

# OPTIV MIGRATION AND IMPLEMENTATION SERVICES

**Microsoft Azure Sentinel**

Microsoft  
Partner

Gold Security  
Gold Cloud Productivity  
Gold Cloud Platform  
Silver Datacenter  
Silver Application Development


OPTIV

TECHNOLOGY

PROCESS

PEOPLE

  
**75**  
tools in the  
average security  
environment\*

  
There is a  
**correlation** between  
the increase in the  
number of tools and  
the increase in  
breaches.\*\*

\*CSO Online  
\*\*Cisco Cybersecurity Report

OPTIV

# COMMON CHALLENGES

## Too Many Technologies



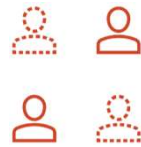
- Market Confusion
- Duplicative Capabilities
- Lack of Tech Integrations

## Consumption Gap



- Shelfware
- Attack Surface
- Tools and Controls

## Skill and Time Gaps



- Reduced Monitoring and Management Capabilities
- Minimal Return on Investment

## Complexity in Environment



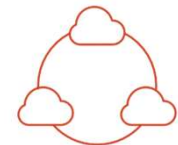
- Perimeter
- Cloud Evolution

## Business Alignment



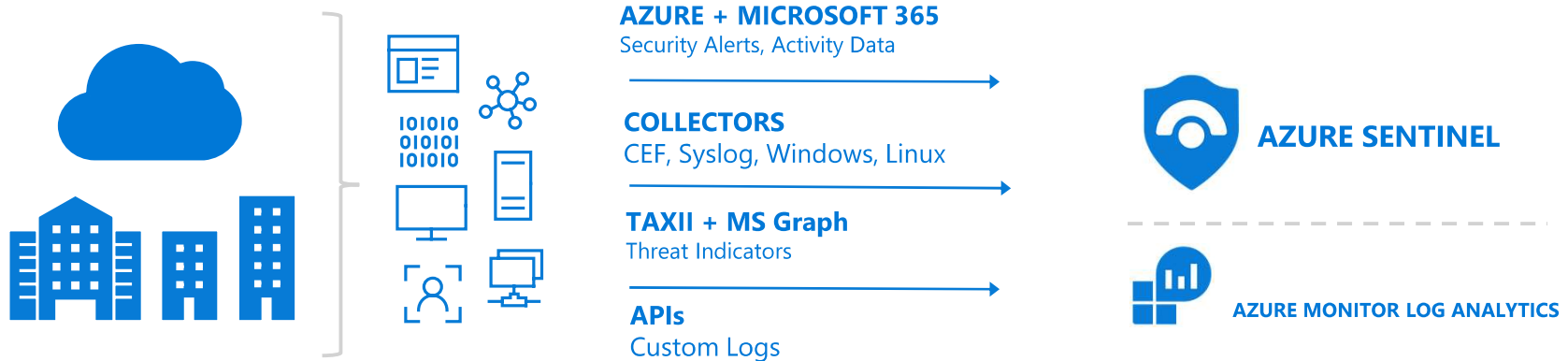
- Program Gaps
- Lack of Business Enablement

## Emerging Trends



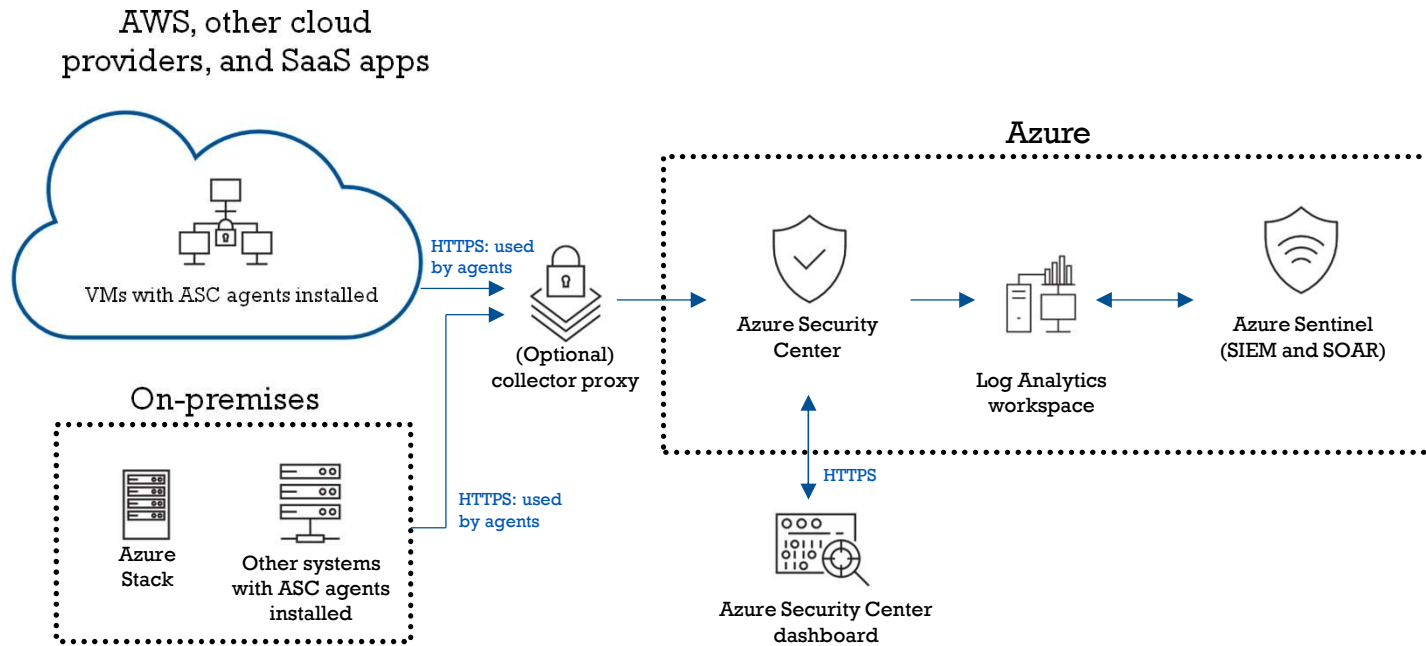
- Remote Access
- Shift to Cloud

# COLLECT SECURITY DATA AT CLOUD SCALE FROM ANY SOURCE



# OPTIV SERVICES FOR AZURE SENTINEL

This reference architecture illustrates how to use Azure Security Center and Azure Sentinel to monitor the security configuration and telemetry of on-premises and azure operating system workloads. This includes Azure Stack.



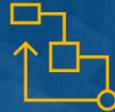
# INTRODUCING MICROSOFT AZURE SENTINEL

Provides clients with collaborative service components to ensure preventative and ongoing real-time operational measures



## Built-in 1<sup>st</sup> and 3<sup>rd</sup> party connectors

Or Microsoft provides APIs and connectors for your Existing SIEM



## Incident Management

Assign an Incident to an Analyst

Open and Ticket (ServiceNow/Jira)

Keep Incident Status in Sync

Post in a Teams or Slack Channel



## Enrichment + Investigation

Lookup Geo for an IP

Trigger Defender ATP Investigation

Send Validation Email to User



## Remediation

Block an IP Address

Block User Access

Trigger Conditional Access

Isolate Machine

# OPTIV MIGRATION AND DEPLOYMENT SERVICES



## **Project Planning Phase**

Detailed review of current SIEM to identify critical data sources and use cases to be migrated to Azure Sentinel.

## **Implementation and Data Source Onboarding Phase**

Enable Sentinel within client's Azure environment following Microsoft best practices.

## **Content Optimization and Tuning Phase**

Enable Sentinel Analytics rules based on onboarded data sources and tune rules to lower false positives.

## **Project Deliverables and Closeout:**

Create a detailed summary of work performed and recommended next steps to mature the Sentinel environment

# WHAT WE DO



## DEPLOYMENT

Identify critical data sources and plan out collection strategy including agent deployment best practices. Create a prerequisite guide for data source onboarding.



## IMPLEMENTATION AND DATA SOURCE ONBOARDING

Enable Sentinel within client's Azure environment following Microsoft best practices. Deploy agents where required and onboard identified critical data sources. Review data ingestion of each data source.



## MIGRATION

Detailed review of current SIEM to identify critical data sources and use cases to be migrated to Azure Sentinel. Architecture workshop to plan out data source collection strategy including agent deployment best practices. Create a prerequisite guide for data source onboarding.



## CONTENT OPTIMIZATION AND TUNING

Enable Sentinel Analytics rules based on onboarded data sources and tune rules to lower false positives. Enable Sentinel workbooks to provide visibility into critical data sources. Create hunting queries based on customer use case requirements. Enable Playbooks to automate and respond to incidents.



## PROJECT DELIVERABLES AND CLOSEOUT

Create a detailed summary of work performed and recommend next steps to mature the Sentinel environment





# MICROSOFT AZURE SENTINEL MIGRATION AND IMPLEMENTATION

The Optiv Approach



**DEDICATED TECHNICAL PROJECT  
MANAGER**



**DESIGNATED CLIENT SUCCESS  
MANAGER**



**CERTIFIED EXPERTS**



**FUTURE-PROOF PLANNING**



# WHY OPTIV FOR MICROSOFT



Gold Cloud Platform  
Silver Application Development

Member of  
Microsoft Intelligent  
Security Association



## Extension of Microsoft Team

Extension of in-house expertise in Access Management, Identity Governance and Data Governance & Protection across Microsoft technologies

### Secure Cloud Adoption

Optiv supports clients as they move to the cloud with security-by-design as a core principle for secure cloud adoption

### Business Alignment

Map strategy to measurable business outcomes (i.e. full optimization of O365 investment)

### Leverage our Strengths

Optiv, as an SSI, goes beyond consulting with implementation, migration and management capabilities to enable clients through their Microsoft security journey

### Holistic Approach

Optiv approaches Microsoft technologies with end-to-end services from multiple practices such as Cyber Operations, Threat, Risk, etc.

### Agile and Proactive

Optiv's approach can advance how Microsoft features are securely used and consumed – with a keen eye for identifying security gaps

### Industry Expertise

Unique and proven methodology quickly shows value leveraging Optiv best practices and Microsoft's guidelines



# QUESTIONS

---

**Thank You!**

