Centrify
ZERO TRUST SECURITY

CENTRIFY ANALYTICS SERVICE

Learning and adapting security policies in real-time based on user behavior

Compromised credentials are today's leading cause of data breaches. Centrify Analytics Services stop compromised credential-based attacks, and eases access for users, based on behavior. Through machine learning, Analytics Services assess risk based on constantly-evolving behavior patterns of both end users and privileged users. This assessment is followed by a risk score assignment and an appropriate enforced access decision, all while simplifying risk monitoring and alerting and enabling detailed analysis.

Compromised Credential-Based Attacks

According to Verizon, 81% of breaches are due to weak, default or stolen credentials. It is no wonder that compromised credential-based attacks are so successful because attackers have the perfect camouflage. Attackers look just like legitimate users, since they are exploiting legitimate accounts — and the attacks raise no suspicion, since all IT sees is regular user activity.

Centrify Analytics Services breaks this breach cycle by applying machine learning to determine, in real time, whether the access being requested is likely to be from a legitimate user, or from an attacker who has compromised that users' account. The user's access risk score determines whether access is granted, requires step-up authentication, or is blocked entirely.

Integrated machine learning enables the automatic creation of user access profiles based on user behavior, with risk scores assigned to a user's access request — across cloud and on-premises applications, VPN, servers, shared account checkout, and more. If an access request is consistent with typical user behavior, it presents low risk. Factors that increase risk include access requests from atypical locations, networks, devices, or from unusual times.

Not only does risk-based access provide real-time security, it also flags high-risk events and elevates them to IT's attention — speeding analysis and greatly minimizing the effort required to assess risk across today's hybrid IT environment.

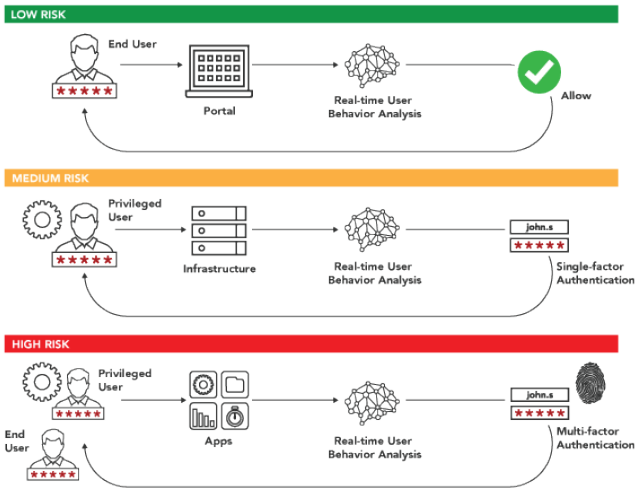
Analytics Services, which consists of Centrify User Analytics and Centrify Privilege Analytics, helps IT to:

- **Increase Security:** High-risk access indicating potential threats can be automatically challenged or blocked to minimize risk
- **Improve User Experience:** User behavior drives policy, to ease access
- **Simplify Analysis:** Anomalous events are flagged as identity threats

Risk-Based Access

Analytics Services uses machine learning to define and enforce access policy, based on user behavior. Through a combination of machine learning, user profiles, and context-aware policy, access decisions can be made in real time.

Centrify makes access decisions at the time and point of access. Rather than forcing administrators to pore through historical data to see where breaches may have occurred, and then manually update policy where required, Centrify risk-based access stops anomalous activity in real time — at the point of access.



Since decisions are made based on risk level, Analytics Service can be easily created to:

- Ease low-risk access for typical access requests
- Step up authentication when requests are outside of typical user behavior
- Block access entirely for requests that present high risk

Protect App Access

Cloud, mobile and on-premises applications are under increasing attack. Often protected only by a simple username and password, apps provide easy targets. Centrify can protect apps, without increasing user hassle, with risk-based policy based on typical access patterns and user behavior — across cloud and on-premises applications, VPNs, and more.

Protect Infrastructure Access

Risk-aware access policies protect critical IT infrastructure against attacks that exploit compromised privileged accounts, using machine learning to define and enforce based on user behavior.

Whether initiating a privileged session, checking out a credential, or executing a privileged command, Analytics Services determines the risk-level and either grants privileged access, requires additional authentication factors or blocks access entirely.

Identity Intelligence

Analytics Services not only provide the real-time decisions to stop breaches — but also allows IT to get an overview of the risk associated to apps and infrastructure, as well as investigate specific access events.

IT Security can build custom dashboards to enhance visibility across access points to ensure policies are working as expected, better understand security risk, as well as user experience, across apps, endpoints and infrastructure. With a detailed rollup of access information, IT can view privileged access activity with information related to unusual privilege change, command runs, what target has been accessed and privilege elevation. Additionally, custom widgets allow IT to see how often users are prompted for MFA to help balance security with productivity.

Investigative Analysis

User and Privilege Analytics Services provide the ability to drill into any access event, and with IT can identify specific risky events with the help of interactive reports — across device, location, time, user and more.

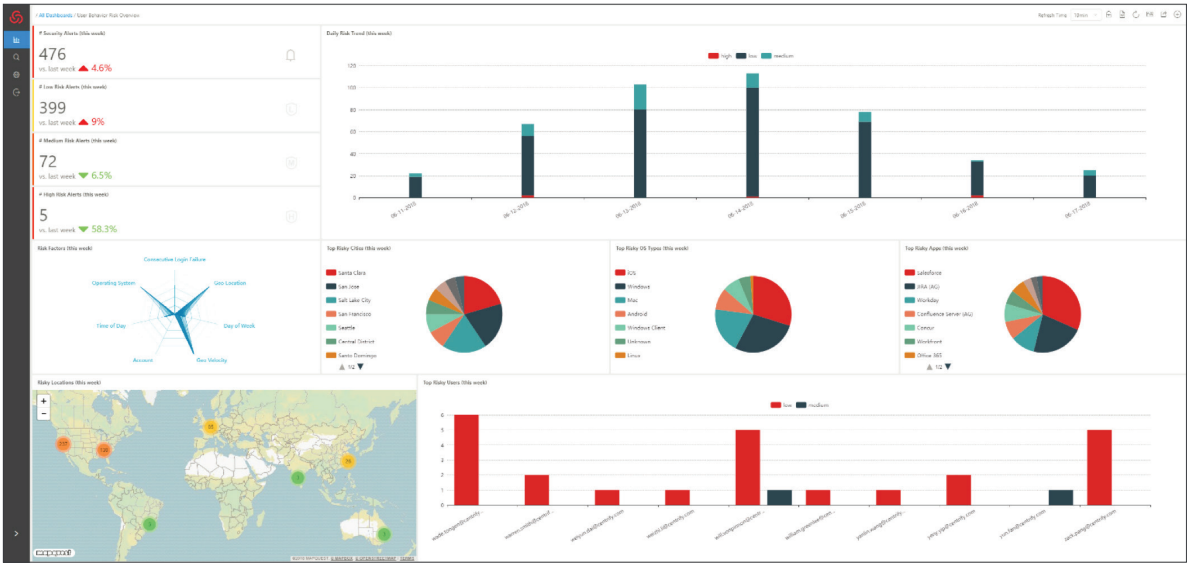
Security Operations can leverage a powerful toolkit specifically streamlined for identity anomaly investigation and learn quickly if specific employee accounts have been targeted by attackers. Helpdesk staff can play or re-play video sessions directly from the dashboard to minimize the hassle of switching views, and drilldown to see why a given employee was prompted for MFA, blocked, or allowed access to resources and applications.

Real-time Alerting and Response

Privilege Analytics Service stops threats in progress with alerts triggered in real-time from a broad set of enforcement points that include endpoints, applications and IT infrastructure. Risk-based policy can be enforced in real time at the point of access, where high-risk threats can be blocked. By integrating with any Webhook-enabled endpoint, IT admins can easily customize alerts for context-based visibility specific to privileged user activity and remediate potential threats directly without having to login to the portal.

Balance Security and User Convenience

IT personnel can define and deploy flexible policies by role, app, endpoint, system, privileged role or account and more – all from a simple management portal. With Analytics Services, this policy can include risk-level, as well as custom rules based on location, browser, operating system, network, user attributes, time of day and more — to combine high levels of assurance with low user frustration.



Centrify User Analytics Service - User Behavior Risk Overview

Centrify
ZERO TRUST SECURITY

Centrify delivers Zero Trust Security through the power of Next-Gen Access. The Centrify Zero Trust Security model assumes that users inside a network are no more trustworthy than those outside the network. Centrify verifies every user, their devices, and limits access and privilege. Centrify also utilizes machine learning to discover risky user behavior and apply conditional access — without impacting user experience. Centrify's Next-Gen Access is the only industry-recognized solution that uniquely converges Identity-as-a Service (IDaaS), enterprise mobility management (EMM) and privileged access management (PAM). Over 5,000 worldwide organizations, including over half the Fortune 100, trust Centrify to proactively secure their businesses. 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