Microsoft Security

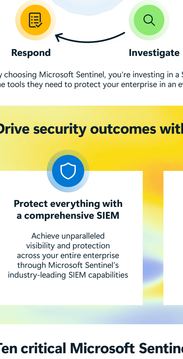
Microsoft Sentinel

AI-powered SIEM, built for modern security

In today's complex cyberthreat landscape, security operations centers (SOCs) face significant challenges. The increasing volume and sophistication of cyberattacks lead to overwhelmed analysts and missed threats. Security teams are hindered by fragmented tools, poor visibility, and the absence of critical features in legacy SIEM solutions, leaving them vulnerable to emerging threats.

To overcome these challenges, you need a trusted SIEM to secure your multi-cloud, multi-platform environment built on leading AI, automation and threat intelligence.

Transform your security operations with Microsoft Sentinel



Modernize your security operations with Microsoft Sentinel—an AI-powered, cloud-native SIEM that defends against evolving cyber threats with unmatched efficiency and intelligence.

- **Easily scale your defenses** with the flexibility and cost efficiency of the cloud to grow with your organization
- **Gain comprehensive threat management** using AI, SOAR, UEBA, and TIP for proactive defense
- **Identify emerging threats faster** with AI-powered, real-time detection and machine learning
- **Automate incident response** to reduce response times and operational workloads
- **Support compliance** with industry-specific security standards and regulatory frameworks

By choosing Microsoft Sentinel, you're investing in a SIEM solution that's designed for the future—equipping your security team with the tools they need to protect your enterprise in an ever-changing threat landscape.

Drive security outcomes with an innovative SIEM

Protect everything with a comprehensive SIEM

Achieve unparalleled visibility and protection across your entire enterprise through Microsoft Sentinel's industry-leading SIEM capabilities

Respond to emergent threats faster

Leverage Microsoft Sentinel's advanced AI and unparalleled threat intelligence to outpace adversaries and stay ahead of merging threats

Scale security coverage with cloud flexibility

Efficiently expand your security operations to match your organization's growth and complexity with Microsoft Sentinel's cloud-native architecture

Ten critical Microsoft Sentinel capabilities to future-proof your SOC

Today's complex security environment demands a SIEM platform that integrates critical capabilities into a unified platform. A unified platform helps security teams streamline operations, enhance threat detection, and accelerate incident response, driving comprehensive protection for your organization.

1. **Cloud-native architecture**
   Microsoft Sentinel's cloud-native architecture enables security teams to scale effortlessly, providing unmatched flexibility and eliminating the costs and complexity of additional infrastructure.
2. **Generative AI for threat detection**
   Security Copilot with Generative AI for threat detection and response can lead to a 30% faster mean time to resolution (MTTR) within just three months, significantly enhancing your security posture.
3. **Broad data collection**
   Microsoft Sentinel integrates with over 350 data connectors, supporting diverse environments including multicloud services and on-premises systems to provide holistic visibility into your entire digital ecosystem.
4. **Flexible data management**
   Microsoft Sentinel offers flexible data tiering and management, enabling you to collect, store and analyze all your security data while optimizing costs.
5. **Machine learning and automation**
   Microsoft Sentinel includes built-in SOAR and UEBA capabilities that combine orchestration, automation and advanced behavioral analytics to streamline threat detection and response, enabling proactive threat identification and efficient incident management.
6. **Advanced threat correlation**
   Microsoft Sentinel's fusion technology correlates data from multiple sources to detect complex, multistage attacks that traditional tools might miss, providing a full view of ongoing threats.
7. **Integrated threat intelligence**
   Microsoft Sentinel includes broad threat intelligence from Microsoft's vast global network and the security community, improving your team's ability to detect, analyze, and respond to threats swiftly and effectively.
8. **Proactive threat hunting**
   Advanced hunting capabilities enable security teams to proactively search for and eliminate potential threats before they cause damage.
9. **SOC optimizations**
   Unique recommendations generated daily provide ways to enhance value of data, manage costs and increase security coverage by 17%.
10. **Customizable dashboards and visualizations**
    Microsoft Sentinel's customizable dashboards provide security teams with tailored, real-time insights in intuitive formats based on operational requirements, enabling faster decision-making and more effective threat response.

Proven SIEM Leader

Microsoft Sentinel is trusted by customers worldwide to confidently protect their organizations from today and tomorrow's threats with comprehensive capabilities, broad coverage, and strong innovation.

A SIEM Leader[1]
in the Gartner® Magic Quadrant™ for Security Information & Event Management

25,000+
organizations worldwide trust Microsoft Sentinel

Comprehensive
SIEM capabilities: AI, SOAR, UEBA, TIP

350+ data connectors
to collect extensive data

Microsoft Sentinel in action: Six ways to boosts your team's efficiency

Microsoft Sentinel leverages AI and automation to enhance every aspect of your SIEM experience, from seamless implementation to advanced threat detection and security analyst assistance. Explore six powerful ways these innovations elevate your team's impact and overall security performance.

1. **Speed implementation with automated migrations**
   Security engineers get access to robust migration tools that simplify the transition from existing SIEM solutions, ensuring seamless data integration, preservation of security configurations, and minimal disruption.
2. **Expand protection across more assets**
   Security engineers can easily expand collection and analysis of security data across identity, email, network, clouds applications, cloud services and endpoints using out-of-the-box connectors.
3. **Accelerate threat detection and response**
   Correlation engine turns alerts into incidents faster. Security Copilot provides analysts with incident summaries, impact analysis, and remediation recommendations, reducing time to respond.
4. **Address any use case**
   Security teams can tap into a rich library of customizable security solutions, including 21,000+ GitHub code contributions, 200+ Microsoft-developed rules and 280+ community-contributed resources for detection, dashboards, and playbooks.
5. **Enhance investigations**
   Security Copilot simplifies complex incidents by summarizing and correlating data across systems, enabling analysts to quickly grasp the scope, impact, and root cause of threats, reducing labor by 85% during investigations.
6. **Automate routine tasks**
   Security Copilot automates routine tasks like log analysis, alert triage and script review, and data correlation, enabling analysts to focus on higher-value strategic activities.

Proven business impact

SIEM ROI

As a cloud-native solution, Microsoft Sentinel eliminates the need for costly infrastructure, reducing both capital and operational expenditures. Organizations can scale their security operations as needed, leading to a higher return on investment.

44% reduction in total costs compared to legacy SIEM providers[2]

234% ROI over three years[2]

Security analyst productivity

Microsoft Sentinel enhances SOC efficiency with AI and automation, reducing the time to detect and respond to threats. By automating common tasks and correlating alerts into prioritized incidents, it allows security teams to focus on critical issues.

85% reduction in labor required for advanced investigations[2]

79% reduction in false positive alerts[2]

Risk profile visibility

The ease of cloud scalability and out-of-box connections with data sources on cloud services and other platforms significantly enhances visibility into the risk profile.

35% reduction in the likelihood of a data breach[2]

93% reduction in time to configure a new connection[2]

Get started

To experience the benefits of Microsoft Sentinel, start with a free trial and explore additional resources and demos. Microsoft Sentinel is the right choice for organizations looking to enhance their security operations, reduce costs, and improve efficiency.

Learn more → | Pricing → | Customer stories →

1. **Gartner, Magic Quadrant for Security Information and Event Management, By Andrew Davies, Mitchell Schneider, Rustam Malik, Eric Ahlm, 8 May 2024** Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.
2. **Forrester Total Economic Impact™ of Microsoft Sentinel** The Total Economic Impact(TM) Of Microsoft Sentinel, a commissioned study conducted by Forrester Consulting, March 2024. Results are based on a composite organization representative of interviewed customers.

Microsoft Security