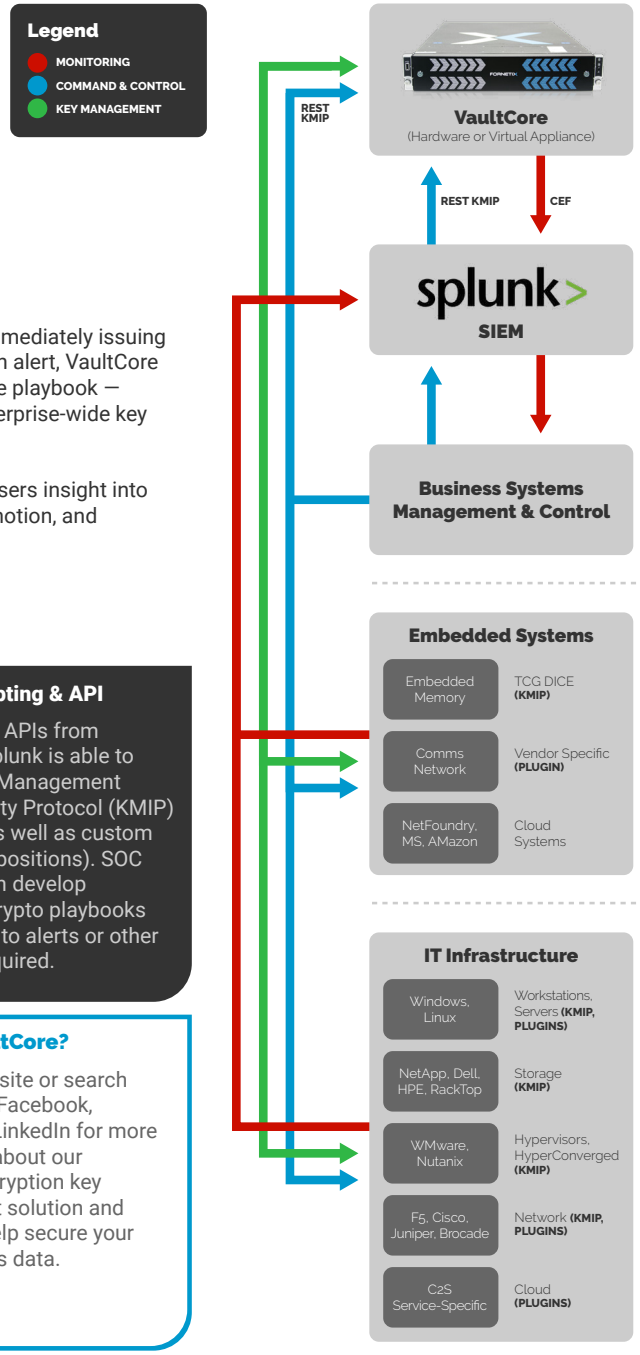
FORNETIX®

Splunk Integration

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

Architecture

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



Capability Overview

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

By leveraging RESTful services from VaultCore, Splunk is capable of rapid response by immediately issuing commands to VaultCore and its network of connected technologies. When triggered by an alert, VaultCore 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 VaultCore utilizes CEF to allow simple and easy integration into leading SIEM providers like Splunk. Every action performed within VaultCore is meticulously logged.

Dashboards

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

Custom Scripting & API

Using secure APIs from VaultCore, 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

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

Policy & Positional Security

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

New to VaultCore?

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.

Fornetix.com | Linkedin.com/company/fornetix | Twitter.com/fornetix | Facebook.com/fornetix | 1-844-539-6724 | 5123 Pegasus Ct, Suite X, Frederick, MD 21704

FORNETIX®