

Progetta e realizza il tuo
sistema ed infrastruttura IoT
Sicuro



Sabato 24 settembre 2022

Marco Dal Pino 

Grazie ai nostri sponsor



Technical Consulting Microsoft

Speaker Bio



- 30+ years in IT (Developer, Architect, Consultant, PM, Trainer)
- Speaker, Community addicted
 - IoT Influencer

Sabato 24 settembre 2022



Comprehensive Security, Compliance, and Identity

Cross-cloud and cross-platform capabilities that integrates with your existing solutions

Industry Partnerships

NIST / CIS / The Open Group / Others

Microsoft Intelligent Security Association

Solution Integration and MDR/MSSP Partners

CERTs / ISACs / Others

Law Enforcement

• • •



Microsoft Security, Compliance, and Identity Capabilities

Threat Intelligence – 8+ Trillion signals per day of security context

Access Control Identity and Network



Modern Security Operations Rapid Resolution with XDR, SIEM, SOAR, UEBA and more



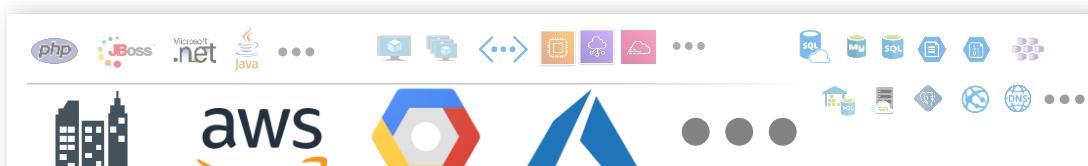
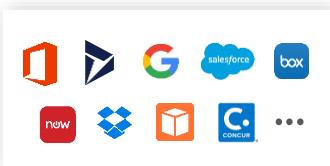
Asset Protection Information Protection and App Security / DevSecOps



Technical Governance Risk Visibility, Scoring, and Policy Enforcement



People Security – User Education/Empowerment and Insider Threats



Endpoints & Devices

Software as a Service (SaaS)

Hybrid Infrastructure – IaaS, PaaS, On-Premises

Operational Technology (OT) and IoT Devices

Security Operations [Center] (SOC) – Reduce attacker time/opportunity to impact business

IoT attacks put businesses at risk



Devices bricked or held for ransom



Devices are used for malicious purposes



Data & IP theft



Data polluted & compromised



Devices used to attack networks

IoT attacks put businesses at risk



Devices bricked or held for ransom



Devices are used for malicious purposes



Data & IP theft



Data polluted & compromised



Devices used to attack networks



The cost of IoT Attacks

Stolen IP & other highly valuable data

Brand impact (loss of trust)

Financial and legal responsibility

Compromised regulatory status or certifications

Recovery costs

Downtime

Security forensics

Microsoft Zero Trust Principles

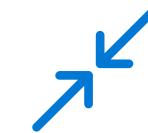
Guidance for technical architecture



Verify explicitly

Always validate all available data points including

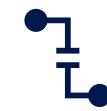
- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies



Use least privilege access

To help secure both data and productivity, limit user access using

- Just-in-time (JIT)
- Just-enough-access (JEA)
- Risk-based adaptive policies
- Data protection against **out of band** vectors



Assume breach

Minimize blast radius for breaches and prevent lateral movement by

- **Segmenting access** by network, user, devices, and app awareness.
- **Encrypting** all sessions end to end.
- **Use analytics** for threat detection, posture visibility and improving defenses

Zero Trust



Strategy to increase security assurances

- **for business assets** data and applications
- **everywhere** including public & untrusted networks

Leads to

User Access

Policy Driven Access
Architecture for
Productivity Environment

1. Explicitly validate trust of access requests
2. Dynamically address insufficient trust

Modern SecOps

Pervasive detection and response

1. Deep asset visibility inside & outside the firewall
2. Rapid remediation with automation and integrated workflows

OT and Datacenter

Monitor and segment assets by business risk

- Workload, App, API, and Device Security
- Operational Technology (OT) + Industrial Internet of Things (IIoT)

Increases security

Increases productivity

Key Zero Trust Initiatives

Prioritize greatest positive impact (often enabling and securing remote work)

User Access (Productivity Environment)

- User Accounts - require passwordless or MFA to access applications + apply threat intelligence and UEBA
- Devices - Require Device Integrity for Access (critically important step)
Increase security for accessing
- Apps - Modern apps + Legacy on-premises/IaaS apps by *modernizing VPN security or going beyond VPN with App Proxy*
- Data - Increased discovery and protection for sensitive data (CASB, CA Access Control, Azure Info Protection)

Governance to continuously monitor and reduce risk (including legacy protocols and applications)

Roll out to IT Admins first

- Targeted by Attackers
- High potential impact
- Provide technical feedback

Modernize Security Operations

- Streamline response to common attacks (Endpoint/Email/Identity)
- Reduce manual effort – using automated investigation/remediation, enforcing alert quality, and proactive threat hunting

OT and IoT Environments
Identify assets with business critical, life safety, and operational/physical impact

- Protection – isolate assets from unneeded internet/production access with static and dynamic controls
- Monitoring – unify threat detection and response processes for OT, IT, and IoT assets

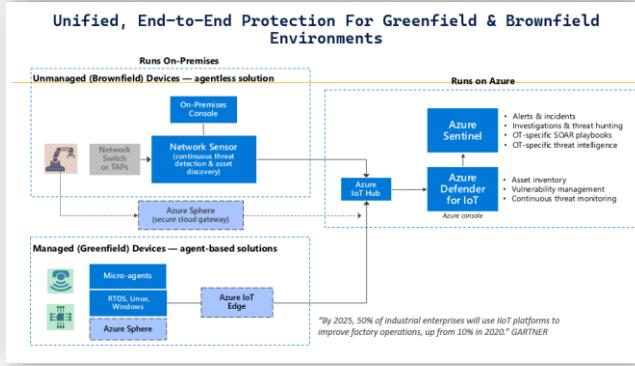
ZT is similar to Classic Security
Align to cloud migration schedule or start after other ZT projects

Datacenter Security

- Retire Legacy - Retire or isolate legacy computing platforms (Unsupported OS/Applications)
- Network Microsegmentation - Additional network restrictions (dynamic trust-based and/or static rules)

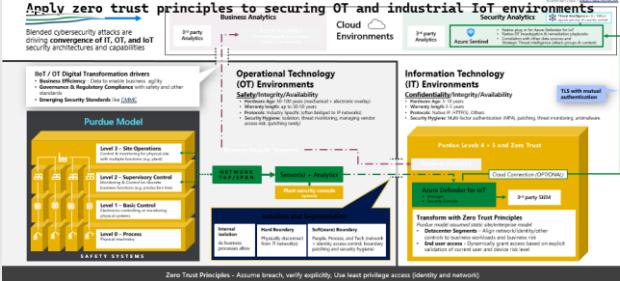
Zero Trust Architectures

IoT + OT Architecture



OT Security

Operational Technology (OT) Security Reference Architecture

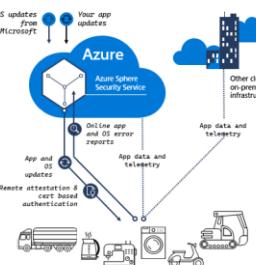


Devices

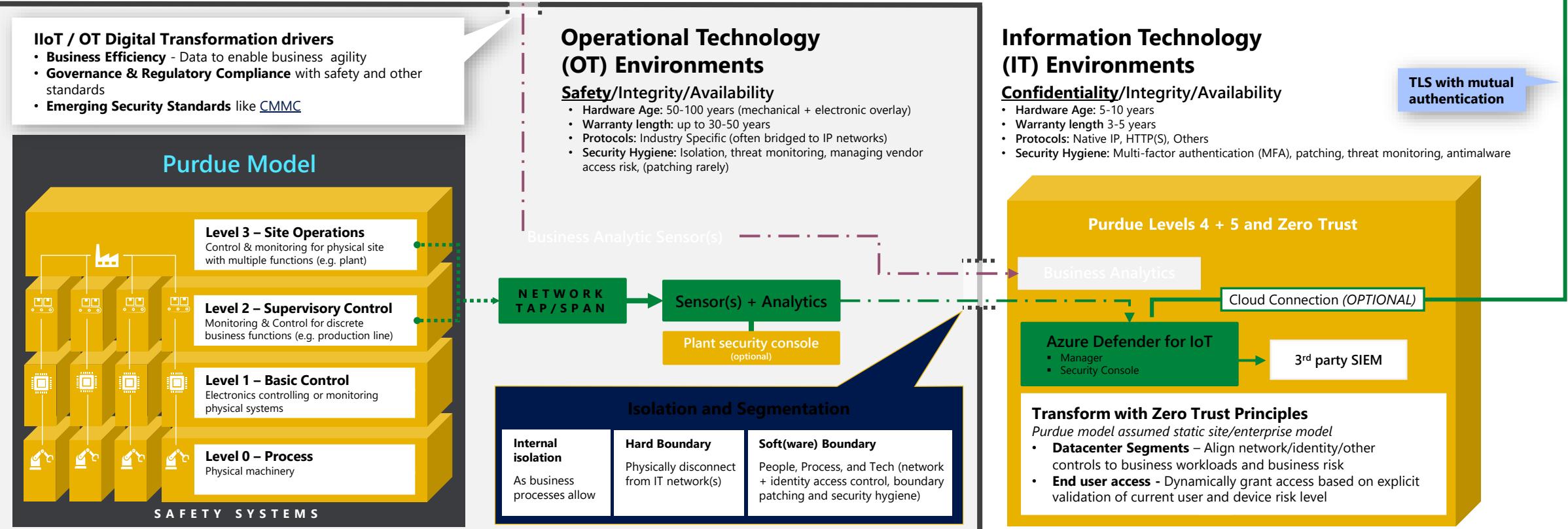
Azure Sphere

Azure Sphere Security Service + Devices

- Protects your devices and your customers with certificate-based authentication of all communication
- Detects emerging security threats through automated processing of on-device failures
- Responds to threats with fully automated on-device updates of OS
- Allows for easy deployment of software updates to Azure Sphere powered devices
- Cloud choice for app data and telemetry



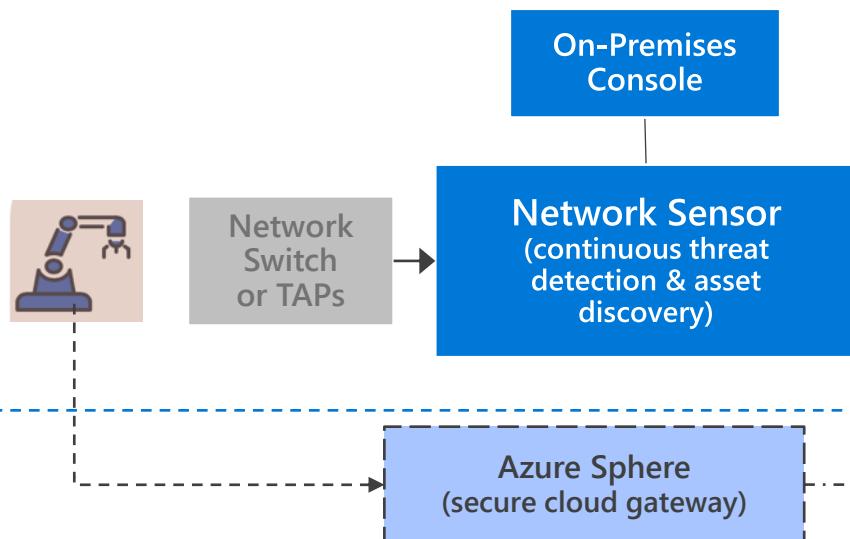
Operational Technology (OT) Security Reference Architecture



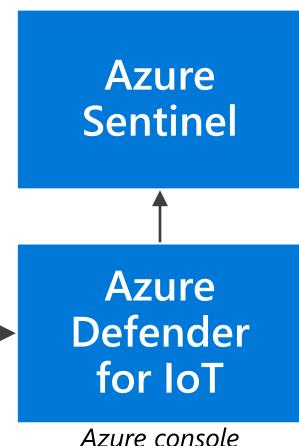
Unified, End-to-End Protection For Greenfield & Brownfield Environments

Runs On-Premises

Unmanaged (Brownfield) Devices — agentless solution



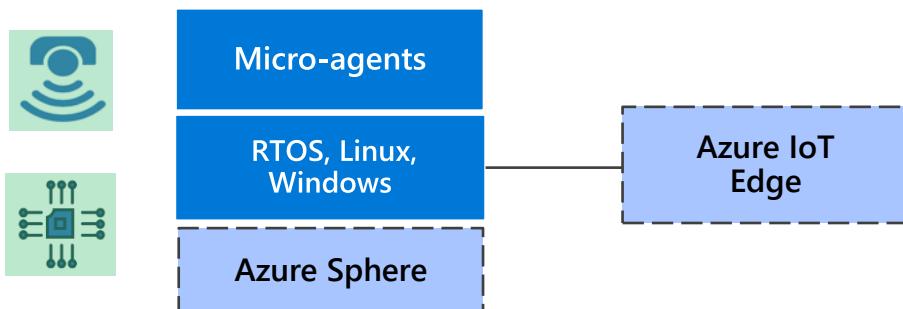
Runs on Azure



- Alerts & incidents
- Investigations & threat hunting
- OT-specific SOAR playbooks
- OT-specific threat intelligence

- Asset inventory
- Vulnerability management
- Continuous threat monitoring

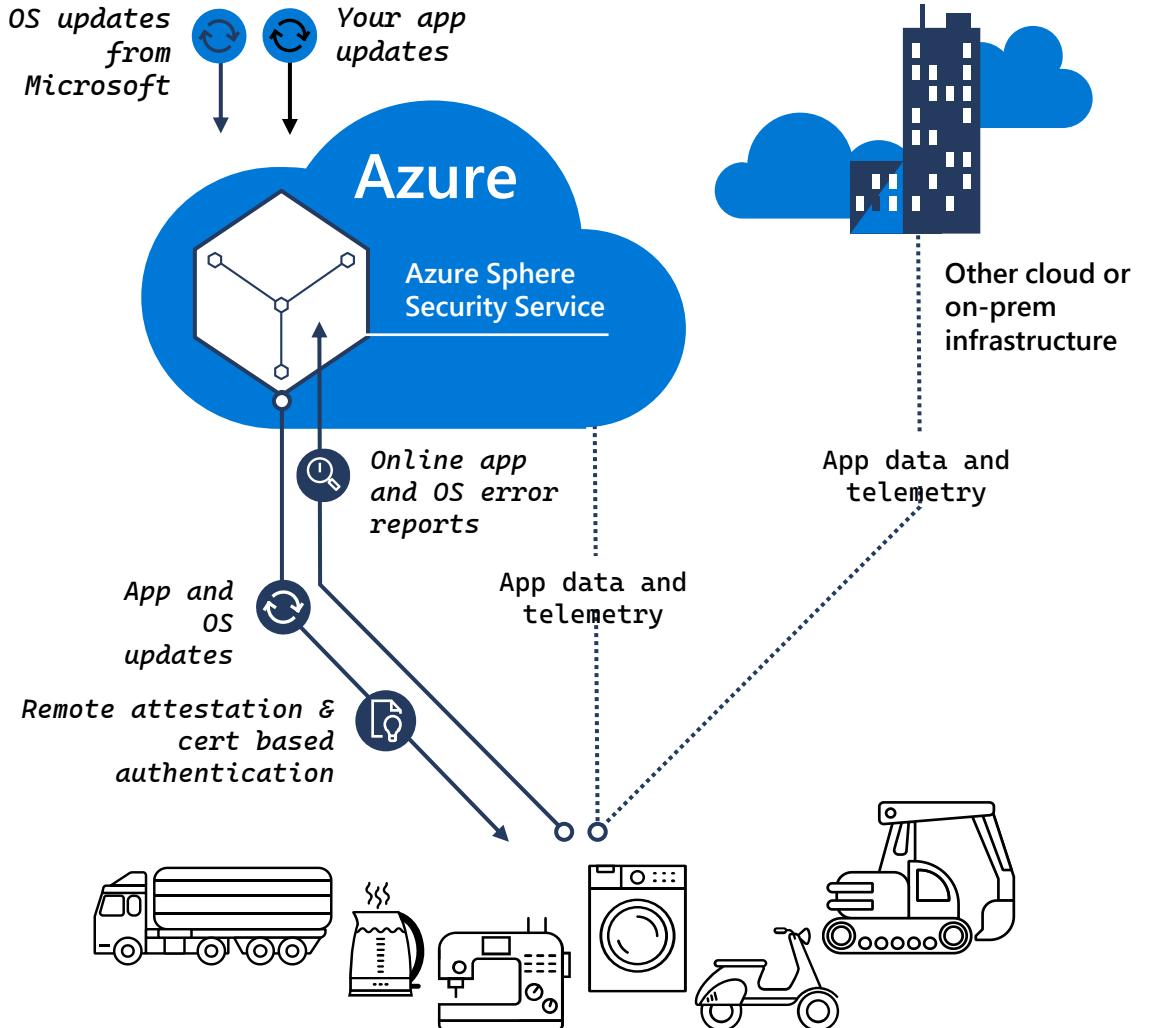
Managed (Greenfield) Devices — agent-based solutions



"By 2025, 50% of industrial enterprises will use IIoT platforms to improve factory operations, up from 10% in 2020." GARTNER

Azure Sphere Security Service + Devices

- Protects your devices and your customers with certificate-based authentication of all communication
- Detects emerging security threats through automated processing of on-device failures
- Responds to threats with fully automated on-device updates of OS
- Allows for easy deployment of software updates to Azure Sphere powered devices
- Cloud choice for app data and telemetry



Understanding when to use what

	More suitable								Less suitable	
Azure RTOS										
Azure Sphere	 Guardian modules									
Windows IoT										

How do I choose what operating system to use?

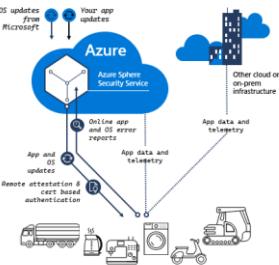
	Azure RTOS	Azure Sphere	Windows 10 IoT
What is it?	An embedded development suite that includes small, fast, reliable and easy-to-use RTOS capabilities for building embedded sensors, and devices – whether they are connected to the Internet or not.	A turnkey device security solution that is purpose-built to allow any developer to create a connected device that is highly secured by default in the everchanging cybersecurity threat landscape.	A member of the Windows 10 family that gives embedded devices a full OS and graphical user interface
When do I use it?	Billions of tiny, resource-constrained devices that require hard real-time processing	Secure IoT apps and devices with seven levels of security and the ability to support a secured root of trust in a smaller footprint.	Specific-use or dedicated devices that need a full Windows OS, complete with graphical user interface.

Zero Trust Architectures

Azure Sphere

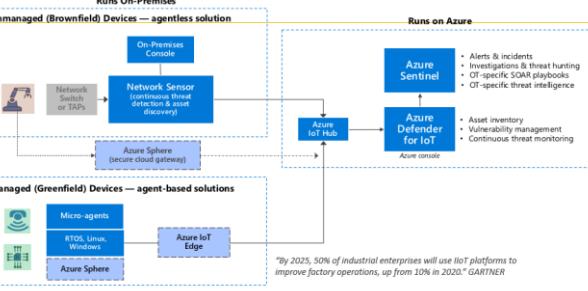
Azure Sphere Security Service + Devices

- Protects your devices and your customers with certificate-based authentication of all communication
- Detects emerging security threats through automated processing of on-device failures
- Responds to threats with fully automated on-device updates of OS
- Allows for easy deployment of software updates to Azure Sphere powered devices
- Cloud choice for app data and telemetry



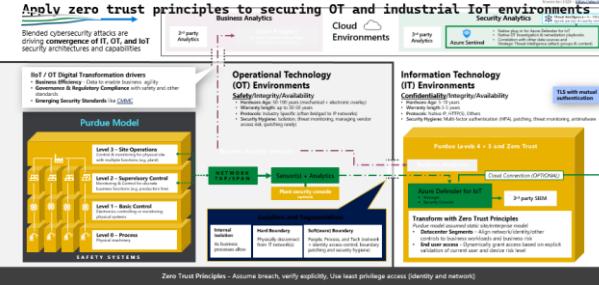
IIoT + OT Architecture

Unified, End-to-End Protection For Greenfield & Brownfield Environments



OT Security

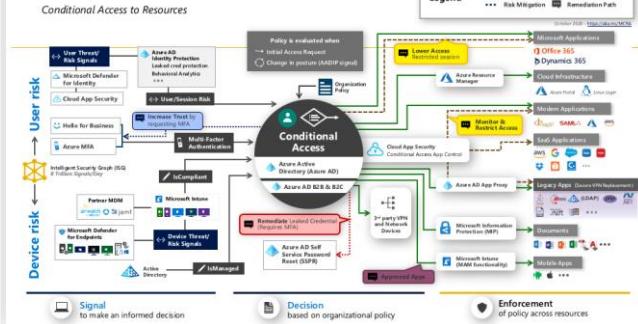
Operational Technology (OT) Security Reference Architecture



Other Zero Trust Architectures

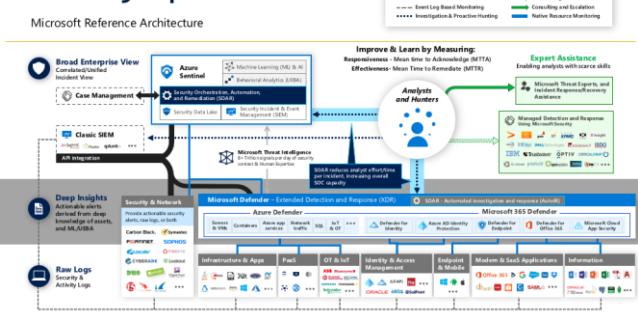
User Access and Productivity

Zero Trust User Access



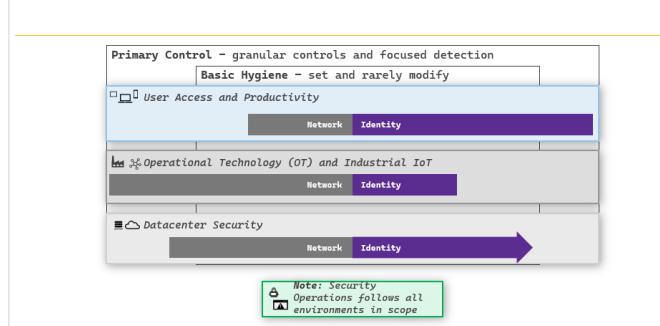
Modernize Security Operations

Security Operations



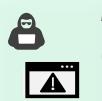
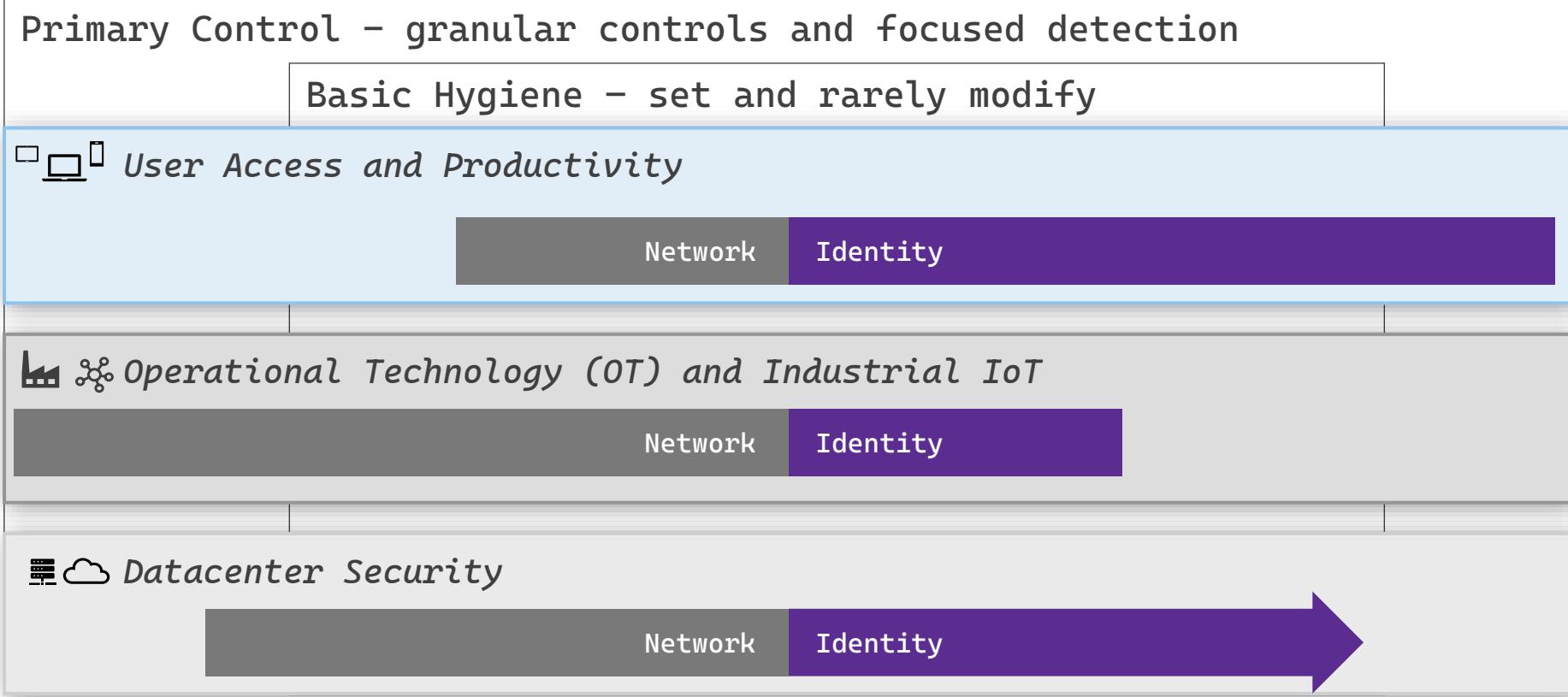
Blend Access Controls

Blend Network and Identity Access Controls



Blend Network and Identity Access Controls

Choose the right tool for the job



Note: Security Operations follows all environments in scope

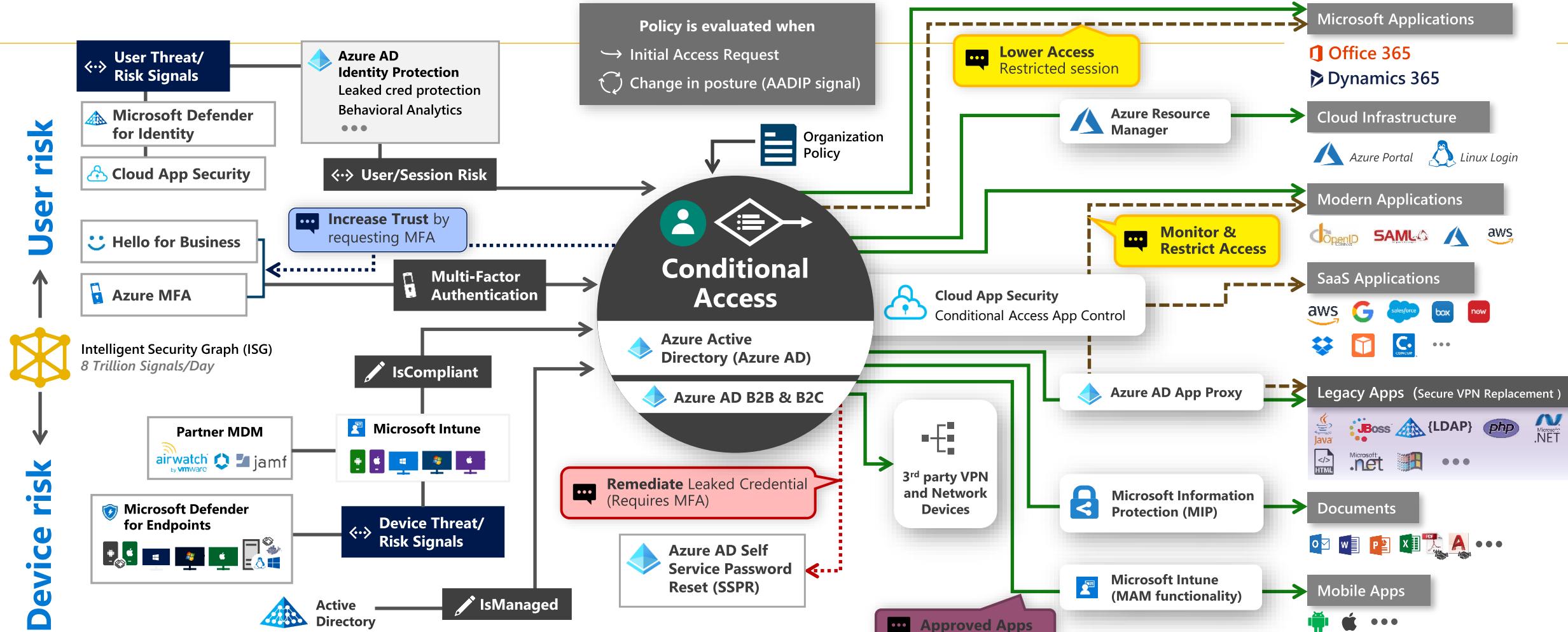
Zero Trust User Access

Conditional Access to Resources

Legend

- Full access
- Limited access
- Risk Mitigation
- Remediation Path

October 2020 – <https://aka.ms/MCRA>



Signal

to make an informed decision



Decision

based on organizational policy

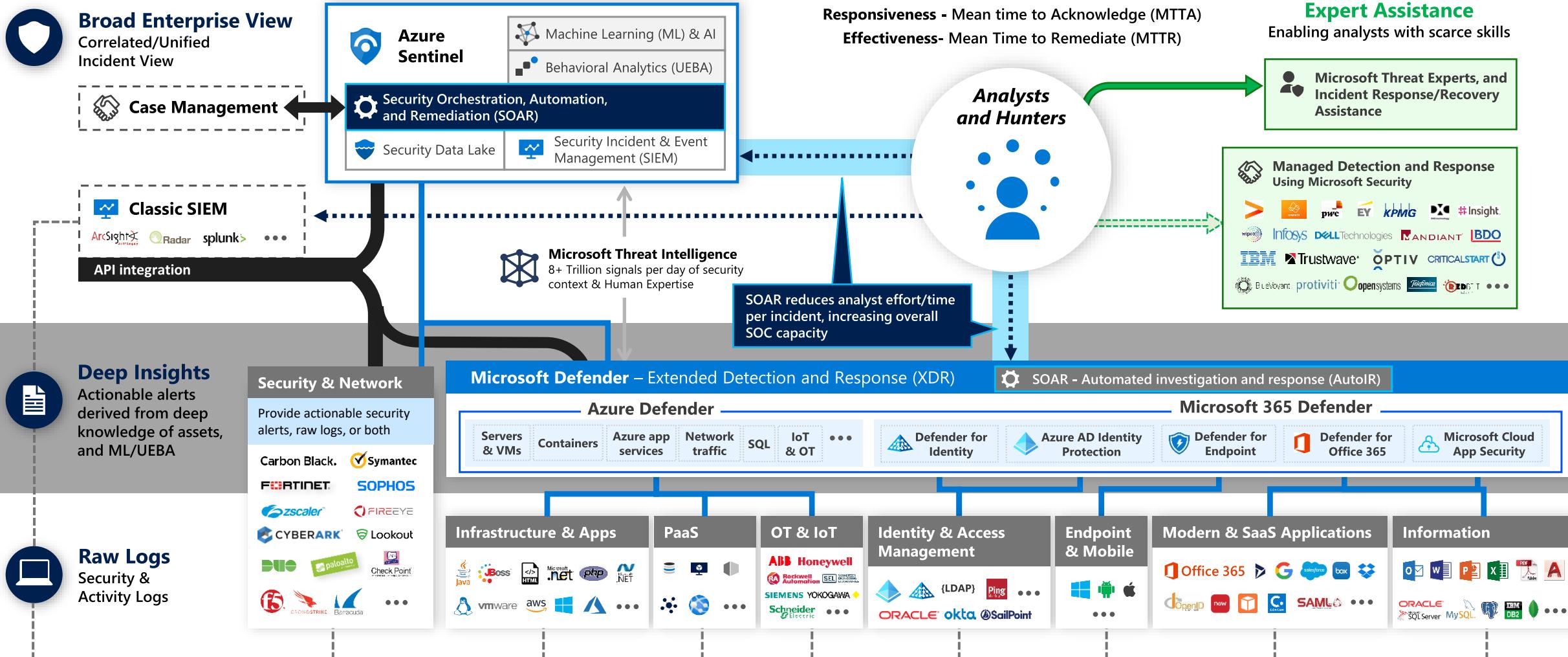


Enforcement

of policy across resources

Security Operations

Microsoft Reference Architecture

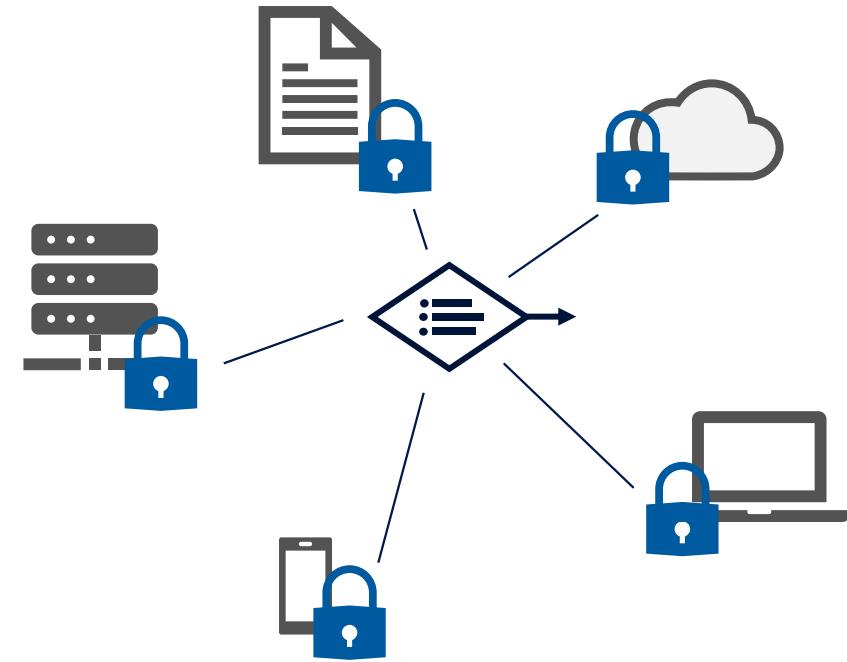


Zero Trust secures assets where they are

enabling secure freedom instead of locking them up in a "secure" network

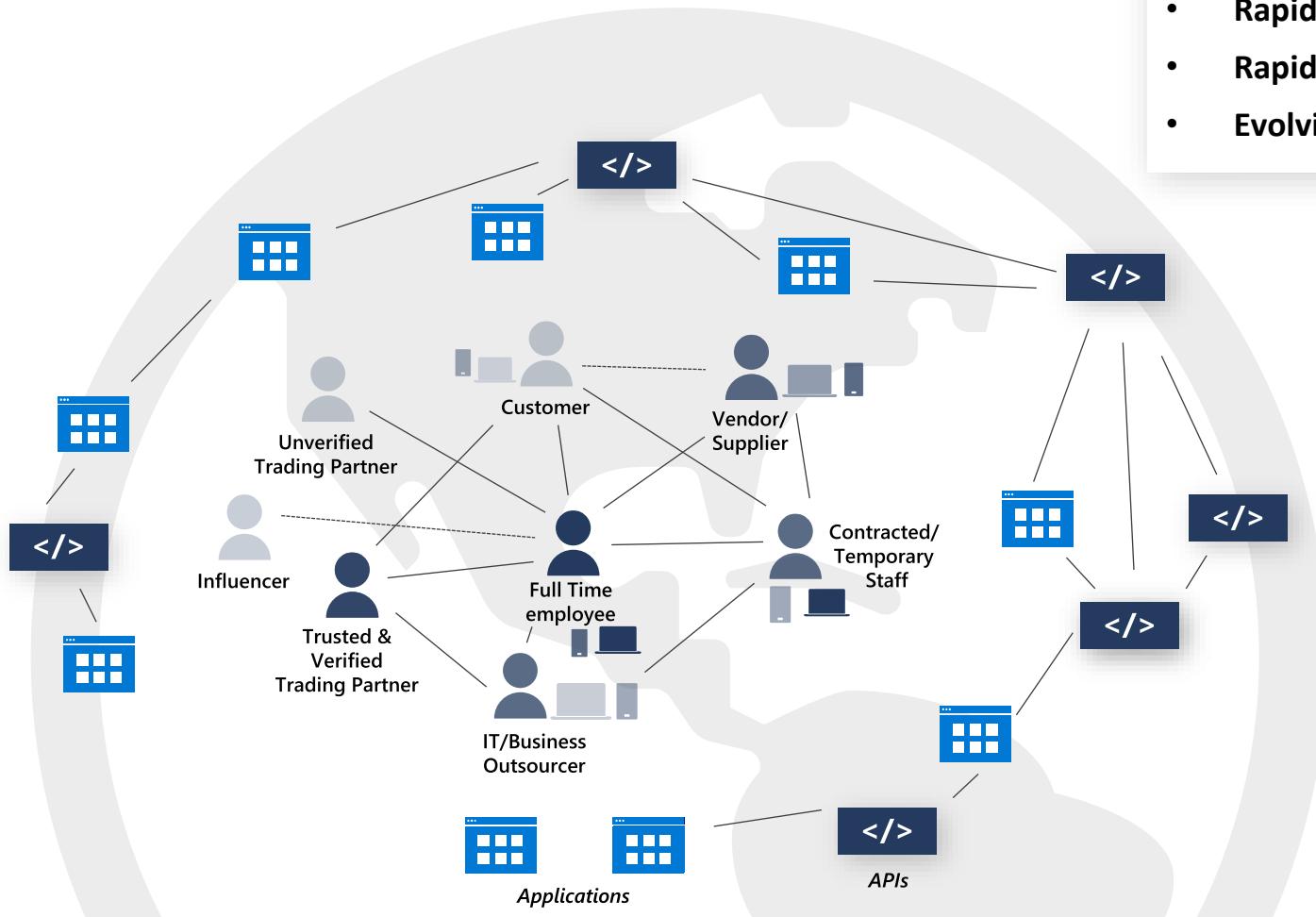


Classic Approach –
Restrict everything to a
'secure' network



Zero Trust – Protect assets
anywhere with central policy

The digitized world is interconnected and dynamic



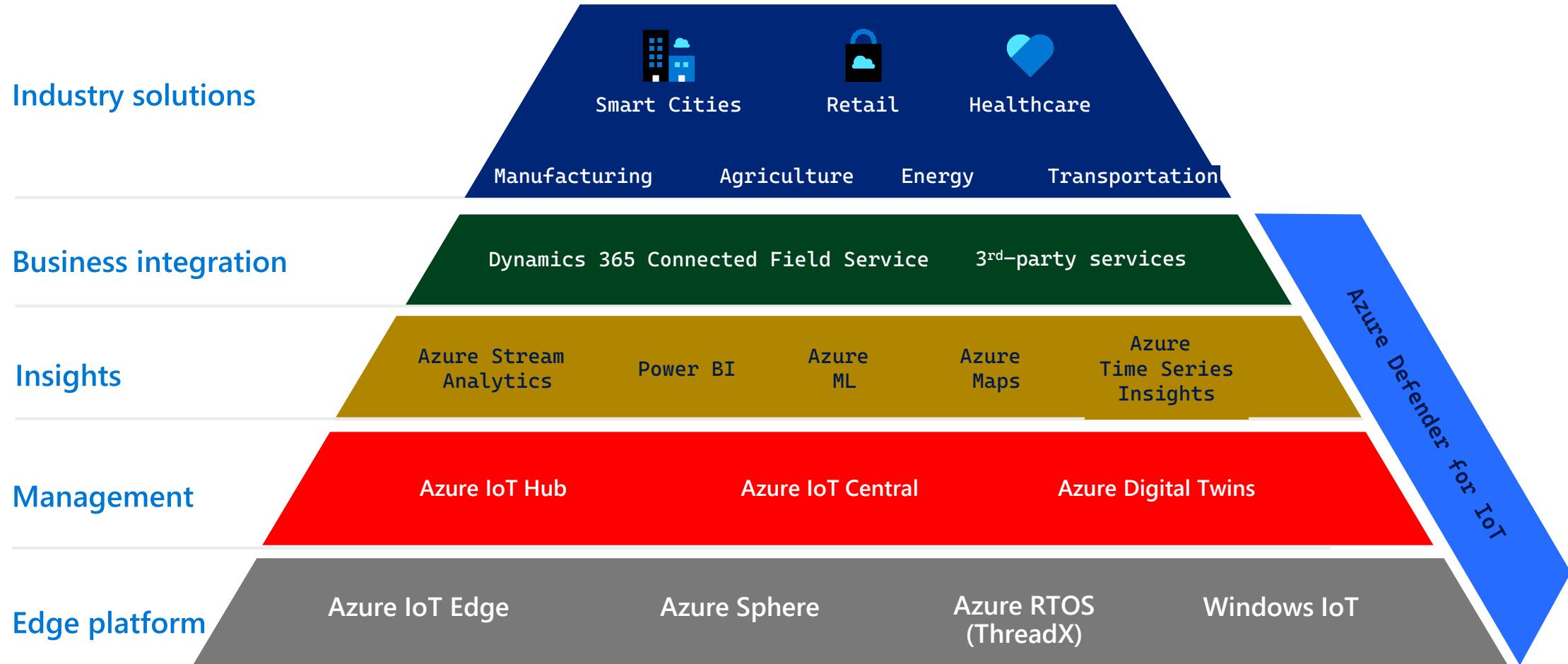
Modern Work Use Cases

- Normalization of remote work
- Rapidly evolving partnerships and competitors
- Rapidly changing communication patterns
- Evolving national interests and regulations

Security Modernization Imperatives

- **Automated Policy Enforcement** - to address changing processes and models in an agile manner at minimum cost
- **Adaptive identity management** - to respond to rapidly changing roles, responsibilities and relationships
- **Data-centric and asset-centric approaches** – to
 - **Better focus security resources** by limiting the scope of what to protect (via trusted zones, tokenization, or similar approaches)
 - **Better monitor assets and respond to threats** regardless of network location.

Enabling and securing IoT from the silicon up





Questions?

Technical Consulting Microsoft

Speaker Bio



- 30+ years in IT (Developer, Architect, Consultant, PM, Trainer)
- Speaker, Community addicted
 - IoT Influencer

Sabato 24 settembre 2022



Thanks!



Sabato 24 settembre 2022

