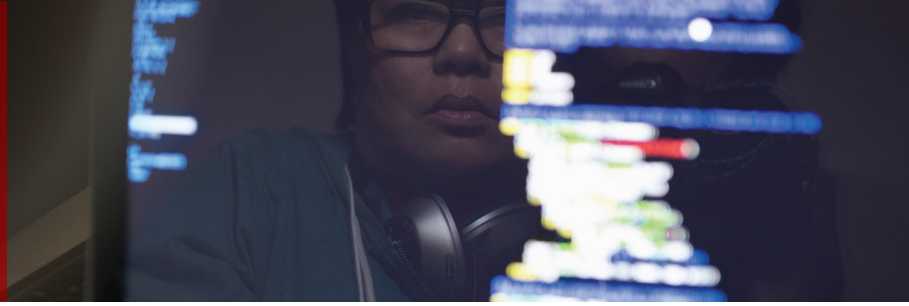
Centrify
ZERO TRUST PRIVILEGE



Centrify Audit and Monitoring Service

Harden Your Environment with High Assurance

For privileged sessions, it is of course best practice to audit everything. With a documented record of all actions performed, audit logs not only can be used in forensic analysis to find exactly the issue, but also to attribute actions taken to a specific user. Because these sessions are so critical, it is also best practice to keep a video recording of the session that can be reviewed or used as evidence for your most critical assets, or in highly regulated industries. There are multiple regulations including PCI-DSS for payment card data that specifically requires this level of auditing. If you have a security department, a good practice is to integrate this audit data with your existing Security Information and Event Management (SIEM) system for automated mining where risky activities can be identified and alerts raised.

Audit Everything

Industry analysts and government regulators have acknowledged that today's number #1 cause of breaches is tied to privileged access abuse. Privileged credentials represent the keys to the kingdom, allowing for a "free ride" throughout the entire infrastructure. It takes just one compromised privileged credential to impact millions. In turn, internal auditors and regulatory mandates set specific controls and reporting requirements for the usage of these credentials.

Even small and mid-sized organizations must comply with a variety of industry and government regulations, which creates its unique challenges when it comes to the collection, aggregation, and attestation of privileged access data.

Often organizations lack the continuous transparency into their compliance posture, leading to audits and certifications becoming a sprint during which the workload for the internal auditors and compliance staff skyrockets.

This often leads to a "sampling" approach, whereby only a subset of specific controls is being evaluated, leaving many blind spots from a compliance and security perspective. Overall, hunting down answers from a wide variety of stakeholders and assessing diverse data sets takes a toll on efficiency and accuracy.

From a security perspective, it is important to gain specific and detailed information about suspicious privileged access activity. Security managers can take immediate remediation action to protect against potential risk or a threat in progress directly from the alert screen, and manually or automatically terminate a session based on the risk.

In recent history, high profile data breaches were made possible by insiders who created back door accounts that circumvented traditional password vault approaches. Privileged users are also known to find ways to bypass the password vault in their environment to make their daily routine easier. This type of rogue access, often leverages SSH keys stored locally on servers, expands an organization's attack surface and puts them at a higher risk of a security breach.

Harden Your Environment with High Assurance

The Centrify Audit and Monitoring Service allows customers to fulfill their compliance mandates through auditing and reporting, as well as shut down any dangerous workarounds by putting host-based monitoring in place. The service assists in recording all privileged sessions and metadata, attributing activity to an individual to deliver a comprehensive picture of intentions and outcomes.

SESSION RECORDING AND AUDITING

Record and manage a holistic view of privileged activity across Windows and Linux servers, IaaS, and databases, establishing a single source of truth for individual and shared accounts. Prove compliance with reports on every user's privileges and associated activity.

GATEWAY SESSION MONITORING AND CONTROL

Gain new levels of oversight for privileged sessions on critical infrastructure. Administrative users watch activity in remote sessions in real-time and can instantly terminate suspicious sessions through the Centrify Admin portal.

HOST-BASED SESSION AUDITING, RECORDING, AND REPORTING

Ensure session recording cannot be bypassed with host-based auditing. Discover rogue activity such as the creation and installation of SSH key pairs that would make it easy to bypass security controls, and attribute activity to the individual user. Audit all privileged session activity at the process level in forensic detail for security review, corrective action for compliance reporting, and to avoid spoofing.

> **"There isn't a regulation that Centrify hasn't helped us to meet. Today, every time an administrator touches a server, I have a record of it. I can pull a report, print it, and hand it to the auditor."**
>
> — Peter Manina, IT Specialist and UNIX Systems Architect, State of Michigan Department of Technology, Management and Budget

Session Recording and Auditing for Privileged Access

Report and audit privileged sessions that leverage shared accounts and individual accounts with full video and metadata capture. The Centrify Audit and Monitoring Service allows customers to conduct forensic analysis and leverage high-fidelity recordings for audit and compliance purposes.

- Capture and collect data in a high-fidelity recording of each privileged session at the gateway-level. The Centrify Audit and Monitoring Service stores sessions in an easily searchable SQL server database for a holistic view of exactly what happened. The service's searchable playback feature gives IT security managers and auditors the ability to see exactly what users did and the results of their action and identify privilege abuse or the source of a security incident.
- Record all privileged sessions and metadata, attributing activity to an individual to deliver a comprehensive picture of intentions and outcomes.
- Show that security controls are in place and working as designed and provide proof of compliance. Search and find session recordings by servers, users, or custom searches. You can find all sessions for a particular user or server, or for a set of custom criteria, simplifying forensic investigations and proactively identifying insider threats or suspicious activity.
- Gain comprehensive visibility with unified access and activity reporting based on a common platform. Customizable and built-in queries, as well as out-of-box reports for SOX and PCI regulatory compliance provide information on privileged account access controls, password checkout, and privileged sessions across Windows, Linux, and UNIX.

Monitor and Control Privileged Sessions Across IaaS and On-Premises

Leverage a common auditing infrastructure to capture and record privileged activities for your infrastructure, whether it's on-premises or in the cloud. Detect suspicious user activity to alert in real time of attacks that may be in progress. The Centrify Audit and Monitoring Service allows to monitor and control privileged access sessions that leverage shared and individual accounts.

- Gain new levels of oversight for privileged sessions on critical infrastructure. Administrative users watch activity in remote sessions in real-time and can instantly terminate suspicious sessions through the Centrify Admin Portal. This 4-Eyes mode allows administrative users to oversee a remote employee or outsourced IT's activities, tuning into the live, ongoing session. You can watch every action the privileged user takes or terminate the session if the activity is suspicious.
- Privileged access data is captured and stored to enable robust querying by log management tools and integration with external reporting tools. Streamlined integration with SIEM and alerting tools such as Micro Focus® ArcSight™, IBM® QRadar™, and Splunk® identify risks or suspicious activity quickly.

Prevent Spoofed or Bypassed Privileged Access with Host-Based Session Auditing, Recording, and Reporting

Taking a host-enforced approach to session auditing, recording, and reporting ultimately results in better control over privileged access in your environment. Centrify Audit and Monitoring Service extends its gateway-based capabilities with a host-based approach that ensures your privileged access controls are not bypassed, as they can be with a password/secrets vault alone.

- Capture and collect data in a high-fidelity recording of each privileged session on any server across your on-premises and cloud-based infrastructure. Store sessions in an easily searchable SQL server database for a holistic view of exactly what happened on any system, by any or all users, and at any given time.
- Centrify host-based session auditing, recording, and reporting comes with capabilities for advanced monitoring at process-level combined with shell-based auditing to identify suspicious application changes.
- Centrify File Integrity Monitoring identifies changes to configurations and critical files in real-time, enabling triggered security alerts within an organization's SIEM system to warn of the creation of a backdoor to bypass the password vault.
- A searchable playback feature gives IT security managers and auditors the ability to see exactly what users did and identify abuse of privilege or the source of a security incident.
- Report on access, checkouts, sessions, and use of privilege across Windows, Linux, UNIX, and network infrastructure.
- Streamlined integration with SIEM, alerting, and reporting tools.

US Headquarters +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
sales@centrify.com

Centrify®
ZERO TRUST PRIVILEGE

www.centrify.com