

The New Shape of Zero Trust

A Zero Trust Approach and Architecture for the AI Age

When Data Knows No Boundaries—Zero Trust

Data no longer sits behind a perimeter. To secure it against internal and external threats in the new boundary-less world, Zero Trust thinking is critical. So, what do security leaders need to know about Zero Trust?

Why Zero Trust Matters Now More Than Ever

690%

jump in password attacks per day since 2021¹

200%

increase in ransomware attacks by human-operated sources from 2022 to 2023¹

\$4.6T

projected cost increase for total attacks by 2028¹

What Is Not Zero Trust:

- NOT a product
- NOT a thing
- NOT a process
- NOT a single technology or tool

It's a **PHILOSOPHY** of **CYBERSECURITY** that assumes **EVERYTHING IS A THREAT**.

And it's been shown to improve customer data protection, access and authentication security, as well as remote work safety.²

Zero Trust has 3 SIMPLE PRINCIPLES



1. VERIFY EXPLICITLY

Continuously authenticate and authorize.



2. USE LEAST-PRIVILEGED ACCESS

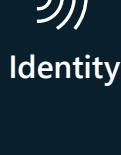
Limit user access with just-in-time, and just-enough-access (JIT/JEA).



3. ASSUME A BREACH

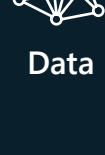
Treat every situation as though you're already compromised.

Applying the principles to a flexible Zero Trust approach



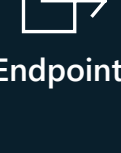
Identity

Automatically authenticate access with tools like multifactor authentication (MFA) and single sign-on (SSO).



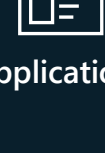
Data

Ensure that data across your environments at rest, in motion, and in use is classified, labeled, and protected.



Endpoints

Manage all types of endpoints accessing your data whatever the device.



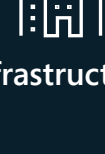
Applications

Simplify and secure access to cloud and mobile apps and on-premises resources for all authorized parties.



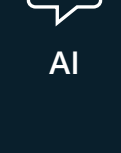
Network

Gain security by reducing perimeter-based scalable vulnerabilities like VPNs.



Infrastructure

Automate protection and security management for on-premises, cloud, and hybrid.



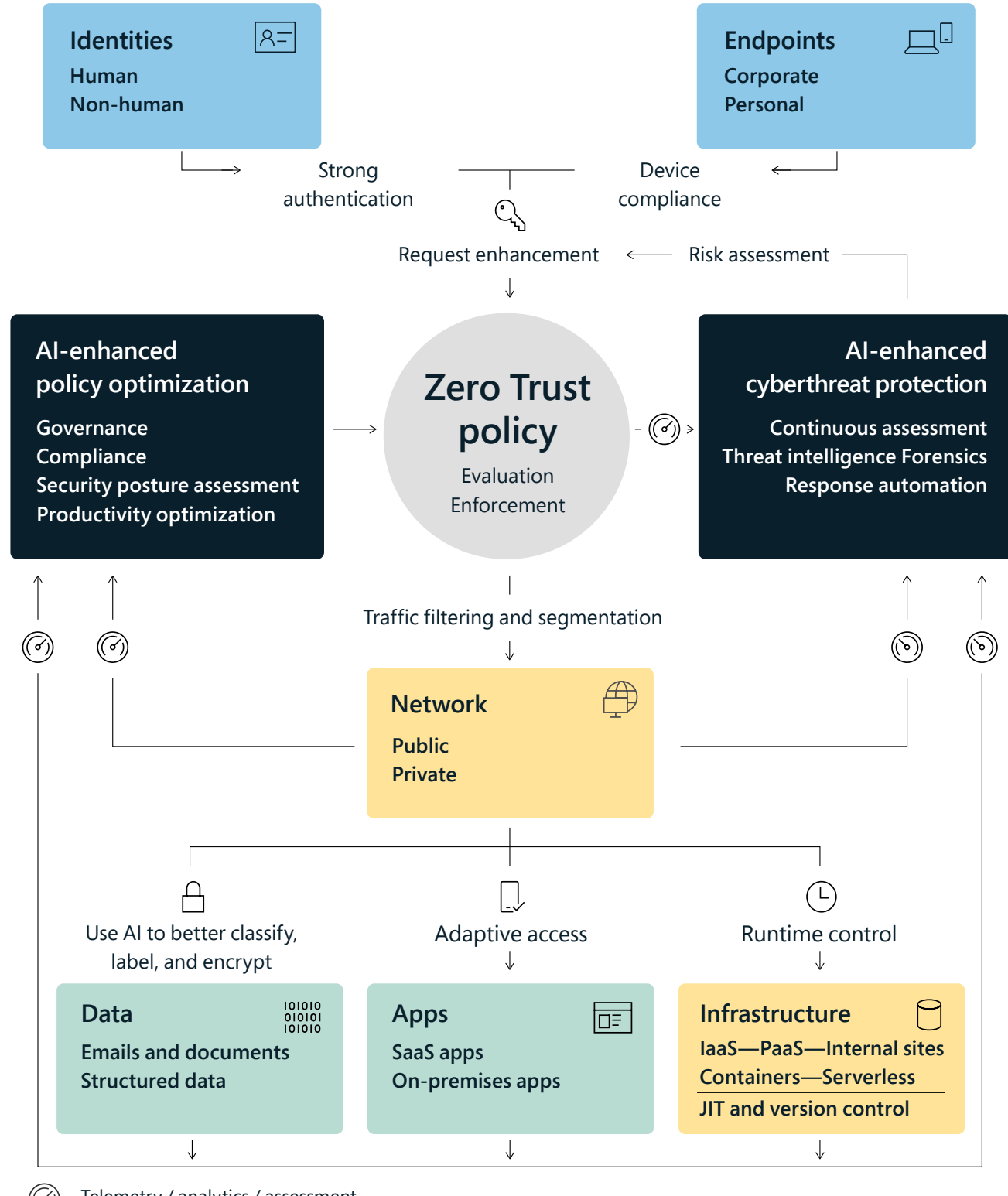
AI

Use the power of AI to identify threats and risks faster and adapt in real-time so you can dynamically adjust security policies and controls.

Envision your Zero Trust architecture

Visualize how Zero Trust affects your organization with this architecture schematic.

Microsoft Zero Trust architecture



Start building on your Zero Trust framework

What's your next step? Apply a Zero Trust approach to your security using the latest technologies, tools, and solutions from Microsoft.



Learn more about the Microsoft approach to Zero Trust

¹"Microsoft Copilot for Security generally available on April 1, with new capabilities," CEE Multi-Country News Center, March 15, 2024

²Zero Trust Adoption Survey, March 2022 Foundry, Base 250. (Foundry surveyed US respondents in February-March 2022 to explore the current state of Zero Trust adoption, capturing the benefits experienced by the respondents' organizations.)