KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | July 2014

Centrify Server Suite

by **Martin Kuppinger**
mk@kuppingercole.com
July 2014

Content

1 Introduction 3
2 Product Description 4
3 Strengths and Challenges 5
4 Copyright 6

1 Introduction

Centrify is a US based Identity Management software vendor that was founded in 2004. Centrify has achieved recognition for its identity management and auditing solutions including single sign-on service for multiple devices and for cloud-based applications. The company is VC funded and has raised significant funding from a number of leading investment companies. The company as of today has more than 5,000 customers. Centrify has licensed key SaaS and mobile components to Samsung for the Samsung KNOX platform and the cloud service that supports it

Centrify is best known for their capability of integrating UNIX and Linux accounts management into Microsoft Active Directory., but also supports integration of Mac OS X This still is at the core of their Centrify Server Suite. However, the overall portfolio of Centrify has grown, adding the Centrify User Suite for access to Cloud services, and the features of the Centrify Server Suite and its various editions have been significantly extended.

The Centrify Server Suite, beyond its core capability of integrating UNIX and Linux accounts into Microsoft Active Directory, supports privilege management capabilities, integrated cross-platform auditing, dynamic server isolation, and single sign-on to on-premises applications. Based on the feature set, it is a player in the Privilege Management market, even while not following the standard approach – centered on an identity "vault", i.e. a central, strongly secured repository – that is common for this particular market.

Privilege Management - which, in the KuppingerCole nomenclature, also is called PxM for Privileged Access/Account/Identity/User Management- is the term used for technologies which help to audit and limit elevated rights and what can be done with shared accounts. During the last few years, PxM has become increasingly popular. The reason for that growth is the increasing demand in the market. When looking at many of the large information security incidents, which have become well known during the past few years, it becomes obvious that many of them are related to privileged user accounts. Data theft on a large scale is most likely caused by user accounts with elevated rights, typically administrative users.

Centrify plays into that market with various capabilities, including the consolidation of UNIX and Linux identities into Microsoft Active Directory, providing centralized management for such accounts and centralized auditing of the use of such accounts. Thus, identity-related risks in these environments can be identified and mitigated, in contrast to managing a vast number of local accounts across the multitude of UNIX and Linux systems many organizations own. Furthermore, it supports Single Sign-On based on the primary Microsoft Active Directory authentication to other system environments such as SAP, Java/J2EE, various web applications, and a number of databases.

Based on that, a well thought-out concept of individual Active Directory accounts can be implemented to control access to other systems based on individual Active Directory accounts that are well managed and audited. Given that Microsoft Active Directory is a core element in most IT infrastructures today, it is a logical starting point for such integration.

Whether the target of using Centrify Server Suite is improving Privilege Management or just optimizing the user management of UNIX and Linux environments or providing Single Sign-On to a number of environments: There are a number of use cases where the suite can provide significant benefit.

2 Product Description

Centrify Server Suite is a comprehensive solution in which you will find Privilege Management as one of the core features. The breadth and positioning is best understood when comparing the various editions of the product.

The Standard Edition consists of three components. The DirectManage component is used for centralized management and user administration of UNIX and Linux accounts via Microsoft Active Directory. The DirectControl component provides authentication and access control capabilities for access to these accounts, in tight integration with the standard features of Microsoft Active Directory. The DirectAuthorize component adds role-based authorization and privilege elevation capabilities.

The second edition is the Enterprise Edition, which adds the DirectAudit component. This feature set provides the capability of detailed auditing of user activity across all managed platforms. It also integrates session recording and monitoring, including capturing detailed meta-data such as commands executed or files accessed. Privileged access is tracked and associated with an individual's account. The DirectAudit component supports both agent-based and non-agent-based deployment models.

Then there is the Platinum Edition, which further enhances the Enterprise Edition by adding the DirectSecure component for server isolation and protection of data-in-motion. Based on these features, servers can be dynamically grouped into isolated and protected environments. This is based on IPsec support and thus protects information that is transferred between servers in isolated zones.

Finally, there is the Application Edition that can be added to any of the other editions. The Centrify for Applications components support integration and Single Sign-On to SAP environments, various Database Servers, Java/J2EE and web applications.

When looking at the aspect of Privilege Management in particular, Centrify offers a full-fledged Privileged Management product. Differing from the "standard" vaulting approach, it works with Active Directory as the central component instead of using a separate repository. This means that the solution is non-intrusive and requires no schema extensions, agents or software on domain controllers. Centrify recommends an agent be installed on each platform to be managed to eliminate the risk of users circumventing audit policies by accessing servers directly, but also supports jump-box deployments for session auditing.

Managing privileged user's permissions through Active Directory is a technique that has been used in a number of in-house built tools, many with great success. Centrify's customers are implementing a least-privilege access model across the datacenter, cloud, and mobile devices that reduces the need for a password repository.

Centrify enables the granular assignment of privileges based on roles, and enables users to elevate privileges as they are needed while capturing a full audit trail including video capture of privileged sessions. This is a clever way of implementing privilege management and leveraging an already existing critical piece of infrastructure rather than having to design and implement a completely new piece of software.

In addition to user-based identity controls, Centrify's approach to Privilege Management also supports the concept of server and domain isolation. Centrify's customers define which servers/devices are trusted or not, and block access based on the systems they are coming from.

By taking a holistic approach to access management, Centrify Server Suite can not only manage your day-to-day requirements for Identity and Access Management but also deliver Privilege Management using a combination of account emulation and least privilege configured through Active Directory. It should be noted that while most of the features are available in the Standard Edition, to have privileged user auditing you would need the Enterprise Edition.

All editions of Centrify Server Suite come with consistent user interfaces and integration based on a shared architecture between the various components.

3 Strengths and Challenges

Centrify Server Suite is an interesting offering for organizations that run both Microsoft Active Directory and UNIX/Linux environments – which applies to most organizations. It allows integration of user management and authentication of UNIX and Linux users into Microsoft Active Directory and fine-grained, role-based authorization and monitoring of the use of Windows, Linux, and UNIX accounts. Thus, it supports managing entitlements. Depending on the administration and user management concept within Microsoft Active Directory, sophisticated Privilege Management concepts can be implemented for the platforms supported by Centrify Server Suite.

In its domain, the product shows a broad feature set going well beyond just mapping UNIX and Linux users to Microsoft Active Directory. The ability of configuring isolated zones of servers, the advanced Windows, UNIX, and Linux authorization management and audit features, and the Single Sign-On capabilities based on the primary Windows authentication make it an interesting tool for securing and optimizing access to cross-platform servers and systems particularly for administrators and operators, but also end users accessing such platforms directly.

Clearly, the security of such environments also depends on the sophistication of security configuration and management in Active Directory. Among the challenges from a Privilege Management, perspective is the lack of support for other environments such as network devices. Looking at the Centrify Server Suite from the perspective of a Microsoft Active Directory-integrated identity management solution, it is a convincing solution. Overall, it is well worth evaluating Centrify Server Suite for both managing users in heterogeneous environments and as an alternative to the common approaches to Privilege Management.

Strengths	Challenges
• Sophisticated integration of UNIX and Linux account management into Microsoft Active Directory • Role-based control of entitlements for Windows, Linux, and UNIX environments • Management and restriction of elevated privilege use • Support for session monitoring and auditing, including capturing of meta-data • Support for isolation of network zones • Tight integration with application environments, support Single Sign-On	• Does not follow the common “vault” approach for managing passwords for privilege management; might not meet all standard customer requirements (but might serve well to their needs anyway) • Excellent target system support for Windows, Linux, and UNIX privilege management, but lack of support for other targets such as network devices

4 Copyright

© 2014 Kuppinger Cole Ltd. All rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole´s initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice.

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Am Schloßpark 129
65203 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com