Microsoft Security

How Strong Identity Management Provides a Foundation for 'Zero Trust' Security

Contents

1 Introduction

Strong identity is one of the foundational pillars of Microsoft's Zero Trust security model, which provides a framework for moving from access control based on implicit trust assumptions to an approach that requires real-time verification of all users, devices, locations, and other signals.

Microsoft 365 E5, which includes Azure Active Directory (Azure AD), is best equipped to deliver a strong identity-management foundation for Zero Trust security.

The ability to connect all cloud and legacy applications to one identity solution helps enterprises gain end-to-end visibility of their digital presence–a critical step in securing the attack surface.

2 Zero Trust overview

Cloud applications and enterprise mobility have redefined the corporate perimeter and are driving the need for a new approach to security that protects applications and data wherever they are located.

The traditional network-perimeter-based security model, in which everything behind the corporate firewall is assumed safe, is obsolete. Corporate applications and data now extend to the public cloud.

Employees need the ability to access and share data wherever they are, using a variety of corporate and personal devices.

Business partners and customers increasingly interact with an organization digitally, further increasing the potential attack surface for bad actors. An attacker who exploits a single, vulnerable endpoint can often gain access to the entire network, moving laterally from one system to another, in search of an organization's crown jewels.

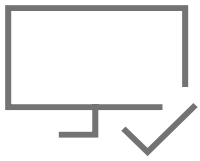
As a result, security policies can no longer be based solely on whether a request originates from inside or outside the corporate perimeter.

Instead of believing everything inside the corporate firewall is safe, the Zero Trust model assumes breach and a "never trust, always verify" access approach. Every request, regardless of whether it originated internally or externally, is strongly authenticated, authorized, and inspected for anomalies. "Least privileged access" principles and micro-segmentation are applied to minimize lateral movement should a breach occur.

In a Zero Trust framework, all users and devices inside and outside the enterprise perimeter are verified in real time.

Every access request is authenticated and authorized based on a multitude of available data points, including user identity, location, device information, data classification, and anomalies. These access policies must strike the proper balance to keep the organization safe yet functional.

Guiding principles of Zero Trust



1

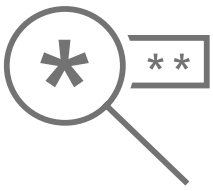
Verify explicitly

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

2

Use least privileged access

Limit user access with Just-In-Time and Just-Enough Access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.



3

Assume breach

Minimize blast radius for breaches and prevent lateral movement by segmenting access by network, user, devices, and application awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility, drive threat detection, and improve defenses.

3 Microsoft 365 provides a foundation for strong identity management

Identity is one of the six foundational pillars of a Zero Trust framework, along with devices, applications, data, infrastructure, and network. Each of these pillars is a source of signal, a control plane for enforcement, and a critical resource to be defended.

Identities–whether they represent people, services, or Internet of Things (IoT) devices–define the Zero Trust control plane. When an identity attempts to access a resource, you need a system that can verify the identity with strong authentication, ensure access is compliant and typical for that identity, and apply principles of least privileged access.

Azure AD, a cloud identity solution included into Microsoft E5, supports strong authentication, access control, identity protection, and policy management requirements for Zero Trust.

Wherever organizations are on their Zero Trust journey, Microsoft 365 E5 can help implement an identity environment featuring cloud identity federation, strong authentication, and Conditional Access at its core.

4 Implementing strong identity

Microsoft recommends four steps for implementing strong identity for a Zero Trust security model:

Multi-factor authentication (MFA)

Policy-based access

Identity protection

Secure access to SaaS and on-premises apps

Multi-factor authentication (MFA)

Password-only authentication mechanisms are no longer sufficient to protect user accounts. Employees and external collaborators connect to enterprise resources from inside and outside the corporate network using a variety of devices, including unmanaged employee-owned smartphones and tablets. In this environment, weak login credentials can provide attackers with easy entry to gain unchallenged access to corporate resources.

MFA adds an additional layer of defense by requiring users to provide two or more forms of authentication to access an account. The forms of authentication can include something the user knows (such as a password), something they have (such as a phone or other trusted device), or something that makes up who they are (such as a fingerprint or other biometric).

Azure AD delivers strong authentication for securing access to business-critical data and applications. Users may be challenged for additional authentication based on contextual data about their login, geolocation, access request, system configuration details, and other signals.

The second-factor authentication methods supported in Azure AD MFA include the following:

- **Microsoft Authenticator App**, available for Android, iOS, and Windows Phone, prevents unauthorized access to applications or services by pushing a notification to smartphones that requires users to verify a legitimate access request.
- **Windows Hello for Business** replaces your passwords with strong two-factor authentication on Windows 10 PCs with credentials tied to your device, as well as a PIN, fingerprint, or facial recognition.
- **FIDO2 security keys** let you sign in without a username or password using an external USB, near-field communication (NFC), or other external security key that supports Fast Identity Online (FIDO) standards.
- **Hardware tokens** can be used to generate a one-time password for authenticating users to apps based on open authentication (OATH) standards.
- **SMS messages** can be sent to a registered device, requiring users to enter a verification code to sign in to an app or service.
- **Automated voice calls** enable users to sign in by pressing the # key on their registered mobile device.
- **Security questions** let users authenticate by answering a set of predefined questions.

Administrators can specify in policy the different authentication methods available to users in specific situations. For example, they can require security questions for self-service password recovery, or a hardware token as a second factor for accessing specific apps. Azure AD Conditional Access, Microsoft's cloud security policy engine, lets administrators determine the policies requiring two-step verification when a specific cloud application is accessed or when sign-in risk is detected.

Strong authentication is so critical to security that Microsoft made MFA available across its solutions and services for free.

All Microsoft customers can enable MFA for free with the Microsoft Authenticator app, and MFA is now enabled as a default for all new Azure AD tenants for Microsoft 365, Office 365, Dynamics, and Azure.

Policy-based access

Organizations need ways to restrict access to applications and systems in certain circumstances, such as gating access to an enterprise application based on signals associated with user and device identity. When user, device, or session risk is detected, access policies can decide whether to block access to a requested resource or request more information, such as MFA, for granting access.

Azure AD Conditional Access can enforce access policies for applications using signals from a variety of different sources, including Azure AD Identity Protection, Microsoft Cloud App Security, and Microsoft Defender for Identity. These signals include user or group identity information, IP location data, device type or state, the kind of application or resource being accessed, and real-time login and session risk data or even GPS location and authentication context. Policies to block or allow access can be targeted to specific groups or users, IP address ranges, specific platforms and applications, and sign-in behavior.

Azure AD Conditional Access enables enforcement of a variety of policy decisions. Common examples include blocking sign-ins involving legacy authentication protocols, access from specific locations, or other high-risk criteria. Other commonly applied

policies include granting access to a requested resource but requiring MFA, or requiring a mobile device to have an approved app or be marked as compliant using Microsoft Endpoint Manager, a cloud-based tool for enterprise mobility management.
For example, Conditional Access can enforce policies that require MFA for systems administrators or for those seeking to perform Azure management tasks.

In addition to enforcing policies for granting or blocking access, Azure AD Conditional Access can enforce session-control policies that limit what users can do with their access.

For example, a Conditional Access policy can limit access to SharePoint and OneDrive content from unmanaged devices. In this scenario, users are given browser-only access to the app with no ability to synch, download, or print files. The goal in supporting policies for limited access is to ensure users have an opportunity to remain productive while minimizing security risks.

Identity protection

A compromised identity credential, even one with low-level privileges, is all hackers need to gain entry into an organization to begin moving laterally, undetected, to gain access to business-critical systems and data. There are countless cases of documented data breaches in which a payload was delivered through a compromised user login and then used to sniff out other username/password combinations, over the course of months or even years, to eventually gain administrator privileges and access to critical systems and data.

To implement strong identity, organizations need a way to rapidly detect compromised identities and proactively prevent them from being misused. Azure AD Identity Protection uses heuristics and adaptive machine learning to detect anomalous behavior and suspicious incidents that indicate potentially compromised identities. It generates alerts and reports that enable administrators to evaluate detected issues and take the appropriate action to remediate or mitigate the issue.

Administrators can configure risk-based policies within Azure AD Identity Protection to automatically respond to detected risks. Policies can be configured to automatically block access when a specified risk threshold has been reached or to require MFA, a password reset, or other adaptive remediation actions. Administrators also can set policies for responding to suspicious user activity or risky sign-ins such as those from an anonymous IP address or unfamiliar location.

Azure AD Identity Protection can proactively detect vulnerabilities that impact user identities, such as users without MFA registration, unmanaged cloud apps, users with unnecessary privileged access, and weak authentication for role activation. Identity Protection also enables timely investigations of detected risks through alerts and notifications and by providing administrators with contextual information on detected risks.

An Identity Protection dashboard provides information on users flagged for risk as well as suspicious and anomalous activity and vulnerabilities.

The dashboard provides access to settings for configuring security policies and MFA registration.

Azure AD supports three directory roles for managing an Identity Protection implementation:

- **A Global Administrator role** with full access to Identity Protection and rights to onboard Identity Protection
- **A Security Administrator role** with full access to Identity Protection but no rights to onboard Identity Protection or to reset user passwords
- **A Directory Reader role** with read-only access and no ability to onboard Identity Protection, configure policies, or reset passwords

Secure access to SaaS and on-premises apps

Organizations need to enable people to access resources securely without impacting their productivity. Having multiple usernames and passwords for different apps and services is a security risk, especially when you don't control access to the app (such as with third-party SaaS apps).

By connecting the sign-in experience for all your apps (on-premises, cloud, and third-party SaaS apps) from any device and managing user directories together, you gain better control and visibility, and simplify user experience. You can reduce the risk posed by multiple credentials for outside apps if they are connected to a single sign-on process. In addition to Microsoft services (Office 365, Azure, Dynamics), Azure AD has an app gallery of thousands of pre-integrated third-party SaaS apps to simplify single sign-on for your users. Plus, you can add your own custom applications easily in the portal.

Azure AD Application Proxy enables organizations to implement secure remote access to on-premises applications so remote users can access them in the same manner they access cloud applications. It does this by externalizing on-premises apps over HTTPS.

By signing in to Azure AD once, users can access both cloud apps and on-premises applications via an external URL or an internal portal.

Azure AD Application Proxy also allows on-premises applications to leverage Azure's security analytics and authorization controls. This makes it easier for organizations to implement the same Conditional Access and MFA policies across cloud apps and internally hosted applications. Because Azure AD Application Proxy is hosted in the cloud, no additional software components or network changes are required to enable remote access to on-premises applications.

Application Proxy also eliminates the need for virtual private networks (VPNs) by serving as a reverse proxy for remote access to on-premises apps. It includes a cloud-based Application Proxy service and a lightweight Application Proxy Connector that runs on a Windows server hosted on-premises.

When a remote user signs into the app with Azure AD, a sign-in token is sent from Azure AD to the user's device, which the Application Proxy uses to authenticate the user.

The token is sent to the connector, which performs additional authentication if needed and connects the user to the requested app (if SSO is enabled). The Application Proxy Connector manages communications between the Application Proxy service and the on-premises application. The Connector only uses outbound connections to communicate with the Proxy Server, so inbound ports need not be opened in the firewall.

Azure AD Application Proxy works with applications hosted behind a Remote Desktop Gateway, with web apps that use Integrated Windows Authentication and APIs that organizations want to expose externally.

As an alternative to Application Proxy, Microsoft also has partnerships with security providers including Akamai, Cisco, Citrix, Datawiza, F5, Fortinet, Kemp, Palo Alto Networks, Perimeter 81, Pulse Secure, Silverfort, Strata, and Zscaler.

These partnerships are designed to simplify secure access to legacy applications that use protocols such as header-based and Kerberos authentication, using Azure AD.

Conclusion

Zero Trust is a journey, not a destination. And the journey is unique to every organization because of differences in enterprise architecture, available resources, and priorities. Regardless of your unique needs, moving from an access model based on implicit trust to a Zero Trust model based on explicit verification requires careful planning and time.

Identities are a logical starting point for implementing a phased Zero Trust security model. Microsoft 365 E5, with its strong authentication, identity protection, and access control capabilities, provides a solid foundation for organizations to get started on their Zero Trust journey.

To learn more about the role of identity management in a Zero Trust security model, visit Microsoft Security.

Microsoft