

WHITE PAPER
CENTRIFY CORP.
APRIL 2010

Using Microsoft Active Directory to Address Payment Card Industry (PCI) Data Security Standard Requirements in Heterogeneous Environments

With Microsoft Active Directory and Centrifify Suite, you can extend the directory that you already own to non-Windows systems, yielding substantial benefits for your organization through stronger security, streamlined IT operations and detailed user activity audit tracking. Most important, together they enable you to address many of the PCI DSS requirements.

ABSTRACT

The Security Standards Council of the Payment Card Industry (PCI) owns and maintains the Data Security Standard (DSS), which is a rigorous set of requirements that all merchants, payment processors, point-of-sale vendors, and financial institutions must follow. The stiff penalties defined by PCI members are designed to ensure that all merchants and service providers work to maintain consumer trust of payment cards since that loss would impact the revenues of all merchants and financial institutions.

This white paper examines the compelling business and technical case for centralizing administration in Microsoft Active Directory, using the Centrifify Suite to integrate UNIX and Linux systems into Active Directory in order to centralize server protection policies, user authentication and access controls as well as to provide accountability through direct auditing of user activities on these sensitive systems. Combined, Active Directory and Centrifify Suite provide a comprehensive solution to address specific PCI DSS requirements.

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, e-mail 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 Centrifly Corporation.

Centrifly 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 Centrifly, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2010 Centrifly Corporation. All rights reserved.

Centrifly is a registered trademark and DirectAudit and DirectControl are trademarks of Centrifly 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.

[WP-011-2010-04-12]

Contents

1	Executive Summary	1
2	Business and Security Risks that Must Be Addressed for PCI Compliance ...	2
2.1	Payment Card Industry Data Security Standard Requirements Overview	2
2.2	All Members Must Ensure Compliance	3
2.3	Penalties for Non-Compliance Go Beyond Fines	5
3	Using Active Directory In Heterogeneous Environments To Secure, Control And Audit	6
3.1	Enforcing Active Directory Authentication And Access Control	6
3.2	Group Policy Enforcement On Unix Systems	7
3.3	Server Protection and Group-based Isolation	8
3.4	Role-based Access and Privilege Controls	9
3.5	Comprehensive Audit Logging	9
4	PCI Requirements Enabled by the Use of Centrify Suite	10
4.1	Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data	10
4.2	Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters	11
4.3	Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks	12
4.4	Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know	13
4.5	Requirement 8: Assign a Unique ID to Each Person with Computer Access	15
4.6	Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data	19
4.7	Requirement 11: Regularly Test Security Systems and Processes	21
5	Summary	23
6	How to Contact Centrify	23

1

Executive Summary

Since the majority of commercial transactions between businesses and individuals is increasingly being performed using some form of electronic payment involving a payment card instead of cash, there is an increased need to protect card holder data to prevent fraud and identity theft. The Payment Card Industry (PCI) Security Standards Council was formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International with the mission to enhance payment account data security by creating the Data Security Standard (DSS), which describes a common set of best practices that must be enforced on all systems that are involved in payment card processing. We have found that in heterogeneous environments many IT managers are struggling to find solutions to help them address DSS's many requirements, particularly when it comes to securing access to non-Windows systems. As a result, many organizations processing credit cards run the risk of failing their PCI Requirements Audit on their non-Windows systems. This paper will describe how Active Directory along with Centrify Suite can be used together to not only to address many of the PCI remediation issues for a heterogeneous environment but also to deliver significant additional benefits in terms of reducing the cost of maintaining current infrastructure and streamlining existing IT and business processes.

Centrify Suite contains several products that address various aspects of the PCI-DSS requirements which will be described in detail in this document. The DirectControl solution allows IT to extend the infrastructure investment it has already deployed – Microsoft Active Directory – to address the identity and access management of its UNIX and Linux systems and their applications. In addition, Centrify DirectControl's patent-pending Zone technology is an innovative, next-generation solution for delivering the type of fine-grained access control and delegated administration that IT managers need to comply with PCI Requirements and manage a diverse and distributed server environment. DirectControl also provides for the enforcement of Active Directory Group Policies to ensure that non-Windows systems are configured to comply with the desired security policy and stay that way.

Building on the integration with Active Directory, DirectAuthorize provides a Role-based management solution to control rights that users require in order to both access specific systems and applications as well as administrators need to run privileged commands in order to manage these systems. DirectAudit goes further by providing detailed auditing, logging and reporting on user activity within your UNIX or Linux environment in an easy-to-use, secure and reliable manner. DirectAudit granularly tracks activity such as commands that were executed and what changes were made to key files and data. DirectSecure provides an additional layer of security enabling you to logically isolate PCI systems without requiring physical network changes by requiring authentication at the network layer in the host OS for any communications. The combination of Centrify Suite and Active Directory provide the controls and audit to meet the requirements set forth by the PCI Data Security Standard.

2 Business and Security Risks that Must Be Addressed for PCI Compliance

The PCI Security Standards Council has defined a rigorous set of security requirements that all merchants, payment processors, point-of-sale vendors, and financial institutions must comply with in order to retain their right to use the payment system. Members such as Visa have defined stiff penalties, starting with fines and ultimately resulting in the loss of the right to use payment cards, as incentives to comply with these security standards. These penalties are designed to ensure that all merchants and service providers work to maintain consumer trust since the loss of the ability to use payment cards would drastically impact their ability to do business with consumers.

2.1 Payment Card Industry Data Security Standard Requirements Overview

The Payment Card Industry (PCI) Data Security Standard (DSS), or PCI, is comprised of 12 very clearly stated requirements in six major groups as shown below, copied directly from the PCI DSS overview (<https://www.pcisecuritystandards.org>).

Group	Requirement
Build and Maintain a Secure Network	Firewalls are computer devices that control computer traffic allowed into a company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employees' Internet-based access via desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.
	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. This is an illustration of the defense in depth principle.
	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks

Group	Requirement
Maintain a Vulnerability Management Program	Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all e-mail systems and desktops to protect systems from malicious software.
	5. Use and regularly update anti-virus software
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	This ensures critical data can only be accessed in an authorized manner.
	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
Regularly Monitor and Test Networks	9. Restrict physical access to cardholder data
	Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.
	10. Track and monitor all access to network resources and cardholder data
Maintain an Information Security Policy	11. Regularly test security systems and processes
	A strong security policy sets the security tone for the whole company, and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.
	12. Maintain a policy that addresses information security for employees and contractors

Information in this table is from the Payment Card Industry Data Security Standard

These PCI DSS requirements apply to all merchants who accept credit card payments – whether at brick-and-mortar stores, by phone, or through online ecommerce. Unlike the federal Sarbanes-Oxley legislation, which lays out a general principle regarding data security and auditing, PCI is a detailed, multi-point standard with unambiguous guidelines. Through many months of working with analysts, auditors, customers, and partners, Centrifly has gained expertise in identifying issues that spell trouble for customers addressing PCI.

2.2

All Members Must Ensure Compliance

All card processing members subject to PCI are called Service Providers by the program, and there are three service provider levels to identify various compliance validations.

- **The Level 1 Service Provider group** includes all processors that are connected to VisaNet and MasterCard networks. The Level 1 Service Provider group includes all payment gateways that operate between merchant and Global Payments or between merchant and other processors. Level 1 Service Providers was expanded to include Data Storage Entities (DSEs) for Level 1 Merchants (more than 6 million MasterCard or Visa transactions regardless of acceptance channel) and Level 2 Merchants (more than 150,000 and less than 6,000,000 electronic commerce transactions).
- **The Level 2 and Level 3 Service Provider groups** include all third-party service providers (example: Third-Party Servicer (TPS), Independent Sales Organizations (ISO), merchant vendor, web hosting company or shopping cart, media back-up company, loyalty program vendor, risk management vendor, chargeback vendor, and credit bureau) not in Level 1 that store, process, or transmit transactions. The number of transactions will be determined based on the gross number of Visa or MasterCard transactions stored, processed, or transmitted—not just for the merchant or member supported but for all entities supported by a service provider. The Level 2 and Level 3 Service Provider group also includes third-party Data Storage Entities storing data on behalf of Level 3 Merchants (more than 20,000 and less than 150,000 electronic commerce transactions) or Level 4 Merchants (all other merchants, regardless of acceptance channels).

Visa holds the central compliance repository for all companies agreeing to the PCI standard. Visa requires service providers to provide compliance validation results directly to Visa. After a Level 1, 2, or 3 service provider has provided compliance documentation demonstrating full compliance to Visa USA, they will be included on the list of Compliant Service Providers which can be found on the Visa site at:

<http://www.visa.com/cisp>.

The following table summarizes the compliance validation steps required for third parties (including ISOs, loyalty program vendors, etc.) that store cardholder data.

Service provider definition	Description	Validation Action	Validated By
Level 1	All VisaNet processors (member and Nonmember) and all payment gateways.	<ul style="list-style-type: none"> ▪ Annual On-site PCI Data Security Assessment ▪ Quarterly Network Scan 	<ul style="list-style-type: none"> ▪ Qualified Security Assessor ▪ Approved Scanning Vendor

Service provider definition	Description	Validation Action	Validated By
Level 2	Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/transactions annually.	<ul style="list-style-type: none"> ▪ Annual On-site PCI Data Security Assessment ▪ Quarterly Network Scan 	<ul style="list-style-type: none"> ▪ Qualified Security Assessor ▪ Approved Scanning Vendor
Level 3	Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 Visa accounts/transactions annually.	<ul style="list-style-type: none"> ▪ Annual PCI Self-Assessment Questionnaire ▪ Quarterly Network Scan 	<ul style="list-style-type: none"> ▪ Service Provider ▪ Approved Scanning Vendor

Reference: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_service_providers.html?it=c|%2Fbusiness%2Faccepting_visa%2Fops_risk_management%2Fcisp%2Ehtml|Service%20Providers

2.3 Penalties for Non-Compliance Go Beyond Fines

Both Visa and MasterCard impose stiff fines on merchants who cannot demonstrate compliance with their data security protection guidelines. For level 1 merchants, these fines are:

- MasterCard: Up to \$100,000 per day (\$10,000 per day after 60 days), up to \$500,000 annually.
- Visa: \$50,000 for a first violation in a rolling 12-month period; \$100,000 for a second violation in a rolling 12-month period, and a fine set by management for more than two violates within a rolling 12-month period.

Additional fines apply for failure to submit compliance documents.

For a level 1 merchant that experiences significant problems meeting PCI requirements, fines could potentially amount to \$500,000 to \$1,000,000 in a one-year period.

Inability to pass an audit and to show progress toward remediation could even potentially lead to the merchant's losing the right to accept credit card charges.

The threat of fines and loss of card processing privileges are of course crucial business concerns. However, the PCI standards should be viewed not as an onerous requirement but as a guidepost toward best practices. The ultimate goal is to keep customer data protected in an era when some of the nation's most respected companies have had to

admit being hacked or having lost customer data. The loss of customer confidence could be a severe and costly blow to the corporate brand, and could potentially lead to both criminal and civil litigation depending on the circumstances. While the overuse of root access and the use of well known generic accounts put companies at extreme risk; it would take only one ill-intentioned or disgruntled employee to do significant damage.

Although everyone involved wants to hope for the best, planning for the worst is best practice. Being on a path toward remediation represents the difference between good-faith effort and negligence.

3 Using Active Directory In Heterogeneous Environments To Secure, Control And Audit

Microsoft's Active Directory has become the de facto standard identity and access management backbone in most enterprises for providing authentication, authorization, account access, computer policy and infrastructure management for Windows systems and applications. Active Directory has proven itself over the years to be highly scalable, very secure and resilient under just about any load. Additionally, with Active Directory being backed by the world's largest software vendor – Microsoft – it is therefore a low risk, well supported, long-term solution for enterprise class identity and access management. The challenge is that the majority of the systems which run business critical applications are typically running on non-Windows operating systems which do not natively integrate with Active Directory. Centrify Suite takes advantage of Active Directory to provide direct integration and management of these non-Windows systems including UNIX, Linux, Mac, Java, web and database platforms. Additionally, while the Active Directory infrastructure provides for centralized logging of domain based activities such as successful or failed login attempts and password changes, the DirectAudit product within the Suite augments that logging to provide full UNIX user activity reporting and session replay to provide visibility into privileged actions and their responses.

The sections in this chapter will describe the components of the Centrify Suite, DirectControl, DirectAuthorize, DirectSecure and DirectAudit, in more detail explaining how each compliment the Active Directory environment to enable compliance with several of the PCI DSS requirements.

3.1 Enforcing Active Directory Authentication And Access Control

Centrify DirectControl's core feature is its ability to enable UNIX, Linux and Mac servers and workstations to participate seamlessly in an Active Directory domain, establishing Active Directory as your single point of administration and security policy enforcement for your heterogeneous environment. Through Active Directory, you can globally control both administrative and end-user access to non-Windows systems and the Java and web applications running on them. Through Group Policy, you can enforce consistent security and configuration policies across heterogeneous systems.

The Centrify DirectControl suite consists of the DirectControl Agent, which is installed on each managed computer, and the DirectControl Management Tools, which can be installed on any Windows computer with access to Active Directory.

The DirectControl Agent enables the managed computer to join an Active Directory domain and provides comprehensive Active Directory services for that system: authenticates administrator and end-user logins, controls access to any hosted web applications, implements Group Policy updates, and manages all other interaction with Active Directory.

On Windows, the DirectControl property extensions to Active Directory Users and Computers enable administrators to set user and group access rights for the managed systems. Administrators can perform these same tasks with the DirectControl Administrator Console, which in addition enables them to set up Centrify Zones, run reports, configure the DirectControl Agents, and import accounts.

Centralizing user account management in Active Directory eliminates common security exposures, such as the existence of orphan accounts and the elimination of the large number of usernames and passwords that your end users need to remember. However, you still need to integrate these systems into Active Directory in a way that preserves existing security boundaries. For example, users that should only have access to HR systems should not be able to log into your financial systems. Centrify's patent-pending Zone technology leverages the power of Active Directory's access control mechanisms to provide even more granular access control within your mixed environment. Any logical grouping of mixed UNIX, Linux or Mac systems can be segregated within Active Directory as a Centrify Zone. Each Zone can have a unique set of users, a unique set of administrators, and a unique set of security policies. For most customers, the Centrify Zones capability for advanced access control is the "must have" feature that enables them to meet SOX, PCI, and other security requirements.

The beauty of the Centrify Zones technology is that granular access control is controlled centrally within Active Directory, not locally managed at each and every system. In addition, with the DirectControl Management Console you also have a visual interface that enables you to easily view and change these Zone-based access controls. Other products don't offer this ability to see who actually has access to specific systems within your environment; they force you to guess which users can access specific systems. And you can address your audit requirements by running the numerous out-of-the box reports that DirectControl provides that can prove to auditors, on-demand, what systems any specific user can access, and which users can access any specific system.

3.2 Group Policy Enforcement On Unix Systems

One of the more powerful features of Active Directory is its ability to centrally manage and enforce policies across a broad installed base of Windows machines within the enterprise. Windows Group Policy works by forcibly setting user and computer registry keys and since almost all of a Windows system is configured through registry settings,

this is a very natural and simple way to enforce almost any policy. In the UNIX world however, there is no equivalent to the Windows registry, the de-facto standard for configuration is ASCII text files, which may in some cases use XML data structures. To enforce Active Directory's Group Policy capabilities in a UNIX environment, DirectControl creates a "virtual registry" by mapping the registry settings that Group Policy would create to entries in various system files. For each configurable application, DirectControl provides a specific mapper that knows what needs to be set in the configuration file for that application and appropriately updates the values as specified by the virtual registry settings.

The DirectControl Agent will at various times load the Group Policy settings into its virtual registry. This load is triggered by:

- System startup. When the DirectControl daemon starts up (usually when the system boots up), it sets the machine registry.
- User log on. When a user logs on, the DirectControl Agent loads the user's settings.
- Signal or time out. The DirectControl Agent can be signaled to reload. It will also refresh the registry on a periodic basis.

The loading of policy is asynchronous (this is equivalent to the behavior in recent Windows versions). The loaded settings are stored on the local machine for disconnected operation.

Centrify includes a unique set of Active Directory Group Policies that are specific to UNIX, Linux and Mac platforms. These policies can be applied to users or systems, as appropriate. DirectControl includes Group Policy objects to manage logon settings, PAM settings, password prompts, timeout settings, Kerberos settings, NSS overrides, password caching, LDAP settings, user/group maps, crontab settings, firewall configuration, graphical desktop properties, sudo permissions and a growing list of other settings that are suitable for being centrally managed.

3.3

Server Protection and Group-based Isolation

DirectControl and DirectSecure provide policy enforcement of several security controls designed to protect servers and the data that they hold. DirectControl provides Group Policy enforcement to control several security policies such as the IPtables firewall to prevent access to unauthorized ports. However, DirectSecure goes beyond the basic on/off access to specific ports to ensure that remote systems must authenticate prior to communications for a given port. Each computer that is required to adhere to PCI-DSS security standards can also be added to an Active Directory group based on their identity and then configured to only allow communication with other computers within this Active Directory Group. This enables you to isolate PCI systems on any network based on the enforcement of a common security policy.

3.4 Role-based Access and Privilege Controls

One of the primary benefits of the DirectControl solution is that it simplifies the configuration of a more secure environment where UNIX administrators will login with their own personal end user accounts and then run sudo in order to execute privileged commands. This enables the organization to lock down the root account and hold its password secret where only the Chief Security Officer or the highest level administrators are the only ones who know the root password.

In order to provide administrators with the ability to execute privileged commands, Centrify provides two solutions through DirectControl and DirectAuthorize. DirectControl provides a Group Policy for managing the sudo configuration file that defines who can run privileged programs on a UNIX, Linux or Mac system. If the configuration of this file is not strictly controlled across every system in your organization, then security is not only compromised on an individual system but also potentially compromised across your organization. Centrify's Group Policy module enables you to ensure that your systems are configured in a consistent manner that is compliant with your security policies. In order to provide a more granular access and privilege policy enforcement that is much more dynamic, DirectAuthorize provides a role-based solution enabling the definition of specific roles that can be granted a set of rights to both access specific computers on specific interfaces as well as provide specific privileges to run sensitive commands. This solution is much more dynamic given its ability to assign rights to a single user upon login as well as to time limit those rights enabling administrators to grant temporary rights on a single system, something that is not easily accomplished without reducing the security on the machine.

3.5 Comprehensive Audit Logging

While DirectControl enables Active Directory users to log into non-Windows systems and these login events are logged on the Active Directory Domain Controllers, there is still little that can be reported on the exact actions that a user or administrator performed while logged into that UNIX or Linux system. DirectAuthorize goes further to provide a better access control model for granting privileged command execution rights, producing a security log of the commands executed by authorized users. Role-based privileges provide the assurance required that only the appropriate people would be granted the privileges they require to perform their duties. However, by itself this does not provide information about what changes were made to files during the execution of a given command. For example, a user editing the `/etc/passwd` file will simply show that the user ran the `vi` command (editor) on this file, and not report what he did to that file, which entry he added or changed or deleted. For those environments that allow a user to login and `su` to the root account, even less can be determined historically about what actions that user took while operating with privilege on the system.

DirectAudit is designed to provide the auditor with a detailed and centralized view into a user's activities across the audited systems within the enterprise. This solution enables the auditor to view a session that any user performed on one of the audited systems just

as if he were watching over the shoulder of the user seeing everything that the user typed as well as the responses to those commands and actions. The centralized repository that DirectAudit establishes for this log data can be queried to find suspicious activity for a user across any of the audited systems within the enterprise with ease.

Based on the robust logging of DirectAudit on these mission critical systems and the direct linkage of the user's UNIX account that DirectControl establishes with the user's Active Directory login account, the combined solution along with Active Directory is well positioned to enable you to rapidly deploy a solution to meet many of the more difficult requirements of the PCI DSS standard.

4 PCI Requirements Enabled by the Use of Centrify Suite

Centrify Suite meets several of the 12 major requirements of PCI and goes into depth on three of them. Centrify DirectControl and DirectAuthorize combine with Active Directory to provide a solution for all of the subsections of Requirement 7, "Restrict access to cardholder data by business need-to-know" and Requirement 8, "Assign a unique ID to each person with computer access." DirectControl and DirectSecure combine to address the critical issue of Requirements 1 "Install and Maintain a Firewall Configuration to Protect Cardholder Data, 2 "Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters" and 4 "Encrypt Transmission of Cardholder Data Across Open, Public Networks". Additionally, Centrify Direct Audit when combined with DirectControl provides a solution to meet all of the requirements defined in Requirement 10 "Track and monitor all access to network resources and cardholder data."

Many of the PCI DSS requirements provide further details to ensure that the requirement is not left ambiguous and to ensure that proper guidance is given to the administrator. In this section we examine the detailed requirements and describe in more detail how Active Directory and Centrify Suite can be used to address these detailed PCI DSS requirements. The requirements in these tables were taken from the Payment Card Industry Data Security Standard.

4.1 Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

DirectControl provides a Group Policy to control the iptables-based firewall on Linux systems to help address the requirement defined in 1.3 of the PCI DSS requirements. This Group Policy can be used to define a firewall policy, enforce that policy on the Linux systems, and ensure that it is properly enforced over time through its built-in periodic refresh interval.

DirectSecure builds on top of this host-based firewall to provide advanced security services to ensure that PCI systems are only able to communicate with other trusted systems. DirectSecure builds upon both IPsec to protect individual packets in a peer-to-

peer configuration once the remote computer has been mutually authenticated and validated as a trust host with authorization to communicate.

PCI Requirement	Centrify Suite Capabilities
<p>1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.</p> <p>1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.</p> <p>1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using</p>	<p>DirectControl provides Group Policy based enforcement of an iptables-based firewall. By using this policy, administrators can restrict inbound traffic to specific ports from specific IP addresses.</p> <p>DirectSecure provides additional protections for the server by requiring authentication before any communication is required. This can be applied to both inbound as well as outbound communications to ensure that PCI systems will only be able to communicate with other PCI systems.</p>
<p>Req 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.</p> <p>1.3.5 Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.</p>	<p>Additionally, when mutual authentication is required prior to communications with any other system, DirectSecure will prevent communications with untrusted systems or any other system outside the corporate network since they are not trusted and cannot authenticate. DirectSecure enforces this method of firewall protection providing the most secure form of network protection ensuring that a computer will only allow communications with other trusted systems.</p>

4.2 Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Requirement 2.3, which mandates the encryption of all non-console administrative access, can additionally be met with the proper configuration and use of OpenSSH. When OpenSSH is combined with DirectControl, it provides administrators single sign-on using their more secure Kerberos ticket for authentication, while OpenSSH ensures that the traffic is encrypted on the network. Centrify also makes available the latest version of OpenSSH as a convenience for our customers that want to provide this functionality across their heterogeneous infrastructure.

PCI Section	Centrify DirectControl Capability
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/Transport Layer Security (TLS) for Web-based management and other non-console administrative access.	<p>While it is common to find telnet in use on many systems, telnet is insecure and should be replaced with SSH since SSH provides for network transport security. Newer versions of OpenSSH support Kerberos as the method for the user to authenticate; when combined with DirectControl, this eliminates the need to manage static ssh keys.</p> <p>Centrify also provides a compiled and easy-to-install version of the latest OpenSSH, which enables our customers to ensure that they have a consistent version of OpenSSH across all their systems to provide the highest level of security.</p>

4.3 Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

While most applications will encrypt data in transit between systems, there are many more applications that were not designed to provide network encryption services themselves. DirectSecure provides both integrity and confidentiality for all communications between trusted systems.

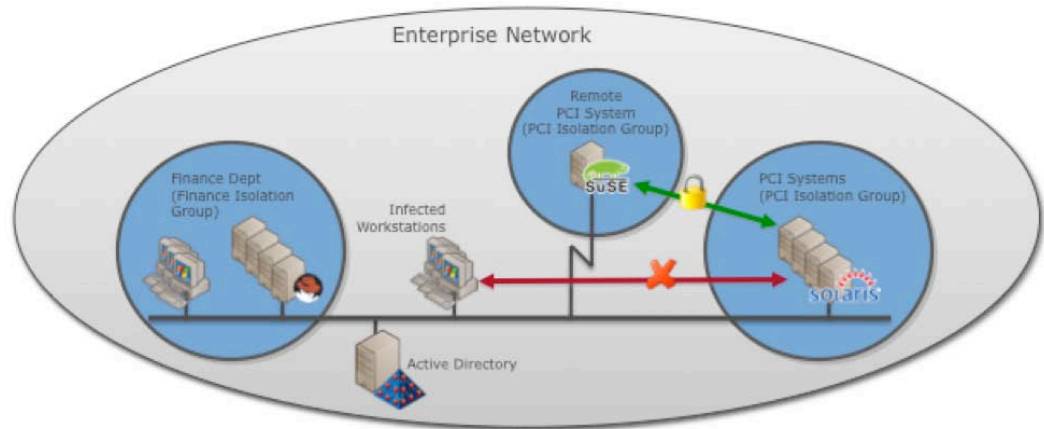
PCI Requirement	Centrify Suite Capabilities
4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.	DirectSecure provides IPsec based integrity and confidentiality services at the network transport layer to encrypt all communications between any application on the system and other trusted remote hosts. Since this solution provides encryption services at the network layer, there is no need to modify any application to support this level of data protection.

The Heartland data breach was one of the largest data breaches of 2009 and even though they were recently certified as PCI-DSS compliant, the hacker was able to gain access to payment card data through malicious code that sniffs the internal network for the data. While requirement 4.1 does not specifically state that encryption is required on internal networks, these attacks are sophisticated in nature and follow the same attack model described earlier requiring strong host isolation and network encryption. There are several other reasons why encryption should be used for all PCI data transfers on both external and internal networks. For example in retail environments the local store network typically provides both wired and wireless connections, which will require proper configuration to ensure that any data does not leak out of the wireless, network connections. Additionally, many retail environments that sell technology product are increasingly requiring Internet access in order to demonstrate those products, again making it difficult to separate the network and traffic based on the usage, PCI

transactions or demonstrations. Again, the best way to address the need to secure PCI data in transit on these networks is to encrypt the data at the source host so that it will never travel over a network connection without being encrypted.

Organizations with wide area networks will find that a host-based solution to provide server isolation and encryption of data in transit will provide much more flexibility than a hardware-based solution, enabling them to easily group and isolate those servers supporting PCI functions regardless of their location on the WAN. Additional benefits of this host-based software solution include:

- Reduces the expense associated with a PCI audit by reducing the number of servers “in scope” for the audit, limiting the scope to your “trusted” PCI systems.
- Eliminates expense and ongoing management costs associated with the acquisition and maintenance of traditional approaches including VLANs, Firewalls and Routers.



▪ Figure 1. Server Isolation and encryption of data-in-transit across a WAN

4.4 Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

Centrify DirectControl provides the unique ability to group similar systems for access control purposes as well as delegated administrative purposes through the use of DirectControl Zones. These Zones can be used to grant a user access to only a specific set of systems on a need-to-know basis. By default, the user is denied the right to login to any other systems in Zones where he does not have membership. Centrify realizes that, in most environments, access to non-Windows systems is granted on a least-access model, where users are granted access only to systems that they need to access, which is quite the opposite of most Windows environments that allow users to log into any system that trusts the Active Directory domain where the user has an account. This Zone concept can

also be coupled with machine-specific, Group Policy-controlled access and deny configurations that can be used to define more restrictive access policies.

PCI Section	Centrify DirectControl Capability
<p>7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access</p>	<p>DirectControl provides several mechanisms to support controlling access to specific non-Windows systems that enable administrators to define and centrally manage user access controls. The following access control methods can be used to restrict access to non-Windows systems:</p> <ul style="list-style-type: none"> • DirectControl Zones • pam.allow and pam.deny rules • Active Directory-allowed hosts <p>DirectControl uses Zones as a way to control which users are granted access to specific systems. By default, Active Directory users do not have permissions to log into any DirectControl-managed system. However, by adding a user to a Zone and creating a UNIX profile for that user within Active Directory, the user will be granted access to the computer systems that are a member of the Zone the user was added to. This results in a configuration where DirectControl can show visually as well as report on which users have access to specific systems.</p> <p>Additionally, Active Directory groups can be used within a pam.allow configuration rule within DirectControl to further restrict which users within a given Zone are allowed to login to that specific system. The pam.allow and pam.deny configuration settings can be used to restrict access for individual users or groups of users. Active Directory Group Policy can also centrally control these rules.</p> <p>Active Directory also provides a profile setting for each user that allows an administrator to define a specific list of computers that the user is allowed to login to. With DirectControl, all non-Windows systems have a valid computer account within Active Directory, which enables Administrators to define not only Windows computers, but also non-Windows systems in this list of allowed computers.</p> <p>These access control rules can all be applied to define the exact access control policy that is required for the specific computer.</p>

PCI Section	Centrify DirectControl Capability
<p>7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.</p>	<p>DirectControl enables administrators to centrally manage a user's UNIX UID and group memberships, which are then used by the operating system to control a user's access to specific files and applications.</p> <p>In order to provide tighter controls around privileged operations, DirectControl provides a Group Policy to enable centralized management of sudo permissions to ensure that the appropriate permissions are applied to local accounts in a consistent manner across the computers where this privilege should be granted. DirectAuthorize extends this functionality to define a set of Roles that will be granted specific access and privileged command Rights. These Roles are defined on Active Directory enabling both AD users and AD groups to be assigned to the Role, simplifying ongoing management.</p> <p>These tools also serve to produce an audit trail of all privileged operations since sudo will log all command execution where the more simple su command does not provide this level of visibility, nor does allowing a user to login as the root account.</p> <p>DirectControl also provides a mechanism to control the root account password policy through Active Directory to further protect those accounts that would otherwise be able to gain unbridled access to a non-Windows system.</p>

4.5 Requirement 8: Assign a Unique ID to Each Person with Computer Access

Centrify DirectControl, with its tight integration with Active Directory, provides complete, centralized control of all user identities for authentication, authorization and access control. It ensures that all users have unique UNIX credentials that are directly associated with the user's Active Directory account, and provides out-of-the-box functionality for the centralized control of passwords and password policies associated with the user's unique credentials.

Centrify DirectControl with Active Directory implements a Kerberos-based authentication solution for both local and remote access, ensuring that the user's password is never transmitted over the network for the authentication event. DirectControl leverages Active Directory's native password policy and authentication policies to ensure that these security policies are enforced regardless of the interface that a user may use for authentication to the host. These Active Directory account and password policies provide the use of first-time passwords, deactivation of users based on time limitations, password complexity, time of use, duration restrictions, account lockout, and idle restrictions on access to applications.

PCI Section	Centrify DirectControl Capability
<p>8.1 Identify all users with a unique username before allowing them to access system components or cardholder data</p>	<p>UNIX systems have limitations such as maximum length of the login name that make it very difficult for IT staff to establish policies to ensure that an account is unique across the enterprise. Additionally, it can be challenging to identify the actual person that owns a specific UNIX account due to the default account database limitations that simply do not provide this ability.</p> <p>By using Active Directory, all users have a single globally unique Active Directory account that DirectControl then links to a user's specific UNIX profile, which eliminates any ambiguity about who owns a specific UNIX account or the files created by that account.</p> <p>We also find in actual deployments that different groups of UNIX systems may actually have a local UID name space that overlaps other groups of systems within the environment. DirectControl Zones provide the ability to allow a user to have more than one UNIX profile for each of these groups of UNIX systems, thus eliminating any account or file ownership ambiguity while at the same time preserving access control integrity.</p>
<p>8.2 Employ at least one of the methods below, in addition to unique identification, to authenticate all users:</p> <ul style="list-style-type: none"> ▪ Password ▪ Token devices (for example, SecureID®, certificates, or public key) ▪ Biometrics 	<p>Active Directory supports both userid and password as well as Smart Card-based login for users' initial login to Windows computers. Once logged into a Windows computer, a user can then access a UNIX system and, depending on the application that they are accessing, can either login with their Active Directory userid and password. Or, if the application supports it, they gain single sign-on access by leveraging the Kerberos ticket that the user was provided at initial login.</p> <p>For interactive login to UNIX systems, DirectControl supports userid and password login only. However, if a user's Active Directory account is configured to only allow an interactive login with a Smart Card, then DirectControl will refuse a userid and password-based login for that user and will require a Kerberos ticket-based authentication.</p>
<p>8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS) with tokens, or VPN with individual certificates.</p>	<p>This requirement must be met by network access control systems prior to a user's access to a UNIX or Linux system. Once a user is authenticated properly to the remote network, access to the UNIX or Linux system is handled as if the user were on the local network.</p>

PCI Section	Centrify DirectControl Capability
8.4 Encrypt all passwords during transmission and storage, on all system components.	DirectControl enforces all Active Directory account and password policies and authenticates users by performing a Kerberos password validation with one of the domain controllers in the domain where the user's Active Directory account is defined. A Kerberos password validation is performed as a cryptographic operation where the password is never transmitted over the network to the domain controllers, since it is only used to encrypt data which can then be used by the domain controllers to validate the authentication attempt.
8.5 Ensure proper user authentication and password management for non-consumer users and administrators, on all system components as follows:	DirectControl enforces all Active Directory authentication and password policies for user login. With Centrify DirectControl, the capabilities of Active Directory are extended to non-Windows systems in addition to Windows systems.
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	User account administration is centrally managed within Active Directory, which provides a robust environment to delegate the administration of user accounts to the appropriate Active Directory administrator. DirectControl extends this delegated administration to support the delegation of UNIX profile management to the appropriate UNIX administrator without requiring the Active Directory administrators to grant elevated privileges within Active Directory. The result is an environment where UNIX administrators are allowed to grant or deny access to UNIX systems, but do not have the right to create a new user within Active Directory. Additional controls are provided to prevent Active Directory administrators from creating a UNIX profile which would result in a UNIX user with elevated privileges.
8.5.2 Verify user identity before performing password resets	DirectControl requires a user to properly authenticate to Active Directory before he is allowed to change his password.
8.5.3 Set first-time passwords to a unique value for each user and change immediately after first use.	DirectControl forces users to change their password upon initial login whenever the Active Directory account is configured to require the password to be changed at next login. This is normally set up on initial account creation as well as any time an administrator resets a user's forgotten password or locked account.
8.5.4 Immediately revoke accesses of terminated users.	Terminated user accounts are controlled through Active Directory with Centrify DirectControl. Upon Active Directory account termination, disabling, or deletion, DirectControl immediately refuses user login.

PCI Section	Centrify DirectControl Capability
8.5.5 Remove inactive user accounts at least every 90 days.	<p>Inactive user accounts are controlled through Active Directory with Centrify DirectControl. DirectControl properly updates the last login time for the user's Active Directory account so that it is possible to determine which accounts have not been used within 90 days.</p> <p>It is up to the administrator of the domain to manually ensure that inactive users are removed from the domain on a 91 day basis.</p>
8.5.6 Enable accounts used by vendors for remote maintenance only during the time needed.	<p>Active Directory provides both a time-of-day restriction as well as an account termination date, which can be used to restrict an account's ability to be used for login to all systems.</p> <p>DirectControl also provides a control to enable the UNIX administrator to selectively enable and disable a user's specific UNIX profile, which can be useful when a user needs periodic access to a group of UNIX systems.</p>
8.5.7 Communicate password procedures and policies to all users who have access to cardholder information.	<p>Administrators need to inform users of the password policies and procedures. However, it is important to note that, with DirectControl, these policies and procedures are enforced identically on both Windows and UNIX and Linux systems.</p>
8.5.8 Do not use group, shared, or generic accounts/passwords.	<p>DirectControl creates an environment where users login with their own Active Directory account and use sudo to gain privileged access for the specific set of commands that the user is required to use for their role within the organization.</p>
8.5.9 Change user passwords at least every 90 days.	<p>Active Directory's password policy can be set to expire and require reset on a time limit of 90 days or less. DirectControl enforces this policy on non-Windows systems.</p>
8.5.10 Require a minimum password length of at least seven characters.	<p>Password policy is set within Active Directory and can be set for any length of password. DirectControl enables non-Windows systems to use passwords of much longer length than would otherwise be possible for the system to handle since Active Directory is used to validate the user's password.</p>
8.5.11 Use passwords containing both numeric and alphabetic characters.	<p>Password policy is set within Active Directory and can be set to require complex password with both mixed case as well as mixed alphanumeric construction. DirectControl enforces this policy on non-Windows systems.</p>
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	<p>Password policy is set within Active Directory and can be set to maintain password history and prevent the reuse of passwords. DirectControl enforces this policy on non-Windows systems.</p>

PCI Section	Centrify DirectControl Capability
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	Account lockout policy is set within Active Directory and can be set to lock out accounts after a specified number of invalid login attempts. DirectControl enforces this policy on non-Windows systems.
8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID.	Account lockout policy is set within Active Directory and can be set to lock the account for a specific duration as needed. DirectControl enforces this policy on non-Windows systems.
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.	Centrify provides a binary distribution of OpenSSH that is configured to use the DirectControl Kerberos libraries to ensure that a user will be able to gain single sign-on access to a remote host. The OpenSSH server can be configured to require that a user session timeout after a specified period or inactivity, such as 15 minutes. After timeout, it will challenge the user for authentication credentials.
8.5.16 Authenticate all access to any database containing cardholder information. This includes access by applications, administrators, and all other users.	Centrify provides configuration tools and plugins as needed in order to integrate the authentication of Oracle, DB2, Sybase and Informix databases into Active Directory to enable centralized account and password policy enforcement.

4.6 Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

Centrify DirectControl with Active Directory consolidates all user authentication logs into Windows Domain Controller logs, additionally all user or group administrative activities are logged centrally by Active Directory. With the use of third-party tools, these logs can be collected, further consolidated, and mined for information on the security and health of the customer's systems. Microsoft Operation Manager can also be used to gather these logs from the domain controllers so that alerts can be triggered for the service provider of both impending and existing problems in security.

Centrify DirectAudit provides auditors with full visibility to all actions that users or administrators have taken while logged into UNIX or Linux systems enabling detailed logging of user session activity. The logs that DirectAudit creates are consolidated into a central SQL based repository to enable auditors to use the DirectAudit Auditor console to query users' actions across a collection of audited systems or to see all currently active user sessions on the audited systems. The combination of DirectControl providing the link between a UNIX login account and the person entry within Active Directory that owns the account and DirectAudit providing full user activity logs will enable your organization to meet the majority of the requirements presented within Requirement 10.

PCI Section	Centrify DirectControl & DirectAudit Capabilities
<p>10.1 Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user.</p>	<p>DirectControl establishes a valid user context for the UNIX account, which is unambiguously linked directly to an Active Directory account to ensure that all audit trails can be traced back to an individual person.</p>
<p>10.2 Implement automated audit trails to reconstruct the following events, for all system components:</p> <ul style="list-style-type: none"> ▪ 10.2.1 All individual user accesses to cardholder data ▪ 10.2.2 All actions taken by any individual with root or administrative privileges ▪ 10.2.3 Access to all audit trails ▪ 10.2.4 Invalid logical access attempts ▪ 10.2.5 Use of identification and authentication mechanisms ▪ 10.2.6 Initialization of the audit logs ▪ 10.2.7 Creation and deletion of system-level objects. 	<p>DirectControl enables tracking of all user authentication and account management operations through the logs maintained on the Active Directory domain controller performing the action. The Active Directory Domain Controllers will log all login attempts, both successful as well as invalid.</p> <p>Additionally, DirectAudit creates and centrally stores a log of all user action taken on the system for both Active Directory users as well as local accounts. The log contains all actions taken regardless of the privilege level of the user, including any user access of the audit trails or logs and system level objects. Since the audit logs are stored within a central system that is not located on the audited system, security is enhanced given that a second machine is involved that also enforces access controls on all database privileged access.</p>
<p>10.3 Record at least the following audit trail entries for each event, for all system components:</p> <ul style="list-style-type: none"> ▪ 10.3.1 User identification ▪ 10.3.2 Type of event ▪ 10.3.3 Date and time ▪ 10.3.4 Success or failure indication ▪ 10.3.5 Origination of event ▪ 10.3.6 Identity or name of affected data, system component, or resource. 	<p>DirectControl logs all authentication events locally via the UNIX standard syslog service. Additionally, all login attempts that are performed on systems that are on the network will also be logged separately on the domain controller that is performing the authentication or account management operation. These logs identify the user performing the action, the date and time of the action.</p> <p>DirectAudit extends the operating system and Domain Controller logs with full details on the user activity that will include date time stamps on all actions such as login, logout, command execution, file access and manipulation that is done via a command shell. The log will show the Active Directory person who performed the action, the shell that they were logged into, where they were connected from as well as the details of their actions and the corresponding results or response to that action.</p>
<p>10.4 Synchronize all critical system clocks and times.</p>	<p>DirectControl automatically configures and enforces the Time Sync Policy that is defined within Active Directory Group Policy on all UNIX and Linux systems that are joined to Active Directory. This time sync will be performed with the Active Directory domain controller infrastructure, which should be configured for time sync with a stratum 1 clock.</p>

PCI Section	Centrify DirectControl & DirectAudit Capabilities
<p>10.5 Secure audit trails so that they cannot be altered.</p> <ul style="list-style-type: none"> ▪ 10.5.1 Limit viewing of audit trails to those with a job-related need ▪ 10.5.2 Protect audit trail files from unauthorized modifications ▪ 10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter ▪ 10.5.4 Copy logs for wireless networks onto a log server on the internal LAN ▪ 10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). 	<p>DirectAudit has been architected to prevent unauthorized viewing or manipulation of the user session logs. This is accomplished by the audit daemon as it securely transmits the audit log to a centralized collector which will store the data into a SQL Server repository under tight access control policies. The audit logs are typically never stored locally, unless the network connectivity to the collector is down at which time it will cache locally and spool off to the collector when network connectivity is restored.</p> <p>DirectAudit's Auditor console will only allow authorized Auditors to view the user sessions once logged in using their Active Directory credentials to the workstation running the console. This is designed to control which personnel have access to the centralized logs.</p> <p>Microsoft SQL Server is used to store and manage the audit data so that established the data can be protected with strong access controls and that access can be logged.</p>
<p>10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and account protocol (AAA) servers (for example RADIUS).</p> <p><i>NOTE: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.</i></p>	<p>DirectAudit stores the audit data in a plain text, non-proprietary format so that other tools such as SQL Reporting Services can be used to analyze the data and generate alerts as needed.</p>
<p>10.7 Retain audit trail history for at least one year, within a minimum of three months online availability.</p>	<p>Standard data backup and restore procedures can be used to manage the log data that DirectAudit stores within the SQL Server repository to enable a backup policy that complies with this requirement.</p>

4.7

Requirement 11: Regularly Test Security Systems and Processes

The strongest form of intrusion prevention is to ensure that all communications into and out of a sensitive system must be authenticated in order to effectively control access to the data held by that system.

PCI Requirement	Centrify Suite Capabilities
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.	<p>While DirectSecure is not exactly designed as an intrusion prevention system, it can be configured as described above to only allow specific trusted systems to communicate, thus preventing intruders from accessing PCI systems.</p> <p>DirectSecure leverages Group Policy to manage the local IPsec and firewall security policies as defined within Active Directory to ensure that these policies are kept up-to-date.</p>

DirectSecure presents a new model for preventing intrusion and data leakage by allowing communications only with other trusted PCI compliance systems. If an attacker were to gain access to an internal network or other untrusted systems on the network, there would be no way to gain access to a properly configured IPsec-protected system thus the intrusion will be prevented.

5 Summary

Active Directory is a proven, secure, scalable, highly available distributed infrastructure and identity management solution backed by the world's largest software vendor – Microsoft – and is therefore a low risk, well supported, long-term solution. Centrify Suite is built by a leading identity management firm – Centrify – which has established strong partner relations with Microsoft and other major enterprise vendors.

With Centrify's DirectControl, DirectAuthorize, DirectSecure and DirectAudit combined with Microsoft's Active Directory, you can now extend the directory you already own to UNIX, Linux, Mac, Java/J2EE, web and database environments, yielding substantial benefits for your organization through lower costs, better security, simplified management, increased productivity, secured and centralized audit tracking and, most important in this case, a significant start on your PCI compliance efforts.

6 How to Contact Centrify

North America
(And All Locations Outside EMEA)

Centrify Corporation
785 N. Mary Avenue., Suite 200
Sunnyvale, CA 94085
United States

Sales: +1 (408) 542-7500

Enquiries: info@centrify.com

Web site: www.centrify.com

Europe, Middle East, Africa
(EMEA)

Centrify EMEA
Asmec Centre
Merlin House
Brunel Road
Theale, Berkshire, RG7 4AB
United Kingdom

Sales: +44 118 902 6580