Microsoft

Safeguard government systems with AI security

Reference Architecture

Safeguard government systems with AI security

1. Detect and disrupt threats in real-time using AI algorithms to protect sensitive data.
2. Strengthen cybersecurity posture of government systems.
3. Prevent cyber attack disruptions from nation state and cyber criminal organizations.
4. Shift cyber defense paradigm from manually-driven detections to automated-scalable remediations.
5. Improve collective cyber defense and threat intelligence across national government.
6. Enhance cyber-resiliency by continuous monitoring to protect against evolving threats.
7. Unified SecOps Experience.
8. Quick Triaging and Attack Disruption.

Improving Resiliency

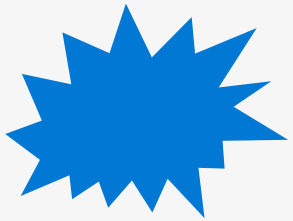
Enable business mission while continuously increasing security assurances

‘Left of Bang’

Prevent or lessen impact of attacks

‘Right of Bang’

Rapidly and effectively manage attacks



IDENTIFY | **PROTECT** | **DETECT** | **RESPOND** | **RECOVER**

GOVERN

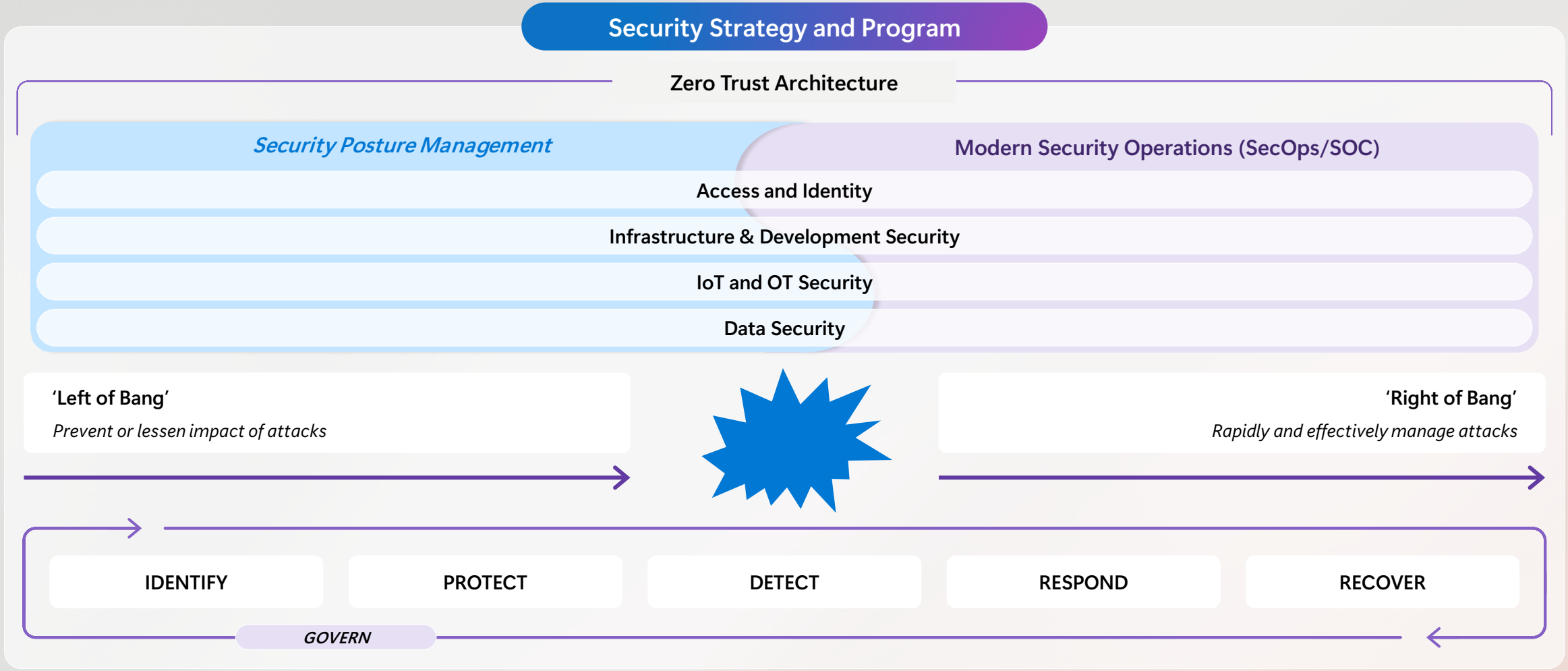
NIST Cybersecurity Framework v2

Use Case 2 – Safeguard government systems with AI security

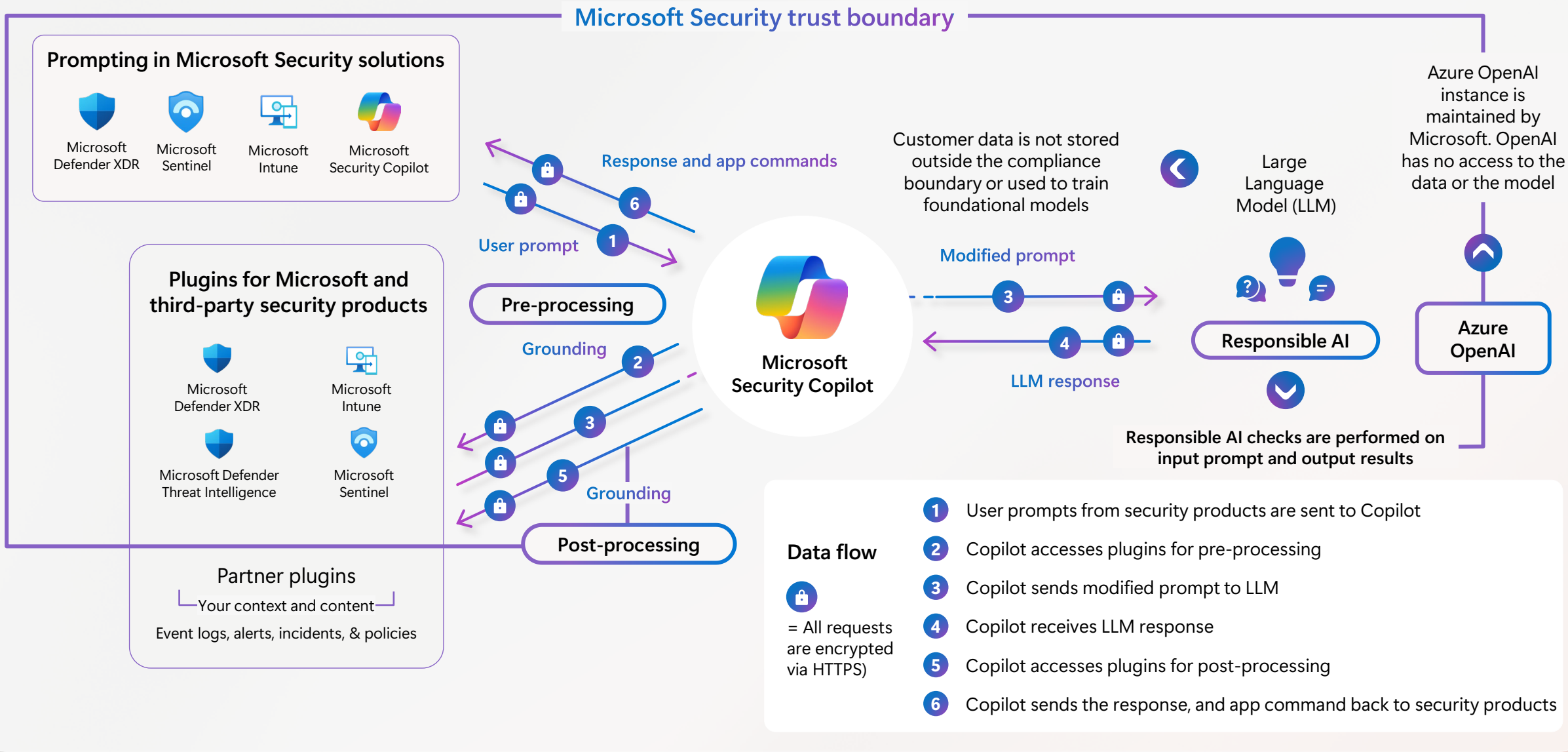
Stage	Microsoft Product	Gen-AI Enhancements
1. Prepare & Baseline	Entra ID, Defender for Cloud, Purview	Generate Zero Trust posture reports, readiness assessments, and policy templates
2. Detect	Microsoft Sentinel (SIEM), Defender XDR, Defender for IoT	Natural language hunts, automated KQL generation, anomaly summarization
3. Triage & Prioritize	Unified SecOps (Sentinel + XDR), Security Copilot	Incident summarization, blast radius scoring, cross-agency prioritization
4. Investigate	Security Copilot, MDTI, Sentinel	Guided investigation steps, root cause hypotheses, IOC expansion with threat intel
5. Disrupt & Contain	Defender XDR, Sentinel SOAR, Entra, Intune	Approve-to-execute automation for account disable, token revocation, device isolation
6. Eradicate & Recover	Defender for Cloud, Purview, Security Copilot	Automated remediation scripts, prioritized hardening plans, executive-ready reports
7. Prevent & Share	MDTI, Unified SecOps, Security Copilot	Policy-as-code templates, reusable promptbooks, national threat briefs

End to End Security

Enable business mission and increasing security assurances with intentional approach



Data flow for Security Copilot



Security Operations

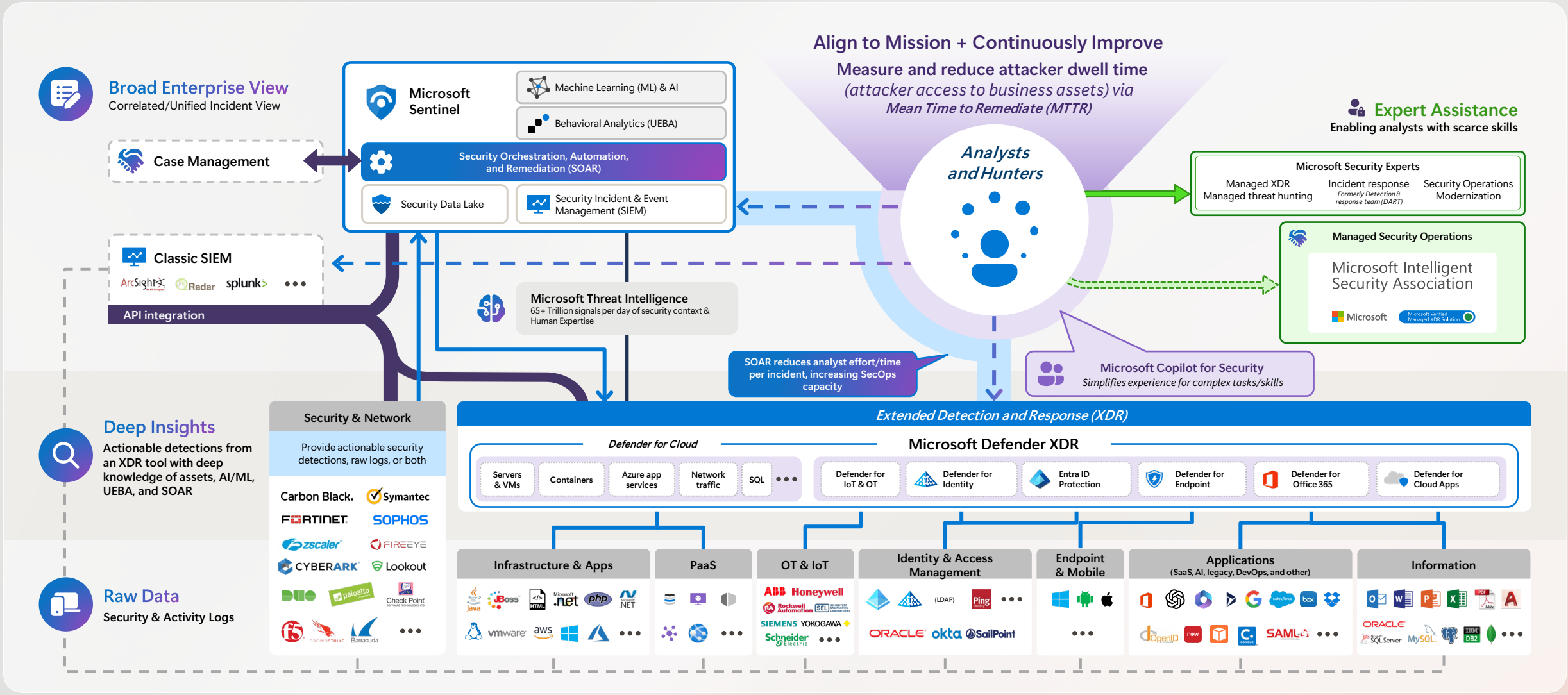
Microsoft Reference Architecture

Legend

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

Microsoft

December 2023 – aka.ms/MCRA



Next Steps

The Chief Information Security Officer (CISO) Workshop

https://learn.microsoft.com/en-us/security/adoption/the-ciso-workshop

Microsoft Cybersecurity Reference Architectures

https://learn.microsoft.com/en-us/security/adoption/mcra

Microsoft Unified Engagements

https://learn.microsoft.com/en-us/security/adoption/adoption#microsoft-unified-engagements

Security Resources

Microsoft

Security Adoption Framework
aka.ms/saf

Security Hub
aka.ms/SecurityDocs

Security Strategy and Program

- CISO Workshop – aka.ms/CISOworkshop | -videos

End to End Security Architecture

- Microsoft Cybersecurity Reference Architectures (MCRA) – aka.ms/MCRA | -videos
- Ransomware and Extortion Mitigation – aka.ms/humanoperated
- Backup and restore plan to protect against ransomware – aka.ms/backup

Driving Business Outcomes Using Zero Trust

- Rapidly modernize your security posture for Zero Trust
- Secure remote and hybrid work with Zero Trust
- Identify and protect sensitive business data with Zero Trust
- Meet regulatory and compliance requirements with Zero Trust

- Zero Trust Workshop – aka.ms/ztworkshop
- Zero Trust Deployment Guidance – aka.ms/ztguide | aka.ms/ztramp

Secure Access and Identities

- Securing Privileged Access (SPA) Guidance aka.ms/SPA
- Access Control Discipline
- Ninja Training
  - Microsoft Defender for Identity aka.ms/mdininja
- MCRA Video
  - Zero Trust User Access
- Microsoft Entra Documentation aka.ms/entradocs

Modern Security Operations (SecOps/SOC)

- Incident Response – aka.ms/IR
- CDOC Case Study – aka.ms/ITSOC
- Ninja Training
  - Microsoft 365 Defender aka.ms/m365dninja
  - Microsoft Sentinel aka.ms/sentinelninja
  - Microsoft Defender for Office 365 aka.ms/mdoninja
  - Microsoft Defender for Endpoint aka.ms/mdeninja
  - Microsoft Cloud App Security aka.ms/mcasninja
- MCRA Videos
  - Security Operations
  - SecOps Integration

Infrastructure & Development Security

- Security Development Lifecycle (SDL)
  - Security Controls
- Microsoft Cloud Security Benchmark aka.ms/benchmarkdocs
- Well Architected Framework (WAF)
  - aka.ms/wafsecure
- Azure Security Top 10
  - aka.ms/azuresecuritytop10
- Ninja Training
  - Defender for Cloud
- MCRA Video
  - Infrastructure Security
- Defender for Cloud Documentation

Data Security

- Secure data with Zero Trust
- Ninja Training
  - Microsoft Purview Information Protection aka.ms/MIPNinja
  - Microsoft Purview Data Loss Prevention aka.ms/DLPNinja
  - Microsoft Purview Insider Risk Management
  - Insider Risk Management
  - Data Security for SOC aka.ms/NinjaDSforSOC
- Microsoft Purview Documentation aka.ms/purviewdocs

IoT and OT Security

- Ninja Training
  - Defender for IoT Training
- MCRA Videos
  - MCRA Video OT & IIoT Security
- Defender for IoT Documentation aka.ms/D4IoTDocs

Product Capabilities
www.microsoft.com/security/business

Security Product Documentation
Azure | Microsoft 365

Microsoft Security Response Center (MSRC)
www.microsoft.com/en-us/msrc

Key Industry References and Resources

The Open Group

- Zero Trust Commandments Standard – https://publications.opengroup.org/c247
- Zero Trust Reference Model – https://publications.opengroup.org/s232
- Security Principles for Architecture – https://publications.opengroup.org/c246

US National Institute of Standards and Technology (NIST)

- Cybersecurity Framework – https://www.nist.gov/cyberframework
- Zero Trust Architecture – https://www.nist.gov/publications/zero-trust-architecture
  - NCCoE Zero Trust Project – https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
- Secure Software Development Framework (SSDF) – https://csrc.nist.gov/pubs/sp/800/218/final

Cybersecurity and Infrastructure Security Agency (CISA)

- Zero Trust Maturity Model – https://www.cisa.gov/zero-trust-maturity-model

Center for Internet Security (CIS)

- CIS Benchmarks – https://www.cisecurity.org/cis-benchmarks/

Public Sector Cybersecurity Skilling Resources

Public Sector Cyber Defense: Skilling for the GenAI Era

aka.ms/PubSecCyberDefenseGenAISkilling

Foundations of a modern public sector security operations center

aka.ms/PublicSector-SOC-Module

All Public Sector Cybersecurity Skilling Content

aka.ms/PublicSectorCybersecurity

Microsoft

Thank you