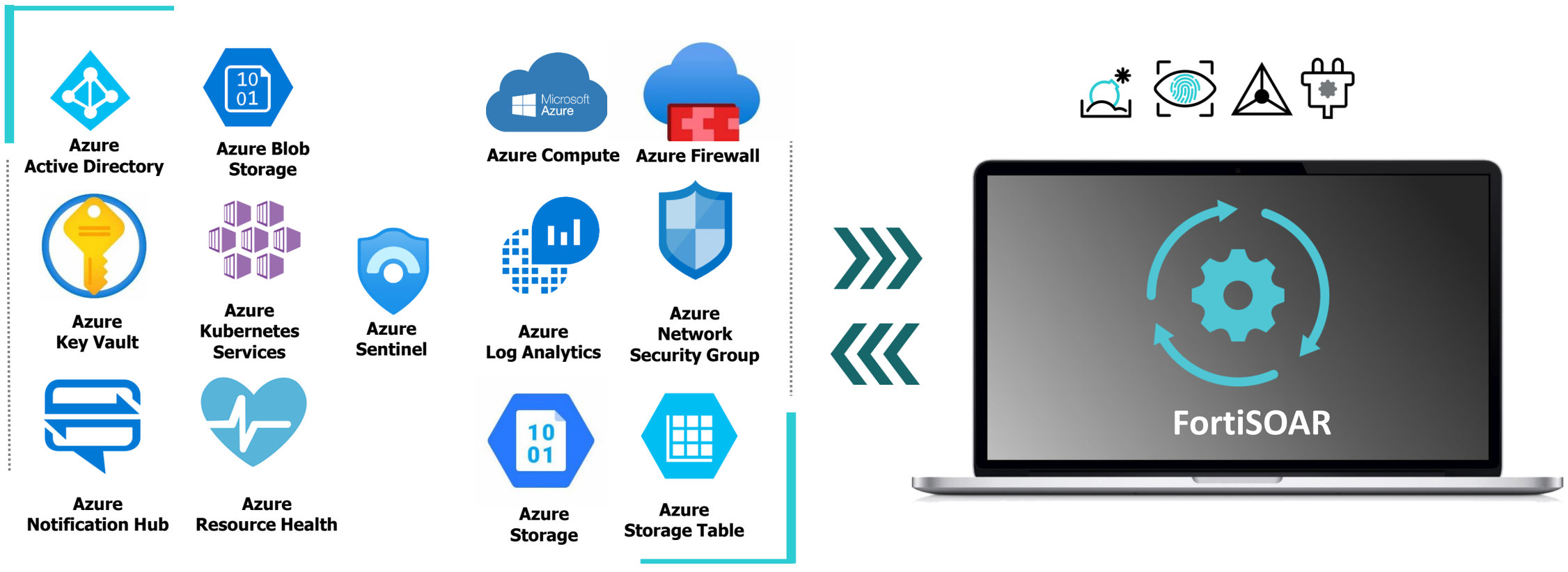
FortiSOAR Integration Brief

Streamlined **O**perations > **A**ccelerated **R**esponse

Overview

The collaboration between **Fortinet** and **Microsoft** brings together the strengths of FortiSOAR and Azure to offer a comprehensive solution for streamlined and accelerated cloud-security incident response. This integrated approach enables organizations to proactively address cloud security challenges, mitigate risks, and maintain a robust cloud-security posture in the evolving digital landscape.



About FortiSOAR

FortiSOAR enables organizations to centralize, standardize, and automate SecOps, IT, OT, and any critical enterprise operation. With broad integrations, rich use-case functions, prebuilt workflows, and simple playbook creation, FortiSOAR can help companies dramatically improve their cybersecurity posture, threat responsiveness, and the efficiency of any operation.

About Microsoft Azure

Azure is a leading public cloud computing services provider globally, provides an enterprise-grade highly reliable, scalable, low-cost computing platform in the cloud that powers businesses in countries around the world. Customers across all industries are using the Azure cloud computing platform to launch applications across a wide variety of use cases taking advantage of the following benefits offered by Azure: low cost, agility, elasticity, security, openness, flexibility, reliability and compliance.

Integration at a Glance

Connectors

- Azure Active Directory
- Azure Blob Storage
- Azure Compute
- Azure Firewall
- Azure Key Vault
- Azure Kubernetes Services
- Azure Log Analytics
- Azure Network Security Group
- Azure Notification Hub
- Azure Resource Health
- Azure Sentinel
- Azure Storage
- Azure Storage Table

Use Cases

- Streamline and Automate Cloud Incident Response
- Forensic Analysis Within Cloud Infrastructure
- Cloud Security Orchestration For Hybrid Model
- Comprehensive Visibility To Cloud Security Posture With Bi-Directional Communication
- Unleash the Power of Cloud With Enhanced Threat Detection and Response for Unrivalled Security

Content Hub and Community

An expanding library of connectors, playbooks, solutions, videos, and community contributions drive continued benefits

https://fortisoar.fortinet.com

Use Case #1 - Streamline and Automate Cloud Incident Response

Integrating Active Directory (IAM) with FortiSOAR provides security teams with enhanced visibility into user activities and potential security risks. By analysing data from Active Directory in collaboration with other security tools, security analysts swiftly identify suspicious behaviour, detect potential insider threats, and proactively respond to security incidents.

When an incident is detected, the analyst can leverage Active Directory to automatically gather relevant user information and perform actions such as disabling accounts, resetting passwords, or revoking access to sensitive resources. This not only reduces mean time to respond **(MTTR)** to cloud security incidents but also minimizes the risk of human error. Thereby, streamlining and automating the entire process of cloud-incident response.

Use Case #2 - Forensic Analysis Within Cloud Infrastructure

By leveraging the integration between FortiSOAR and Azure Log Analytics, organizations can effectively collect forensic data from log files, examine network traffic, review system configurations, and examine storage and compute resources within the cloud environment. This integration enhances the incident response capabilities and enables thorough forensic analysis using the log data stored in Azure Log Analytics.

Once you have defined and executed a log search query in FortiSOAR, you can save the search and its results for future reference. This is useful for recurring investigations or monitoring specific security events.

Use Case #3 - Cloud Security Orchestration For Hybrid Model

Sentinel and FortiSOAR combine their capabilities to provide enhanced visibility into security incidents across both the cloud and on-premise systems. This ensures that security teams have a holistic view of the security landscape and can effectively respond to incidents regardless of their origin.

Additionally, the integration allows for easy identification of MITRE ATT&CK techniques associated with the alerts. This empowers security analysts to understand the attack techniques being employed by threat actors and take appropriate actions to mitigate the risks.

Importantly, FortiSOAR acts as a single trusted pane of glass for managing and responding to security incidents across the hybrid environment. This ensures that security teams do not lose sight of incidents associated with either the cloud or the on-premise infrastructure.

Use Case #4 - Comprehensive Visibility To Cloud Security Posture With Bi-Directional Communication

Sentinel can provide valuable threat intelligence insights to FortiSOAR, which can be used to enhance incident response and automate threat hunting. Similarly, FortiSOAR can provide additional threat intelligence feeds or enrichment data to Sentinel, improving the accuracy of threat detection and analysis. This bi-directional communication between Sentinel and FortiSOAR for sharing threat intelligence gives visibility that is more comprehensive. Thereby, enhancing the overall cloud security posture.

Use Case #5 - Unleash the Power of Cloud With Enhanced Threat Detection and Response for Unrivalled Security

Azure Firewall monitors network traffic, detecting potential threats, while FortiSOAR integrates with it to receive real-time alerts. FortiSOAR can then take automated actions like blocking IP addresses and updating firewall rules to mitigate identified threats and prevent future incidents.