Microsoft

Zero Trust

Security built for the modern world

Unpredictable change

The information security landscape is transforming in ways most organizations couldn't have predicted even five years ago. The complexity of the modern workplace is overwhelming the capabilities of traditional security strategies and tools.

Remote work

1.87 billion workers, nearly half of the global workforce, will be mobile workers by **2022**

Personal devices

64% of employees now use personal devices for work purposes

Third-party services

28% increase in cloud and SaaS threats over the last year alone[1]

Cyber attacks

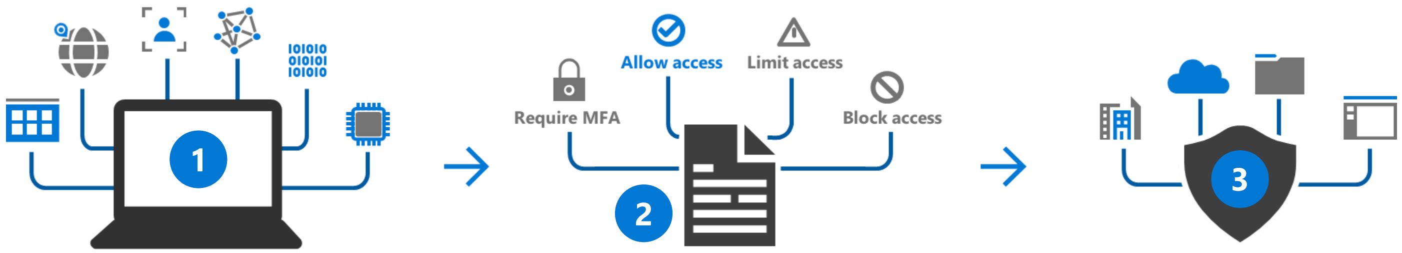
11% increase in cyberattacks in the last year, **67%** over the last five years[2]

Privacy & compliance

Organizations are bombarded by more than **200** updates a day from more than **75** regulatory bodies around the world.

A new approach

Organizations are now charged with protecting organizational resources in a world without boundaries. Enter Zero Trust—the security model that turns the complexity of the modern workplace into an asset. Every asset, activity, and point of connection provides rich context that can be used to make smarter decisions before granting access to organizational resources. Zero Trust's maxim is "trust no one, verify everything." In practical terms this means before a user can access any resource, all requests are fully authenticated, authorized and encrypted in real time.



Validate users and their devices with rich context (normal sign-in location and sign-in risk, etc.)

Make access decisions based on finely-tuned policies that deliver granular access control

Enforce decisions across the entire digital estate

[1] AI reveals 2018's biggest cyber-threats: Part one — the rise of nontraditional IT, Darktrace Blog, January 28, 2019

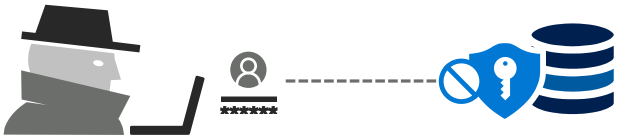
[2] Ninth Annual Cost of Cybercrime Study, Independently conducted by Ponemon Institute LLC and jointly developed by Accenture, 2019

Zero Trust in practice

Because a Zero Trust security model grants access to resources based on organizational policy, access can be fine-tuned to better meet the unique needs of the application and its users.

1 Hacker uses stolen credentials to try and login into company resources

Because of a risky IP address and an unmanaged corporate device, the login attempt is challenged with two factor authentication.

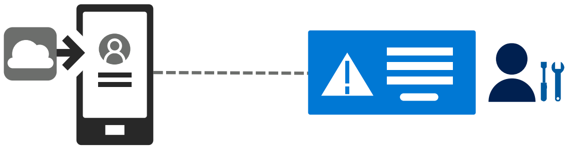


2 Employee needs access to on-premises LOB app while away from their desk

Because user is outside of the corporate network, access privileges are limited to read only.

3 User downloads corporate SaaS app on their personal device

User is prompted to register device with corporate IT to be issued a security certificate, ensuring device compliance and securing user sessions.



4 User needs to share document with external partner

Document has protection label applied that limits document viewing only to authorized users and devices.

5 Employee requests access to corporate resource outside of their business group

Access policy automatically denies access due to a conflict of interest.