FORTINET | **SpryIQ**

Fortinet and Freshworks Security Solution

Streamlined Incident Management with Automated Ticket Creation and Synchronization

Executive Summary

Fortinet FortiSOAR and Freshworks Freshdesk offer streamlined incident management by automating the creation and synchronization of tickets when security alerts are triggered. This integrated solution enhances collaboration among security analysts and support teams, ensuring efficient incident response workflows.

The Challenge of Managing Security Incidents

Organizations often face challenges in efficiently managing security incidents, resulting in manual processes and delayed responses. Key requirements include the need for automated ticket creation and synchronization to streamline incident management workflows.

Joint Solution

The Freshservice Desk MSP connector facilitates integration between FortiSOAR and Freshdesk, enabling automated synchronization of security alerts and ticket creation.

Solution Components

Freshworks Freshdesk

Cloud-based customer support software designed to streamline customer communication and incident management processes.
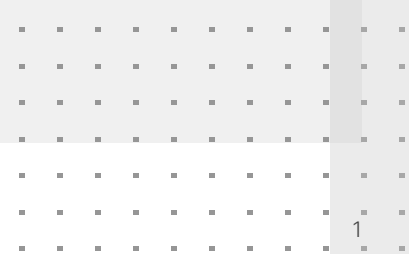
Fortinet FortiSOAR

FortiSOAR enables organizations to centralize, standardize, and automate IT/OT security operations and critical enterprise functions. With broad integrations, rich use-case functions, hundreds of prebuilt workflows, and simple playbook creation, FortiSOAR supports best-in-class procedures tailored to customers' specific needs. FortiSOAR is an integrated security operations hub that helps to protect organizations from attack. FortiSOAR is also designed to function as the central hub for threat management by automatically triaging, enriching, and assessing alerts. Routine alerts are automatically handled and closed, while priority alerts are additionally mapped to the MITRE ATT&CK framework and intelligently grouped into incidents for deeper investigation. Recommended playbooks augment rich investigation features, suggest actions, and can execute complete remediation steps. Escalated incidents can also activate a full war room that facilitates collaboration and includes detailed forensic logging. And analysts can take action anywhere and anytime via the FortiSOAR secure mobile application.

Solution Components

- Fortinet FortiSOAR
- Freshworks Freshdesk and Freshservice Desk MSP connector

Solution Benefits

- Efficient incident response
- Improved collaboration among teams
- Enhanced incident visibility and tracking
- Consistent data integrity across platforms
- Comprehensive security protection with the Fortinet Security Fabric
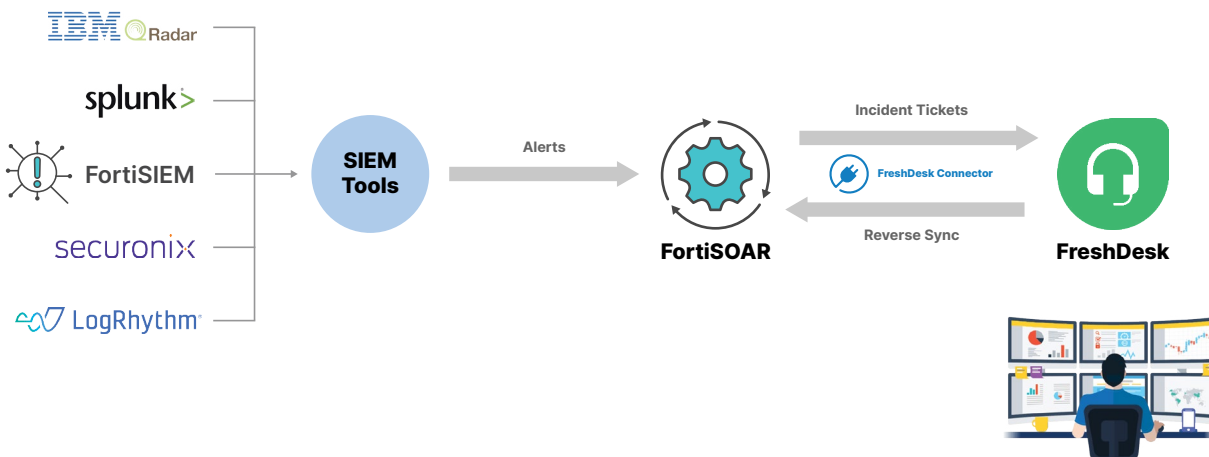
FORTINET. FABRIC-READY

Figure 1: Freshworks and Fortinet integration architecture

Solution Integration

When an alert is triggered within FortiSOAR from SIEM tools, the integration facilitates the creation of a corresponding ticket in Freshdesk, including pertinent incident details. Any updates made to the ticket in Freshdesk can be instantly synchronized back to FortiSOAR and vice versa, ensuring stakeholders maintain real-time visibility into the incident's status and progress.

Joint Use Cases

Use case #1: Automated ticket creation and synchronization

The integration between FortiSOAR and Freshdesk automates ticket creation and synchronization when a security alert is triggered. This enhances incident response by ensuring seamless collaboration between security analysts and support teams.

Use case #2: Real-time alert update synchronization with ticket changes

The seamless communication between FortiSOAR and Freshdesk for incident updates ensures real-time synchronization between FortiSOAR alert updates and Freshdesk ticket modifications, facilitating efficient communication and alignment between incident management systems.

Use case #3: Bidirectional ticket details synchronization between FortiSOAR and ticketing system

Bidirectional synchronization between FortiSOAR and the ticketing system ensures that ticket modifications are accurately reflected in associated FortiSOAR alerts, enabling organizations to maintain data consistency and improve incident management efficiency.

About SpryIQ Technologies Private Limited

SpryIQ, an Essential Technology Partner specializing in Cyber Security Services, is dedicated to delivering innovative and reliable solutions to businesses of all sizes. As a Fortinet Technology Alliance Partner, SpryIQ actively contributes to building new integrations for FortiSOAR. With deep expertise in various Fortinet offerings, particularly FortiSOAR and FortiSIEM, SpryIQ assists Fortinet customers in automating their incident response through custom response playbooks using FortiSOAR. SpryIQ's team of experts has years of experience in the software development industry and utilizes the latest tools and technologies to create customized software solutions tailored to meet your unique business needs.

F⌀RTINET   www.fortinet.com