



Solution Brief

MobileIron + Splunk Turn Mobile Data into Security Intelligence

SOLUTION BENEFITS

Turn mobile data into operational intelligence with a holistic view of the entire IT infrastructure.

Quickly identify compliant vs. non-compliant devices, reasons for non-compliance, location, OS, and more.

See which mobile devices are violating regulations such as HIPAA, PCI, and CJIS.

View historical trends of system health that include metrics such as CPU, memory, and disk space.

ABOUT SPLUNK

Splunk Inc. provides the leading platform for Operational Intelligence. Over 10,000 customers use Splunk® software to search, monitor, analyze and visualize their machine-generated big data.

MobileIron and Splunk have joined forces to help customers achieve greater visibility into their mobile data. With these powerful insights, IT can intercept security threats, meet compliance requirements, and maintain the overall health of their information systems.

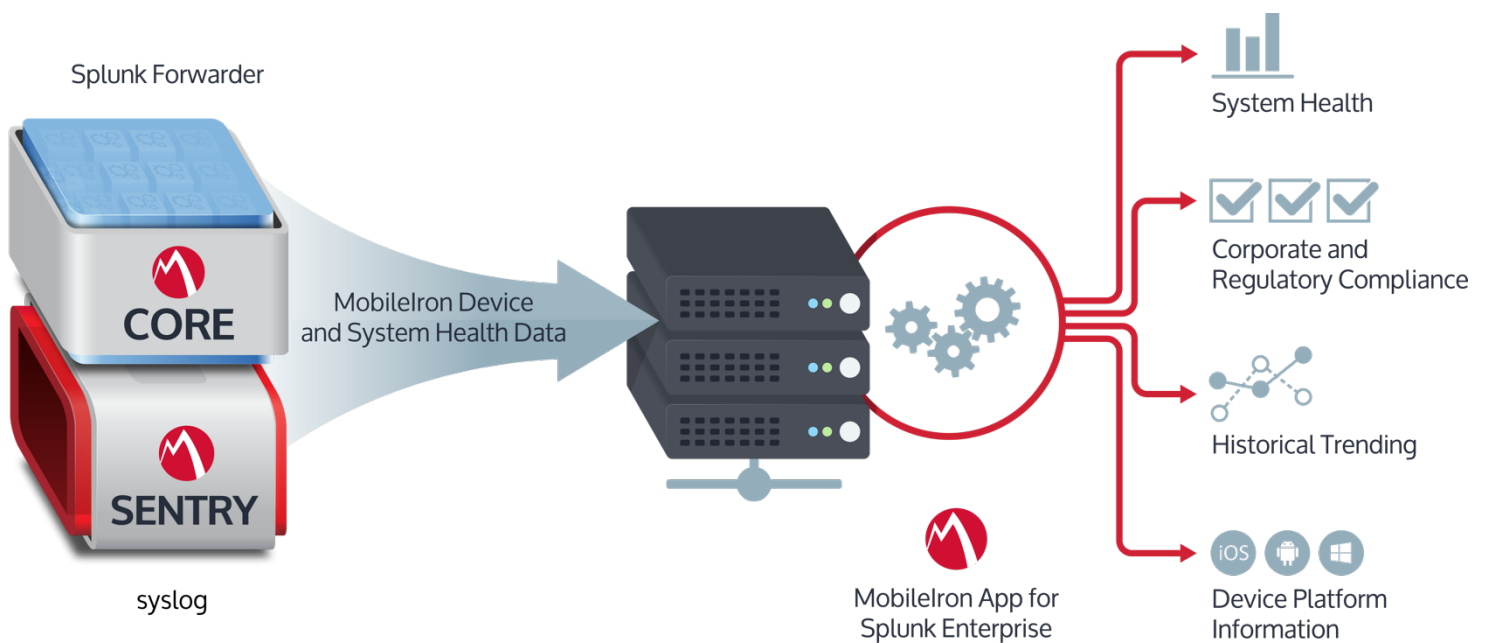
Business Challenge

The inability to view mobile data can create a security blind spot for IT organizations. Mobile data can enable insights that help IT identify security gaps and meet compliance standards, but this data is typically in the silo of the enterprise mobility management (EMM) infrastructure and inaccessible to conventional security solutions. Turning mobile data into operational intelligence therefore requires a solution that provides a holistic view across the entire IT infrastructure.

How the Joint Solution Works

MobileIron's integration with Splunk software addresses the critical security, compliance, and operational requirements IT organizations must manage every day. Together, MobileIron and Splunk enable IT admins to forward system health information and mobile device data to a Splunk app designed to work with MobileIron Core. They can then generate security and compliance visualizations from this data and quickly pinpoint any system health or mobile device issues. Admins can also map relevant mobile device information to the Splunk Common Information Model (CIM), which helps to correlate security events across the infrastructure and services such as firewalls, VPN gateways, and servers.





Key Features

The MobileIron solution for Splunk Enterprise is available with MobileIron Core and includes two key components: the Splunk Forwarder and the MobileIron App for Splunk Enterprise.

Splunk Forwarder: The Splunk Forwarder allows data contained within the MobileIron EMM platform to be forwarded to the Splunk indexers.

MobileIron App for Splunk Enterprise: This app is designed to help IT visualize the data aggregated from the Splunk Forwarder by providing granular views into mobile data and overall system health. Dashboard views allow IT to quickly identify non-compliant devices, understand why they are out of compliance, view statistics of device compliance by operating system, monitor devices anywhere in the world, and maintain availability and overall system health.

What it Does For You

With the ability to visualize critical device data and break it down by operating system, geographical region, and other key metrics, security teams can quickly identify any issues affecting their environment. For example, geographical views allow admins to view the spread of devices around the world and analyze compliant vs. non-compliant devices by region and operating system. Admins can even zoom in to street level to identify the exact location of a non-compliant device.

In addition, IT admins can also monitor historical trends and set up alerts whenever system health falls below certain thresholds.

The MobileIron App for Splunk Enterprise also enables IT admins to monitor mobile device compliance with HIPAA, PCI, and CJIS regulations.