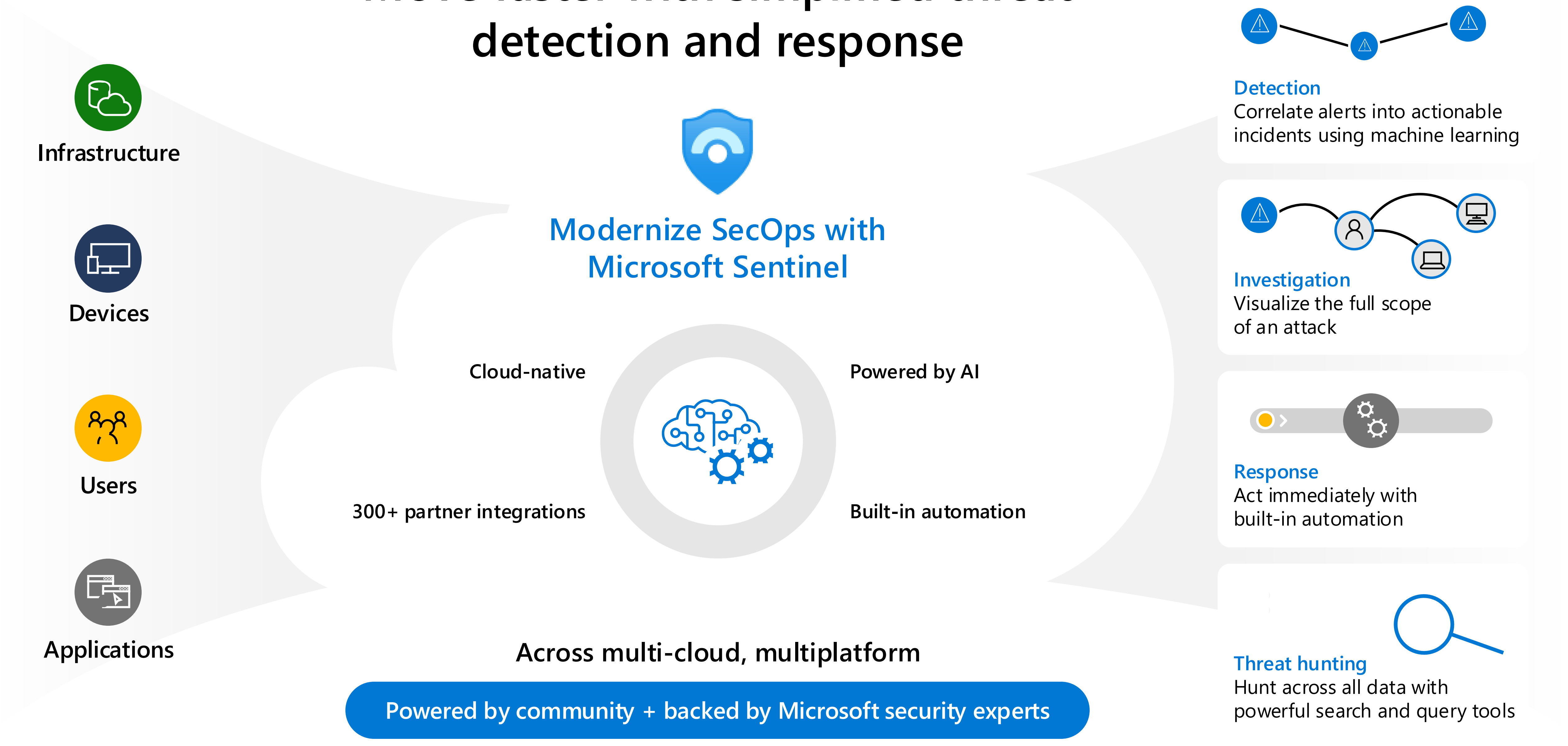
THE PARTNER MASTERS

# Microsoft Sentinel Migration and Modernization

# Triggers of the need for a modern SIEM solution

- Attack surface is expanding due to growing digital estates and hybrid work
- Rapid acceleration and increasing sophistication of cybercrime
- Rising costs of silos, licenses and staff
- Complex set-up and maintenance of on-premises infrastructure

# 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

# Save money and reduce time to value

**201% ROI**
over three years[1]

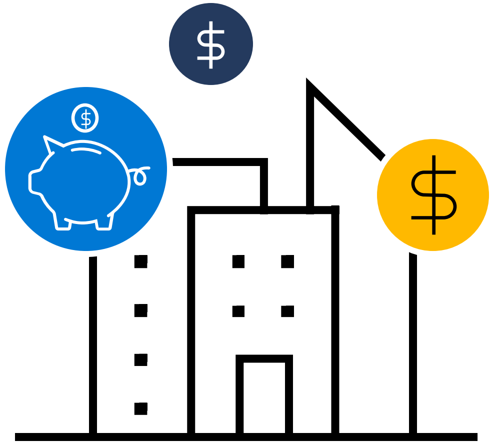
**80% reduction**
in investigation effort [1]

**48% less expensive**
compared to legacy SIEMs[1]

**79% decrease** in false positives over three years[1]

**56% reduction in management effort**
for infrastructure and SIEM[1]

**67% decrease in time to deployment**
with pre-built SIEM content and out-of-the box functionality[1]



- Cloud-native SAAS solution, with benefits like automatic updates, no on-premises infrastructure to set up and maintain and elastic scalability.
- Unified SIEM solution with SOAR, UEBA and TI
- Unparalleled integration with out-of-the-box solutions enabling value on day one. Don’t spend time and money on set up
- Mature and feature-rich SecOps platform built on top of core SIEM capabilities with native XDR integrations

[1] The Total Economic Impact™ of Microsoft Azure Sentinel from Forrester Consulting

# Flexible collecting and archiving options

## Eliminate blind spots with affordable solutions to collect, store, and analyze all your security data

### Analytics logs

**Security and activity logs**

- Used for continuous threat monitoring, near real-time detections, and behavioral analytics
- Available for 90 days, with option to archive
- Affordable pay-as-you-go pricing with volume discounts and predictable commitment tiers

### Basic logs

**High-volume, investigation logs**

- Accessed on-demand for ad-hoc querying, investigations, and automation
- Supports ingestion-time parsing and transformation
- Available for eight days, with option to archive

### Archive

**Low-cost, long-term storage**

- Meet compliance requirements
- Archive data up to seven years
- Easily search and restore archived logs

**Solve the SOC's hardest challenges while managing the total cost of operations**

# Microsoft Sentinel Migration – phases & key activities

## Discovery

**Conduct a discovery** to better understand the current state of your SIEM. Collect monitoring and alerting use cases and requirements.

### Key Activities

- Identify requirements and detailed use cases
- Identify and document your existing automation, remediation, and alerting tools and processes.
- Identify your existing SOC processes, including investigation, automation, and remediation.
- Identify critical security assets.
- Assess existing security portfolio.
- Identify integrations with IT service management (ITSM), threat intelligence, and automation solutions.

### Deliverables

- Project plan
- Current state analysis
- Business and technical requirements
- Use cases

## Design

**Create a comprehensive design** that aligns with the current security portfolio and existing data sources.

### Key Activities

- Design integration of Microsoft and third-party sources.
- Map rules to Sentinel built-in rules.
- Map dashboards to Sentinel workbooks.
- Map automation to Sentinel playbooks.
- Design custom alerting for Sentinel.
- Map existing SOC processes to Sentinel features.
- To migrate historical logs, review the available target platforms and data ingestion tools.

### Deliverables

- Design workshops
- Design documentation
  - Data source integration
  - Automation
  - Custom alerting

## Implement

**Implement** the design phase: Integrate data sources that will connect to Microsoft Sentinel; ensure that Microsoft Sentinel works as designed.

### Key Activities

- Connect Microsoft sources, cloud logs (AWS/GCP), network devices, and third-party security solutions.
- Deploy Azure Monitor Agent to collect logs from VMs (Windows/Linux) and network devices.
- Review your MITRE ATT&CK coverage.
- Implement automation via Azure Logic Apps.
- Convert remaining rules to Sentinel rules.
- Deploy/create playbooks and automation rules.
- Deploy playbooks for ITSM platforms, SOAR, and threat intelligence platform integration.
- Deploy workbooks and convert dashboards to workbooks.
- Review SOC operations migration best practices.

## Operationalize

**Operationalize Microsoft Sentinel Investigation and Response** within existing security monitoring, alerting, and incident response processes.

### Key Activities

- Assist with refining monitoring and alerting processes.
- Assist with security incident management processes.
- Assist with triage/investigation processes.
- Assist with alerting use cases refinement.
- Define SOC processes based on the mapping done in the design phase.

*Committed Migrating to Microsoft Sentinel*

### Deliverables

- Microsoft Sentinel PoC Plan
- Connect Microsoft data sources
- Connect external data sources
- Deploy Azure Monitor agent
- Implement workbooks and Playbooks

### Deliverables

- Microsoft Sentinel configuration documentation
  - Workbooks
  - Playbooks
  - Custom slerts
  - KQL queries

# Next Steps

Schedule your migration and implementation today!

sales@thepartnermasters.com

Microsoft
Solutions Partner

Security