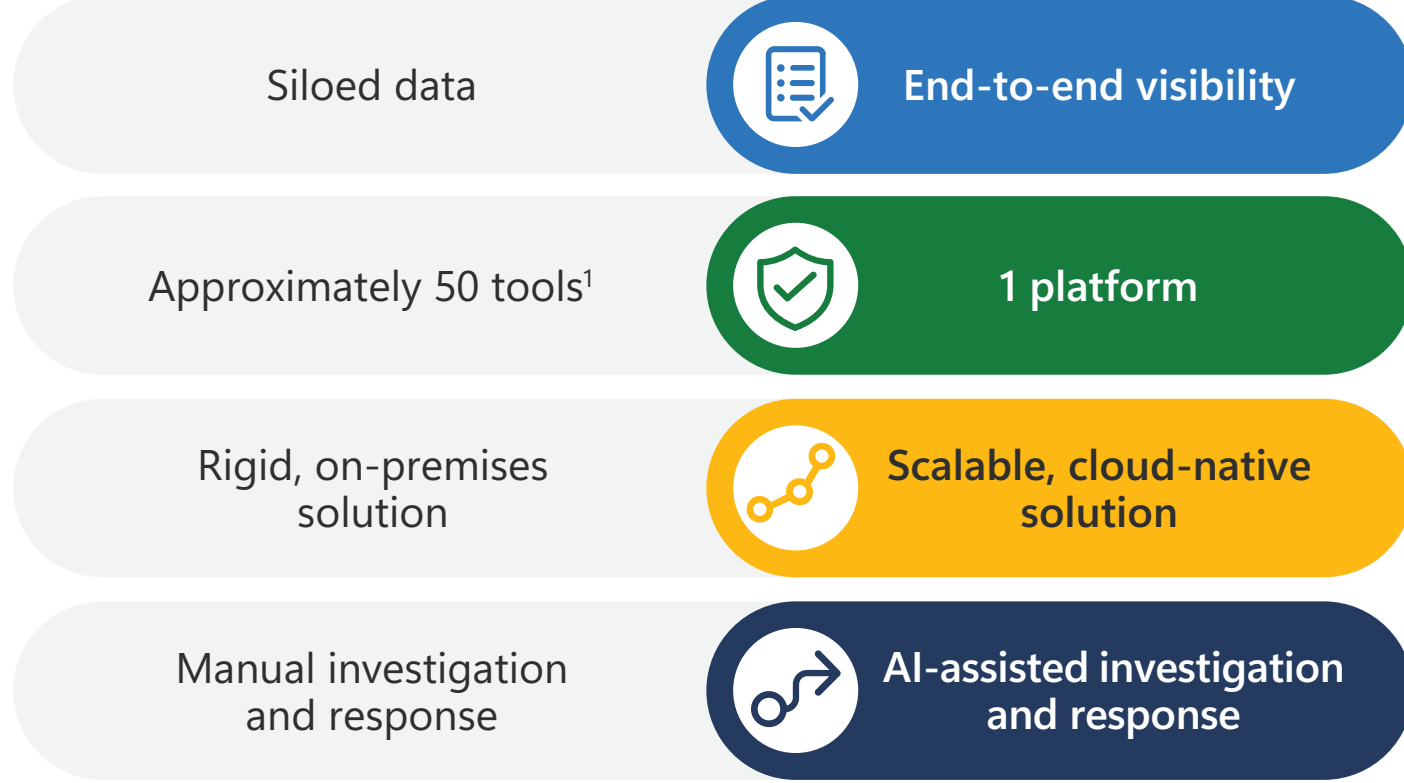
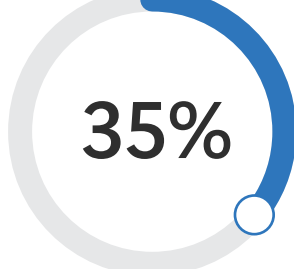


## Build future-ready security operations

With rising cyberthreats and limited resources, organizations need modern solutions that help them continuously adapt to an ever-evolving security landscape.



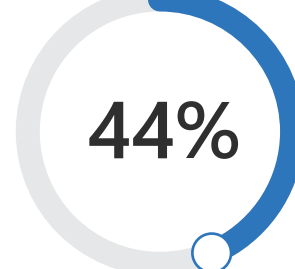
Bring innovation and efficiency to your security operations center (SOC) with Microsoft Sentinel, a cloud-based, AI-powered security information and event management (SIEM) solution.



35%  
reduction in likelihood of data breach<sup>2</sup>



234%  
return on investment over three years<sup>2</sup>



44%  
less expensive compared to legacy SIEM solutions<sup>2</sup>



### Stay ahead of cyberthreats with an end-to-end solution

Get a more complete picture of the cyberthreat landscape and spot patterns quickly by bringing together large volumes of data from across your enterprise.

- Uncover atypical user behavior and compromised identities with user and entity behavior analytics (UEBA).
- Understand the cyberthreat landscape and get context that helps accelerate your response with threat intelligence.
- Coordinate cyberthreat protection across people and tools with security orchestration, automation, and response (SOAR) capabilities.



Microsoft Threat Intelligence processes

65 trillion  
signals every day



### Empower analysts with an innovative security operations platform

Simplify protection of your endpoints, cloud apps, identities, and data. Microsoft Sentinel is built into a unified security operations platform that includes comprehensive extended detection and response (XDR) capabilities.

All these capabilities, all from one portal:

- XDR
- SIEM
- Threat intelligence
- UEBA
- SOAR
- AI



93%

decrease in time to configure and deploy new connections with pre-built SIEM content and out-of-the box functionality<sup>2</sup>



### Fine-tune security to your specific needs

Customize Microsoft Sentinel for your unique technology integrations, compliance requirements, or novel threats with more than 3,000 out-of-the-box, flexible tools, such as:

- Data connectors
- Workbooks
- Analytics rules
- Queries
- Playbooks

Plus, get recommendations that help you optimize your costs.



196

Microsoft-authored solutions



335+

Partner solutions



228

Connectors to third-party systems and apps, including Cisco, AWS, SAP, Fortinet, CrowdStrike, standard CEF, and SysLog



### Defend at AI speed

Outpace cyberthreats and empower analysts of all levels to build new skills with industry-leading generative AI. Take a proactive approach to security with:

- Prioritized, summarized incidents.
- Correlated alerts.
- Actionable recommendations.
- Step-by-step guidance.

And if you have your own innovative machine learning solution, bring it into Microsoft Sentinel to further customize the experience for your needs.



65%

reduction in time to investigate threats<sup>3</sup>



91%

reduction in time to onboard new security professionals<sup>3</sup>



88%

reduction in time to respond to threats<sup>3</sup>



79%

reduction in false positives over three years<sup>2</sup>

## Start planning your migration to Microsoft Sentinel

Reduce your costs and modernize security operations with a single platform for threat protection. A new migration tool for Splunk customers makes it faster and easier to migrate your SIEM.

Get started with Microsoft Sentinel today >

<sup>1</sup>February 2022 survey of 200 US compliance decision makers (n 100 599 999 employees, n 100 1000+ employees) commissioned by Microsoft with MDC Research

<sup>2</sup>The Total Economic Impact™ Of Microsoft Sentinel, a commissioned study conducted by Forrester Consulting, 2023

<sup>3</sup>The Total Economic Impact™ Of Microsoft SIEM and XDR, a commissioned study conducted by Forrester Consulting, August 2022