bluecycle

Modernize your security operations center with a Microsoft Sentinel Proof of Concept

Microsoft Security

Why chose Blue Cycle for Your Microsoft SIEM Exploration?

Hyper-focused

150+

SIEM deployments

1PB+

Daily capacity deployed since 2020

Cloud and SIEM Experience

Experience across common SIEMs and Cloud Providers, easing migration pains.

Increase ROI

40% Reduction

In daily ingest cost vs. self-serve implementation or proof of concept

44%

Reduction in total cost of operating compared to legacy solutions

Better SecOps

Detections As Code

Deploy analytics and config in Microsoft Sentinel as Code

Automate Task

With or without Security Copilot, we help teams accelerate daily Secops tasks.

blue cycle

Microsoft Sentinel Proof of Concept

Let us help you accelerate your security modernization project through our unique service offerings.

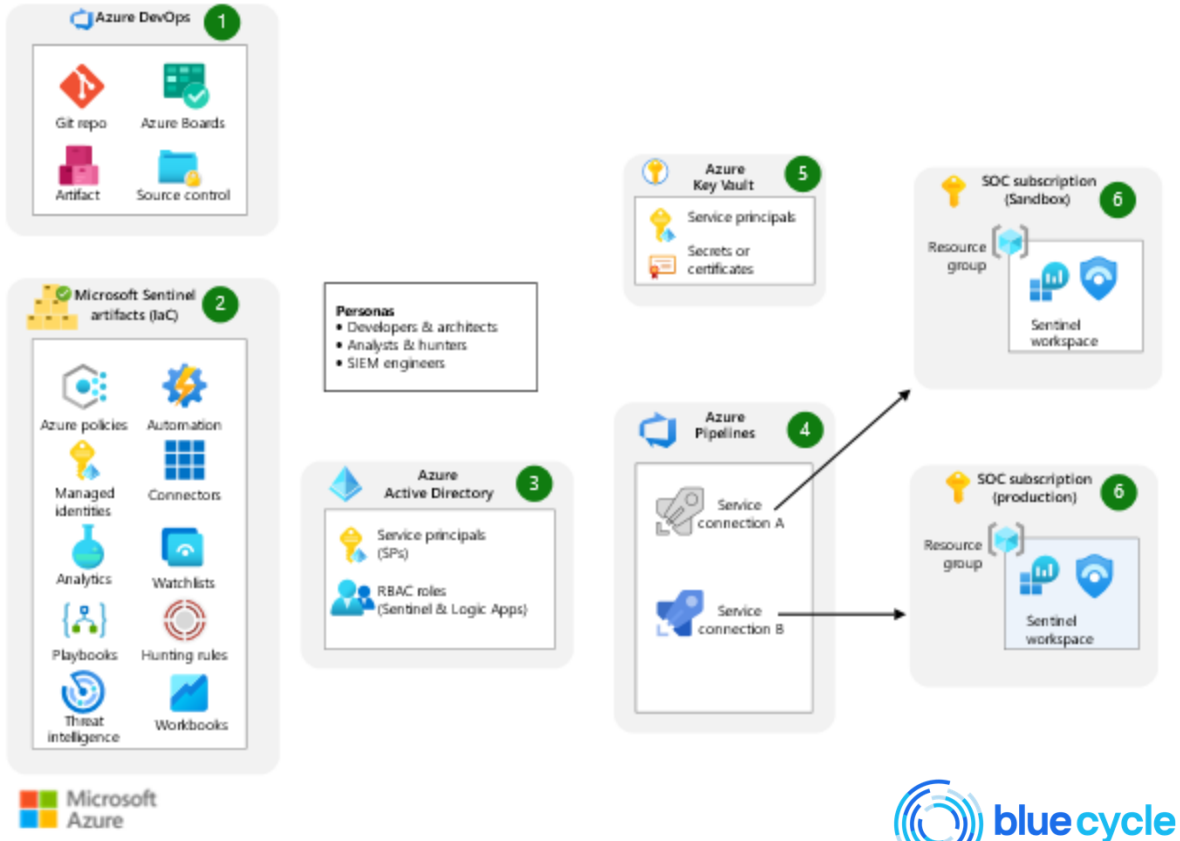
Click here to learn more

In 30 days or less:

- Connect critical data sources to understand benefits of Microsoft Sentinel
- Experience Microsoft Sentinel with your own data
- Get clarity on the investment required to adopt Microsoft Sentinel

Average Cost Savings:
40% over self serve implementation

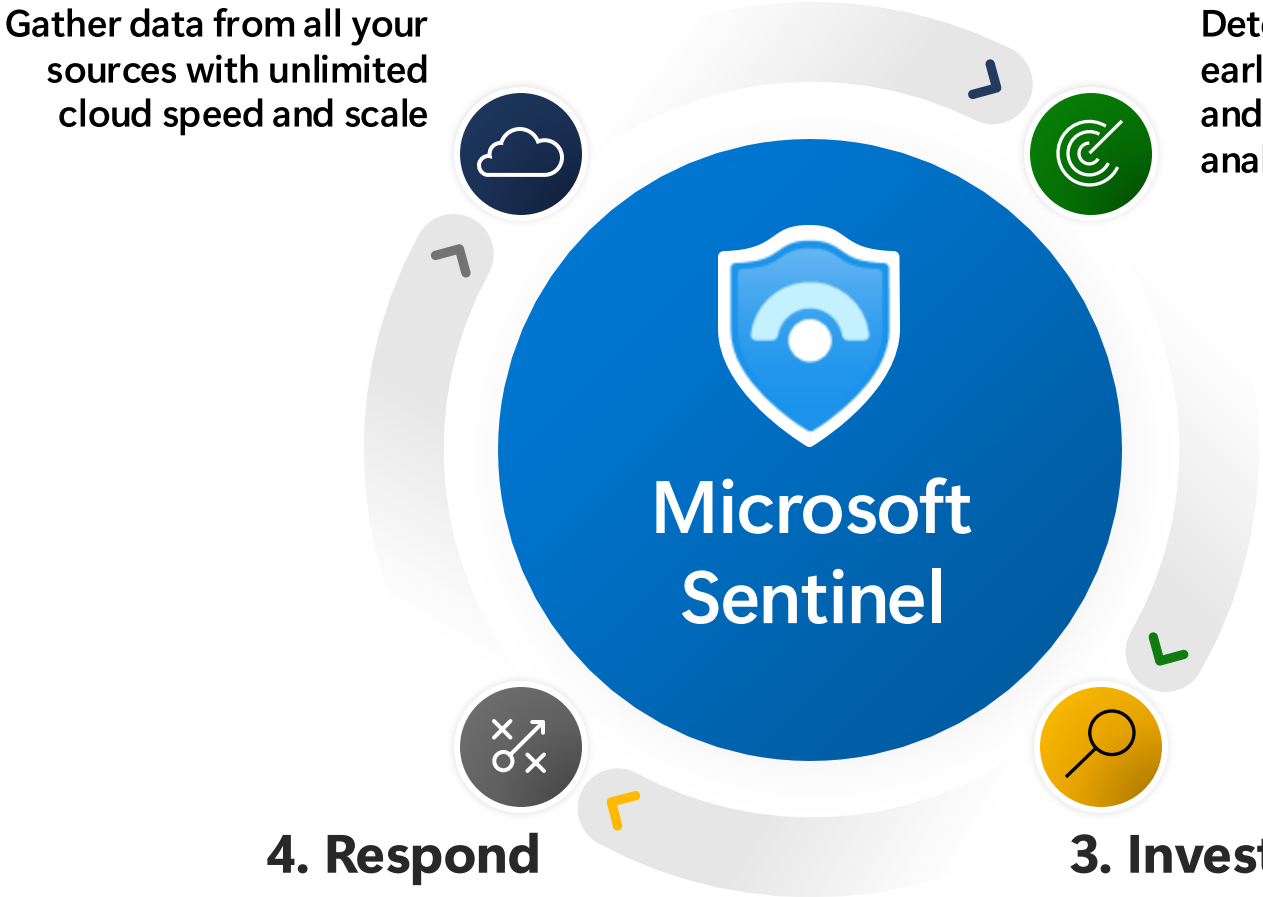
Time to Value:
30-50% quicker than self service implementation



blue cycle

Image Source: https://learn.microsoft.com/en-us/azure/architecture/example-scenario/devops/automate-sentinel-integration

Flexible protection across your multicloud, multi-platform environments



1. Collect

Gather data from all your sources with unlimited cloud speed and scale

2. Detect

Detect anomalies early with user entity and behavior analytics

3. Investigate

Correlate alerts into prioritized incidents for a full picture of attacks

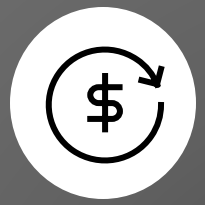
4. Respond

Respond rapidly with built-in security orchestration, automation, and response (SOAR)

Microsoft Sentinel supports the needs of a modern SOC

Protect everything

Extensible security for your entire digital estate



Increase return on investment (ROI)

Maximize value and manage costs

Move faster

Drive SOC efficiency with AI and automation

300+ out of the box connectors | 100+ MSSP marketplace offers | 200+ Content Hub partner solutions | 2100+ GitHub contributions

Application

- Apache HTTP Server
- Apache Tomcat
- Atlassian Confluence
- Box
- GitHub
- Jboss
- Microsoft Dynamics 365
- Microsoft Office 365
- Microsoft Teams
- Nginx
- Oracle Database
- Oracle WebLogic Server
- SAP
- Salesforce Service Cloud
- SIGNL4 Mobile
- Slack
- Snowflake
- SQL PaaS
- The Hive
- Workplace from Facebook
- Zoom

IoT

- Claroty
- Microsoft Defender for IoT

Information protection and data loss prevention

- Broadcom
- Cognni
- Digital Guardian
- Forcepoint
- NC Protect Data Connector
- Squadra Technologies

Cloud provider

- AWS Cloudtrail
- AWS GuardDuty
- AWS VPC Flow
- Azure Activity
- Azure DDoS Protection
- Azure Defender
- Azure Firewall
- Azure Information Protection
- Azure Key Vault
- Azure Kubernetes Service
- Azure Preview
- Azure Storage Account
- Google Apigee
- GCP Cloud Monitoring
- GCP DNS
- GCP IAM
- Google Workspace
- Microsoft Entra ID
- Oracle Cloud Infrastructure

Identity

- Cisco Duo Security
- Cisco ISE
- CyberArk
- ForgeRock
- Microsoft Defender for Identity
- Okta Single Sign-On
- OneIdentity
- PingFederate
- RSA SecurID
- 1 Password

IT operations

- AgileSec Analytics
- Atlassian Jira
- Cisco UCS
- Corelight
- Ivanti Unified Endpoint Management
- NXLog BSM macOS
- NXLog Linux
- Orca Security Alerts
- vArmour Application Controller
- VMwareESXi
- Contraforce

Networking

- Aruba ClearPass
- DNS
- Infoblox NIOS
- NXLog AIX
- NXLog DNS Logs
- Ubiquiti UniFi

Endpoint security

- Cisco Secure Endpoint
- CrowdStrike Falcon
- Microsoft Defender for Endpoint
- SentinelOne
- Sophos Endpoint Protection
- Symantec Endpoint Protection
- Trend Micro Apex One
- Trend Micro Vision One (XDR)
- VMWare Carbon Black

Network firewall

- Check Point
- Cisco ASA
- Cisco Firepower
- Cisco Meraki
- CloudFlare
- F5 Big IP
- Forcepoint
- Fortinet Fortigate
- Juniper SRX
- Palo Alto Panos
- SonicWall
- Sophos XG
- Windows Firewall

Email security

- Cisco SEG
- Proofpoint On Demand
- VMRay Email Threat Defender

Threat intelligence

- Recorded Future
- Reversing Labs
- RiskIQ Illuminate
- TitaniumCloud File Enrichment

Vulnerability management

- Beyond Security
- InsightVM CloudAPI
- Onapsis
- Qualys VM
- Tenableio

Web application firewall

- Azure Web Application Firewall
- Barracuda
- Citrix
- Impreva

Insider threat and user entity behavior analytics

- FalconFriday Content
- Microsoft Insider Risk Mangement

Network security

- Awake Security Arista Networks
- Cisco Stealthwatch
- Cisco WSA
- Citrix Analytics for Security
- F5 Networks (Data)
- FireEye Network Security
- Forescout
- IronNet Collective Defense
- Juniper IDP
- McAfee Network Security Platform
- Perimeter 81
- Pulse Connect Secure
- SquidProxy
- Symantec Proxy SG
- Symantec VIP
- Vectra
- Watchguard Firebox
- WireX Network Forensics Platform

Threat protection

- Abnormal Security
- Agari
- AIShield AI Security
- Akamai
- Alcide KAudit
- Alsid for AD
- Armorblox
- Automated Logic WebCTRL
- Better MTD
- Blackberry Cylance
- Contrast Protect
- Cyberpion
- Darktrace
- Deception Honey Tokens
- Delinea Secret Server
- Dev-0537 Detection & Hunting
- Elastic
- ESET Enterprise Inspector
- ESET PROTECT
- ExtraHop Reveal(x)
- Flare Systems Firework
- HYAS Insight
- Illusive Attack Management System
- Infoblox Cloud Data Connector
- Kaspersky Security Center
- Log4j Vulnerability Detection
- Lookout Mobile Threat Defense
- McAfee ePolicy Orchestrator
- Microsoft Defender XDR
- Microsoft Defender for Office 365
- Morphisec UTPP
- Proofpoint TAP
- SailPoint
- Security Threat Essentials
- Semperis Directory Services Protector
- Sophos Cloud Optix
- Symantec Integrated Cyber Defense Exchange (iCDX)
- Threat Analysis Response
- Trend Micro Deep Security
- Zimperium Mobile Threat Defense

Compliance

- CMMC
- Maturity Model for Event Log Management M2131
- NIST SP 80053
- Senserva Offer
- Sonrai Security
- Zero Trust (TIC 3.0)

Cloud security

- Barracuda CloudGen Firewall
- Bitglass
- Cisco Umbrella
- Forcepoint CASB
- Forcepoint CSG
- Microsoft Defender for Cloud Apps
- Netskope
- PAN Cortex Data Lake
- PAN Prisma
- Trend Micro Cloud App Security
- Zscaler
- Wiz

Protect everything

Extensible security for your entire digital estate

Easily onboard data

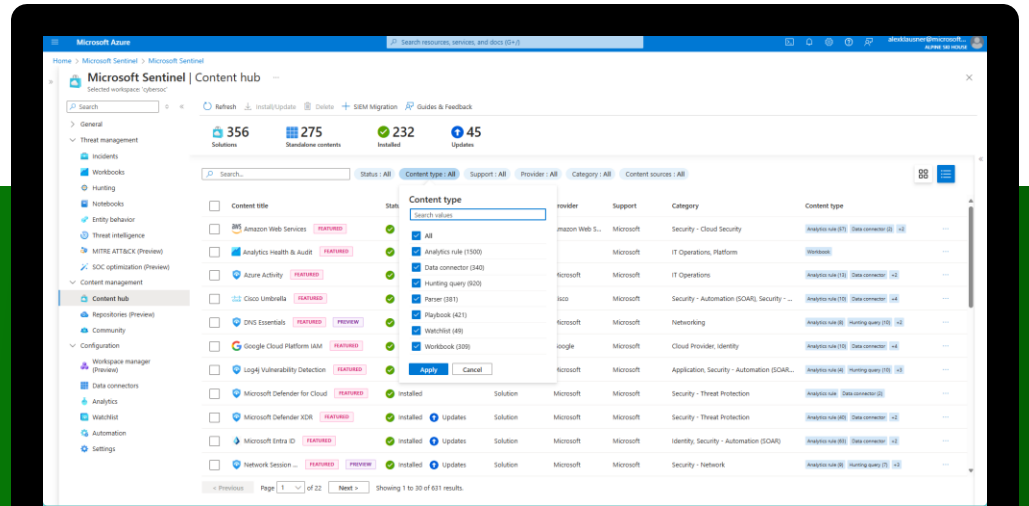
Benefit from over 300+ out-of-the-box connectors and our codeless connector platform to onboard data

Address your needs

Library of customizable content to meet the evolving demands of your organization

Focus on what matters

Correlate alerts into prioritized incidents while reducing false positives by 79%* with native machine learning



Microsoft Sentinel content hub

*The Total Economic Impact™ Of Microsoft Sentinel (forrester.com)

Increase ROI

Maximize value and manage costs

Cloud flexibility

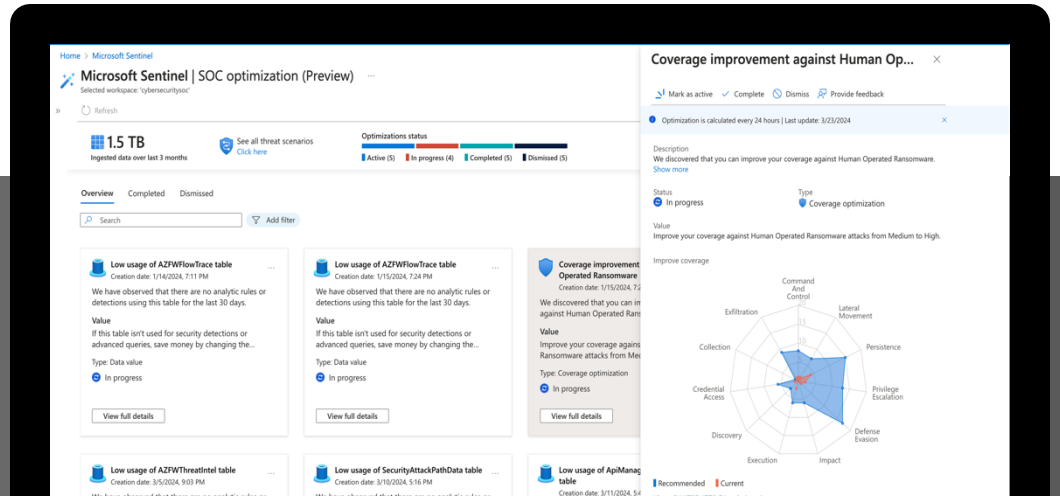
Moving from a legacy SIEM can reduce costs by 44%.* while allowing you to scale up and down as needed

Optimize costs and protections

SOC optimizations deliver targeted recommendations to improve security and manage costs

Tiered data

Manage your data at scale with affordable solutions for storage and volume-based savings



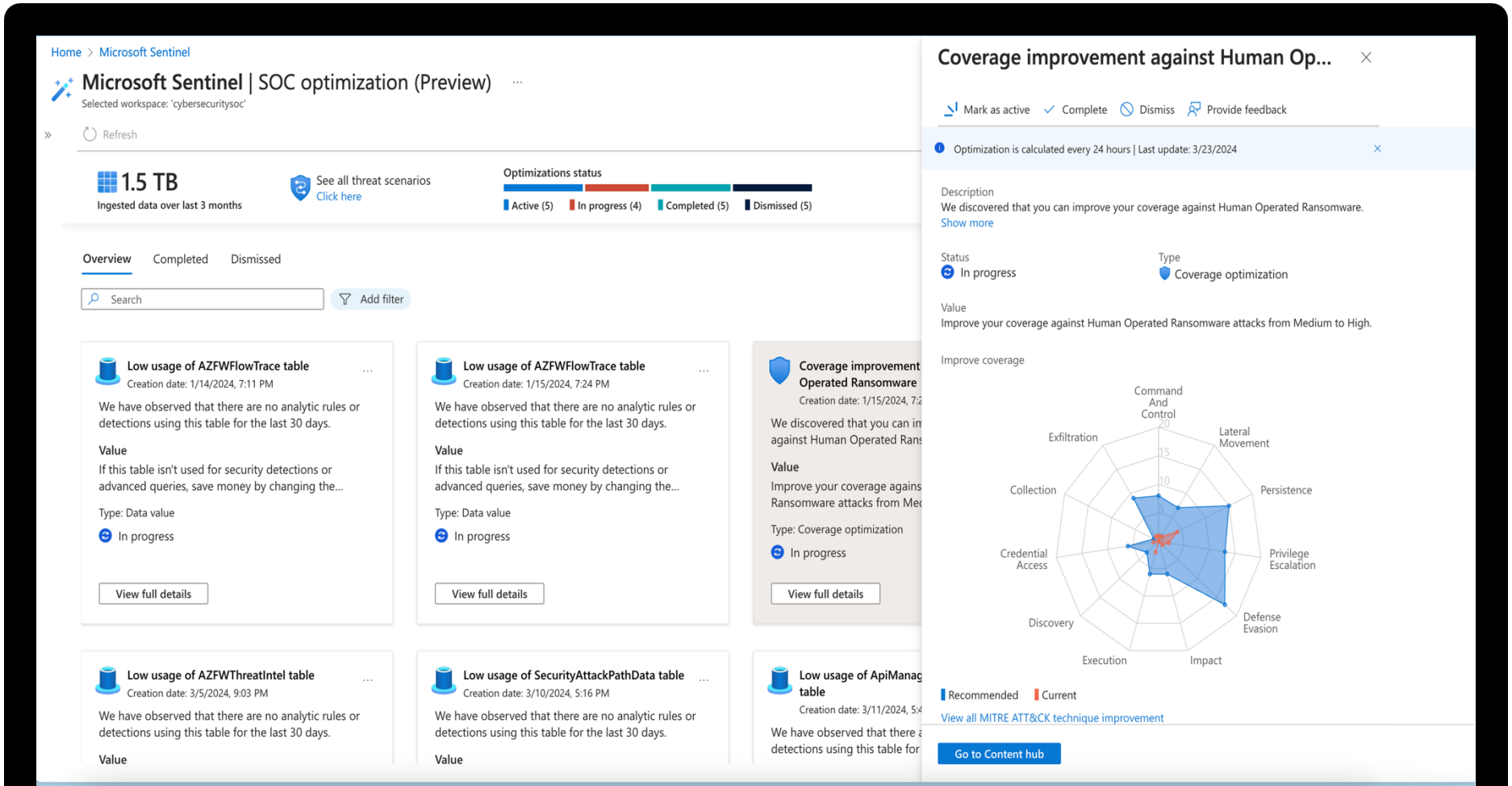
234%

ROI*

*The Total Economic Impact™ Of Microsoft Sentinel (forrester.com)

SOC optimization delivers daily tailored recommendations to help manage your data

Save time | **Manage costs** | **Stay safer** | **Drive value**



Move faster

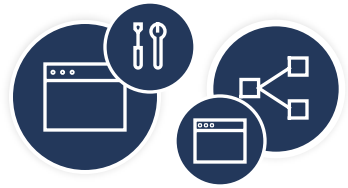
Drive SOC efficiency with AI and automation

Automated response

Native SOAR platform enables customizable automation for rapid response via logic apps

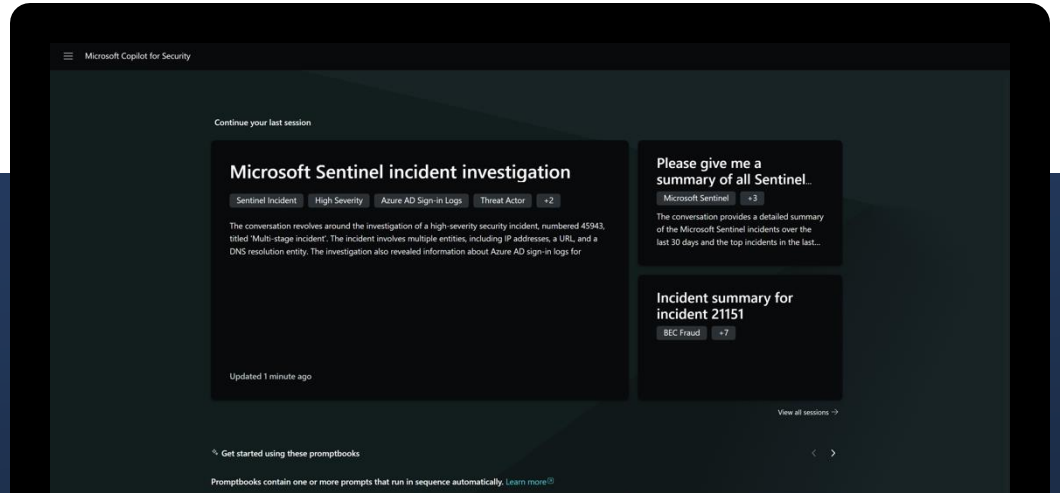
Generative AI

Copilot for Security embedded into the experience can guide work, accelerate response, and improve quality



AI- powered SIEM

Machine learning is embedded into many functions of Microsoft Sentinel, helping customers to respond faster



Embedded generative AI that can support every step of the security lifecycle

Copilot for Security in the SOC

Skills to level-up security analysts

- Accelerate full resolution for every incident
- Identify and prioritize with built-in context
- Prevent breaches with dynamic threat insights
- Elevate analysts with intelligent assistance

Why chose Microsoft Sentinel for your SIEM?

Protect everything

3,800+

Standalone content and package solutions ready out of the box

93%

Reduction in time to configure and deploy new connections

70T

Signals analyzed each day

Increase ROI

234%

ROI

44%

Reduction in total cost of operating compared to legacy solutions

Move faster

22%

Copilot for Security users were faster across all tasks

85%

Reduction of labor effort for advanced, multitouch investigations

The Total Economic Impact™ Of Microsoft Sentinel (forrester.com)

bluecycle

Thank you

Microsoft Security

Managing costs with Microsoft Sentinel

Optimize data ingestion

- Avoid ingesting non-SOC or performance-related data.
- Identify key dimensions from a log that are necessary to manage security.
- Separate non-security data in a different workspace.

Data collection transformation

- Filter out any data that is not required.
- This can be done by removing rows or columns, parsing important information from a column, or sending certain rows to basic logs.

Manage data retention policies

Data storage may vary compliance requirements or use cases for a specific data type (such as forensic analysis).

Use different log types when needed

Reduce long-term data retention costs with archived logs or take advantage of basic logs data ingestion for high-volume, low-security value data.

Use workspace management best practices

Decisions about workspace architecture are typically driven by business and technical requirements, however, costs should be a major part of designing architecture. Consider best practices to balance needs.

Take advantage of AI and automation capabilities

Using SOAR capabilities to automate response to familiar threats and using AI to fuse alerts into incidents and prioritize issues can reduce time to response, the risk of breach, and ultimately reduce the costs and time spent by analysts on issues.

Take advantage of Microsoft Sentinel offers

Microsoft provides a data ingestion benefit to E5, A5, F5, and G5 customers for Sentinel that can help customers save money.

Save money and reduce time to value

93% decrease in time to configure and deploy new connections with prebuilt SIEM content and out-of-the-box functionality

234% ROI over three years

35% reduction in likelihood of data breach

44% less expensive compared to on-premises SIEMs

79% reduction in false positives over three years

85% reduction of labor for advanced, multitouch investigations

Source: The Total Economic Impact™ of Microsoft Sentinel, a commissioned study conducted by Forrester Consulting, 2024