

## Using Likewise to Comply with the PCI Data Security Standard

### AUTHOR:

**Steve Hoenisch**  
Likewise Software

### Abstract

This document describes how Likewise Enterprise and Microsoft Active Directory can foster compliance with the Payment Card Industry Data Security Standard, a set of requirements for businesses that process payment card information. Developed by Visa, American Express, Discover Financial Services, and other members of the PCI Security Standards Council, the standard sets forth policies, procedures, and practices to protect customer account data. The standard includes specific requirements for strictly controlling access to customer data, authenticating business users, monitoring access, maintaining a secure network, and auditing system resources.

Likewise integrates Linux, Unix, and Mac OS X workstations and servers into Active Directory, providing the basis to assign each user a unique ID for authentication, authorization, monitoring, and tracking. Likewise also provides group policies for non-Windows computers so that their security settings and other configurations can be centrally managed in the same way as Windows computers.

The information contained in this document represents the current view of Likewise Software on the issues discussed as of the date of publication. Because Likewise Software must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Likewise, and Likewise Software cannot guarantee the accuracy of any information presented after the date of publication.

These documents are for informational purposes only. LIKewise SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED.

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, by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Likewise Software.

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

© 2008 Likewise Software. All rights reserved.

Likewise and the Likewise logo are either registered trademarks or trademarks of Likewise Software in the United States and/or other countries. All other trademarks are property of their respective owners.

Likewise Software  
15395 SE 30th Place, Suite #140  
Bellevue, WA 98007  
USA

## Table of Contents

<b>Introduction</b> .....	<b>4</b>
<b>The Payment Card Industry Data Security Standard</b> .....	<b>5</b>
<b>How Likewise and Active Directory Foster Compliance with PCI Requirements</b> .....	<b>7</b>
One User, One ID.....	8
Granular Access Control .....	8
Group Policies .....	9
<b>Feature Support for PCI DSS Requirements</b> .....	<b>10</b>
Requirement 2.....	10
Requirement 7.....	10
Requirement 8.....	12
Requirement 10.....	16
<b>Summary</b> .....	<b>18</b>
<b>For More Information</b> .....	<b>19</b>

### Introduction

You have a mixed network of Unix, Linux, Mac OS X, and Windows computers, and you've got to bring your environment into compliance with the Payment Card Industry Data Security Standard, the set of security requirements for businesses that process credit card information. The standard requires that you authenticate individual users and strictly control access to customer data. If you don't comply by a set date, or if you have a security breach, your company faces hefty fines from Visa, MasterCard, and American Express. They might even suspend your ability to accept payment cards.

Or maybe your environment is already in compliance or near compliance, but only because of a Herculean effort on the part of your system administrators to manage users on an individual basis and control their access to resources that contain sensitive cardholder data.

Why does compliance require so much work? For many businesses, it is because they use different Identity Management Systems for different operating systems: Windows users might authenticate through Active Directory, Linux and Unix users might authenticate through NIS, and Mac OS X users might authenticate through an ad hoc Kerberos key distribution center. Every time a user joins or leaves your company, you have to update each of these Identity Management Systems separately — a time-consuming process that can leave security holes. The complexity of these Identity Management Systems and their lack of central management increases the likelihood that something will go wrong. A user account with access to protected data, for example, might not get deprovisioned from one of the systems when the user leaves the company. The PCI compliance auditors won't like that.

With the requirements of the PCI security standard, the stakes are high. In addition to some very bad press, security breaches can lead to fines that run up to \$500,000 or more. But the stakes go beyond the potential of a public relations nightmare or substantial fines. Because you don't have a single, centralized Identity Management System in place, adapting to the standard as it evolves and changes will continue to be a grueling – and expensive – challenge.

Likewise helps overcome the challenges of complying with the PCI data security standard by integrating Linux, Unix, and Mac OS X computers into Active Directory. Joining non-Windows computers to an Active Directory domain immediately yields the benefit of providing a centralized Identity Management System. Likewise lets you use Active Directory to securely authenticate Linux and Unix users, control their access to customer data, and apply group policies to manage passwords policies and root access.

This document describes how you can use Likewise with Active Directory to comply with a number of the requirements of the Payment Card Industry Data Security Standard.

## The Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard describes a set of security requirements for businesses that process payment card information. Developed by Visa, American Express, Discover Financial Services, and other members of the PCI Security Standards Council, the standard sets forth policies, procedures, and practices to protect customer account data. The standard includes specific requirements for strictly controlling access to customer data, authenticating business users, monitoring access, maintaining a secure network, and auditing system resources.

The PCI DSS requirements apply to businesses that store, process, or transmit a customer's Primary Account Number, or PAN. If a PAN is not stored, processed, or transmitted, the PCI DSS requirements do not apply.

Payment brands such as Visa and American Express have established their own requirements and timeframes for businesses and merchants to comply with version 1.1 of the standard — as well as penalties for noncompliance. The payment brands can levy hefty fines on businesses that fail to comply or suspend their payment card processing privileges.

The standard comprises 12 high-level requirements grouped into 6 categories. These high-level requirements, shown below, contain additional requirements, which are discussed later.

These requirements apply to all system components – any network component, server, or application that is connected to that part of the network that contains cardholder data or sensitive authentication data. The following table is an excerpt from the PCI DSS:

### **Build and Maintain a Secure Network**

- Requirement 1:** Install and maintain a firewall configuration to protect cardholder data
- Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters

### **Protect Cardholder Data**

- Requirement 3:** Protect stored cardholder data
- Requirement 4:** Encrypt transmission of cardholder data across open, public networks

### **Maintain a Vulnerability Management Program**

- Requirement 5:** Use and regularly update anti-virus software
- Requirement 6:** Develop and maintain secure systems and applications

### **Implement Strong Access Control Measures**

- Requirement 7:** Restrict access to cardholder data by business need-to-know
- Requirement 8:** Assign a unique ID to each person with computer access
- Requirement 9:** Restrict physical access to cardholder data

### **Regularly Monitor and Test Networks**

- Requirement** Track and monitor all access to network resources and

**10:** cardholder data

**Requirement** Regularly test security systems and processes

**11:**

### Maintain an Information Security Policy

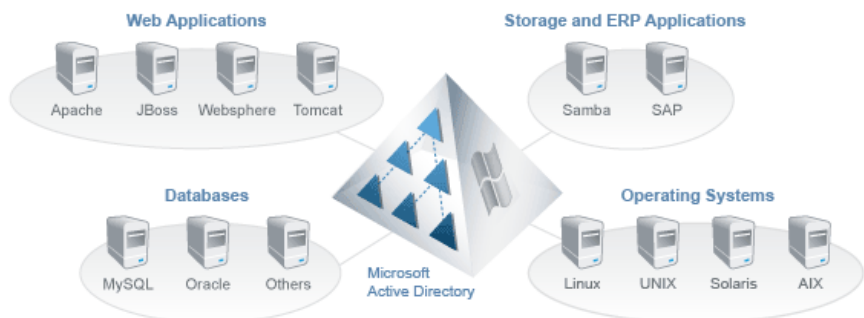
**Requirement** Maintain a policy that addresses information security

**12:**

Depending on the size and type of a business, PCI DSS compliance is determined by an on-site PCI data security assessment by a qualified security assessor, a quarterly network scan, or a self-assessment questionnaire.

## How Likewise and Active Directory Foster Compliance with PCI Requirements

The cornerstone of Likewise is that it joins Linux, Unix, and Mac OS X computers to Microsoft Active Directory – a secure, scalable, stable, and proven Identity Management System.



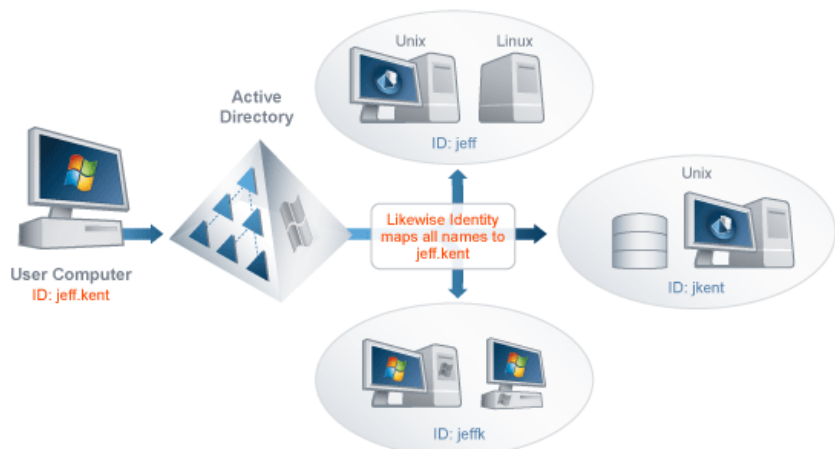
Joining non-Windows computers to Active Directory gives you the power to manage all your users' identities in one place, use the highly secure Kerberos 5 protocol to authenticate users in the same way on all your systems, apply granular access controls to sensitive resources, and centrally administer Linux, Unix, Mac, and Windows computers with

group policies. You can seamlessly manage both Windows and non-Windows computers within Active Directory.

### One User, One ID

Requirement 8 of the PCI DSS is to assign a unique ID to each person with computer access. By using Likewise with Active Directory, you can easily do just that –for both Windows users and Linux and Unix users. Active Directory makes ID assignment simple: one ID, one user. Likewise extends that functionality to Linux, Unix, and Mac OS X users. With one unique ID provisioned and centrally managed through Active Directory, a user can log on Windows, Unix, Linux, and Mac OS X computers with an encrypted password that is securely authenticated against the Active Directory database.

More: You can assign each user a unique ID in Active Directory while maintaining your NIS domain user information. When you migrate Linux and Unix users from NIS domains to Active Directory, Likewise uses *cells* to preserve the user information in your NIS domains. A cell provides a custom mapping of a unique and identifiable Active Directory user to that user's UIDs and GIDs:



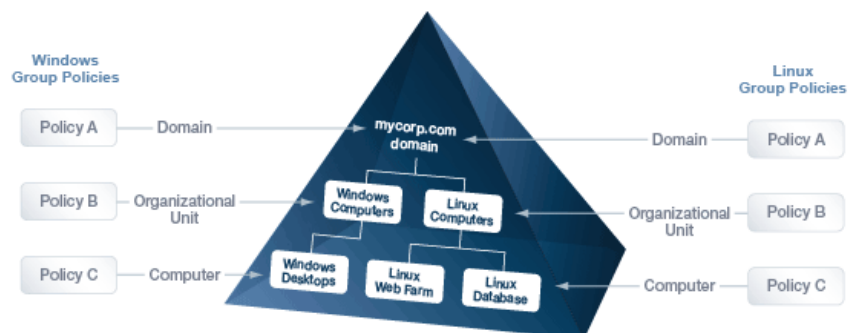
### Granular Access Control

Requirement 7 is to restrict access to cardholder data by business need-to-know. With Likewise and Active Directory, you can use your pre-

existing UIDs to control access to cardholder data at a granular level. In fact, Likewise allows all users that are provisioned in Active Directory to access resources on Unix and Linux hosts. Unix and Linux permission settings for users and groups are defined by UIDs and GIDs. In Active Directory, on the other hand, a security identifier (SID) uniquely identifies a user, group, or computer. Likewise overcomes this mismatch by mapping SIDs to UIDs and primary GIDs and storing the information in the Program Data node of the Active Directory database. By mapping SIDs to UIDs and GIDs, Likewise makes Active Directory's granular access control available to Unix, Linux, and Mac OS X computers, users, and groups.

### Group Policies

Requirement 2 is to not use vendor-supplied defaults for system passwords and other security parameters. With Likewise, you can centrally manage the security settings on non-Windows systems by using the Group Policy Object Editor or the Group Policy Management Console to create group policies and then apply them to computers running Linux, Unix, and Mac OS X. Likewise comes with more than 100 group policies for Linux, Unix, and Mac OS X computers, including policies for setting security parameters. Likewise applies group policies to Linux and Unix systems in the same way that Active Directory applies group policies to Windows systems:



Likewise group policies can also be used to help comply with Requirement 10 -- track and monitor all access to network resources and cardholder data. For example, one of Requirement 10's subrequirements

is that you “establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.” Likewise includes a group policy for the sudo configuration file. The policy can specify which users can run which commands as root, eliminating the need for users to log on as a root user to run commands.

## Feature Support for PCI DSS Requirements

This section details how Likewise Enterprise can help you comply with specific requirements of PCI DSS Version 1.2 (October 2008).

### Requirement 2

*“Do not use vendor-supplied defaults for system passwords and other security parameters.”*

Likewise provides group policies for managing security parameters on Linux and Unix computers through Active Directory (AD).

PCI DSS Requirement	Likewise and AD Feature Support
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Likewise provides group policies to manage files, directories, symbolic links, file system mounts, cron jobs, and scripts.
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.	Likewise extends Kerberos authentication to Linux, Unix, and Mac OS X computers, providing users with authenticated single sign-on access through SSH and other methods to authorized resources.

### Requirement 7

*“Restrict access to cardholder data by business need-to-know. This requirement ensures critical data can only be accessed by authorized personnel.”*

Likewise ports the granular access control of Active Directory to Linux, Unix, and Mac OS X workstations and servers.

PCI DSS Requirement	Likewise and AD Feature Support
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	Likewise and Active Directory empower you to control access to computer resources. Specifically, you can use Active Directory groups to control access to customer data only to those with a business need to know.  User identifiers (UIDs) and group identifiers (GIDs) from NIS domains can be migrated to Active Directory and their mapping to Linux and Unix resources can be maintained through the use of Likewise <i>cells</i> . Cells provide a custom mapping of Active Directory users to UIDs and GIDs.
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.	Likewise Enterprise's Allow Logon Rights Group Policy ( <i>require_membership_of</i> ) can specify that a user be a member of a particular group to log on a computer within the scope of the group policy object. You can designate one or more groups. A user is allowed to log on only if he or she is a member of at least one of the designated groups – and you can use AD to limit the privileges available to the group to the least necessary to perform the job in question.
7.1.2 Assignment of privileges is based on individual personnel's job classification and function.	With Likewise and AD, you can use groups to assign privileges to a user or group of users based on job classification and function.
7.1.4 Implementation of an automated access control system.	Active Directory is an automated access control system; Likewise extends it to Linux, Unix, and Mac.
7.2 Establish a mechanism for systems with multiple users that	Likewise and Active Directory provide a mechanism for granular access

<p>restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.</p>	<p>control. You decide who needs to know: Only the users that you authorize get access to the systems that you specify, and all other users are denied.</p> <p>Likewise and Active Directory can restrict access in two ways: groups and sudo configuration files.</p> <p>In Active Directory, security groups are an efficient way to assign access to resources.</p> <p>A sudo configuration file can restrict access to commands on a computer to the users or groups that you specify.</p>
<p>7.2.1 Coverage of all system components.</p>	<p>The computer access reports in Likewise Enterprise give you instant visual (and printable) confirmation that all your system components are covered by the access control system.</p>
<p>7.2.2 Assignment of privileges to individuals based on job classification and function.</p>	<p>The Enterprise version of Likewise, with its cell technology and AD sudo group policy and other access control group policies, provide a powerful tool for enforcing role-based access control for Unix, Linux, and Mac OS X computers.</p>
<p>7.2.3 Default "deny-all" setting.</p>	<p>With Likewise Enterprise, by default all users are denied access.</p>

### Requirement 8

*"Assign a unique ID to each person with computer access. Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users."*

Likewise bridges the gap between the Linux and Unix world of UIDs and GIDs and the Active Directory world of security identifiers to provide a unique ID for each user while maintaining pre-existing NIS domain information.

PCI DSS Requirement	Likewise and AD Feature Support
<p>8.1 Identify all users with a unique user name before allowing them to access system components or cardholder data.</p>	<p>With Active Directory you can assign a unique user name to each user. The user name can then be used on all the computers that are joined to Active Directory.</p> <p>In addition, Likewise lets you assign multiple UIDs to a single user to maintain NIS domain information.</p>
<p>8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: password; token devices (e.g., SecureID, certificates, or public key); biometrics.</p>	<p>Active Directory can authenticate users with passwords on all the computers that they log on. In addition, Likewise group policies can disallow the use of null passwords and define a sudo policy that eliminates the need for shared local password accounts.</p>
<p>8.4 Encrypt all passwords during transmission and storage on all system components.</p>	<p>If you are using NIS, a NIS client might be able to retrieve the whole password database for offline inspection. NIS passwords are typically transmitted without encryption.</p> <p>Using Likewise with Active Directory makes Kerberos available to Unix, Linux, and Mac OS X as well as Windows computers; Kerberos encrypts the transmission and storage of passwords.</p>
<p>8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components [as specified in requirements 8.5.1 through 8.5.16].</p>	<p>Active Directory provides strong authentication and password management.</p>
<p>8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects</p>	<p>With Likewise, you can use Active Directory Users and Computers to assign the next unique UID to a new user, set a specific UID for a user, and delete UIDs.</p>
<p>8.5.2 Verify user identity before performing password resets</p>	<p>You can automatically verify the identity of users by having users supply their old password before a</p>

	password reset.
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use	Using your internal processes or password-generation tools, you can set a unique original password. Then, in Active Directory, you can check a box that requires users to reset passwords upon initial logon.
8.5.4 Immediately revoke access for any terminated users	In Active Directory, you can select a single check box and immediately disable account access for all the machines that a user has access to — regardless of operating system.
8.5.5 Remove inactive user accounts at least every 90 days	The Likewise Console generates reports that identify disabled accounts. You can then simply delete the account from Active Directory.
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed	In Active Directory, you can specify the exact hours during which a vendor may log on.
8.5.7 Communicate password procedures and policies to all users who have access to cardholder data	Standardizing on Active Directory and Likewise simplifies password policies and procedures, makes it easier to cross-train your teams, and ensures that everyone follows the same procedure regardless of a computer's operating system.
8.5.8 Do not use group, shared, or generic accounts and passwords	A Likewise group policy empowers you to manage and distribute sudo policies from a central source. Instead of letting users share the root password, you can use a sudoers file to control access to root commands. You also benefit from being able to track which users are logging on systems that contain protected data, as opposed to everyone just logging on as root. Likewise Enterprise provides reports that enable you to confirm that group accounts, shared accounts, or generic passwords are not in use.

8.5.9 Change user passwords at least every 90 days	By using Likewise with Active Directory, you can enforce security settings for passwords, including password change intervals.
8.5.10 Require a minimum password length of at least seven characters	A Likewise group policy lets you set the minimum password length for all the computers in your network.
8.5.11 Use passwords containing both numeric and alphabetic characters	A Likewise group policy for computers lets you require complex passwords, which must contain both numeric and alphabetic characters.
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	A group policy can enforce password history on computers that are joined to Active Directory.
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	With Active Directory, a group policy can specify the account lockout threshold — the number of invalid logon attempts before the account is locked.
8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID	With Active Directory, a group policy can specify the account lockout duration.
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	Likewise provides a number of group policies for controlling the screen saver, including policies that lock the system after a set number of idle minutes.
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users	Likewise and Active Directory give you not only secure authentication for applications and users but also single sign-on: Users authenticate once against the Active Directory database and receive a Kerberos ticket-granting ticket. Users can then seamlessly obtain authenticated access to other resources, including databases, for which they are authorized.

### Requirement 10

*“Track and monitor all access to network resources and 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.”*

Likewise and Active Directory can help track and monitor access to system resources.

PCI DSS Requirement	Likewise and AD Feature Support
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	Active Directory can control access to all system components at the level of the user. Individual users can be authorized for access to system components at a granular level. Likewise includes a group policy for setting a sudo configuration file. The sudo configuration file can specify which users can run which commands as root, eliminating the need for users to log on as a root user to run commands.
10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.1 All individual user accesses to cardholder data	The Active Directory event log can track individual user access to cardholder data.
10.2.2 All actions taken by any individual with root or administrative privileges	The Likewise Enterprise event log and reporting system can log and report on actions taken by a user with a root account.
10.2.4 Invalid logical access attempts	The Likewise Enterprise event log tracks invalid access attempts.
10.2.5 Use of identification and authentication mechanisms	The Likewise Enterprise logging system shows the use of identification and authentication mechanisms.
10.3 Record at least the following audit trail entries for all system components	The Likewise Enterprise event log system can record audit trail entries for

<p>for each event:</p> <ul style="list-style-type: none"> <li>10.3.1 User identification</li> <li>10.3.2 Type of event</li> <li>10.3.3 Date and time</li> <li>10.3.4 Success or failure indication</li> <li>10.3.5 Origination of event</li> <li>10.3.6 Identity or name of affected data, system component, or resource</li> </ul>	<p>each of these events and display the information graphically in the Likewise Operations Dashboard or in reports, which can be viewed or printed.</p>
<p>10.5.2 Protect audit trail files from unauthorized modifications.</p>	<p>The access control mechanisms of both Active Directory and Likewise Enterprise can be employed to protect audit trail files from unauthorized access and modification.</p>
<p>10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.</p>	<p>The Likewise Enterprise log collection service and integrated database server can automatically collect and back up audit trail files to a centralized server that only those who have been granted permission can access.</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 accounting protocol (AAA) servers (for example, RADIUS).</p>	<p>The Likewise Enterprise log collection service, integrated database server, and Operations Dashboard let you monitor logs in real-time for authentication, authorization, and other security functions for Linux, Unix, and Mac OS X systems that are connected to Active Directory.</p>
<p>10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).</p>	<p>Part of the Likewise Enterprise log collection service, the Event Archiving Utility archives old events into a more compact form in the central Likewise Enterprise database. The utility will take any events older than one year and combine them into compressed archives. A separate archive is created for each period of old event data. Archives are stored in a separate database table, but remain available for analysis.</p>

### Summary

To foster compliance with the Payment Card Industry Data Security Standard, Likewise seamlessly integrates Linux, Unix, and Mac computers into Active Directory – a stable, secure, and scalable Identity Management System.

Likewise gives you the power not only to join non-Windows computers to Active Directory but also to migrate Linux and Unix users to Active Directory while maintaining their identities and permissions. And once you have joined non-Windows computers to Active Directory and migrated your Linux and Unix users, Likewise and Active Directory can help you comply with a number of key PCI DSS requirements, including the following:

- One user, one ID: Assign a single ID and password to each user and then use that ID to monitor and track the user.
- Authenticate the encrypted passwords of users and groups with the highly secure Kerberos authentication protocol.
- Authorize and control access to resources, including those that contain customer account information.
- Apply group policies, such as for sudo configuration files and for password settings, to configure Linux, Unix, and Mac computers to comply with PCI DSS requirements.

Together, Likewise and Active Directory provide a proven Identity Management System, ease management of your mixed network, improve security, and, most important, help you comply with many of the PCI DSS requirements.

### For More Information

For more information on Likewise or to download a free 30-day trial version, visit the Web site at <http://www.likewisoftware.com>.

For general questions, call (800) 378-1330 or e-mail [info@likewisoftware.com](mailto:info@likewisoftware.com).

For technical questions or support for the 30-day free trial, e-mail [support@likewisoftware.com](mailto:support@likewisoftware.com).

#### ABOUT LIKEWISE

Likewise® Software solutions improve management and interoperability of Windows, Linux, and UNIX systems with easy to use software for Linux administration and cross-platform identity management.

Likewise provides familiar Windows-based tools for system administrators to seamlessly integrate Linux and UNIX systems with Microsoft Active Directory. This enables companies running mixed networks to utilize existing Windows skills and resources, maximize the value of their Active Directory investment, strengthen the security of their network and lower the total cost of ownership of Linux servers.

Likewise Software is a Bellevue, WA-based software company funded by leading venture capital firms Ignition Partners, Intel Capital, and Trinity Ventures. Likewise has experienced management and engineering teams in place and is led by senior executives from leading technology companies such as Microsoft, F5 Networks, EMC and Mercury.