

Microsoft Azure Sentinel

Modernize security operations and focus on what matters most with cloud-native SIEM, powered by AI.

Azure Sentinel is a cloud-native security information and event management (SIEM) platform that uses built-in AI to 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. By eliminating on-premises infrastructure, it lowers costs by 48% compared to legacy SIEMs, as found by the commissioned [Forrester Consulting Total Economic Impact™ of Azure Sentinel](#) study. What's more, it reduces alert fatigue by 90% with machine-learning (ML) and analytics. With Azure Sentinel, your team can focus on what matters most: protecting your organization.



Collect data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.



Detect threats and reduce alert fatigue by as much as 90% using built-in analytics, ML, and unparalleled threat intelligence from Microsoft.



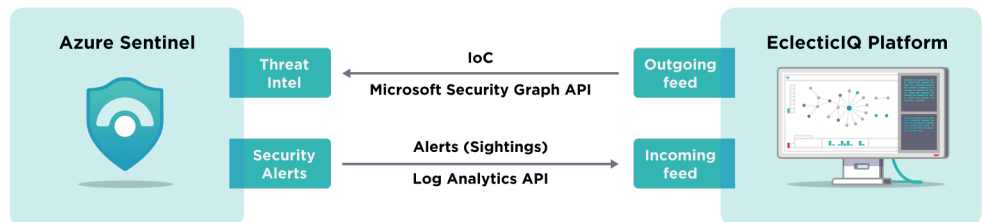
Investigate incidents and hunt suspicious activities at scale, with pre-built queries and workbooks from Microsoft security experts



Respond to incidents rapidly with built-in orchestration and automation of common tasks.


Helping customers harness the power of threat intelligence

EclecticIQ Platform is an analyst-centric Threat Intelligence Platform (TIP) that empowers threat analysts to perform faster, better, and deeper investigations while disseminating intelligence at machine-speed.



CUSTOMER BENEFITS

- EclecticIQ Platform provides a rich threat intelligence dataset
- EclecticIQ Platform allows you to significantly enhance your prevention and detection rules in Azure Sentinel.
- Important sightings and alerts are then fed back into EclecticIQ Platform for automatic dissemination and analyst review.

 **Learn More**

For demo or info contact

<https://www.eclecticiq.com/contact>

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

aka.ms/MISA

© 2019 Microsoft Corporation. All rights reserved. The information in this document represents the current view of Microsoft on the content. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Member of
Microsoft Intelligent Security Association

 Microsoft