Microsoft Security

The Definitive SIEM Buyer's Guide

Five SIEM Essentials to Future-Proof the SOC

APRIL 2025

Contents

A New Era of Cybersecurity: The Need for a NextGen SIEM

It has never been more complex to secure your digital estate. Digital transformation and the evolution of hybrid work models has dramatically expanded the attack surface, while cybercriminals continuously develop more sophisticated methods, increasingly fueled by advances in AI. The result: Security Operations Center (SOC) teams are inundated with an overwhelming volume of security data and alerts, making it nearly impossible for traditional Security Incident and Event Management (SIEM) solutions to keep up.

These challenges are compounded by staffing shortages and operational inefficiencies. Legacy SIEM tools often demand specialized skills, increasing competition for experienced analysts and leaving many organizations struggling to maintain adequate threat coverage. Furthermore, traditional solutions are slow to adapt to emerging threats, such as zero-day vulnerabilities, exposing organizations to heightened risks of breaches. To stay ahead of these ever-evolving threats, SOC teams require a proactive approach—one that empowers them with cutting-edge innovation, advanced threat intelligences, resources, and capabilities to detect and neutralize threats effectively.

The SIEM market itself has grown increasingly fragmented. Organizations must navigate a complex mix of legacy vendors, new entrants, and do-it-yourself (DIY) solutions. Many traditional SIEM solutions frequently fail to meet the demands of modern security operations, plagued by high costs, limited scalability, and outdated functionality. Emerging solutions, while promising, often provide only partial capabilities, falling short of addressing the full spectrum of security needs.

This Buyer's Guide highlights the urgent need to modernize your SIEM. It outlines the advantages of transitioning from legacy systems to cloud-native solutions and explores five essentials to consider when evaluating a SIEM platform. In addition , we will share how Microsoft Sentinel addresses these priorities — all supported by insights from an independent survey of security leaders commissioned by Microsoft.

Selecting the right SIEM solution is no longer just about managing logs.

Dave Gruber

Principle Analyst, Enterprise Strategy Group

Modernizing the SIEM

Organizations must transform the Security Operations Center (SOC) to enhance threat detection and response capabilities, streamline operations, and mitigate escalating security risks, or risk facing increased vulnerabilities, prolonged incident response times, and potential financial and reputational damage.

Many SIEM solutions in the market continue to burden SOC teams with manual setups, limited scalability, and overly complex automation configurations. These outdated systems require analysts to invest significant time addressing false positives, managing updates, and maintaining integrations—leaving critical gaps in organizational defenses against today's dynamic and sophisticated threats. The rise of generative AI and other advanced technologies in the attacker's arsenal has only magnified the limitations of traditional SIEMs.

In today's rapidly evolving threat landscape, adopting a modern, cloud-native SIEM is no longer optional—it's essential. Cloud-native solutions are purpose-built to deliver the flexibility and scalability required to manage complex multi-cloud and multi-platform environments. By seamlessly integrating machine learning and advanced automation, they minimize low-value tasks, enabling SOC teams to focus on high-priority threats. With embedded AI-driven assistance, modern SIEMs empower organizations to stay ahead of attackers, facilitating faster and more effective responses to emerging threats.

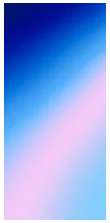
Microsoft's research found several key challenges SOC leaders face with traditional SIEMs, including scaling costs, complex configurations, limited integrations, and a lack of innovation—all of which hinder effective security operations.

By transforming your SOC with a cloud-native, AI-powered platform, you gain a scalable and cost-effective security solution that integrates seamlessly across your digital ecosystem. These advanced solutions not only enhance analyst efficiency but also provide the innovation required to outpace attackers. With the right next generation SIEM, you can future-proof your operations and strengthen your defenses against tomorrow's most sophisticated threats.

Common SIEM Challenges for SOC Leaders

Platform Complexity & Lack of Critical Capabilities

Organizations face challenges with SIEMs due to platform complexity, requirement for disparate tools, high training requirements, and extensive infrastructure management, leading to inefficiencies in security operations.



Restricted Flexibility & High Costs

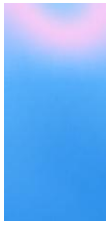
Organizations face challenges with SIEMs due to restricted flexibility to support digital ecosystem, data ingestion costs, add-on module licensing, need for on-premises infrastructure, and high consultancy overhead, leading to operational inefficiencies and security posture gaps.

Limited Integrations & Slow Time to Value

Organizations face challenges with SIEMs due to complex integrations, long implementation cycles, and limited interoperability with the ecosystem, leading to slow time to value.

Ineffective Threat Detection Automation

Organizations face challenges with SIEMs due to ineffective threat detection automation, alert fatigue, slow MTTD/MTTR, low staff efficiency, and long incident investigations, leading to increased vulnerabilities.



Lack of Innovation

Organizations face challenges with SIEMs because of insufficient innovation and a constrained roadmap vision. This results in security analyst inefficiency, limited generative AI, and a lack of machine learning-driven capabilities, ultimately leading to outdated security operations and heightened vulnerability.

01

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Built-in Security Essentials

> If you want to add SOAR for automation or UEBA for internal threat analysis and prevention, many SIEM vendors have add-on costs.
>
> Security Leader, Banking

SIEMs with built-in critical capabilities eliminates data silos, reduces alert fatigue, and streamlines management, giving SecOps teams real-time visibility across the entire environment.

Unified Capabilities that Transform Security Operations

The complex threat landscape requires a shift away from disjointed security tools toward unified solutions that consolidate essential capabilities. A modern SIEM platform integrates essential functions—Security Orchestration, Automation, and Response (SOAR), Threat Intelligence Platform (TIP), User and Entity Behavior Analytics (UEBA), and Generative AI—within one solution, enabling faster threat detection, streamlined management, and more efficient responses.

SOAR capabilities automate repetitive tasks, orchestrate response across security tools, and accelerate incident resolution.

TIP capabilities provide real-time, actionable intelligence, empowering teams to detect emerging threats proactively.

UEBA capabilities identify anomalous behaviors indicative of insider threats or compromised accounts, enhancing threat visibility.

Generative AI and Machine Learning enhance analyst productivity by intelligently automating detection, response, and workflow optimization.

Consolidating these capabilities reduces alert fatigue, lowers operational costs, enhances resource allocation, and positions organizations to proactively address evolving cybersecurity threats.

01

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Built-in Security Essentials

Checklist of Capabilities

When evaluating a SIEM solution, look for these capabilities:

- [ ] **Security Orchestration, Automation, and Response (SOAR)**
  Does the SIEM include built-in, automated incident response workflows?
  Can the SIEM orchestrate actions seamlessly across multiple security tools?
  Does it offer customizable playbooks to facilitate rapid incident handling?

- [ ] **Generative AI and Machine Learning**
  Does the SIEM utilize generative AI to enhance threat detection and response processes?
  Can it apply machine learning models that continuously adapt to identify emerging threats?
  Does it optimize workflows by providing intelligent recommendations and automating routine analyst tasks?

- [ ] **Threat Intelligence Platform (TIP)**
  Does the SIEM natively integrate real-time threat intelligence feeds?
  Can it enrich collected data with contextual threat insights for improved detection accuracy?
  Does it correlate threat intelligence data across multiple sources to deliver advanced insights?

- [ ] **User and Entity Behavior Analytics (UEBA)**
  Does the SIEM establish behavioral baselines to effectively detect insider threats?
  Can it monitor user and entity activities to detect anomalies in real-time?
  Is it capable of correlating anomalous behaviors with other security events to identify risks comprehensively?

- [ ] **Native Integration with Other Security Solutions**
  Does the SIEM provide seamless integration capabilities with XDR and cloud security solutions?
  Does it offer built-in exposure management capabilities?
  Can it consolidate and centrally manage data from endpoints, cloud platforms, and third-party security tools?

01

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Built-in Security Essentials

> One of the benefits of Microsoft Sentinel is the fact that it's already a bundled environment that you can turn on. It gives a comprehensive view of your ecosystem.

Security Leader, Manufacturing

01

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Built-in Security Essentials

The Microsoft Sentinel Advantage

Microsoft Sentinel includes built-in Security Orchestration, Automation, and Response (SOAR), Threat Intelligence Platform (TIP), User and Entity Behavior Analytics (UEBA), and Artificial Intelligence (AI) that together, simplifies security management, enhances threat detection and response, and provides unparalleled visibility and control across the entire digital landscape.

Microsoft Sentinel delivers essential security capabilities in a unified, integrated solution designed specifically for modern Security Operations Centers (SOCs).

Microsoft Sentinel's integrated SOAR capability offers automated, customizable incident response playbooks that streamline workflows, significantly accelerating threat resolution. The solution's robust UEBA capability continuously monitors user activities and immediately flags anomalous behaviors indicative of insider threats or account compromises, enabling rapid intervention.

Advanced Generative AI and Machine Learning embedded in Microsoft Sentinel enhance proactive threat identification and significantly reduce false positives. Additionally, integration with Microsoft Security Copilot transforms complex threat analysis tasks into simplified, natural-language-based actions. Analysts can quickly turn insights into automated response actions, streamlining investigations and response workflows.

With its powerful Threat Intelligence platform, Microsoft Sentinel aggregates threat data from diverse global sources, providing enriched, contextual threat insights that proactively protect the organization. The native integration with Microsoft Defender's Extended Detection and Response (XDR) solution extends visibility across endpoints, cloud environments, and infrastructure, ensuring comprehensive protection and operational efficiency.

Together, these unified capabilities in Microsoft Sentinel empower security teams with greater visibility, faster threat response, reduced complexity, and increased effectiveness in the face of evolving cyber threats.

01

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Built-in Security Essentials

The Microsoft Sentinel Advantage

Explore Key Capabilities in Microsoft Sentinel

Security Orchestration, Automation, and Response (SOAR)

Automate and orchestrate incident responses with built-in, customizable playbooks, significantly enhancing SOC efficiency.

Generative AI and Machine Learning

Proactively detect sophisticated threats with intelligent automation, augmented by natural language capabilities via Microsoft Security Copilot.

Native XDR Integration

Seamlessly integrate with XDR platform, providing comprehensive visibility across endpoints, networks, and cloud resources.

User and Entity Behavior Analytics (UEBA)

Detect insider threats by continuously monitoring and analyzing user behavior, identifying anomalies in real-time.

Advanced Threat Intelligence

Ingest, curate, and manage real-time threat indicators, empowering proactive threat detection and timely response.

02

Scalable & Flexible Cloud Architecture

> My current SIEM solution is cumbersome and has a huge learning curve. It requires a lot of training to get there.
>
> CISO, Infrastructure

A scalable and flexible cloud architecture provides the confidence to handle future growth and evolving threats while maintaining operational effectiveness and cost efficiency.

Achieving Scalability & Flexibility in SecOps

In today's dynamic enterprise security landscape, organizations face escalating threats across increasingly complex IT environments, spanning on-premises, hybrid, and multi-cloud infrastructures. With data volumes continually growing, SIEM solutions must be capable of scaling flexibly and cost-effectively without sacrificing performance or visibility.

On-premise SIEM solutions often fail to efficiently scale to handle this complexity, leading to operational delays and coverage gaps. A modern SIEM should leverage cloud-native architecture, delivering effortless scalability to manage fluctuating data demands without sacrificing performance.

Cloud-native solutions automatically scale resources to match data ingestion needs, eliminating manual adjustments and expensive hardware investments. Additionally, built-in integrations ensure visibility across multi-cloud and hybrid environments, enabling unified threat detection and management. Elastic resource scaling ensures consistent performance even during peak demand, while automated scaling prevents performance bottlenecks and unnecessary infrastructure expenditures.

Organizations must also focus on reducing the cost and complexity of SIEM solutions, including data ingestion costs, reliance on expert consultants, and improving team efficiency. By adopting cloud-native SIEM solutions, organizations can streamline operations, reduce overhead, and enhance overall security posture.

A flexible and scalable cloud-native architecture positions organizations to quickly adapt to emerging threats, seamlessly accommodate infrastructure growth, and maintain robust security operations.

02

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Scalable & Flexible Cloud Architecture

Checklist of Capabilities

When evaluating a SIEM solution, look for these capabilities:

- [ ] **Cloud-Native Architecture**
  Does the SIEM provide cloud-native scalability, eliminating reliance on traditional on-premises hardware?
  Can it efficiently scale to manage increasing security demands without performance degradation?

- [ ] **Elastic Resource Scaling**
  Does it automatically scale resources to handle data ingestion fluctuations?
  Can it scale seamlessly without manual intervention or additional infrastructure?

- [ ] **Hybrid and Multi-Cloud Support**
  Does the SIEM seamlessly integrate with multi-cloud and hybrid environments?
  Can it centralize management across on-premises, cloud, and geographically dispersed data sources?

- [ ] **Flexible Data Handling**
  Does SIEM ingest both structured and unstructured logs and telemetry data?
  Can it effectively normalize and correlate diverse data types from varied sources?

- [ ] **Cost Efficiency (ROI/TCO)**
  Does the SIEM offer cost-effective management solutions for large volumes of data?
  Is extensive third-party consulting required, or does it provide intuitive, efficient operation?

02

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Scalable & Flexible Cloud Architecture

> With Microsoft Sentinel, if we want to scale something out or add a new ingestion, it's literally just a click of a few buttons. If we want to change stuff out, it only takes a few minutes.

Director of IT Operations, Manufacturing

02

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Scalable & Flexible Cloud Architecture

The Microsoft Sentinel Advantage

Microsoft Sentinel's scalable and flexible cloud architecture delivers a comprehensive, integrated solution that adapts to the evolving needs of modern security operations, providing unparalleled visibility, control, and efficiency across the entire digital landscape.

Microsoft Sentinel's cloud-native architecture delivers exceptional scalability and flexibility, enabling organizations to confidently manage evolving security demands without additional infrastructure costs. Built entirely on Microsoft's Azure cloud, Microsoft Sentinel effortlessly scales with increasing volumes of data and complex operational needs, automatically adjusting resources to maintain peak performance. Organizations leveraging Microsoft Sentinel gain seamless operational continuity, even amid spikes in threat activity or rapid infrastructure growth.

With comprehensive multi-cloud and hybrid environment support, Microsoft Sentinel integrates effortlessly across diverse platforms, unifying threat visibility and ensuring operational consistency across all infrastructure layers. Its sophisticated data ingestion capabilities handle structured and unstructured telemetry, enabling analysts to correlate complex threat data efficiently.

Additionally, Microsoft Sentinel provides optimized ingestion strategies, eliminating redundant data and focusing on information that delivers genuine security value.

Microsoft Sentinel's SOC optimization recommendations further distinguish its scalability and flexibility advantages. These precision-driven insights help organizations continuously improve security coverage (by up to 17%) and increase meaningful data utilization (by up to 31%), ensuring cost-effective and targeted security operations.

Finally, the Forrester Total Economic Impact™ (TEI) Study underscores Microsoft Sentinel's cost benefits, demonstrating a 44% reduction in total cost of ownership (TCO) over three years, confirming exceptional scalability, flexibility, and financial advantages.

02

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Scalable & Flexible Cloud Architecture

The Microsoft Sentinel Advantage

Explore Key Capabilities in Microsoft Sentinel

Cloud-Native Scalability

Automatically scales resources without the need for additional infrastructure to accommodate expanding data needs and operational complexity.

Multi-Cloud, Multi Platform Support

Comprehensive security monitoring and threat detection across multiple cloud environments and platforms, ensuring seamless protection and visibility for your entire digital estate.

SOC Optimization

Actionable recommendations improve security coverage, data utilization, and efficiency, ensuring continuous optimization of resources.

Optimized Data Handling

Handles both structured and unstructured data, adapting flexibly to diverse and changing data sources.

Proven Cost Efficiency

Scalable and flexible cloud architecture enhances cost efficiency by aligning resource usage with business needs, leading to lower TCO.

03

> Some SIEM solution providers offer fewer features and less AI integration compared to competitors.
>
> Security Leader, Manufacturing

Generative AI & Machine Learning

Generative AI enables innovative applications like automated incident response playbooks, natural language processing for threat intelligence analysis, and predictive threat modeling.

Harnessing AI to Revolutionize Threat Detection and Analyst Workflows

The current threat landscape is characterized by increasing sophistication, velocity, and volume. Traditional SIEM solutions relying primarily on rule-based detection are increasingly overwhelmed by alert fatigue, unable to keep pace with advanced threats, and insufficiently agile to address rapidly evolving attack patterns, including zero-day attacks, sophisticated phishing attacks, and multi-vector attacks. SOC teams urgently need accurate detection capabilities, greater automation, and predictive insights to proactively manage threats rather than simply reacting to breaches after they occur.

Generative AI and machine learning (ML) technologies address these critical limitations by providing advanced analytical capabilities to improve effectiveness of security automation and augment analyst workflows. ML algorithms continuously learn from vast amounts of diverse security data, detecting anomalies indicative of emerging threats and uncovering subtle patterns invisible to rule-based systems. Additionally, generative AI enables unprecedented automation of response workflows through natural language processing (NLP), transforming complex threat intelligence into clear, actionable insights and guiding security teams toward proactive threat management.

By embedding AI and ML capabilities, modern SIEM solutions empower SOCs to dramatically reduce false positives, enhance analyst productivity, and accelerate mean-time-to-response (MTTR). This approach allows analysts to shift from reactive firefighting toward strategic threat hunting and prevention. Integrating generative AI-driven predictive modeling further enables proactive identification of vulnerabilities, significantly bolstering an organization's resilience and overall security posture.

03

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Generative AI & Machine Learning

Checklist of Capabilities

When evaluating a SIEM solution, look for these capabilities:

- [ ] **Machine Learning Features**
  Does the SIEM use ML to detect anomalies and reveal complex attack patterns?
  Can it identify sophisticated, multi-stage threats missed by traditional detection methods?

- [ ] **Generative AI for Automation and Analysis**
  Can the SIEM automate tasks such as incident classification, alert triage, and reporting?
  Does it employ NLP to deliver clear, actionable intelligence and human-readable incident summaries?

- [ ] **Behavioral Analytics**
  Does the solution leverage AI/ML to establish behavioral baselines for users and entities?
  Can it detect anomalies indicative of insider threats or compromised credentials?
  Does it correlate behavioral anomalies with broader security indicators?

- [ ] **Real-Time Processing and Insights**
  Can it process security data in real-time to rapidly detect emerging threats?
  Does it provide immediate, actionable intelligence and prioritized response recommendations?
  Is the solution scalable enough to handle large data volumes without sacrificing speed or accuracy?

- [ ] **Predictive Threat Modeling**
  Does the SIEM utilize historical and real-time data to forecast potential threats?
  Can it proactively prioritize risks and vulnerabilities for preventative measures?

03

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Generative AI & Machine Learning

> Unlike their competitors, Microsoft has shown they're the leader when it comes to its AI functionality.

Head of IT & Security, Healthcare

03

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Generative AI & Machine Learning

The Microsoft Sentinel Advantage

Microsoft Sentinel is at the forefront of using Generative AI and Machine Learning to enhance threat detection and response, while augmenting analyst workflows for a more efficient and adaptive security operation.

Microsoft Sentinel delivers superior security operations efficiency by seamlessly embedding generative AI and machine learning (ML) throughout its platform. Central to this capability is Security Copilot, a generative AI assistant specifically designed to reduce analyst workloads by automating detection, investigation, and response workflows. Security Copilot synthesizes complex security data into clear, actionable incident summaries, offers intelligent recommendations, and streamlines response processes to accelerate threat resolution significantly.

The User and Entity Behavior Analytics (UEBA) built into Microsoft Sentinel leverages powerful ML algorithms to detect subtle anomalies in user and entity behavior, uncovering insider threats and compromised credentials that conventional tools might miss. Complementing this, Microsoft Sentinel's advanced threat detection applies sophisticated ML models to identify previously unknown threats rapidly and accurately, minimizing alert noise and ensuring analysts can focus on genuine threats. Microsoft Sentinel has been shown to reduce false positives (by up to 79%).

Microsoft Sentinel leverages machine learning algorithms combined with KQL queries over historical data to detect unknown threats. This improves prevention strategies by providing a comprehensive view of suspicious activities over time. This interconnected view, combined with AI, transforms the ability to manage security incidents dynamically and efficiently.

For organizations seeking customized analytic models, Microsoft Sentinel offers Bring Your Own Machine Learning (BYO-ML) capabilities via Azure Databricks/Apache Spark environment and Jupyter Notebooks, empowering security teams to tailor analytics precisely to their specific operational and threat landscape requirements.

Together, the AI and ML capabilities ensure proactive, automated, and intelligent threat management, essential for effectively countering today's complex cybersecurity challenges.

03

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Generative AI & Machine Learning

The Microsoft Sentinel Advantage

Explore Key Capabilities in Microsoft Sentinel

Microsoft Security Copilot

Leverages AI to enhance threat detection and incident response by providing actionable insights and guided recommendations. This capability helps security teams improve efficiency and accuracy, enabling them to address threats more effectively and maintain a robust security posture.

ML-Powered Behavior Analytics

ML-powered behavior analytics capabilities provide deep insights into user and entity behavior, helping to identify anomalies that may indicate potential threats. By analyzing patterns and behaviors, Microsoft Sentinel can detect insider threats, compromised accounts, and other malicious activities that traditional security measures might miss.

Historical Data Analysis with Machine Learning

Integrates machine learning algorithms with KQL queries for anomaly detection over historical data. This capability enhances the detection of suspicious activities and improves prevention strategies.

Machine Learning Features

Embedded AI assistance across the platform enhances threat detection, investigation, and response processes, improving effectiveness of SOC teams.

Bring Your Own Machine Learning (BYO-ML)

Microsoft Sentinel allows organizations to integrate their own machine learning models using Azure Databricks/ Spark environment and Jupyter Notebooks. This flexibility enables customized threat detection tailored to specific security needs, enhancing the overall effectiveness of security operations.

04

> AI is key to delivering a proactive understanding and detection of potential threats based on historical usage patterns.
>
> Security Leader, Healthcare

Advanced Detection & Response Automation

Advanced threat detection and response automation allows security teams to move beyond static rule-based detection by incorporating behavioral analytics, machine learning, and AI-powered correlation to uncover hidden and advanced threats.

Empowering Detection Engineering for Modern Threats

Security leaders today face increasingly complex cyber threats that routinely evade traditional, static rule-based detection methods. The dynamic nature of modern cyberattacks requires proactive detection engineering—leveraging behavioral analytics, real-time correlation, machine learning (ML), and automation—to identify hidden and advanced threats swiftly and accurately.

Static rules alone often lead to alert fatigue, high false positives, and delayed response, leaving organizations vulnerable.

Advanced threat detection and response automation integrates behavioral analytics, machine learning, and real-time AI-powered correlation to detect anomalies indicative of sophisticated, multi-stage threats. Machine learning models adapt continuously, improving detection accuracy over time, while AI-driven behavioral analytics establish baselines of normal behavior, swiftly highlighting suspicious activities. Integrating automated response capabilities reduces the time between detection and remediation, significantly limiting potential damages.

By adopting advanced threat detection and response capabilities, organizations dramatically reduce false positives, empowering security teams to prioritize genuine threats effectively. Automating detection and response processes ensures rapid containment, streamlined workflows, and greater analyst productivity—essential attributes for managing today's rapidly evolving threat environment.

04

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Advanced Detection & Response Automation

Checklist of Capabilities

When evaluating a SIEM solution, look for these capabilities:

- [ ] **Integrated Threat Intelligence**
  Does the SIEM integrate seamlessly with threat intelligence feeds for real-time threat context?
  Can it enrich alerts with contextual insights for enhanced analyst decision-making?
  Does it allow customizable integrations for tailored intelligence needs?

- [ ] **Advanced ML-Based Detection**
  Does the SIEM leverage machine learning to detect sophisticated, multi-stage threats?
  Can it analyze vast datasets in real-time to identify hidden or subtle attack patterns?
  Does it continuously adapt and refine its detection capabilities?

- [ ] **Behavioral Analytics**
  Does the SIEM establish and analyze behavioral baselines for users and entities?
  Can it detect anomalous behaviors associated with insider threats or credential compromise?
  Does it correlate behavioral anomalies with other security indicators for comprehensive insights?

- [ ] **Real-Time Threat Detection & Response**
  Does it process data in real-time for rapid threat identification and mitigation?
  Can it prioritize threats immediately with actionable intelligence?
  Does it scale efficiently without performance degradation?

- [ ] **Automated Incident Response**
  Does the solution provide automated playbooks and workflows for rapid threat containment?
  Can it streamline repetitive tasks, such as alert triage, incident classification, and reporting?
  Does it automate correlation of alerts to accelerate incident resolution?

Advanced Detection & Response Automation

> Leveraging Microsoft Sentinel's AI detection, machine learning and the analytics behind it makes our life a lot easier and enables us to fine tune and create new detection rules.

Security Leader, Healthcare

04

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Advanced Detection & Response Automation

The Microsoft Sentinel Advantage

Microsoft Sentinel empowers detection engineering with advanced AI/ML-driven threat detection and response to proactively identify and mitigate sophisticated cyber threats, enhancing security posture and minimizing the impact of incidents.

Microsoft Sentinel delivers advanced threat detection and response by empowering security teams with comprehensive, AI-driven detection engineering capabilities. Leveraging Microsoft's expansive threat intelligence, Microsoft Sentinel processes trillions of signals daily, enriching alerts with contextual insights for informed and effective threat mitigation.

Organizations benefit directly from Microsoft's global network of 10,000+ security experts who continuously monitor threats, deliver actionable intelligence, and support robust security postures.

The unified correlation model integrates XDR and SIEM alerts, correlating threats (up to 50% faster). Enhanced by AI/ML-driven automatic attack disruption, Microsoft Sentinel swiftly stops in-progress attacks, reducing organizational risk and attacker dwell-time.

To accelerate incident resolution, Microsoft Sentinel employs automated playbooks and rules, ensuring rapid and consistent responses through continuous monitoring and prioritized threat correlation. Embedded within these workflows, Security Copilot provides analysts powerful assistance at every investigation stage, reducing labor for sophisticated investigations (by up to 85%) and accelerating response tasks (by up to 22%).

Together, these advanced capabilities enable highly-effective detection engineering, dramatically enhancing detection accuracy, accelerating threat response, and significantly strengthening organizations' security posture against sophisticated cyber threats.

04

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Advanced Detection & Response Automation

The Microsoft Sentinel Advantage

Explore Key Capabilities in Microsoft Sentinel

Contextual Threat Intelligence

Microsoft Sentinel integrates with Microsoft's expansive threat intelligence feed, which processes trillions of signals daily. This integration enriches alerts with contextual information, providing security teams with the insights needed to make informed decisions and respond effectively.

Analyst Guidance with Security Copilot

Security Copilot helps streamline the investigation process by automatically correlating threat signals and security alerts, reducing noise and enabling analysts to focus on the most critical issues.

Multi-Stage Attack Disruption

Microsoft's unique correlation engine based on scalable machine learning algorithms, to automatically detect multistage attacks by identifying combinations of anomalous behaviors and suspicious activities observed at various stages of the kill chain.

Automation Playbooks and Rules

Automation rules and playbooks enable predefined responses to specific threats, ensuring consistent and rapid mitigation actions. These rules continuously monitor and analyze data to detect threats, generating alerts and incidents that are automatically correlated and prioritized for investigation.

Access to 10,000+ Microsoft Security Experts

Microsoft customers benefit from the support of Microsoft's global security team. This network of experts actively monitors threats, provides insights, and assists organizations in maintaining their security posture.

05

Ease of Configuration and Adoption

> One SIEM provider we evaluated doesn't integrate well with our enterprise environments.
>
> Security Leader, Healthcare

Simplifying SOC operations through the ease of configuration and adoption of SIEM enables organizations to streamline security processes, reduce operational complexity, enhance overall efficiency, and reduce costs.

Driving Effectiveness Through Simplicity

Managing a SIEM should empower security operations teams to focus on identifying and mitigating threats, not navigating the challenges of a complex system. Unfortunately, many SIEM solutions often involve intricate configurations, lengthy deployment timelines, and ongoing maintenance demands. These complexities frequently necessitate hiring external consultants, incurring additional costs, and requiring staff to undergo extensive training to achieve operational proficiency.

Such burdens not only strain budgets but also slow down response times and hinder the organization's agility in adapting to evolving threats. This reality makes simplified management a critical consideration when evaluating SIEM solutions. A modern SIEM should eliminate these pain points through intuitive design, streamlined operations, and automation, enabling faster deployment, ease of use, and seamless integration with existing infrastructure.

Simplified management translates to reduced costs, quicker ROI, and a security platform that scales with the organization. For SecOps teams, it means focusing less on system maintenance and more on proactive threat detection and response, ensuring a more effective and efficient security posture.

05

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Ease of Configuration and Adoption

Checklist of Capabilities

When evaluating a SIEM solution, look for these capabilities:

- [ ] **Rapid Deployment**
  Does the SIEM leverage a cloud-native architecture to enable quick start-up and eliminate hardware requirements?
  Does the SIEM provider have robust resources available to assist in configuration and adoption?

- [ ] **Ease of Use**
  Does the SIEM provide intuitive, customizable dashboards tailored to your SOC's needs?
  Are workflows streamlined for efficient investigation and incident response?

- [ ] **Automation and Pre-Built Features**
  Does the SIEM offer automated data ingestion, normalization, and analytics?
  Are there pre-configured detection rules to reduce the time and effort required for configuration?

- [ ] **Seamless Integration**
  Does the SIEM include native connectors for enterprise applications and multi-cloud platforms?
  Are APIs available for seamless integration with third-party tools?

- [ ] **Low Operational Overhead**
  Does the SIEM support automated updates, patches, and scalability to reduce maintenance requirements?
  Is role-based access control available to streamline secure team collaboration?

05

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Ease of Configuration and Adoption

> 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

05

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Ease of Configuration and Adoption

The Microsoft Sentinel Advantage

Microsoft Sentinel simplifies management by streamlining security operations, offering, reducing operational burdens, and enhancing SOC performance to significantly reduce security risks.

Microsoft Sentinel delivers streamlined security operations management by combining cloud-native flexibility, automation, and comprehensive integrations. Microsoft Sentinel accelerates deployment with 350+ pre-built connectors, including custom and codeless options, simplifying the integration of diverse data sources without complex coding. This reduces setup time, eliminating reliance on external consultants and minimizing onboarding training.

A rich repository of security resources, featuring 200+ Microsoft-developed solutions and 280+ community contributions, provides detection rules, customizable dashboards, and automated playbooks ready for immediate use. Comprehensive documentation, best practices, and guided deployment tutorials accelerate Sentinel adoption, ensuring ease of use for teams regardless of expertise level.

To further support ease of adoption, Microsoft provides comprehensive documentation, best practice guides, and deployment tutorials. These resources are tailored to help SecOps teams quickly set up, manage, and optimize Sentinel, ensuring both new and experienced users can easily adopt the platform.

Microsoft Sentinel's intuitive, single-pane-of-glass interface consolidates security data from multi-cloud and hybrid environments, offering real-time visibility and efficient incident management. Built-in automation features handle routine tasks such as data ingestion, alert correlation, and incident prioritization, significantly reducing operational overhead. Microsoft Sentinel's scalable design, granular access controls, and automated platform maintenance allow SecOps teams to focus on proactive threat detection rather than system administration, delivering simplified management and faster return on investment.

05

FIVE CAPABILITIES TO FUTURE PROOF THE SOC

Ease of Configuration and Adoption

The Microsoft Sentinel Advantage

Explore Key Capabilities in Microsoft Sentinel

350+ Out-of-Box Connectors

Supports over 350 out-of-the-box connectors, enabling seamless integration with diverse environments, including multi-cloud services and on-premises systems.

Single Unified Dashboard

Intuitive, single-pane-of-glass dashboard consolidates data from hybrid and multi-cloud environments. This unified interface enables real-time visibility, streamlined investigations, and simplified management of alerts and incidents.

Codeless Connector Platform

The Codeless connector capabilities enables organizations to easily integrate unique data sources in hours without the need for complex coding or development.

SOC Resources

Access a library of customizable security solutions to meet changing demands of your organization. Leverage out of the box connectors, detection rules, dashboards and playbooks.

Comprehensive Documentation

Microsoft provides detailed documentation, best practice guides, and deployment tutorials tailored to help SecOps teams quickly set up, manage, and optimize Sentinel. These resources ensure both new and experienced users can easily adopt the platform.

Why Microsoft Sentinel Stands Out

As a trusted enterprise leader, Microsoft leverages decades of cybersecurity expertise and an unparalleled global reach, supported by a team of over 10,000 engineers, researchers, and security experts. Microsoft Sentinel embodies this leadership, offering a proven, cloud-native SIEM platform capable of addressing the most complex security challenges with ease and efficiency.

While other SIEMs may excel in certain areas, none match Microsoft Sentinel's innovative roadmap, platform maturity, and extensive user base. Its ability to handle complex workloads is reinforced by numerous customer success stories, positive third-party reviews, and recognition in industry benchmarks, all of which establish Microsoft Sentinel as a trusted choice for over 25,000 organizations worldwide.

To further ensure customer success, Microsoft provides ongoing technical support alongside comprehensive, user-friendly documentation. These resources streamline onboarding, empower users of all skill levels, and enable seamless navigation across the platform, ensuring organizations can quickly realize value. With its unique combination of innovation, reliability, and support, Microsoft Sentinel is the ideal SIEM for securing today's dynamic digital landscapes.

Sources:

SIEM Market Research, A commissioned study by Microsoft, October 2024 Results are based on interviewed security leaders in enterprise organizations.

Forrester Total Economic Impact™ of Microsoft Sentinel, A commissioned study conducted by Forrester Consulting, March 2024 Results are based on a composite organization representative of interviewed customers.

Generative AI and Security Operations Center Productivity: Evidence from Live Operations, Microsoft study, By James Bono, Alec Xu, Justin Grana, November 24

Free trial

New users are welcome to trial Microsoft Sentinel free for 31 days, with no obligation to renew.

To help you achieve maximum impact during your free trial period, we've waived data ingestion and analysis charges (up to 10GB per day) for the full 31 days. Feel free to use as much data as you need during your trial, with additional data beyond the free 10GB daily limit charged using our simplified pricing tiers. This free trial is subject to a 20 workspace limit per Azure tenant.

Microsoft Sentinel is designed for you to start seeing returns immediately. Deploy built-in data connectors, analytics rules, playbooks, and more to get started, customizing the platform as needed.

Get started with trial

Microsoft Security

To learn more about modernizing your security operations and getting the most out of your Microsoft Sentinel experience:

- Learn more about Microsoft Sentinel
- Download Microsoft Sentinel Data Sheet
- Learn more about Microsoft Unified SecOps