Centrify
ZERO TRUST SECURITY

SOLUTION BRIEF

Centrify Analytics Service

Stop breaches in real-time based on user behavior

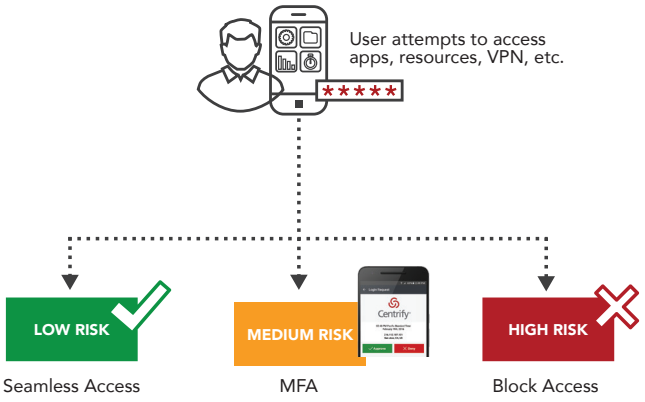
Compromised credentials are today's leading cause of data breaches. Centrify Analytics Service stops compromised credential-based attacks, and eases access for users, based on behavior. Through machine learning, Analytics Service assesses risk based on constantly-evolving user behavior patterns. It then assigns a risk score, and enforces an appropriate access decision, all while simplifying risk monitoring and 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 Service 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.

Thanks to integrated machine learning in the Centrify Identity Platform, user access profiles are automatically created based on user behavior. Risk scores are then assigned to each access request made by users – across cloud and on-premises applications, VPN, servers, shared account checkout, and more. If the 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 odd times.



Not only does risk-based access provide real-time security, but 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.

Centrify Analytics Service Helps IT to:

- **Increase Security:** High-risk access can be 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

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

Understanding Risk

Centrify Analytics Service not only provides 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.

Access Insights

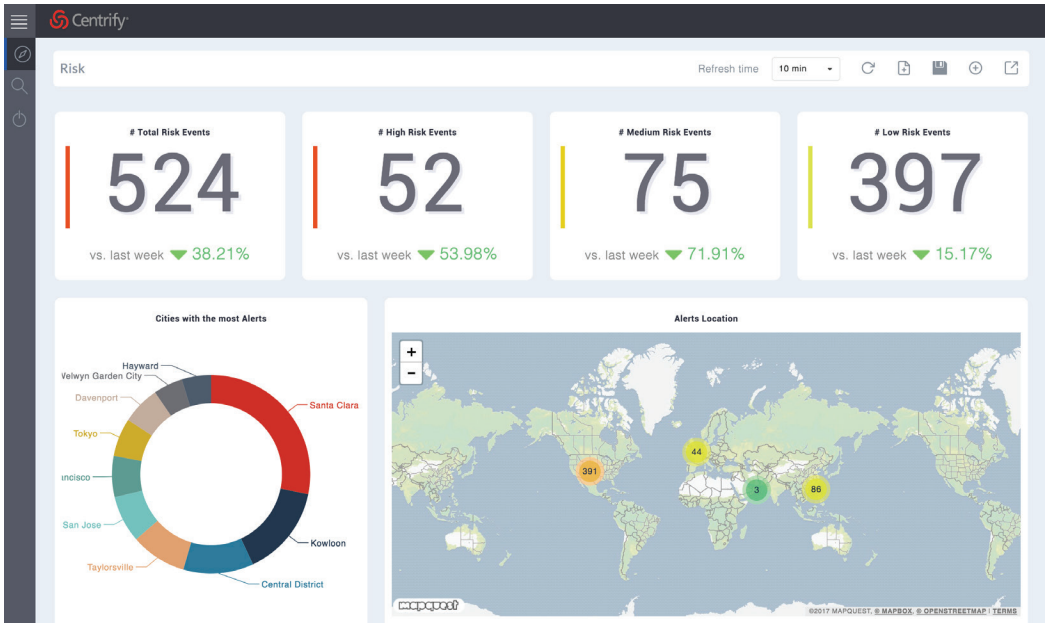
IT Security can build custom dashboards to better understand security risk, as well as user experience, across Apps and Infrastructure. With detailed rollup of access information, IT can see the total number of alerts, as well as trending, to ensure that policy is working as expected. Additionally, custom widgets allow IT to see how often users are prompted for MFA to help balance security with productivity.

Events Explorer

The Centrify Identity Platform provides the ability to drill into any access event, and thanks to interactive reports, IT can identify specific risky events – across device, location, time, user and more. Security Operations can learn quickly if specific employee accounts have been targeted by attackers, and the helpdesk staff can drill in to see why a given employee was prompted for MFA, blocked, or allowed access to resources and applications.

Balance Security and User Convenience

IT can define flexible policy and deploy it by role, app, endpoint, system, privilege account and more – all from a simple management portal. With Centrify Analytics Service, 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 Analytics Service
Access Insights

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

BRF004076EN-05292017