Microsoft Security

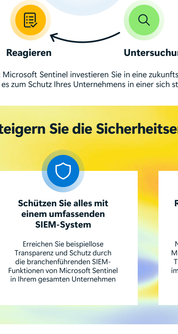
# Microsoft Sentinel

## KI-gestütztes SIEM, für moderne Sicherheit konzipiert

In der komplexen Cyberbedrohungslandschaft von heute stehen Security Operations Center (SOCs) vor großen Herausforderungen. Das zunehmende Volumen und die Raffinesse von Cyberangriffen führen dazu, dass die Analysts überfordert sind und Bedrohungen übersehen werden. Sicherheitsteams werden durch fragmentierte Tools, schlechte Transparenz und das Fehlen kritischer Funktionen in veralteten SIEM-Lösungen behindert. Dadurch sind sie anfällig für neue Bedrohungen.

Um diese Herausforderungen zu meistern, benötigen Sie ein zuverlässiges SIEM zur Sicherung Ihrer Multi-Cloud- und Multi-Plattform-Umgebung, das auf führender KI, Automatisierung und Threat Intelligenc basiert.

## Transformieren Sie Ihre Sicherheitsabläufe mit Microsoft Sentinel




Modernisieren Sie Ihre Sicherheitsabläufe mit Microsoft Sentinel – einem KI-gesteuerten, Cloud-nativen SIEM, das sich mit unübertroffener Effizienz und Intelligenz gegen sich entwickelnde Cyberbedrohungen wehrt.

- **Skalieren Sie Ihre Verteidigungsmechanismen** mit der Flexibilität und Kosteneffizienz der Cloud, um mit Ihrer Organisation zu wachsen
- **Profitieren Sie von umfassendem Bedrohungsmanagement** mit KI, SOAR, UEBA und TIP zur proaktiven Verteidigung
- **Schnellere Identifizierung neuer Bedrohungen** mit KI-gestützter Echtzeiterkennung und Machine Learning
- **Automatisieren Sie die Incident-Reaktion** , um Reaktionszeiten und Betriebslasten zu reduzieren.
- **Unterstützung der Compliance** mit branchenspezifischen Sicherheitsstandards und gesetzlichen Rahmenbedingungen

Mit Microsoft Sentinel investieren Sie in eine zukunftsorientierte SIEM-Lösung, die Ihrem Sicherheitsteam die Tools an die Hand gibt, die es zum Schutz Ihres Unternehmens in einer sich ständig verändernden Bedrohungslandschaft benötigt.

## Steigern Sie die Sicherheitsergebnisse mit einem innovativen SIEM

### Schützen Sie alles mit einem umfassenden SIEM-System

Erreichen Sie beispiellose Transparenz und Schutz durch die branchenführenden SIEM-Funktionen von Microsoft Sentinel in Ihrem gesamten Unternehmen

### Reagieren Sie auf dringende Sicherheitsbedrohungen schneller

Nutzen Sie die fortschrittlichste KI von Microsoft Sentinel und die beispiellose Threat Intelligence, um Angreifenden immer einen Schritt voraus zu sein und sich gegen zusammenführende Bedrohungen zu behaupten

### Skalieren Sie Ihre Sicherheit mit flexibler Cloud

Erweitern Sie Ihre Security Operations effizient, um mit der Cloud-nativen Architektur von Microsoft Sentinel mit dem Wachstum und der Komplexität Ihres Unternehmens Schritt zu halten.

## Zehn wichtige Microsoft Sentinel-Funktionen, um Ihr SOC zukunftssicher zu machen

Die komplexe Sicherheitsumgebung von heute erfordert eine SIEM-Plattform, die wichtige Funktionen in eine einheitliche Plattform integriert. Eine einheitliche Plattform hilft den Sicherheitsteams, ihre Abläufe zu optimieren, die Erkennung von Bedrohungen zu verbessern und die Reaktion auf Vorfälle zu beschleunigen, um einen umfassenden Schutz für Ihr Unternehmen zu gewährleisten.

1. **Cloudnative Architektur**
   Die Cloud-native Architektur von Microsoft Sentinel ermöglicht Sicherheitsteams eine mühelose Skalierbarkeit, bietet beispiellose Flexibilität und beseitigt die Kosten und Komplexität zusätzlicher Infrastruktur.
2. **Generative KI zur Bedrohungserkennung**
   Security Copilot mit generativer KI zur Erkennung und Antwort auf Bedrohungen kann innerhalb von nur drei Monaten zu einer um 30 % schnelleren mittleren Problemlösungszeit (Mean Time to Resolution, MTTR) führen und Ihre Sicherheitslage erheblich verbessern.
3. **Microsoft Sentinel integriert über 350 Datenschnittstellen und unterstützt verschiedene Umgebungen, einschließlich Multi-Cloud-Dienste und On-Premises-Systeme,** um einen ganzheitlichen Einblick in Ihre gesamte digitale Infrastruktur zu bieten.
4. **Flexible Datenverwaltung**
   Microsoft Sentinel bietet flexible Dateneinteilung und -verwaltung, mit der Sie alle Ihre Sicherheitsdaten erfassen, speichern und analysieren können, während Sie gleichzeitig die Kosten optimieren.
5. **Machine Learning und Automatisierung**
   Microsoft Sentinel verfügt über integrierte SOAR- und UEBA-Funktionen, die Orchestrierung, Automatisierung und fortschrittliche Verhaltensanalysen kombinieren, um die Erkennung von und Reaktion auf Bedrohungen zu optimieren und eine proaktive Identifizierung von Bedrohungen sowie ein effizientes Incident Management zu ermöglichen.
6. **Erweiterte Bedrohungskorrelation**
   Die Fusionstechnik von Microsoft Sentinel korreliert Daten aus verschiedenen Quellen, um komplexe, mehrstufige Angriffe zu erkennen, die herkömmliche Tools möglicherweise übersehen würden, und bietet so einen vollständigen Überblick über laufende Bedrohungen.
7. **Integrierte Threat Intelligence**
   Microsoft Sentinel enthält umfassende Bedrohungsintelligenz aus dem riesigen globalen Netzwerk von Microsoft und der Sicherheitscommunity und verbessert so die Fähigkeit Ihres Teams, Bedrohungen schnell und effektiv zu erkennen, zu analysieren und darauf zu reagieren.
8. **Proaktive Bedrohungssuche**
   Mithilfe der erweiterten Hunting-Funktionen können Sicherheitsteams proaktiv nach potenziellen Bedrohungen suchen und diese beseitigen, bevor diese Schaden anrichten.
9. **SOC-Optimierungen Einzigartige Empfehlungen** , die täglich generiert werden, bieten Möglichkeiten, den Wert von Daten zu verbessern, Kosten zu verwalten und die Sicherheitsabdeckung um 17 % zu erhöhen.
10. **Anpassbare Dashboards und Visualisierungen**
    Die anpassbaren Dashboards von Microsoft Sentinel bieten Sicherheitsteams maßgeschneiderte Echtzeit-Einblicke in intuitive Formate, die auf betrieblichen Anforderungen basieren. Dies ermöglicht eine schnellere Entscheidungsfindung und eine effektivere Reaktion auf Bedrohungen.

## Bewährter SIEM Leader

Kunden auf der ganzen Welt vertrauen darauf, dass Microsoft Sentinel ihre Unternehmen mit umfassenden Funktionen, breiter Abdeckung und starker Innovation zuverlässig vor den Bedrohungen von heute und morgen schützt.

**Ein SIEM Leader**[1]
im Gartner® Magic Quadrant™ for Security Information & Event Management

**Mehr als 25.000**
Organisationen auf der ganzen Welt vertrauen auf Microsoft Sentinel

**Umfassend**
SIEM-Funktionen: AI, SOAR, UEBA, TIP

**350+ Daten-Connectors**
für die umfangreiche Sammlung von Daten

## Microsoft Sentinel in Aktion: Sechs Wege zur Steigerung der Effizienz Ihres Teams

Microsoft Sentinel nutzt KI und Automatisierung, um jeden Aspekt Ihrer SIEM-Erfahrung zu verbessern, von der nahtlosen Implementierung bis zur fortschrittlichen Erkennung von Bedrohungen und der Unterstützung von Sicherheitsanalysts. Lernen Sie die sechs leistungsstärksten Möglichkeiten kennen, wie diese Innovationen die Wirkung Ihres Teams und die Gesamtsicherheitsleistung verbessern.

1. **Beschleunigen Sie die Implementierung durch automatisierte Migrationen**
   Sicherheitsfachkräfte erhalten Zugriff auf robuste Migrationstools, die den Übergang von bestehenden SIEM-Lösungen vereinfachen und eine nahtlose Datenintegration, die Beibehaltung von IT-Sicherheitskonfigurationen und minimale Unterbrechungen gewährleisten.
2. **Ausweitung des Schutzes auf weitere Assets**
   Sicherheitsfachkräfte können die Erfassung und Analyse von Sicherheitsdaten über Identitäts-, E-Mail-, Netzwerk-, Cloud-Anwendungen, Cloud-Services und Endpunkte hinweg mithilfe von sofort einsatzbereiten Connectors einfach erweitern.
3. **Beschleunigte Erkennung von und Reaktion auf Bedrohungen**
   Das Korrelationsmodul verwandelt Alarme schneller in Vorfälle. Security Copilot liefert Analysts Zusammenfassungen von Vorfällen, Auswirkungsanalysen und Empfehlungen für Abhilfemaßnahmen und verkürzt so die Reaktionszeit.
4. **Sprechen Sie jeden Anwendungsfall an**
   Sicherheitsteams können auf eine umfangreiche Bibliothek mit anpassbaren Sicherheitslösungen zurückgreifen, darunter mehr als 21.000 Github-Code-Beiträge, mehr als 200 von Microsoft entwickelte Regeln und mehr als 280 von der Community beigesteuerte Ressourcen für Erkennung, Dashboards und Playbooks.
5. **Verbesserung der Untersuchungen**
   Security Copilot vereinfacht komplexe Vorfälle durch das Zusammenfassen und Korrelieren von Daten in allen Systemen. So können Analysts den Umfang, die Auswirkungen und die Ursache von Bedrohungen schnell erfassen und so den Arbeitsaufwand bei der Untersuchung um 85 % reduzieren.
6. **Automatisieren Sie Routineaufgaben**
   Security Copilot automatisiert Routine-Tasks wie Protokollanalyse, Alert-Triage und Skriptüberprüfung sowie Datenkorrelation. So können sich Analysts auf strategische, höherwertige Aktivitäten konzentrieren.

## Nachgewiesene Auswirkungen auf das Geschäft

**SIEM-ROI**
Microsoft Sentinel macht als Cloud-native Lösung kostspielige Infrastrukturen überflüssig und senkt sowohl Investitions- als auch Betriebskosten. Unternehmen können ihre Sicherheitsabläufe nach Bedarf skalieren, was zu einer höheren Rendite führt.

**44 %**
geringere Gesamtkosten im Vergleich zu herkömmlichen SIEM-Anbietern[2]

**234 %**
ROI über drei Jahre[2]

**Produktivität von Sicherheitsanalysts**
Microsoft Sentinel steigert mit AI und Automatisierung die SOC-Effizienz und verkürzt die Zeit, die für die Erkennung und Reaktion auf Bedrohungen erforderlich ist. Durch die Automatisierung häufiger Aufgaben und die Korrelation von Warnungen zu priorisierten Incidents können sich Sicherheitsteams auf kritische Probleme konzentrieren.

**85 %**
Reduzierung des Arbeitsaufwands für fortgeschrittene Untersuchungen[2]

**79 %**
Verringerung der Fehlalarme[2]

**Sichtbarkeit des Risikoprofils**
Die einfache Skalierbarkeit der Cloud und die Out-of-the-Box-Verbindungen mit Datenquellen in Cloud-Diensten und anderen Plattformen erhöhen die Transparenz des Risikoprofils erheblich.

**35 %**
Verringerung der Wahrscheinlichkeit einer Datenschutzverletzung.[2]

**93 %**
Verkürzung der Zeit für die Konfiguration einer neuen Verbindung[2]

## Jetzt einsteigen

Um die Vorteile von Microsoft Sentinel zu erleben, beginnen Sie mit einer kostenlosen Testversion und erkunden Sie zusätzliche Ressourcen und Demos. Microsoft Sentinel ist die richtige Wahl für Unternehmen, die ihre Sicherheitsabläufe verbessern, Kosten senken und die Effizienz steigern wollen.

**Erfahren Sie mehr →** | **Preismodell →** | **Kundenreferenz →**

1. **Gartner, Magic Quadrant for Security Information and Event Management, Von Andrew Davies, Mitchell Schneider, Rustam Malik, Eric Ahlm, 8. Mai 2024** Gartner befürwortet keine Anbieter, Produkte oder Dienstleistungen, die in seinen Forschungspublikationen dargestellt werden, und rät Technologieanwendern nicht, nur die Anbieter mit den höchsten Bewertungen oder anderen Bezeichnungen auszuwählen. Die Marktbetrachtung von Gartner gibt die Meinung der Forschungs- und Beratungsorganisation von Gartner wieder und sollten nicht als Tatsachenbehauptungen ausgelegt werden. Gartner übernimmt keinerlei Gewährleistung für diesen Bericht, weder ausdrücklich noch stillschweigend, einschließlich der Gewährleistungen für die allgemeine Gebrauchstauglichkeit oder die Eignung für einen bestimmten Zweck. GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder seinen Tochtergesellschaften in den USA und international. Magic Quadrant ist eine eingetragene Marke von Gartner, Inc. und/oder seinen Tochtergesellschaften und wird hier mit Genehmigung verwendet. Alle Rechte vorbehalten.
2. **Forrester Total Economic Impact™ of Microsoft Sentinel**
   The Total Economic Impact(TM) Of Microsoft Sentinel, eine Auftragsstudie von Forrester Consulting, März 2024. Die Ergebnisse basieren auf einer zusammengesetzten Organisation, die repräsentativ für die befragten Kunden ist.

Microsoft Security