Centrify
ZERO TRUST PRIVILEGE

Centrify Privilege Threat Analytics Service

Machine Learning Controls for the Modern Threatscape

Zero Trust Privilege controls need to be adaptive to the risk-context. Gartner promotes CARTA – Continuous, Adaptive, Risk, and Trust Assessment – and it's absolutely required for privileged access too. Zero Trust Privilege means knowing that even if the right credentials have been entered by a privileged user, but the request comes in with risky context, then a stronger verification is needed to permit access. Modern machine learning algorithms are now used to carefully analyze a privileged user's behavior and identify "anomalous" or "non-normal" (and therefore risky) activities and apply the proper level of control for the corresponding risk.

Today's Threatscape Requires Adaptive Controls

Cyber adversaries are getting more and more sophisticated and therefore it is best practice to apply multiple security layers when protecting against privileged access abuse. Today's threatscape requires security controls to be adaptive to the risk-context and to use machine learning to carefully analyze a privileged user's behavior.

Adaptive control means not only notifying of risky activity in real time, but also being able to actively respond to incidents by cutting off sessions, adding additional monitoring, or flagging for forensic follow up.

Machine learning allows companies to pore through millions of events and scan for that needle in the haystack on an ongoing and continuous basis, which would never be achievable by manual forensics. Even more valuable is performing machine learning-based analytics inline and in real time and thus being able to enforce truly adaptive preventive controls and not just after-the-fact detective controls.

Pinpoint Privileged Access Abuse in Near Real Time

The Centrify Privilege Threat Analytics Service leverages advanced behavioral analytics in combination with the Centrify Zero Trust Privilege adaptive multi-factor authentication (MFA) capabilities to add an additional layer of security and applies adaptive MFA for abnormal user behavior. Leveraging Centrify Privilege Threat Analytics Service can make the difference between falling victim to a breach or stopping it in its tracks.

ADAPTIVE MULTI-FACTOR AUTHENTICATION

Add an extra layer of security to stop the breach with risk-aware, adaptive MFA for IT admins who access Windows and Linux systems, elevate privilege, or leverage privileged credentials.

USER BEHAVIOR ANALYTICS

Leverage modern machine learning algorithms to carefully analyze a privileged user's behavior and identify "anomalous" or "non-normal" and therefore risky activities and alert or notify security. Detecting risky activity is also leveraged when making real time access control decisions, for instance in the context of authentication or step-up authentication. In addition, privileged user behavior analytics can be used to analyze most used and least used privileges and serve as a governance function to suggest changes to roles and rights.

"When you get a clear picture of the breadth of capabilities Centrify Zero Trust Privilege Services provide, you begin to understand just how many security check boxes it ticks. I'm still surprised at the number of issues I was able to address with just this single solution."

— Matt Horn, IT Operations Manager, GSI

Reinforce Secure Access to Critical Systems

Add an extra layer of security only when needed — and based on risk rating — to reduce the threat associated with compromised privileged credentials. Configure behavior-based access control for IT admins who access Windows and Linux servers, elevate privilege, or leverage privileged credentials.

- Identify anomalous behavior while it is happening, by enforcing risk-aware policies for users who are initiating a privileged session, checking out a password, or elevating privilege. Combining risk-aware policies with role-based access controls, user context, and MFA enable intelligent, automated, real-time decisions on whether to grant privileged access. These dynamically enforced access policies grant the user access, prompt for a second factor of authentication, or block access completely.
- Centrify Zero Trust Privilege Services support the broadest range of authenticators to provide the flexibility to support authenticating your IT staff using the most convenient form factor, as well as to enable you to leverage existing MFA systems and authenticators that you may already have. Authenticators supported by Centrify include:
  - Mobile push notification;
  - Security questions;
  - Phone call with PIN verification;
  - OATH tokens;
  - One-time passcode servers;
  - FIDO U2F security keys; and
  - Smart cards.
- Centrify's adaptive MFA capabilities are designed to work well with existing investments in RSA, OATH-based tokens, and smart cards such as PIV/CAC. These can all be brought under Centrify's centralized management and enforced across your enterprise.
- The Centrify mobile app for iOS and Android provides the privileged user with a simple interface to receive MFA notifications or workflow requests for approval. The app also provides an interface to enable the user to manage OATH tokens where the seed or secret is vaulted by the Centrify Privileged Access Service to support user validation of OTP codes, as required by various privileged applications or services that enforce their own OATH-compliant MFA validation such as the AWS® Console. Furthermore, the mobile app supports "break-glass" password checkout/check-in.
- Centrify also supports providing MFA services for network devices such as routers, switches, or firewalls where administrative access should require MFA prior to privileged user access.

Leverage User Behavior Analytics to Minimize Your Risk Exposure

Today's threatscape requires security controls to be adaptive to the risk-context, using machine learning to carefully analyze a privileged user's behavior. Adaptive control means not only being notified of risky activity in real time, but also being able to actively respond to incidents by cutting off sessions, adding additional monitoring, or flagging for forensic follow up.

- Leverage a series of customizable dashboards and interactive widgets to better understand IT risk and access patterns across your infrastructure. By tailoring security policy to each user's behavior and automatically flagging risky behavior, gain immediate visibility into account risk, eliminating the overhead of sifting through millions of log files and massive amounts of historical data.
- Better comprehend access and events by drilling into details around events, across systems, location, time, privileged commands, and more. IT users can drill into individual events to understand the risk nature of any specific event. Risk is computed in real time for every event and expressed as high, medium, or low for any anomalous activity.
- Gain streamlined insight into anomalous activity with a detailed timeline view. Identify the specific factors contributing to an anomaly for a comprehensive understanding of a potential threat, all from a single console. Security teams can view system access, anomaly detection in high resolutions with analytics tools such as dashboards, explorer views, and investigation tools.
- Privileged access data is captured and stored to enable robust querying by log management tools and integration with external reporting tools. Streamlined integrations with SIEM tools such as Micro Focus® ArcSight™, IBM® QRadar™, and Splunk® identify risks or suspicious activity quickly.
- Leverage any Webhook-enabled application (e.g., Slack® or existing on-board incident response systems such as PagerDuty®) to enable real-time alert delivery, eliminating the need for multiple alert touch points and improving time to response. When an alert event occurs, Centrify Privilege Threat Analytics Service allows the user to easily fire off alerts into third-party applications via Webhook. This capability enables the user to respond to a threat alert and contain the impact.
- Gain specific and detailed information about suspicious privileged activity. IT admins can take immediate remediation actions to protect against potential risk or a threat in progress directly from the alert screen and manually or automatically terminate a session based on risk.
- Events analyzed from the Centrify Privilege Threat Analytics Service are used to profile the normal behavior pattern for a user on any login or privileged activity including commands, so anomalies can be identified in real-time to enable risk-based access control. High-risk events are immediately flagged, alerted, notified, and elevated to IT's attention, speeding analysis and greatly minimizing the effort required to assess risk across today's hybrid IT environments.

Our mission is to stop the leading cause of breaches – privileged access abuse. Centrify empowers our customers with a cloud-ready Zero Trust Privilege approach to secure access to infrastructure, DevOps, cloud, containers, Big Data and other modern enterprise attack surfaces. To learn more, visit www.centrify.com.

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