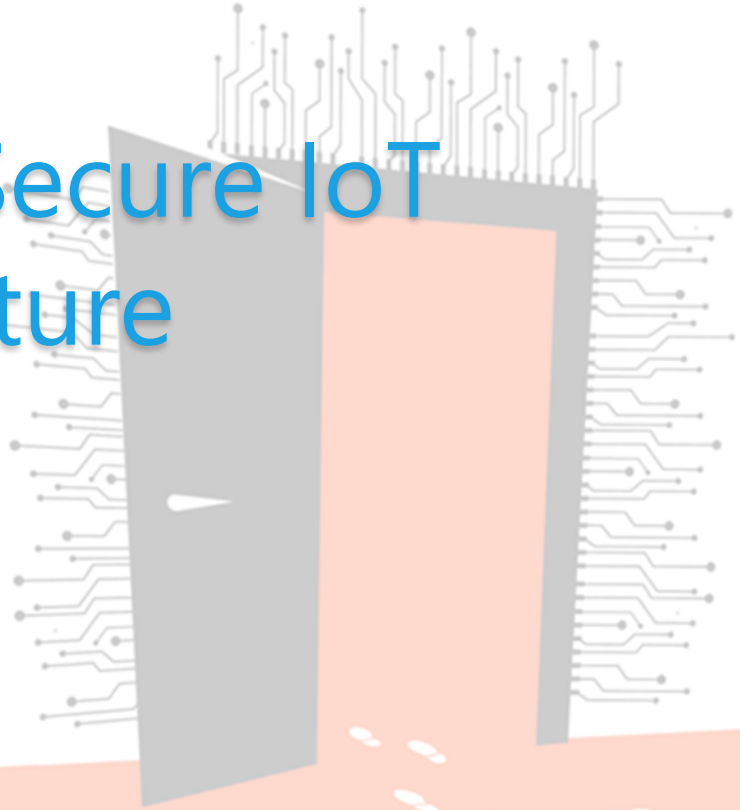
Microsoft

Design and architect your Secure IoT system and infrastructure



AI and IoT Bulgaria Summit, 2022

Sept 17th

Sofia, Bulgaria

by Bulgaria BI & .Net Geeks Group / Azure User Group Bulgaria

Speaker Bio

Technical Consulting
Microsoft

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

https://www.linkedin.com/in/marcodalpino
https://about.me/marcodalpino
https://twitter.com/marcodalpino
info@contoso.blog
https://www.twitch.tv/dpcons

Thanks to our Sponsors

Platinum Sponsors:

Microsoft

Anthill

BOSCH
Invented for life

THE Coca-Cola COMPANY

Gold Sponsor:

Strypes

Silver Sponsor:

epam

Venue Partner:

SOFIA TECH PARK

AI

INTERNET of THINGS

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

Compromised regulatory status or certifications

Brand impact (loss of trust)

Recovery costs

Financial and legal responsibility

Downtime

Security forensics

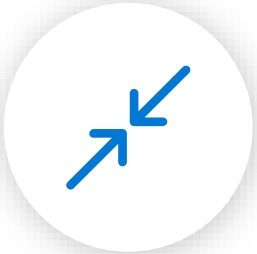
Microsoft Zero Trust Principles

Guidance for technical architecture

Verify explicitly

Always validate all available data points including

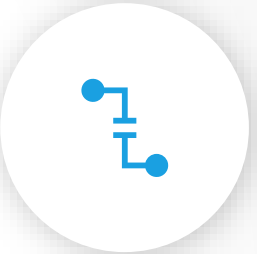
- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies



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** polices
- 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)

Increase and explicitly validate trust for
- **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

- **Visibility –** Discover and classify 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

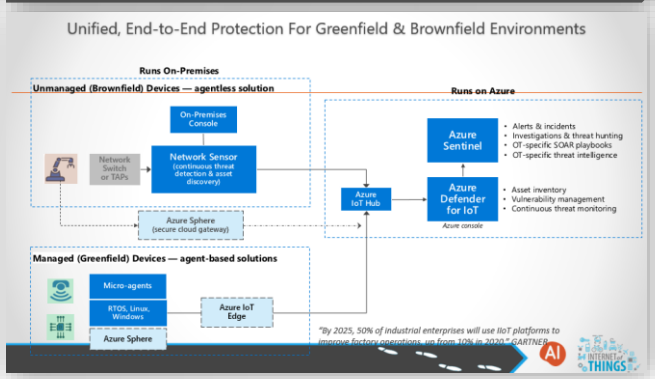
ZT is similar to Classic Security
Align to cloud migration schedule *or* start after other ZT projects

Datacenter Security

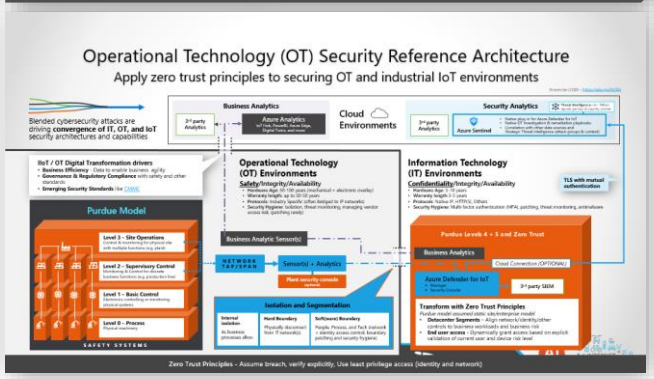
- **Retire Legacy** - Retire or isolate legacy computing platforms (Unsupported OS/Applications)
- **Network Microsegmentation** - Additional network restrictions (dynamic trust-based and/or static rules)

Zero Trust Architectures

IoT + OT Architecture

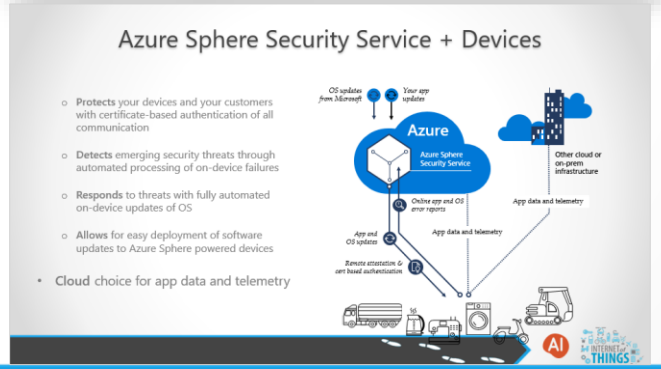


OT Security



Devices

Azure Sphere



Operational Technology (OT) Security Reference Architecture

Apply zero trust principles to securing OT and industrial IoT environments

November 2020 – https://aka.ms/MCRA

Blended cybersecurity attacks are driving **convergence of IT, OT, and IoT** security architectures and capabilities

Business Analytics

3rd party Analytics

Azure Analytics
IoT Hub, PowerBI, Azure Edge, Digital Twins, and more

Cloud Environments

Security Analytics

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

3rd party Analytics

Azure Sentinel

- Native plug-in for Azure Defender for IoT
- Native OT investigation & remediation playbooks
- Correlation with other data sources and Strategic Threat intelligence (attack groups & context)

IIoT / OT Digital Transformation drivers

- **Business Efficiency** - Data to enable business agility
- **Governance & Regulatory Compliance** with safety and other standards
- **Emerging Security Standards** like CMMC

Operational Technology (OT) Environments

Safety/Integrity/Availability

- **Hardware Age:** 50-100 years (mechanical + electronic overlay)
- **Warranty length:** up to 30-50 years
- **Protocols:** Industry Specific (often bridged to IP networks)
- **Security Hygiene:** Isolation, threat monitoring, managing vendor access risk, (patching rarely)

Information Technology (IT) Environments

Confidentiality/Integrity/Availability

- **Hardware Age:** 5-10 years
- **Warranty length** 3-5 years
- **Protocols:** Native IP, HTTP(S), Others
- **Security Hygiene:** Multi-factor authentication (MFA), patching, threat monitoring, antimalware

TLS with mutual authentication

Purdue Model

Level 3 – Site Operations
Control & monitoring for physical site with multiple functions (e.g. plant)

Level 2 – Supervisory Control
Monitoring & Control for discrete business functions (e.g. production line)

Level 1 – Basic Control
Electronics controlling or monitoring physical systems

Level 0 – Process
Physical machinery

SAFETY SYSTEMS

Business Analytic Sensor(s)

NETWORK TAP/SPAN

Sensor(s) + Analytics

Plant security console (optional)

Isolation and Segmentation

Internal isolation	Hard Boundary	Soft(ware) Boundary
As business processes allow	Physically disconnect from IT network(s)	People, Process, and Tech (network + identity access control, boundary patching and security hygiene)

Purdue Levels 4 + 5 and Zero Trust

Business Analytics

Cloud Connection *(OPTIONAL)*

Azure Defender for IoT
- Manager
- Security Console

3rd party SIEM

Transform with Zero Trust Principles

Purdue model assumed static site/enterprise model

- **Datacenter Segments** – Align network/identity/other controls to business workloads and business risk
- **End user access -** Dynamically grant access based on explicit validation of current user and device risk level

Zero Trust Principles - Assume breach, verify explicitly, Use least privilege access (identity and network)

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

Runs On-Premises

Unmanaged (Brownfield) Devices — agentless solution

Network Switch or TAPs

On-Premises Console

Network Sensor (continuous threat detection & asset discovery)

Azure Sphere (secure cloud gateway)

Runs on Azure

Azure IoT Hub

Azure Sentinel

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

Azure Defender for IoT

- Asset inventory
- Vulnerability management
- Continuous threat monitoring

Azure console

Managed (Greenfield) Devices — agent-based solutions

Micro-agents

RTOS, Linux, Windows

Azure Sphere

Azure IoT Edge

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

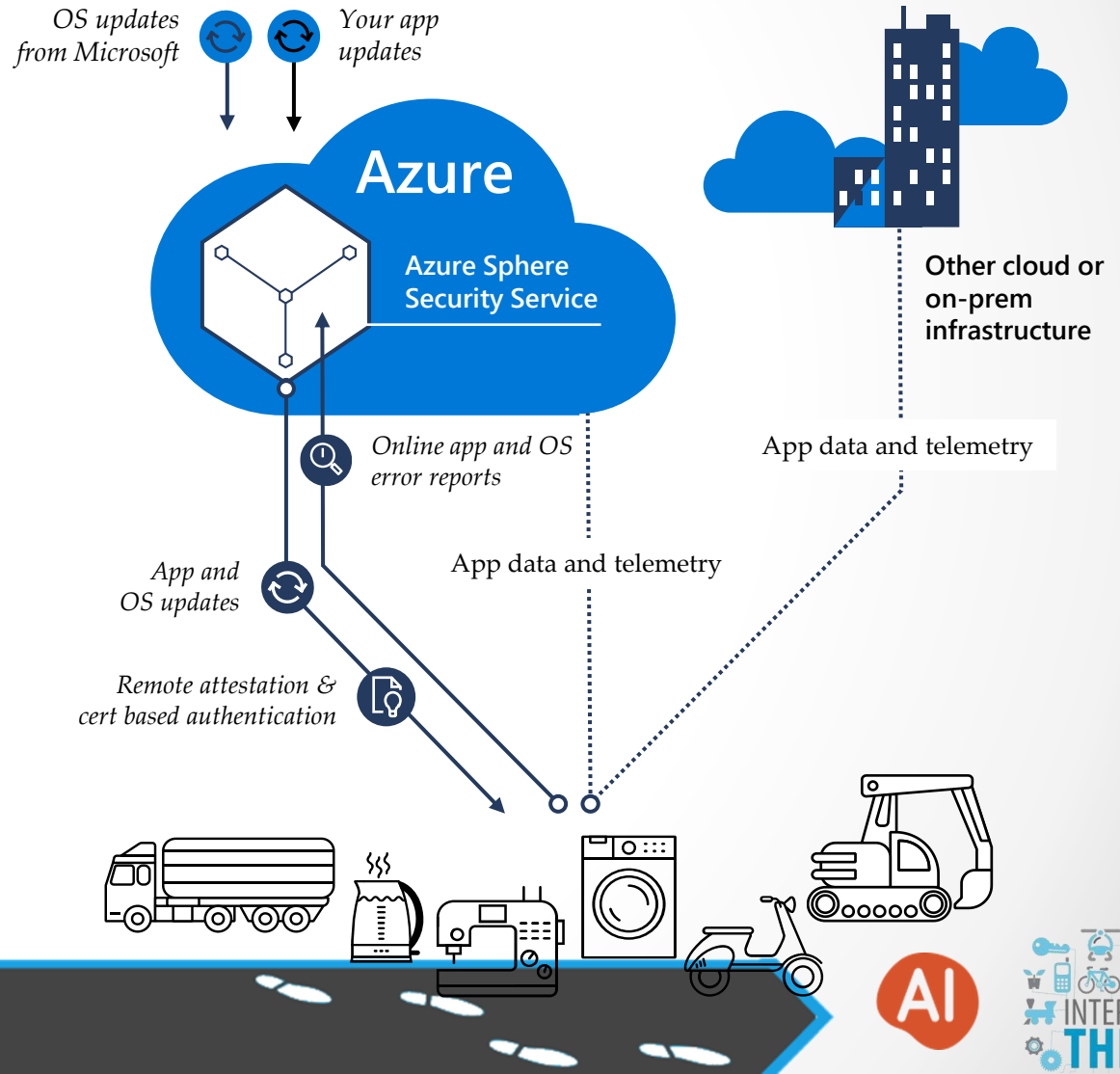
AI

INTERNET of THINGS

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


Smart phones


Fitness trackers


Sensors


Consumer Electronics


Thermostats, Smoke Alarms


Medical diagnostics


POS, Kiosks ATMs, Gas Pumps, Vending, Digital signage


PLC/Indus. Automation Embedded Servers

Azure Sphere


Connector Boards Guardian modules


Medical diagnostics


Home appliances


IOT Gateways


Consumer Electronics


Smart phones


Fitness trackers

Windows IoT


POS, Kiosks ATMs, Gas Pumps, Vending, Digital signage


HMIs, PLC/Indus. Automation Embedded Servers


MRI, Xray devices


Industrial Robots & gateways


Consumer Electronics


Smart phones


Fitness trackers

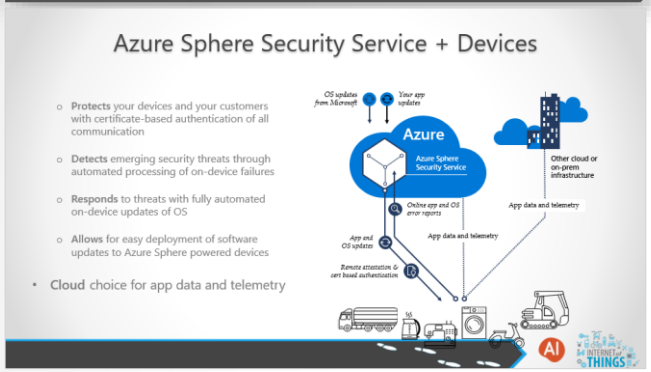

Sensors

How do I choose what operating system to use?

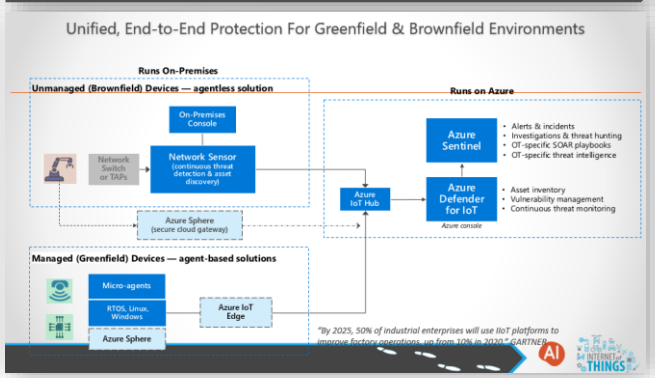
	Azure RTOS	Azure Sphere	Windows 10 IOT
What is it?	An embedded development suite that includes small, fast, reliable and easy-to-use RTOS capabilities for building embedded sensors, and devices – whether they are connected to the Internet or not.	A turnkey device security solution that is purpose-built 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

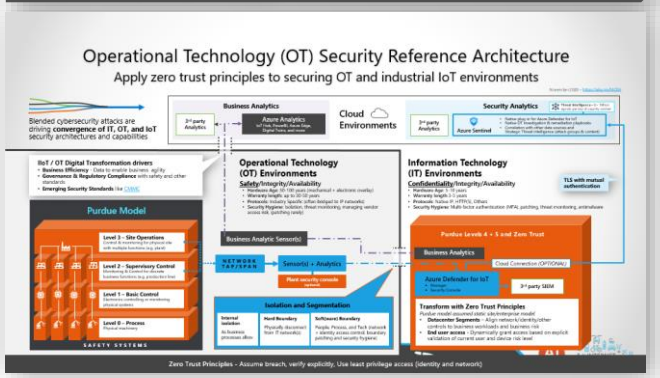
Azure Sphere



IIoT + OT Architecture

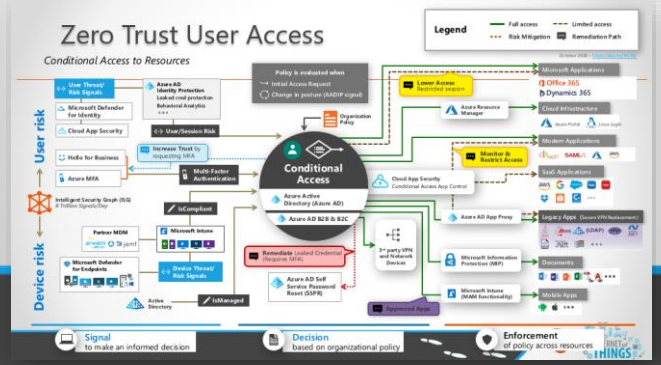


OT Security

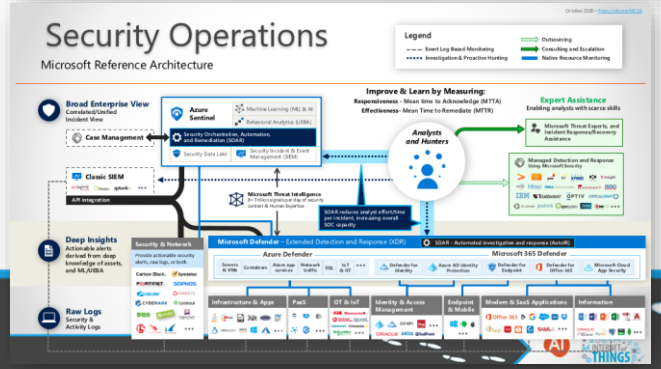


Other Zero Trust Architectures

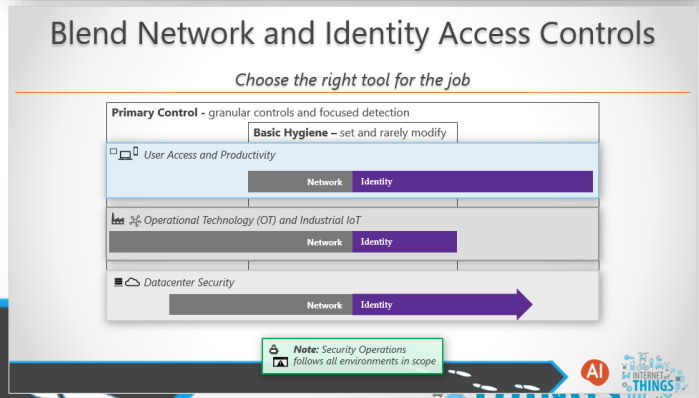
User Access and Productivity



Modernize Security Operations

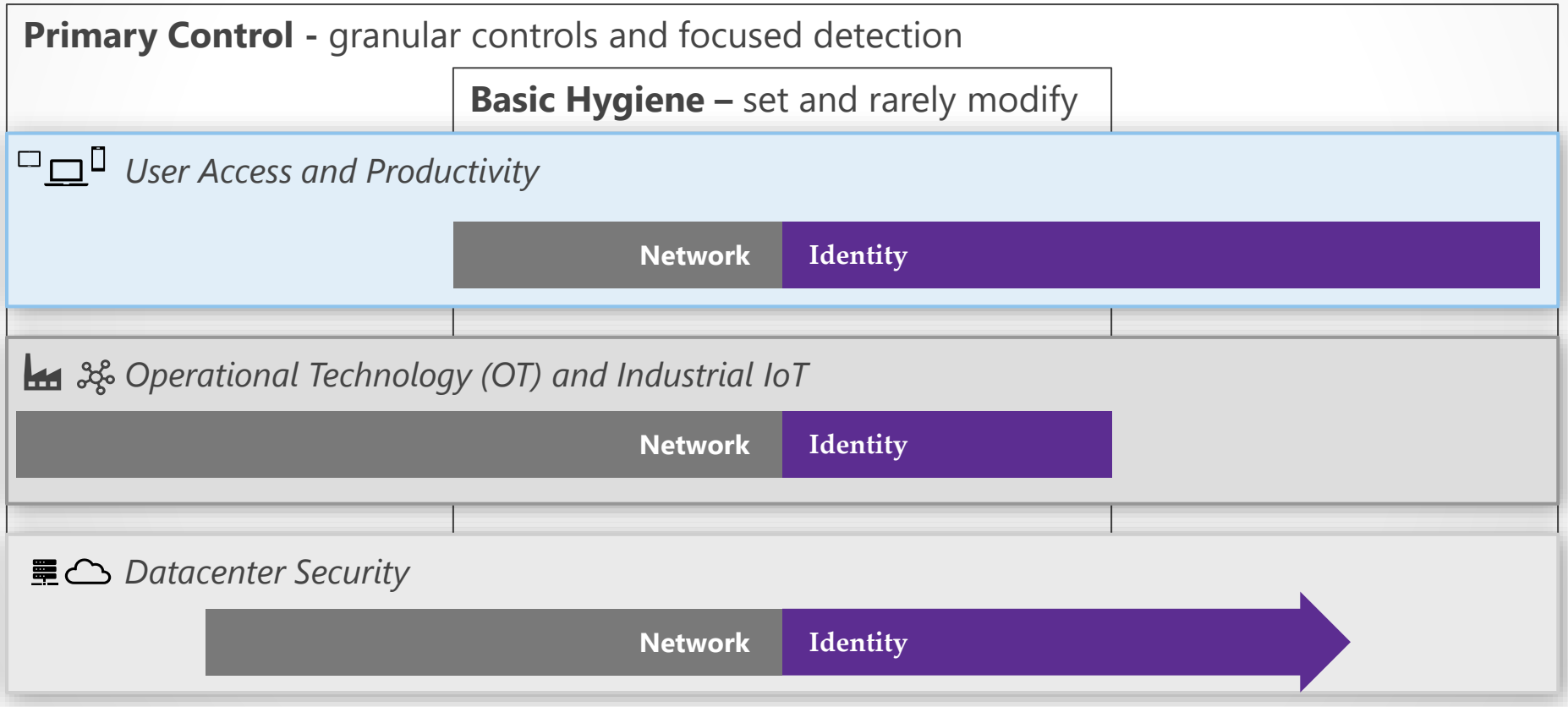


Blend Access Controls



Blend Network and Identity Access Controls

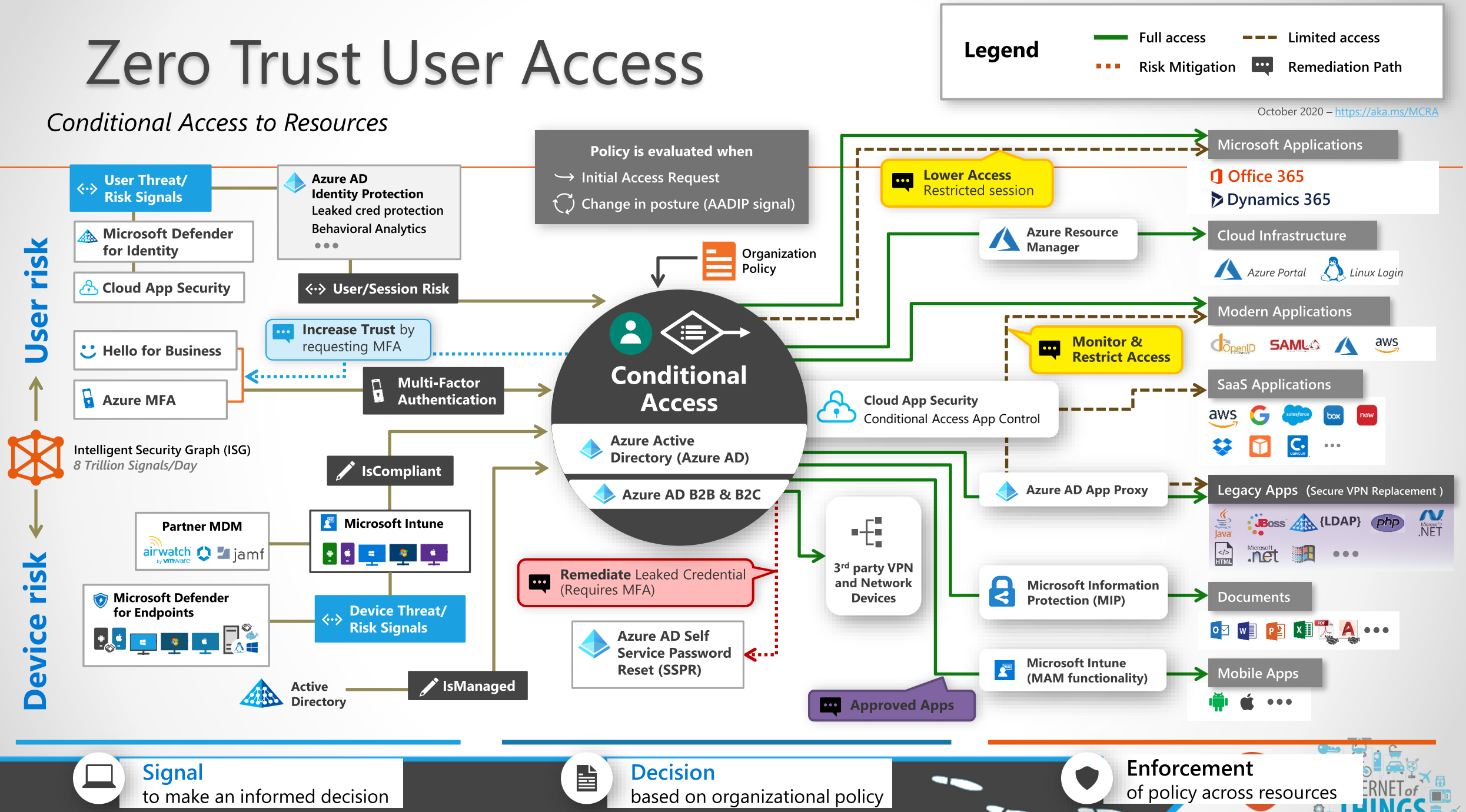
Choose the right tool for the job



Note: *Security Operations follows all environments in scope*

Zero Trust User Access

Conditional Access to Resources



Security Operations

Microsoft Reference Architecture

Legend

- Event Log Based Monitoring
- Investigation & Proactive Hunting
- Outsourcing
- Consulting and Escalation
- Native Resource Monitoring

Improve & Learn by Measuring:

Responsiveness - Mean time to Acknowledge (MTTA)

Effectiveness- Mean Time to Remediate (MTTR)

Broad Enterprise View

Correlated/Unified Incident View

Case Management

Azure Sentinel

- Machine Learning (ML) & AI
- Behavioral Analytics (UEBA)
- Security Orchestration, Automation, and Remediation (SOAR)
- Security Data Lake
- Security Incident & Event Management (SIEM)

Classic SIEM

ArcSight, Radar, splunk>, ...

API integration

Microsoft Threat Intelligence

8+ Trillion signals per day of security context & Human Expertise

SOAR reduces analyst effort/time per incident, increasing overall SOC capacity

Analysts and Hunters

Expert Assistance

Enabling analysts with scarce skills

Microsoft Threat Experts, and Incident Response/Recovery Assistance

Managed Detection and Response Using Microsoft Security

Deep Insights

Actionable alerts derived from deep knowledge of assets, and ML/UEBA

Security & Network

Provide actionable security alerts, raw logs, or both

Carbon Black., Symantec, FORTINET, SOPHOS, zscaler, FIREEYE, CYBERARK, Lookout, DUO, paloalto, Check Point, f5, CROWDSTRIKE, Barracuda, ...

Microsoft Defender – Extended Detection and Response (XDR)

SOAR - Automated investigation and response (AutoIR)

Azure Defender

Servers & VMs | Containers | Azure app services | Network traffic | SQL | IoT & OT | ...

Microsoft 365 Defender

Defender for Identity | Azure AD Identity Protection | Defender for Endpoint | Defender for Office 365 | Microsoft Cloud App Security

Infrastructure & Apps

Java, JBoss, HTML, Microsoft .net, php, .NET, vmware, aws, ...

PaaS

OT & IoT

ABB, Honeywell, Rockwell Automation, SEL, SIEMENS, YOKOGAWA, Schneider Electric, ...

Identity & Access Management

{LDAP}, Ping, ORACLE, okta, SailPoint, ...

Endpoint & Mobile

Modern & SaaS Applications

Office 365, salesforce, box, OpenID, now, SAML, ...

Information

ORACLE, SQL Server, MySQL, IBM DB2, ...

Raw Logs

Security & Activity Logs

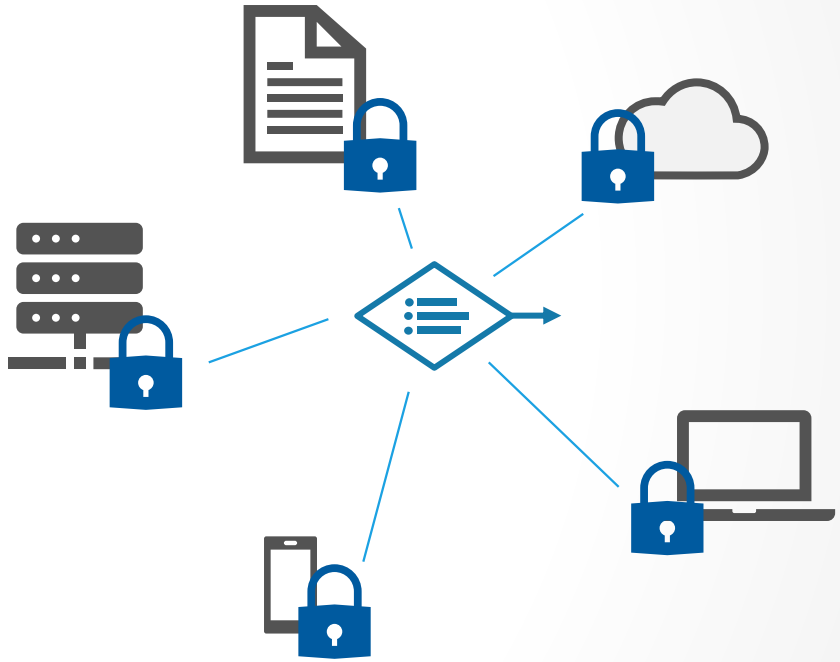
AI

INTERNET of THINGS

Zero Trusts secures assets where they are

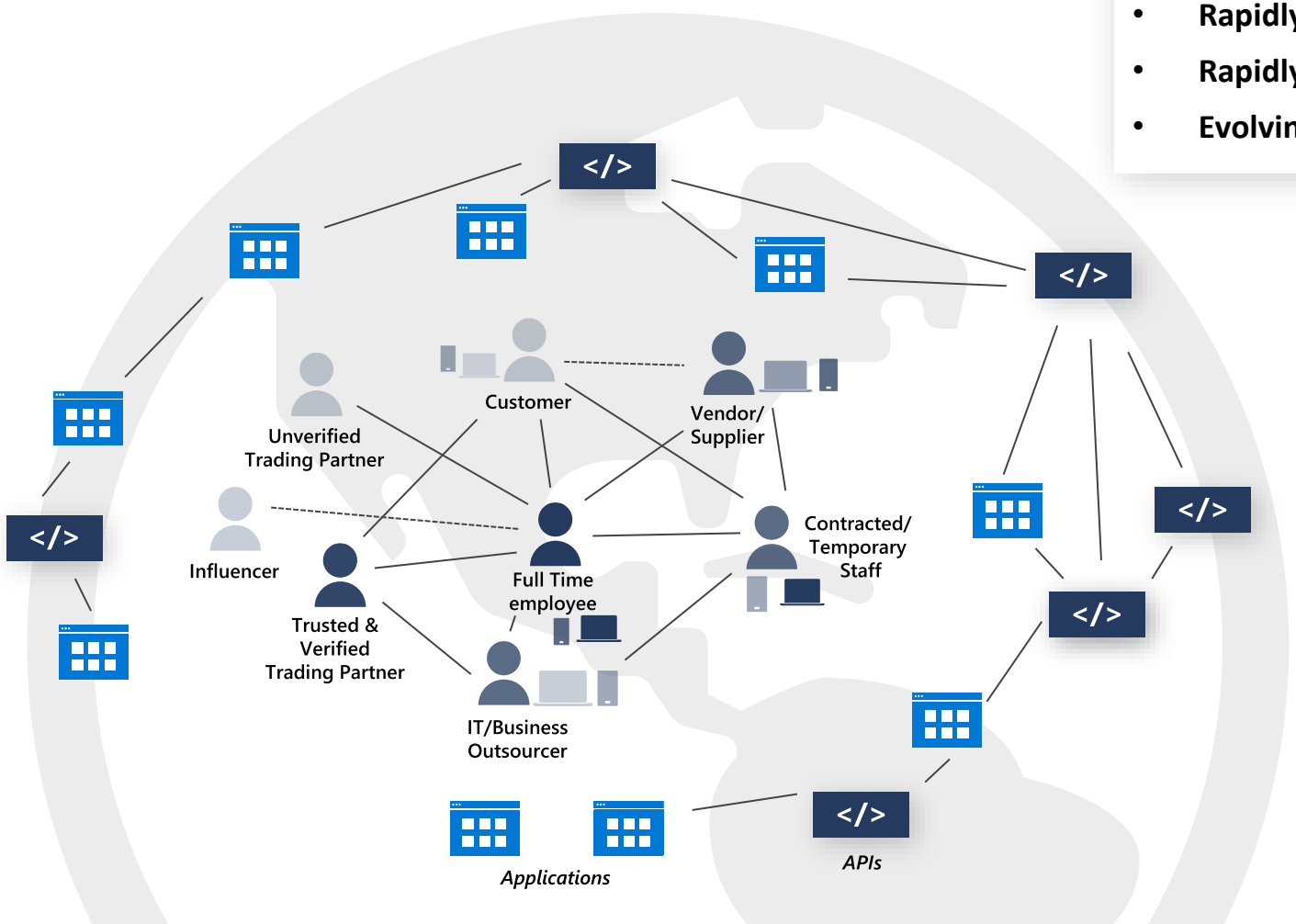
enabling secure freedom instead of locking them up in a "secure" network

Classic Approach – Restrict everything to a 'secure' network



Zero Trust – Protect assets anywhere with central policy

The digitized world is interconnected and dynamic



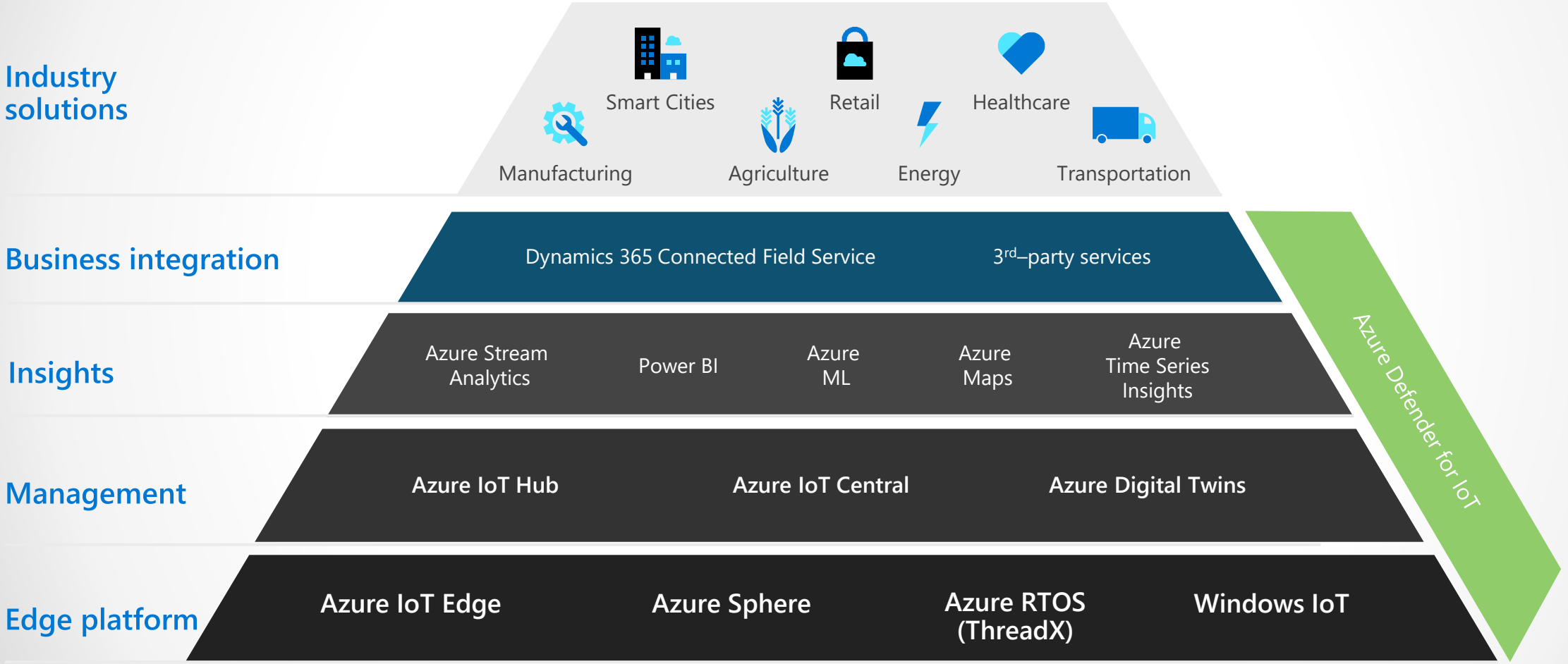
Modern Work Use Cases

- **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



Upcoming Events

Data Saturday Sofia, 2022

Oct 08

Eventbrite

js.talks();

JSTalks, 2022

Nov 11-12

http://jstalks.net/

Thanks to our Sponsors

Platinum Sponsors:

Microsoft

Anthill

BOSCH
Invented for life

THE Coca-Cola COMPANY

Gold Sponsor:

Strypes

Silver Sponsor:

epam

Venue Partner:

SOFIA TECH PARK

AI

INTERNET of THINGS