DATASHEET

Centrify
THE BREACH STOPS HERE

Centrify Endpoint Services

Too much access for untrusted endpoints

Today's traditional measures of security are clearly not sufficient. With 81% of breaches originating from compromised credentials and 95% of phishing attacks followed by malicious software installation, it is time to ensure your endpoint and application management solutions are integrated with your identity and access management strategies. The need for an identity-centric approach to stopping breaches is critical. With so many disparate systems and devices, IT needs a single solution from which to provision users and manage access policy across all apps, from any endpoint, regardless of location.

Managing Access is the Problem

Too much access

Managing and securing access to corporate applications and data should be limited to authorized and authenticated users on secure and trusted endpoints.

Too much privilege on endpoints

Enforcing least privilege security on the endpoint is a fundamental part in protecting against malware infection that lead to today's breaches.

Strengthen your existing endpoint security by providing end users local user rights and a solution for local privilege elevation as needed.

Same administrative account used across all endpoints

Eliminate one of the most common security deficiencies found in most IT organizations — the use of a common and static admin password across all endpoints. Inevitably this admin password is shared with a user with a critical escalation. This puts your organization at considerable risk as this password can be used to gain admin privileges on your endpoints. This issue is compounded by the fact that these passwords rarely change and IT staff or employees retain knowledge of them after leaving the company — possibly on poor terms. Centrify mitigates this significant issue by generating a strong and unique password for each endpoint that is rotated per policy and stored securely in the Centrify password vault. Authorized personnel can check out these unique passwords upon request.

Identity is the Solution

Manage and secure your heterogeneous environment through a single source of identity and least privileged access approach.

Centrify Endpoint Services leverages identity to secure and manage users' access to applications from any device, regardless of location. It uses endpoint posture such as location of device, browser, or OS to provide secure access and prevents data from being accessed from devices that aren't trusted nor managed. With Centrify Endpoint Services, you can enable unified management across all endpoint management platforms, providing a single pane of glass for policy and management of all end user devices.

DEVICE MANAGEMENT

Stop breaches that target mobile devices. Combine device posture with access policy for next-dimension, context-based security and enable secure BYOD, with simple device enrollment and integrated single sign-on to business apps.

APP MANAGEMENT

Protect against rogue apps and malware. Control and manage applications automatically, ensuring up-to-date security.

ADAPTIVE MFA FOR ENDPOINTS

Leverage endpoint posture to provide access to corporate resources and protect endpoints. Allow users to authenticate quickly without dedicated infrastructure or tokens. Integrated MFA with SSO provides seamless and secure access from trusted devices.

SMART CARD AND DERIVED CREDENTIALS

Eliminate passwords across apps and devices and comply with Smart Card regulations, while enabling device choice and embracing the cloud.

Endpoint Services also ensures access is limited to authorized users with Multi-factor Authentication the endpoint login screen through flexible options such as mobile authentication, smart cards and OTP tokens. With Centrify Endpoint Services, you can enable unified management across all endpoint management platforms, providing a single pane of glass for policy and management of all end user devices. In addition, Centrify prevents users from installing unwanted applications through just-in-time privilege and just-enough-privilege through temporary and time-bound access to critical endpoints. Users can elevate privileges based on roles and on-demand privilege elevation is seamless.

Centrify Endpoint Services: An Identity-Centric approach to securing endpoints

Centrify Endpoint Services provide security, simplicity and control. IT allows access to apps and infrastructure only from trusted and secured endpoints. Users get single sign-on across cloud and mobile apps from any device. Through a unified view, IT is able to manage endpoints and set policies for how apps are accessed.

Security

- Eliminate use of static local admin passwords across endpoints through password rotation and time bound privilege access provided by Local Administrator Password Management (LAPM)
- Ensure access to data is safe through full EMM features and integrated SSO
- Deliver unmatched robust Mac smart card support including PIV, CAC and CAC-NG
- Implement a secure BYOD policy with Centrify's integrated Mac and mobile device management. Secure the Centrify app on mobile devices by unlocking with NFC, PIN, passcode or fingerprint.
- Leverage endpoint posture (location of device, browser, or OS) to provide secure access

Simplicity

- Unified Endpoint Management across all endpoint platforms including Windows, Mac, Linux, iOs and Android devices
- Common policy mechanism tied to application access thereby simplifying the decision-making process of who can access what from where
- Integrated mobile and endpoint MFA
- Easy-to-use, cloud-based management
- Endpoint Management across all endpoint platforms including Windows, Mac, Linux, iOs and Android devices

Control

- Full control over access to corporate resources and apps
- Provide stronger controls over endpoint admin accounts through a least-privilege access approach
- Enforce user policy from a single authoritative source, applied across devices, apps, and locations
- Control access using Active Directory, LDAP, Google Directory, Cloud Directory, external users, or any combination
- Ensure access is limited to authorized users with multi-factor authentication at login
- Block access to sensitive information from non-compliant devices through role-based access controls

Centrify
THE BREACH STOPS HERE

As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify 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, Centrify is enabling over 5,000 customers, including over half the Fortune 50, to defend their organizations. Centrify is a privately held company based in Santa Clara, California. To learn more visit **www.centrify.com**. The Breach Stops Here.

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	**sales@centrify.com**
WEB	**www.centrify.com**

DSH004077EN-07132017-A4