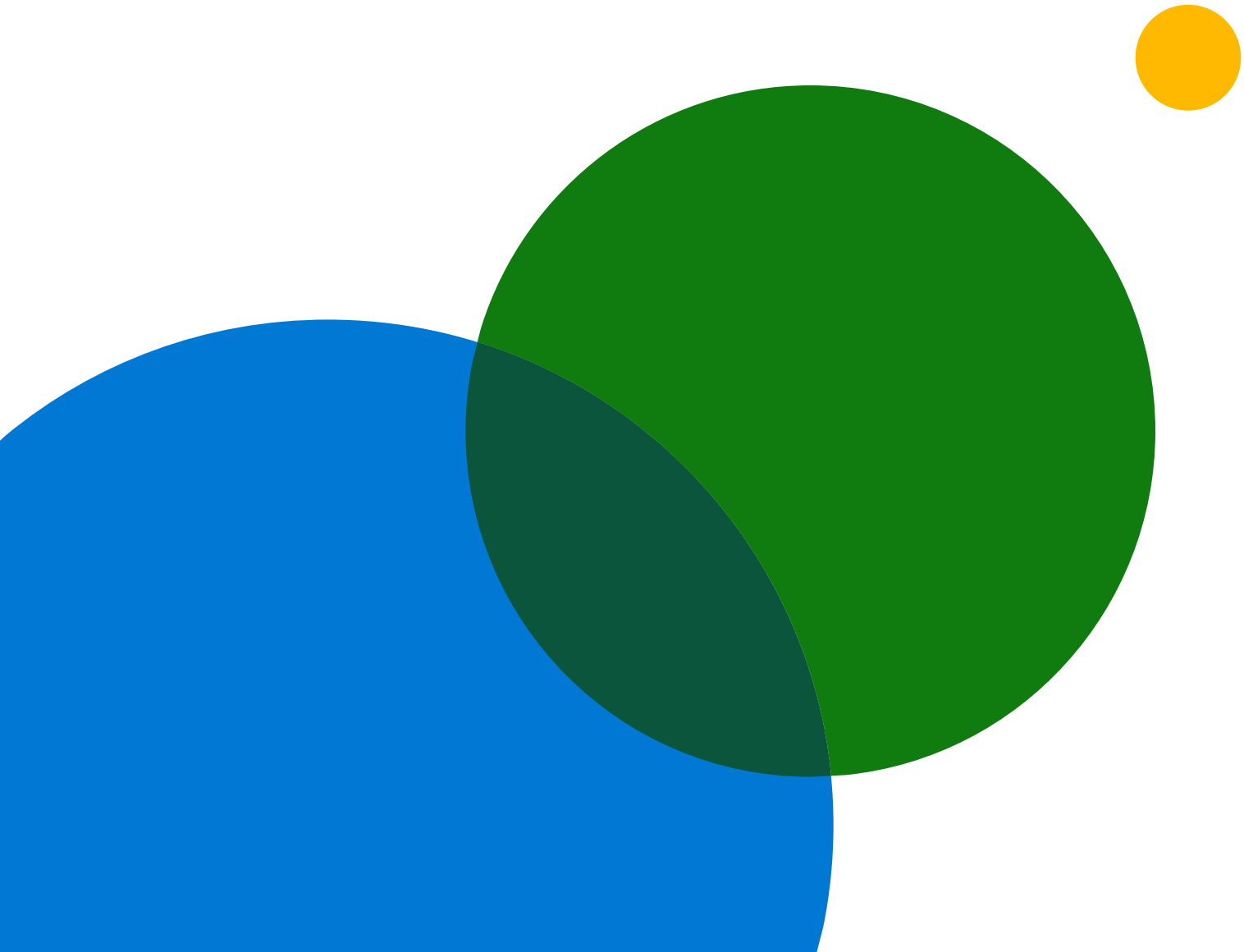
Microsoft

Evolving Zero Trust

How real-world deployments and attacks are shaping the future of Zero Trust strategies



Abstract

Microsoft has helped thousands of organizations evolve their Zero Trust deployments to respond to transitions to remote and now hybrid work in parallel with a growing intensity and sophistication of cyberattacks. This paper distills what we've learned from these customers informing the trends evolving Zero Trust, the updates to our viewpoint of this model from an architecture and implementation maturity perspective, and key recommendations to ensure you're best prepared for our new reality.

Introduction

Zero Trust is the essential security strategy for today's reality. In 2020, the global pandemic compelled nearly every organization to embrace a Zero Trust strategy as employees went remote, virtual private networks (VPNs) were breached or overwhelmed, and digital transformation became critical to organizational sustainability. The mandate emerged for a Zero Trust approach to verify and secure every identity, validate device health, enforce least privilege, and capture and analyze telemetry to better understand and secure the digital environment. Governments and businesses worldwide recognized this imperative and accelerated the adoption of a Zero Trust strategy. Through supporting thousands of deployments and observing the expanding threat landscape, we have revised and evolved the Zero Trust architecture and maturity model we released two years ago based on what we have learned. We want to share those learnings for organizations to implement today and tomorrow.

Zero Trust is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to threats.

Five lessons learned over the last two years

1. Improve user experience and productivity with Zero Trust.

Zero Trust enabled users to safely work from home, enroll new devices from anywhere, hold secure meetings, and achieve new levels of productivity. Successful Zero Trust deployments use all available telemetry to prioritize user experience and business enablement, and more effectively delegate responsibilities to the right level of the organization. These organizations further empower users and admins with automatic protection and security insights that allow them to execute with confidence and agility.

A Zero Trust approach empowers people to work productively and securely when, where, and how they want.

2. Apply Zero Trust to your entire digital estate.

Recent nation-state attacks demonstrate that attackers will exploit any vulnerability. In our observations, the organizations that fared best against such attacks had embraced Zero Trust strategies broadly. These organizations began with a full inventory and assessment of resources across on-premises and cloud environments, prioritizing protections based on their relative importance to the business. This was coupled with verifying and protecting all aspects of their digital estate—including all human and non-human identities, endpoint platforms, networks, microservices, virtual machines, and workloads.

Implementing Zero Trust requires a comprehensive vision and plan, prioritizing milestones based on the most important assets first.

Multi-factor authentication (MFA) reduces the effectiveness of identity attacks by more than 99%

Five lessons learned over the last two years (continued)

3. Integrate verification and controls across security pillars.

Attackers exploit gaps exposed by siloed programs and processes. To prevent incursions, end-to-end visibility and control across the security estate is critical. Organizations with separate tools to monitor individual aspects like network, internet access, and internet triage will lack a complete view of their estate. Integrating controls and telemetry across security pillars enables organizations to apply unified policies and enforce them consistently, resulting in a more robust security posture.

Unifying strategy and security policy with Zero Trust breaks down siloed information technology (IT) teams to enable better visibility and protection across the IT stack.

4. Monitor your security posture with strong governance.

Strong governance is directly linked to the performance of Zero Trust initiatives. Organizations with advanced strategies verify business security assertions by regularly validating technical security assertions like "is this device registered" or "is this data confidential?" The best Zero Trust strategies are founded on governance models that ensure the integrity of data to drive continuous assessment and improvement. Analyzing these productivity and security signals also helps evaluate security culture, identifying areas for improvement or best practices.

Enforcing strong governance with a Zero Trust approach includes validating business assertions, assessing security posture, and understanding the impact of security culture.

5. Automate to simplify and strengthen your security posture.

Automation is critical to a robust and sustainable security program. The best Zero Trust deployments automate routine tasks like resource provisioning, access reviews, and attestation. These organizations use machine learning and AI in threat protection tactics like security automation and orchestration to defend themselves, enabling them to build back infrastructure quickly after an attack. Given the inundation of threat notifications and alerts hitting the security operations center (SOC) today, automation is critical to managing the digital environment at the speed and scale needed to keep up with today's attacks.

A Zero Trust approach prioritizes routine task automation, reducing manual efforts so security teams can focus on critical threats.

Guiding principles of Zero Trust

Real-life deployments have tested and proven the core principles of a successful Zero Trust strategy.

Verify explicitly

Always make security decisions using all available data points, including identity, location, device health, resource, data classification, and anomalies.

Use least privilege access

Limit access with just-in-time and just-enough-access (JIT/JEA) and risk-based adaptive polices.

Assume breach

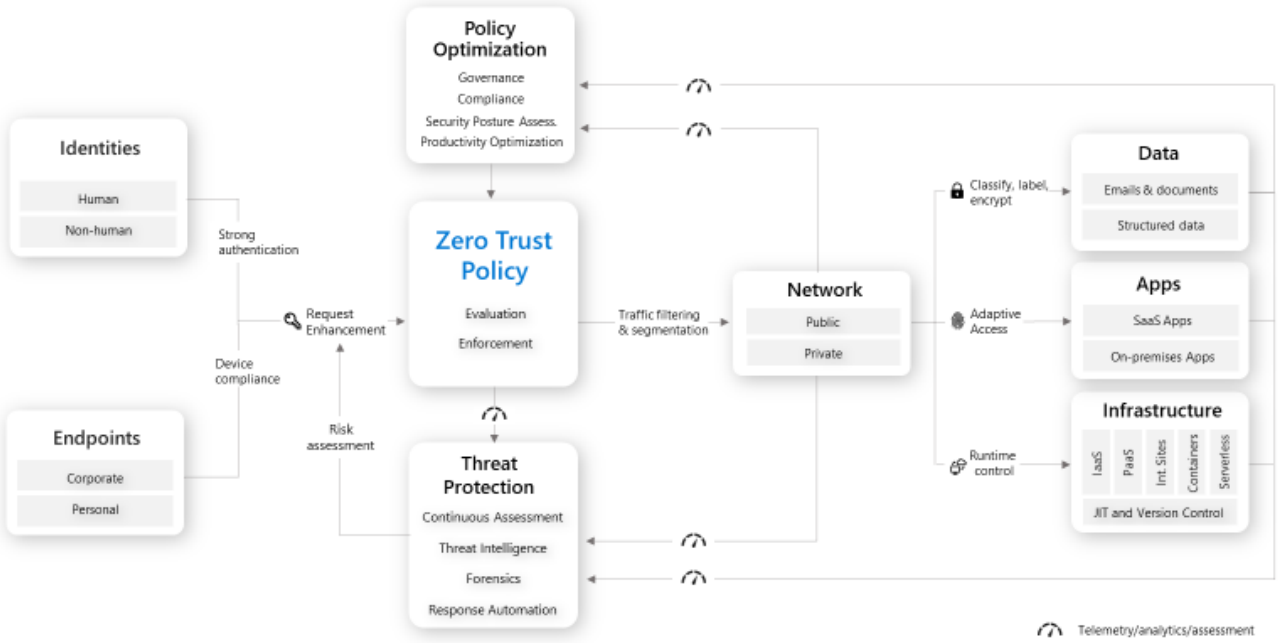
Minimize blast radius with micro-segmentation, end-to-end encryption, continuous monitoring, and automated threat detection and response.

Verify explicitly has expanded to include verifying the software in your supply chain

Zero Trust deployments apply least privilege access to infrastructure, ensuring compartmentalized access to systems which can add or modify permissions or policies

Zero Trust architecture

Learnings from the past two years refined our Zero Trust architecture to emphasize the critical importance of integrating policy enforcement and automation, threat intelligence, and threat protection across security pillars. These integrated elements act upon telemetry across every pillar to inform decisions with real-time signals.



Maturity model

Gauge where your organization is in its Zero Trust journey with the following questions:

First stage

- Are you reducing password risks with strong auth methods like MFA and providing SSO access to cloud apps?
- Do you have visibility into device compliance, cloud environments, and logins to detect anomalous activity?
- Are your networks segmented to prevent unlimited lateral movement inside the firewall perimeter?

Significant progress

- Are you using real-time risk analytics to assess user behavior and device health to make smarter decisions?
- Can you correlate security signals across multiple pillars to detect advanced threats and quickly take action?
- Are you proactively finding and fixing vulnerabilities from misconfigurations and missing patches to reduce threat vectors?

Most mature stage

- Are you able to dynamically enforce policies after access has been granted to protect against violations?
- Is your environment protected using automated threat detection and response across security pillars to react more quickly to advanced threats?
- Are you analyzing productivity and security signals to help drive user experience optimization through self-healing and actionable insights?

See Appendix of this document for definitions of architecture components and a full breakdown of the maturity model by security pillar.

What's next for Zero Trust

Zero Trust is a dynamic model that will continue to evolve. Here are the trends that Microsoft expects to accelerate:

Deeper integration across pillars will simplify unified policy enforcement.

The focus of Zero Trust is shifting from securing individual pillars with the right policies and controls to policy unification across pillars, ensuring consistent enforcement and holistic protection. For example, the policy unification between identity and endpoints has already been possible. Now we're seeing the convergence of access controls between identity and network, allowing security teams to apply granular, consistent policies for all users to all resources. Going forward, such policy unification will extend to more Zero Trust pillars so that security teams can automate enforcement across their entire estate and achieve an even stronger security posture.

Threat intelligence and automated response will further empower security teams.

As attacks become more sophisticated and extensive, threat intelligence is critical to correlate signals across pillars and prioritize incidents. Integrated extended detection and response (XDR) across pillars will play a pivotal role providing the end-to-end visibility and automated response to protect assets, remediate threats, and support investigations. This approach will also empower security teams with the time and telemetry they need to detect, deter, and defeat the most critical attacks and risks they face, both internally and externally.

Software and DevOps processes will be informed by Zero Trust principles.

User access to code and development tools will utilize just-in-time and just-enough-access to minimize the exposure of secure information and resources. Organizations will explicitly verify application and software security integrity using in-house and external testing. Modern applications and network management tools will continuously verify signals and enforce policies in real time to protect data more effectively. Organizations will be able to implement a Zero Trust approach without needing to retrofit applications. Native integrations, built-in connectors, and configurable application program interfaces (APIs) will simplify the effort required to integrate across vectors.

Zero Trust will increase the efficiency of security posture management.

As security tools become more intelligent, they will empower IT and help simplify the complexity of configuring and managing policies. Zero Trust posture management will assess risks like configuration drift, missed software patches, and gaps in security policies. As posture management tools mature, we expect them to better support organizations improving their posture by identifying areas for improvement based on best practices and historical context, enable one-click configuration changes, and offer impact assessments to optimize coverage and rollouts that enhance end-user productivity.

Advisory competencies will play a vital role in adapting and scaling Zero Trust.

With nearly every organization implementing or preparing to implement Zero Trust architecture, security services will be essential to address IT skills shortages, staff capacity, and strengthen security posture. As the silos between security pillars are broken down, security advisory services will evolve to more efficiently adapt Zero Trust strategies to the requirements of organizations varying in size and industry.

Conclusion

Zero Trust is an imperative for business, technology, and security teams working to protect everything as it is, and as it could be. It is an ongoing journey for security professionals, but getting started begins with simple first steps, a continuing sense of urgency, and continuous iterative improvements. Beyond the lessons and trends covered in this document, the included technical guidance and resources can help your teams start or advance your Zero Trust journey.

Guidance and technical resources

The following resources will expand upon the principles, lessons learned, and requirements covered earlier to provide actionable guidance and help accelerate your Zero Trust readiness:

- Assess your maturity stage with our Zero Trust Maturity Assessment
- For a repository of technical resources, check out the Zero Trust Guidance Center.
- For developers and partners, check out the Zero Trust Guidance Center for resources on technology partner integrations.
- Learn about our own Zero Trust deployment journey at Microsoft Digital Inside Track.

Appendix

Zero Trust Architecture components

Security Pillar	Definition
Identities	Identities—whether they represent people, workloads, endpoints, 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 and ensure access is compliant and typical for that identity and follows least privilege access principles.
Endpoints	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.
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.
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 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.
Policy optimization	The organization-specific security policies applied throughout an organization's programs across the entire digital estate. The policies are optimized for business processes, governance, compliance, and the end user experience.
Policy enforcement	The Zero Trust policy intercepts the request, and explicitly verifies signals from all 6 foundational elements based on policy configuration and enforces least privileged access. Signals include the role of the user, location, device compliance, data sensitivity, application sensitivity and much more. In additional to telemetry and state information, the risk assessment from threat protection feeds into the policy to automatically respond to threats in real-time. Policy is enforced at the time of access and continuously evaluated throughout the session.
Threat protection	Telemetry and analytics from all the 6 foundational elements feeds into the threat protection system with our Zero Trust architecture. Large amounts of telemetry and analytics enriched by threat intelligent generates high quality risk assessments that can either be manually investigated or automated. The risk assessment feeds into the policy engine for real-time automated threat protection.

Appendix

Maturity Model table, part 1 of 2

	Getting Started	Advanced	Optimal
Identity	• Authentication using a weak credential such as password • Cloud identity federates with on-premises system and some apps connected with the cloud identity provider • Manual provisioning, governance, and limited visibility into risk	• Authentication using strong authentication such as MFA • Most apps are federated with cloud identity for authentication, authorization, provisioning, and deprovisioning • Visibility into identity and session risk	• Authentication using passwordless and phishing resistant methods • All apps are modern and federated with cloud identity for authentication, authorization, provisioning, and deprovisioning • Automated access reviews ensure proper management of group memberships, access to apps, and role assignments
Endpoints	• On-premises management using basic endpoint protection (EPP) • Configuration settings managed with Group Policy • Limited visibility into compliance	• On-premises management connected to cloud MDM for security configuration and devices registered with cloud identity • Compliance enforcement based on device posture on first access • EPP + EDR to include post-breach monitoring and response coverage, basic automatic remediation playbooks	• Device health, antimalware status, and security are constantly monitored and validated • Device security settings enforced with baselines across all devices • EPP + EDR + TVM for posture management, advanced automatic remediation playbooks, and XDR integration
Network	• Permissions are manually managed and static • Some internet resources are accessible to users directly; VPNs and open networks provide access to majority of resources. • Workloads are monitored for known threats and static traffic filtering; Some internal and external traffic is encrypted	• Permissions are managed with policy and adjusted based on recommendations • Access across sensitive workloads is isolated by session; cloud apps, internet resources, and sensitive private networks are accessible without location-assumed trust • Traffic is monitored; most internal and external traffic is encrypted	• Adaptive access policies explicitly check evolving permissions automatically to resources based on risk and usage • All sessions are continuously evaluated for policy violations and access is revoked dynamically, based on data signals powered by a cloud-based service • Traffic is monitored to identify potential threats and dynamic signaling; All data and network traffic is encrypted end-to-end
Applications	• Cloud shadow IT risk is assessed, and critical apps are monitored and controlled • Some critical cloud apps are accessible to users	• On-premises apps are internet-facing • Cloud apps are configured with SSO	• 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

Appendix

Maturity Model table, part 2 of 2

	Getting Started	Advanced	Optimal
Data	• Rule-based and keyword methods are used to discover and classify sensitive data across some locations, apps, services • Access is governed by perimeter control, not data sensitivity • Sensitivity labels are applied manually, with inconsistent data classification	• Automated discovery and classification across all locations, apps, and services and heterogenous data types • Access is governed irrespective of perimeter or app boundary • Restricting flow of sensitive data	• Continuous discovery and correlation of signals using machine learning to identity data exfiltration risks • Access decisions are governed by a cloud security policy engine • Proactive data governance and risk assessment
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
Threat protection	• Reactive threat and vulnerability detection • Pre-breach protection using tools like AV for endpoints, EOP for email • Isolated or siloed security and response • Basic endpoint monitoring	• Proactive threat and vulnerability detection and post-breach response • Automated investigation and remediation (AIR) enabled for test groups and basic threats • XDR capabilities across at least two security pillars and some security information and event management (SIEM) integration	• AIR has been fully enabled • Actively using threat analytics, threat intelligence, and recommended mitigations to close vulnerabilities and misconfigurations • XDR capabilities applied across all pillars and fully integrated with SIEM for advanced threat hunting, detection, response, and prevention
Policy enforcement	• Access decisions are based on limited signals • Access decisions are not centralized • Access decisions are made at only the time of access and are not continuous	• Access decisions are based on signals from at least two pillars • Centralized policy engine used to make access decisions	• Access decisions are based on signals from all pillars • Decisions are continuously evaluated, and policy is enforced in real time • Real-time threat assessment used in access decision

Accelerate your journey today with resources from Microsoft.

aka.ms/zerotrust/