Microsoft Security

Modernize SecOps with Microsoft Sentinel

A Guide for Security Leaders

Business continuity depends on stringent cybersecurity

Attack surfaces, data volume, and threat complexity are increasing. Traditional security information and event management systems (SIEMs) aren't keeping up.

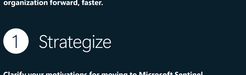
Conventional SIEMs are complex to set up and maintain, and have limited scalability. The result? Maintenance overhead and churn. Disjointed tools lead to missed threats and security gaps—all contributing to overwhelmed security teams and organizational inefficiencies.

Organizations need a SIEM solution with built-in intelligence to help them reduce noise, focus on what matters, and drive efficiency—while staying ahead of evolving threats.

Microsoft Sentinel: A modern approach to security

Transform the security operations center (SOC) with a multi-cloud, multi-platform SIEM built on leading AI, automation, and threat intelligence.

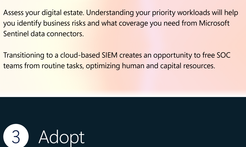
Microsoft Sentinel empowers analysts to seamlessly protect assets with native integrations of XDR, cloud security, and exposure management in Microsoft's unified SecOps platform.



Attack detection | Threat visibility | Proactive hunting | User and entity behavior analytics | Threat response

Microsoft Sentinel eliminates infrastructure setup and manual management complexity while saving your organization money.

Our latest **Total Economic Impact™ Of Microsoft Sentinel Study** commissioned by Microsoft shows the benefits of using Microsoft Sentinel.



234% return on investment (ROI)

79% reduction in false positives

35% reduced likelihood of a data breach

Consider the following staged deployment approach to move your organization forward, faster.

1 Strategize

Clarify your motivations for moving to Microsoft Sentinel

Understanding motivations for implementing Microsoft Sentinel can reveal better business outcomes.

Consider motivations that are event driven, financially driven, future driven, or efficiency driven—like keeping up with evolving threats, consolidating your security stack, or reducing integration and training time.

Once you understand your motivation, you can list concrete objectives and KPIs to best measure progress.

2 Plan

Create an action plan to onboard with Microsoft Sentinel

Assess your digital estate. Understanding your priority workloads will help you identify business risks and what coverage you need from Microsoft Sentinel data connectors.

Transitioning to a cloud-based SIEM creates an opportunity to free SOC teams from routine tasks, optimizing human and capital resources.

3 Adopt

Start, customize, and innovate with Microsoft Sentinel

Breaking down the adoption journey into three stages can enhance your SOC team's focus and allow your team members to build the skills to handle threats faster and more effectively.

30 days – Get started

When you first implement Microsoft Sentinel, concentrate on your priority workloads. You'll also be set up to address the following areas:

- Tracking your deployment
- Validating your data
- Creating custom connectors
- Defining and tackling a first incident
- Identifying security partners

60 days – Customize

Leverage automation to increase productivity and tackle deeper analysis and remediation by:

- Optimizing your SOC
- Adding missing data sources
- Creating custom analytics rules
- Automating threat responses
- Embedding AI assistance with Microsoft Security Copilot

90 days – Innovate

Explore advanced hunting techniques and embrace innovation to help your team become more productive through:

- Enabling basic and archived logs
- Integrating cyberthreat intelligence (CTI)
- Identifying advanced threats with user and entity behavior analytics (UEBA)
- Detecting threats with customizable anomalies
- Bringing your own machine learning into Microsoft Sentinel

4 Manage

Establish Microsoft Sentinel as the guardian of your digital estate

Your organization can keep tabs on who is accessing Microsoft Sentinel, what actions they take, and when. Assign roles in your SOC and grant levels of access to Microsoft Sentinel.

Cost Management features help you set budgets, monitor costs, and review forecasts and spending trends to identify areas where you might want to act.

Dial resources up and down based on your organization's needs, enabling you to:

- Optimize your investigation and hunting experience with Auxiliary Logs
- Set retention policies for individual tables
- Extend Microsoft Sentinel with APIs and integrations
- Monitor metrics for continuous improvement

Move faster with simplified threat detection and response

Microsoft Sentinel is revolutionizing the SOC with an innovative SIEM that delivers built-in SOAR, UEBA, TI, and generative AI.

With Microsoft Sentinel, customers can confidently protect their organizations from today's and tomorrow's threats with unparalleled visibility, cloud flexibility, and comprehensive coverage.

Organizations of all sizes can take advantage of Microsoft Sentinel's out-of-the-box features to start seeing faster ROI, and move forward fearlessly.

Get started with Microsoft Sentinel today

*"The Total Economic Impact™ Of Microsoft Sentinel," A Forrester Total Economic Impact™ Study Commissioned By Microsoft, Forrester Research, Inc., March 2024