Centrify
ZERO TRUST SECURITY

# CENTRIFY ENDPOINT SERVICES

Secure Access Starts with Trusted 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. Whether it's a corporate owned, BYOD or public desktop, laptop or mobile device, enforce access control policies based on the device identity and security posture. Only allow access to corporate resources from trusted endpoints.**

## 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. Enable safe and seamless access through a Zero Trust approach, combining device posture with access policy for next dimension, context-based security.

**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.

## A Zero Trust Security Approach

Control access to corporate resources through a zero trust model by verifying identity of users and endpoints, coupled with conditional access policies to govern what users have access to. 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.

### CONDITIONAL ACCESS

Combine Identity Assurance and Endpoint Security Posture to enforce Identity-centric conditional access policies to corporate applications and infrastructure.

### ADAPTIVE MFA & STRONG AUTHENTICATION

Secure access to endpoints with risk-aware MFA that adapts to your requirements.

### DEVICE SECURITY MANAGEMENT

Control endpoint security posture with policy and configuration management ensuring consistent preventative security.

### ENDPOINT PRIVILEGE MANAGEMENT

Increase endpoint security posture by minimizing the attack surface and controlling privileged access.

Endpoint Services also ensures access is limited to authorized users with Multi-factor Authentication at 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 including remote locate, lock and wipe capability across devices
- Deliver 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
- Centralize discovery, management and user administration to enable rapid identity consolidation into Active Directory

**Control**

- Combine identity assurance and endpoint security posture to control access to apps and corporate resources when identity-centric conditions are met
- 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
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