DATASHEET

Centrify
ZERO TRUST SECURITY

Centrify Infrastructure Services

Minimize the Attack Surface and Control Privileged Access to the Hybrid Enterprise

IT organizations are increasingly deploying and managing hybrid environments that combine cloud-based and data center infrastructure, while working to mitigate the risk of insider and cyberthreats and meet PCI DSS, SOX or other industry mandates and government regulations. Hybrid enterprises require a purpose-built, privileged access security solution that enables centralized control and visibility over privileged access and simplified compliance to protect against the evolving threat landscape.

Today's Security is NOT Secure

The number of breaches has skyrocketed in recent years, with global cybercrime-related damage costs expected to exceed $6 trillion annually by the year 2021.

Malicious insiders and hackers are becoming more targeted and sophisticated — breaching systems with direct access via compromised credentials. Nearly two-thirds of all recent confirmed data breaches involved weak, default or stolen credentials, causing business disruption and cost. To add to this challenge, the proliferation of users and accounts beyond the data center to cloud-based infrastructure further amplifies the complexities of securing privileged access to critical systems and network devices.

The Next Dimension in Security

Security technology of the past — including firewalls, virtual private networks (VPNs) and antivirus software — has proven to be ineffective protection against these breaches. IT organizations need to look beyond their current security solutions into the next dimension in security to stop breaches — through the power of identity services.

Stop Breaches that Abuse Privilege

Today's organization must control access to hybrid infrastructure, enforce individual accountability and consistently control privileged access to both on-premises and remote users while improving IT productivity. Implementing a least privilege access model, securely managing shared privileges, and associating privileged activity to an individual are at the root of reducing threats, intentional or not.

Centrify Infrastructure Services minimizes the attack surface and controls privileged access to the hybrid enterprise with identity assurance, just-in-time and just enough privilege, and advanced monitoring. Infrastructure Services increases security and accountability by enabling IT to ensure users are who they say they are because they log in as themselves with multi-factor authentication, govern privileged access through roles and approval workflows, and associate all privileged activity to an individual with shell and process level monitoring.

IT management can leverage a cloud service, private cloud and data center flexible deployment options to meet their specific business needs.

IDENTITY BROKER

Consolidate identities and leverage a common enterprise authentication service.

ADAPTIVE MFA FOR PRIVILEGED ACCESS

Prove users are who they say they are with risk-aware multi-factor authentication.

PRIVILEGE ELEVATION

Grant just enough privilege across Windows and Linux systems.

SHARED PASSWORD MANAGEMENT

Reduce the risk of security breach when sharing privileged accounts.

PRIVILEGED ACCESS REQUEST

Govern access to privileged roles and accounts with approval workflows.

SECURE REMOTE ACCESS

Establish privileged sessions to targeted infrastructure without a VPN.

SESSION RECORDING AND MONITORING

Monitor and record privileged sessions and changes to critical files in real-time.

AUDITING AND REPORTING

Improve accountability, conduct forensic investigations and prove compliance.

© 2018 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

The Security of a Single Identity

Consolidate identities and leverage a common enterprise authentication service across on-premises and cloud based infrastructure and apps. Have your users log in as themselves using their unique identity across infrastructure and apps, while federating privileged access for outsourced IT and other third parties to avoid creating new identities.

Identity Broker seamlessly connects servers deployed on-premises or in the cloud to an organization's identity provider of choice — including Active Directory, LDAP or cloud-based directories such as Centrify, Google G-Suite — without having to replicate complex identity infrastructure.

Natively join Linux and UNIX systems to Active Directory, turning the host system into a client. Secure systems using the same authentication and Group Policy services currently deployed for Windows systems.

Reinforce Secure Access to Critical Systems

Combining risk-level with role-based access controls, user context and adaptive multi-factor authentication enables intelligent, automated, real-time decisions on whether to grant privileged access.

Just Enough Privilege

Reduce the risk of a breach and the damage that can be done when administrators have broad and unmanaged privilege with a flexible, fine-grained privilege elevation service. Simplify implementation of a least-privilege model by assigning pre-defined roles, importing existing sudo files and automating the creation of new roles.

Assigning just enough privilege based on a job function increases security and accountability. Having users log in as themselves and elevate privilege based on their role within the organization minimizes your attack surface by reducing the number of shared accounts and vaulted credentials.

Control Shared Access to Privileged Accounts

Give your authorized internal users, outsourced IT and third party vendors secure, always-on access to critical shared account passwords while maintaining control over who has access, which passwords they have access to and how those passwords are managed. Provide a single location for super-user, service, database and application accounts for all on-premises and cloud-based systems and network infrastructure.

Self-service, Just-in-Time Privileged Access

Govern access to privileged account credentials, privileged sessions and roles that grant privilege to individuals with approval workflows.

Self-service, just-in-time access enables choice — implement static, long-lived access, incident-based and time-bound access, or a combination of the two — for privileged accounts and privileged roles. Capture who requested access and who approved it, and easily reconcile approved access with actual access for privileged access governance.

Targeted Privileged Access Without a VPN

Control privileged access to specific data center and cloud-based resources without the increased risk and overhead of implementing full VPN access. Secure remote access to data center and cloud-based infrastructure is enabled for third parties, vendors and outsourced IT through a cloud service or on-premises deployment, all without having to manage their identities.

Monitor, Manage and Record Privilege Sessions

Detect suspicious user activity to alert in real time to stop breaches in progress. Monitor and control privileged sessions that leverage shared and individual accounts with full video and metadata capture. Ensure session recordings cannot be bypassed with host-based auditing, and avoid spoofing with shell-level and process-level monitoring.

Enforce Accountability and Prove Compliance

Gain visibility across all your privileged activity and tie everything back to the individual by recording and managing a holistic view across Windows and Linux servers, and network devices. Leverage out-of-box reports for PCI and SOX compliance. Eliminate spoofing with advanced auditing capabilities that combine application and file change monitoring with video recording and time-indexed command auditing.

Benefits

- **Reduce the risk of a security breach –** protect critical information and minimize attack surface by providing only necessary access levels to IT systems.
- **Save cost with an integrated solution –** simplified, true cross-platform least privilege access, shared account password management, multi-factor authentication (MFA) and fully
  integrated auditing and monitoring using your existing directory investment
- **Sustain compliance and simplify IT audits –** easily prove compliance with reports showing who has privileged access — across individual and shared accounts – and who has used that access, including full video capture of privileged sessions.

Centrify
ZERO TRUST SECURITY

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 100, to defend their organizations. Centrify is a privately held company based in Santa Clara, California. 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 is a registered trademark, and The Breach Stops Here and Next Dimension Security are trademarks of Centrify Corporation. Other trademarks mentioned herein are the property of their respective owners. ©2018 Centrify Corporation. All Rights Reserved.

DSH004076EN-07122017