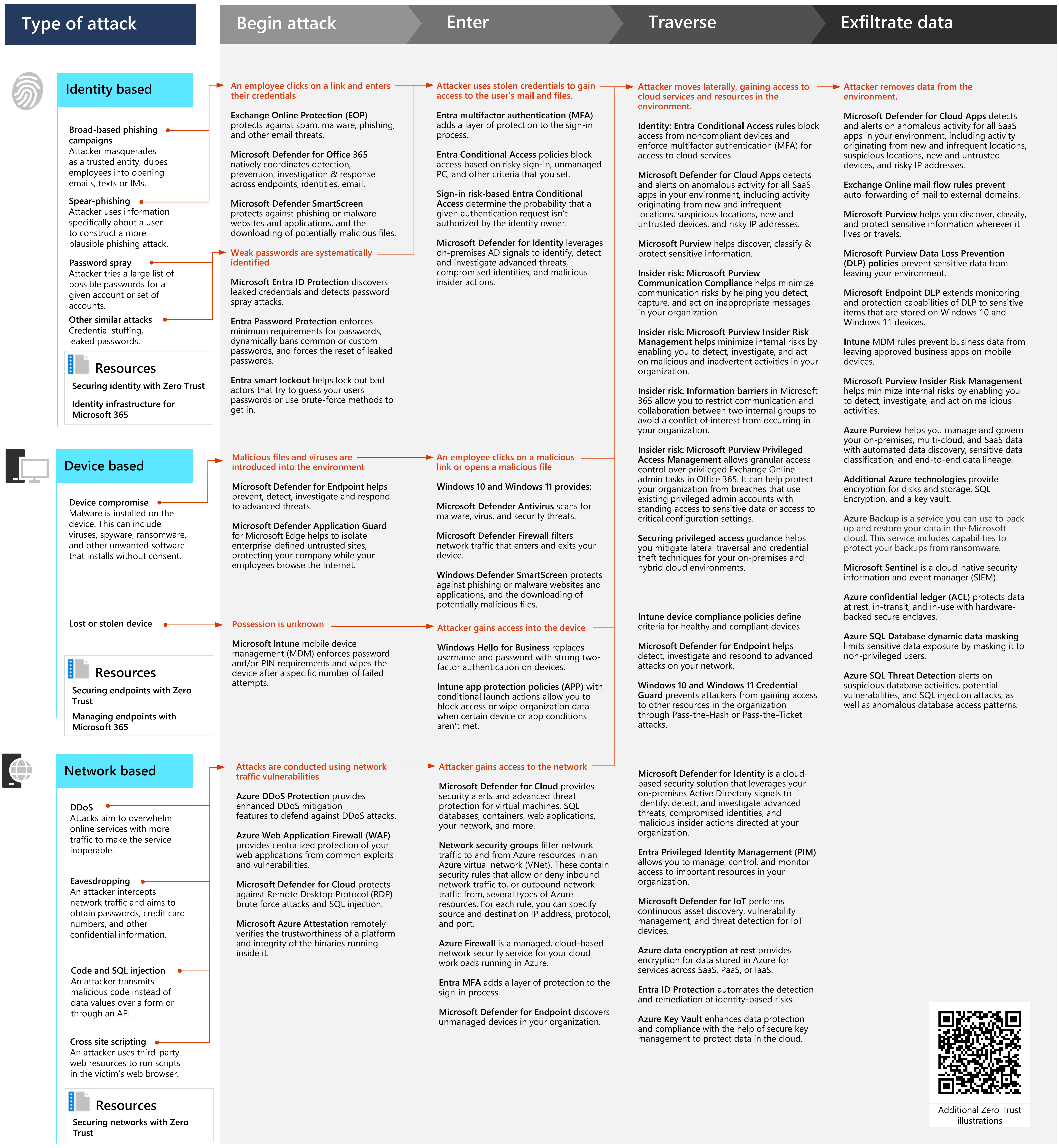
Common attacks and how Microsoft capabilities for Zero Trust can protect your organization

Zero Trust is a security strategy and approach for designing and implementing the principles of verify explicitly, use least privilege access, and assume breach. Instead of believing everything behind the corporate firewall is safe, Zero Trust principles assume a breach and verifies each request as though it originated from an uncontrolled network.

Zero Trust capabilities in Microsoft's cloud platforms provide proactive protection against the phases of the most common types of cyberattacks.

Resources

Zero Trust Guidance Center



Type of attack | Begin attack | Enter | Traverse | Exfiltrate data

Identity based

Broad-based phishing campaigns
Attacker masquerades as a trusted entity, dupes employees into opening emails, texts or IMs.

Spear-phishing
Attacker uses information specifically about a user to construct a more plausible phishing attack.

Password spray
Attacker tries a large list of possible passwords for a given account or set of accounts.

Other similar attacks
Credential stuffing, leaked passwords.

Resources

Securing identity with Zero Trust

Identity infrastructure for Microsoft 365

Begin attack

An employee clicks on a link and enters their credentials

Exchange Online Protection (EOP) protects against spam, malware, phishing, and other email threats.

Microsoft Defender for Office 365 natively coordinates detection, prevention, investigation & response across endpoints, identities, email.

Microsoft Defender SmartScreen protects against phishing or malware websites and applications, and the downloading of potentially malicious files.

Weak passwords are systematically identified

Microsoft Entra ID Protection discovers leaked credentials and detects password spray attacks.

Entra Password Protection enforces minimum requirements for passwords, dynamically bans common or custom passwords, and forces the reset of leaked passwords.

Entra smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in.

Enter

Attacker uses stolen credentials to gain access to the user's mail and files.

Entra multifactor authentication (MFA) adds a layer of protection to the sign-in process.

Entra Conditional Access policies block access based on risky sign-in, unmanaged PC, and other criteria that you set.

Sign-in risk-based Entra Conditional Access determine the probability that a given authentication request isn't authorized by the identity owner.

Microsoft Defender for Identity leverages on-premises AD signals to identify, detect and investigate advanced threats, compromised identities, and malicious insider actions.

Traverse

Attacker moves laterally, gaining access to cloud services and resources in the environment.

Identity: Entra Conditional Access rules block access from noncompliant devices and enforce multifactor authentication (MFA) for access to cloud services.

Microsoft Defender for Cloud Apps detects and alerts on anomalous activity for all SaaS apps in your environment, including activity originating from new and infrequent locations, suspicious locations, new and untrusted devices, and risky IP addresses.

Microsoft Purview helps discover, classify & protect sensitive information.

Insider risk: Microsoft Purview Communication Compliance helps minimize communication risks by helping you detect, capture, and act on inappropriate messages in your organization.

Insider risk: Microsoft Purview Insider Risk Management helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization.

Insider risk: Information barriers in Microsoft 365 allow you to restrict communication and collaboration between two internal groups to avoid a conflict of interest from occurring in your organization.

Insider risk: Microsoft Purview Privileged Access Management allows granular access control over privileged Exchange Online admin tasks in Office 365. It can help protect your organization from breaches that use existing privileged admin accounts with standing access to sensitive data or access to critical configuration settings.

Securing privileged access guidance helps you mitigate lateral traversal and credential theft techniques for your on-premises and hybrid cloud environments.

Exfiltrate data

Attacker removes data from the environment.

Microsoft Defender for Cloud Apps detects and alerts on anomalous activity for all SaaS apps in your environment, including activity originating from new and infrequent locations, suspicious locations, new and untrusted devices, and risky IP addresses.

Exchange Online mail flow rules prevent auto-forwarding of mail to external domains.

Microsoft Purview helps you discover, classify, and protect sensitive information wherever it lives or travels.

Microsoft Purview Data Loss Prevention (DLP) policies prevent sensitive data from leaving your environment.

Microsoft Endpoint DLP extends monitoring and protection capabilities of DLP to sensitive items that are stored on Windows 10 and Windows 11 devices.

Intune MDM rules prevent business data from leaving approved business apps on mobile devices.

Microsoft Purview Insider Risk Management helps minimize internal risks by enabling you to detect, investigate, and act on malicious activities.

Azure Purview helps you manage and govern your on-premises, multi-cloud, and SaaS data with automated data discovery, sensitive data classification, and end-to-end data lineage.

Additional Azure technologies provide encryption for disks and storage, SQL Encryption, and a key vault.

Azure Backup is a service you can use to back up and restore your data in the Microsoft cloud. This service includes capabilities to protect your backups from ransomware.

Microsoft Sentinel is a cloud-native security information and event manager (SIEM).

Azure confidential ledger (ACL) protects data at rest, in-transit, and in-use with hardware-backed secure enclaves.

Azure SQL Database dynamic data masking limits sensitive data exposure by masking it to non-privileged users.

Azure SQL Threat Detection alerts on suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns.

Device based

Device compromise
Malware is installed on the device. This can include viruses, spyware, ransomware, and other unwanted software that installs without consent.

Lost or stolen device

Resources

Securing endpoints with Zero Trust

Managing endpoints with Microsoft 365

Begin attack

Malicious files and viruses are introduced into the environment

Microsoft Defender for Endpoint helps prevent, detect, investigate and respond to advanced threats.

Microsoft Defender Application Guard for Microsoft Edge helps to isolate enterprise-defined untrusted sites, protecting your company while your employees browse the Internet.

Possession is unknown

Microsoft Intune mobile device management (MDM) enforces password and/or PIN requirements and wipes the device after a specific number of failed attempts.

Enter

An employee clicks on a malicious link or opens a malicious file

Windows 10 and Windows 11 provides:

Microsoft Defender Antivirus scans for malware, virus, and security threats.

Microsoft Defender Firewall filters network traffic that enters and exits your device.

Windows Defender SmartScreen protects against phishing or malware websites and applications, and the downloading of potentially malicious files.

Attacker gains access into the device

Windows Hello for Business replaces username and password with strong two-factor authentication on devices.

Intune app protection policies (APP) with conditional launch actions allow you to block access or wipe organization data when certain device or app conditions aren't met.

Traverse

Intune device compliance policies define criteria for healthy and compliant devices.

Microsoft Defender for Endpoint helps detect, investigate and respond to advanced attacks on your network.

Windows 10 and Windows 11 Credential Guard prevents attackers from gaining access to other resources in the organization through Pass-the-Hash or Pass-the-Ticket attacks.

Network based

DDoS
Attacks aim to overwhelm online services with more traffic to make the service inoperable.

Eavesdropping
An attacker intercepts network traffic and aims to obtain passwords, credit card numbers, and other confidential information.

Code and SQL injection
An attacker transmits malicious code instead of data values over a form or through an API.

Cross site scripting
An attacker uses third-party web resources to run scripts in the victim's web browser.

Resources

Securing networks with Zero Trust

Begin attack

Attacks are conducted using network traffic vulnerabilities

Azure DDoS Protection provides enhanced DDoS mitigation features to defend against DDoS attacks.

Azure Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities.

Microsoft Defender for Cloud protects against Remote Desktop Protocol (RDP) brute force attacks and SQL injection.

Microsoft Azure Attestation remotely verifies the trustworthiness of a platform and integrity of the binaries running inside it.

Enter

Attacker gains access to the network

Microsoft Defender for Cloud provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, and more.

Network security groups filter network traffic to and from Azure resources in an Azure virtual network (VNet). These contain security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination IP address, protocol, and port.

Azure Firewall is a managed, cloud-based network security service for your cloud workloads running in Azure.

Entra MFA adds a layer of protection to the sign-in process.

Microsoft Defender for Endpoint discovers unmanaged devices in your organization.

Traverse

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Entra Privileged Identity Management (PIM) allows you to manage, control, and monitor access to important resources in your organization.

Microsoft Defender for IoT performs continuous asset discovery, vulnerability management, and threat detection for IoT devices.

Azure data encryption at rest provides encryption for data stored in Azure for services across SaaS, PaaS, or IaaS.

Entra ID Protection automates the detection and remediation of identity-based risks.

Azure Key Vault enhances data protection and compliance with the help of secure key management to protect data in the cloud.

Additional Zero Trust illustrations

Extended detection and response (XDR)

Microsoft XDR solutions deliver intelligent, automated, and integrated security across domains.

These solutions help you connect seemingly disparate alerts and incidents and get ahead of attackers.

Evaluate and pilot Microsoft Defender XDR
aka.ms/defender-xdr-eval

Microsoft Defender XDR

A solution for identities, endpoints, cloud apps, email, and documents. Its built-in self-healing technology fully automates remediation more than 70% of the time.

It combines:

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender Vulnerability Management
- Microsoft Entra ID Protection
- Microsoft Data Loss Prevention
- App Governance

Microsoft Defender for Cloud

Delivers XDR capabilities to protect multi-cloud and hybrid workloads, including virtual machines, databases, containers, and more.

It combines:

- Azure Defender for Servers
- Azure Defender for Storage
- Azure Defender for SQL

Microsoft Sentinel

To gain visibility across your entire environment and include data from other security solutions such as firewalls and existing security tools, connect Microsoft Defender XDR to Microsoft Sentinel, Microsoft's cloud-native SIEM.

Microsoft Sentinel is deeply integrated with Microsoft Defender XDR so you can integrate your XDR data in only a few clicks and combine it with all your security data from across your entire enterprise.

Resources

Microsoft Zero Trust Guidance Center
Prescriptive adoption and deployment guidance to implement a Zero Trust architecture.
docs.microsoft.com/security/zero-trust

Microsoft Security documentation
Technical guidance to help security professionals build and implement cybersecurity strategy, architecture, and prioritized roadmaps.
docs.microsoft.com/security

Microsoft 365 security documentation
docs.microsoft.com/microsoft-365/security

Azure security documentation
docs.microsoft.com/azure/security

Zero Trust documentation for common attacks

Microsoft

A clickable resource in the Zero Trust universe

Click on the following documentation sets and articles to quickly apply Zero Trust principles to your organization or apps.

Technology pillar	Common attacks	Concepts and deployment objectives	Rapid Modernization Plan (RaMP)	Microsoft 365 deployment	Microsoft Azure deployment	Developer guidance	Partner integrations	Zero Trust evaluation
Identities	• Phishing • Password spray • Attacker-in-the-middle (AITM)	✓	✓	✓		✓	✓	✓
Endpoints	• Device compromise • Lost or stolen	✓	✓	✓	✓		✓	✓
Apps	• App consent grant • Compromised or malicious app	✓	✓	✓		✓	✓	✓
Data	• Exfiltration • Encryption • Corruption	✓	✓	✓	✓		✓	✓
Infrastructure	• DoS and DDoS	✓			✓		✓	✓
Network	• Eavesdropping • DNS spoofing	✓	✓		✓		✓	✓
Threat protection		✓		✓	✓		✓	

Click on the following articles to apply Zero Trust principles from C-suite engagement to implementation phases and steps.

Business scenarios in the Zero Trust adoption framework

- Rapidly modernize your security posture
- Secure remote and hybrid work
- Prevent or reduce business damage from a breach
- Identify and protect sensitive business data
- Meet regulatory and compliance requirements

February 2024

To send feedback about this documentation, please write to us at CloudAdopt@microsoft.com.