Security IoT
Key Services positioning

Ian Banham

Customer **S**uccess **U**nit IoT - EMEA

Graziano Galante

Global **P**artner **S**olution IoT - EMEA

Before starting, let’s share some common terms

- SIEM “security information and event management”:
  - SIEMs provide security teams with a single pane of glass for all of their security alerts
- SOAR “security orchestration, automation and response”:
  - SOAR generally refers to any technology, solution, or collections of preexisting tools that allow organizations to streamline the handling of security processes in three key domains; threat and vulnerability management, incident response, and security operations automation
- XDR “Extended detection and response”:
  - By collecting, normalizing and analyzing data from multiple sources, XDR solutions are able to better validate alerts, thereby reducing false positives and increasing reliability
- SOC “Security Operation Center”
  - SOC is a centralized location run by a security operations (SecOps) team that continuously monitors, analyzes and responds to security incidents

Navigating a shifting world

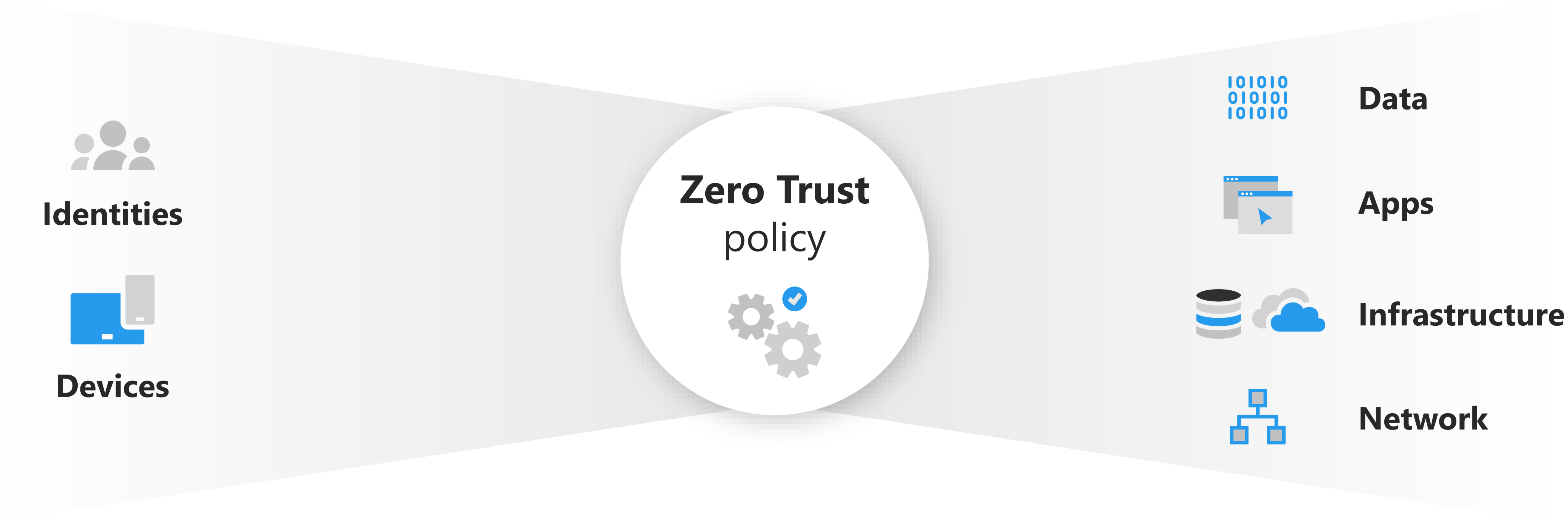
Attacks growing
more sophisticated

Conventional security
tools **have not kept pace**

Regulatory landscape
becoming **more complex**

Securing your organization with Zero Trust

Verify **explicitly** | Use **least-privileged access** | Assume **breach**



Identities

Devices

Zero Trust policy

Data

Apps

Infrastructure

Network

Essential Cloud Security

Actionable, Holistic, Short- and long-term

People

Process

Technology

Foundational Architecture Decisions

OT Components Within the Purdue Model

PLC – Programmable Logic Controller

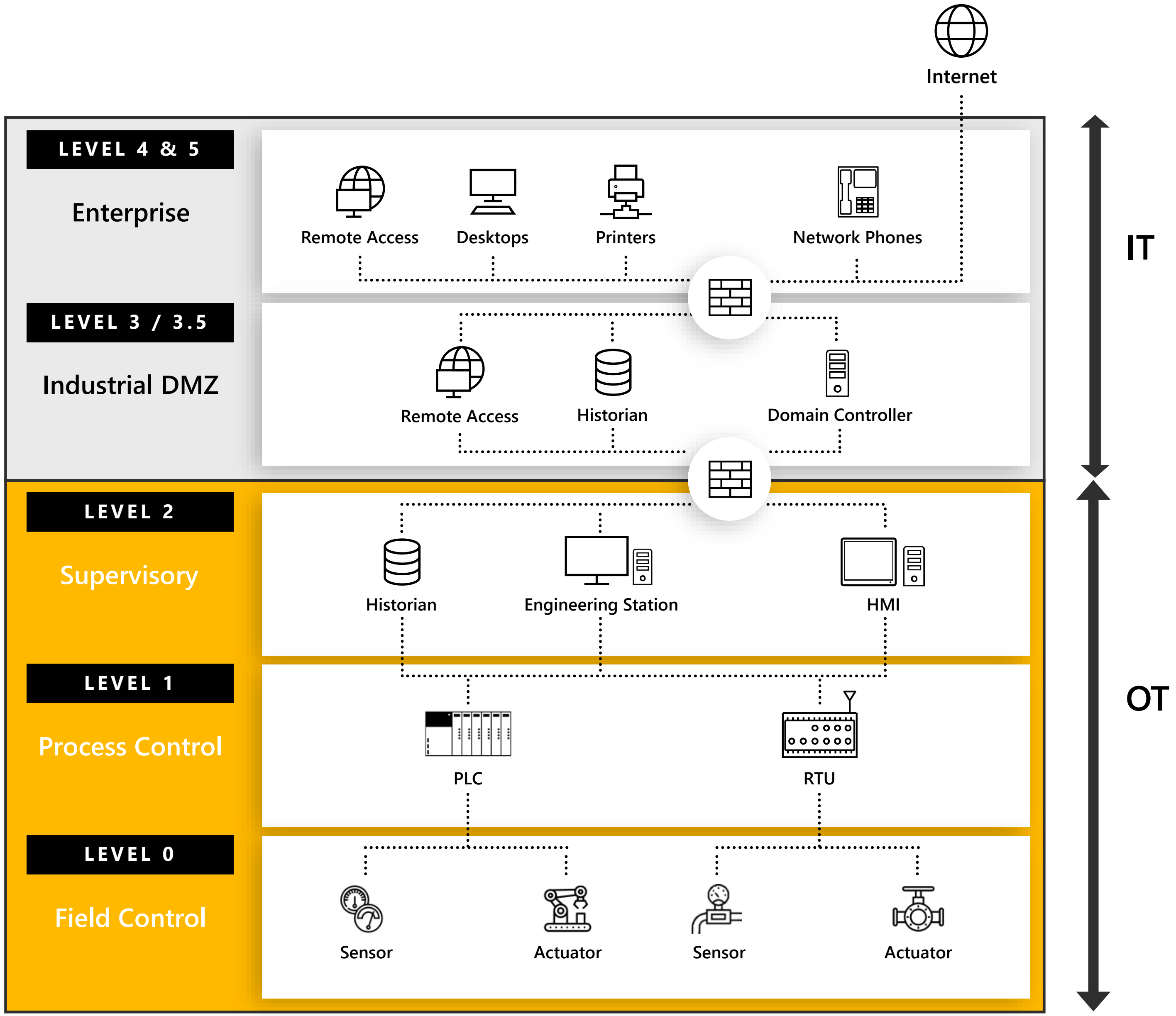
RTU – Remote Terminal Unit

HMI – Human Machine Interface

EWS – Engineering WorkStation

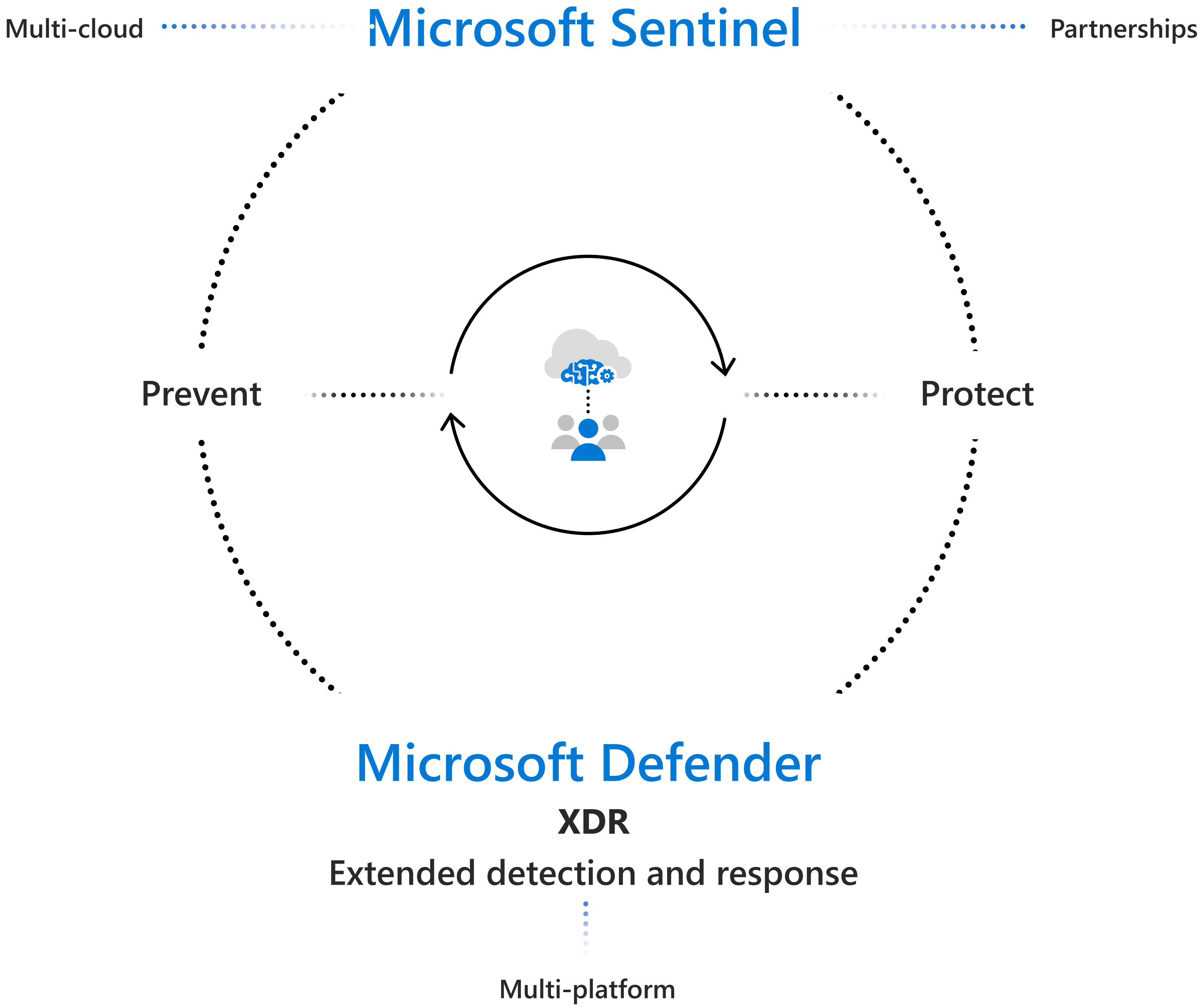
Historian

Purdue is a connectivity model and common language; security must be layered on top of it



SIEM

security information and event management



Multi-cloud

Microsoft Sentinel

Partnerships

Prevent

Protect

Microsoft Defender

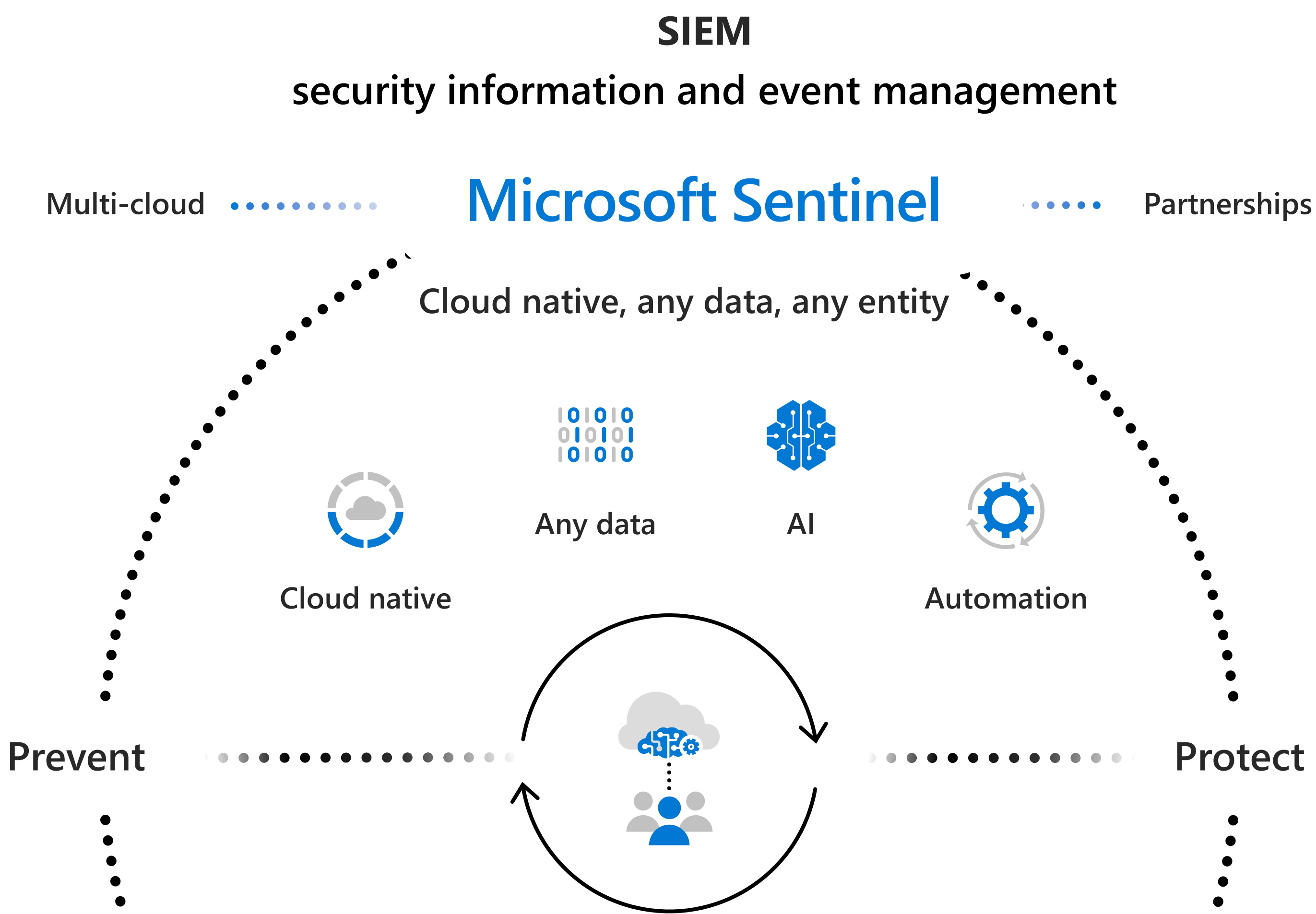
XDR

Extended detection and response

Multi-platform

Gain insights across your entire enterprise

Visualize and investigate the attack chain with cloud-native SIEM



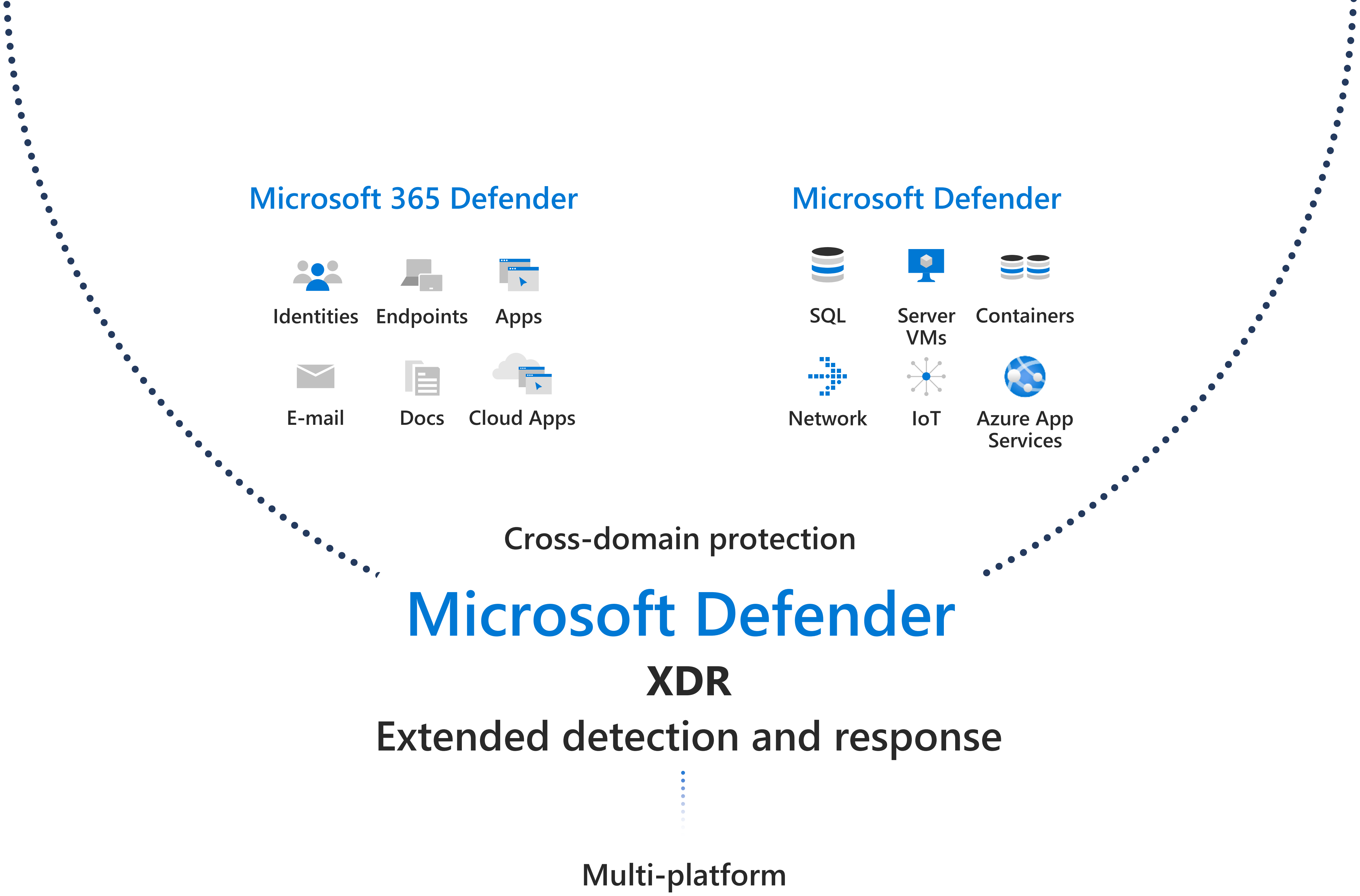
SIEM

security information and event management

Microsoft Sentinel

Cloud native, any data, any entity

- Collect security data at cloud scale and integrate with your existing tools
- Leverage AI to detect emergent threats and reduce alert fatigue by 90 percent
- Respond rapidly with built-in orchestration and automation



Microsoft 365 Defender

- Identities
- Endpoints
- Apps
- E-mail
- Docs
- Cloud Apps

Microsoft Defender

- SQL
- Server VMs
- Containers
- Network
- IoT
- Azure App Services

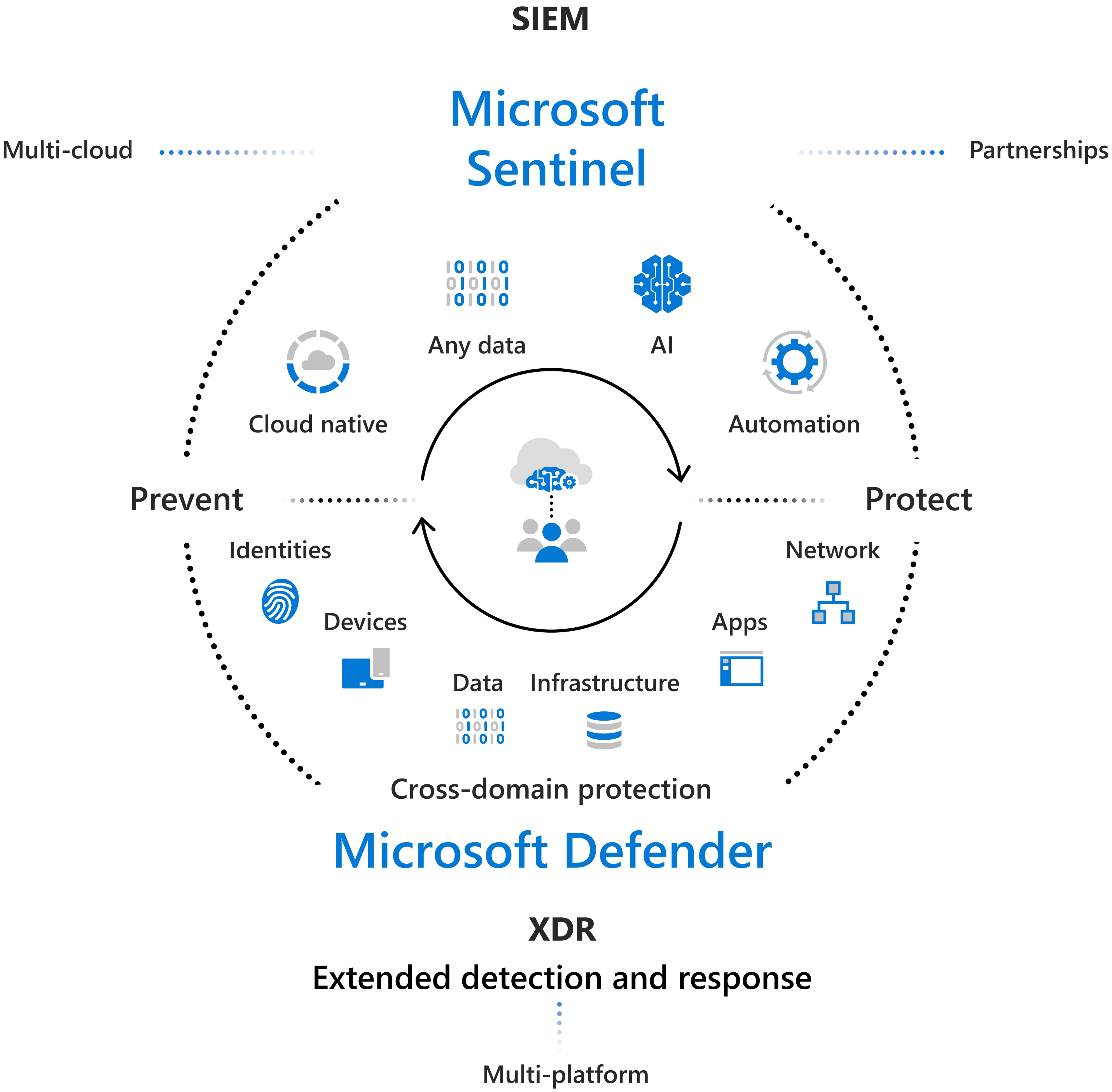
Cross-domain protection

Microsoft Defender

XDR

Extended detection and response

Multi-platform



SIEM

Microsoft Sentinel

Multi-cloud

Partnerships

Any data

AI

Cloud native

Automation

Prevent

Protect

Identities

Network

Devices

Apps

Data

Infrastructure

Cross-domain protection

Microsoft Defender

XDR

Extended detection and response

Multi-platform