



Microsoft Ignite



Microsoft Sentinel Lab

Kerinne Browne, Senior Product Manager (Federal)
Beth Bischoff, Global Black Belt

Your enhanced security team

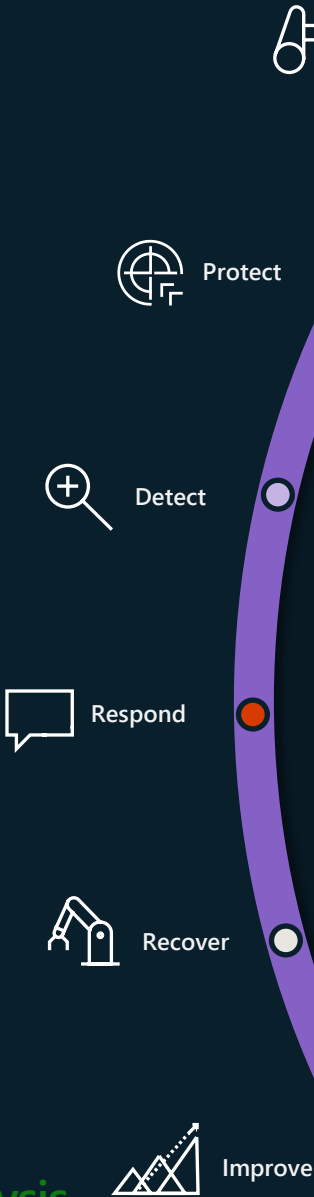




Start Secure
Stay Secure



CNAPP & Attack Path Analysis
Attack Disruption with Defender XDR
Microsoft Security Experts



Train



Protect



Detect



Respond



Recover



Improve

Microsoft Defender for Cloud

Secure your infrastructure

MULTI-CLOUD COVERAGE



Microsoft Defender for Cloud
Security Posture Management

Eliminate attack paths before they are exploited



Microsoft Defender External
Attack Surface Management

See your attack surface from the POV of an adversary



Microsoft Defender for
Vulnerability Management

Reduce cybersecurity risk



Microsoft Defender for OT / IOT

Secure IoT and OT devices



Microsoft Defender Threat Intelligence

Uncover your adversaries



Microsoft Defender for IaaS / PaaS / Containers

Server VMs, SQL, Kubernetes, Network Traffic



Microsoft Defender XDR

Cutting-edge AI empowering defense experts to:
Detect multi-stage attack paths. Automatically disrupt adversaries. Stop breaches.



Microsoft 365 Defender

Secure your end users

MULTI-PLATFORM COVERAGE



Microsoft Defender Experts for XDR

Proactive threat hunting and initial response



Microsoft Defender for Endpoint

Secure endpoint devices



Microsoft Entra

SSE (Private/Public Network Access),
Verified ID, IAM, CIEM

Microsoft Defender for Identity

Identity Threat Detection & Response



Microsoft Defender for Office 365

Protection for all of Microsoft 365



Microsoft Defender for Cloud Apps

Secure access and posture for SaaS

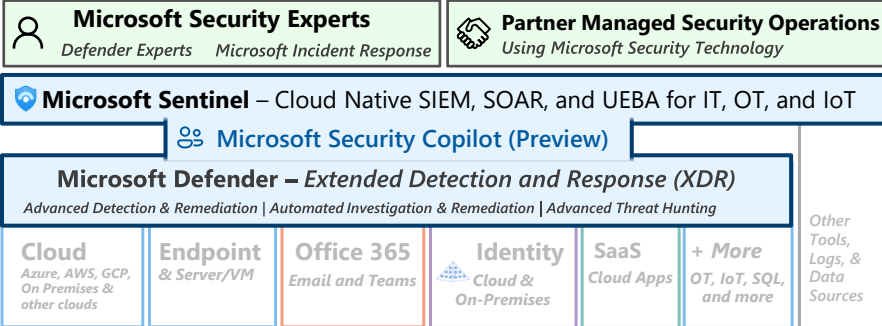
Microsoft
Security
Copilot

Microsoft Sentinel

SIEM | Threat Hunting | DFIR

Menu

Security Operations (SecOps/SOC)



Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

October 2023 – <https://aka.ms/MCRA>

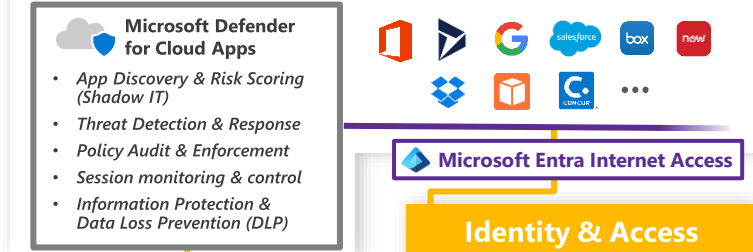
This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

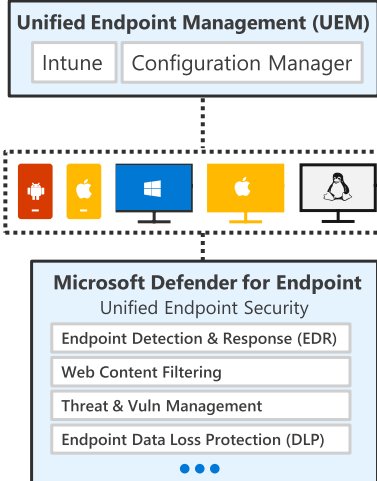
1. [Security Adoption Framework](#)
2. [Security Documentation](#)
3. Cloud Security [Benchmark](#)

Software as a Service (SaaS)

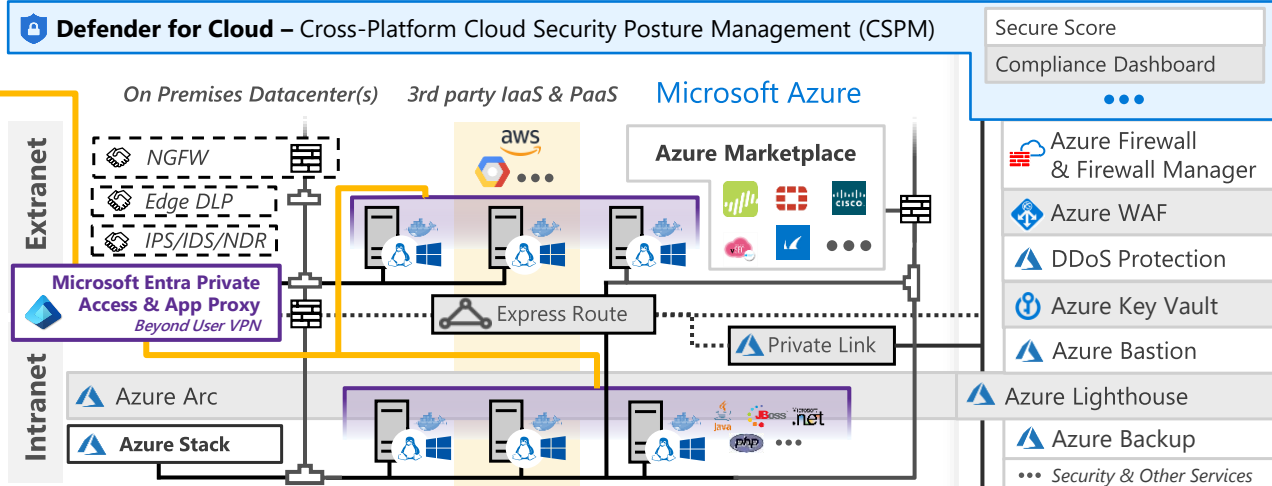


Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

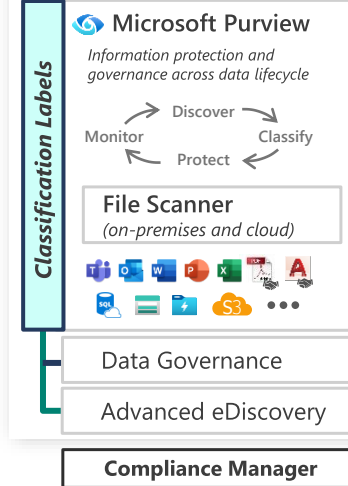
Endpoints & Devices



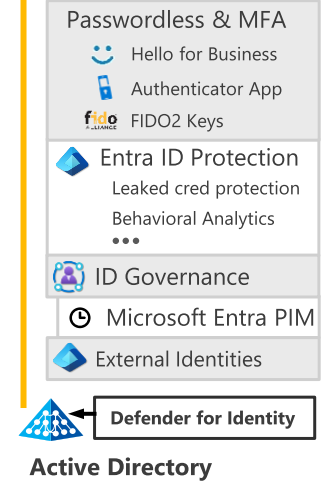
Hybrid Infrastructure – IaaS, PaaS, On-Premises



Information Protection



Microsoft Entra



Securing Privileged Access – aka.ms/SPA

Entra Permission Management – Discover and Mitigate Cloud Infrastructure Permission Creep

Privileged Access Workstations (PAWs) – Secure workstations for administrators, developers, and other sensitive users

Security Posture Management – Monitor and mitigate technical security risks using [Secure Score](#), [Compliance Score](#), [CSPM: Defender for Cloud](#), [Microsoft Defender External Attack Surface Management \(EASM\)](#) and [Vulnerability Management](#)

Windows 11 & 10 Security

Network protection
Credential protection
Full Disk Encryption
Attack surface reduction

App control
Exploit protection
Behavior monitoring
Next-generation protection

IoT and Operational Technology (OT)



Microsoft Defender for IoT (and OT)

- ICS, SCADA, OT
- Internet of Things (IoT)
- Industrial IoT (IIoT)
- Asset & Vulnerability management
- Threat Detection & Response

Defender for Cloud – Cross-Platform, Multi-Cloud XDR
Detection and response capabilities for infrastructure and development across IaaS, PaaS, and on-premises

Defender for APIs (preview)

People Security

Attack Simulator

Insider Risk Management

Communication Compliance



GitHub Advanced Security & Azure DevOps Security
Secure development and software supply chain



Threat Intelligence – 65+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

Ignite Pre-Day Cloud Security Labs

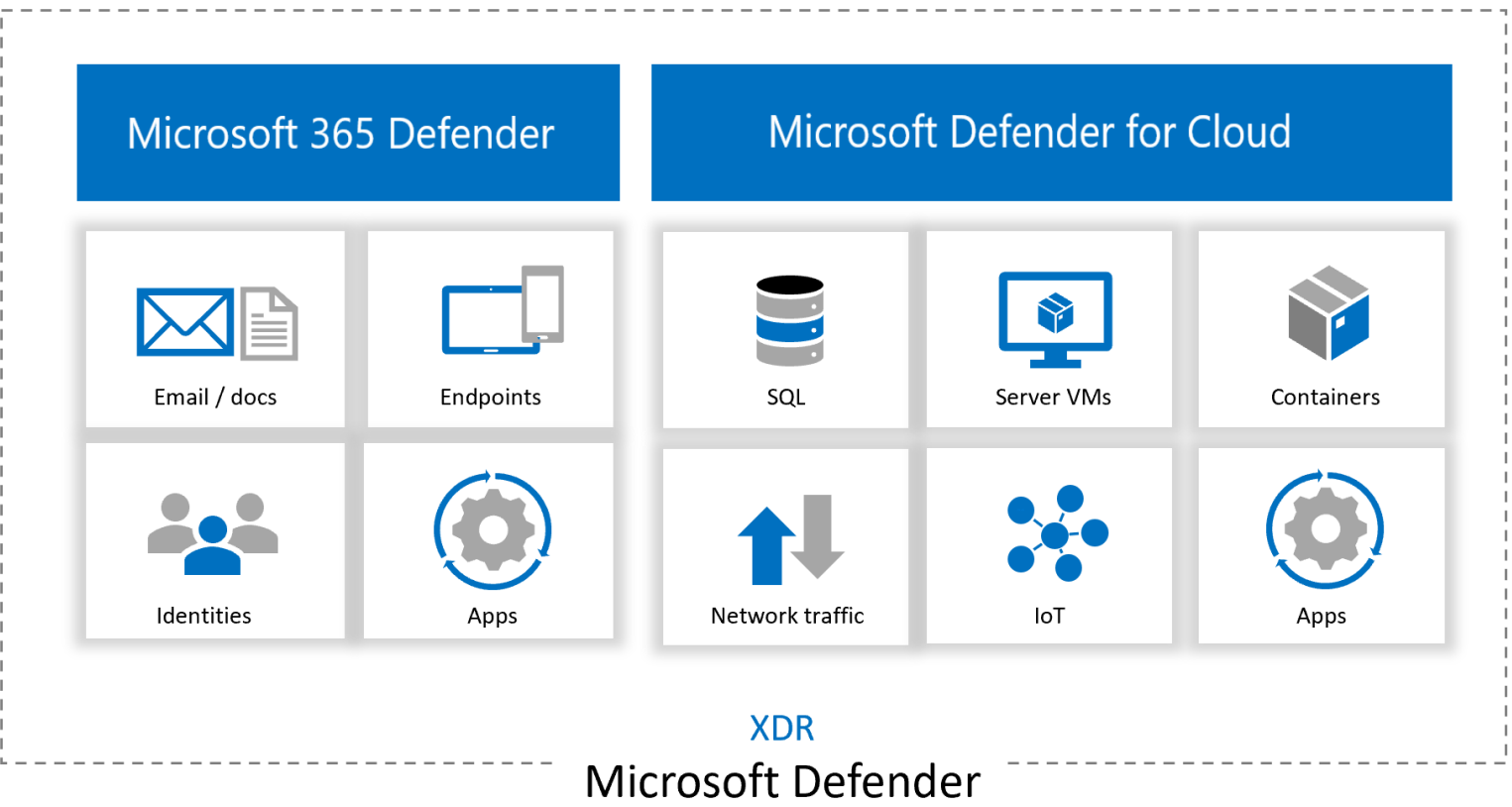
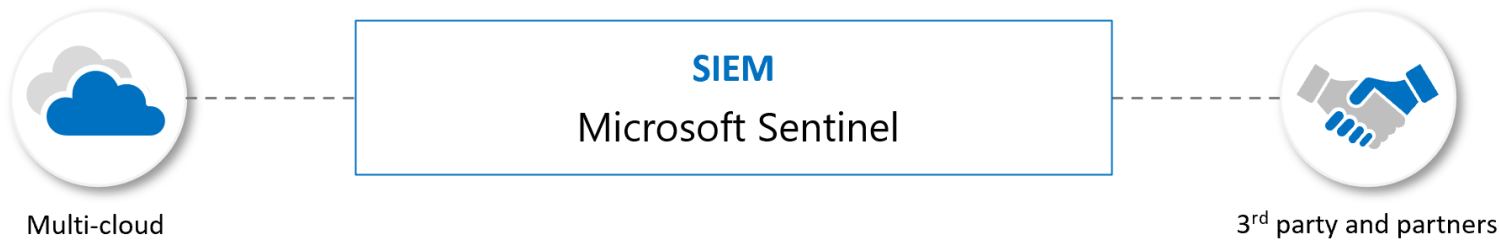
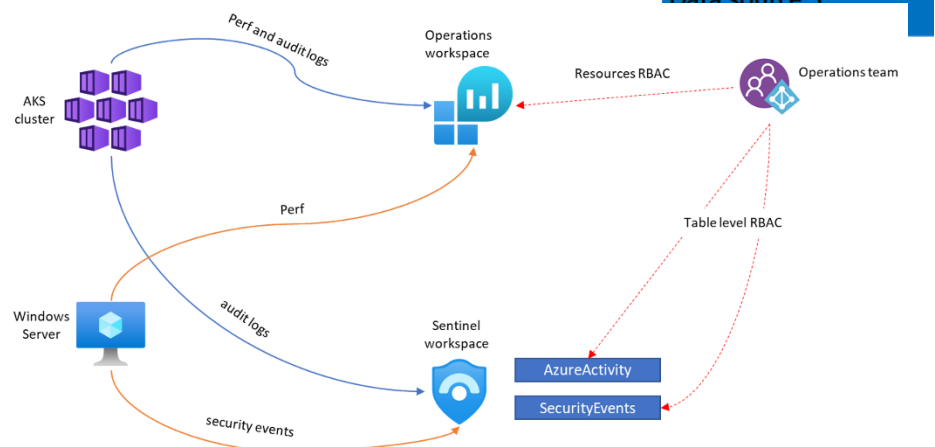
Sentinel

- [Task 1: Initialize the Microsoft Sentinel Workspace. 52](#)
- [Task 2: Configure log retention. 53](#)
- [Task 3: Connect the Microsoft Defender for Cloud data connector 54](#)
- [Task 4: Connect the Azure Activity data connector 55](#)
- [Task 5: Creating an Analytics Rule. 56](#)
- [Task 6: Explore workbook templates. 57](#)
- [Task 7: Save and Modify a workbook template. 58](#)
- [Task 8: Create a hunting query. 58](#)
- [Task 9: Access the KQL testing area. 62](#)
- [Task 10: Run Basic KQL Statements. 63](#)
- [Task 11: Analyze Results in KQL with the Summarize Operator 66](#)
- [Task 12: Create visualizations in KQL with the Render Operator 69](#)

Log Analytics and Sentinel



Defender for Servers

- 500 MB Free Ingestion/Node/Day
- **API-based** connections
- **Diagnostic Settings**
some of which are managed by Azure Policy
- **Agent-based** connections



Secure your business with easily discoverable content

Supported by...



196
Microsoft
authored
solutions

335+
Microsoft Intelligent
Security Association
offerings including
solution, SaaS, and

350+
contributing
community
members



3,000+
Out-of-the-box and
customizable
standalone content
and packaged
solutions

- › Data connectors, parsers
- › Workbooks
- › Analytic rules
- › Hunting, queries, notebooks, watchlists
- › Playbooks, Logic App connectors



Microsoft Sentinel
makes content
more powerful



- ✓ On-demand, single step installation
- ✓ Customization
- ✓ Multi-workspace management
- ✓ Normalization
- ✓ DevOps tools



Expand product coverage



Defend against a new threat



Manage a specific domain



Industry-specific needs

Microsoft Integrated XDR+SIEM

Provides more SecOps visibility with less integration burden

Direct Risk Reduction

Your Maintenance Burden

Vendor Maintenance Burden

Classic SIEM Model
AV, network, other data

Limited XDR
EDR only or EDR+

 Microsoft Security
Integrated XDR+SIEM

Investigate, Remediate, and Hunt			
Write/Update Automation (SOAR)			
Create/Maintain Email Detections			
Create/Maintain Cloud App Detections			
Create/Maintain Cloud Identity Detections			
Create/Maintain On-Prem Identity Detections			
Create/Maintain Endpoint Detections			
Create/Maintain DevOps Detections			
Create/Maintain Database Detections			
Create/Maintain Storage Detections			
Create/Maintain Container Detections			
Create/Maintain Cloud Infra Detections			
Create/Maintain IoT & OT/ICS Detections			
SIEM - Integrate Threat Intelligence		(If SIEM Present)	
SIEM - Integrate UEBA and ML		(If SIEM Present)	
SIEM - Harmonize Definitions & Semantics		(If SIEM Present)	
Ensure tools provide APIs			
Select & Implement Tools			


Microsoft 365
Defender


Defender
for Cloud


Microsoft
Sentinel

Primary Focus: Reduce Risk
by removing attacker access to resources. All other activities support this and should not distract from it.

Integrated XDR+SIEM

Simplifies SecOps and reduces wasted time by providing and maintaining:

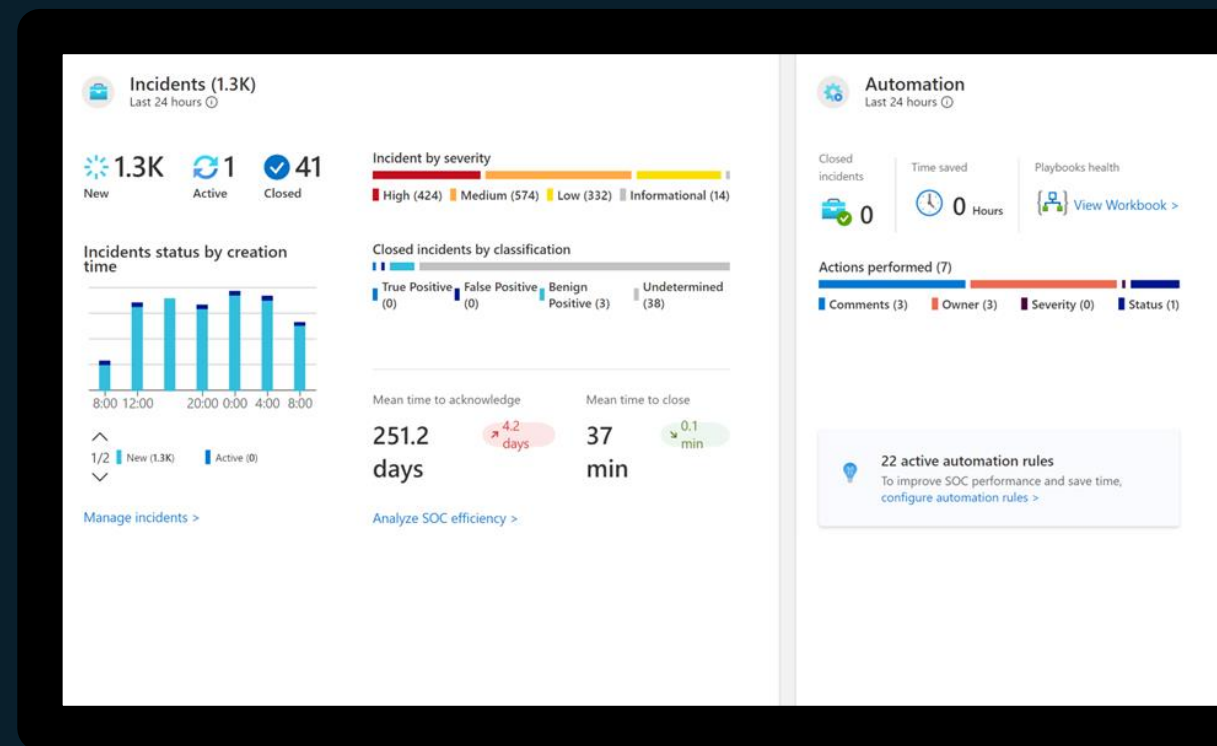
- Asset-specific detections
- Tooling integration
- Threat Intelligence integration
- MITRE ATT&CK coverage
- Additional detailed data for investigation and advanced hunting

This allows analysts to focus on *responding to incidents & reducing organizational risk*

Protect your entire digital estate

Secure more with scalable, integrated coverage for a hybrid, multi-cloud, multi-platform business

- » Extensive content including connectors, dashboards, detection rules, playbooks, and hunting queries all packaged as solutions to accelerate defense against threats
- » Integrate any security logs or tools
- » Get started on day one with more than 225 out of the box integrations that enable ingestion, enrichment, and delivery of data from multiple clouds, SaaS, CASB, endpoint, network and OT/IoT.
- » Business application threat detection, investigation and response for SAP, Dynamics and more



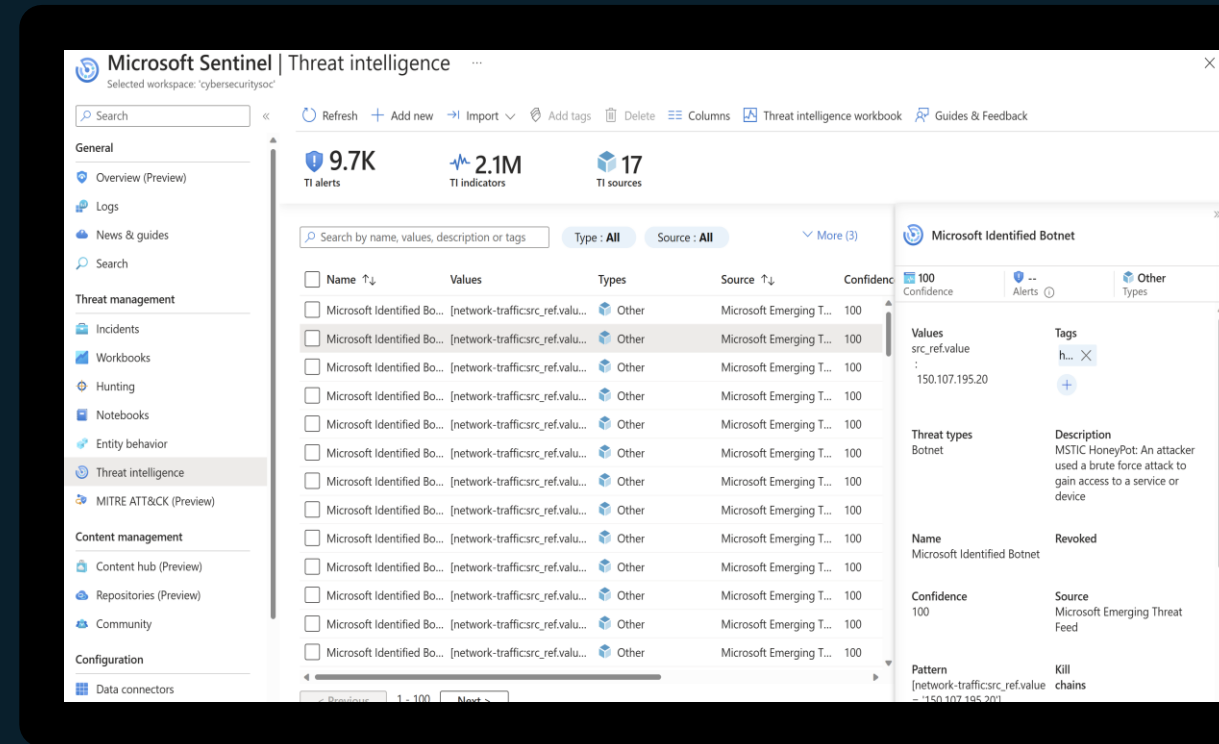
67% decrease in time to deployment with pre-built SIEM content and out-of-the box functionality¹

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

Level up with Microsoft Intelligence

Power your SecOps team with advanced AI, world-class security expertise and comprehensive threat intelligence

- » Broadly trained AI for scoring and tuning, noise reduction, guided help and recommendations based on customers-like-me insights.
- » Integrate enhanced UEBA, automation, hunting capabilities and threat intelligence (TI) into your day-to-day operations workflow to expedite investigation and response
- » Leverage fusion and build-your-own-machine-learning (BYO ML) to stay ahead of evolving attacks



Reduce false positives by 79% by correlating alerts into prioritized incidents¹

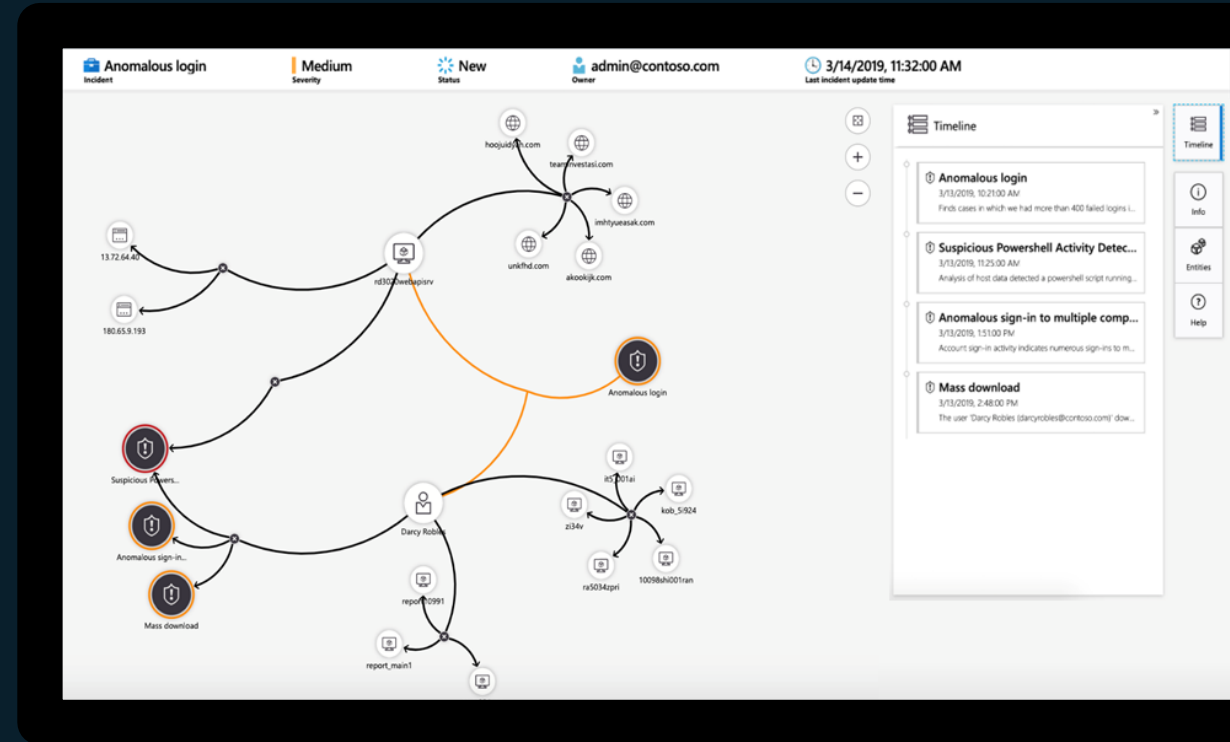
¹: [Commissioned study-The Total Economic Impact™ of Microsoft Azure Sentinel](#) conducted by Forrester Consulting, 2020

Detect and respond efficiently

Stay ahead of evolving attacks with a unified set of tools to monitor, manage and respond to incidents

- » Easily hunt for threats across all data types at cloud speed. Machine learning automatically correlates alerts into prioritized incidents, reducing noise.
- » Built in case management for SOC teams supports quick response to issues through collaboration across the organization.
- » Built-in UEBA allows for quick identification of anomalous user behavior, and industry-leading threat intelligence provides insight into bad actors across the internal and external attack surface.

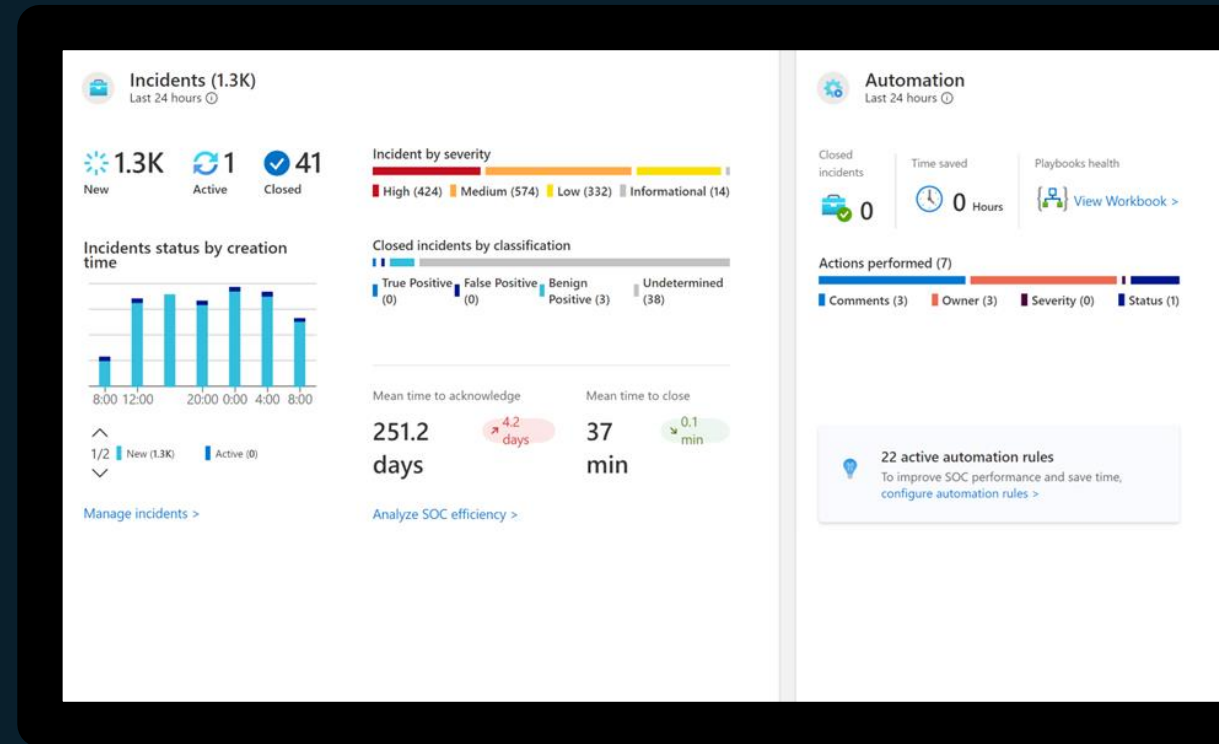
Reduce mean time to respond (MTTR) by 80% ¹



Scale your security operations

Address the growing demands of security with a solution that addresses your business' needs

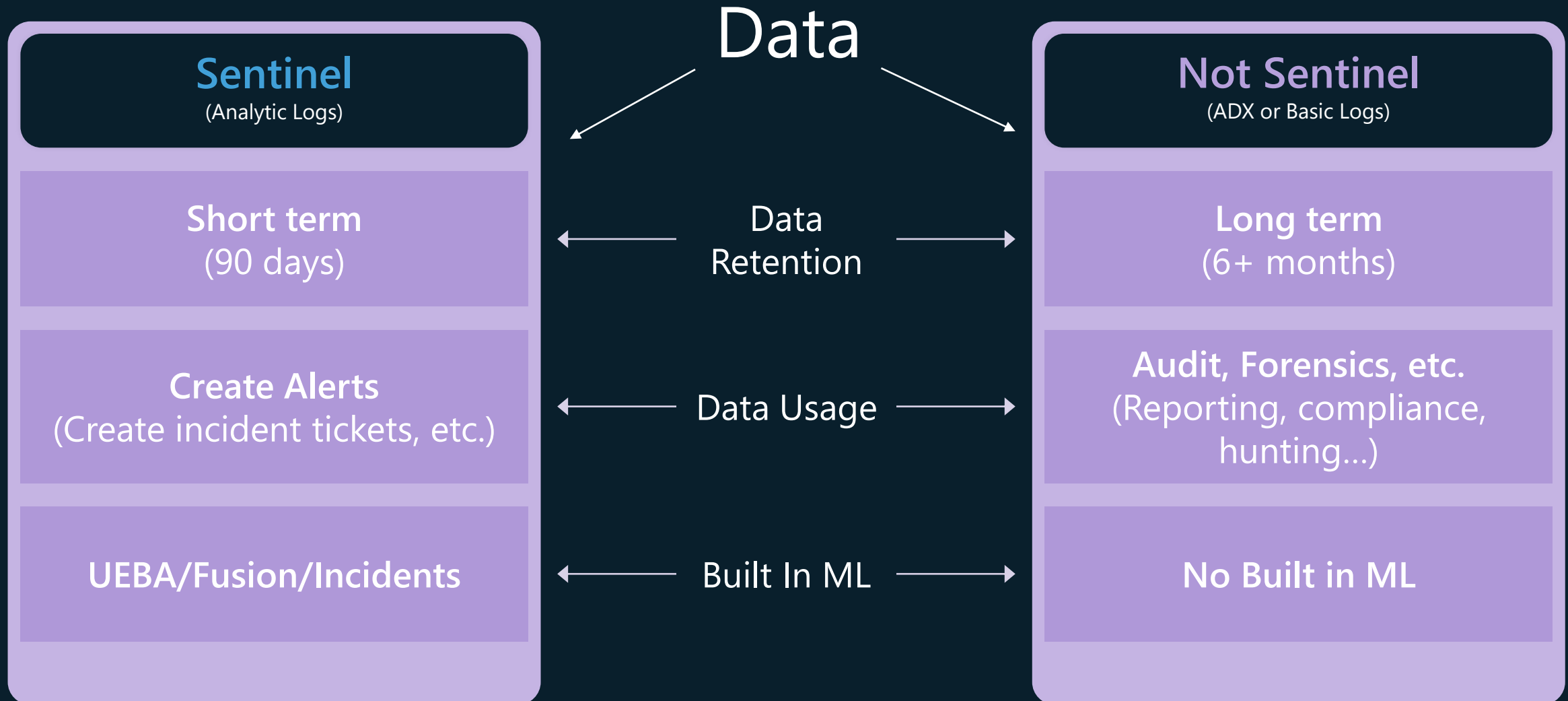
- » Eliminate infrastructure setup or maintenance
- » Put no limits to compute or storage resources and scale at will
- » Collect and analyze data across your entire organization at cloud scale with a SaaS solution
- » Spend less time integrating various security tools with a unified SecOps platform and out of the box integrations into Microsoft 365 Defender
- » Microsoft Sentinel is already field-proven with companies of all sizes, industries, MSSPs and MDPs with a community of Microsoft Security experts



Reduce costs by 48% and management efforts by 56% compared to legacy SIEMs¹

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

Data: To Sentinel or Not to Sentinel...



Flexible collecting and archiving options

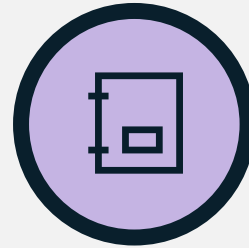
Eliminate blind spots with affordable solutions to collect, store, and analyze all your security data



Analytics logs

Security and activity logs

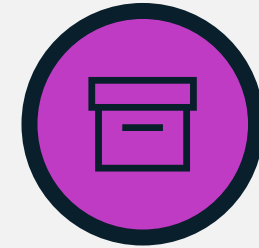
- » Used for continuous threat monitoring, near real-time detections, and behavioral analytics
- » Available for 90 days, with option to archive
- » Affordable pay-as-you-go pricing with volume discounts and predictable commitment tiers



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

Menu

Save money and reduce time to value



201%

ROI over three years¹



48%

less expensive
compared to prem SIEMs¹



56%

reduction in
management effort
for infrastructure and SIEM¹

67% decrease in time
to deployment

with pre-built SIEM content and
out-of-the box functionality¹



80%

reduction
in investigation effort¹



79%

decrease in false
positives over
three years¹



- **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**.

- Mature and feature-rich SecOps platform built on top of core SIEM capabilities with native XDR integrations
- Unparalleled integration with out-of-the-box solutions enabling value on day one. Don't spend time and money on set up.
- Microsoft Sentinel is already field-proven with companies of all sizes, industries, MSSPs and MDPs with a community of Microsoft Security experts.

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



Microsoft Defender 365 customers - save money and get more protection

Extend XDR to modern SIEM to better secure your full digital estate



Save up to \$2,200 per month
on Microsoft Sentinel for a
3,500-seat deployment¹



Discount applied automatically

Reduce response time by up to 88%² with bi-directional incident integration between SIEM and XDR
Cut infrastructure and maintenance costs while gaining the scalability and machine speed you need



Microsoft 365 E5, A5, F5, G5
customers can benefit with up
to **5MB per user/day**³ of free data
ingestion into Microsoft Sentinel

Data sources included in offer:

- » Azure Active Directory (Azure AD) sign-in and audit logs
- » Microsoft Defender for Cloud Apps shadow IT discovery logs
- » Microsoft Information Protection logs
- » Microsoft 365 Defender advanced hunting data

Get started:

<https://aka.ms/m365-sentinel-offer> >>

¹Calculation based on pay-as-you-go prices for Microsoft Sentinel and Azure Monitor Log Analytics for US East region. Exact savings will depend on benefit utilization and customer's effective price after any applicable discount

² According to The Total Economic Impact™ Of Microsoft SIEM and XDR, A Forrester Total Economic Impact™ Study Commissioned by Microsoft, August 2022

³Up to 5MB of data/per day free with Microsoft Sentinel for Microsoft 365 E5, A5, F5 and G5** or Microsoft 365 E5, A5, F5 and G5** security customers. Microsoft waives all entitlement to compensation for the services provided to you under this agreement. Microsoft intends that these services and associated terms be in compliance with applicable laws and regulations with respect to gratuitous services. It is specifically understood that all services and services deliverables provided are for the sole benefit and use of the government entity and are not provided for personal use or benefit of any individual government employee.



Benefit for Microsoft Defender for Server customers



Defender for Server P2 customers receive a 500MB per VM per day free data benefit for specific security data tables



Customers with **Defender for Servers Plan 2** enabled, get 500 MB per VM per day of free data ingestion on qualifying security data types.

Qualifying security data types:

- SecurityAlert
- SecurityBaseline
- SecurityBaselineSummary
- SecurityDetection
- SecurityEvent
- WindowsFirewall
- SysmonEvent
- ProtectionStatus
- Update and UpdateSummary

[Get started](#)



[Learn more](#)



[Menu](#)

Why is Kusto Important?

Every organization in Microsoft uses Kusto in one way or another



Parse in Query (ASIM)

Syslog

| where ProcessName == "containerd"

| where Computer == "ip-192-168-40-20"

//Parse (add)

| parse SyslogMessage with "time=\"\" Time:datetime \"\" level=\"

Level:string \" msg=\"\" Message:string \"\" id=\" Id:string

| where Level == "warning"

Cross Resource Query

```
adx("gbbsentineladx.eastus/GBBSentinelLTS").DeviceEvents
```

```
| where AccountName == "dczero$"
```

```
| join kind=leftouter
```

```
(
```

```
SecurityAlert
```

```
| where ProviderName == "MDATP"
```

```
| extend HostName_ = tostring(parse_json(Entities)[0].HostName)
```

```
)
```

```
on $left.AccountName == $right.HostName_
```

Security Copilot working with Microsoft Security



Microsoft Defender for Endpoint

Monitor devices in real-time
Detect and prevent threats
Control policy and access
Respond to incidents and hunt



Microsoft Sentinel

Manage logs
Detect advanced threats
Monitor and alert in real-time
Get compliance and reporting



Microsoft Intune

Manage device inventory
Enforce configurations and policies
Deploy and update software
Deliver conditional access

Security Copilot

- Run queries using natural language
- Prepare reports, summaries, and graphs
- Upskill teams via prompts and guidance
- Reverse engineer malware
- Enrich alerts



- Run queries using natural language
- Prepare reports, summaries, and graphs
- Upskill teams via prompts and guidance
- Reverse engineer malware
- Enrich alerts
- Enrich incidents



- Run queries using natural language
- Prepare reports, summaries, and graphs
- Upskill teams via prompts and guidance
- Reverse engineer malware
- Enrich alerts
- Enrich incidents
- Assess security posture of devices

Ignite Pre-Day Cloud Security Labs

As you walk through the lab, consider:

- 1) The XDR+ SIEM Platform is built to work together and create efficiencies on your behalf while offering extensibility.
- 2) Sentinel plus Defender creates a continuous feedback loop to empower your SecOps team to “shift left” and secure your Hybrid Estate
- 3) Costs are controllable—the ecosystem provides the options needed to mitigate unnecessary costs based on the Data, ingest and Egress and Storage
- 4) Dashboards are purpose built and customizable to your company’s individual metric driven needs
- 5) The common data platform (Kusto with KQL) empowers collaboration and ensures scale and innovation



Thank You