Cyber threats monitoring with Microsoft Sentinel

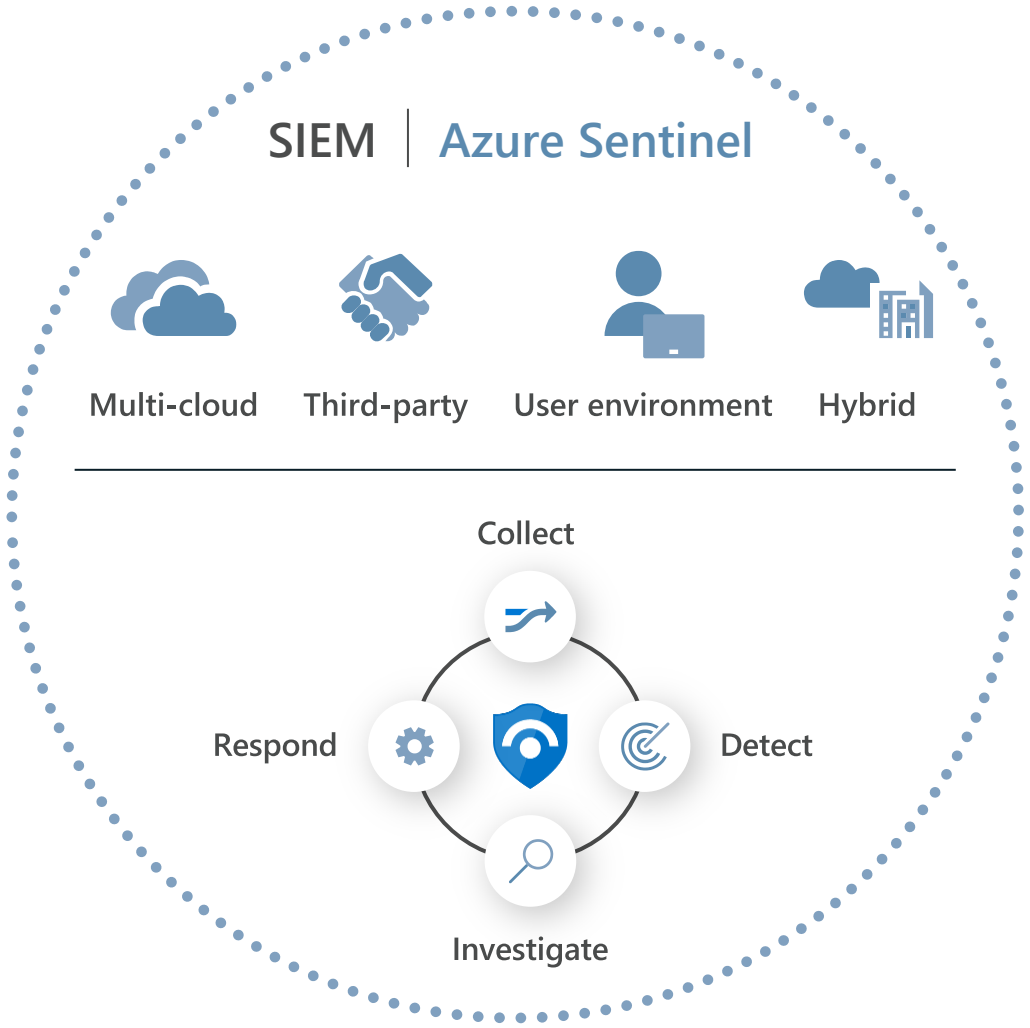
Viktor Golub

Cloud Security Architect
MCT, MCP
Cloud Solutions LLC

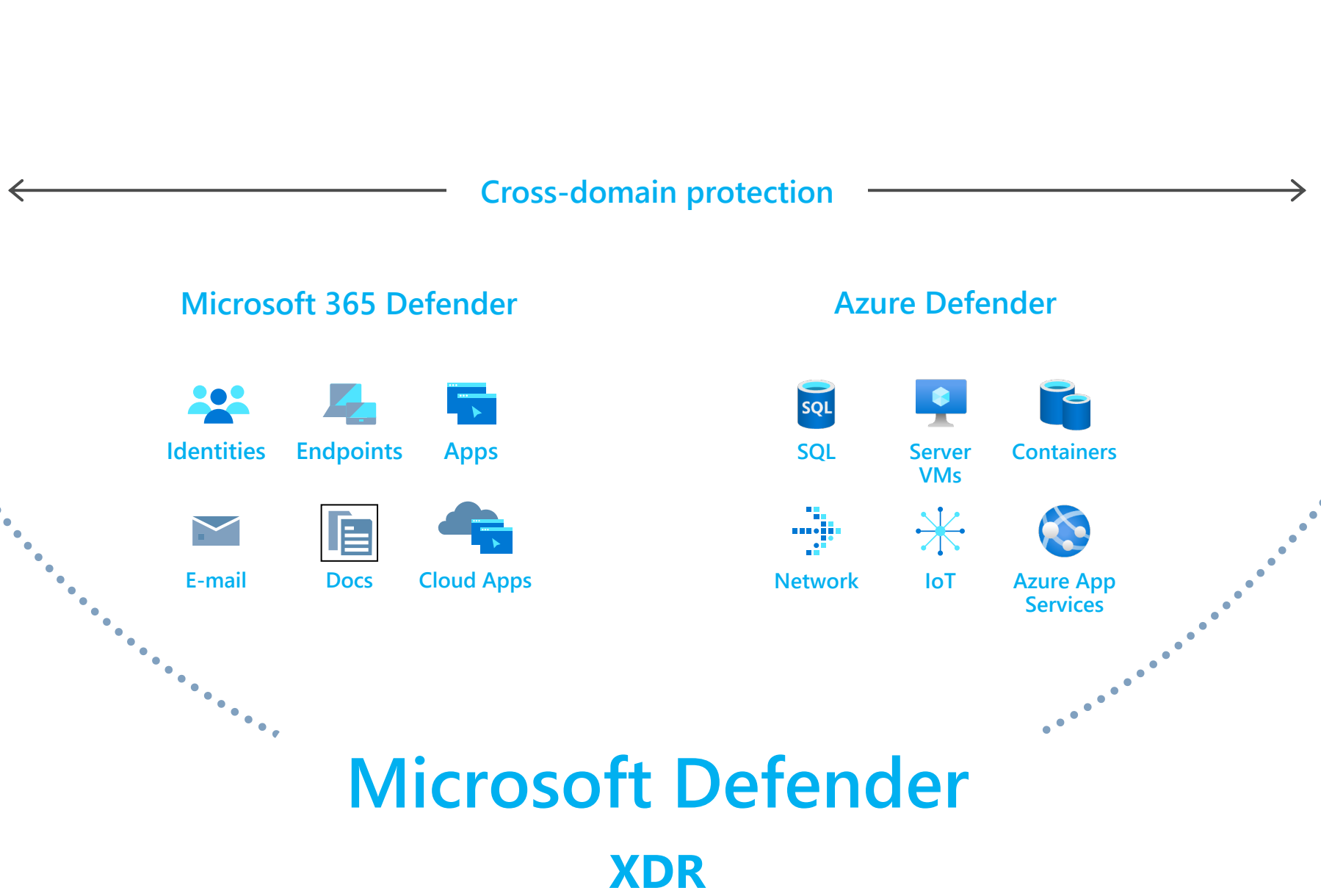
October 11, 2022

Gain insights across your entire enterprise

Visualize and investigate the attack chain with cloud-native SIEM



- 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 Defender

XDR

Detect and respond across end-user environments

Prevent and detect threats, hunt for attacks, and coordinate response across domains

- Stop attacks before they occur by reducing your attack surface
- Detect and automate across domains, integrating threat data for rapid response
- Hunt across domains and create custom tools using your unique expertise
- View alerts and remediate across your Microsoft 365 environment in a single dashboard

Introducing Azure Sentinel

Cloud-native SIEM for intelligent security analytics for your entire enterprise

Delivers instant value to your defenders

Scales to support your growing digital estate

Uses AI and automation to improve effectiveness

Security Operations Center

Based on Microsoft Reference Architecture