

- Microsoft Defender for Endpoint Advanced Threat Protection is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
- Defender for Endpoint uses a combination of technology including endpoint behavioral sensors, cloud security analytics, and threat intelligence.
- Built-in threat and vulnerability management uses a risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations.

Deploy a Security Information and Event Management solution

As the value of digital information continues to increase, so do the number and sophistication of attacks. Security information event management (SIEM) solutions provide a central way to mitigate threats across the entire estate.

- Microsoft Sentinel is a cloud-native SIEM and security orchestration automated response (SOAR) solution that will allow your Security Operations Center (SOC) to work from a single pane of glass to monitor security events across your enterprise.
- Microsoft Sentinel aggregates data from all sources, including users, applications, servers, and devices running on-premises or in any cloud, letting you reason over millions of records in a few seconds. It includes built-in connectors for easy onboarding of popular security solutions. Collect data from any source with support for open standard formats like CEF and Syslog.
- Microsoft Sentinel integrates with many enterprise tools, including best-of-breed security products, homegrown tools, and other systems like ServiceNow. It provides an extensible architecture to support custom collectors through REST API and advanced queries. It enables you to bring your own insights, tailored detections, machine learning models, and threat intelligence.

Implement behavioral analytics

When you create new infrastructure, you need to ensure that you also establish rules for monitoring and raising alerts. This is key for identifying when a resource is displaying unexpected behavior.

- Microsoft Defender for Identity enables signal collection to identify, detect, and investigate advanced threats, compromised identity, and malicious insider actions directed at your organization.
- Microsoft Defender for Identity helps eliminate on-premises vulnerabilities to prevent attacks before they happen, helps security operations teams use their time effectively by understanding the greatest threats, and prioritize information to focus on actual threats, not false signals.

Set up automated investigations

Security operations teams face challenges in addressing the multitude of alerts that arise from the never-ending flow of threats. Implementing a solution with automated investigation and remediation (AIR) capabilities can help your security operations team address threats more efficiently and effectively.

- Microsoft Defender for Endpoint Advanced Threat Protection includes automated investigation and remediation capabilities, which can significantly reduce alert volume, allowing security operations to focus on more sophisticated threats and other high-value initiatives.
- The technology in automated investigation uses various inspection algorithms and is based on processes that are used by security analysts. AIR capabilities are designed to examine alerts and take immediate action to resolve breaches. AIR capabilities significantly reduce alert volume, allowing security operations to focus on more sophisticated threats and other high-value initiatives.
- All remediation actions, whether pending or completed, are tracked in the Action center. The Action center is where pending actions are approved (or rejected) and completed actions can be undone if needed.

Govern access to privileged resources

Personnel should use administrative access sparingly. When users require administrative functions, they should receive temporary administrative access, based on the principle of just-in-time network access.

- Privileged Identity Management (PIM) in Azure AD enables you to discover, restrict, and monitor access rights for privileged identity. PIM can help ensure your admin accounts stay secure by limiting access to critical operations using just-in-time, time-bound, and role-based access control.
- Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources.
- With PIM, organizations can give users just-in-time privileged access to Azure and Azure AD resources and can oversee what those users are doing with their privileged access.

Learn more about solutions for Zero Trust infrastructure

Azure Security Center

Managed identities

Microsoft Defender for Endpoint
Advanced Threat Protection

Microsoft Sentinel

Microsoft Defender for Identity

Automated investigations

Privileged Identity Management (PIM)

Find out more about securing Infrastructure with Zero Trust

Making Zero Trust a reality with help from Microsoft

Microsoft advocates for Zero Trust in part because the framework has increased security and efficiency throughout the company's own environment. Based on that experience, Microsoft builds Zero Trust capabilities that integrate with and expand on its technology solutions, such as granular access controls, network isolation by design, and AI-based detection of suspicious access attempts. In addition, Microsoft security features and services are designed to work together, helping IT teams simplify the adoption and ongoing management of their security technology stack.

Most importantly, Microsoft recognizes that Zero Trust is a journey, not a destination. Because it has implications for every aspect of IT security, it can seem overwhelming at first. A phased approach targeting high-impact, low-effort areas first can lead to rapid improvements and clarify which steps to take next. You can build a larger strategy as you go. The important thing is to get started.

Successfully implementing Zero Trust can help improve security in a world where work relies on devices, apps, and data outside perimeter-based controls. It helps reduce the risk of data breaches and keep your business operating 24/7.

Discover how Microsoft technology and guidance can help you implement the Zero Trust framework.

Learn more >

Microsoft