Microsoft Security

The Strategic SIEM Buyer's Guide

Building an AI-ready platform
for the agentic era

Advancing security operations in the agentic era

Across industries, a new frontier is emerging where humans and AI agents collaborate in real time to drive innovation. While this agentic era unlocks unprecedented opportunity, it also introduces new risks and dramatically expands the attack surface.

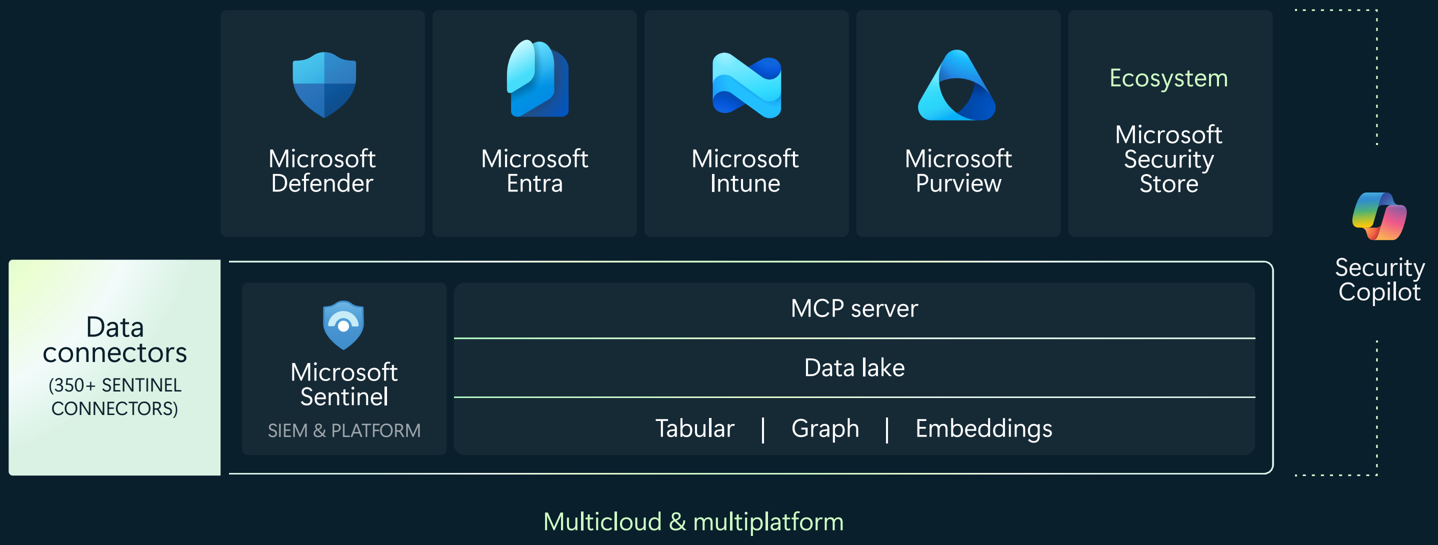
The reality is, many organizations are still operating on legacy security architectures. These fragmented solutions, often requiring 40+ disparate tools, were never designed for the scale, speed, and complexity of today's threat landscape. The result is a Security Operations Center (SOC) overwhelmed by data silos and unable to adapt at AI speed—leaving the business unable to innovate boldly and safely.

To navigate this new era, organizations must move beyond traditional SIEM and adopt an AI-ready security platform. This guide explores the three essentials of a modern platform, equipping you to choose a solution that can:

1. Build a unified, future-proof foundation
2. Accelerate detection and response with AI
3. Maximize your ROI and accelerate time-to-value

An AI-first, end-to-end security platform delivers these essentials by unifying critical security functions and leveraging advanced analytics. Its comprehensive architecture is illustrated below:

Microsoft Sentinel: The security platform for the agentic era



1 Build a unified, future-proof foundation

Today’s SOCs are hampered by legacy on-premises SIEMs and a sprawling collection of 40-plus disparate tools. This fragmented approach creates data silos, operational bottlenecks, and a rigid architecture that cannot scale to meet the demands of hybrid environments and exponential data growth, leaving organizations exposed.

Capabilities of a modern security platform:

A unified security data lake
Centralizes all security data—logs, telemetry, and analytics—into a single repository, eliminating data silos and providing the foundation for AI-powered defense.

Elastic, cloud-native architecture
Scales automatically to handle explosive data growth without costly hardware, ensuring peak performance and cost-effective data retention.

Graph-powered visibility
Uncovers the full story of an attack by visualizing relationships across your digital estate, enabling analysts to instantly trace attack paths and prioritize response.

Integrated SIEM, SOAR, and XDR
Unifies core security functions, analytics, and workflows in a single platform, eliminating costly context-switching and correlating incidents across the full attack chain.

Comprehensive threat intelligence and UEBA
Shifts defense from reactive to proactive by integrating global threat intelligence and AI-powered user and entity behavior analytics (UEBA) to detect advanced threats.

The Sentinel advantage

Microsoft Sentinel delivers these capabilities on a single, AI-ready platform. Its cloud-native architecture, built on Microsoft Azure, provides the effortless scale and economic advantage that legacy systems lack. This is validated by a Forrester Total Economic Impact™ study, which found that organizations using Sentinel achieve a **44% reduction in total cost** of ownership[1].

> "Microsoft Sentinel supports our move towards proactive security delivery by empowering us to be more efficient and effective."

Philomena Lavery, Chief Information Security Officer, AVEVA

[1] The Total Economic Impact™ Of Microsoft Sentinel (March 2024)

Buyer’s tip

Challenge vendors on true unification and cloud-native scale. If essential capabilities like SOAR or UEBA are paid add-ons, or if scaling requires manual intervention, you are inheriting hidden costs and complexity.

2 | Accelerate detection and response with AI

Sophisticated attackers can breach private data in under 75 minutes, yet many SIEMs leave the critical step of response to slow, manual effort. Without real-time correlation and automation, the SOC remains in a perpetually reactive posture, trying to catch up to damage that has already been done.

Capabilities for AI-powered security:

Automated orchestration (SOAR)
Rapidly contains threats by orchestrating playbooks that execute remediation and notifications across integrated security tools, accelerating MTTR. When combined with AI-driven insights from Microsoft Security Copilot and advanced analytics, SOAR enables more informed and adaptive incident response.

Agentic AI for autonomous response
Enables AI agents to autonomously investigate, correlate, and act on threats. With standardized access to the data lake, agents can execute intelligent, automated responses.

AI fueled by high-quality, unified data
Empowers AI models with the rich, contextual data needed for accurate detection. By reasoning over the complete historical and real-time data in a unified lake, AI can precisely predict attack paths and reduce false positives.

AI-assisted investigation
Stops attacks in progress by automatically correlating anomalous behaviors across the kill chain. With tools like Microsoft Security Copilot, analysts are guided through complex investigations, accelerating response tasks by 22%

The Sentinel advantage

Microsoft Sentinel combines generative AI with its unified data lake to power superior detection and autonomous response. This intelligence translates directly into superior outcomes, with organizations achieving up to a **79% reduction in false positives** and a **30% reduction in MTTR**, freeing analysts to focus on strategic threat hunting[2].

> "Security Copilot is an innovative tool that's allowing us to grow and mature as a security team. It's almost like having an extra person—a mentor—guiding us to be more successful."

David Finkelstein, Chief Information Security Officer, St. Luke's University Health Network

Buyer's tip

Question the data behind the AI. If a platform's AI relies on fragmented data, you are investing in an engine that is blind to the full context of your environment, limiting its accuracy and speed.

[2] Generative AI and Security Operations Center Productivity: Evidence from Live Operations, Microsoft, November 2024

3 | Maximize your ROI and accelerate time to value

Traditional SIEM deployments can take months, requiring extensive customization, specialized expertise, and ongoing maintenance. This complexity creates a significant barrier to value, forcing organizations to invest heavily in professional services and lengthy training cycles, delaying ROI and increasing operational overhead.

Capabilities for rapid adoption:

Out-of-the-box value
Accelerates deployment with a vast library of pre-built resources, including 350-plus data connectors and hundreds of Microsoft-developed solutions and community contributions, enabling threat detection on day one.

A single, intuitive experience
Streamlines operations by consolidating all security data and workflows into a single, intuitive dashboard. This unified view eliminates the need to learn and manage multiple tools, dramatically reducing the learning curve.

AI-powered optimization
Delivers continuous value by using AI to provide dynamic recommendations that help you optimize costs and improve security coverage, ensuring your security budget is invested with maximum impact.

Flexible, no-code customization
Empowers your team to easily tailor detection rules, dashboards, and automation playbooks to match your organization's specific needs, without requiring deep coding expertise.

The Sentinel advantage

Microsoft Sentinel is designed to **deliver value immediately**. Its rich repository of out-of-the-box content and intuitive tutorials reduce deployment time by 93%, enabling threat detection in hours, not months. This rapid adoption delivers a powerful 234% return on investment (ROI), according to a Forrester Total Economic Impact™ study, minimizing reliance on external consultants and maximizing your security investment from day one[3].

> "Microsoft Sentinel's ease of use means we can go ahead and deploy our solutions much faster. It means we can get insights into how things are operating more quickly."
>
> Director of IT, Healthcare

[3] The Total Economic Impact™ Of Microsoft Sentinel (March 2024)

Buyer's tip

Focus on time to value, not time to configure. If a vendor's path to value depends heavily on professional services or custom development, you are inheriting project risk and a higher total cost of ownership.

The new standard for security operations

The three essentials outlined in this guide—a unified foundation, AI-powered acceleration, and rapid time to value—are the new standard for modern security. Choosing a platform that delivers on these criteria is fundamental to building a resilient, adaptive, and efficient SOC.

This leadership is recognized across the industry. For 2025, Gartner has again named Microsoft a Leader in the Magic Quadrant™ for Security Information and Event Management, highlighting Sentinel's strengths in its breadth of integrations, customizable analytics, and enhanced AI capabilities[4]. This recognition, alongside being named a Leader in The Forrester Wave™: Security Analytics Platforms, Q2 2025, validates Sentinel as the definitive platform for securing the agentic era.

[4] 2025 Gartner® Magic Quadrant™ for Security Information and Event Management (SIEM)

Take the next step in modernizing your security operations.

↗ **Learn more about Sentinel**

Explore how Sentinel's cloud-native architecture, AI-powered detection, and automation can modernize your security operations.

↗ **Discover Microsoft Unified SecOps**

See how Sentinel integrates with Microsoft Defender to deliver AI-powered, end-to-end security operations.

Share this guide | Help your colleagues and peers build a more resilient security operation.

Microsoft Security