Microsoft Security

# Future-proof Your Security Operations Centre (SOC)

Safeguard your organisation with Microsoft Sentinel – a cloud-native, AI-enriched SIEM for modern security operations

To keep up with increasingly sophisticated threats, security operations centres need a modern solution. Built on leading AI, automation and threat intelligence, Microsoft Sentinel transforms the SOC with an innovative SIEM to confidently secure your multicloud, multi-platform environment.

| The challenge | Our solution | Why it works |
|---|---|---|
| Inflexible and costly on-prem SIEM | Scalable, cloud-native solution | Flexible data management allows for scaling of security coverage, optimising costs |
| Disparate or siloed tools | Unified security operations platform | A single interface with built-in critical capabilities: XDR, SIEM, SOAR, UEBA, GenAI and Threat Intelligence |
| Overwhelmed SOCs with alert fatigue causing inefficient response times | AI-assisted investigation and response | GenAI reduces the noise, prioritises incidents and helps accelerate response |
| Staying ahead of the latest threat actors and tactics | Robust threat intelligence | Leverages Microsoft Threat Intelligence to deliver timely and actionable insights |

The chart illustrates four challenges that were addressed, the Microsoft-provided solution, and the reasoning behind its effectiveness.

Looking to modernise your security operations while addressing increasing threats, tool complexity and cost pressures? **Microsoft Sentinel can help.**

It offers comprehensive detection, investigation, and response capabilities across multicloud and multi-platform environments. As part of Microsoft's unified security operations platform, Sentinel empowers analysts to seamlessly protect assets with native integrations of XDR, cloud security and exposure management.

**35%**
lower likelihood of data breach[1]

**44%**
less expensive than legacy solutions[1]

**234%**
potential ROI over three years[1]

## Scale security coverage

Adopt a cost-effective solution that can meet your evolving needs.

**Cloud-native platform**
As a cloud-native SIEM, Microsoft Sentinel offers unparalleled scalability, flexibility and efficiency.

**Flexible data management**
Expand protection with cost-effective tiered data storage options.

**Make it your own with dynamic recommendations**
Get **up to 17%** increased security coverage and **31%** better data utilisation.

## Gain comprehensive protection

Leverage robust, built-in capabilities to secure your entire multicloud, multi-platform ecosystem.

**Full-spectrum SIEM capabilities**
Built-in SOAR, UEBA, Threat Intelligence Platform (TIP) and Generative AI offer more effective threat management.

**Streamline the analyst experience**
Work seamlessly within Microsoft's unified security operations platform to get a single list of prioritised incidents, built-in response actions and other benefits that greatly improve efficiency and protection.

**Secure your entire digital estate**
**350+** out-of-the-box connectors deliver a **93%*** reduction in configuration time.

*Forrester Total Economic Impact™ study

## Catch emergent threats faster

Empower your security team to respond quickly and confidently with world-class AI and TI.

**Reduce noise with UEBA and machine learning**
Confidently detect threats with UEBA, then focus on what matters with ML that automatically correlates alerts into prioritised incidents, reducing false positives by 79%.

**Disrupt advanced attacks in real time**
Stop in-progress attacks with automatic attack disruption powered by AI and ML.

**Stay ahead of emerging threats with TI**
Gain actionable insights from the Microsoft Threat Intelligence community of 10,000+ world-class experts.

**Move at top speed with Microsoft Security Copilot**
With Security Copilot integrated, tasks are **22% faster** and investigation labour is reduced by **85%**.

## Trusted worldwide

As a leader in the 2024 Gartner® Magic Quadrant™ for Security Information and Event Management, Microsoft Sentinel is trusted by tens of thousands of organisations.

**Activate future-ready security today**

With Microsoft Sentinel, customers can confidently protect their organisations from today's and tomorrow's threats with unparalleled visibility, cloud flexibility and comprehensive coverage. Start planning your migration now to experience the power of an innovative, unified security operations platform.

[1] The Total Economic Impact™ of Microsoft Sentinel, Forrester Consulting, 2024