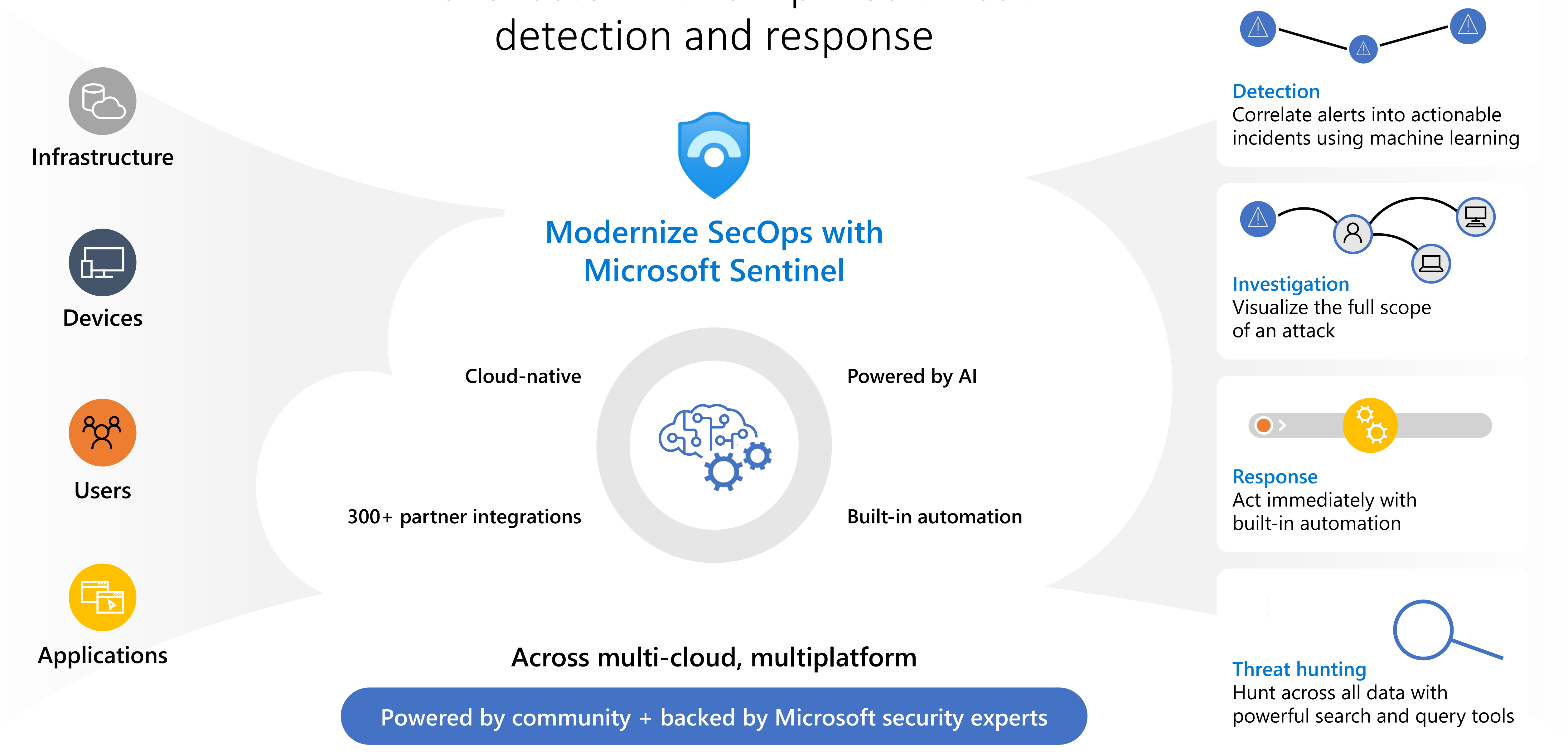
Proof of Concept

Microsoft Sentinel

ELEVATE

SOLUTIONS

Move faster with simplified threat detection and response



Infrastructure

Devices

Users

Applications

Modernize SecOps with Microsoft Sentinel

Cloud-native

Powered by AI

300+ partner integrations

Built-in automation

Across multi-cloud, multiplatform

Powered by community + backed by Microsoft security experts

Detection
Correlate alerts into actionable incidents using machine learning

Investigation
Visualize the full scope of an attack

Response
Act immediately with built-in automation

Threat hunting
Hunt across all data with powerful search and query tools

Microsoft Sentinel PoC Approach

Analyze

- Business and IT requirements
- Existing SIEM/SOC tools
- Data sources to be connected
- Security Operations automation requirements

Define scope & deploy

- Define the scope of the Microsoft Sentinel deployment
- Deploy and configure Microsoft Sentinel
- Connect Microsoft Sentinel to ingest data from:
  - Office 365 & Azure
  - Azure AD Identity Protection
  - Microsoft 365 Defender
    - Microsoft Defender for Office 365
    - Microsoft Defender for Identity
    - Microsoft Defender for Cloud Apps
    - Microsoft Defender for Endpoint
  - Agreed 3rd party Syslog integration (firewalls, proxy servers)
  - Limited number of servers

Discover

- Use Microsoft Sentinel to analyze and discover threats to your organization
- **Optional -** Use Microsoft Sentinel to proactively hunt for security threats across all ingested data

Recommend

- Map found threats to Microsoft 365 security products
- Provide a Microsoft Sentinel deployment roadmap