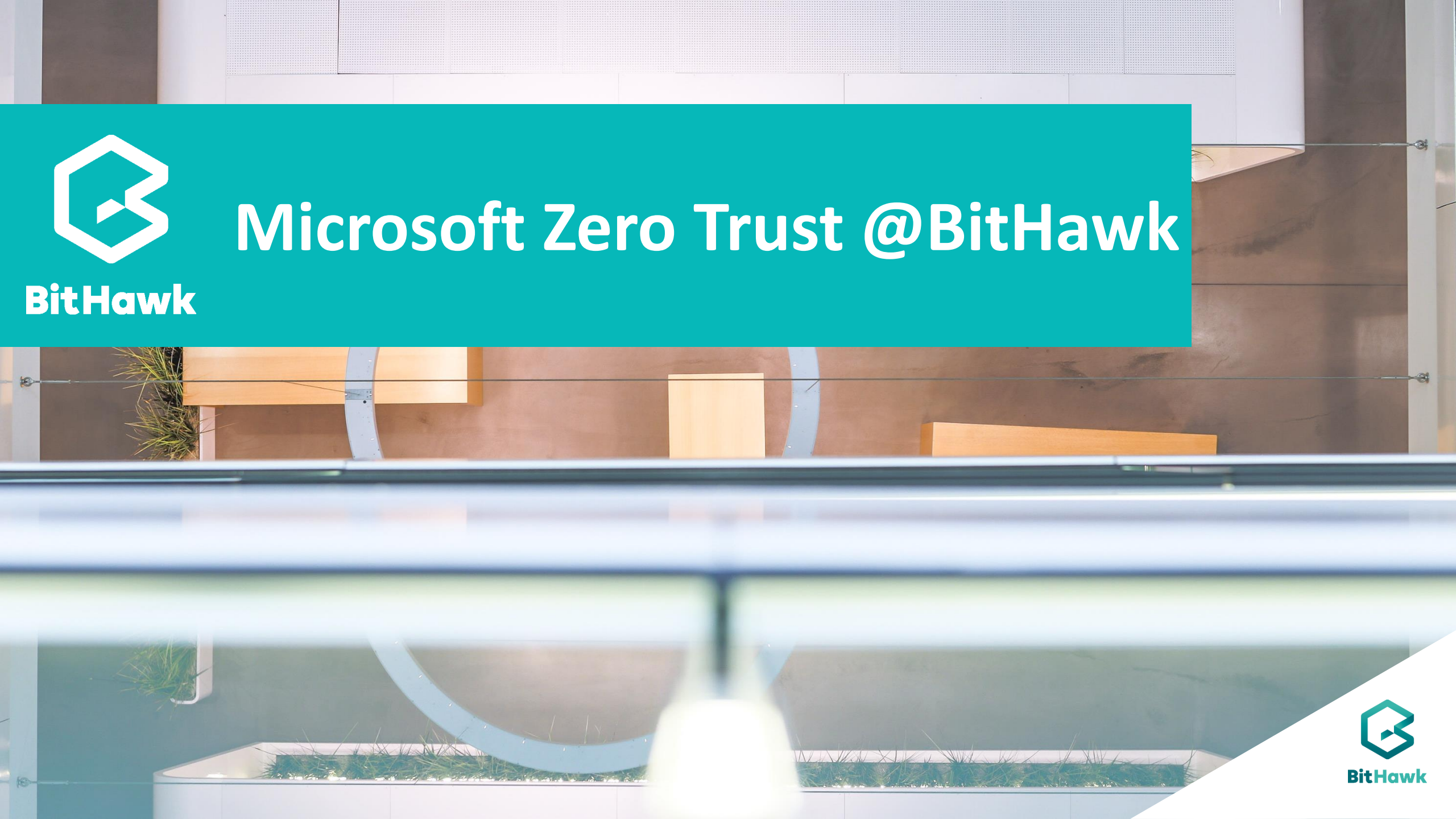


BitHawk

Microsoft Zero Trust @BitHawk

BitHawk

Agenda

Introduction Microsoft Zero Trust Architecture

BitHawk Zero Trust Project Approach

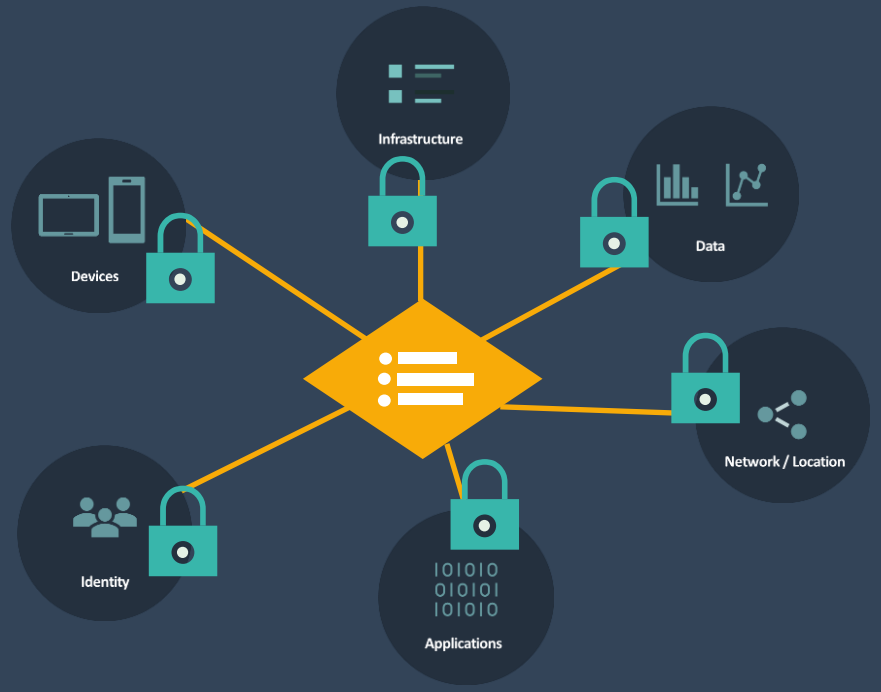
BitHawk

Introduction
Microsoft Zero Trust Architecture

Security Transformation

Classic Approach

Big Walls | Hardening | Protect



Modern Approach

Zero Trust

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

Identities

Devices

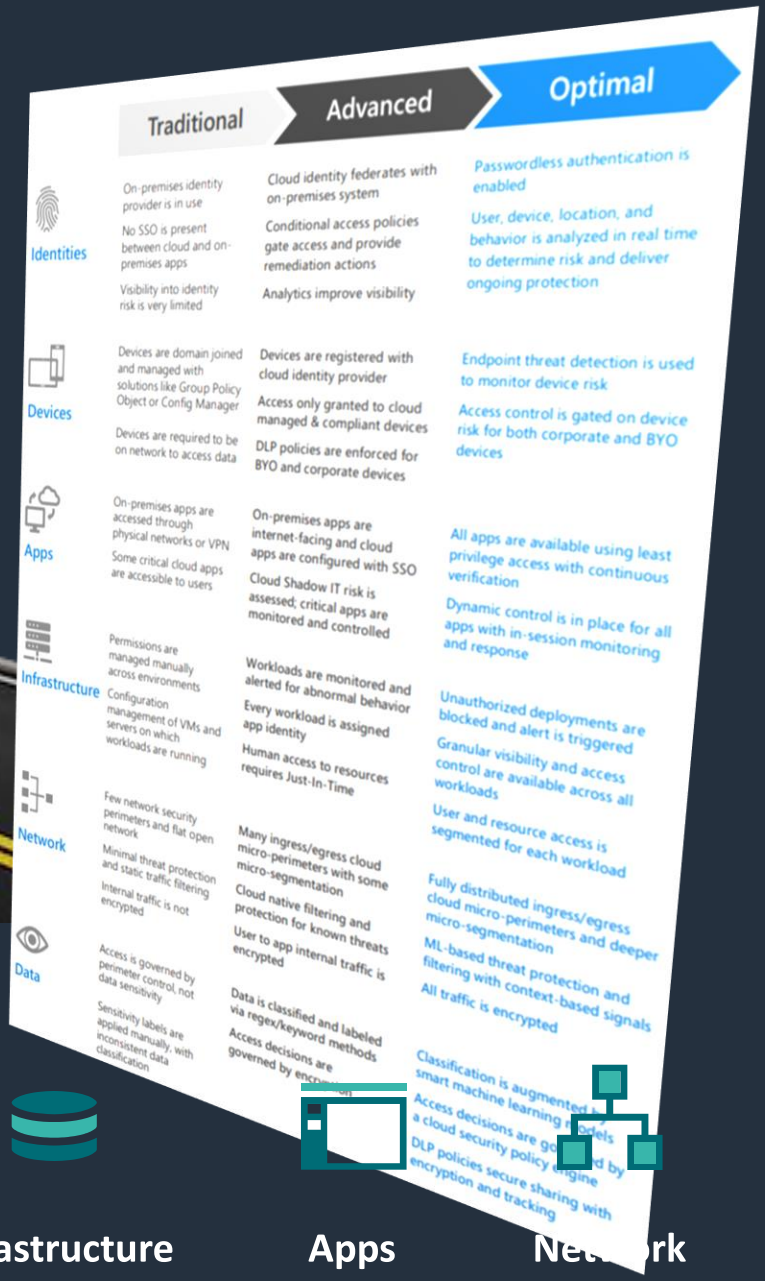
Data

Infrastructure

Apps

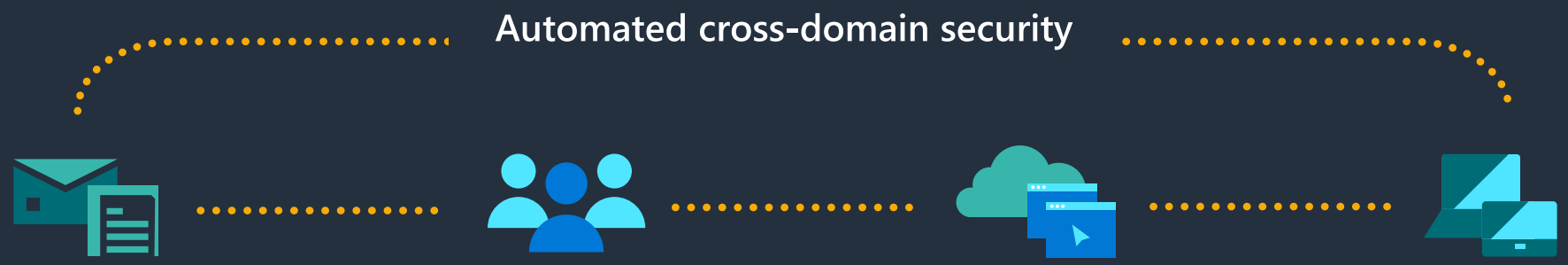
Network

Road to Zero Trust



Identities Devices Data Infrastructure Apps Network

Microsoft 365 Defender Security Products



Shift from individual silos to coordinated cross-domain security

Microsoft 365 Defender

Automated cross-domain security

One portal
- unified entities

Coordinated active protection from threats

Automatic healing of affected assets

Unified threat intelligence and analytics

Cross-domain threat hunting

Management · APIs · Connectors

Learn more: http://aka.ms/m365d

Try it today: http://security.microsoft.com

Defend across attack chains

Insider and external threats

Microsoft Defender for Office 365

Phishing mail

Open attachment

Click a URL

Browse a website

Microsoft Defender for Endpoint

Exploitation and Installation

Command and Control

Azure AD Identity Protection

Brute force account or use stolen account credentials

Microsoft Defender for Cloud Apps

Attacker accesses sensitive data

Exfiltration of data

Defender for Identity

User account is compromised

Attacker collects reconnaissance & configuration data

Domain compromised

Attacker attempts lateral movement

Privileged account compromised

EXTERNAL THREATS

Microsoft Sentinel

INSIDER RISKS

Leading indicators

History of violations

Distracted and careless

Disgruntled or disenchanted

Subject to stressors

Insider risk management

Insider has access to sensitive data

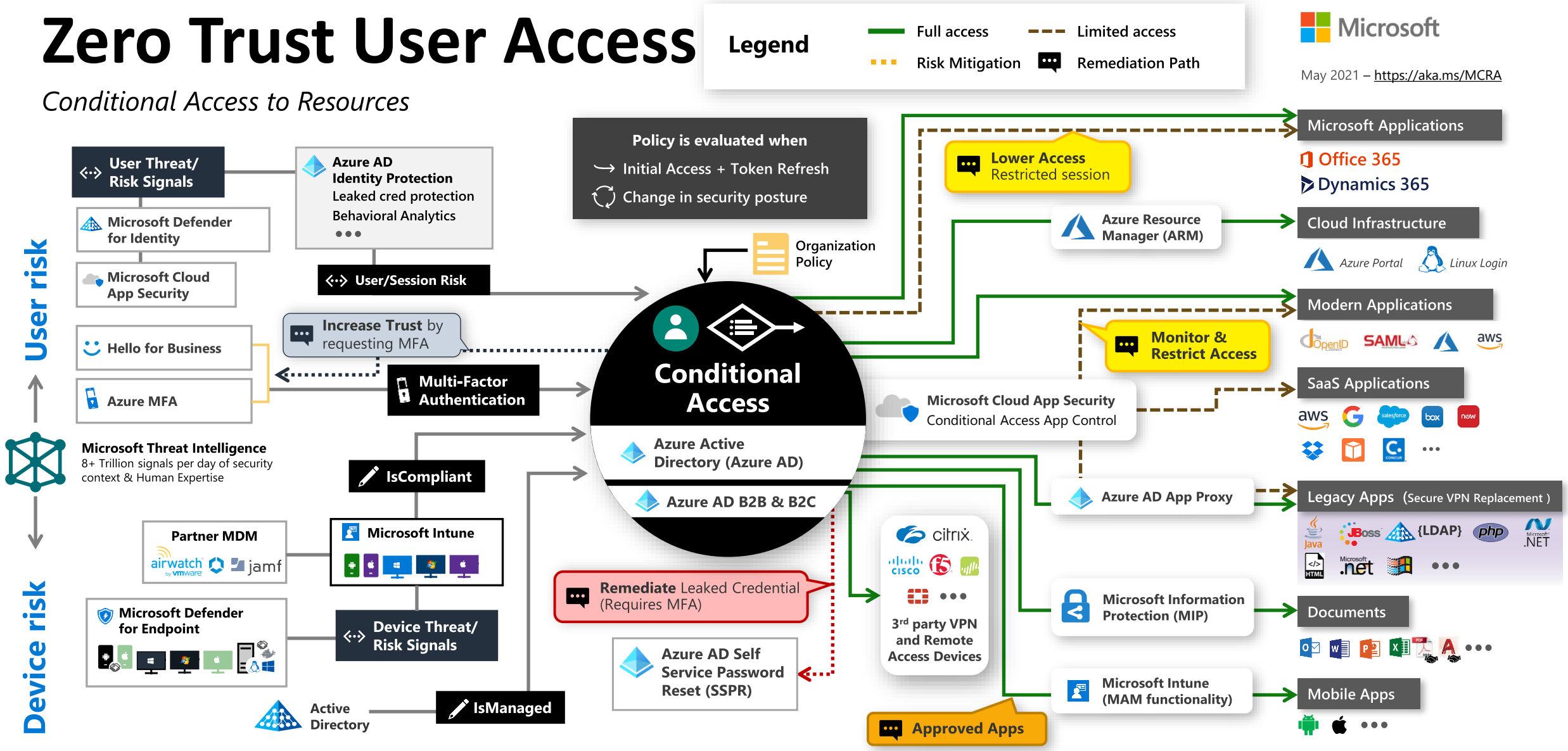
Anomalous activity detected

Data leakage

Potential sabotage

Zero Trust User Access

Conditional Access to Resources



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