Microsoft

Microsoft Sentinel

SIEM + SOAR All-In-One

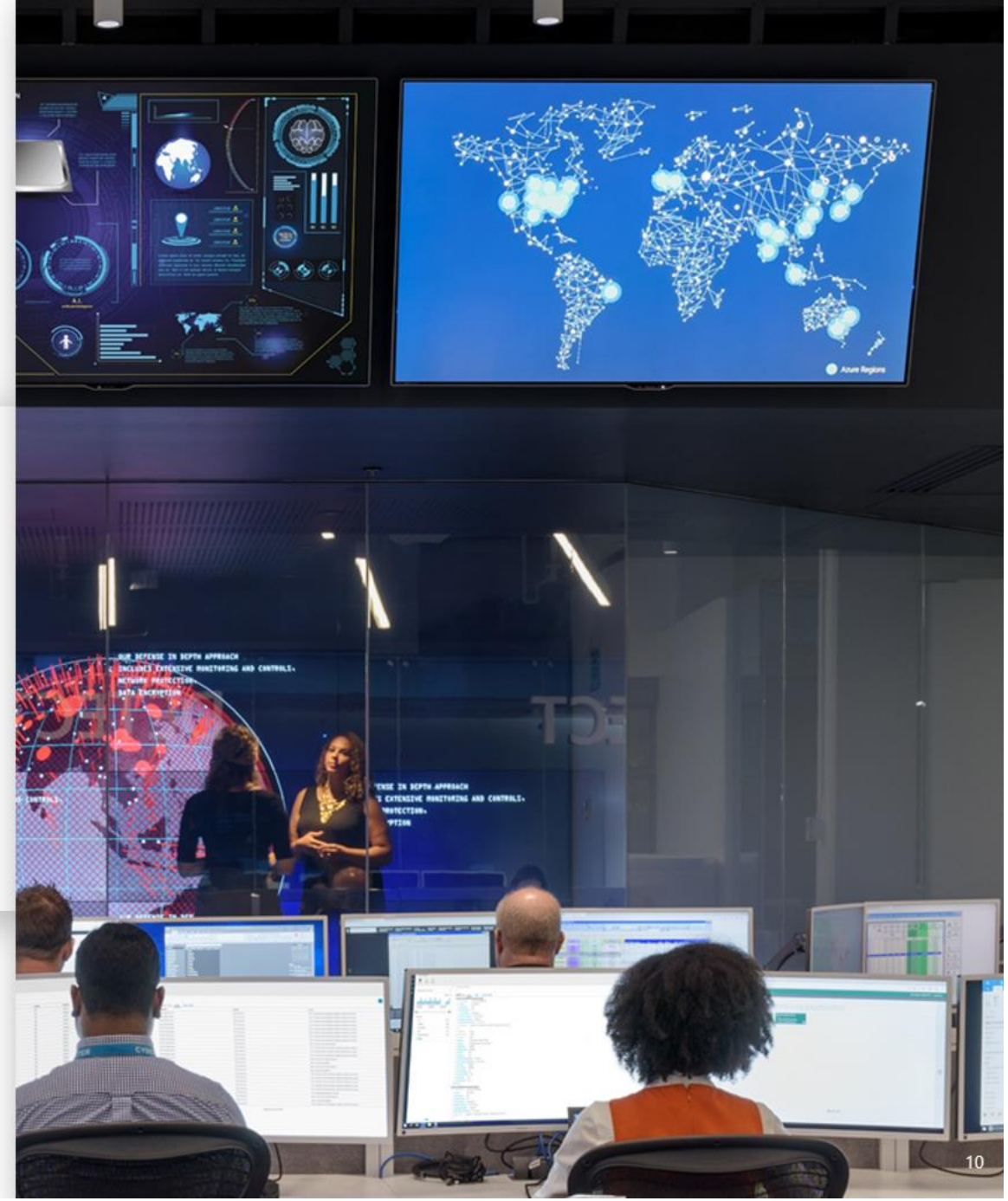
Security: Microsoft Sentinel

Microsoft

Overview of Microsoft Sentinel

Microsoft Security Advantage

- **$4B** annual investment in cybersecurity.
- **3500+** global security experts.
- **Trillions of** diverse signals for unparalleled threat intelligence.



SIEM and SOAR Explained

Security Information & Event Management

- *SIEM* centralizes collection of log data.
- Analyzes for trends, anomalies, and alerts.
- Creates reports, dashboards, and notifications.
- Often involves massive amounts of data (EPS).

Related Topics:

- Incident management and response
- Data parsing and normalization
- Correlation of issues spanning multiple sources
- Data retention and archival (compliance)

Security Orchestration, Automation & Response

- *SOAR* automates and coordinates response procedures.
- Improves and speeds repetitive tasks and responses.
- Scheduled, response-based, and manual automation.
- *Playbooks* are automated tasks (running 24x7).

Related Topics:

- Data collection & integration methods
- Cloud-based, serverless script execution
- Authentication and Key management
- REST API capabilities and development

Microsoft Sentinel

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

Limitless cloud speed and scale

Bring your **Office 365 data for Free**

Easy integration with your **existing tools**

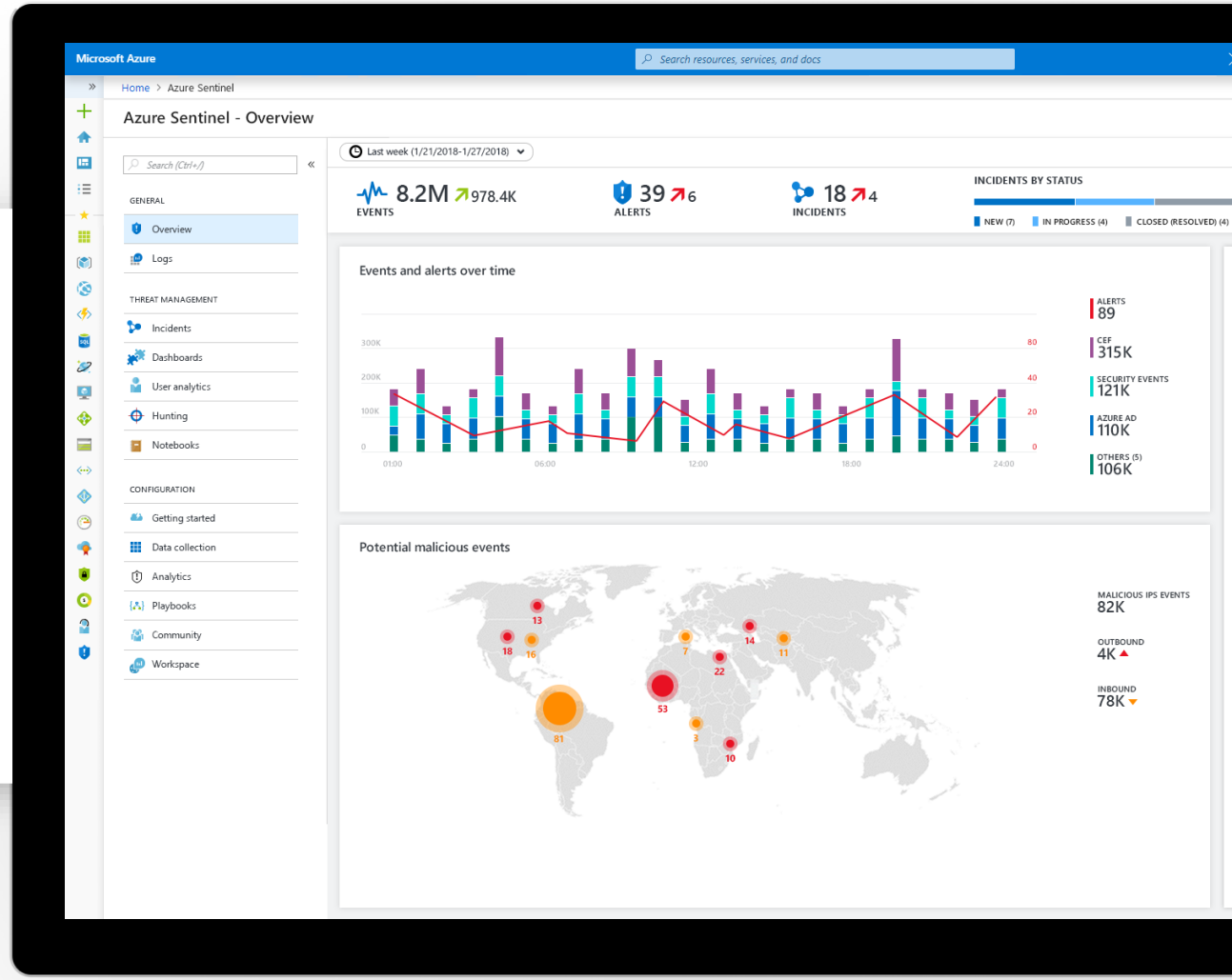
Faster threat protection with **AI by your side**

Focus on security, unburden SecOps from IT tasks

No infrastructure setup or maintenance

SIEM Service available in **Azure portal**

Scale automatically, put no limits
to compute or storage resources



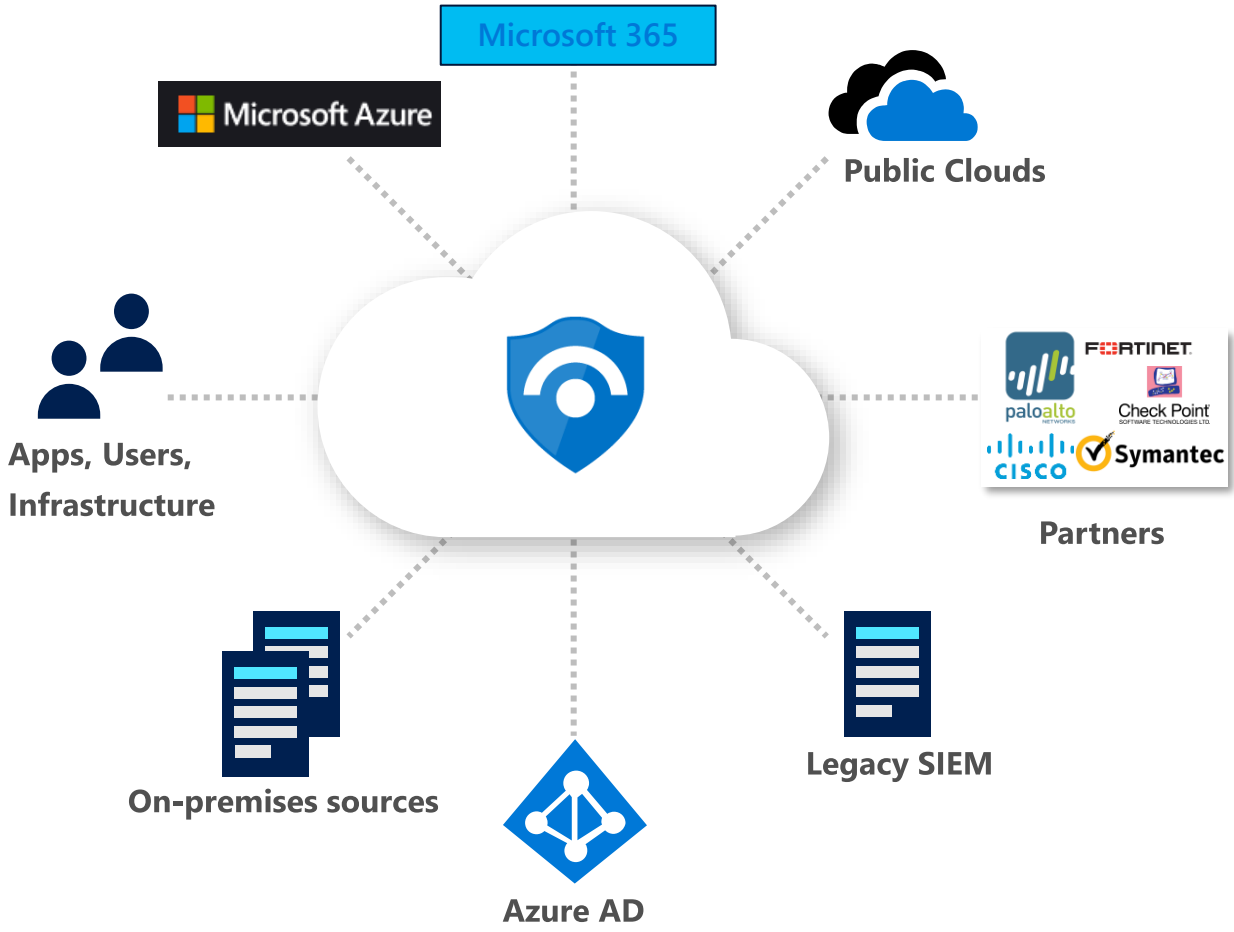
Collect security data at cloud scale from all sources across your enterprise

Pre-wired integration with Microsoft solutions

Connectors for many partner solutions

Standard log format support for all sources

Proven log platform with **more than 10 petabytes** of daily ingestion



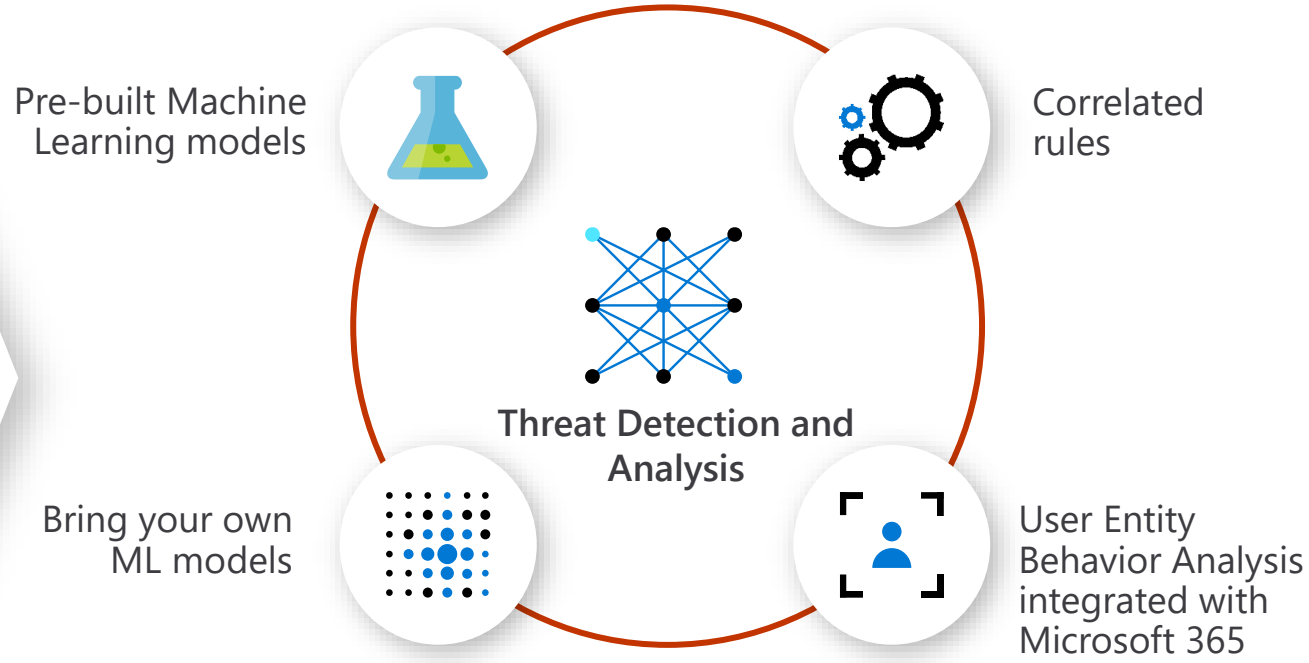
Detect threats and analyze security data quickly with AI

ML models based on **decades of Microsoft security experience and learnings**

Millions of signals filtered to few **correlated and prioritized incidents**

Insights based on vast **Microsoft threat intelligence** and your own TI

Reduce alert fatigue by up to 90%

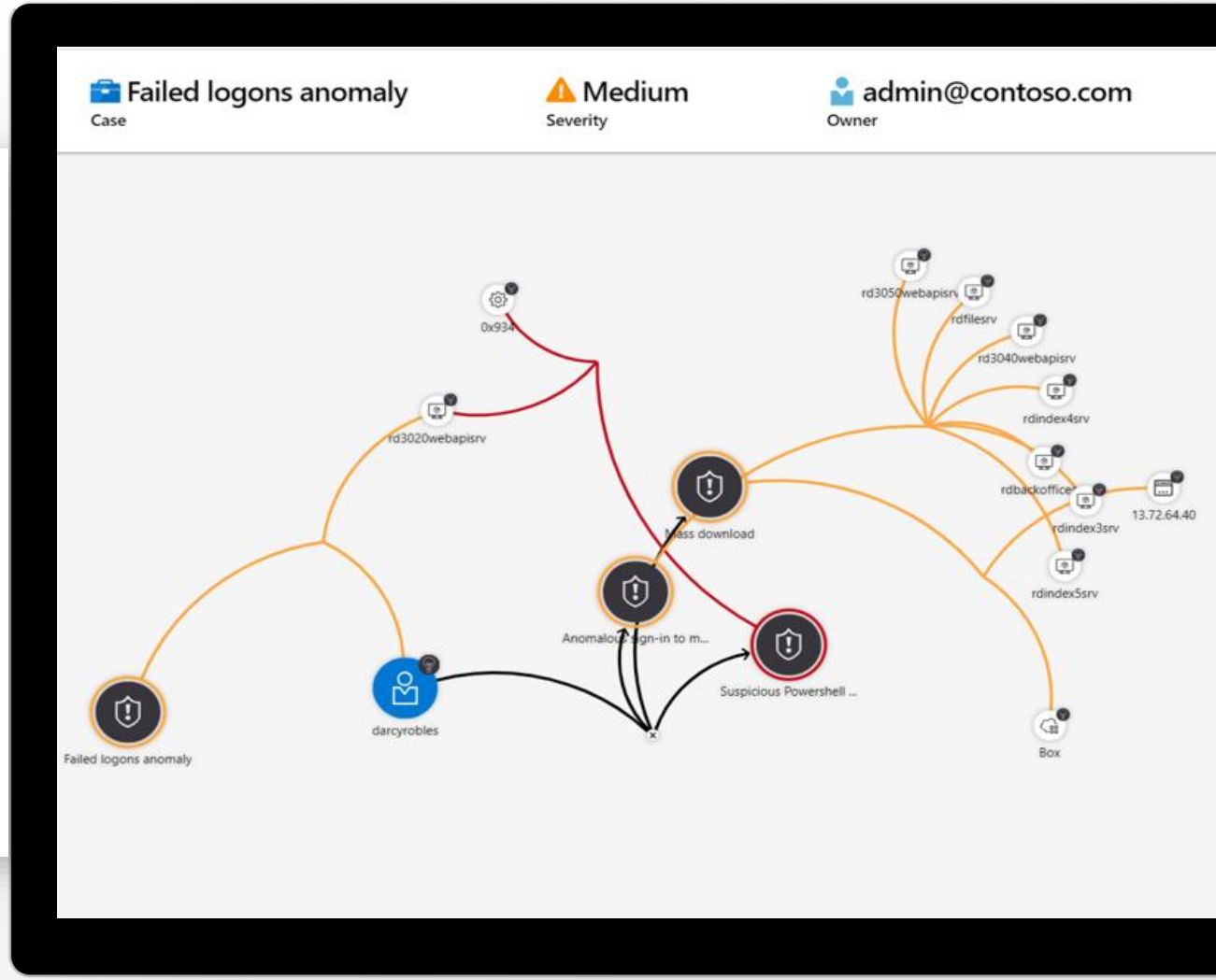


Investigate threats with AI and hunt suspicious activities at scale, tapping into years of cybersecurity work at Microsoft

Get prioritized alerts and **automated expert guidance**

Visualize the entire attack and its impact

Hunt for suspicious activities using **pre-built queries and Azure Notebooks**



AZURE SENTINEL

Core capabilities

Collect

Microsoft Services

Apps, users, infrastructure

Public Clouds

Security solutions

Analyze & detect threats

Machine learning, UEBA

Investigate & hunt suspicious activities

Interactive Attack Visualization, Azure Notebooks

Automate & orchestrate response

Playbooks

Enrichment with Intelligence (Geo location, IP Reputation)

Data Ingestion

Data Repository

Data Search

Azure Monitor (log analytics)

Integrate

ServiceNow

Other tools

Community

Microsoft

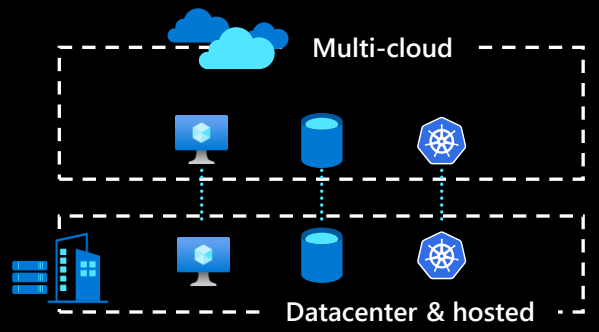
Bonus Section: Azure Arc

Microsoft Sentinel is in the cloud how can I leverage the service?

Note: Dark Theme Slides Next

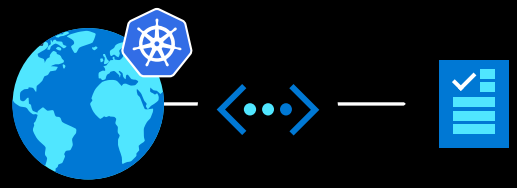
Azure Arc

Extend Azure management and services anywhere



Gain central visibility, operations, and compliance

Standardize visibility, operations, and compliance across a wide range of resources and locations by extending the Azure control plane. Right from Azure, you can easily organize, govern, and secure Windows, Linux, SQL Server, and Kubernetes clusters across datacenters, edge, and multi-cloud.



Build Cloud native apps anywhere, at scale

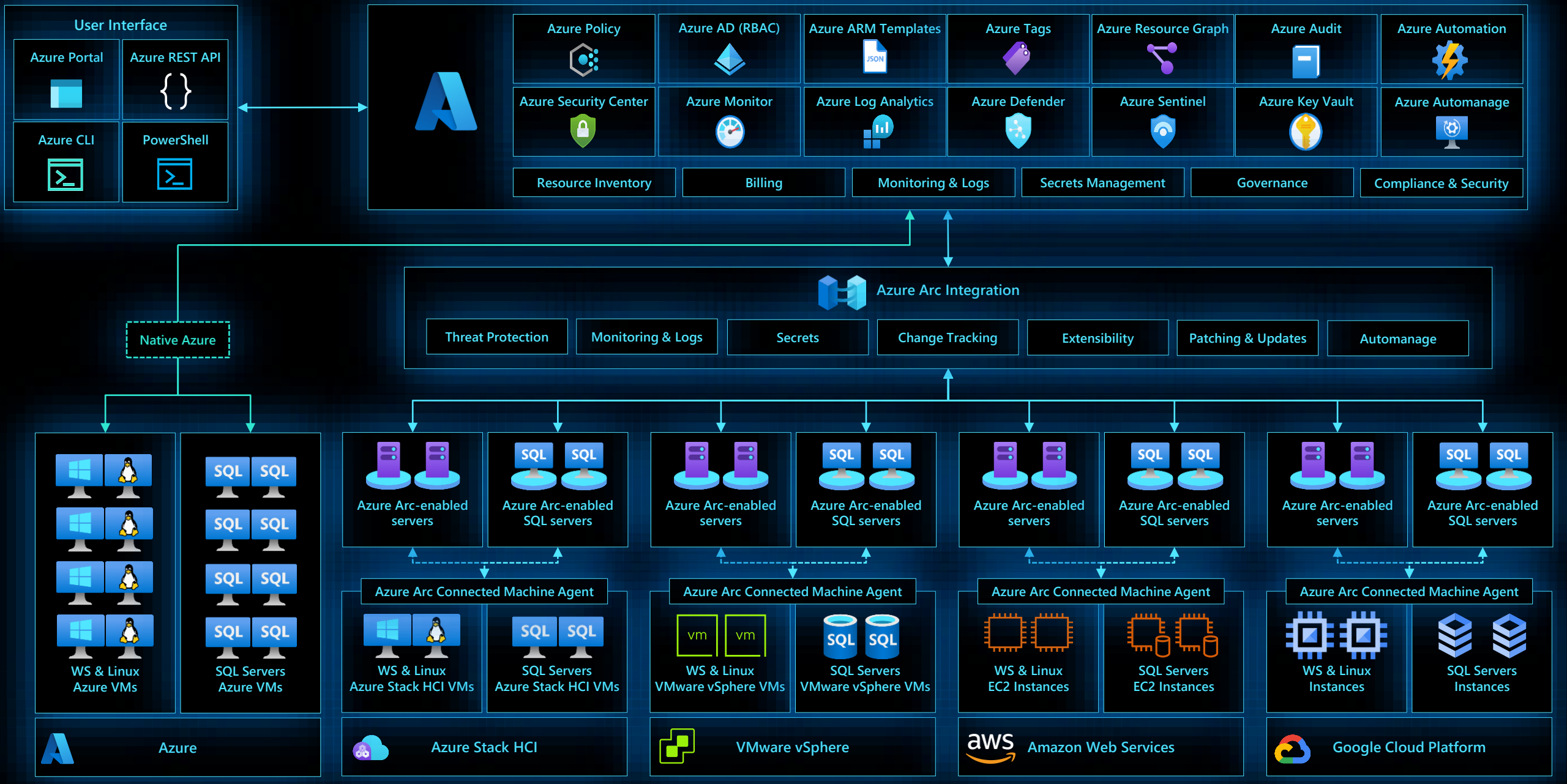
Centrally code and deploy applications confidently to any Kubernetes distribution in any location. Accelerate development by using best in class application services with standardized deployment, configuration, security, and observability.

Run Azure services anywhere

Flexibly use cloud innovation where you need it by deploying Azure services anywhere. Implement cloud practices and automation to deploy faster, consistently, and at scale with always-up-to-date Azure Arc-enabled services.

Azure Arc-enabled servers & Azure Arc-enabled SQL server

On-premises and multi-cloud integration



Microsoft

Close