Platform Approach to Securing Enterprise Identities
Platform Approach to Securing Enterprise Identities

Contents

Executive Summary 3
Introduction 4
Identity is the New Perimeter 5
Today's Threats Require a Next-Generation Identity Platform 7
Centrify Secures Enterprise Identities 8
Centrify Identity Platform 9
Centrify Identity Solutions 13
Why Choose Centrify 14
Next Steps 14

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Centrify Corporation. Centrify may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Centrify, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Centrify, DirectControl and DirectAudit are registered trademarks and Centrify Suite, DirectAuthorize, DirectSecure and DirectManage are trademarks of Centrify Corporation in the United States and/or other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Executive Summary

Like the ocean tides and tsunamis flowing inland, cyber attackers will always find the path of least resistance into your protected networks and resources. With the majority of cyber attacks, the research has shown the weakest point is your users and their credentials. And while unfettered privileged access is the holy grail of cyber attacks, often the easiest way for attackers to gain access is through compromised end user accounts.

At the same time, traditional perimeter based security is insufficient to protect cloud and hybrid infrastructure, new styles of working, and new ways of connecting remotely. Security vendors offer solutions for parts of the growing identity problem but only Centrify offers a complete security platform that gives you full identity security.

Centrify secures enterprise identities against cyberthreats that target today’s hybrid IT environment of cloud, mobile and on-premises. The Centrify Identity Platform protects against the leading point of attack used in data breaches — compromised credentials — by securing an enterprise’s internal and external users as well as its privileged accounts. Centrify delivers stronger security, continuous compliance and enhanced user productivity through single sign-on, multi-factor authentication, mobile and Mac management, privileged access security and session monitoring.
Introduction

With massive data breaches making headlines every day, security awareness has never been higher. Security issues are demanding the attention of every C-suite and boardroom across the globe.

Unfortunately, the breach headlines are even more striking than most could predict. Recent breaches involved high-profile criminal and state sponsored attacks. Millions of personnel records of government employees, tens of millions of records of insurance customers, and hundreds of millions of customer records from various other companies were among the information compromised. Even news of a BILLION-dollar bank heist has been reported!

In this paper we will examine how securing identity is at the center of protecting your users, systems and data. In fact, today's threats require a next-generation identity platform. And how Centrify secures enterprise identities through the Centrify Identity Platform.

In 2015, the number of security incidents rose to 60 million from 43 million in 2014, resulting in a 38% increase. (Source: PwC)

The weakest point in any organization is privileged identities with root, admin or read/write access privileges to critical infrastructure, apps and data. (Source: Verizon)

100% of recent high-profile data breaches were due to compromised credentials. (Source: Mandiant)

59% of US companies surveyed reported breaches that together cost millions of dollars. (Source: Centrify survey)

In 2015, 59% of US IT decision makers reported sharing access credentials with other employees at least somewhat often. (Source: Centrify survey)
Identity is the New Perimeter

The majority of breaches are caused by compromised credentials of end users and privileged users. Attackers know that with the right credentials, they no longer have to fight through the perimeter-style defenses. They simply use stolen credentials to gain access to your critical data, just like an employee. Add in the added complexity of cloud and hybrid infrastructure, new styles of working, and new ways of connecting remotely, a new type of perimeter is needed. Identity is the foundation for the new security perimeter.

#1 Point of Attack is Compromised Credentials

At the core of the vast majority of cyberthreats is the malicious exploitation (or unintended misuse) of user, system or application credentials. According to cyber security experts Verizon and Mandiant, over half — and trending toward 100% — of recent data breaches were due to compromised credentials. These credentials are the digital “keys to the kingdom” and give hackers everything they need to access corporate apps, siphon off sensitive data and damage or destroy critical systems. The Centrify Identity Platform protects against compromised credentials by securing an enterprise’s internal and external users as well as its privileged accounts.

Attackers Target Both End and Privileged Users

Privileged user credentials are the holy grail of cyber attacks. But protecting privileged accounts only solves half the problem. Attackers are increasing their focus on compromising end user credentials in order to leverage corporate access to move laterally into sensitive servers or elevate into privileged accounts. Centrify secures both end users and privileged accounts to stop threats at multiple points in the cyber attack chain.
Traditional Perimeter-based Security is Not Enough

Today's enterprises are rapidly adopting cloud and hybrid infrastructure, new styles of working, and new ways of connecting remotely. Traditional network perimeters secure only the ingress and egress points of the company managed network. Antivirus, next-gen firewalls and VPN aren't enough to thwart attacks on the modern enterprise. Modern enterprises need to define a new perimeter based on identity that secures company resources that are located anywhere; including users, devices, apps, data and infrastructure.

Security Requires Context-based Policies

Unfortunately compromised credentials are the new normal, requiring enterprises to mitigate the risk they represent. Complex and unique passwords are a start but multi-factor authentication and adaptive access are required to detect and stop suspicious login attempts. Additionally, granular privilege management is needed to reduce the impact of compromised credentials. The Centrify Identity Platform allows you to define and enforce context-based policies based on the user’s role, location, device security posture, work schedule and risk profile to mitigate the risk of compromised credentials.
Today’s Threats Require a Next-Generation Identity Platform

Unfortunately compromised credentials are the new normal, requiring enterprises to mitigate the risk they represent. Most enterprises find themselves in the “danger zone” related to their organization’s identity risk.

The major risk for end users are the myriad passwords that they are asked to create, remember, update regularly and self manage. Facing increasing “password fatigue” users often cope by reusing their username and passwords across many apps, use simple mnemonic passwords or worse write down passwords on sticky notes or poorly secured spreadsheets. Worse yet, users are only faced with the most rudimentary of authentication security requiring only a password which may easily be compromised. The result is that end users represent tremendous password related risk.

Privileged users represent a related privilege and policy risk. Privileged users are often granted too much privilege either because temporary access is never rescinded, leading to privilege accumulation over time. Another reason is the false perception that it is “easier” to leave the privileged accounts in place and simply govern shared access to the password. This does little to reduce the attack surface by logging a user into a server without controlling individual privileged actions on that server.

Optimizing your identity risk requires layers of identity and access security. Consolidation of identity silos reduces fragmentation and management overhead. Complex and unique passwords are a start, but only multi-factor authentication and adaptive access are sufficient to detect and stop suspicious login attempts or inappropriate privilege elevation. Workflow is required to manage access requests, grants and revokes. Round these out with complete user session-level auditing and support across all of modern hybrid IT.

With attackers targeting both end users and privileged users any identity security solution must seamlessly covers both. Unfortunately, current solutions focus too myopically on a single aspect of identity security. So what are enterprises to do?
One option is to select, purchase, deploy and integrate a patchwork of partial security solutions for privileged users including a solution for identity consolidation, another for shared account password management (SAPM), one for superuser password management (SUPM), another for privileged access management (PAM), and one for privileged session management (PSM), don’t forget privileged session recording and monitoring (Audit); and solutions for end-users including web and SaaS SSO (IDaaS), a solution for enterprise app SSO (ESSO), multifactor authentication tokens and management (MFA), enterprise mobility management (EMM), mac management, a solution for big data, a solution for cloud infrastructure and the list goes on.

Another approach is to invest in a security platform that gives you full identity security.

Centrify Secures Enterprise Identities

The Centrify Identity Platform provides an integrated solution that secures identities for both end users and privileged users. Additionally, Centrify seamlessly extends beyond an enterprise’s internal users to manage external users such as contractors, vendors, partners and customers who access enterprise resources. As attackers cast a wide net, targeting any and all users, a unified and comprehensive approach to managing identities results in better visibility and more effective protection against breaches. A single integrated Identity solution enables enterprises to avoid the higher costs associated with procuring, integrating and deploying disparate identity solutions designed for just one silo of identity.

Broad Coverage Across Today’s Hybrid IT

The Centrify Identity Platform is a hybrid solution that secures enterprise identities and delivers context-aware access control in the cloud or on-premises to meet the needs of any IT environment. The platform supports thousands of cloud-based and on-premises applications. Supported apps include Office 365, Google Apps, ServiceNow, Dropbox, SAP, Apache, DB2 and Hadoop. The platform also supports hundreds of versions of operating systems that span mobile devices running Android and iOS, laptops running Mac OS X and Windows, UNIX, Linux and Windows servers and mainframes running zLinux.

The Centrify Identity Platform unifies identity to minimize the attack surface, control access and gain visibility across today’s hybrid IT world of cloud, mobile and data center. The result is stronger security, continuous compliance and significantly reduced risk of costly breaches.
Centrify Identity Platform

The Centrify Identity Platform is a next-generation enterprise identity platform purpose-built to protect against the leading point of attack used in data breaches — compromised credentials. The Centrify Platform is delivered as a cloud service and is offered from a choice of global datacenters for privacy and performance. User, administrative and mobile UIs automatically support 15 popular local languages to ensure your users can be productive no matter their locale.

The Centrify Platform built from the ground up to allow Centrify identity solutions to be rapidly created, updated and delivered to you in the shortest time possible ensuring your enterprise identities are always protected with the most up-to-date innovations. The innovations for one solution can quickly be adopted by other solutions reducing costs to you while improving functionality to meet the rapidly changing security landscape. The Centrify Platform offers an array of shared identity services including:

<table>
<thead>
<tr>
<th>Identity Service</th>
<th>Privilege Service</th>
<th>Server Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Directory</td>
<td>Authentication Engine</td>
<td>Multi-factor (MFA)</td>
</tr>
<tr>
<td>Cloud Connector</td>
<td>Federation Engine</td>
<td>Policy Engine</td>
</tr>
<tr>
<td></td>
<td>Reporting Engine</td>
<td></td>
</tr>
</tbody>
</table>

Cloud Connector

The Centrify Identity Platform seamlessly integrates on-premises directories, applications, Macs and mobile devices, servers and network devices through one or more Cloud Connectors. The Cloud Connector is a lightweight and all-in-one windows service that provides enterprise connectivity to the Centrify cloud service. Multiple cloud connectors can be deployed to provide automatic load balancing and failover. This outbound-only connection from the enterprise is secured through a mutually authenticated and encrypted link to the Centrify cloud service.

For Active Directory, the Cloud Connector extends directory data and group policy management for provisioning and management of users, roles, applications accounts, Mac and mobile devices. Helpdesk calls are reduced with support for password expiration reminders, self-service account unlock and forgotten/expired password reset for Active Directory. User self-service for AD attributes allows users to self-manage select AD attributes (such as cell phone number for BYOD environments) while still obeying the access controls of AD.

For applications, the Cloud Connector has built-in services for desktop SSO (via IWA/Kerberos) and Office 365 supporting all of the rich clients such as Outlook and OneDrive ensure seamless access for employees and easy deployment for IT. Built-in app gateway capabilities deliver secure remote access to internal web apps like SharePoint, and SAP — without the hassles and risk of VPN.
For Macs and mobile devices, the Cloud Connector delivers management via Active Directory or the Centrify Admin Portal to ensure appropriate security settings, profiles, certificates and restrictions. Group Policy-based management administers and enforces security settings, device and application restrictions over-the-air and in near real-time. Automated de-provisioning when user accounts are disabled or deleted guarantees all policies and data are removed and computer accounts and certificates are revoked.

For servers and network devices, the Cloud Connector delivers secure remote access over SSH and RDP sessions via the browser and automates shared account password management to on-prem servers and network devices. Privileged sessions and commands on servers can be protected via step-up multifactor authentication via the Cloud Connector.

Cloud Directory

Centrify also provides a cloud storage option for companies that do not use Active Directory or have users that do not belong in AD such as partners or customers. Centrify provides the flexibility to manage just these users in the cloud while also leveraging the users in AD. The Cloud Directory is automatically available to every Centrify cloud tenant owned by the enterprise.

For self-service registration and authentication, Centrify enables users to log in with their existing social credentials from Facebook, LinkedIn, Google or Microsoft. Customers who prefer not to use their social identity can create a Cloud Directory account.

Authentication Engine

Identity Service provides simple, secure, single sign-on for apps both in the cloud and behind your firewall. Thousands of pre-configured app templates take the hassle out of adding your custom internal apps. Custom applications that don't have a pre-configured template can easily be added by your IT admins with a minimum of hassle whether you use SAML, WS-Federation, NTLM, OpenID or username/password for authentication.

Centrify Infinite Apps lets you add web apps in seconds, from your browser, without the need for any custom scripting or configuration. Just use the Centrify App Capture plug-in to automatically discover where credentials need to be entered, and add the new app.

Multi-factor Authentication (MFA)

The single most effective protection to mitigate the risk of compromised credentials is to use additional factors of authentication that cannot be readily used by an attacker. Centrify supports “step up” authentication for application access or privileged user access that considers the user’s complete context including device location, device security posture, network location, time of day, user attributes, and more.

Centrify MFA currently supports the following authentication factors.

- **Mobile authenticator, with fingerprint option**: User will receive a pop-up notification on their iOS or Android smart phone, tablet, or wearable device. Tapping on the Confirm key, or using the fingerprint sensor will complete the authentication.

- **Soft token**: in the Centrify mobile app, user can tap on the Mobile Authenticator code if prompted during sign in or when launching an app. If the device is offline, the user can type the one-time passcode into the authentication prompt.
• **Phone call with simple 1-key response:** User will receive a phone call to the registered phone number (land line or mobile phone). A correct response to the voice prompt will complete the authentication.

• **SMS or email confirmation code:** User can click on a temporary code sent to your registered mobile device or email account. Clicking on this link will complete the authentication.

• **User defined security question:** from the Centrify Identity Service™ user portal, users can define their own security question and answer in free text. The correct response will complete the authentication.

**Federation Engine**

Secures collaboration via federation for business partners and single sign-on (SSO) for end customers. Partner identity management is delivered through identity federation support with leading identity providers, making it easier for organizations to share identity information. Centrify enables customer identity management, social identity support and SSO support for OpenID Connect applications, making it easy for customers to login to an enterprise’s customer-facing applications.

For privileged users, Centrify federates privileged access across an organization’s entire security eco-system, including secure outsourcing of IT and application development. Enables secure remote access for outsourced IT administrators and outsourced developers to its infrastructure through federated authentication.

**Workflow Engine**

Automatically routes self-service app requests, automates management approval, creates necessary accounts, manages entitlements within those accounts, provisions mobile app clients and and revokes automatically when user terminates or changes their role.

Empowers IT admins to request temporary access to the specific systems and network devices they need to manage — from anywhere. Enables administrators to request access to privileged account credentials or to request a privileged session to perform a designated task. Access is granted or denied through an automated management approval workflow.

The Workflow engine also allows ecosystem integration with existing trouble ticket and request/approval systems such as market-leading IT service management products.

**Policy Engine**

The policy engine allows IT to centrally define who has access to what applications and resources through an adaptive access policy based on the user’s context which may include location, user or device attributes and roles layered with multifactor and step-up authentication. The policy engine is also used to enroll devices, detect jailbroken devices, remotely lock or wipe devices and manage hundreds of settings for iOS, Android and Mac devices.
Reporting and Dashboarding Engine

The reporting and dashboard analytics engine allows customers to prove compliance, track usage across the globe, audit and report on user access. Our platform offers more than 50 pre-defined reports and the capability to customize or create reports from scratch to ensure the appropriate information is available to the right decision makers at the right time. Report on who did what, where and when, who has access to what and how they can use that access to meet complex regulatory requirements. Select or schedule packaged attestation reports or create your own.

Robust Management Framework

The Centrify Cloud Manager is an administrative portal unifying delegable admin interfaces for managing the shared services of the Centrify Platform including app access and single sign-on, mobile app management, application account provisioning/deprovisioning, server and network device management, mobile device management, user identity management, role management, policy management, monitoring/dashboarding/reporting on all user and admin activity and administrative settings.

Additional Centrify management tools centralize the discovery, management and user administration of systems through Active Directory. You can configure the UNIX profile of Active Directory users, manage computer properties, and create and manage Centrify Zones and their memberships. Your IT admins leverage tools they are already familiar with; Centrify provides Microsoft Active Directory Users and Computers (ADUC) and Group Policy Object Editor (GPOE) extensions to allow for delegated administration. Day-to-day administration stays within the existing tools and processes that are already established in your organization.

Comprehensive Platform APIs

All of Centrify’s shared platform services and REST APIs can be leveraged by external developers to integrate their own applications with our Centrify Identity Platform.

Centrify also provides a comprehensive set of UNIX command-line and PowerShell tools designed to enable administrators to manage Server Suite Zone data, UNIX data and Active Directory accounts and groups. These command-line tools have also been carefully crafted to integrate with in-house automation or provisioning scripts.
Centrify Identity Solutions

Centrify Identity Service, Centrify Privilege Service® and Centrify Server Suite® products — built on the Centrify platform — secure an organization’s increasingly vast array of cloud applications, mobile devices and datacenter systems across multiple platforms.

**Centrify Identity Service**

Centrify Identity Service is an Identity and Access Management as a Service (IDaaS) solution with integrated mobile and Mac management delivered as a multi-tenant service in the cloud. Identity Service lets enterprises provide access to SaaS and on-premises apps without burdening users with multiple passwords for their work-related applications. Identity Service gives IT and security departments the ability to centrally control which users can access what applications, layers in additional levels of security for access by enforcing policies for Multi-Factor Authentication, and provides context-aware security for users' Mac and mobile devices. Deployment time is reduced with Centrify's catalog of 1000's of pre-integrated web and mobile applications. Identity Service also delivers broad support for 100's of on-premises apps including SAP, DB2 and Sharepoint. Remote workers and third-party users can remotely access on-premises web apps without a VPN, improving security and unlocking the value of existing application investments.

**Centrify Privilege Service**

Centrify Privilege Service improves security when sharing privileged accounts. Privilege Service gives your IT admins secure, always-on access to critical shared account passwords. You control who has access, which account passwords they have access to, and how those passwords are managed.

Privilege Service automates password management and governs privileged access requests for 100’s of UNIX, Linux and Windows OS versions and Juniper, Cisco and HP network devices. Privilege Service delivers secure remote access to UNIX, Linux and Windows systems without a VPN. Privilege Service enables you to monitor and audit access by both internal and third-party users, remote workers and outsourced IT.

**Centrify Server Suite**

Server Suite secures a broad range of mission-critical servers from external and insider attacks by uniquely combining comprehensive bridging of Linux and UNIX systems with Active Directory and powerful privilege management, auditing and session monitoring across Windows, Linux and UNIX systems. Server Suite seamlessly enables Multifactor Authentication (MFA) for step-up authentication when logging into a privileged shared account or when executing commands with elevated privilege. Server Suite automates the implementation of a least-privilege access model, reduces or eliminates risks caused by the proliferation of highly privileged accounts, and makes regulatory compliance repeatable and sustainable.
Why Choose Centrify

Centrify protects against the leading point of attack used in data breaches — compromised credentials

Uniquely protects both end users and privileged users — for both internal and external use cases

Secure cloud, mobile and on-premises resources

Trusted by over 5000 customers, including more than half of the Fortune 50

Validated by leading industry analysts as the market leader

When it comes to protecting against the leading point of attack — compromised credentials — don’t be half protected. Get full identity security with Centrify.

Next Steps

Register for a trial subscription of Centrify Identity Service today to see how it can benefit your organization: www.centrify.com/saas/trial.asp

Centrify is the leader in securing enterprise identities against cyberthreats that target today’s hybrid IT environment of cloud, mobile and on-premises. The Centrify Identity Platform protects against the leading point of attack used in data breaches — compromised credentials — by securing an enterprise’s internal and external users as well as its privileged accounts. www.centrify.com.

Centrify, Centrify Identity Platform and Centrify Server Suite are registered trademarks, and Centrify Identity Service and Centrify Privilege Service are trademarks of Centrify Corporation. Other trademarks mentioned herein are the property of their respective owners.