alesonITC
data thinking

4 BEST PRACTICES TO IMPLEMENT A COMPREHENSIVE ZERO TRUST SECURITY APPROACH

INDEX

00 INTRODUCTION

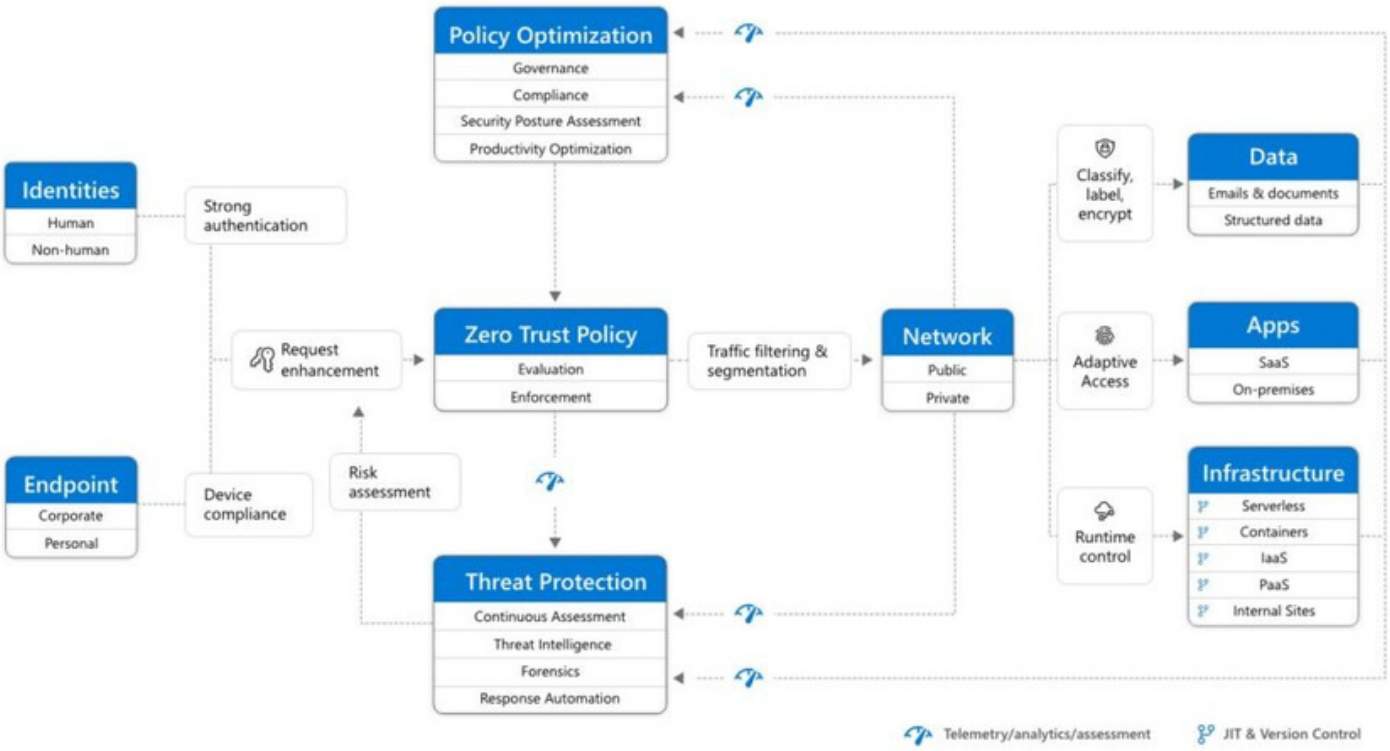
Today's threat actors don't see barriers, they see opportunities. As the old firewalls protecting the corporate network become obsolete amid the rush to adopt a hybrid workspace, implementing Zero Trust security has become an imperative across all sectors, both public and private.

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.

This means you need to determine how to implement a comprehensive Zero trust security approach. Next, you will find 4 best practices to implement It:

1. Build Zero Trust with comprehensive coverage.
2. Strengthen Zero Trust with AI and integration.
3. Simplify for easier compliance and identity and access management (IAM)
4. Look for best-in-breed protection

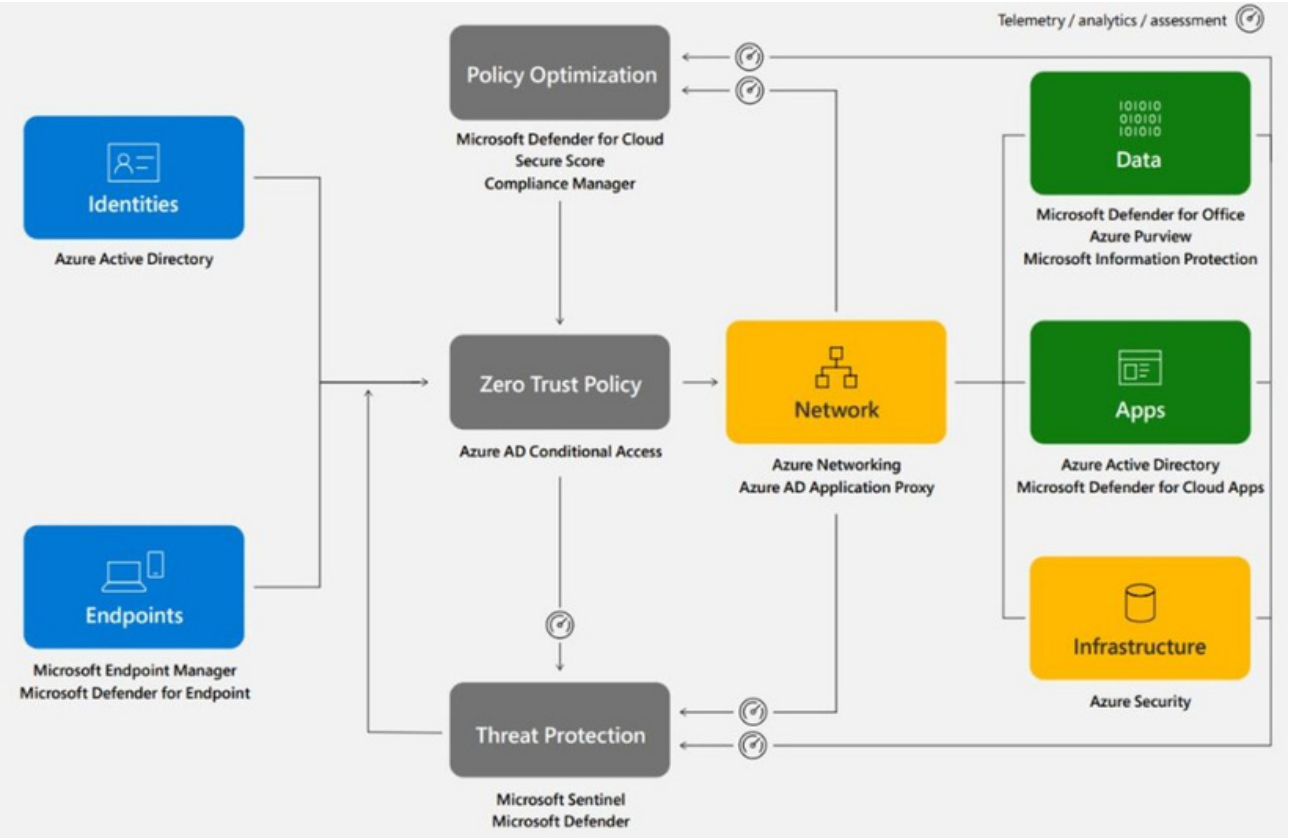
Microsoft Zero Trust architecture



01 BUILD ZERO TRUST WITH COMPREHENSIVE COVERAGE

A Zero Trust approach empowers organizations to grant employees greater freedom across all data, apps, and infrastructure. In a recent Microsoft-commissioned study conducted by Forrester Consulting, The Total Economic Impact™ (TEI) of Zero Trust Solutions From Microsoft, the principal architect at a logistics firm described how Microsoft's comprehensive Zero Trust implementation allowed them to create a bring your own device (BYOD) program for the company's seasonal frontline workers, leading to efficiency gains. "Before, our seasonal workers would have to be paired with our full-time employees when [performing field visits]. But now, they can go out on their own."

This had a bonus effect of reducing the number of agents installed on a user's device, there by increasing device stability and performance. "For some organizations, this can reduce boot times from 30 minutes to less than a minute," the study states. Moreover, shifting to Zero Trust moved the burden of security away from users. Implementing single sign-on (SSO), multifactor authentication (MFA), leveraging passwordless authentication, and eliminating VPN clients all further reduced friction and improved user productivity.



02 STRENGTHEN ZERO TRUST WITH AI AND INTEGRATION

The Forrester study also found that "existing solutions failed to provide the high-fidelity signals, comprehensive visibility, and end-to-end self-healing capabilities needed to defend against today's sophisticated attackers and volume of cyberthreats.

Microsoft Sentinel solves the problem of vulnerable security silos by providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. As a cloud-native security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution, Microsoft Sentinel uses AI to eliminate security infrastructure setup and maintenance by automatically scaling to meet user needs. Because Microsoft Sentinel is available out of the box with service-to-service connectors, it's easy to gain real-time integration with Microsoft 365 Defender, Microsoft Azure Active Directory (Azure AD), Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps.

Any truly comprehensive Zero Trust implementation requires functionality across multiple platforms. Microsoft Sentinel also contains 30 new out-of-the-box data connectors for Cisco, Salesforce Service Cloud, Google Workspace, VMware ESXi, Thycotic, and many more. These data connectors include a parser that transforms the ingested data into Microsoft Sentinel normalized format, enabling better correlation for end-to-end outcomes across security monitoring, hunting, incident investigation, and response scenarios. Microsoft Sentinel automates routine tasks—with a 90 percent reduction in alert fatigue—so, your security team can focus on the most critical threats.

For example, by adhering to the values of Zero Trust, the Microsoft security operations center (SOC) assumes that any device or user can be breached. That means we end up scrutinizing roughly 600 billion security events each month. But because we utilize Microsoft Sentinel and our other security tools that leverage machine learning, threat intelligence, and data science, we're able to filter 600 billion monthly events down to around 10,000 alerts. We also use Microsoft Defender for Endpoint Automated Investigation and Response (AIR) capabilities to find and fix low-level malware instances and other nuisance alerts. Microsoft Defender for Endpoint AIR capabilities can also clean up a device, delete the service, erase the file, and tell us when the problem has been remediated. This reduces noise for our SOC and helps shrink those 10,000 monthly alerts down to a manageable 3,500 cases for investigation. Whittling those numbers down is what helps us—and you—zero in on real threats.

03 SIMPLIFY FOR EASIER COMPLIANCE AND IDENTITY AND ACCESS MANAGEMENT (IAM)

As a feature in the Microsoft 365 compliance center, Microsoft Compliance Manager solves the complexity ofaudit the organizationsenviroments oreffectively implementgovernance policies problem with intuitive management and continuous assessments. From taking inventory of data risks to implementing controls, staying current with regulations and certifications, and reporting to auditors.

To make compliance even easier, the new Microsoft Sentinel: Zero Trust (TIC 3.0) Workbook features: a redesigned user interface, new control card layouts, dozens of new visualizations, better-together integrations with Microsoft Defender for Cloud and provides a mechanism for viewing log queries.

Microsoft also offers more than 300 pre-built risk assessment templates to help you comply with evolving regulations, as well as integrated workflows to help ensure the right people across security, HR, legal, and compliance can investigate as soon as a risk is identified.

Azure Active Directory integration enabled to businesses to streamline sign-in and easily deploy applications companywide, as well as enable SSO and automate user provisioning. These efficiency gains allowed their IAM teams to focus on improving security by implementing additional Zero Trust policies.

By adopting Azure AD, the IAM teams also reduced time spent managing IAM infrastructure, provisioning and de-provisioning users, managing vendors, and dealing with application downtime and remediation.

04 LOOK FOR BEST-IN-BREED PROTECTION

When looking for a Zero Trust solution you can rely on, there's a confidence that comes from knowing your security provider has seen more than 40 percent year-over-year growth and more than USD10 billion in revenue.

Microsoft Security is:
-leader in five Gartner Magic Quadrants.
-Leader in eight Forrester Wave™ categories.
-Ranked the highest in the MITRE Engenuity® ATT&CK
-Leader in IDC MarketScape for Modern Endpoint Security.

By unifying security, compliance, and identity, we can help you improve productivity and protect your entire environment.