Adopt and Deploy Microsoft Sentinel

Planning to deploy Microsoft Sentinel? Do you have any thoughts, like how to adopt Microsoft Sentinel with your business-critical services securely and dependably? If no, use our recommendations to get to see how to break down existing IT assets, evaluate what you have, recognize the advantages of Sentinel within your organization.

QDS is helping customers to provide clear and precise approach to adopt and deploy the Sentinel. These changes can have long-lasting effects on day-to-day efficiencies and overall business process and procedures.

Keys to success:

- Assessment and plan for the overall environment
- Technical readiness
- Deployment
- Enhancements
- Learnings
- Used cases.

How does Microsoft Sentinel work?

Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution. It provides intelligent security analytics, real-time threat detection, and automated response to help organizations manage and defend against cyber threats.

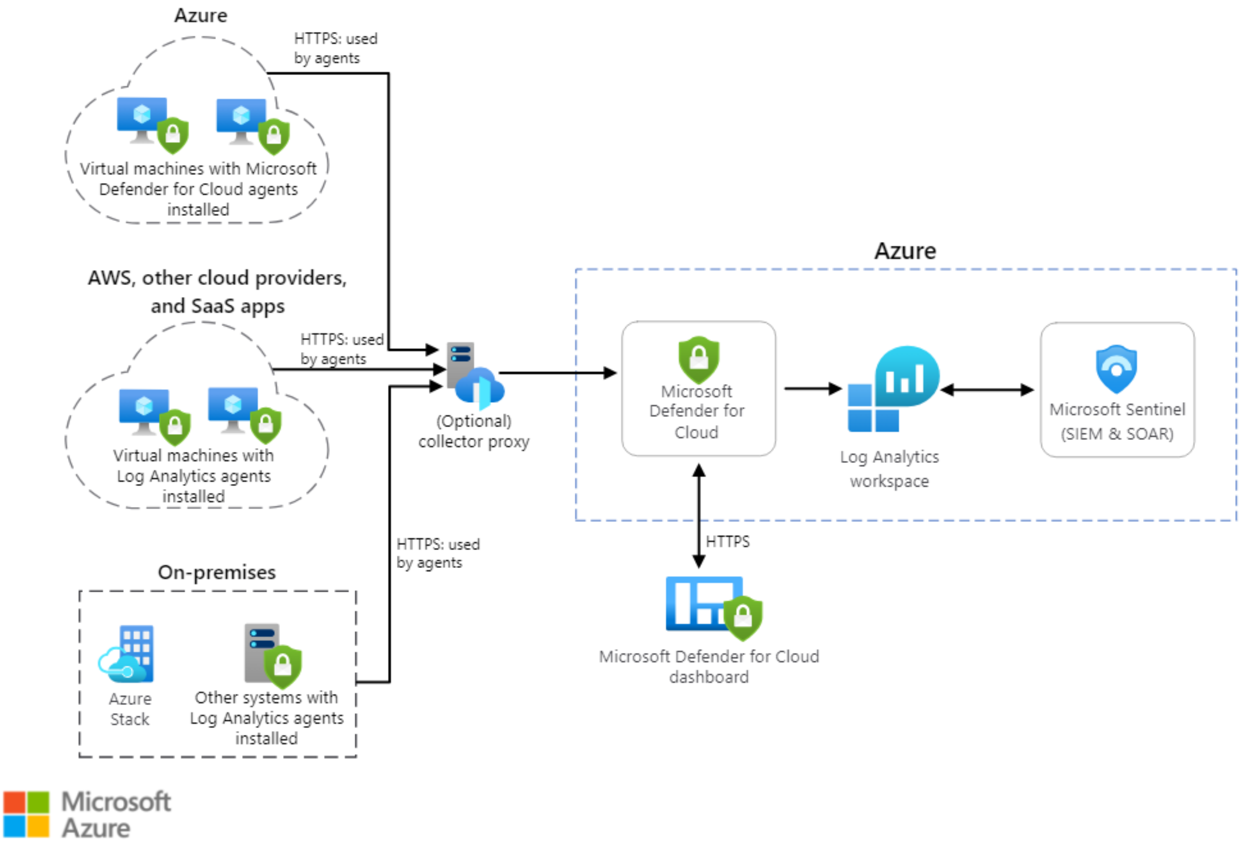
Microsoft Sentinel works by collecting and integrating data from a variety of sources, applying advanced analytics and AI to detect threats, and helping security teams investigate and respond effectively. It automates incident response through playbooks, enables proactive threat hunting, and provides a centralized view of security operations through customizable dashboards. Continuous updates and integrations with the Microsoft security ecosystem ensure that Sentinel remains adaptable to evolving threats and changing business requirements. This holistic approach makes Sentinel a powerful tool for modern cybersecurity, offering both real-time defense and long-term security posture improvements.

Key Features of Microsoft Sentinel’s Operation:

- Cloud-Native and Scalable: Sentinel is built on the Azure platform, making it inherently scalable and easy to deploy across cloud, hybrid, and on-premises environments.
- AI and Machine Learning: Sentinel leverages AI and machine learning to identify sophisticated threats, reducing false positives and catching advanced attack techniques that may evade traditional detection methods.
- Automation: Playbooks and automated workflows help streamline the security response, reducing manual intervention and speeding up recovery times.
- Integration with Microsoft Ecosystem: Sentinel seamlessly integrates with Microsoft’s broader security portfolio, including Microsoft Defender and Azure Security Center, allowing for more comprehensive protection.
- Customizable Detection: Through KQL and custom rules, Sentinel allows security teams to adapt to the unique needs and threats of their specific environment.

- Comprehensive Reporting and Compliance: Built-in workbooks and reports provide insights into security trends, incidents, and compliance statuses, making Sentinel valuable for both threat detection and audit requirements.

High-Level Azure Sentinel Architecture on Azure


Azure
HTTPS: used by agents
Virtual machines with Microsoft Defender for Cloud agents installed
AWS, other cloud providers, and SaaS apps
HTTPS: used by agents
Virtual machines with Log Analytics agents installed
On-premises
Azure Stack
Other systems with Log Analytics agents installed
HTTPS: used by agents
(Optional) collector proxy
Azure
Microsoft Defender for Cloud
Log Analytics workspace
Microsoft Sentinel (SIEM & SOAR)
HTTPS
Microsoft Defender for Cloud dashboard
Microsoft Azure

Engage with QDS to discuss in detail for your requirements, and plan to support you in adopting and deploying Microsoft Sentinel.

Contact US:

info@qdsnet.com
Phone: +974-44439900
Fax: +974-44432154
sales@qdsnet.com
www.qdsnet.com