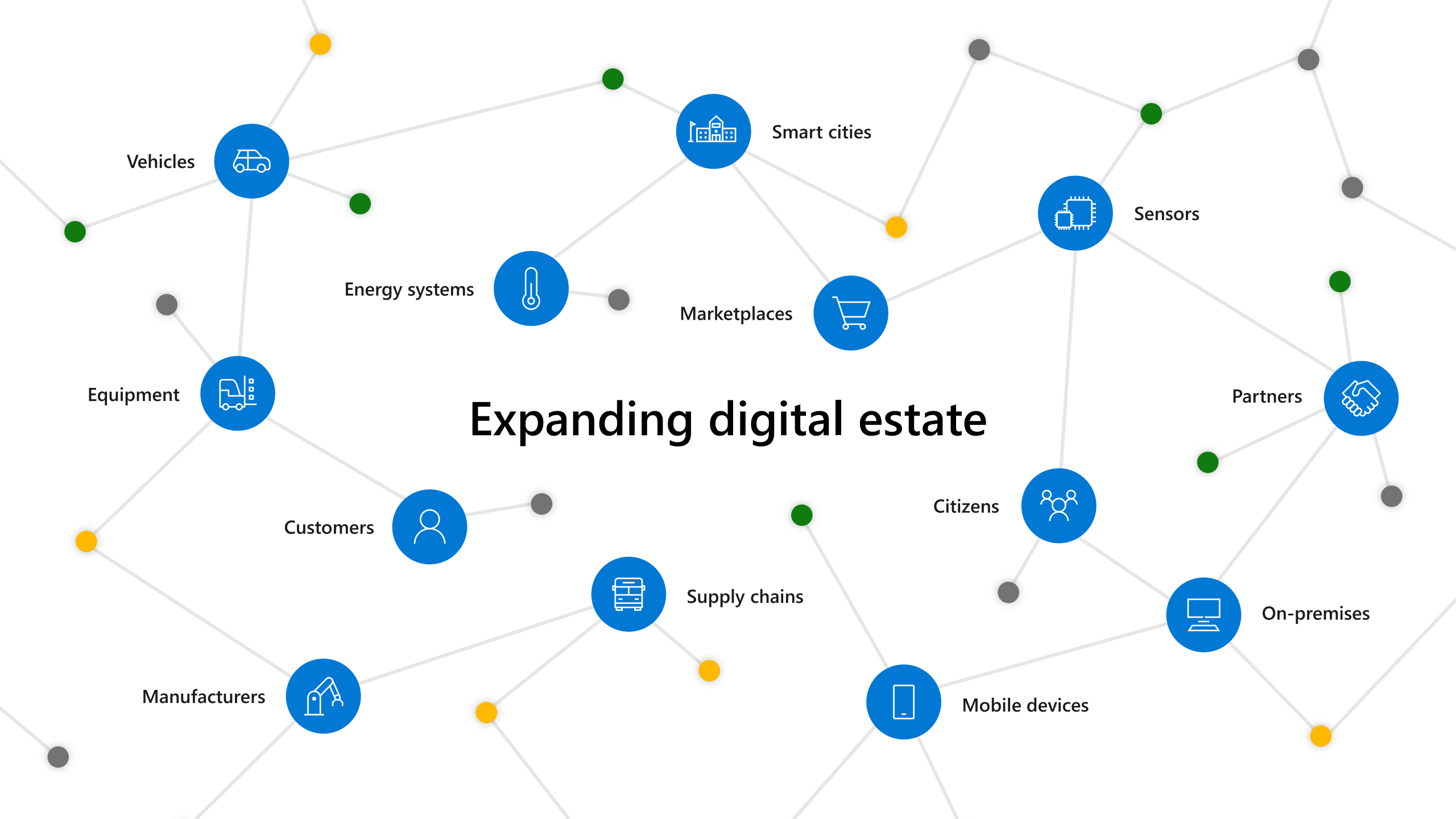
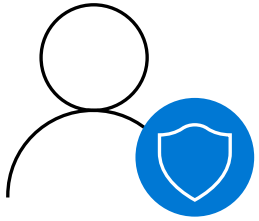
Microsoft Security

Microsoft Sentinel

Author name
Date



Expanding digital estate



Security operations challenges

76% report increasing security data*

Sophistication of threats

IT deployment and maintenance

44% of alerts are never investigated*

Too many disconnected products

3.5M unfilled security jobs in 2021**

Lack of automation

*ESG: Security Analytics and Operations: Industry Trends in the Era of Cloud Computing 2019
**CSO Magazine


Security
Operations Team
Cloud + Artificial Intelligence

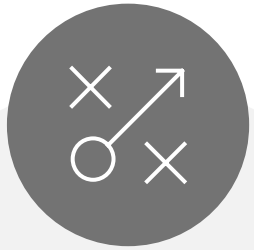
Microsoft Sentinel

Optimize security operations with cloud-native SIEM powered by AI and automation

Harness the scale of the cloud

Detect evolving threats

Expedite incident response



Get ahead of attackers

Harness the scale of cloud-native SIEM

- Eliminate infrastructure setup or maintenance
- Put no limits to compute or storage resources and scale at will
- Collect and analyze data across your entire organization at cloud scale
- Pay only for what you use—resulting in a SIEM 48% less expensive than traditional SIEMs*

*Forrester Consulting, Total Economic Impact™ of Microsoft Sentinel, 2020

Detect evolving threats

- Harness ML based on decades of Microsoft security experience and learnings
- Leverage threat intelligence from Microsoft's expert security team, or bring in your own
- Dive deeper with XDR with Microsoft 365 Defender and Microsoft Defender for Cloud integration

Expedite investigation and response

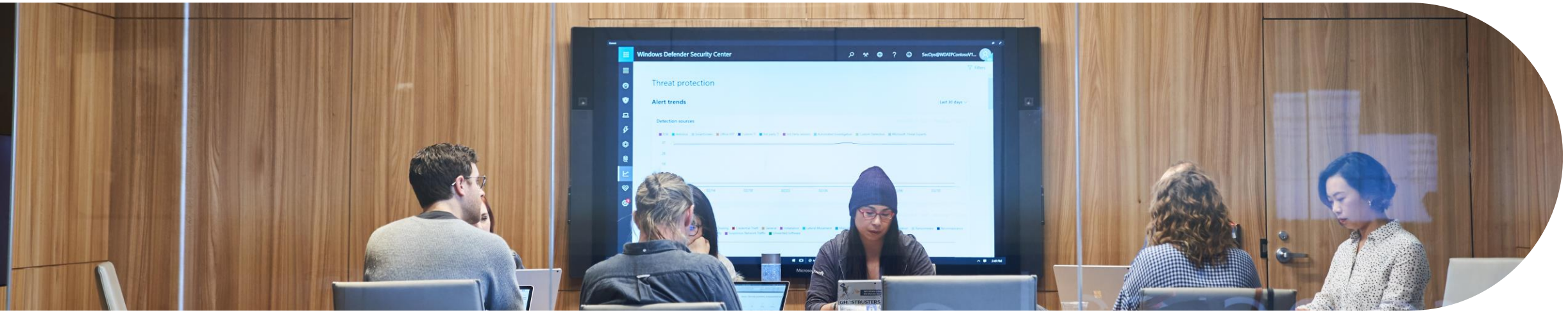
- Focus on what matters with AI that reduces false positives by 79%*
- Easily understand the scope of an attack with incidents that automatically map related entities
- Integrate automation into your day-to-day operations workflow

*Forrester Consulting, Total Economic Impact™ of Microsoft Sentinel, 2020

Stay ahead of attackers

- Rapidly hunt for threats with the speed of the cloud with robust threat hunting tooling
- Get advanced insights into entities fueled by built-in User and Entity Behavior Analytics (UEBA)
- Conduct advanced, custom hunting with built-in Jupyter notebooks

An empowered SecOps team:



48%
less expensive compared to legacy SIEMs

79%
decrease in false positives over three years

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

56%
reduction in management effort for infrastructure and SIEM

80%
reduction in investigation labor effort

201%
ROI over 3 years

Forrester Consulting, Total Economic Impact™ of Microsoft Sentinel, 2020

FORRESTER®

Microsoft Sentinel—a Leader in the Forrester Wave™: Security Analytics Platform

"**Microsoft roars into the security analytics market…**
The vendor's entry into the security analytics space captivated security buyers. Microsoft's bold move to allow the ingestion of Microsoft Azure and Microsoft Office 365 activity logs into Sentinel at no cost makes the solution attractive to enterprises invested in Azure and Microsoft 365."

- **The Forrester Wave™: Security Analytics Platforms, Q4 2020 report**

Microsoft Sentinel has more than 10,000 paying customers analyzing 5 petabytes of data per month

RapidDeploy
CLOUD AIDED DISPATCH™

asos

thycotic

avanade

FIRSTWEST
CREDIT UNION

LinkedIn

MVP
HEALTH CARE

OFFICE OF THE STATE TREASURER OF GEORGIA 1776

"We use Microsoft Sentinel (formerly Azure Sentinel) to gain a bird's-eye view of everything. We now have a lot more data connections, a far better view of all incidents, and security processes that are more efficient and effective."

Stuart Gregg
Cyber Security Operations Lead
ASOS

asos

An end-to-end solution for security operations

Powered by community + backed by Microsoft's security experts

Collect

Visibility

Detect

Analytics

Hunting

Intelligence

Investigate

Incidents

Respond

Automation

Visibility

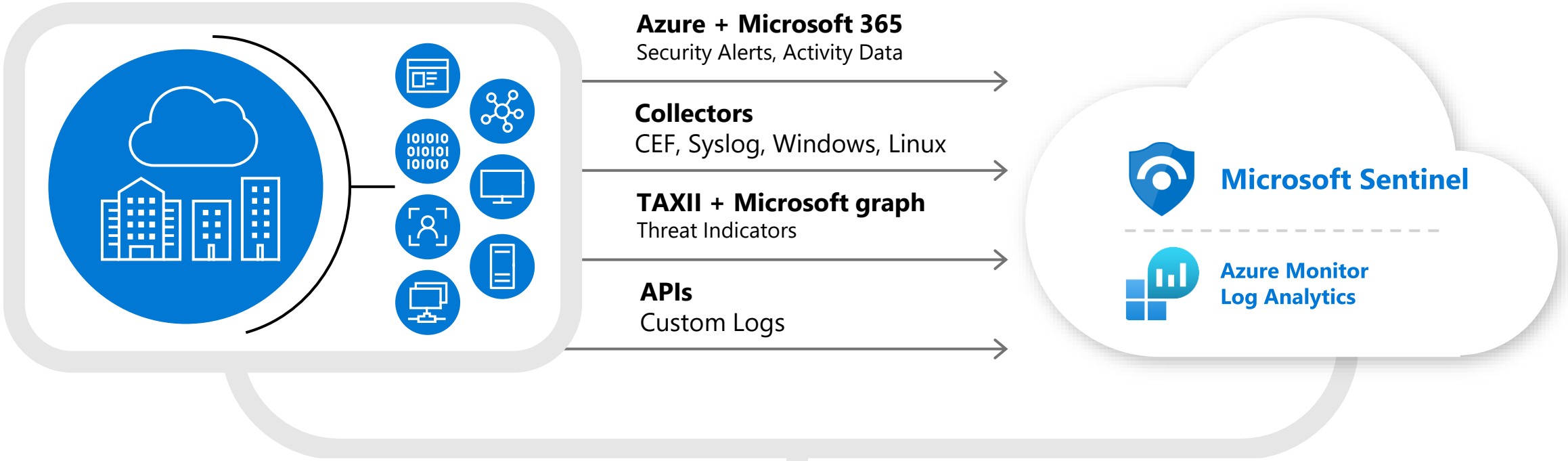
Collect data at cloud scale from any source

Hundreds of out-of-the-box integrations

Collect data from Azure, other clouds, and on-prem

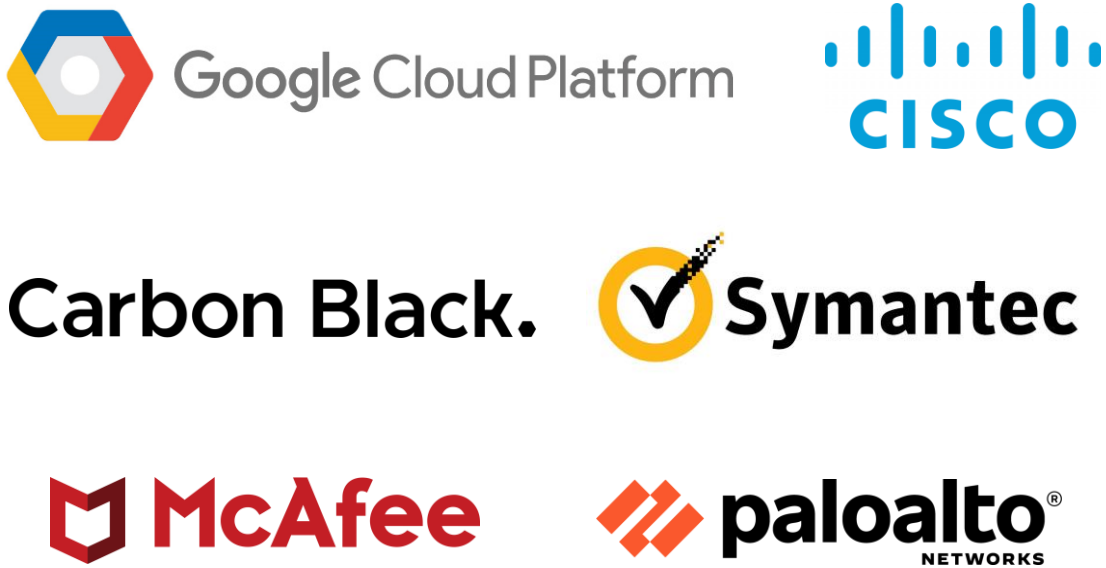
Build customizable visualizations

Collect security data at cloud scale from any source



Proven log platform with more than 10 petabytes of daily ingestion

Integrate out-of-the-box with your existing tools in Azure, on-premises, or in other clouds



150+ out-of-the-box integrations, with more on the way

Get interactive dashboards for powerful insights

- Choose from a gallery of workbooks
- Customize or create your own workbooks using queries
- Take advantage of rich visualization options
- Gain insight into one or more data sources

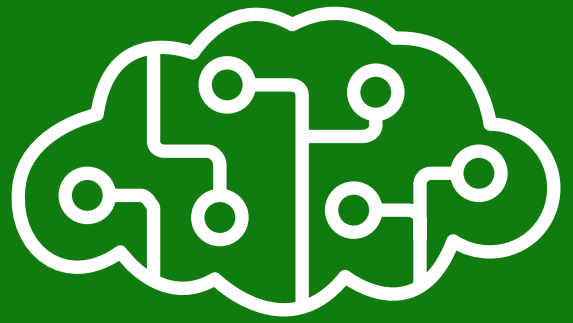
Analytics

Detect threats with machine learning (ML) and advanced analytics

Reduce false positives by 78%*

ML trained by trillions of signals daily

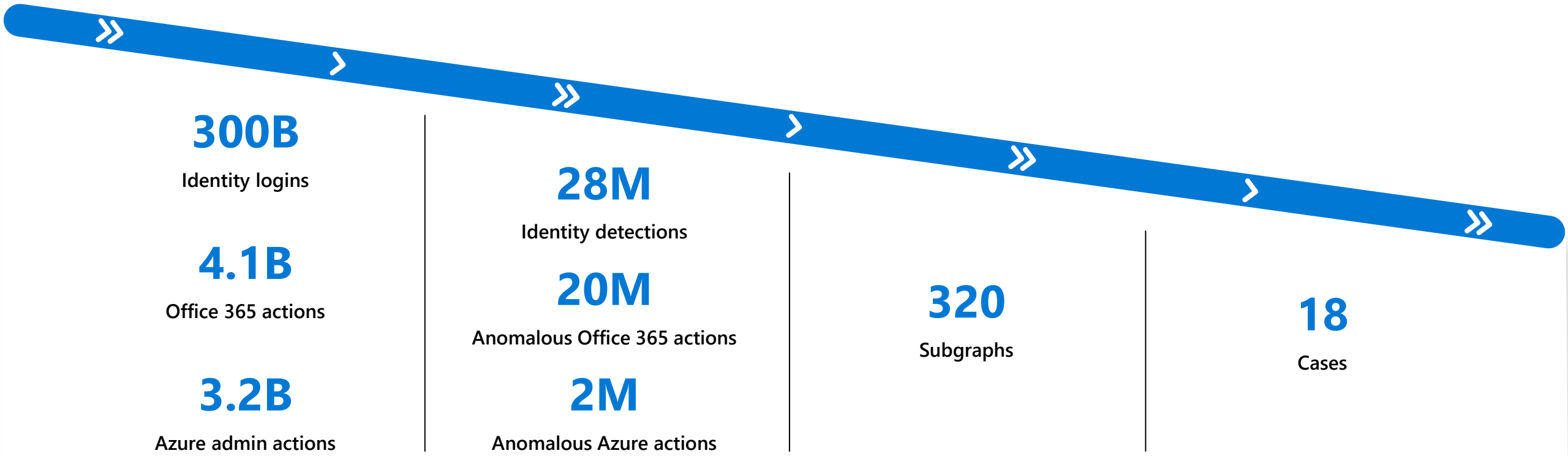
Built-in UEBA



*Forrester Consulting, Total Economic Impact™ of Microsoft Sentinel, 2020

Reducing alert fatigue

Analyzing activities across multiple cloud services into high-fidelity security cases



Service layer raw events

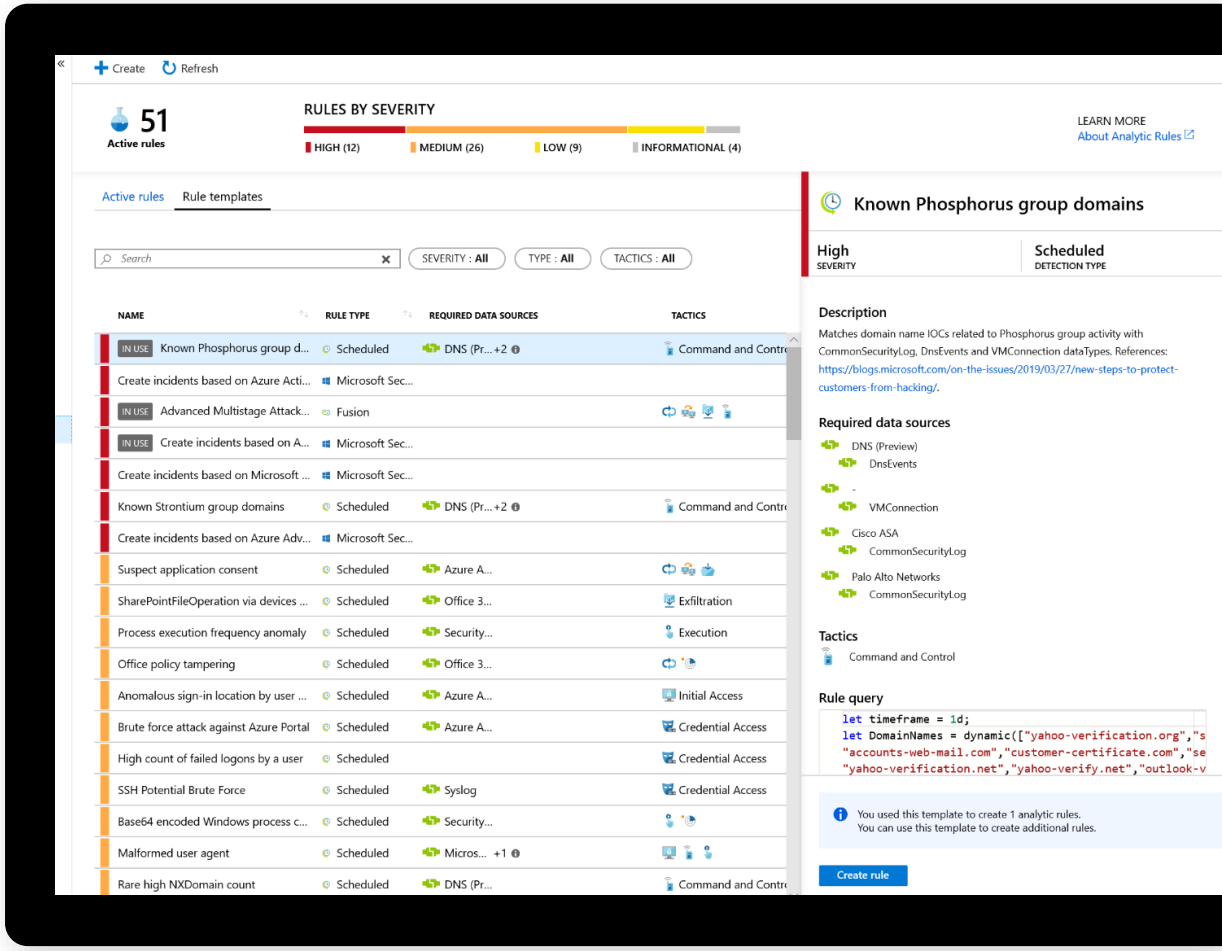
Anomalous behaviors and detections

Convert to graph

Score each subgraph with Machine Learning

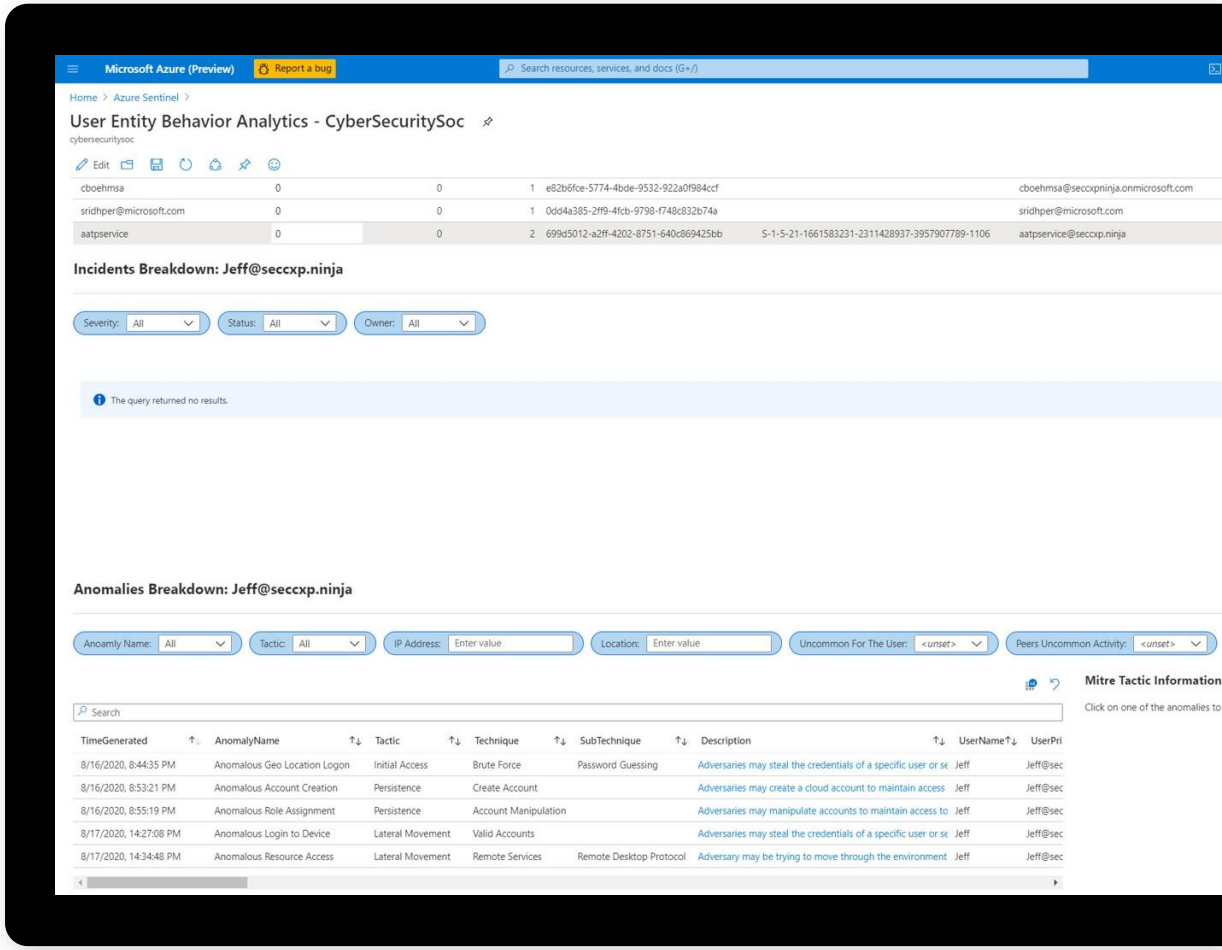
Leverage extensive library of detections or build your own

- Choose from more than 100 built-in analytics rules
- Customize and create your own rules using KQL queries
- Correlate events with your threat intelligence and now with Microsoft URL intelligence + network data
- Democratize machine learning with code-free, customizable ML anomaly detections



Improve insider and unknown threat detection with User and Entity Behavior Analytics

- Use behavioral insights to detect anomalies, understand the relative sensitivity of entities, and evaluate potential impact
- Get baseline behavioral profiles of entities across time and peer group horizons



Powered by the proven Microsoft User and Entity Behavior Analytics (UEBA) engine

Hunting

Get ahead of threats with advanced hunting tools

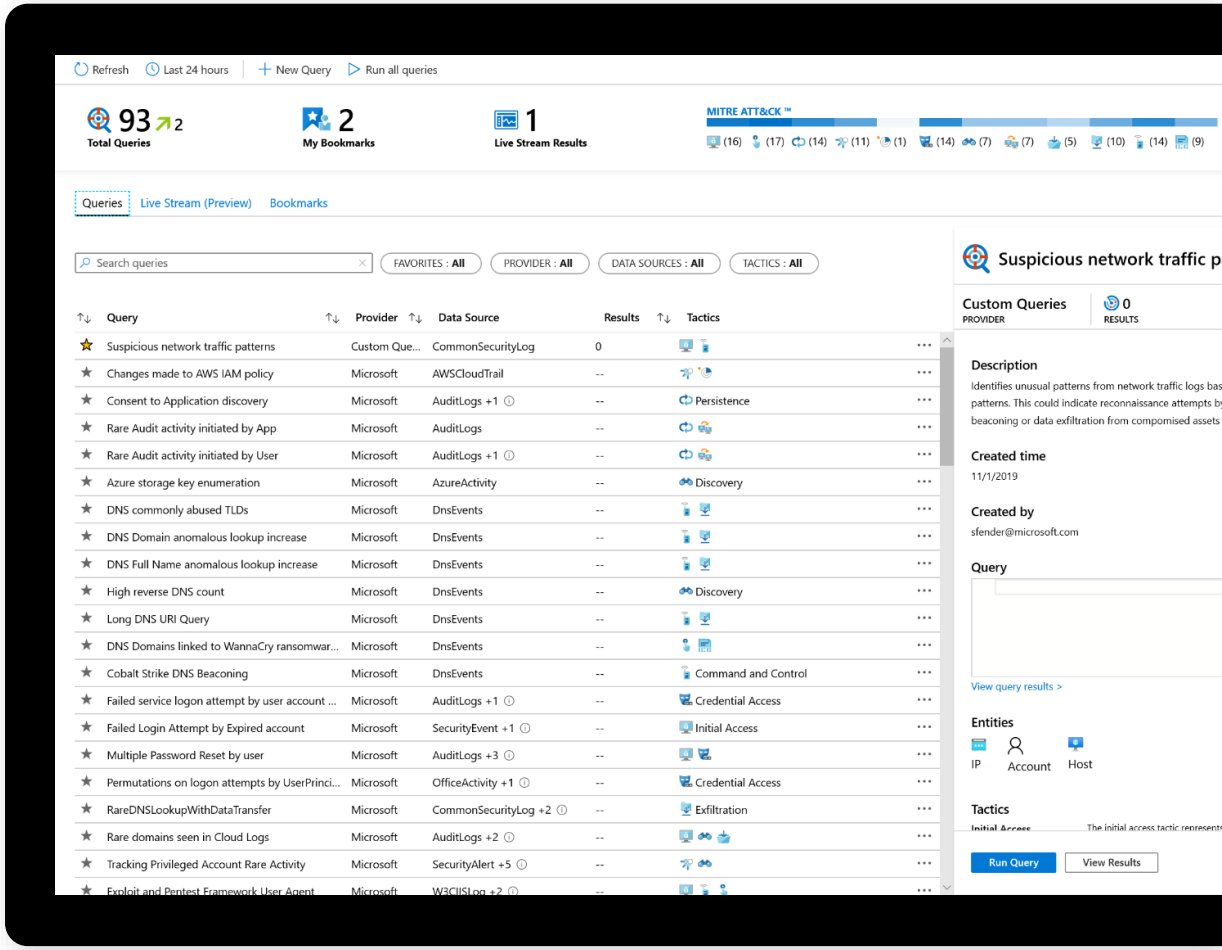
Enrich hunting with threat intelligence

Customize hunts with watchlists

Conduct advanced hunting with Jupyter Notebooks

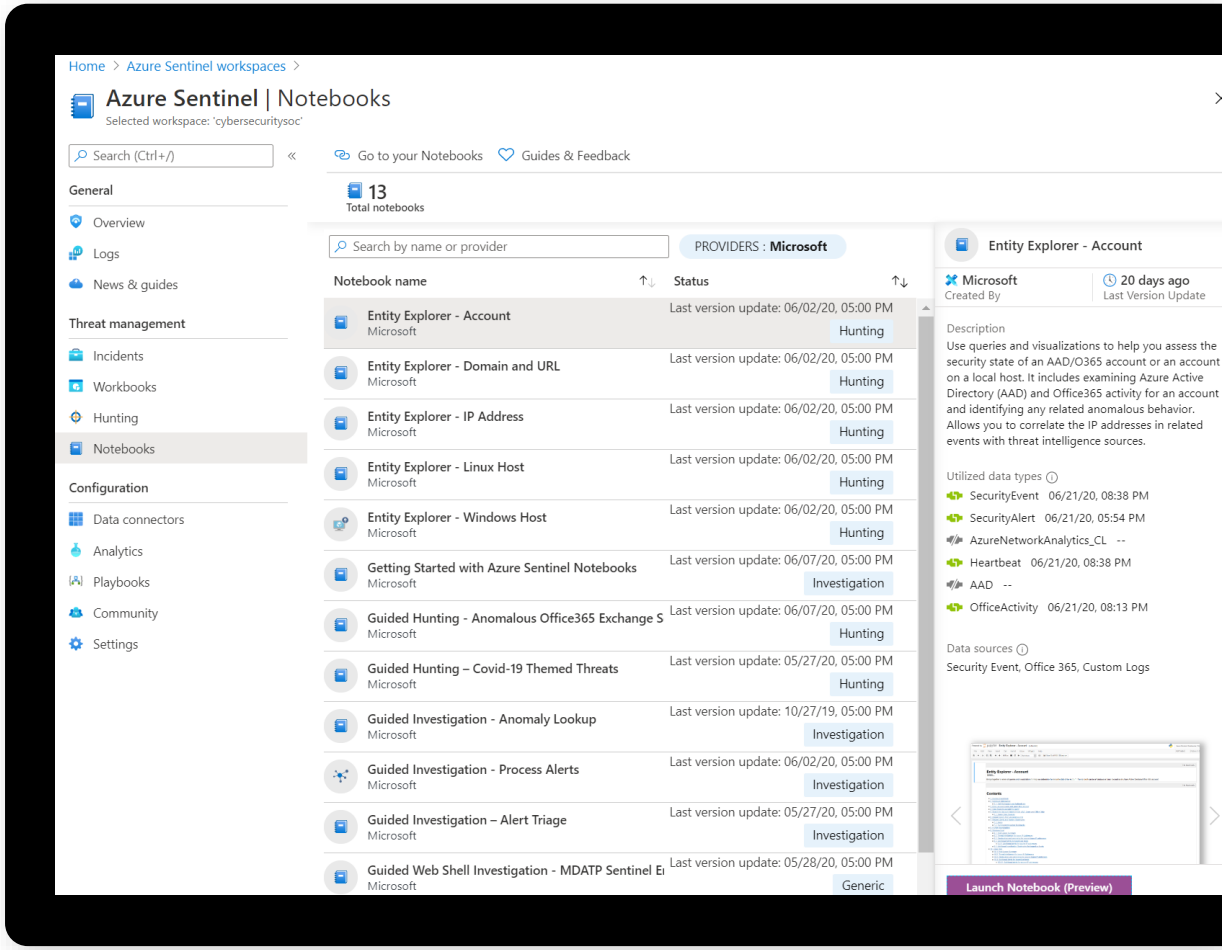
Start hunting over security data with fast, flexible queries

- Run built-in threat hunting queries—no prior query experience required
- Customize and create your own hunting queries using KQL
- Integrate hunting and investigations
- Use bookmarks and live stream to manage your hunts



Use Jupyter notebooks for advanced hunting

- Run in Azure Machine Learning
- Use sample templates to help you get started
- Save as sharable HTML/JSON
- Query Microsoft Sentinel data and bring in external data sources
- Use your language of choice—Python, SQL, KQL, R, …



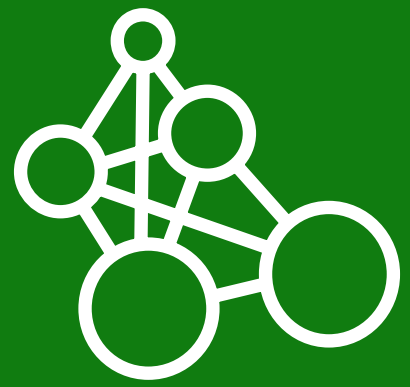
Intelligence

Fuel threat detection and hunting with advanced threat intelligence

Unify management of TI from any source

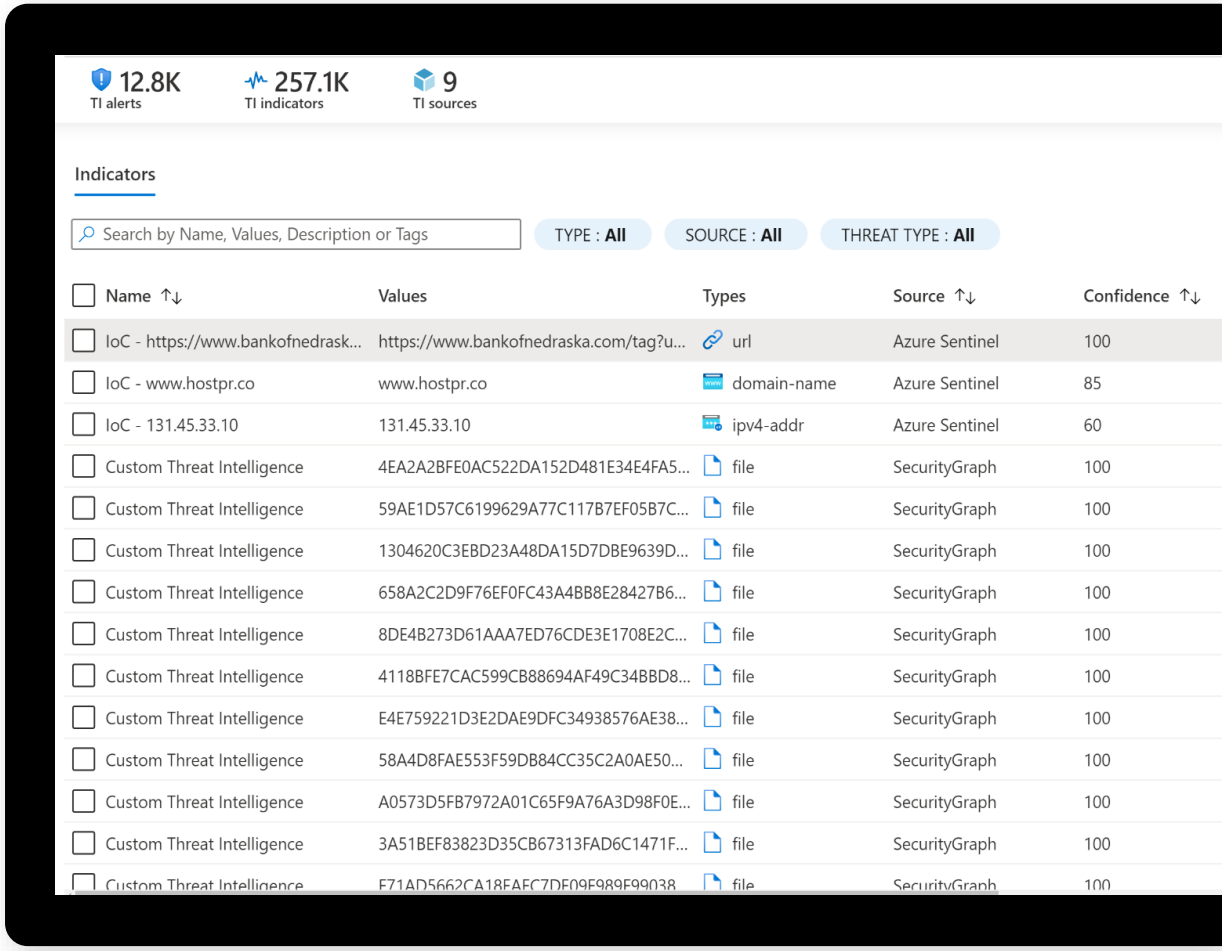
Integrate insights with watchlists

Get entity insights with UEBA profiles



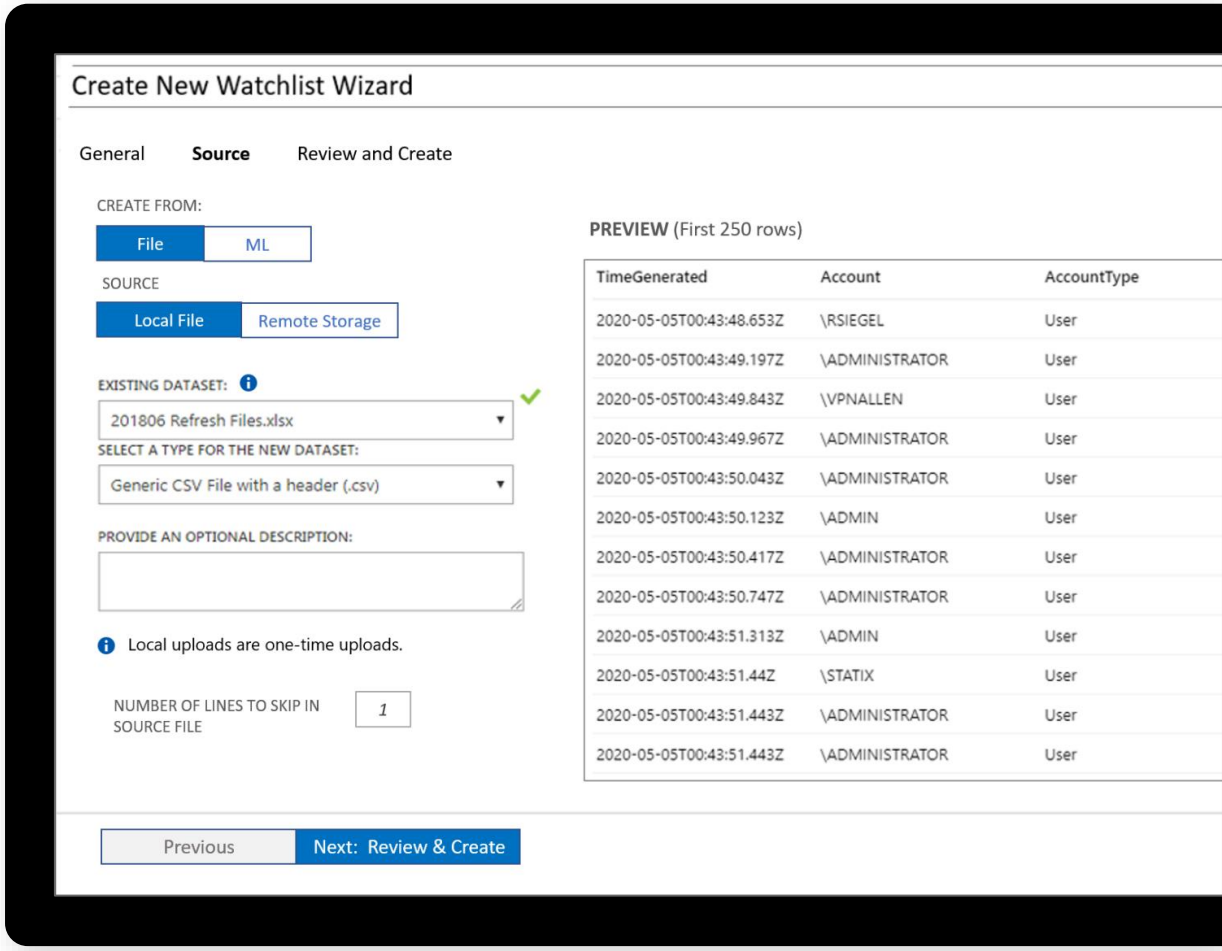
Monitor and manage threat intelligence

- Create, view, search, filter, sort, and tag all your threat indicators in a single pane
- Use alert metrics to help understand top threats targeting your organization
- Use automation playbooks for leading threat intelligence providers to enrich alerts



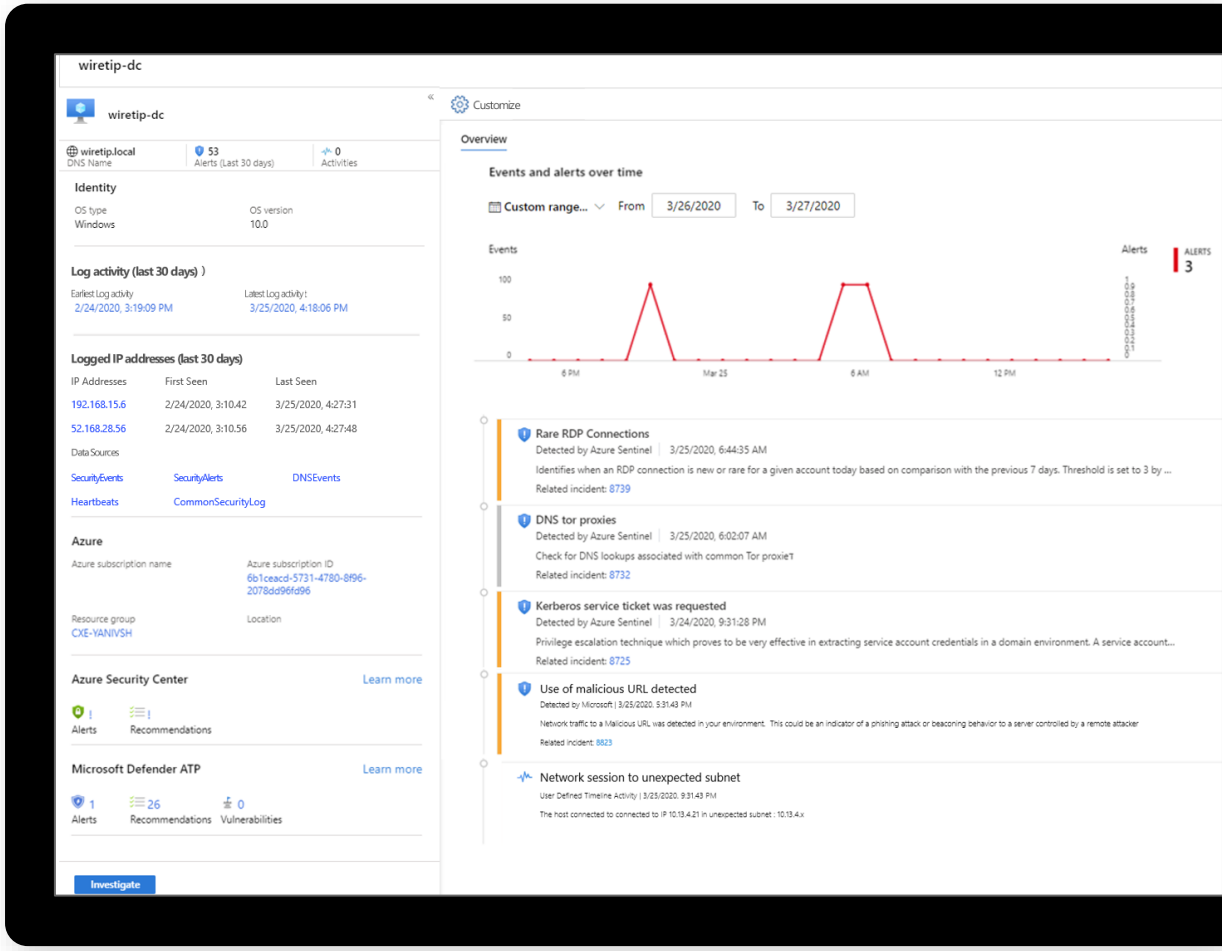
Use Watchlists to integrate business insights

- Create collections of data for threat hunting and detection (e.g. restricted IPs, trusted systems, critical assets, risky users, vulnerable hosts)
- Incorporate watchlists into analytic rules, hunting queries, workbooks, and more—create allow/deny lists, add context, and add enrichments
- Upload a CSV file, create automation playbooks upload



Access unified insights with entity profiles

- Get a complete view of a host or user by bringing together data from multiple sources, including UEBA
- View timeline information across the most relevant data sources
- Use Insights to quickly identify activities of interest
- Customize timeline to tune results and add other data sources
- Link directly to Microsoft 365 and Microsoft Defender for Cloud where relevant for more information



Incidents

Streamline investigation with incident insights

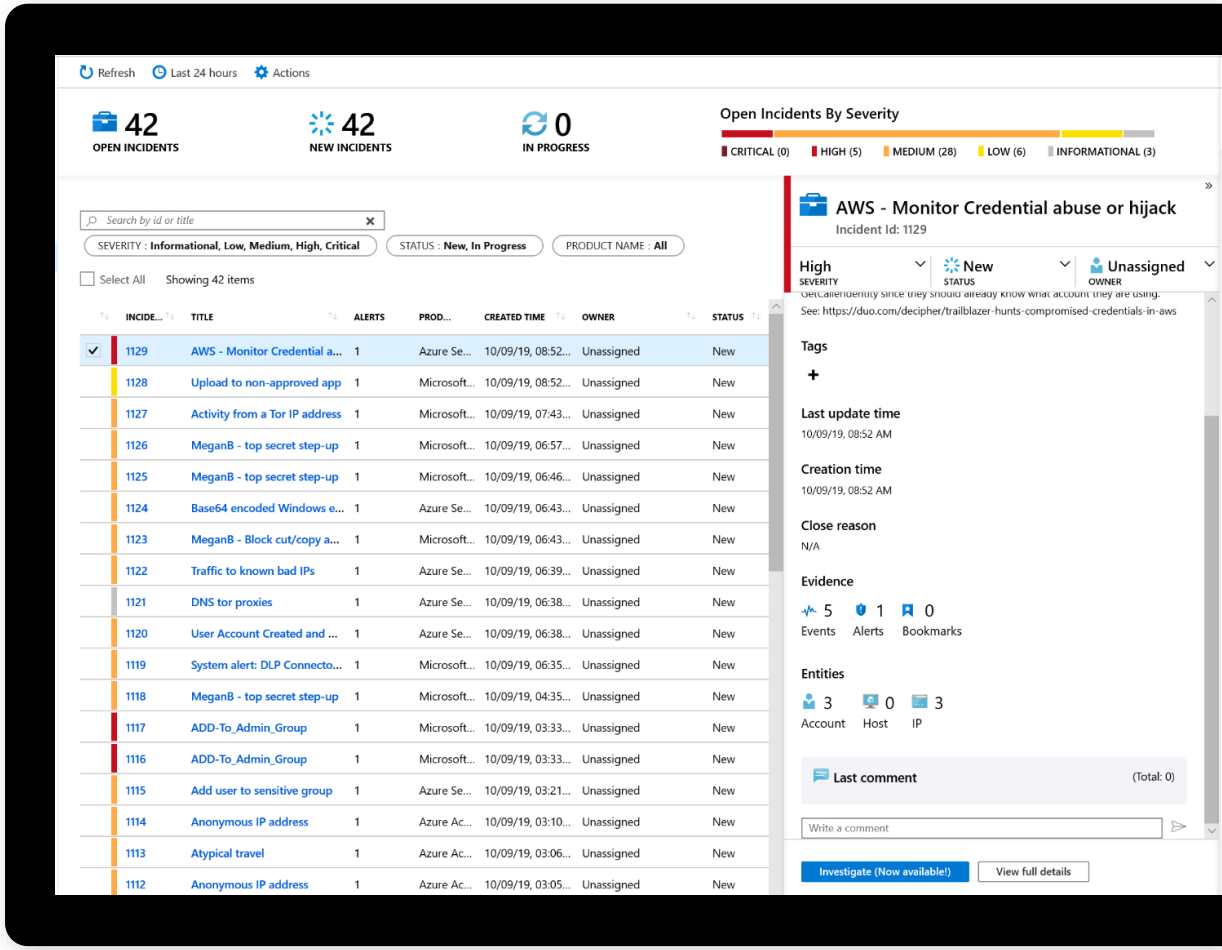
Centralize investigations with prioritized incidents

Understand the full scope of the attack

Ask the right questions with AI

Start and track investigations from prioritized, actionable security incidents

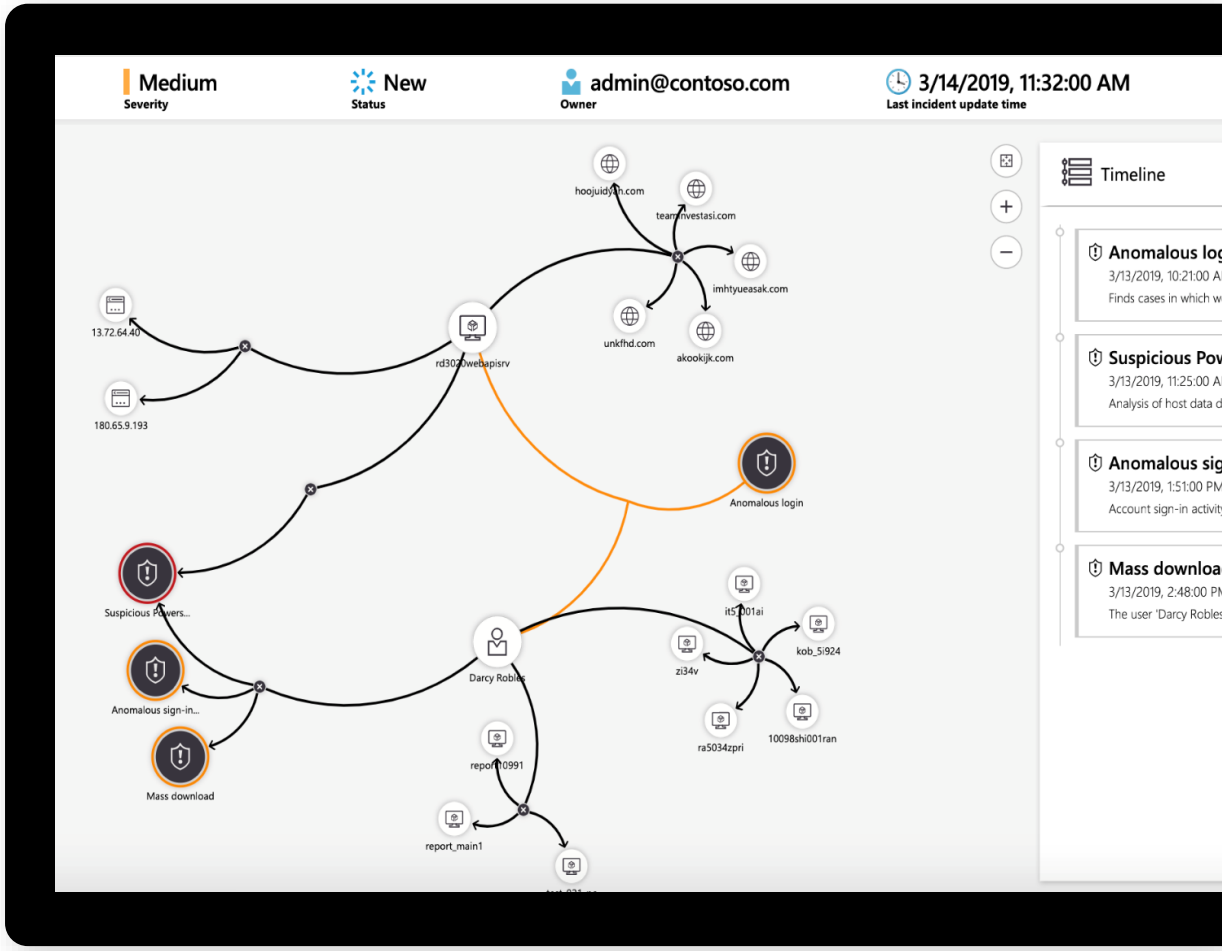
- Use incident to collect related alerts, events, and bookmarks
- Manage assignments and track status, with automation at your fingertips
- Collaborate easily with built-in Microsoft Teams integration



Visualize the entire attack to determine scope and impact

- Navigate the relationships between related alerts, bookmarks, and entities
- Expand the scope using exploration queries
- Gain deep insights into related entities—users, domains, and more

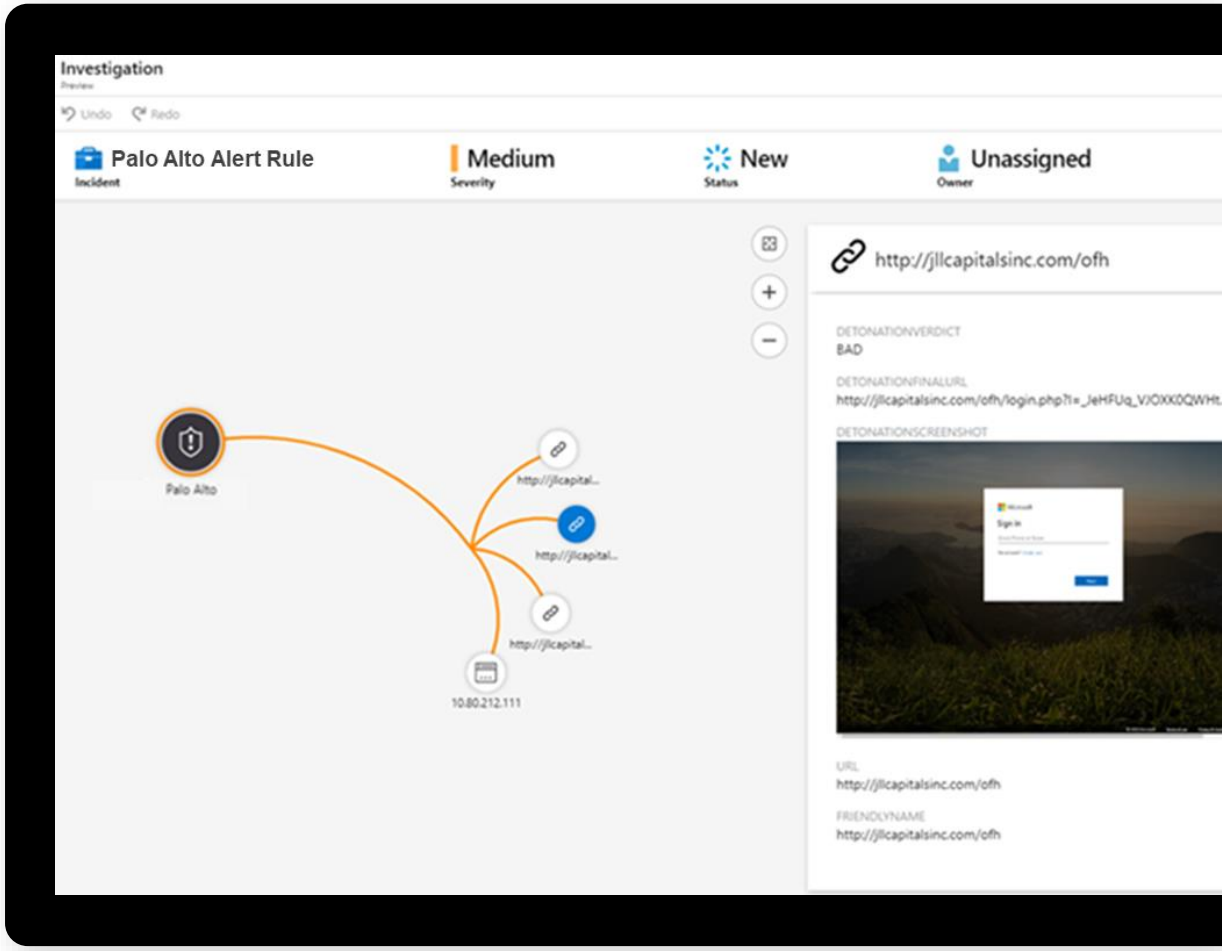
80% reduction in investigation effort compared to legacy SIEMs[1]



1: Commissioned study-The Total Economic Impact™ of Microsoft Sentinel, conducted by Forrester Consulting, 2020

Gain deeper insight with built-in automated detonation

- Configure URL Entities in analytics rules
- Automatically trigger URL detonation
- Enrich alerts with Verdicts, Final URLs and Screen Shots (e.g. for phishing sites)



Automation

Accelerate response and save time on common tasks

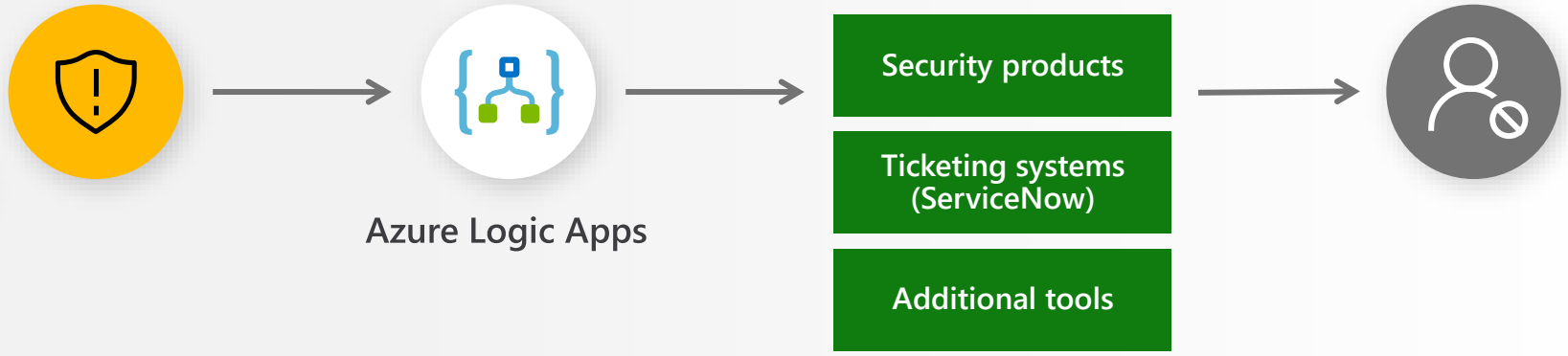
Integrate automation across tools

Streamline incident management

Automate your daily routines

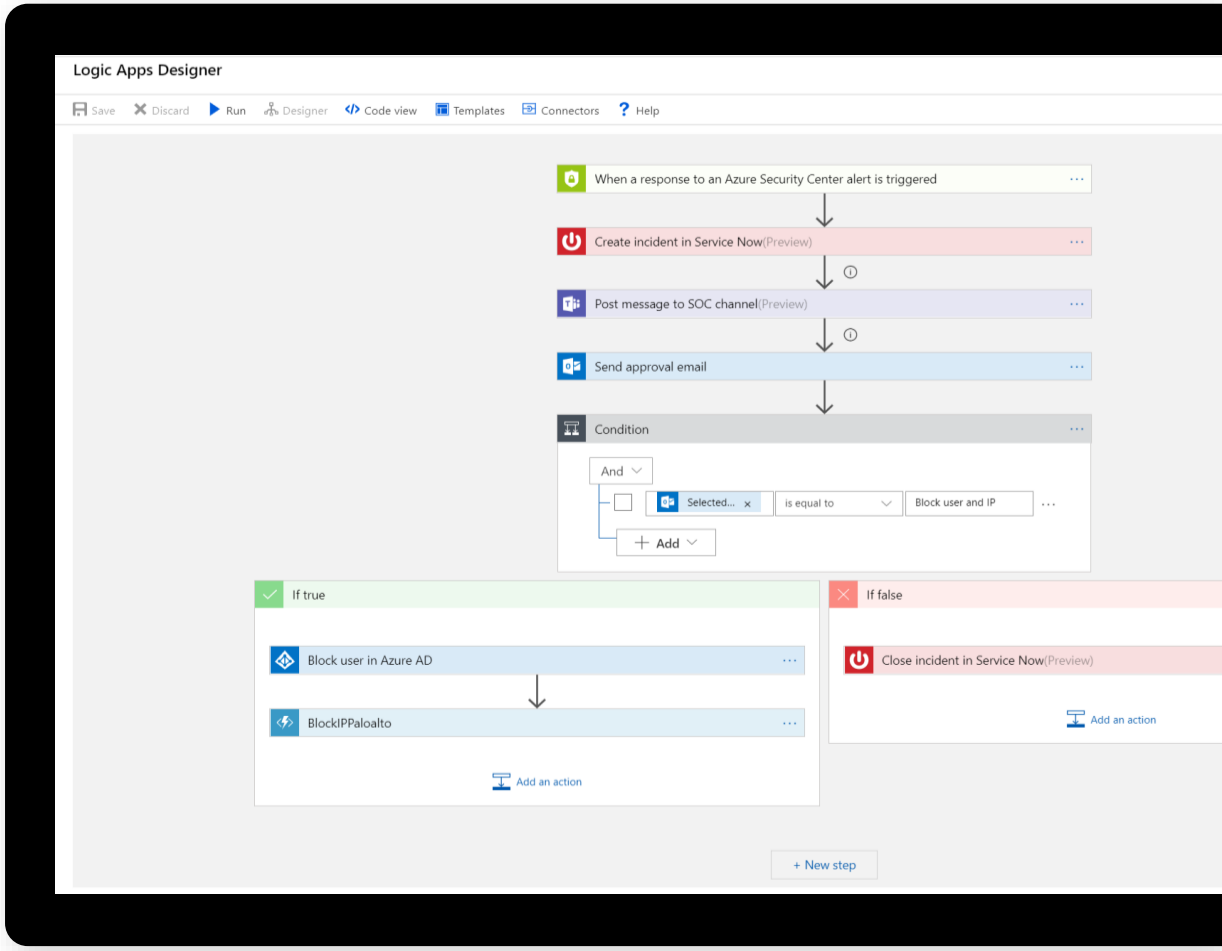
Respond rapidly with built-in orchestration and automation

Build automated and scalable playbooks that integrate across tools



Automate and orchestrate security operations using integrated Azure Logic Apps

- Build automated and scalable playbooks that integrate across tools
- Choose from a library of samples
- Create your own playbooks using 200+ built-in connectors
- Trigger a playbook from an alert or incident investigation



Take actions today: Get started with Microsoft Sentinel

Start
Microsoft Azure trial

Open Microsoft Sentinel
dashboard in Azure portal

Connect
data sources

To learn more, visit
https://aka.ms/MicrosoftSentinel

Microsoft Security

Thank you

Appendix

Total Economic Impact™ of Microsoft Sentinel
from Forrester Consulting

48% less expensive compared to legacy SIEMs

79% decrease in false positives over three years

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

56% reduction in management effort for infrastructure and SIEM

80% reduction in investigation labor effort

→ 201% ROI over three years

→ Less than 6-month payback

RapidDeploy
CLOUD AIDED DISPATCH™

Customer:
RapidDeploy

Industry:
Partner Professional Services

Size:
75 employees

Country:
United States

Products and services:
Microsoft Sentinel
Microsoft Defender for Cloud
Azure Monitor

Read full story here

Microsoft

"We're here to help first responders and stop terrorists, nation-state attackers, and others from threatening public safety—and we use Microsoft Sentinel to help us do it."

—Alex Kreilein, Chief Information Security Officer, RapidDeploy

Situation:

To safeguard its cloud aided dispatch systems for emergency first responders from an array of serious cybersecurity threats, RapidDeploy wanted to add a Security Information and Event Management (SIEM) system to its security infrastructure.

Solution:

The company implemented Microsoft Sentinel, Microsoft Defender for Cloud, and Azure Monitor to provide complete threat visibility across its on-premises systems, cloud infrastructure, and IoT assets and to automate responses to identified threats.

Impact:

RapidDeploy now has more visibility and control over its infrastructure and can deploy Microsoft Sentinel in a fraction of the time and cost of alternative SIEMs, helping it safeguard vital public safety systems and deliver more value to customers.

ASOS

Customer
ASOS

Industry
Retailers

Size
1,000 - 9,999 employees

Country
United Kingdom

Products and Services
Azure
Azure Active Directory
Azure Monitor
Microsoft Defender for Cloud
Microsoft Sentinel
Office 365

Read full story here

Microsoft

"We found Microsoft Sentinel easy to set up, and now we don't have to move data across separate systems. We can literally click a few buttons and all our security solutions feed data into Microsoft Sentinel."

— Stuart Gregg, Cyber Security Operations Lead, ASOS

Situation:

To help deal with daily cyberthreats, online retailer ASOS needed to gain a bird's-eye view of all its security activities, spread across five teams and two separate security operation centers.

Solution:

Already an Azure user, the company opted to feed data from multiple security solutions into Microsoft Sentinel, using its as a single source of truth for all security information and processes.

Impact:

With Microsoft Sentinel, ASOS has enabled more efficient security processes, captured 3.7 billion events, generated 23,100 alerts, resolved 519 incidents, and reduced the time spent on case management and resolution by 50 percent.

avanade

Customer
Avanade

Industry
Partner Professional Services

Size
36,000 employees

Country
United States

Products and Services
Microsoft Sentinel
Microsoft Defender for Cloud
Azure Active Directory

[Read full story here]

Microsoft

"Using Microsoft Sentinel helps us move beyond managing our SIEM on-premises and instead focus on the value add that's on top of it—how to do more interesting strategic work."

— Greg Petersen, Senior Director, Security Technology and Operations Team, Avanade

Situation:

As a Microsoft software integrator, Avanade wanted to stay on the leading edge of security technology, speed threat detection, and centralize security management in the cloud.

Solution:

Avanade turned to Microsoft Sentinel, one of the world's first cloud-native security information and event management (SIEM) systems. The company used out-of-the-box connectors in Microsoft Sentinel to quickly integrate its data across Microsoft applications.

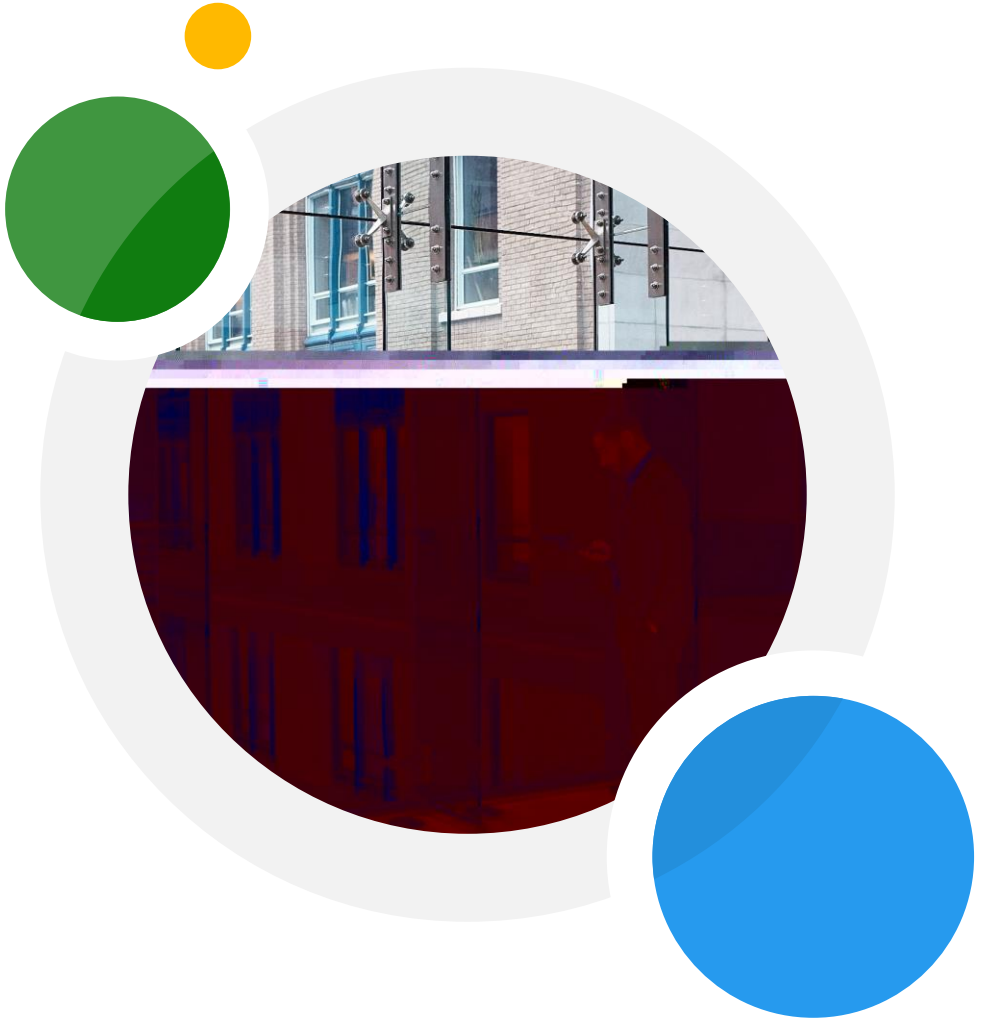
Impact:

By deploying Microsoft Sentinel, Avanade leaped forward with its cloud-first strategy. It has integrated data, improved automation, freed up IT staff time, and will use machine learning to improve threat detection and response.

SWC | TECHNOLOGY PARTNERS
A BDO USA Company

"With Microsoft threat intelligence built into Microsoft Sentinel, we've improved our reaction time to threats and attacks. What used to take hours, we now get done in minutes."

- Ric Opal, Vice President of Marketing, SWC Technology Partners



SWC | TECHNOLOGY PARTNERS
A BDO USA Company

"Microsoft has found the right mix. The ease of interoperation among Microsoft tools like Azure Active Directory, Cloud App Security, and Office 365 is fantastic. With Microsoft Sentinel, our team can focus on client problems and not SIEM integration issues."

- Ric Opal, Vice President of Marketing, SWC Technology Partners