



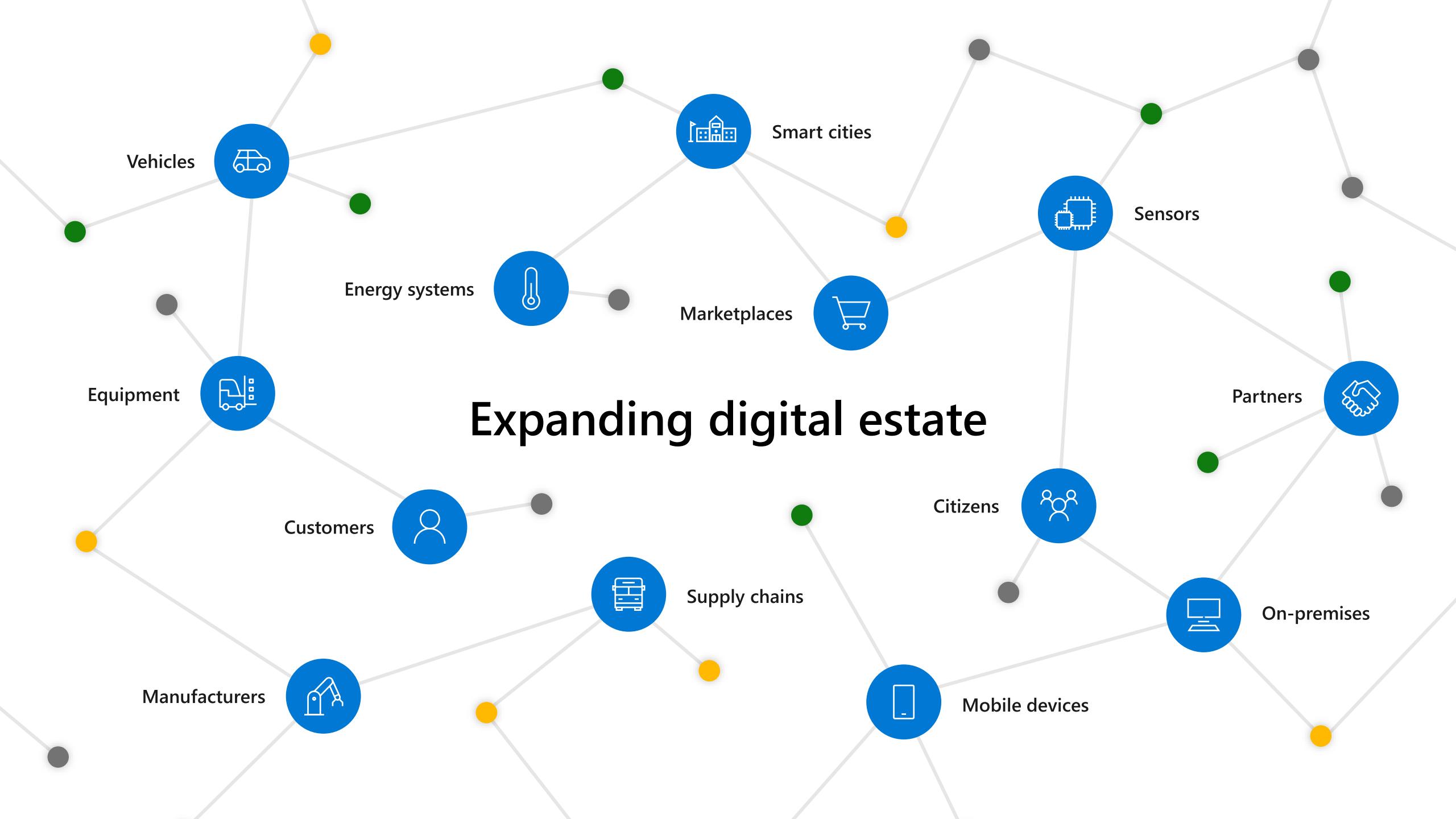
# Microsoft Sentinel

Author name

Date



# Expanding digital estate



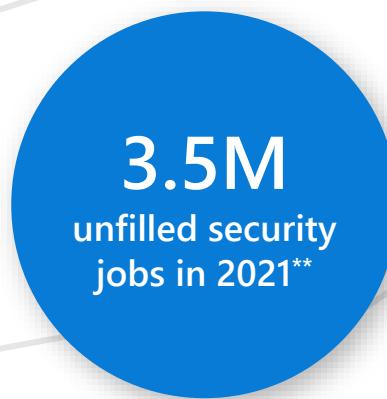


Sophistication  
of threats

IT deployment and  
maintenance

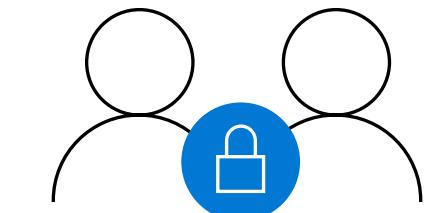


Too many  
disconnected  
products



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

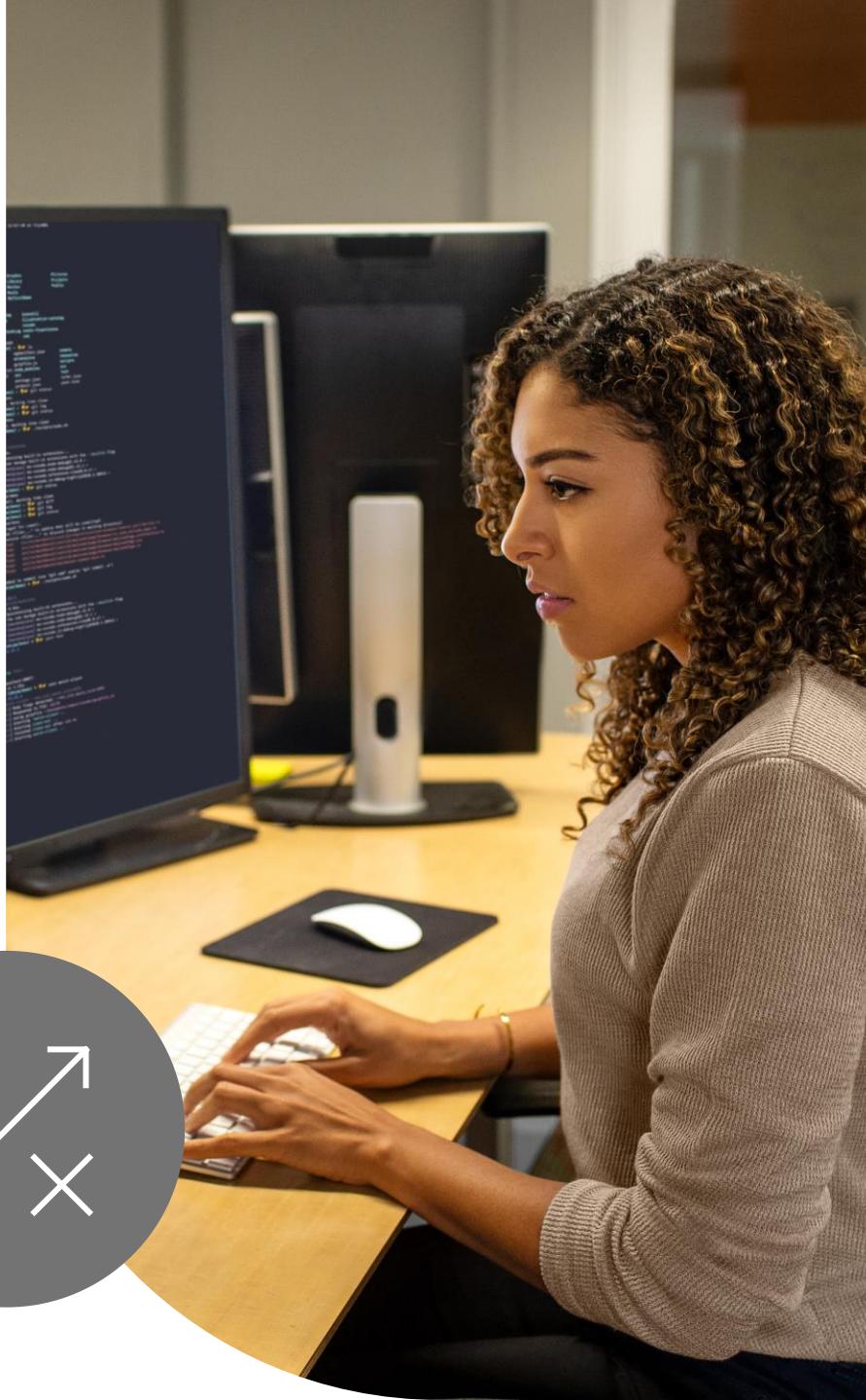
- Focus on what matters with AI that reduces false positives by 79%\*
- Easily understand the scope of an attack with incidents that automatically map related entities
- Integrate automation into your day-to-day operations workflow



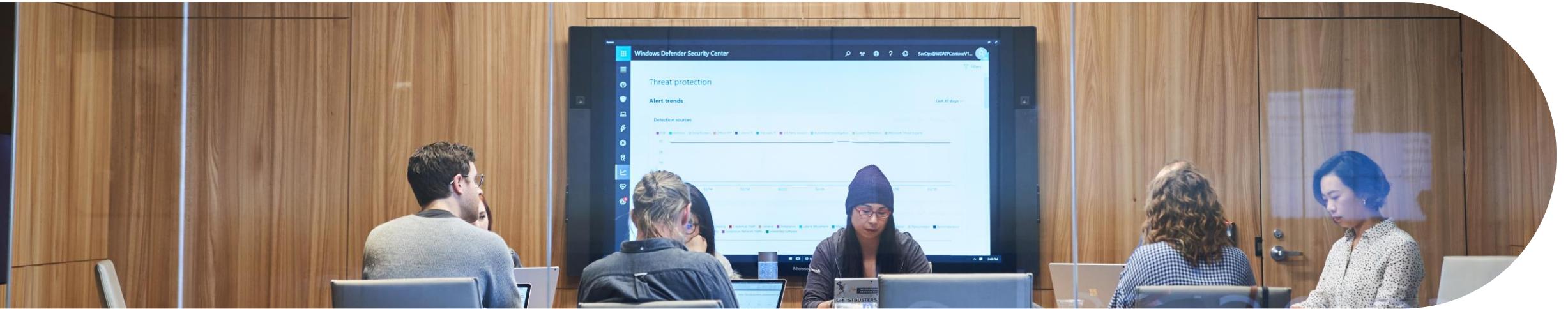
\*Forrester Consulting, Total Economic Impact™ of Microsoft Sentinel, 2020

# 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**



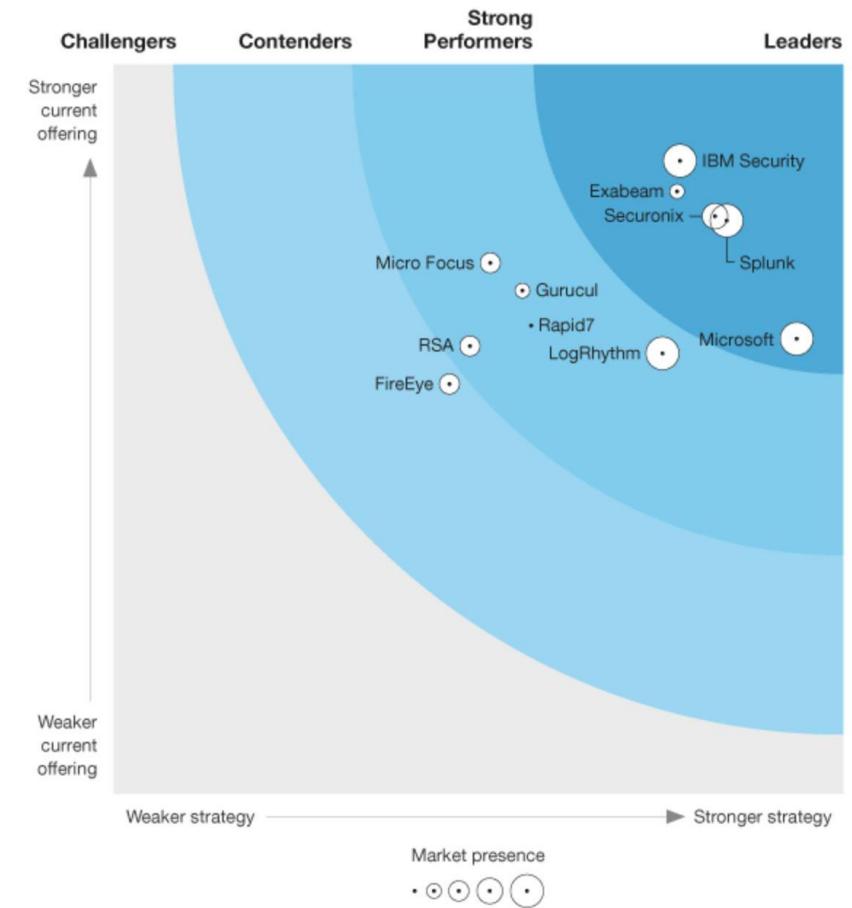
## Microsoft Sentinel—a Leader in the Forrester Wave™: Security Analytics Platform

**"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

THE FORRESTER WAVE™  
Security Analytics Platforms  
Q4 2020



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



**"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



# 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

---

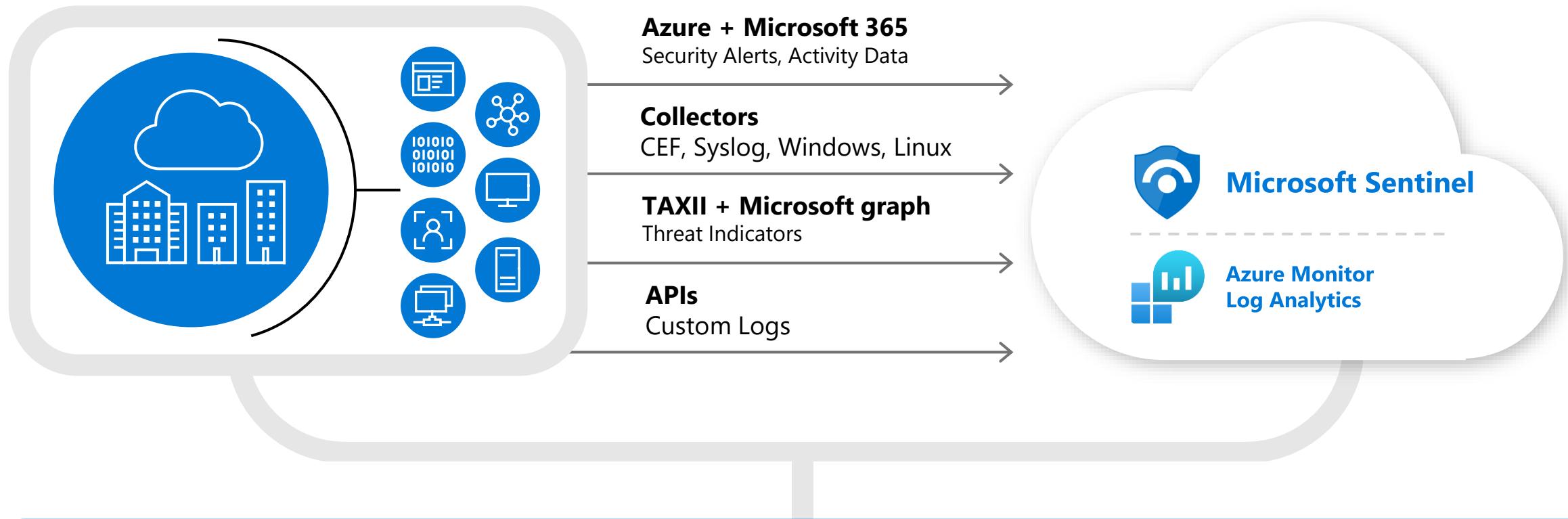
Collect data from Azure, other clouds,  
and on-prem

---

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**



Google Cloud Platform



**Carbon Black.**



**Symantec**



**McAfee**



**paloalto<sup>®</sup>  
NETWORKS**

**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



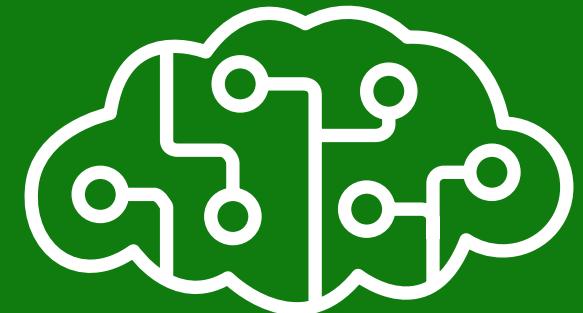
# Analytics

Detect threats with machine learning (ML)  
and advanced analytics

Reduce false positives by 78%\*

ML trained by trillions of signals daily

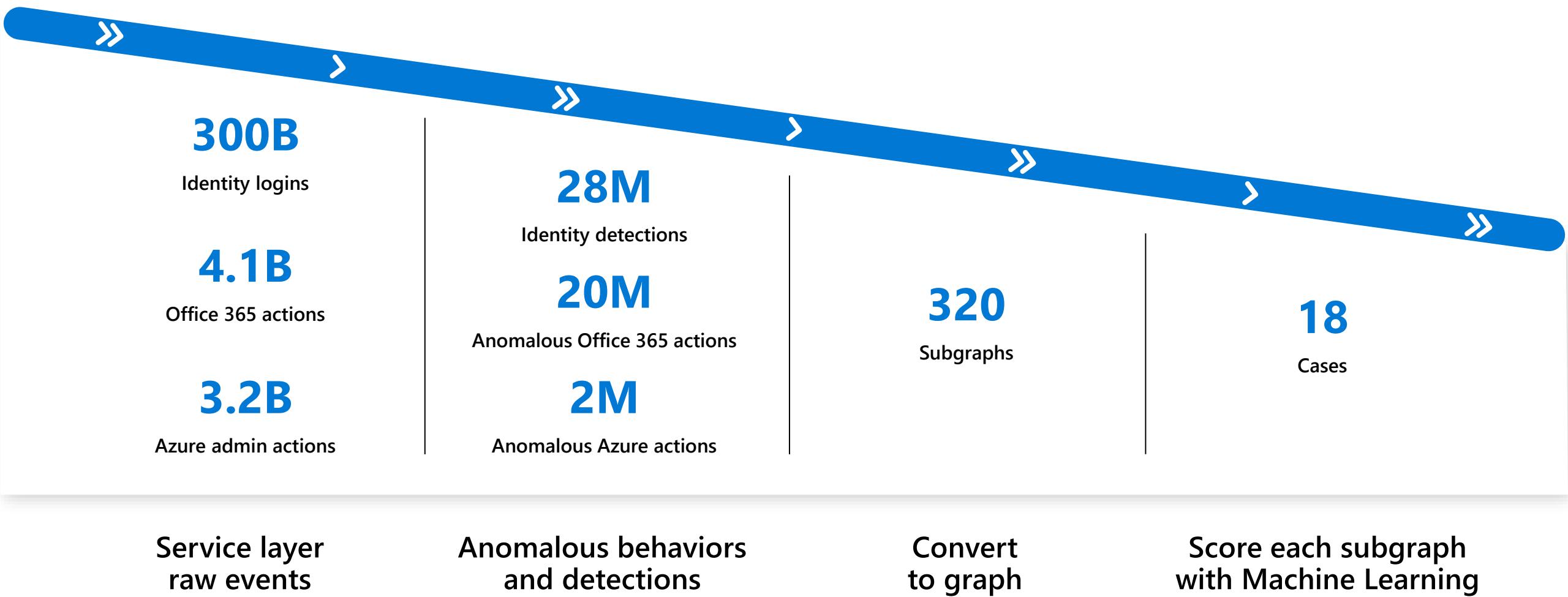
Built-in UEBA



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

# Reducing alert fatigue

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



# 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

The screenshot shows the Microsoft Defender XDR interface. At the top, there's a navigation bar with 'Create' and 'Refresh' buttons, and a search bar. Below it is a 'RULES BY SEVERITY' chart with 51 active rules: 12 High, 26 Medium, 9 Low, and 4 Informational. A 'Known Phosphorus group domains' rule is highlighted. The main pane displays a table of rules with columns: NAME, RULE TYPE, REQUIRED DATA SOURCES, and TACTICS. The 'NAME' column lists various detection templates like 'Known Phosphorus group domains', 'Advanced Multistage Attack...', etc. The 'TACTICS' column shows categories like Command and Control, Exfiltration, Execution, Initial Access, Credential Access, and Syslog. To the right of the table, there are sections for 'Required data sources' (listing DNS (Preview), DnsEvents, VMConnection, Cisco ASA, CommonSecurityLog, Palo Alto Networks, and CommonSecurityLog), 'Tactics' (Command and Control), and a 'Rule query' editor containing KQL code. The code in the editor is:

```
let timeframe = 1d;
let DomainNames = dynamic(["yahoo-verification.org","accounts-web-mail.com","customer-certificate.com","se-yahoo-verification.net","yahoo-verify.net","outlook-v
```

At the bottom right, there's a 'Create rule' button.

# 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

The screenshot shows the Microsoft Azure (Preview) interface for Azure Sentinel. The main title is "User Entity Behavior Analytics - CyberSecuritySoc". Below it, there's a table showing "Incidents Breakdown" for three users: cboehmsa, sridper@microsoft.com, and aatpservice. Each user has 0 incidents. To the right of the table, there are email addresses and corresponding user IDs. Below the table, a message says "The query returned no results." Further down, there's a section titled "Anomalies Breakdown: Jeff@seccxp.ninja" with various filters like "Anomaly Name: All", "Tactic: All", etc. At the bottom, there's a table of "Mitre Tactic Information" with columns for TimeGenerated, AnomalyName, Tactic, Technique, SubTechnique, Description, UserName, and UserP. Several rows of data are listed, each with a link to "Click on one of the anomalies to...".

TimeGenerated	AnomalyName	Tactic	Technique	SubTechnique	Description	UserName	UserP
8/16/2020, 8:44:35 PM	Anomalous Geo Location Logon	Initial Access	Brute Force	Password Guessing	Adversaries may steal the credentials of a specific user or se	Jeff	Jeff@sec
8/16/2020, 8:53:21 PM	Anomalous Account Creation	Persistence	Create Account		Adversaries may create a cloud account to maintain access	Jeff	Jeff@sec
8/16/2020, 8:55:19 PM	Anomalous Role Assignment	Persistence	Account Manipulation		Adversaries may manipulate accounts to maintain access to	Jeff	Jeff@sec
8/17/2020, 14:27:08 PM	Anomalous Login to Device	Lateral Movement	Valid Accounts		Adversaries may steal the credentials of a specific user or se	Jeff	Jeff@sec
8/17/2020, 14:34:48 PM	Anomalous Resource Access	Lateral Movement	Remote Services	Remote Desktop Protocol	Adversary may be trying to move through the environment	Jeff	Jeff@sec

# 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

The screenshot displays the Microsoft Threat Hunting interface. At the top, there are navigation links: Refresh, Last 24 hours, New Query, and Run all queries. Below this, a summary bar shows 93 Total Queries, 2 My Bookmarks, and 1 Live Stream Results. A MITRE ATT&CK " icon is also present.

The main area is divided into three tabs: Queries, Live Stream (Preview), and Bookmarks. The Queries tab is selected, showing a table of built-in hunting queries. The table includes columns for Query, Provider, Data Source, Results, and Tactics. Each query row has a star icon, a description, and three small icons representing different data sources.

On the right side, a detailed view of a specific query is shown. The query is titled "Suspicious network traffic p" and is categorized under "Custom Queries". It has 0 results. The details pane includes sections for Description, Created time (11/1/2019), Created by (sender@microsoft.com), and Query. The Query section contains a text input field and a "Run Query" button. Below the query details, there are sections for Entities (IP, Account, Host) and Tactics (Initial Access, Credential Access, Persistence, etc.). A note states: "The initial access tactic represents the first step in a threat actor's attack cycle, often used to gain initial access to a system or network." There are also "View query results >" and "View Results" buttons.

# 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, ...

The screenshot shows the Azure Sentinel Notebooks interface. On the left, there's a sidebar with navigation links: General, Overview, Logs, News & guides, Threat management (Incidents, Workbooks, Hunting, Notebooks), Configuration (Data connectors, Analytics, Playbooks, Community, Settings). The 'Notebooks' link under Threat management is highlighted. The main area displays a list of 13 total notebooks, each with a thumbnail, name, provider (Microsoft), last update time, status (Hunting or Investigation), and a description. A detailed description for the first notebook, 'Entity Explorer - Account', is shown on the right, listing utilized data types like SecurityEvent, SecurityAlert, AzureNetworkAnalytics\_CL, Heartbeat, OfficeActivity, and AAD, along with their last update times. At the bottom right, there's a 'Launch Notebook (Preview)' button.

Notebook name	Provider	Last version update	Status	Description
Entity Explorer - Account	Microsoft	06/02/20, 05:00 PM	Hunting	Use queries and visualizations to help you assess the security state of an AAD/O365 account or an account on a local host. It includes examining Azure Active Directory (AAD) and Office365 activity for an account and identifying any related anomalous behavior. Allows you to correlate the IP addresses in related events with threat intelligence sources.
Entity Explorer - Domain and URL	Microsoft	06/02/20, 05:00 PM	Hunting	
Entity Explorer - IP Address	Microsoft	06/02/20, 05:00 PM	Hunting	
Entity Explorer - Linux Host	Microsoft	06/02/20, 05:00 PM	Hunting	
Entity Explorer - Windows Host	Microsoft	06/02/20, 05:00 PM	Hunting	
Getting Started with Azure Sentinel Notebooks	Microsoft	06/07/20, 05:00 PM	Investigation	
Guided Hunting - Anomalous Office365 Exchange S	Microsoft	06/02/20, 05:00 PM	Hunting	
Guided Hunting – Covid-19 Themed Threats	Microsoft	05/27/20, 05:00 PM	Hunting	
Guided Investigation - Anomaly Lookup	Microsoft	10/27/19, 05:00 PM	Investigation	
Guided Investigation - Process Alerts	Microsoft	06/02/20, 05:00 PM	Investigation	
Guided Investigation – Alert Triage	Microsoft	05/27/20, 05:00 PM	Investigation	
Guided Web Shell Investigation - MDATP Sentinel Ei	Microsoft	05/28/20, 05:00 PM	Generic	

# Intelligence

Fuel threat detection and hunting  
with advanced threat intelligence

---

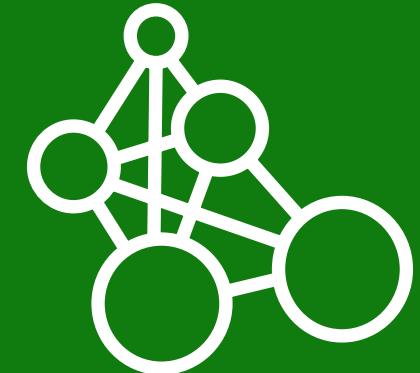
Unify management of TI from any source

---

Integrate insights with watchlists

---

Get entity insights with UEBA profiles



# Monitor and manage threat intelligence

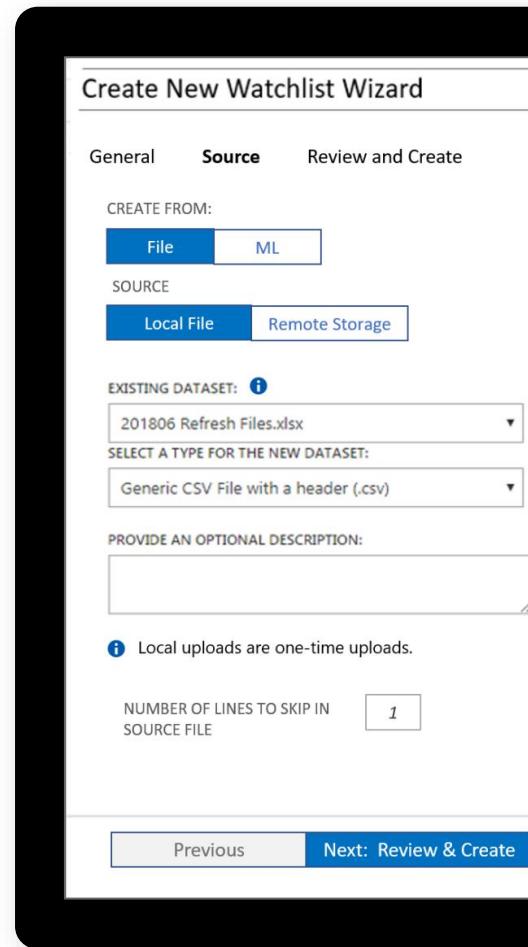
- Create, view, search, filter, sort, and tag all your threat indicators in a single pane
- Use alert metrics to help understand top threats targeting your organization
- Use automation playbooks for leading threat intelligence providers to enrich alerts

The screenshot displays a user interface for managing threat intelligence. At the top, there are three summary statistics: 12.8K TI alerts, 257.1K TI indicators, and 9 TI sources. Below this, a section titled "Indicators" shows a table of threat indicators. The table includes columns for Name, Values, Types, Source, and Confidence. The "Values" column contains URLs and IP addresses, while the "Types" column includes "url", "domain-name", and "ipv4-addr". The "Source" column lists Azure Sentinel and SecurityGraph, with confidence scores ranging from 60 to 100. The "Name" column is sorted by confidence.

Name ↑↓	Values	Types	Source ↑↓	Confidence ↑↓
IoC - https://www.bankofnedraska...	https://www.bankofnedraska.com/tag?u...	url	Azure Sentinel	100
IoC - www.hostpr.co	www.hostpr.co	domain-name	Azure Sentinel	85
IoC - 131.45.33.10	131.45.33.10	ipv4-addr	Azure Sentinel	60
Custom Threat Intelligence	4EA2A2BFE0AC522DA152D481E34E4FA5...	file	SecurityGraph	100
Custom Threat Intelligence	59AE1D57C6199629A77C117B7EF05B7C...	file	SecurityGraph	100
Custom Threat Intelligence	1304620C3EBD23A48DA15D7DBE9639D...	file	SecurityGraph	100
Custom Threat Intelligence	658A2C2D9F76EF0FC43A4BB8E28427B6...	file	SecurityGraph	100
Custom Threat Intelligence	8DE4B273D61AAA7ED76CDE3E1708E2C...	file	SecurityGraph	100
Custom Threat Intelligence	4118BFE7CAC599CB88694AF49C34BBD8...	file	SecurityGraph	100
Custom Threat Intelligence	E4E759221D3E2DAE9DFC34938576AE38...	file	SecurityGraph	100
Custom Threat Intelligence	58A4D8FAE553F59DB84CC35C2A0AE50...	file	SecurityGraph	100
Custom Threat Intelligence	A0573D5FB7972A01C65F9A76A3D98F0E...	file	SecurityGraph	100
Custom Threat Intelligence	3A51BEF83823D35CB67313FAD6C1471F...	file	SecurityGraph	100
Custom Threat Intelligence	F71AD5662CA18FAFC7DF09F989F99038...	file	SecurityGraph	100

# Use Watchlists to integrate business insights

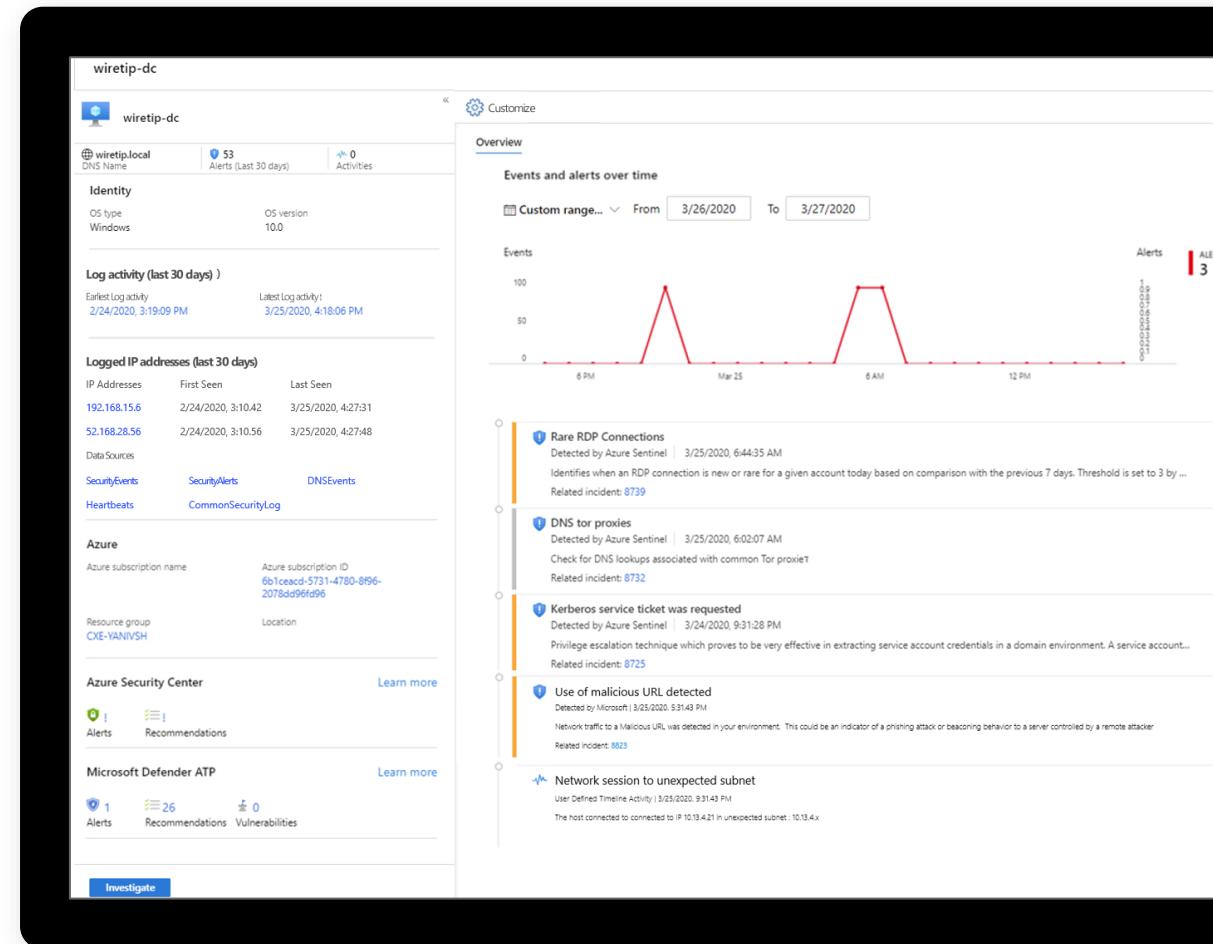
- Create collections of data for threat hunting and detection (e.g. restricted IPs, trusted systems, critical assets, risky users, vulnerable hosts)
- Incorporate watchlists into analytic rules, hunting queries, workbooks, and more—create allow/deny lists, add context, and add enrichments
- Upload a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



TimeGenerated	Account	AccountType
2020-05-05T00:43:48.653Z	\RSIEGEL	User
2020-05-05T00:43:49.197Z	\ADMINISTRATOR	User
2020-05-05T00:43:49.843Z	\VPNALLEN	User
2020-05-05T00:43:49.967Z	\ADMINISTRATOR	User
2020-05-05T00:43:50.043Z	\ADMINISTRATOR	User
2020-05-05T00:43:50.123Z	\ADMIN	User
2020-05-05T00:43:50.417Z	\ADMINISTRATOR	User
2020-05-05T00:43:50.747Z	\ADMINISTRATOR	User
2020-05-05T00:43:51.313Z	\ADMIN	User
2020-05-05T00:43:51.442Z	\STATIX	User
2020-05-05T00:43:51.443Z	\ADMINISTRATOR	User
2020-05-05T00:43:51.443Z	\ADMINISTRATOR	User

# 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

The screenshot shows a digital tablet displaying a security incident management application. The top navigation bar includes 'Refresh', 'Last 24 hours', and 'Actions' buttons. Key statistics are shown: 42 OPEN INCIDENTS, 42 NEW INCIDENTS, and 0 IN PROGRESS. A color-coded legend titled 'Open Incidents By Severity' shows the distribution across Critical (0), High (5), Medium (28), Low (6), and Informational (3) levels. The main area displays a table of 42 incidents, each with a unique ID, title, number of alerts, product name, creation time, owner, and status. The first incident listed is 'AWS - Monitor Credential abuse or hijack'. To the right of the table, detailed information for this specific incident is shown, including its ID (1129), title, severity (High), status (New), and owner (Unassigned). It also provides links to the incident's details and a comment section. Below the table, there are sections for Tags, Last update time, Creation time, Close reason, Evidence, and Entities.

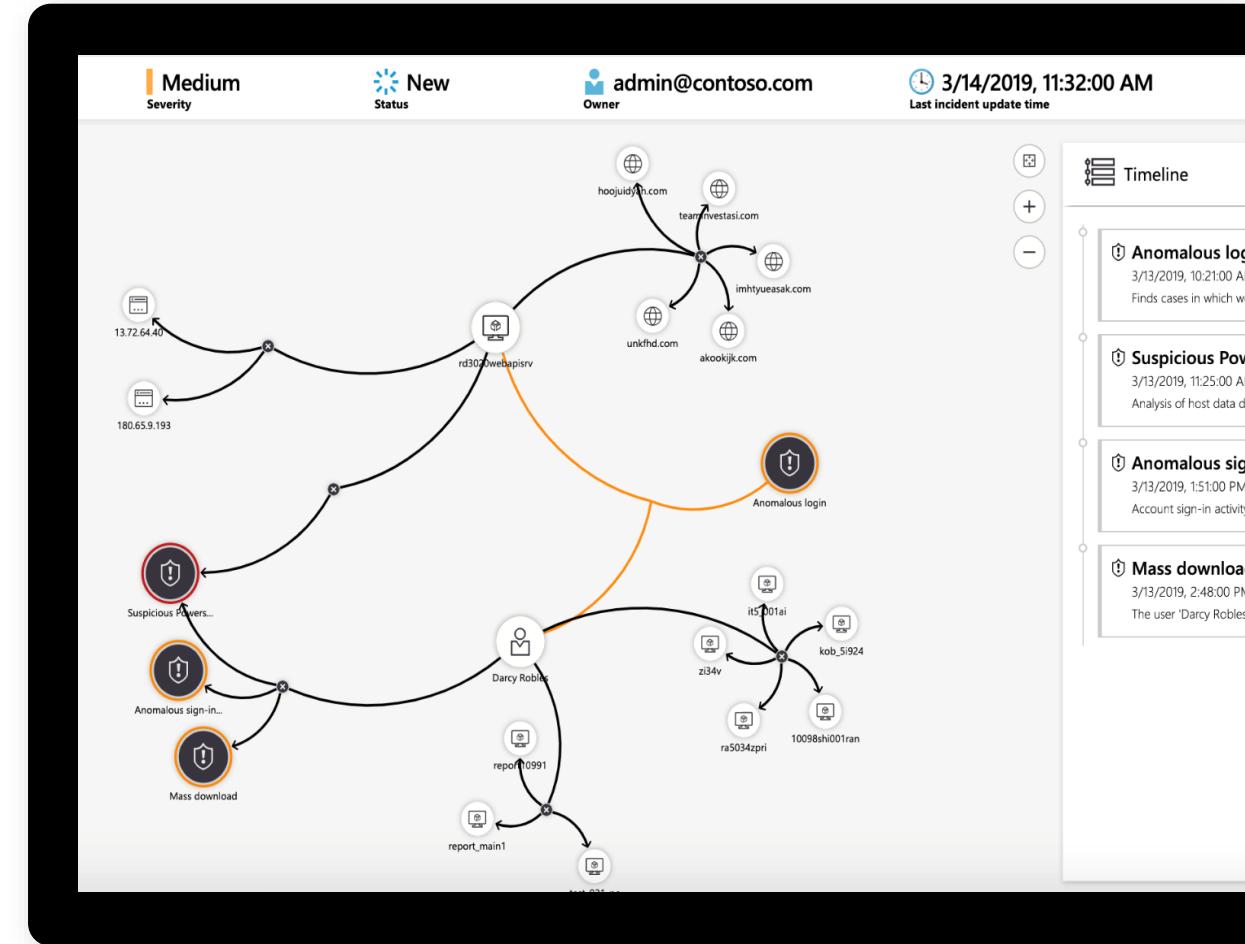
INCIDE...	TITLE	ALERTS	PROD...	CREATED TIME	OWNER	STATUS
1129	AWS - Monitor Credential a...	1	Azure Se...	10/09/19, 08:52...	Unassigned	New
1128	Upload to non-approved app	1	Microsoft...	10/09/19, 08:52...	Unassigned	New
1127	Activity from a Tor IP address	1	Microsoft...	10/09/19, 07:43...	Unassigned	New
1126	MeganB - top secret step-up	1	Microsoft...	10/09/19, 06:57...	Unassigned	New
1125	MeganB - top secret step-up	1	Microsoft...	10/09/19, 06:46...	Unassigned	New
1124	Base64 encoded Windows e...	1	Azure Se...	10/09/19, 06:43...	Unassigned	New
1123	MeganB - Block cut/copy a...	1	Microsoft...	10/09/19, 06:43...	Unassigned	New
1122	Traffic to known bad IPs	1	Azure Se...	10/09/19, 06:39...	Unassigned	New
1121	DNS tor proxies	1	Azure Se...	10/09/19, 06:38...	Unassigned	New
1120	User Account Created and ...	1	Azure Se...	10/09/19, 06:38...	Unassigned	New
1119	System alert: DLP Connecto...	1	Microsoft...	10/09/19, 06:35...	Unassigned	New
1118	MeganB - top secret step-up	1	Microsoft...	10/09/19, 04:35...	Unassigned	New
1117	ADD-To_Admin_Group	1	Microsoft...	10/09/19, 03:33...	Unassigned	New
1116	ADD-To_Admin_Group	1	Microsoft...	10/09/19, 03:33...	Unassigned	New
1115	Add user to sensitive group	1	Azure Se...	10/09/19, 03:21...	Unassigned	New
1114	Anonymous IP address	1	Azure Ac...	10/09/19, 03:10...	Unassigned	New
1113	Atypical travel	1	Azure Ac...	10/09/19, 03:06...	Unassigned	New
1112	Anonymous IP address	1	Azure Ac...	10/09/19, 03:05...	Unassigned	New

# 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

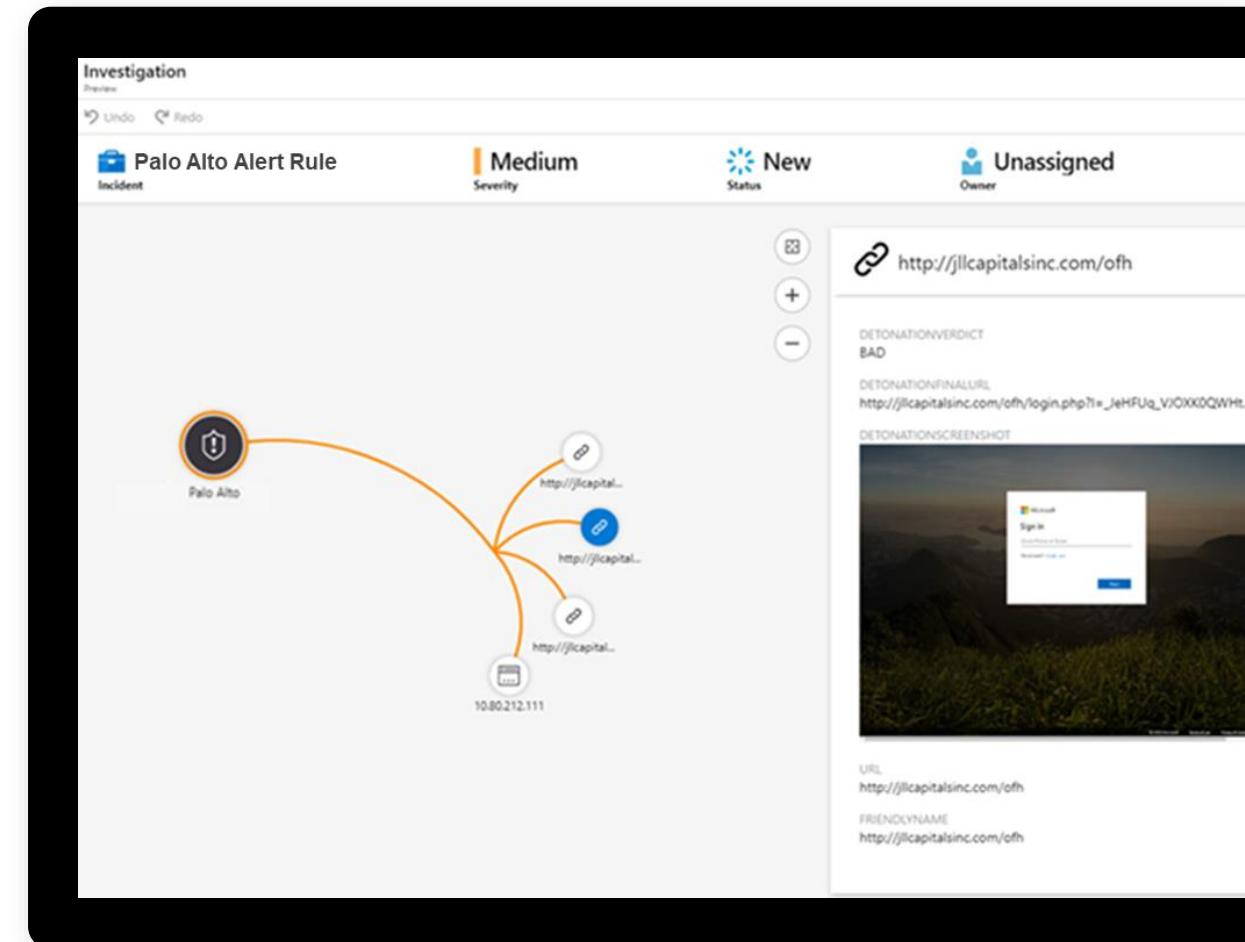
80% reduction in investigation effort compared to legacy SIEMs<sup>1</sup>

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

---

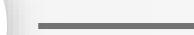
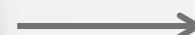
Automate your daily routines



# Respond rapidly with built-in orchestration and automation

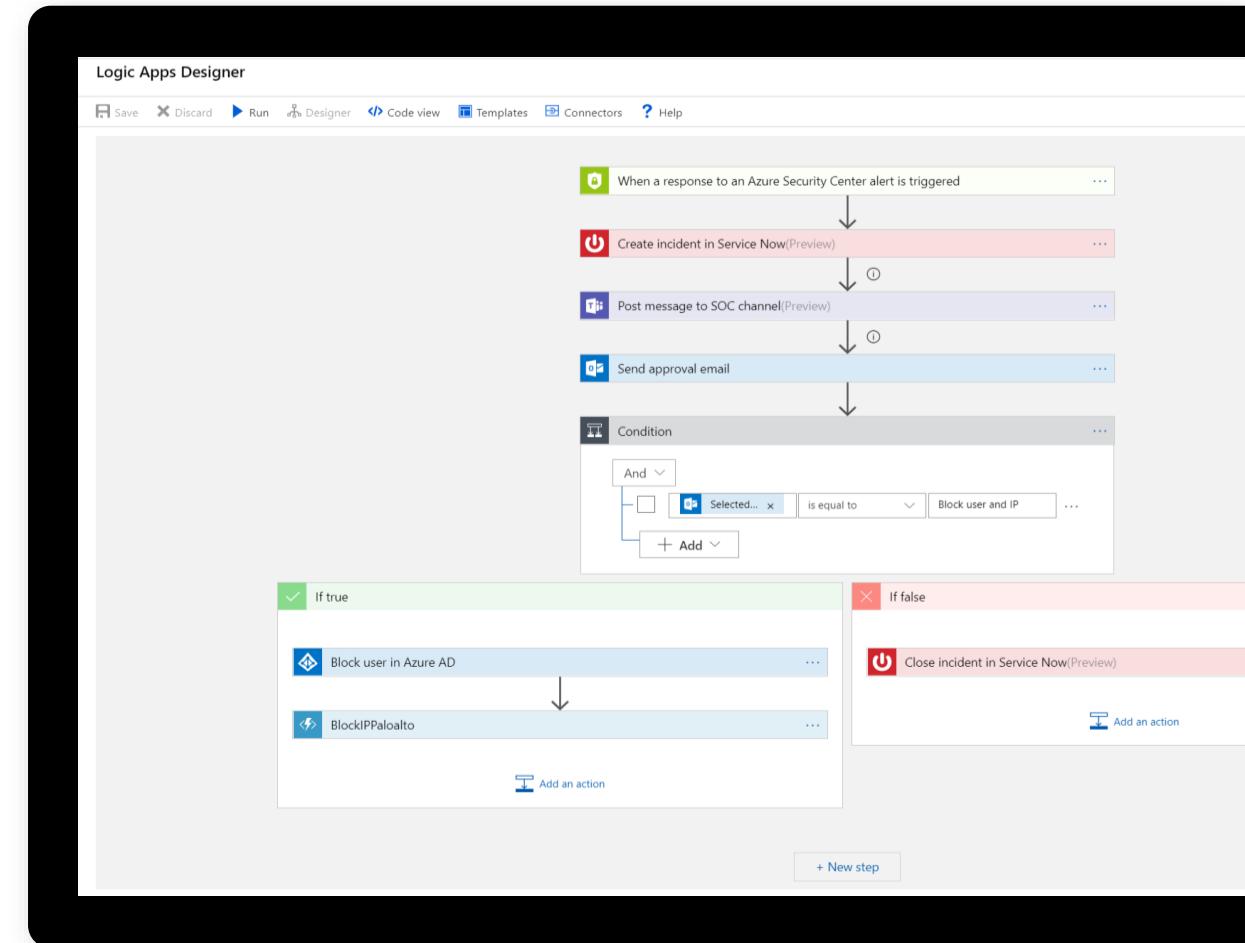


Build automated and scalable playbooks that integrate across tools



# 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



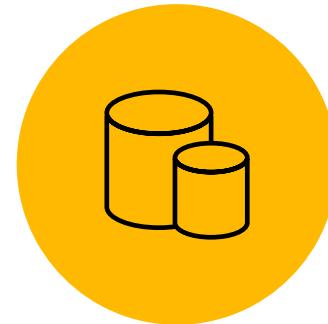
# Take actions today: Get started with Microsoft Sentinel



Start  
Microsoft Azure trial



Open Microsoft Sentinel  
dashboard in Azure portal



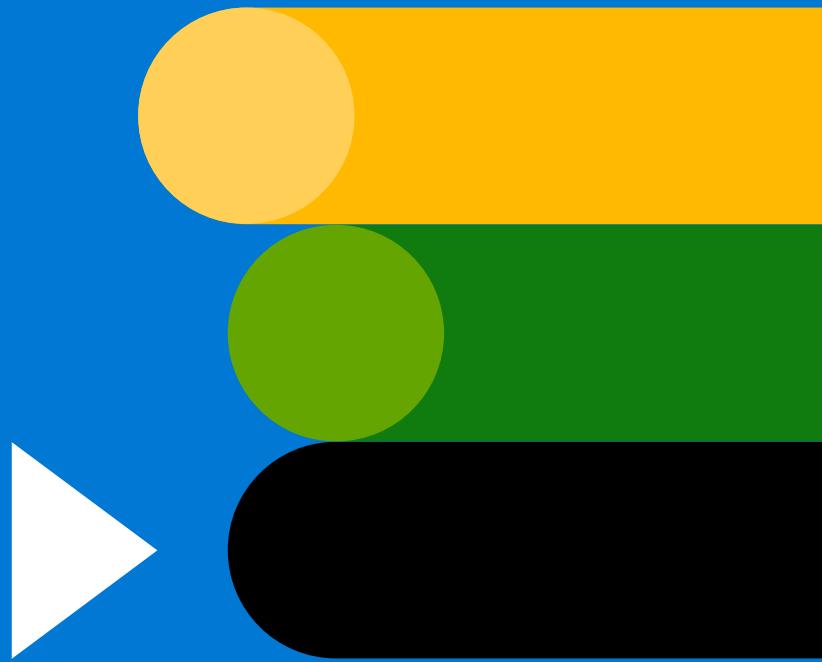
Connect  
data sources

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



# 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



**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](#)



**"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.



**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](#)



**"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.

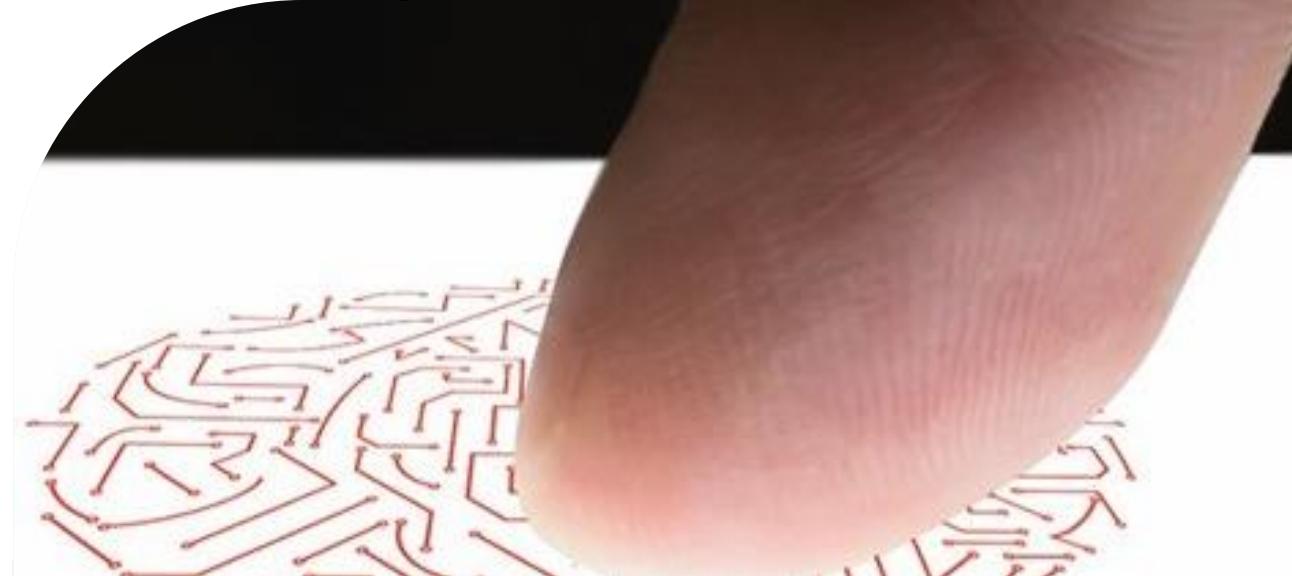
**Solution:**

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.





**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](#)

**"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.

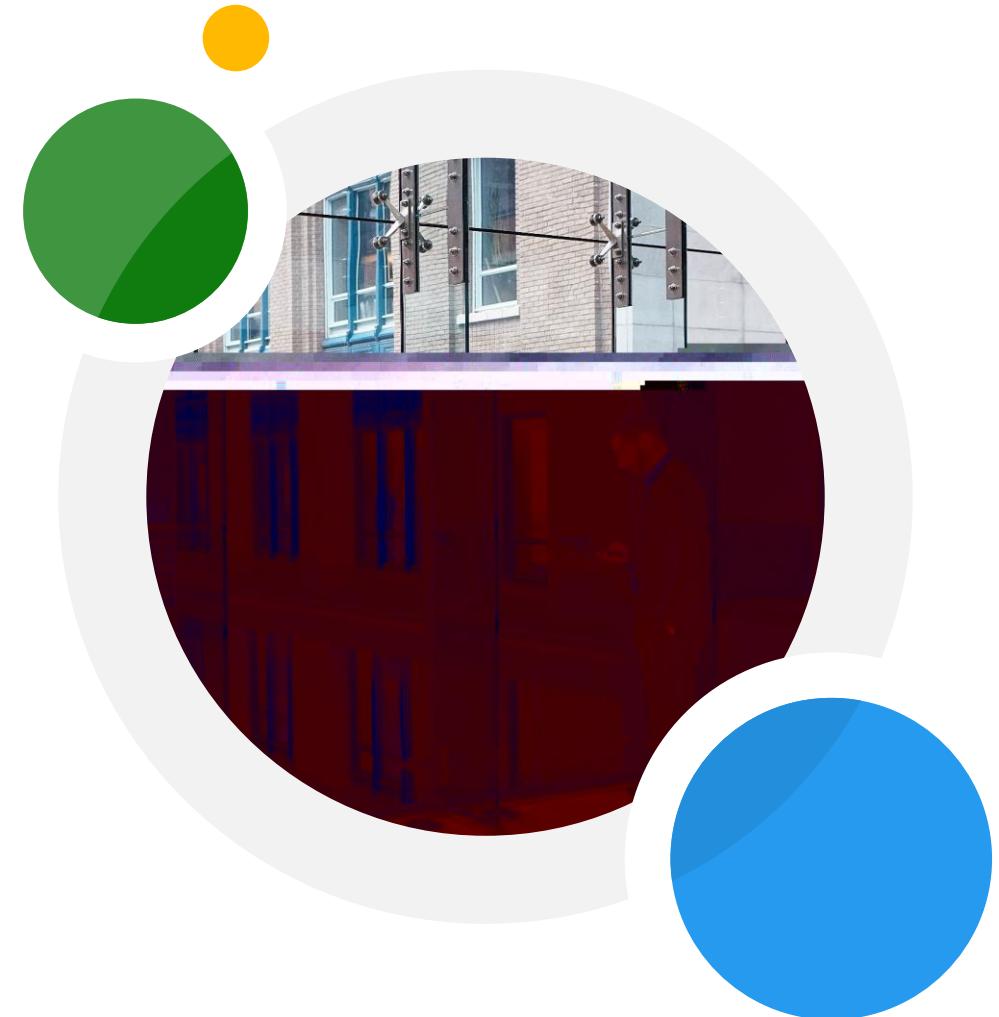
**Impact:**

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.



**"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



**"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

