

Agenda

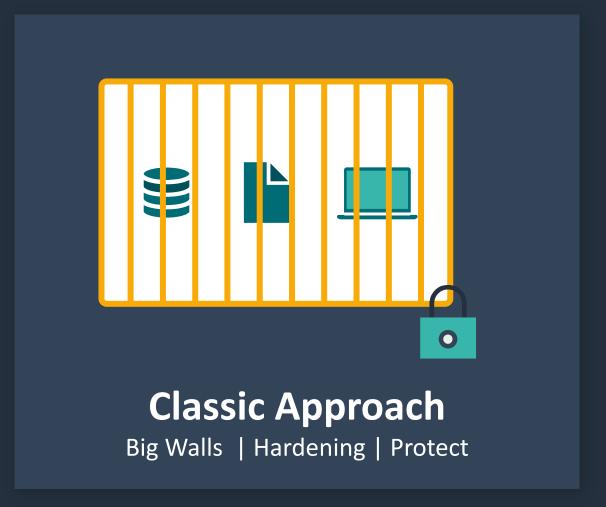
Introduction Microsoft Zero Trust Architecture

BitHawk Zero Trust Project Approach



Introduction Microsoft Zero Trust Architecture

Security Transformation





Principles of Zero Trust







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.

Use least privilege access

Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Assume breach

Minimize blast radius for breaches and prevent lateral movement by segmenting access by network, user, devices, and app awareness.

Verify all sessions are encrypted end to end.

Use analytics to get visibility and drive threat detection and improve defenses.



Zero Trust Objectives







Devices



Data



Infrastructure



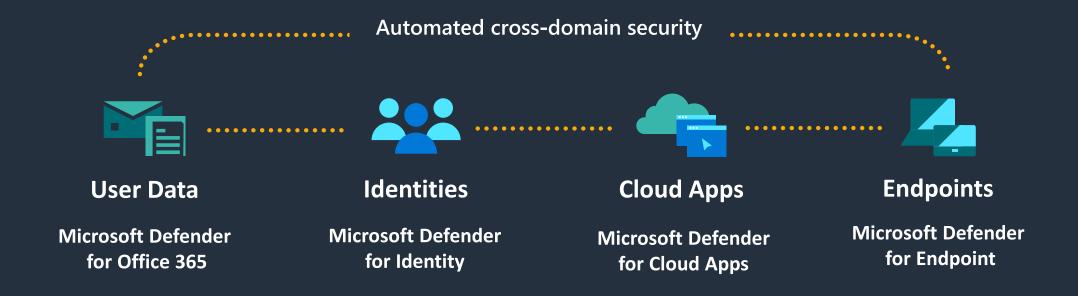
Apps



Network

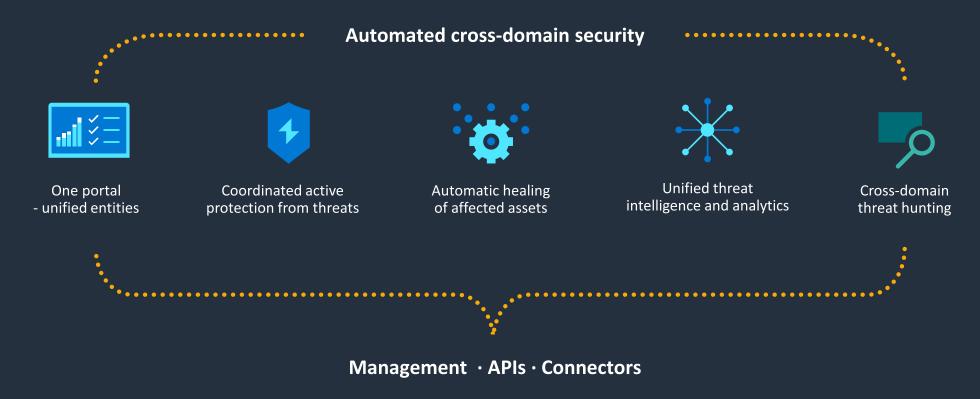
Optimal Advanced **Road to Zero Trust** Traditional Passwordless authentication is Cloud identity federates with On-premises identity enabled on-premises system provider is in use User, device, location, and Conditional access policies No SSO is present behavior is analyzed in real time gate access and provide between cloud and on to determine risk and deliver premises apps remediation actions ongoing protection Visibility into identity Analytics improve visibility risk is very limited Devices are domain joined Devices are registered with Endpoint threat detection is used and managed with cloud identity provider to monitor device risk solutions like Group Policy Object or Config Manager Access only granted to cloud Access control is gated on device managed & compliant devices risk for both corporate and BYO Devices are required to be DLP policies are enforced for on network to access data BYO and corporate devices On-premises apps are On-premises apps are accessed through All apps are available using least physical networks or VPN internet-facing and cloud apps are configured with SSO Some critical cloud apps privilege access with continuous are accessible to users verification Cloud Shadow IT risk is assessed; critical apps are Dynamic control is in place for all monitored and controlled apps with in-session monitoring Permissions are managed manually Workloads are monitored and alerted for abnormal behavior Unauthorized deployments are Every workload is assigned blocked and alert is triggered management of VMs and Granular visibility and access workloads are running Human access to resources control are available across all requires Just-In-Time User and resource access is segmented for each workload micro-perimeters with some Fully distributed ingress/egress cloud micro-perimeters and deeper User to app internal traffic is ML-based threat protection and Atering with context-based signals 101010 010101 101010 **Identities** Infrastructure **Devices** Data **Apps** New

Microsoft 365 Defender Security Products



Shift from individual silos to coordinated cross-domain security

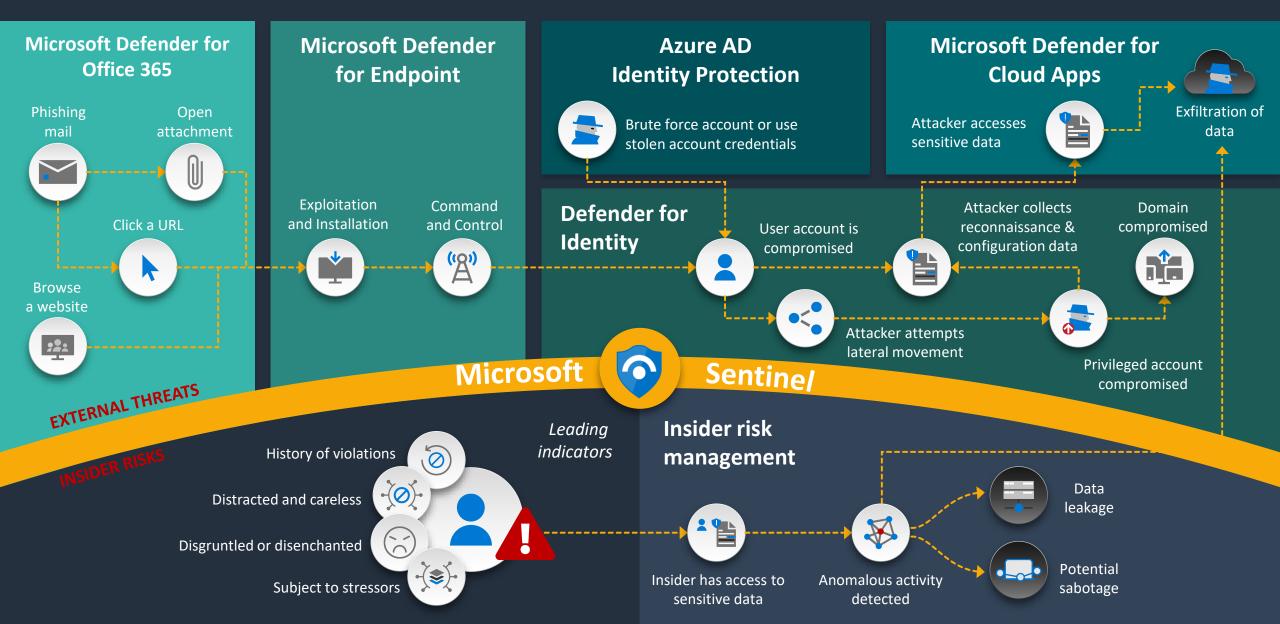
Microsoft 365 Defender

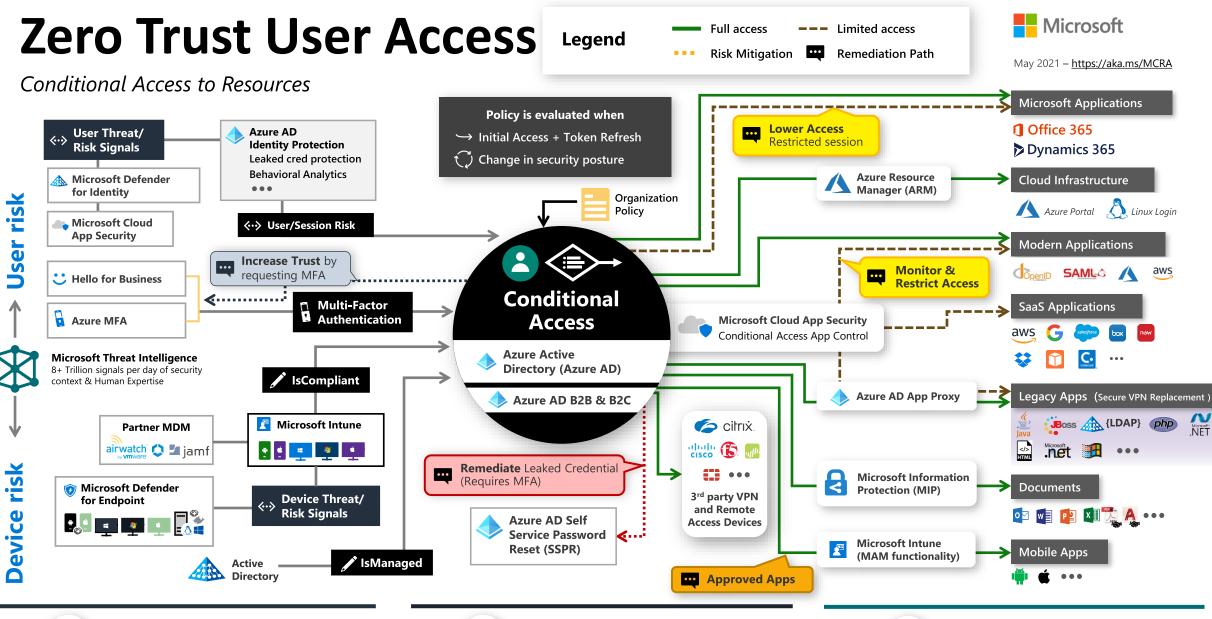


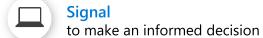
Learn more: http://aka.ms/m365d Try it today: http://security.microsoft.com

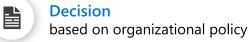
Defend across attack chains

Insider and external threats











BitHawk Zero Trust Projects

BitHawk Zero Trust Project Approach

Customer Inputs

Current Architecture
Requirements
Pain Points
Goals
Compliance

BitHawk Inputs

MS Zero Trust Principles
BitHawk Best Practices
KnowHow and Experience
Innovation



Design Workshops



Concept



Engineering



Proof-of-Concept



Compliance Check



Zero Trust Architecture and Roadmap