Implementing a Zero Trust security model at Microsoft

Cloud-based services and mobile computing have changed the technology landscape for the modern enterprise. Today's workforce often requires access to applications and resources outside traditional corporate network boundaries, rendering security architectures that rely on firewalls and virtual private networks (VPNs) insufficient. Changes brought about by cloud migration and a more mobile workforce have led to the development of an access architecture called *Zero Trust*.

The Zero Trust model

Based on the principle of "*never trust, always verify*," Zero Trust helps secure corporate resources by eliminating unknown and unmanaged devices and limiting lateral movement. Implementing a true Zero Trust model requires that all components—user identity, device, network, and applications—be validated and proven trustworthy. Zero Trust verifies identity and device health prior to granting access to corporate resources. When access is granted, applying the principle of *least privilege* limits user access to only those resources that are explicitly authorized for each user, thus reducing the risk of lateral movement within the environment. In an ideal Zero Trust environment, the following four elements are necessary:

- Strong **identity** authentication everywhere (user verification via authentication)
- Devices are enrolled in **device** management and their health is validated
- Least-privilege user rights (**access** is limited to only what is needed)
- The health of **services** is verified (future goal)

For Microsoft, Zero Trust establishes a strict boundary around corporate and customer data. For end users, Zero Trust delivers a simplified user experience that allows them to easily manage and find their content. And for customers, Zero Trust creates a unified access platform that they can use to enhance the overall security of their entire ecosystem.

Zero Trust scenarios

We have identified four core scenarios at Microsoft to achieve Zero Trust. These scenarios satisfy the requirements for strong identity, enrollment in device management and device health validation, alternative access for unmanaged devices, and validation of application health. The core scenarios are described here:

- **Scenario 1:** Employees can enroll their devices into device management to gain access to company resources.
- **Scenario 2:** Security organizations can enforce device health checks per application or service.
- **Scenario 3:** Employees and business guests have a secure way to access corporate resources when not using a managed device.
- **Scenario 4:** Employees have user interface options (portal, desktop apps) that provide the ability to discover and launch the applications and resources they need.

Zero Trust scope and phases

Microsoft is taking a structured approach toward Zero Trust that will span many years. Figure 1 illustrates a roadmap, organized by phase, that includes an overview of milestones, goals, and current status. The process emphasizes identity-driven security solutions and centers on securing user identity with strong authentication as well as the elimination of passwords, the verification of device health, and secure access to corporate resources.

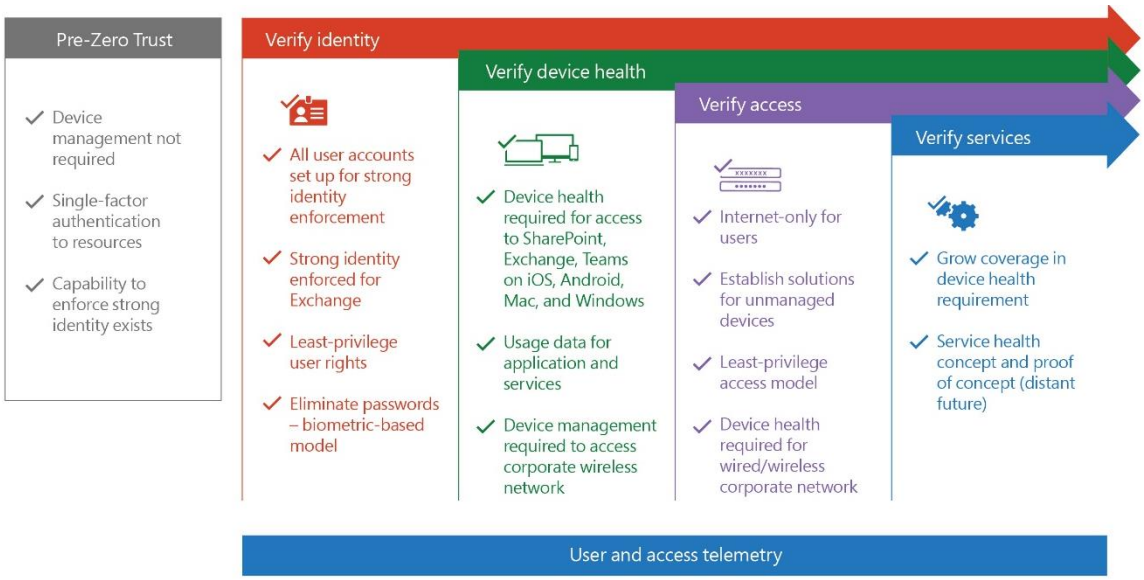

Figure 1. The major components of work performed in each phase of Zero Trust

Scope

Our initial scope for implementing Zero Trust focuses on common corporate services used across our enterprise by information workers—our employees, partners, and vendors. Our Zero Trust implementation focuses on the core set of applications that Microsoft employees use daily (e.g., Microsoft Office apps, line-of-business apps) on platforms like iPhone, Android, Mac, and Windows (Linux is an eventual goal). Device management through Microsoft Intune is required for any corporate-owned or personal device that accesses company resources.

Verify identity phase

Microsoft began the Zero Trust journey by implementing two-factor authentication (2FA) via smartcards for all users to access the corporate network remotely. The rapid adoption of mobile devices for work—which require connection to corporate resources—drove the evolution of the 2FA experience from the physical smartcard to a phone-based challenge, and later to the more modern experience of Azure Authenticator. As we move forward, the largest and most strategic effort presently underway is eliminating passwords in favor of biometric authentication through services like Windows Hello for Business.

Verify device health phase

In this phase, we are working toward enrolling all user devices into a device management system, such as Intune, to enable device-health verification. This capability is essential to setting device-health policy for accessing Microsoft resources. We started by requiring that devices be managed (enrolled in device management via cloud management or classic on-premises management). Next, we required devices to be healthy in order to access major productivity applications ("hero" applications) such as Exchange, SharePoint, and Teams.

Verify access phase

In this phase, we have defined a plan to minimize the means of access to corporate resources and to require identity and device-health verification for all access methods. As we work toward making primary services and applications that users require reachable from the internet, access methods will transition from legacy (corporate network), to internet-first (internet plus VPN when needed), then to internet-only (internet without VPN). This will reduce users accessing the corporate network for most scenarios.

Despite the strong focus on implementing device health everywhere, some scenarios require users to work from unmanaged devices—for instance, in the cases of vendor staffing, acquisitions scenarios, and guest projects. We plan to address the needs of users with unmanaged devices by establishing a set of managed virtualized services that make applications or full Windows desktop environments available.

Verify services phase

The primary goal in this phase is to expand verification from identity and device to service health, making it possible to ensure service health at the start of every interaction. This phase is in a proof-of-concept stage to validate the concept and potential operational capability.

Zero Trust architecture with Microsoft services

Figure 2 provides a simplified reference architecture for our approach to implementing Zero Trust. The primary components of this process are Intune for device management and device security policy configuration, Azure AD conditional access for device health validation, and Azure AD for user and device inventory.

The system works with Intune, pushing device configuration requirements to the managed devices. The device then generates a statement of health, which is stored in Azure AD. When the device user requests access to a resource, the device health state is verified as part of the authentication exchange with Azure AD.

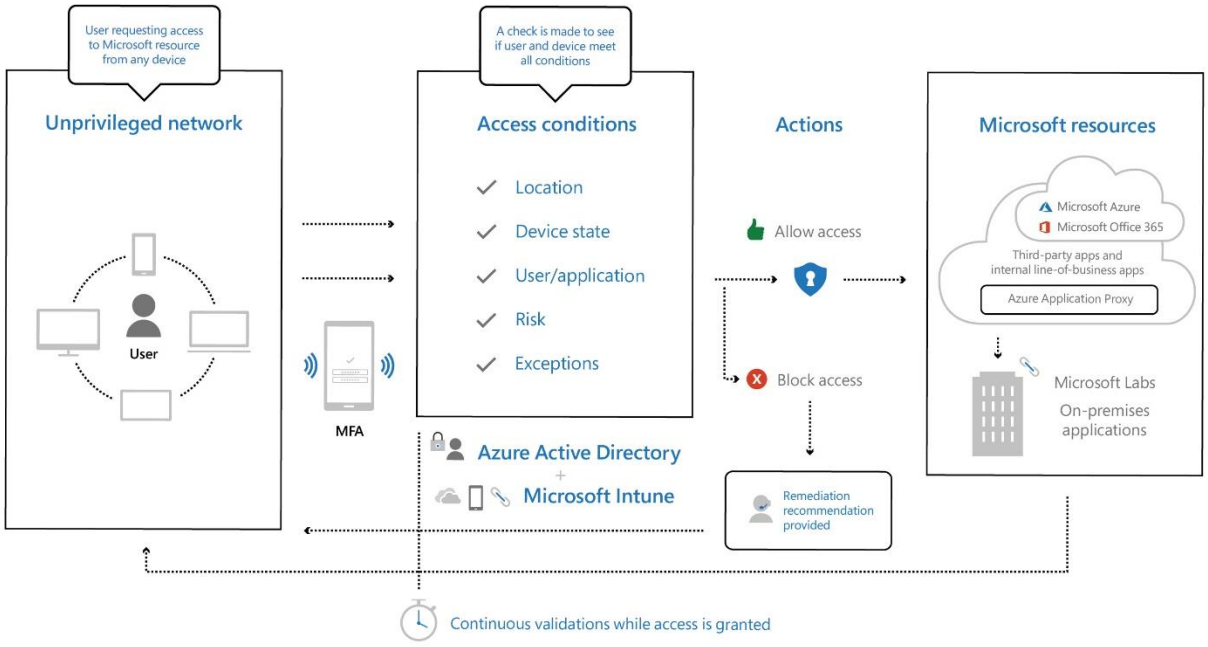

Figure 2. Zero Trust architecture

A transition in progress

Our transition to a Zero Trust model, in which identity and device health are verified by resources and services, is in progress. In the past two years we have increased identity-authentication strength with expanded coverage of strong authentication and an aggressive transition to biometrics-based authentication. We are now focused on building device management and device-health validation capabilities. Mobile platforms and MacOS are complete today, and setting up Windows device health for Office 365 services is in process. Along with this device-health capability, we are also developing the proper access model for unmanaged devices, to provide secure access for vendors and guests.

Customers will need to determine what approach is best for their environment. This includes balancing risk profiles with access methods, defining the scope for the implementation of Zero Trust in their environments, and determining what specific verifications they want to require for users to gain access to their company resources.

For more information

Transitioning to modern access architecture with Zero Trust

Reach the optimal state in your Zero Trust journey

Microsoft Security Zero Trust blogs

The top 9 ways Microsoft IT is enabling remote work for its employees

Running on VPN: How Microsoft is keeping its remote workforce connected