Identity, Endpoints, Applications, Network, Infrastructure and Data are important links in the end to end chain of the Zero Trust security model. The approach advocates protection at each layer, as they could be used as entry points or channels to leak sensitive information.

**Zero Trust principles**

In the past, as an organization, you may have focused your defenses on protecting network access with on-premises firewalls and VPNs, assuming that everything inside the network was safe. But today, as data footprints have expanded to sit off-premises in the Cloud, or across hybrid networks, the Zero Trust security model has evolved to address a more holistic set of attack vectors.

Core to Zero Trust, are the principles of **verify explicitly, apply least privileged access** and **always assume breach**.

These principles are applied across a comprehensive control plane to provide multiple layers of defense.
Zero Trust security layers

Identity
Zero Trust starts with **identity**, verifying that only the people, devices and processes that have been granted access to your resources can access them.

Endpoints
Next comes assessing the security compliance of device **endpoints** - the hardware accessing your data - including the IoT systems on the edge.

Applications
This oversight applies to your **applications** too, whether local or in the Cloud, as the software-level entry points to your information.

Network
Next, there are protections at the **network** layer for access to resources – especially those within your corporate perimeter.

Infrastructure
Followed by the **infrastructure** hosting your data on-premises and in the cloud. This can be physical or virtual, including containers and micro-services and the underlying operating systems and firmware.

Data
And finally, protection of the **data** itself across your files and content, as well as structured and unstructured data wherever it resides.
Microsoft’s approach to Zero Trust

Both Microsoft 365 and Azure are designed with Zero Trust as a core architectural principle. Protections span beyond the Microsoft cloud, to hybrid or even multi-cloud environments. Fundamental to Microsoft’s approach for Zero Trust is **not to disrupt end users**, but work behind the scenes to keep users secure and in their flow as they work.

The key here is end-to-end visibility and then bringing all this together with threat intelligence, risk detection and conditional access policies to reason over access requests and automate response across all of the Zero Trust layers of defense.
**Azure Active Directory** is the cloud identity service that assigns identity and conditional access controls for your people, the service accounts used for apps and processes, and your devices.

Importantly beyond Microsoft services, Azure AD can provide a single identity control plane with common authentication and authorization services for all your apps and services, including popular SaaS apps, or line-of-business cloud and on-premises apps.

This prevents the use of multiple credentials and weak passwords across different services and helps you to universally apply strong authentication methods such as passwordless multi-factor authentication for your users. For example, biometric methods or a FIDO2 key.

Also, to make the authentication process less intrusive to users, you can take advantage of real-time intelligence at sign-in with **Conditional Access** in Azure AD.

Conditional Access lets you set policies to assess the risk levels. This can be risk of the user or a sign-in, the device platform, the sign-in location, and apps, to make point-of-logon decisions and enforce access policies in real time to either block access and require password reset, grant access but require an additional authentication factor or limit it, for example, to view-only privileges.
Granting or blocking access through Conditional Access policies

Endpoints

When users access resources including your data and apps, their endpoints may not be owned and managed by your organization. If endpoints are not up-to-date, or appropriately protected, they run the risk of data exfiltration from unknown apps or services.

Using Microsoft Endpoint Manager, you can make sure that devices and their installed apps meet your security and compliance policy requirements, regardless of whether the device is owned by your organization or the user. This protection applies no matter where the device may be connecting from – whether that’s inside the network perimeter, including over a VPN, on a home network, or the public internet.

Microsoft Endpoint Manager gives you easy access to device and client app management capabilities from the cloud. It enables secure productivity across all of your device types including Windows, iOS, macOS, and Android.
Also, Microsoft Defender with its Extended Detection and Response or XDR management controls, can identify and contain breaches discovered on an endpoint and force the device back into a trustworthy state before it is allowed to connect back to resources.

There are several ways that we help you to apply Zero Trust protections to your applications. We have already looked at the benefits of Azure AD as the single entity provider for authenticated sign-in, as well as the use of conditional access. These recommendations also apply to your cloud and local apps that connect to cloud-based services.

Additionally, Microsoft Endpoint Manager can be used to configure and enforce policy management for both desktop and mobile apps, including browsers. For example, you can prevent work related data from being copied and used in personal apps.
Knowing which apps are used within your organization is critical to mitigating new vulnerabilities. This includes apps acquired by individuals and teams, often referred to as Shadow IT. With its catalog of more than 17,000 apps, Microsoft Cloud App Security (MCAS) can discover and manage Shadow IT services.

You can then set policies against your security requirements to scope how information may be accessed or shared by these services. For example, you can use policies to block actions within a cloud app, such as downloading confidential files, or discussing sensitive topics while using unmanaged devices.
The network is the fourth layer in the Zero Trust security model. With modern architectures and hybrid services spanning on-premises and multiple cloud services, virtual networks – or VNETs – and VPNs, we give you a number of controls, starting with: **1. Network Segmentation** to limit the blast radius and lateral movements of attacks on your network.

**2. Threat protection** to harden the network perimeter from things like DDoS or brute force attacks, **then the ability to quickly detect and respond to incidents**

**3. Encryption** for all network traffic, whether it’s internal, inbound or outbound
Microsoft offers several solutions to help secure your network, including Azure Firewall and Azure DDoS Protection to protect your Azure VNET resources. Importantly, Microsoft’s XDR and SIEM solution, comprising Microsoft Defender and Azure Sentinel, help you quickly identify and contain security incidents.

**Infrastructure**

The most important consideration with infrastructure is around configuration management and software updates so that all deployed infrastructure meets your security and policy requirements.

Here for cloud resources, Azure landing zones, blueprints and policies ensure that newly deployed infrastructure meets compliance requirements. And the Azure Security Center along with Log Analytics helps with configuration and software update management for your on-premises, cross-cloud and cross-platform infrastructure.
Monitorıng is critical for the detection of vulnerabilities, attacks and anomalies. Microsoft Defender with Azure Sentinel provides depth and breadth threat protection for multi-cloud workloads enabling automated detection and response.

At the end of the day Zero Trust is all about understanding and then applying the right controls to protect your Data.

We give you the controls to limit data access only to the people and processes that need it. The policies you set, along with real-time monitoring, can then restrict or block the unwanted sharing of sensitive data and files.

For example, with Microsoft Information Protection, you can automate labeling and classification of files and content.

Policies are then assigned to labels to trigger protective actions, such as encryption or limiting access, restricting third party apps and services and much more.
For data outside of Microsoft 365, Azure Purview automatically discovers and maps the data sitting across your Azure data sources, on-premises, and SaaS data sources; it works with Microsoft Information Protection to help you to classify your sensitive information.

Moving to a Zero Trust security model doesn’t have to be all-or-nothing. We recommend using a phased approach, closing the most exploitable vulnerabilities first.

For hands-on demonstrations of the tools for implementing the Zero Trust security model across the six layers of defense, watch our Microsoft Mechanics series at aka.ms/ZeroTrustMechanics.

You can also learn more at aka.ms/zerotrust.

Additional Resources