

# Centrify Infrastructure Services for Splunk

## Seamless SIEM integration to thwart in-progress attacks

Data breaches are constantly on the rise — according to a recent Verizon report, 70% of breaches involving insider misuse took months or years to recover from the damage. Identity-related attacks are becoming more sophisticated and target environments with too many shared accounts and admins with too much privilege. To protect against these types of attacks, organizations need visibility across the privileged access activity in their environment to identify risk and take action against attacks already in progress.

### The Need for a Centralized View

High-profile breaches, insider threats and numerous regulatory and industry security standards are highlighting the risks associated with poorly managed privileged access to corporate systems. In many organizations, administrators are routinely granted broad privileges to accomplish narrow tasks. Malicious users, bots and malware are relentless in their pursuit of this type of broad access and the anonymity that shared accounts represent, and many of these bad-actors go unnoticed as they navigate the organization.

Security information and event management (SIEM) technology supports threat detection and security incident response through the real-time and historical analysis of security events from a wide variety of event and contextual data sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources.

### Privileged Identity Management Meets SIEM

One of the guiding principles of privileged identity management is to implement least privilege access to reduce the attack surface. Least-privilege access provides strong controls over user's privilege and reduces the risk associated with shared accounts and too much privilege.

With Centrify, users log in as themselves for their daily tasks, elevating privilege when necessary. Centrify's patented Zones technology provides highly granular, role-based access controls that simplify the implementation of a least-privilege access model.

The combined benefits of Centrify's privileged identity management and Splunk's SIEM solutions enable security teams to quickly detect and respond to internal and external attacks, simplify threat management while minimizing risk and safeguard organizations.

### Leveraging SIEM Without Additional Costs

Centrify Infrastructure Services leverage a customer's existing investment in Active Directory to provide centralized identity management and monitoring across Windows, Linux, and UNIX

servers both on premises and in the cloud. Infrastructure Services integrate with Splunk's SIEM tools to provide privileged access data attributed to the individual user. This enables real time analysis to identify potential attacks already in progress.

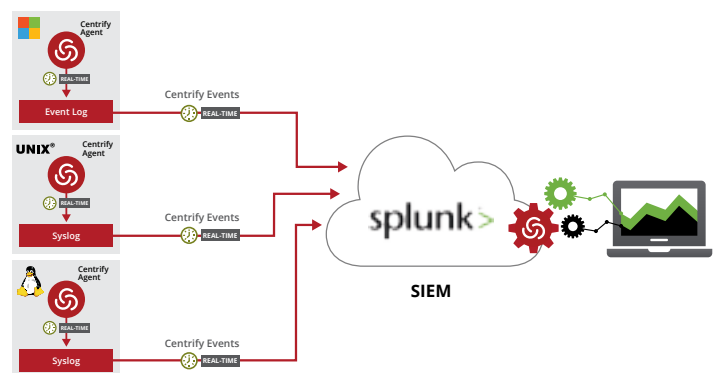
### Easily Import Categorized Privileged Access Data

Infrastructure Services capture privileged activity associated with an individual and normalizes the data for consumption by Splunk's SIEM solution. These, and other infrastructure system events are correlated for centralized alert creation to identify the most critical security issues across the organization and facilitate the interruption of an attack.

### How It Works

Centrify's agent can track over 300 different types of events in real-time on 450+ flavors of Windows, Linux and UNIX machines. A few sample categories of the Centrify events are:

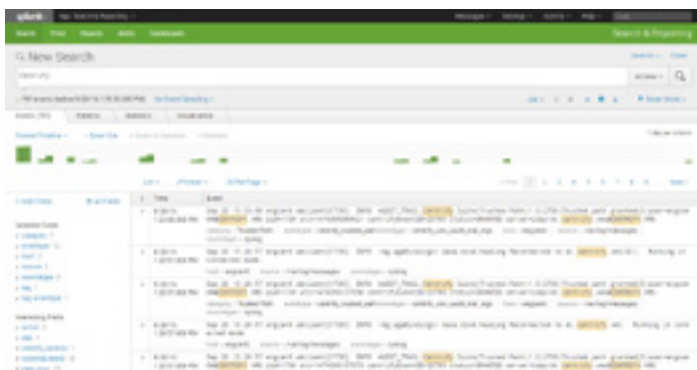
- User activity events on Centrify tools
- Log in events on Windows, Linux & UNIX systems
- Privilege escalation events on Windows, Linux and UNIX systems



Centrify events are available locally in standard logs either in Syslogs or Windows event logs.

## Splunk's Common Information Model

Splunk's Common Information Model (CIM) enables the tagging of common events from a variety of vendors or source types, resulting in the unification of events from the data domain of interest across the enterprise. Centrifly has mapped events to Splunk's authentication data model and can easily be found as shown in the following image.



## Easily Searchable Events

Centrifly event data is categorized and normalized prior to input into the Splunk database.

The following is a list of all the Centrifly event categories and their corresponding Splunk event type.

Centrifly Event Category	Splunk Event Type
DirectAudit System Management	centrifly_directaudit_system_management
Audit Manager	centrifly_audit_manager
Audit Analyzer	centrifly_audit_analyzer
DirectAuthorize - Windows	centrifly_directauthorize_windows
DirectAudit - Windows	centrifly_directaudit_windows
Centrifly Configuration	centrifly_configuration
DirectControl UNIX Agent	centrifly_directcontrol_unix_agent
DirectAudit UNIX Agent	centrifly_directaudit_unix_agent
Centrifly Commands	centrifly_commands
Trusted Path	centrifly_trusted_path
PAM	centrifly_pam
dzdo	centrifly_dzdo
dzsh	centrifly_dzsh

Centrifly Event Category	Splunk Event Type
dzinfo	centrifly_dzinfo
command	centrifly_command
Local Account Management	centrifly_local_account_management
Centrifly sshd	centrifly_sshd

## Splunk and Centrifly — Better Together

Splunk Inc. is the market-leading platform that powers Operational Intelligence. We pioneer innovative, disruptive solutions that make machine data accessible, usable and valuable to everyone. More than 11,000 customers in over 110 countries use Splunk software and cloud services to make business, government and education more efficient, secure and profitable. Splunk was named a leader in Gartner's 2016 Magic Quadrant for Security Information and Event Management (SIEM) for the fourth straight year, and is positioned as having the most complete vision in the Leaders quadrant.

Centrifly was named a leader in the Forrester Research, Inc., July 2016 report, "The Forrester Wave™: Privileged Identity Management, Q3 2016." The report evaluated the 10 most significant vendors based on 22 criteria, including current offering, strategy and market presence. Centrifly's evaluated solution achieved the highest score in strategy.

Together, Centrifly and Splunk's partnership delivers a streamlined integration for customers who need to identify risks or suspicious activity quickly to remediate threats to their valued assets.

## Benefits

- **Minimize the risk** associated with privileged access to critical data and infrastructure by capturing individual user activity, and creating security alerts for quick visibility into suspicious events
- **Centralize visibility** across enterprise deployments by correlating privileged access event data with other activity generated across the organization
- **Easily import categorized data sets** from privileged activity attributed to the individual into the prescribed SIEM schema for security alert creation
- **Leverage existing investments** in SIEM and alert tools without additional costs



As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrifly provides a single platform to secure every user's access to apps and infrastructure in today's boundaryless hybrid enterprise through the power of identity services. This is the Next Dimension of Security in the Age of Access.

Founded in 2004, Centrifly is enabling over 5,000 customers, including over half the Fortune 50, to defend their organizations. Centrifly is a privately held company based in Santa Clara, California. To learn more visit [www.centrifly.com](http://www.centrifly.com). The Breach Stops Here.

Centrifly is a registered trademark and The Breach Stops Here and Next Dimension Security is a trademark of Centrifly Corporation in the United States and other countries. Other trademarks mentioned herein are the property of their respective owners.

SANTA CLARA, CALIFORNIA	+1 (669) 444 5200
EMEA	+44 (0) 1344 317950
ASIA PACIFIC	+61 1300 795 789
BRAZIL	+55 11 3958 4876
LATIN AMERICA	+1 305 900 5354
EMAIL	<a href="mailto:sales@centrifly.com">sales@centrifly.com</a>
WEB	<a href="http://www.centrifly.com">www.centrifly.com</a>

BRF003883EN-07012017