splunk>

FACT SHEET

Splunk App for Centrify Insight

Delivering the Control, Visibility and Security of Your Cross-Platform Data Center

The Challenge

Heterogeneous IT environments have become the standard both for server operating systems and the applications that run on them. With diverse operating systems and applications spanning physical, virtual and cloud-based environments, along with more Java- and web-based applications, the trend toward diversity is only accelerating.

Not surprisingly, interoperability among these diverse platforms is a key concern for IT managers. Reducing complexity has become even more critical in the past few years as an uncertain economy has put renewed focus on reducing expenses and leveraging existing investments.

Meanwhile, security and compliance have become even more critical as organizations cope with a dynamic business environment that includes mergers and acquisitions, staff reductions and outsourcing.

The Solution

Splunk Enterprise and Centrify can deliver the control and visibility you need to establish and manage the security of your cross-platform data center. You get a deeper insight into Active Directory status and the local system changes that affect the security and compliance of your environment.

Centrify Suite

The Centrify Suite lets you centrally control, secure and audit the access to your cross-platform systems and applications by leveraging your existing Active Directory infrastructure. Built on an integrated architecture, the Centrify Suite enables organizations to strengthen security, enhance regulatory compliance initiatives, reduce IT expense and complexity and improve end-user productivity. The Centrify Suite—consisting of DirectControl, DirectAuthorize, DirectAudit, DirectSecure and DirectManage—delivers secure authentication and single sign-on, role-based access control, privileged identity management, user-level auditing, server isolation and encryption of data-in-motion for the industry's broadest set of heterogeneous systems and applications.

Splunk for Active Directory

Splunk is perfectly suited for monitoring and auditing Active Directory logs because it matches the flexibility of Active Directory and can scale linearly as your Active Directory environment grows. Splunk can manage and analyze any data from any source type without requiring connectors. In addition, Splunk can not only manage Active Directory's huge amount of data for trending and compliance requirements, it can handle complex event processing for real-time monitoring and alerting.

Splunk is the engine for machine data that gives system administrators and security specialists visibility and control of highly complex Active Directory environments. Splunk aggregates, correlates and monitories all security event logs and changes to AD schema.

Why Splunk for Centrify Insight

Centrify Suite can easily create reports that show what systems users have accessed and reveal their *NIX attributes. All of this information is centrally stored in Centrify Zones within Active Directory, making it easy to manage and report. Using Splunk for Centrify Insight you can also determine:

- Who Zone-enabled a user?
- When *NIX attribute(s) were changed?
- What Zone-groups have been modified?
- What changes were made to Active Directory Users, Groups and Computer objects?

Active Directory Security Insights

Understanding and monitoring changes to the settings of Active Directory Objects can mean the difference between the right or wrong person having access to proprietary data or specific applications. The ability to be alerted to changes, see the change deltas and know who made the changes, supports the security and compliance best practice of separation of duties. Changes to Active Directory objects (users, groups and computers) and the timing (adds, modifies, deletes or undeletes) can indicate malicious activity and the first step in the compromise of your proprietary data.

Splunk App for Centrify Insight

Centrify Insight is a Splunk application that listens to Active Directory domain controllers and security event logs as well as *NIX syslog and Centrify Suite logs to provide the insight you need to answer security and forensic questions about Centrify secured systems. This data is captured and summarized into a series of reports and metrics that can be displayed, reported, alerted and analyzed at a granular level. Centrify Insight provides the visibility you need with an easy-to-use search interface and pre-built interactive reports based on the mature and popular Splunk platform. And best of all, Centrify is making this available for free!

About Splunk

Splunk collects, indexes and harnesses machine data generated by an organization's IT systems and infrastructure—physical, virtual and in the cloud. Machine data is unstructured, massive in scale and contains a categorical record of all transactions, systems, applications, user activities, security threats and fraudulent activity.

Splunk has the flexibility to collect all your data sources, the scalability to work across your entire infrastructure and the power to provide deep drilldown, statistical analysis and real-time, custom dashboards to anyone in your organization.

About Centrify

Centrify delivers integrated software solutions that centrally control, secure and audit access to cross-platform systems and applications using Microsoft Active Directory. Centrify is deployed in production on hundreds of thousands of mission critical servers. Over 3,000 organizations rely on Centrify's identity consolidation and privilege management solutions to reduce IT expenses, strengthen security and meet compliance requirements.

Features

- Real-time views and alerts of scheduled or ad-hoc policy changes
- Intuitive visualizations of key performance indicators (KPIs) using pre-built dashboards that monitor configuration changes
- Timely alert-setting to notify you when specific changes are made to Active Directory
- Robust scheduling and reporting
- Customizable graphics and dashboards
- Scalable, universal real-time log event collection and indexing from any application, server, network or security device
- Easy-to-use interface facilitates communication of status and issues across the organization

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

250 Brannan St, San Francisco, CA, 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.splunkbase.com