Microsoft

Zero Trust Maturity Model

Abstract

In this document, we will share guiding principles for implementing a Zero Trust security model and a maturity model to help assess your Zero Trust readiness and plan your own implementation journey. While every organization is different and each journey will be unique, we hope the Microsoft Zero Trust Maturity Model will expedite your progress.

Introduction

Cloud applications and the mobile workforce have redefined the security perimeter. Employees are bringing their own devices and working remotely. Data is being accessed outside the corporate network and shared with external collaborators such as partners and vendors. Corporate applications and data are moving from on-premises to hybrid and cloud environments.

The new perimeter isn't defined by the physical location(s) of the organization—it now extends to every access point that hosts, stores, or accesses corporate resources and services. Interactions with corporate resources and services now often bypass on-premises perimeter-based security models that rely on network firewalls and VPNs. Organizations which rely solely on on-premises firewalls and VPNs lack the visibility, solution integration and agility to deliver timely, end-to-end security coverage.

Today, organizations need a new security model that more effectively adapts to the complexity of the modern environment, embraces the mobile workforce, and protects people, devices, applications, and data wherever they are located. This is the core of Zero Trust.

Zero Trust overview

Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an uncontrolled network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to "never trust, always verify."

In a Zero Trust model, every access request is strongly authenticated, authorized within policy constraints and inspected for anomalies before granting access. Everything from the user's identity to the application's hosting environment is used to prevent breach. We apply micro-segmentation and least privileged access principles to minimize lateral movement. Finally, rich intelligence and analytics helps us identify what happened, what was compromised, and how to prevent it from happening again.

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 polices, 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.

Controlling access with policy

Today, organizations need to be able to provide secure access to their resources regardless of user or application environment. Before we allow access, we want to assess a user's location, their role in the organization, the health of their device, the type of service and classification of the data they're requesting access to, and more. To do this effectively, we need to use signal and automated policy enforcement to deliver the right balance between security and optimal user experience.

A Zero Trust security model relies on automated enforcement of security policy to ensure compliant access decisions throughout the digital estate. The framework of controls built into your security solutions and tools enables your organization to fine-tune access policies with contextual user, device, application, location, and session risk information to better control how users access corporate resources and backend resources communicate. These policies are used to decide whether to allow access, deny access, or control access with additional authentication challenges (such as multi-factor authentication), terms of use, or access restrictions.

Building Zero Trust into your organization

A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy. This is done by implementing Zero Trust controls and technologies across six foundational elements: **identities, devices, applications, data, infrastructure,** and **networks.**

Each of these six foundational elements is a source of signal, a control plane for enforcement, and a critical resource to be defended. This makes each an important area to focus investments.

Identities

Identities – whether they represent people, services, or IOT devices – define the Zero Trust control plane. When an identity attempts to access a resource, we need to verify that identity with strong authentication, ensure access is compliant and typical for that identity, and follows least privilege access principles.

Devices

Once an identity has been granted access to a resource, data can flow to a variety of different devices—from IoT devices to smartphones, BYOD to partner managed devices, and on-premises workloads to cloud hosted servers. This diversity creates a massive attack surface area, requiring we monitor and enforce device health and compliance for secure access.

Applications

Applications and APIs provide the interface by which data is consumed. They may be legacy on-premises, lift-and-shifted to cloud workloads, or modern SaaS applications. Controls and technologies should be applied to discover Shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, monitor for abnormal behavior, control of user actions, and validate secure configuration options.

Data

Ultimately, security teams are focused on protecting data. Where possible, data should remain safe even if it leaves the devices, apps, infrastructure, and networks the organization controls. Data should be classified, labeled, and encrypted, and access restricted based on those attributes.

Infrastructure

Infrastructure (whether on-premises servers, cloud-based VMs, containers, or micro-services) represents a critical threat vector. Assess for version, configuration, and JIT access to harden defense, use telemetry to detect attacks and anomalies, and automatically block and flag risky behavior and take protective actions.

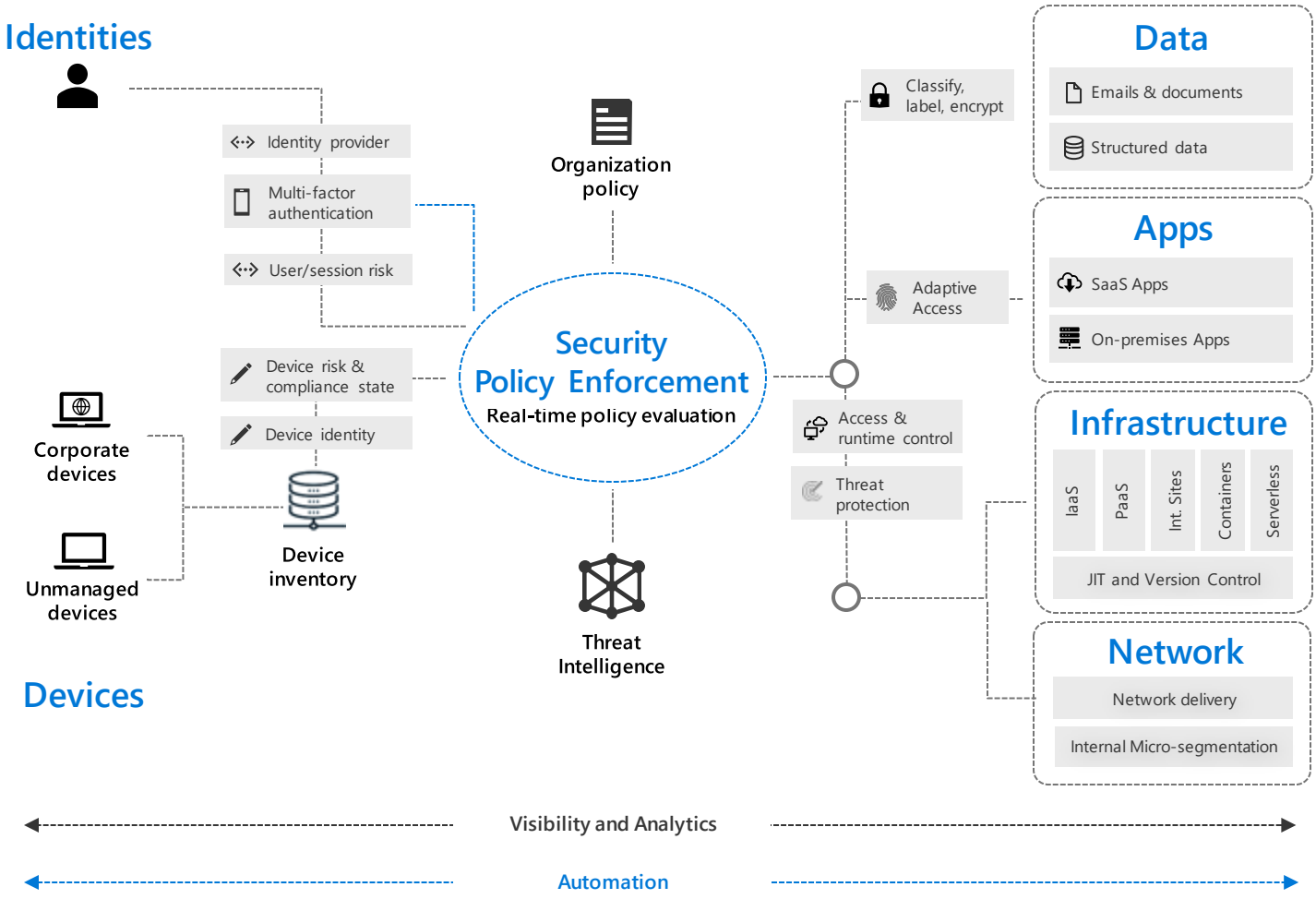
Networks

All data is ultimately accessed over network infrastructure. Networking controls can provide critical "in pipe" controls to enhance visibility and help prevent attackers from moving laterally across the network. Networks should be segmented (including deeper in-network micro segmentation) and real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.

Zero Trust across the digital estate

In an optimal Zero Trust implementation, your digital estate is connected and able to provide the signal needed to make informed access decisions using automated policy enforcement.

Let's explore how the major components of the Zero Trust model all work together to deliver end-to-end coverage.



Improving visibility and embracing security automation

Because Zero Trust relies heavily on signal and solution integration to be successful, this is a great time to work towards providing greater visibility into your threat landscape and embracing security automation. The Security Operations Center (SOC) should have a multi-tier incident response team in place that uses advanced threat detection and AI-driven alert management capabilities to cut through the noise and deliver prioritized security alerts. Response to common incidents, such as denying access to infected devices, should be automated to improve response times and reduce risk exposure.

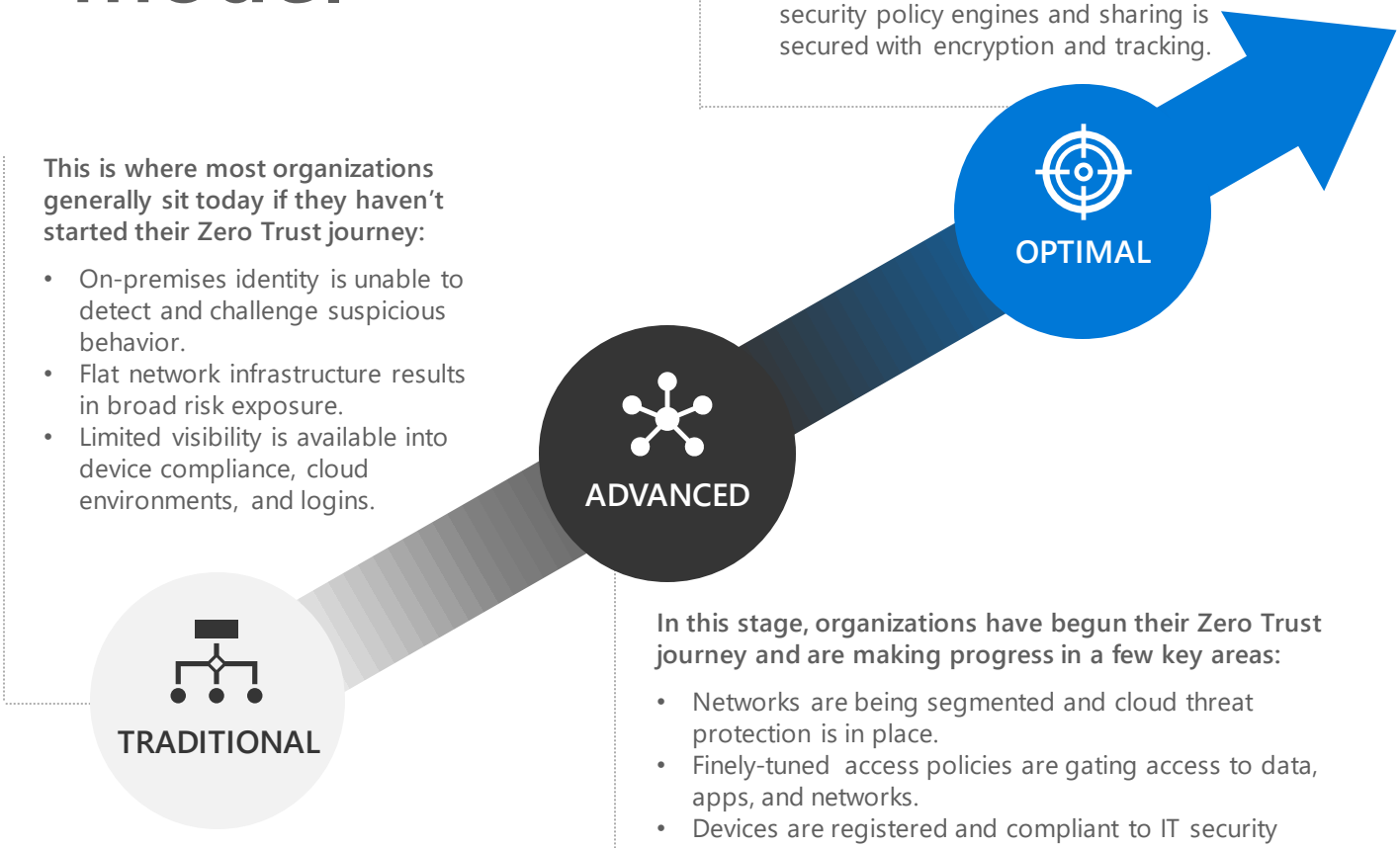
Not every Zero Trust model implementation is the same

Different organizational requirements, existing technology implementations, and security stages all affect how a Zero Trust security model implementation is planned. Using our experience in helping customers to secure their organizations as well as implementing our own Zero Trust model, we've developed the following maturity model to help you assess your Zero Trust readiness and build a plan to get to Zero Trust.

Maturity model

Organizations in the optimal stage have made large improvements in security:

- Trust has been removed from the network entirely—micro cloud perimeters, micro-segmentation, and encryption are in place.
- Real-time analytics dynamically gate access to applications, workloads, networks, and data.
- Automatic threat detection and response is implemented.
- Data access decisions are governed by cloud security policy engines and sharing is secured with encryption and tracking.



This is where most organizations generally sit today if they haven't started their Zero Trust journey:

- On-premises identity is unable to detect and challenge suspicious behavior.
- Flat network infrastructure results in broad risk exposure.
- Limited visibility is available into device compliance, cloud environments, and logins.

In this stage, organizations have begun their Zero Trust journey and are making progress in a few key areas:

- Networks are being segmented and cloud threat protection is in place.
- Finely-tuned access policies are gating access to data, apps, and networks.
- Devices are registered and compliant to IT security policies.
- Analytics are starting to be used to assess user behavior and proactively identify threats.

On the next page you will find an expanded maturity model to help you assess your own Zero Trust readiness across your user identities, devices, application, data, infrastructure, and networks.

	Traditional	Advanced	Optimal
 **Identities**	On-premises identity provider is in use No SSO is present between cloud and on-premises apps Visibility into identity risk is very limited	Cloud identity federates with on-premises system Conditional access policies gate access and provide remediation actions Analytics improve visibility	Passwordless authentication is enabled User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection
 **Devices**	Devices are domain joined and managed with solutions like Group Policy Object or Config Manager Devices are required to be on network to access data	Devices are registered with cloud identity provider Access only granted to cloud managed & compliant devices DLP policies are enforced for BYO and corporate devices	Endpoint threat detection is used to monitor device risk Access control is gated on device risk for both corporate and BYO devices
 **Apps**	On-premises apps are accessed through physical networks or VPN Some critical cloud apps are accessible to users	On-premises apps are internet-facing and cloud apps are configured with SSO Cloud Shadow IT risk is assessed; critical apps are monitored and controlled	All apps are available using least privilege access with continuous verification Dynamic control is in place for all apps with in-session monitoring and response
 **Infrastructure**	Permissions are managed manually across environments Configuration management of VMs and servers on which workloads are running	Workloads are monitored and alerted for abnormal behavior Every workload is assigned app identity Human access to resources requires Just-In-Time	Unauthorized deployments are blocked and alert is triggered Granular visibility and access control are available across all workloads User and resource access is segmented for each workload
 **Network**	Few network security perimeters and flat open network Minimal threat protection and static traffic filtering Internal traffic is not encrypted	Many ingress/egress cloud micro-perimeters with some micro-segmentation Cloud native filtering and protection for known threats User to app internal traffic is encrypted	Fully distributed ingress/egress cloud micro-perimeters and deeper micro-segmentation ML-based threat protection and filtering with context-based signals All traffic is encrypted
 **Data**	Access is governed by perimeter control, not data sensitivity Sensitivity labels are applied manually, with inconsistent data classification	Data is classified and labeled via regex/keyword methods Access decisions are governed by encryption	Classification is augmented by smart machine learning models Access decisions are governed by a cloud security policy engine DLP policies secure sharing with encryption and tracking

Tools to drive your Zero Trust implementation

As you begin to assess your Zero Trust readiness and begin to plan on the changes to improve protection across **identities, devices, applications, data, infrastructure,** and **networks,** consider these key investments to help drive your Zero Trust implementation more effectively. Through our own experience, we've found each of the following to be critical to closing important capability and resources gaps:

1. **Strong authentication.** Ensure strong multi-factor authentication and session risk detection as the backbone of your access strategy to minimize the risk of identity compromise.
2. **Policy-based adaptive access.** Define acceptable access policies for your resources and enforce them with a consistent security policy engine that provides both governance and insight into variances.
3. **Micro-segmentation.** Move beyond simple centralized network-based perimeter to comprehensive and distributed segmentation using software-defined micro-perimeters.
4. **Automation.** Invest in automated alerting and remediation to reduce your mean time to respond (MTTR) to attacks.
5. **Intelligence and AI.** Utilize cloud intelligence and all available signals to detect and respond to access anomalies in real time.
6. **Data classification and protection.** Discover, classify, protect, and monitor sensitive data to minimize exposure from malicious or accidental exfiltration.

In closing

While a Zero Trust security model is most effective when integrated across the entire digital estate, most organizations will need to take a phased approach that targets specific areas for change based on their Zero Trust maturity, available resources, and priorities. It will be important to consider each investment carefully and align them with current business needs. The first step of your journey does not have to be a large lift and shift to cloud-based security tools. Many organizations will benefit greatly from utilizing hybrid infrastructure that helps you use your existing investments and begin to realize the value of Zero Trust initiatives more quickly.

Fortunately, each step forward will make a difference in reducing risk and returning trust in the entirety of your digital estate.

Microsoft is currently on its own Zero Trust journey. Head over to our IT Showcase to learn more about how we've approached our Zero Trust journey, our current progress, and upcoming milestones.