FORNETIX®

Splunk Integration

Take Command of Your Data With Powerful Monitoring, Analytics, and Automated Response

Bringing cyber situation awareness to enterprises through the integration of Fornetix Key Orchestration and Splunk

Capability Overview

Achieving full cyber situational awareness is a critical component in securing your most important assets. Tight integration between Fornetix Key Orchestration (KO) and SIEMs such as Splunk brings monitoring and analysis to all activity on your network. KO's forensic-level logging in Common Event Format (CEF) allows Splunk to easily consume comprehensive log data.

By leveraging RESTful services from KO, Splunk is capable of rapid response by immediately issuing commands to Key Orchestration and its network of connected technologies. When triggered by an alert, Key Orchestration can automatically execute complex encryption actions from the customer's cyber defense playbook — actions such as revoking credentials, tearing down a VPN tunnel, or even initiating an enterprise-wide key rotation.

The power of this combined approach allows visibility into the crypto domain and gives users insight into how other systems are consuming encryption key management for data-at-rest, data-in-motion, and data-in-processing solutions.

Key Features

Common Event Format

The syslog output from Key Orchestration utilizes CEF to allow simple and easy integration into leading SIEM providers like Splunk. Every action performed within KO is meticulously logged.

Dashboards

Operations performed by KO are easily added to custom dashboards within Splunk, whether they are internal KO operations or those aligned with other services.

Custom Scripting & API

Using secure APIs from Key Orchestration, Splunk is able to execute Key Management Interoperability Protocol (KMIP) operations as well as custom scripts (compositions). SOC operators can develop automated crypto playbooks that respond to alerts or other events as required.

Alerts

Key Orchestration actions such as running compositions or triggering key management operations can be executed as responses to alerts from Splunk.

Policy & Positional Security

Key Orchestration's policy engine and positional security allow operators to set up specific controls around key management and other operations. As a policy decision point, KO can become a secure coordination point for cyber defense.

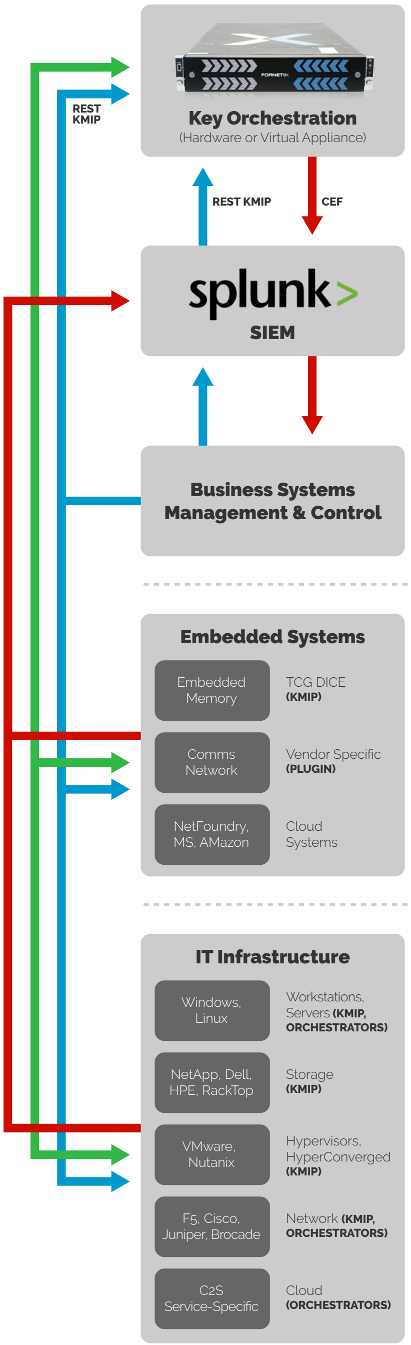
New to Key Orchestration?

Visit our website or search 'Fornetix' on Facebook, Twitter, and LinkedIn for more information about our powerful encryption key management solution and how it can help secure your organization's data.

Architecture

Legend

- 🔴 MONITORING
- 🔵 COMMAND & CONTROL
- 🟢 KEY MANAGEMENT



REST KMIP
Key Orchestration
(Hardware or Virtual Appliance)
REST KMIP
CEF
splunk>
SIEM
Business Systems Management & Control
Embedded Systems
Embedded Memory
TCG DICE (KMIP)
Comms Network
Vendor Specific (PLUGIN)
NetFoundry, MS, AMazon
Cloud Systems
IT Infrastructure
Windows, Linux
Workstations, Servers (KMIP, ORCHESTRATORS)
NetApp, Dell, HPE, RackTop
Storage (KMIP)
VMware, Nutanix
Hypervisors, HyperConverged (KMIP)
F5, Cisco, Juniper, Brocade
Network (KMIP, ORCHESTRATORS)
C2S Service-Specific
Cloud (ORCHESTRATORS)