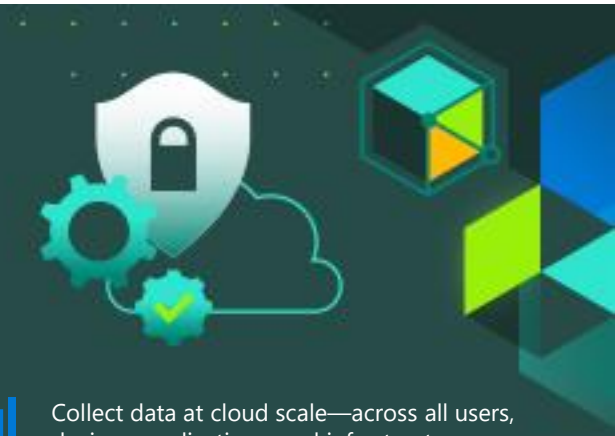
Microsoft Azure Sentinel



Cloud-native SIEM with built-in AI so security analysts can focus on what matters most.

Azure Sentinel is a cloud-native security information and event manager (SIEM) platform that uses built-in AI to help analyze large volumes of data across an enterprise—fast. Azure Sentinel aggregates security data from all sources, including users, applications, servers, and devices running on-premise or in any cloud, letting you reason over millions of records in a few seconds. It includes built-in connectors for easy onboarding of popular security solutions and supports standard formats like CEF and Syslog.

- Collect data at cloud scale—across all users, devices, applications, and infrastructure, both on-premise and in multiple clouds.
- Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft.
- Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- Respond to incidents rapidly with built-in orchestration and automation of common tasks.

Enhanced visibility of users and data on your enterprise network.

Data security is a never-ending challenge. IT organizations are required to keep up with regulations and protect intellectual property from targeted attacks and accidental exposure while simultaneously adapting to macro IT movements, such as the adoption of cloud applications, hybrid cloud environments and BYOD trends, all of which increase the ways data can leave your organization. The key is to gain visibility into user interactions with data and applications. Our integration with Azure Sentinel allows you to quickly zero in on what's happening in both your Azure environment and your physical network. Armed with this knowledge, you can apply a level of control based on specific user's risk and the sensitivity or value of the data.

CUSTOMER BENEFITS

- Gain visibility into what apps are being used by employees to quickly determine if they meet governance rules and avoid compliance issues
- Identify anomalous and risky user behavior in the cloud to restrict user activities that do not meet organizational standards.
- Export log events from Forcepoint CASB to Azure Sentinel in near real time for centralized visibility of activity across your entire enterprise, both on premise and in the cloud.
- Leverage pre-built workbooks within Sentinel to gain insights and visualize relevant events.

Learn More

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, Entrusted to safeguard organizations while driving digital transformation and growth. Our solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

Contact

www.forcepoint.com

The Microsoft Intelligent Security Association (MISA) is an ecosystem of independent software vendors that have integrated their security solutions with Microsoft to better defend against a world of increasingly sophisticated, fast-moving threats.
aka.ms/MISA

Member of Microsoft Intelligent Security Association

Microsoft