

WHITE PAPER
CENTRIFY CORP.
FEBRUARY 2006

Centrifify DirectControl & Regulatory Compliance

With Centrifify's DirectControl and Microsoft's Active Directory, you can now extend the directory you already own to Linux, UNIX, Mac, Java/J2EE and web environments, yielding substantial benefits for your organization through stronger security and streamlined IT operations. Most important, DirectControl delivers a big jump start on your regulatory compliance efforts.

ABSTRACT

This white paper provides an overview of the four major compliance regulations and what they mean to the IT community. It categorizes the relevant solutions using a technical framework, and it identifies seven areas where Centrifify DirectControl extends compliance beyond the existing Windows operation system. This paper also introduces the background of regulatory compliance laws, then describes how these laws map to IT solution areas, and finally takes an in-depth look at how Centrifify DirectControl with Active Directory meets the requirements of regulatory compliance in these solution areas.

In addition, this whitepaper continues the review and analysis of how Centrifify DirectControl assists users with compliance. A companion white paper, [Using Microsoft Active Directory to Address Sarbanes-Oxley \(SOX\) Compliance in Heterogeneous Environments](#) by the Robert Francis Group (October 2005), examined how Active Directory can address compliance at a higher, less detailed level. This paper takes a specific look at how Centrifify DirectControl can address regulatory compliance and how it enhances technology solutions for compliance.

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.

© 2006 Centrifly Corporation. All rights reserved.

Centrifly 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-007-2006-02-28]

Contents

Introduction	1
1 Introduction to Regulatory Compliance	1
1.1 Sarbanes-Oxley Act (SOX)	2
1.2 Gramm-Leach-Bliley Act (GLBA)	2
1.3 Health Insurance Portability and Accountability Act (HIPAA)	2
1.4 European Union Data Protection Directive (EUDPD)	3
2 The Business Opportunities of Compliance	3
2.1 Improve Processes	3
2.2 Create a Competitive Advantage	3
2.3 Further Integrate IT Into the Business	4
2.4 Avoid the Checklist Approach.....	4
3 Mapping Regulations to Control Categories	4
3.1 Mapping Technology Solutions for Regulatory Compliance	5
3.2 Centrifly Coverage of Compliance Technology Solutions	5
3.3 Centrifly and Identity Management Solutions.....	5
3.3.1 A Solution for NIS/NIS + and etc/passwd Issues	6
3.3.2 Directories	7
3.4 Centrifly and Authentication, Authorization, and Access Control Solutions	7
3.5 Centrifly and Host Control Solutions	8
3.6 Centrifly and Change Management Solutions	9
3.7 Centrifly and Network Security Solutions.....	10
3.8 Centrifly and Data Encryption and Transmission Solutions.....	11
3.9 Centrifly and Security Integration	12
4 Active Directory and DirectControl – the Right Choice for Compliance	12
5 How to contact Centrifly.....	13

Introduction

This white paper provides an overview of the four major compliance regulations and what they mean to the IT community. It categorizes the relevant solutions using a technical framework, and it identifies seven areas where Centrify DirectControl extends compliance beyond the existing Windows operation system.

Centrify DirectControl with Active Directory provides at least seven ways to meet the requirements of regulatory compliance. Centrify DirectControl with Active Directory lets you:

- Solidify identity management with a consolidated directory service
- Provide a comprehensive approach to authentication, authorization and access control
- Standardize on the control of all hosts (platforms)
- Efficiently implement change control on your environment
- Improve control and monitoring of network security
- Harden data transmission
- Help integrate security applications such as a consolidated LDAP

This paper introduces the background of regulatory compliance laws, then describes how these laws map to IT solution areas, and finally takes an in-depth look at how Centrify DirectControl with Active Directory meets the requirements of regulatory compliance in these solution areas.

In addition, this whitepaper continues the review and analysis of how Centrify DirectControl assists users with compliance. A companion white paper, [Using Microsoft Active Directory to Address Sarbanes-Oxley \(SOX\) Compliance in Heterogeneous Environments](#), by the Robert Francis Group (October 2005), examined how Active Directory can address compliance at a higher, less detailed level. This paper takes a specific look at how Centrify DirectControl can address regulatory compliance and how it enhances technology solutions for compliance.

1

Introduction to Regulatory Compliance

Increased government oversight has resulted in new regulations that impact many organizations in a wide range of industries. Some of the most significant regulations include the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and national legislation based on the European Union Data Protection Directive (EUDPD), such as the Finnish Personal Data Act (523/1999) and Amendment (986/2000) of Finland. Given the

impact these regulations have on a large number of companies, we discuss only the first four in this paper, but other compliance regulations apply, including: the Credit Card Processing Industries, Payment Card Industry Data Security Standard; FDA CFR 21; SEC 17a-4; the USA Patriot Act; California SB 1386; BASEL II; and the Japan Privacy Act.

1.1 Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act of 2002 (SOX) was enacted in response to several corporate scandals. The most prominent part of SOX, from an IT and internal control perspective, is Section 404. This section requires that the annual reports of public companies include an assessment, such as of the end of each fiscal year, of the effectiveness of internal controls over financial reporting. Section 404 also requires that the company's independent auditors attest to, and report on, this assessment. The assessment of financial controls has been extended into the IT space by the opinion of the Public Company Accounting Oversight Board (PCAOB), which is a private-sector, non-profit organization created by the Sarbanes-Oxley Act of 2002 to oversee the auditors of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, fair and independent audit reports. This extension of financial controls into the IT space provides most of the impetus for IT controls.

1.2 Gramm-Leach-Bliley Act (GLBA)

The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act, (GLBA), protects the privacy and security of private financial information that is collected, held, and processed by financial institutions. The privacy component of GLBA requires financial institutions to provide their customers with an annual notice of their privacy practices and to allow customers to choose not to share such information. The safeguards component of the regulation requires that financial institutions establish a comprehensive security program to protect the confidentiality and integrity of the private financial information in their records.

1.3 Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) includes, among its various components, privacy and security rules. These rules focus on Protected Health Information (PHI) and Electronic PHI (ePHI) that are gathered in the process of streamlining the health care system and mandate the standardization of electronic transactions, code sets, and identifiers. The privacy and security rules are detailed and prescriptive. Although the regulation focuses on the healthcare industry, other companies can be impacted if they engage in certain activities, such as the management of employee group health plans, or if they provide services to companies that are directly impacted by the regulation.

1.4 European Union Data Protection Directive (EUDPD)

The European Union Data Protection Directive (EUDPD) standardizes the protection of data privacy for citizens throughout the European Union (EU) by providing baseline requirements that all EU member states must achieve in national regulations. The EUDPD has a strong influence on international regulations due to the limitations it puts on sending EU citizens' personal information outside of the European Union to areas that are deemed to have less than adequate standards for data security. Examples of specific laws in countries representing EU member states are: the Finnish Personal Data Act (523/1999) and Amendment (986/2000) of Finland; the Act on Processing of Personal Data (Act No. 429) of 31 May 2000 of Denmark; and the Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000 - DSG 2000) of Austria. The EUDPD and the regulations enacted pursuant to it impact companies that do business in the EU, or that handle the data of EU citizens.

2 The Business Opportunities of Compliance

Regulatory compliance not only presents obstacles to be overcome, it can also offer opportunities to improve the business. These business opportunities include a chance to improve processes, create a competitive advantage, and further integrate IT into the business. But like any opportunity there is also a risk of focusing too closely on compliance and missing overall security issues.

2.1 Improve Processes

Most regulations require that organizations have documented and repeatable business processes, and that those processes have appropriate controls in place to prevent mistakes or fraud. Because automated processes generally have more effective controls than manual processes, and because auditors generally prefer automated processes to manual ones, many organizations can use regulatory compliance to justify automating inefficient processes. Although the primary justification for automating processes is to improve controls and repeatability, it has the side effect of improving efficiency.

An example of this phenomenon is identity management. Many auditors have drawn attention to the lack of controls around the user life cycle management process (user account creation, modification, and deletion). To address this deficiency, companies have implemented automated identity management tools. Although the purpose of such tools was primarily to automate the controls around a critical business process, they also improve the efficiency of the user management process.

2.2 Create a Competitive Advantage

Strong or early adherence to regulations can also be a competitive advantage to a company. Organizations that provide services to other businesses (for example, IT outsourcers, service bureaus, and health insurance administrators) can benefit from early

and provable compliance with regulations, because other organizations are more likely to do business with companies that help them meet their regulatory compliance requirements.

Privacy is a significant concern for businesses and individuals, and strong compliance with privacy regulations also provides a competitive advantage to an organization. For example, compliance with privacy regulations can be marketed to consumers, taking advantage of the general and prevalent concern over privacy and identity theft. In addition, because compliance with the European Union Data Protection Directive (EUDPD) is a prerequisite to doing business in some European countries, compliance with this regulation can open up new marketplaces for a company's products and services.

2.3 Further Integrate IT into the Business

The need for regulatory compliance can help IT managers further integrate IT security with the business. Although many regulations do not specifically require IT-based controls, it is often IT management that ends up implementing the controls that the regulations require. This increases the need for IT and business management to work closely together to solve the difficult topic of regulatory compliance.

As the IT manager becomes a trusted partner to business management, he or she can use this trust to influence business management to take on other IT initiatives to help the company through providing business-enabling technology, efficiency gains, cost savings, and so on.

2.4 Avoid the Checklist Approach

The advantages of using compliance to drive security in the enterprise can become a weakness because of a tendency to become over-reliant on checklists. When companies try to manage risks by using a checklist of compliance items, there is a very real danger of overlooking other critical security issues. Checklists can cast the world in black-and-white terms, which can misrepresent the actual conditions and not allow organizations to take a comprehensive, rational, and logical view of all the circumstances that affect security risks. Moreover, organizations with a solid security framework in place can easily handle any regulations thrown at them.

3 Mapping Regulations to Control Categories

Leading subject experts created a framework that mapped these four major regulations to auditing control categories. We use this framework in this paper for clarity rather than as a leading model of interpretation of financial controls. This framework is heavily weighted toward CoBIT, which is used by auditors to examine financial systems for IT risk.

3.1 Mapping Technology Solutions for Regulatory Compliance

This control framework was then used to tie the control categories from CoBIT to specific technology solutions. This list was validated against ISO 17799, the recommendations of the National Institute of Standards and Technology (NIST SP800), and other well recognized frameworks. Based on this process, the following 20 technology solution categories were identified:

- Document Management Solutions
- Project Management Solutions
- Change Management Solutions
- Host Control Solutions
- Application Security Solutions
- Data Encryption and Transmission Solutions
- Identity Management Solutions
- Security and Compliance Training Delivery Solutions
- Vulnerability Identification Solutions
- Disaster Recovery and Failover Solutions
- Business Process Management Solutions
- Risk Assessment Solutions
- Network Security Solutions
- Malicious Software Prevention Solutions
- E-mail and Collaboration Solutions
- Security Integration
- Authentication, Authorization, and Access Control Solutions
- Physical Security Solutions
- Audit and Logging Solutions
- Incident Management and Trouble-Tracking Solutions

3.2 Centrify Coverage of Compliance Technology Solutions

The capabilities of Centrify DirectControl with Active Directory provides benefits to customers in seven of these categories:

- Identity Management Solutions
- Authentication, Authorization, and Access Control Solutions
- Host Control Solutions
- Change Management Solutions
- Network Security Solutions
- Data Encryption and Transmission Solutions
- Security Integration

3.3 Centrify and Identity Management Solutions

In an information network, identity management represents the software and processes used to manage the digital identities of users and their digital entitlements. Identity management at a high level involves two steps: controlling the privileges of identities (such as password policy), and controlling the privileges assigned to resources. This solution category applies to many if not all of the critical control categories in regulatory compliance. From field experience, identity management solutions are one of the top

recommendations for remediation, to meet regulatory compliance requirements. Examples of solutions include developing processes to ensure accounts are disabled in a timely fashion, and developing processes to review the access controls on data resources.

- Centrify DirectControl with Active Directory tackles the problem of Identity Management in the most straightforward and efficient manner possible. Instead of trying to synchronize identity information in multiple systems – for example, in Active Directory and NIS – DirectControl integrates multiple platforms into Active Directory, reducing the total number of managed systems and making Identity Management inherently easier. With an Identity Management solution using DirectControl with Active Directory, access permissions and policies can be centrally managed, resulting in better security for all systems.
- Centralized password management and consistent user names are introduced. Users can have one user ID and one password that work on multiple machines, as opposed to having to remember different logins and passwords for each system. Administrators can provision or decommission users for all systems with one account record update, greatly simplifying the account provisioning process and possibly eliminating the need for costly provisioning software altogether. The result is lower management costs because less time is required to provision or decommission a user's account – even for use on multiple machines. Administrators have immediate control over access to machines and no longer need to manage access rights machine by machine.
- Finally, all systems can benefit from Active Directory's ability to enforce password policies such as length, complexity, resets, login failure lockouts, and aging.

3.3.1

A Solution for NIS/NIS + and etc/passwd Issues

To provide an example of how Centrify DirectControl with Active Directory improves Identity Management, let's take the use of NIS as an Identity Management solution and explore it further. NIS (Network Information System) is a network naming and administration system for networks that was developed by Sun Microsystems and is found in wide use today to manage UNIX and Linux systems. NIS+ is a later version that provides additional security and other facilities. Using NIS, each host client or server computer in the system has knowledge about the entire system. A user at any host can get access to files or applications on any host in the network with a single user identification and password. NIS is similar to the Internet's domain name system (DNS) but somewhat simpler and designed for a smaller network. It's intended for use on local area networks.

The primary issue with NIS as an Identity Management solution is a lack of ability to enforce strong passwords, weak authentication mechanisms, and exposure of the password files. All of these issues are exploitable by the determined attacker and are on the list of issues that auditors are looking for.

With Centrify DirectControl, user policies such as password strength are enforced by Active Directory, which is much more capable in this regard. In those situations where NIS is still needed, the Centrify DirectControl NIS Server can operate on each system as a local service or as a network service to other remote hosts and appliances. Centrify DirectControl ensures that all systems within a DirectControl Zone share a common set of NIS Maps. UNIX Admins can edit and manage netgroup, automount, and auto.master NIS Maps, as well as generic custom maps. Other solutions that extend Active Directory allow any user who has access to Active Directory Users and Computers to add, change or delete information for any UNIX system – a serious security risk.

3.3.2

Directories

A common Identity Management problem that Centrify DirectControl with Active Directory solves is the problem of multiple directories. In this decade, both UNIX and Windows directories have gradually evolved to favor Lightweight Directory Access Protocol (LDAP)-based technology. These solutions include Sun's Java System Directory Server (formerly known as iPlanet or SunOne Directory), eDirectory from Novell, OpenLDAP on Linux, and Active Directory from Microsoft. The good news for customers was that all these directories had a common underlying structure based on the LDAP protocol, and each system had a similar method for storing user and computer information. However, as is the case with most "open systems" technology, there were enough differences between each solution that in fact these systems did not fully interoperate. As a result, most organizations still end up maintaining separate directory systems for each operating system platform. With Centrify DirectControl with Active Directory, all these directories can be consolidated in one directory, Active Directory.

3.4

Centrify and Authentication, Authorization, and Access Control Solutions

Authentication usually involves a user name and a password, but can include additional methods to verify identity, such as a smart card, retina scan, voice recognition, or fingerprints. Authorization is finding out if the person, after they are identified and authenticated, is permitted to have the requested resource. This control objective is critical to meeting the requirements of the core security principles of confidentiality, integrity, and availability. Much of the Active Directory directory service within the Microsoft Windows 2000 Server and Windows Server 2003 operating systems focuses on authentication, authorization, and access control.

- Centrify DirectControl with Active Directory applies to Authentication, Authorization, and Access Control by directly integrating non-Windows platforms with the robust capabilities of Active Directory. This provides a distributed model for high availability, increased performance and organizational compartmentalization, including the ability to manage cross-domain relationships and trusts. This means that users in each part of the organization can always access their systems, even in the event of a server failure.

- With DirectControl, non-Windows platforms can take advantage of industry-standard authentication technologies such as Kerberos V5 authentication, including logon with Public Key-based Smartcards. Centrally managed Active Directory security groups mapped to UNIX groups simplify the problem of configuring Access Control by being able to express roles for users in one directory and having those roles enforced in any system the user accesses.
- Using patent-pending DirectControl Zones technology, IT managers have the ability to manage access to UNIX, Linux, and Macintosh systems with a level of both ease and granularity that is unmatched by alternative solutions. Centrify's Zone-based delegated administration is the industry's only enterprise-class solution for securely enabling local administration of UNIX, Linux and Mac systems and applications through Active Directory. Each Centrify Zone can have its own set of administrators. Each administrator's privileges can be fine-tuned to fit their job function. Access control is set up using the Zone Delegation of Control Wizard. In this wizard, IT managers specify where home directories are created and how user IDs are generated, and they can view or change Zone properties. In Read or Modify Zone Membership, two key properties are controlled. These properties are which Active Directory user accounts are allowed to access specific UNIX, Linux or Mac systems, and secondly which computers are a member of a zone. With Zones heterogeneous large enterprises are able to easily control access.
- Finally, access rights for each user, group, and computer can easily be reported for auditing purposes using the tools in DirectControl and Active Directory. In addition, data regarding user logins and system access attempts, for all systems in the domain, is stored in one central location where it can be easily retrieved on demand by auditors, greatly easing the task of proving conformance with data access regulations.
- Active Directory is a highly scalable platform and integrates well not only with business-critical applications such as email, but also with key infrastructure components (DNS, certificate servers, firewall/proxy/VPN, Radius, etc.).

3.5

Centrify and Host Control Solutions

The term host control means control of the operating systems in servers and workstations. Host control is fundamental to all of the core security control categories, which include three that meet the security definitions of confidentiality, integrity, and availability. Host control solutions also include each host implementing security best practices at all levels of the operating system, having the most current updates and hotfixes, and using secure methods for daily operations.

- Centrify DirectControl understands the nature of the Unix/Linux environment: existing users have user IDs (UIDs) that may conflict with each other on different sets of systems. With its innovative Centrify Zone technology, Centrify DirectControl gives the IT Pro the flexibility to group multiple Unix/Linux systems

together and map multiple Unix UIDs to a single Active Directory account. Each user can be authorized for each Centrify Zone, with a unique UID in each Centrify Zone. So with Centrify DirectControl, you don't have to worry about individually and manually reconfiguring each user account on each affected Unix/Linux computer to develop a single global unique UID for each user

- Centrify DirectControl with Active Directory applies to Host Control Technology Solutions by integrating the control of different infrastructure services which can be enabled for targeted machines and users, and these services can be associated with other services and system policies.
- DirectControl allows administrators to map special UNIX accounts such as root to trusted Active Directory users. No longer do administrators have to manage special UNIX accounts machine by machine, or manage each individual user account with the use of Group Policy.
- DirectControl provides a repeatable method to control systems administrators as well as users. With Group Policy, all systems' lockdown settings can be applied at one time, consistently over the entire enterprise, as opposed to lockdown settings being applied individually to each specific host operating system.
- A key advantage of Active Directory's ticket-based authentication system is that, once the user has successfully logged into a system, his or her credentials can be used to automatically access other systems and applications based on established security access rights.
- Active Directory's Group Policy functionality provides integrated bulk configuration and security policy management adding to the management of all hosts in the enterprise.

3.6 Centrify and Change Management Solutions

A change management system is a structured process that causes proposed changes to be reviewed for technical and business readiness in a consistent manner that can be relaxed or tightened to adjust to business needs and experiences. The system can involve a database to help staff make better decisions about future changes based on historical data such as success or failure of similar changes. Change management is also a structured process that communicates the status and existence of changes to all affected parties. It can yield an inventory system that indicates what and when actions were taken that affected status of key resources, as an aid in problem-determination or resource management.

Active Directory using security Group Policy provides solid change control at the operating systems level, which Centrify DirectControl enhances by bring Zone capability to collections of heterogeneous machines.

- Since Group Policy is so misunderstood, we begin by going through the definition of groups in Windows Active Directory. A group is a named list of user accounts. Groups can be distribution lists or security groups, but we are most concerned with security groups in compliance. The rights and permissions granted to a group are extended to all members of the group. In this extension process, groups simplify administration and control the rights and permissions of users and computers providing change control on the operating systems.
- If administration of a group changes, it can be moved anywhere in the domain without affecting the permissions or rights assigned to the group. This adaptability is controlled by the groups' scope. Group scope determines the systems in a domain, tree, or a forest to which a group can be assigned permissions and right, what user and other groups can be added as members, and what other groups can be added as a member. The choices on scope – Universal, Global, Domain Local, and Machine Local – allow rights and permissions to be granted at the forest, domain, or system level.
- Also, by using group nesting in group implementation strategy, verification of access control is achieved, and maintenance effort reduced. By group nesting, we mean that, for each high-level resource (directory branch, database, application or registry key, a resource access group for each level of access needed by that resources is created. User groups are then created for users that share a common responsibility or qualification. Lastly these user groups are placed in resource access groups as necessary.
- Centrify DirectControl with Active Directory brings all the data on the configuration of its critical systems using Zones under one umbrella, where it can be managed most effectively using Active Directory and groups.
- Centrify DirectControl with Active Directory collects all the host (computer) information in one place where the configurations of all machines can be managed and maintained. Using Active Directory groups can be placed at the root of the domain or in an organizational group. Groups should be placed in the OU hierarch according to who should administer the group. For instance, if your organization is administered by department and the domain is divided into OUs by departments, the HRStaff group would be placed in the HR OU. When combined with enterprise management server (EMS) solutions the management of configurations becomes even more manageable.

3.7

Centrify and Network Security Solutions

Network security solutions fall into a broad category that addresses the security of all parts of the network, including firewalls, servers, clients, routers, switches, and any access points. The purpose of network security solutions is to use current best practices to set up all parts of the network to ensure that good preemptive practices are followed in the design and operation of the networks. Although many network security solutions

involve hardware that only deals with the perimeter network, the overall problem is much broader and include areas of traditional network engineering and data center architecture.

- Centrify DirectControl with Active Directory addresses Network Security Technology Solutions by integrating into the directory key infrastructure services such as DNS, VPN, certificate services, remote access services, printer management, Smartcard / biometric security and Radius. Other infrastructure solutions such as Microsoft's ISA Server and Identity Integration Server also work within the Active Directory architecture to further extend the secure infrastructure.
- Using Centrify DirectControl with Active Directory, applications can easily leverage the directory's account, computer and management interfaces to provide a seamlessly integrated, secure experience. Microsoft Exchange, IIS and SQL Server are just a few examples of Active Directory-integrated applications.
- End-users also have easy access to infrastructure information in Active Directory, using features such as looking up other users in the Global Catalog, location-based printer discovery and server browsing – all without having to know directory and infrastructure concepts.

3.8

Centrify and Data Encryption and Transmission Solutions

This solution category deals with protecting data that is at rest or in transmission. Cryptographic solutions are the most common method of providing data protection; however, variations of information rights management, IPSec, and document-based rights management systems also provide control of sensitive information. File protection and the encryption of sensitive information, whether at rest or in transit, is required by all compliance guidelines and is specifically called out in CoBIT. The compliance process creates huge amounts of very sensitive data, primarily in non-structured applications such as Microsoft Word or Excel files. Control and protection of this compliance data is very important because this data contains a complete list of the enterprise's known weaknesses and vulnerabilities.

- Centrify DirectControl with Active Directory applies to Data Encryption and Transmission solutions by easily and seamlessly moving critical control functions from UNIX and Linux control systems such as NIS/ NIS + that send passwords in clear text to a Kerberos-encrypted solution based on Active Directory. Kerberos is a highly secure, ticket-based authentication mechanism for transmission and encryption.
- Furthermore, other infrastructure solutions such as Microsoft's ISA Server and Identity Integration Server also work within the Active Directory architecture to provide a tightly integrated solution to security and compliance. Active Directory's highly secure, token-based authentication, using industry-standard Kerberos, can be used across Windows, UNIX, Linux, Mac and Java platforms. This results in a single sign-on experience that spans all Windows, UNIX, Linux and Mac systems.

3.9 Centrify and Security Integration

Data classification deals with how to apply security classification levels to the data contained on a system or in transmission. Security integration is the integration of security to data at rest or in transmission, and dashboard solutions refer to the broad array of reporting and presentation options for security data. Examples of data classification are high, medium, or low business impact or reverting to the military system, Top Secret, Secret, Confidential and Un-Classified. Data security refers to security of the actual data at rest, such as storage security and database security. Data classification is important to compliance because it is a method of communicating to users of data a level of importance of the data, and how that data must be handled, safeguarded and disposed of. Data integration refers to the transfer of data between applications and includes both data in transmission and at rest. Control and protection of data is specifically called out in most regulatory compliance activities and must be thoroughly addressed to be compliant. Dashboard solutions address the larger issue of reporting and display of data in methods that allow the stakeholders to control monitor and adjust for security and compliance. Dashboards also help you to understand the metrics of the compliance process itself.

Centrify DirectControl with Active Directory applies to Data Classification, Security Integration, and Dashboards Solutions with an integration of User accounts which can be stored in a single secure database as opposed to being stored and managed at each machine. DirectControl with patent-pending Zone technology makes it easy to manage which UNIX users have access to specific machines and the sensitive data they host from a single management console.

4 Active Directory and DirectControl – the Right Choice for Compliance

Centrify DirectControl with Active Directory is a security solution that makes compliance easier by providing one solution that matches with many of the control areas.

- Identity Management Solutions
- Authentication, Authorization, and Access Control Solutions
- Host Control Solutions
- Change Management Solutions
- Network Security Solutions
- Data Encryption and Transmission Solutions
- Data Classification, Security Integration, and Dashboards Solutions

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. DirectControl

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 and Microsoft’s Active Directory, you can now extend the directory you already own to UNIX, Linux, Mac, and Java environments, yielding substantial benefits for your organization through lower costs, better security, simplified management, and increased productivity, and most importantly in this case a big jump start on your regulatory compliance efforts.

5

How to Contact Centrify

Centrify Corporation
444 Castro St., Suite 1100
Mountain View, CA 94041

U.S. Sales Office: +1 (650) 961-1100
Enquiries: info@centrify.com
Web site: www.centrify.com