White Paper

How to Avoid the High Cost of Security Audits

Abstract

The majority of regulations are centered on identity and policy management. While such management is a part of Windows environment, its existence in the non-windows world is very limited. Thus, administrators are attempting to use Microsoft Windows as a common ground for storage, management, and monitoring of policies governing non-Windows environments. This could be done with Open Source tools or professional, scalable and supported solutions such as PowerBroker Identity Services Enterprise. The present paper discusses the advantages and disadvantages of both approaches.

Contents

Executive Summary

Modern computing is governed by a number of security regulations. These particularly affect companies offering services to the government, processing credit card payments, or handling medical or financial records. The birth of these regulations originated with legislative attempts to perform post facto due diligence, while dumping the complexity of implementation on the complying entities. In addition, the regulations are enforced with stiff fines, suspension of privileges, or even personal liability for executive officers in cases of non-compliance.

The majority of these regulations are centered on identity and policy management. While such management is a part of Windows environment, its existence in the non-windows world is very limited. Thus, administrators are attempting to use Microsoft Windows as a common ground for storage, management, and monitoring of policies governing non-Windows environments. This could be done with Open Source tools or professional, scalable and supported solutions such as PowerBroker Identity Services Enterprise. The present paper discusses the advantages and disadvantages of both approaches.

Over the past decade a large number of network security and financial accounting fraud incidents have occurred, resulting in greatly increased federal and local regulation of many aspects of business computing. This white paper discusses the requirements of these security standards and demonstrates how these requirements can be fulfilled with the PowerBroker Identity Services Enterprise solution.

The paper begins with a high-level discussion of several of today's key U.S. security standards, what they are, and how they apply to different businesses. The paper then discusses the cost effects of failed audits, whether through legal action or loss of business. The next section discusses some of the common attributes of the technical requirements of regulatory compliance. The next section discusses how technologies from BeyondTrust Software enable enforcement of compliance requirements in heterogeneous operating system computer networks.

Security Standards

Depending on the nature of their business and customer relationships, companies are required to comply with a number of fairly complex security requirements such as PCI, SOX, FISMA, HIPPA, and several others. The most widely used requirements of these regulations are discussed below.

PCI

PCI DSS (Payment Card Industry Data Security Standard) was put forward by the Payment Card Industry Security Standards Council (PCI SSC) to prevent credit card fraud, hacking, and various other security vulnerabilities and threats. The standard applies to all organizations that store, process, or transmit cardholder data. Guidance is offered for software developers and manufacturers of applications and devices used in such transactions. The standard was recently upgraded to version 1.2 with stricter requirements.

SOX

The Sarbanes-Oxley Act is a United States federal law enacted on July 30, 2002 in response to a number of major corporate and accounting scandals, including those affecting Enron, Tyco International, and WorldCom. The act is a complex regulatory requirement that establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms. The act provides for new levels of auditing, CEO, CFO, and board accountability, and increased criminal and civil penalties for securities violations.

FISMA

The Federal Information Security Management Act of 2002 (FISMA) places requirements on government agencies and components, with the goal of improving the security of federal information and information systems. The goals of FISMA include the following:

- Protection of information and computing systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure integrity, confidentiality, and availability
- Management of risks in information security
- Mechanism for effective oversight of federal agency information security programs.
- Among many requirements, FISMA law demands each federal agency to develop, document, and implement an agency-wide information security program, with appropriate information access control measures designed to attain higher consistency levels

HIPAA

The United States Health Insurance Portability and Accountability Act of 1996 (HIPAA) seeks to establish standardized security measures for healthcare and medical information. It requires the establishment of national standards for electronic health care transactions, security, and confidentiality of all health care-related data. Besides a number of format standardizations, the act mandates security mechanisms to ensure confidentiality and data integrity for any information that identifies an individual. Specifically, HIPPA mandates the following technical safeguards for computer systems access:

- Protection from electronic intrusion to the digital systems
- Encryption of the information exchange
- Procedures to ensure that the data within its systems has not been changed or erased in an unauthorized manner
- Data integrity services, including check sum, double-keying, message authentication, and digital signature
- Authentication of data access, including: password systems, two- or three-way handshakes, telephone call back, and token systems
- Existence of the documented risk analysis and risk management programs
- In addition to imposing fairly complex and stringent sets of requirements, these standards are updated on a regular basis imposing additional demands on the security and audibility of the IT infrastructure. Therefore, becoming and staying compliant is a never-ending task for the security and systems administrators

Cost of Failed Audits

In order to enforce the security regulations, the penalties imposed on non-compliant vendors are quite strict and affect the overall cost (or even the ability) of doing business.

PCI

The penalties and fines for failure to comply with the requirements or rectify a security issue range from $10,000 to $500,000 per incident, depending on the severity and magnitude of the situation. In the case of a security breach, the company may be also liable for the cost of required forensic investigations, fraudulent purchases, and the cost of re-issuing credit cards. Finally, in the most severe cases, the credit card acceptance privilege can be suspended or terminated.

SOX

Depending on the section of the act that was violated, the penalties range from the loss of stock exchange listing through the loss of D&O insurance to multimillion dollar fines and imprisonment. A CEO or CFO submitting a wrong certification is subject to a fine of up to $1 million and imprisonment for up to ten years. Should the wrong certification be submitted willfully, the fine can be increased up to $5 million and the prison term can be increased up to twenty years. Indirect costs of non-compliance include the lack of investor confidence and the corresponding decrease in business value or the degradation of business operations.

FISMA

Though there are no applicable criminal sanctions, non-compliance costs the violator bad publicity. U.S. Congress conducts an annual audit of federal agencies and publicly issues an information security scorecard. A low score means a loss in public confidence and additional government scrutiny. Additionally, the CIOs of low-performing agencies can be asked to explain before Congress why they scored poorly. In cases of noncompliance, the Office of Management and Budget (OMB) may delay or cancel funding for agency programs.

HIPAA

Penalties for non-compliance may be civil, criminal, or financial. These penalties include the following:

- Fines for noncompliance as high as $100 per offense, with a maximum of $25,000 per year for any person who violates a provision of this part
- Fines up to $25,000 for multiple violations of the same standard in a calendar year
- Fines up to $50,000, or up to 1 year in prison, or both
- Fines up to $100,000, up to 5 years in prison, or both for offense committed under false pretenses
- Fines up to $250,000 and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information

Passing Security Audits

Each regulatory security standard includes specific requirements for controlling access to customers' financial or medical records, authentication of business users, adequate access to monitoring and auditing facilities, and maintenance of a secure network. The situation is aggravated by the business need to create and maintain identities across all nodes of heterogeneous environments, with multiple operating systems dealing with different aspects of customer data on the processing, storage, and presentation level.

Although the various data-handling regulations have different natures, origins, and focus, most of them share the same set of technical requirements for data protection. The differentiators are that for each regulatory regime, each requirement is detailed in voluminous regulatory documents, supplementary third-party materials, and industry publications. Therefore, it makes sense to summarize the common aspects of these regulations. They include the following:

- Installation and maintenance of firewall to limit inbound access to computing host
- Strong password policy, including length, strength, expiration time, maximum, number of retries, and number of remembered old passwords. This offers a more secure access to host and prevents brute-force attacks against password repository
- Encryption of data transmission to protect sensitive data in transit
- Assignment of unique ID to individual users to be able to track down system and data access on per-individual basis
- Implementation and update of anti-virus/anti-malware software to protect system against external access with Trojans or key loggers
- Availability of dada on the need-to-know basis and denial of access unless explicitly allowed. This is the industry-standard approach to granting access permissions
- Strong access control and auditing to allow report-based, query-based and alert-based control of access to sensitive data.

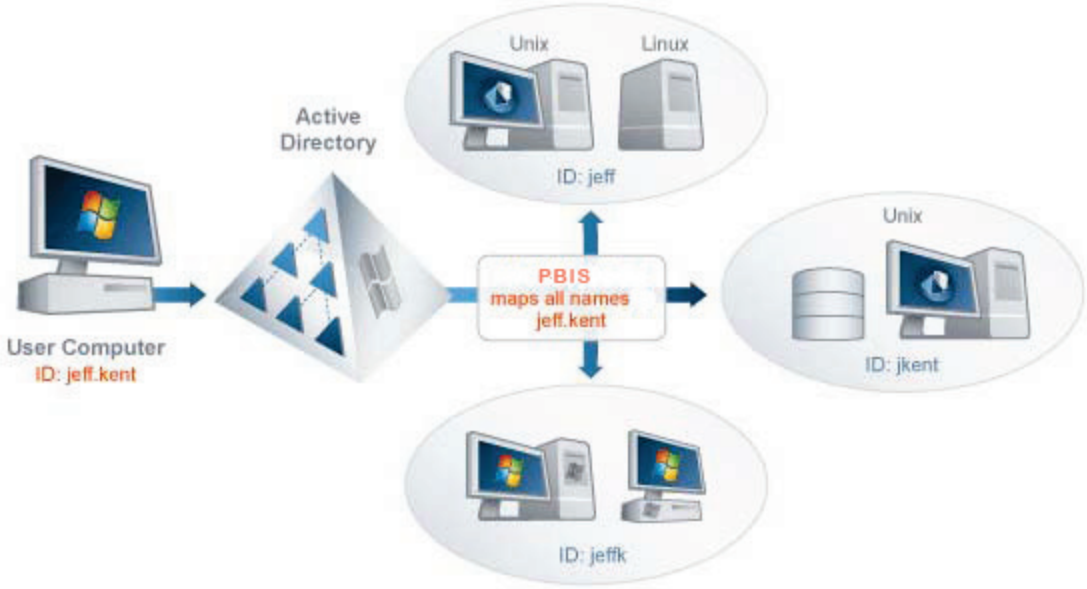
Enforcement of the Compliance Requirements

Enforcing compliance on a single platform is by far easier than across multiple platforms, including Mac OS X, multiple UNIX variants and several flavors of Linux. The complexity is associated with different tools, file locations, files formats and approaches for desktop and policy management. PowerBroker Identity Services Enterprise allows companies with heterogeneous computing environments to easily comply with the above discussed data security requirements.

By joining non-Windows computers to Active Directory and migrating users to AD while retaining their identities and permissions, BeyondTrust technology provides administrators with a stable, secure, and scalable identity management system. From this point on all user authentications, authorization, provisioning, and logging of domain-based activities is handled by a single, centralized, secure, scalable, and stable repository.

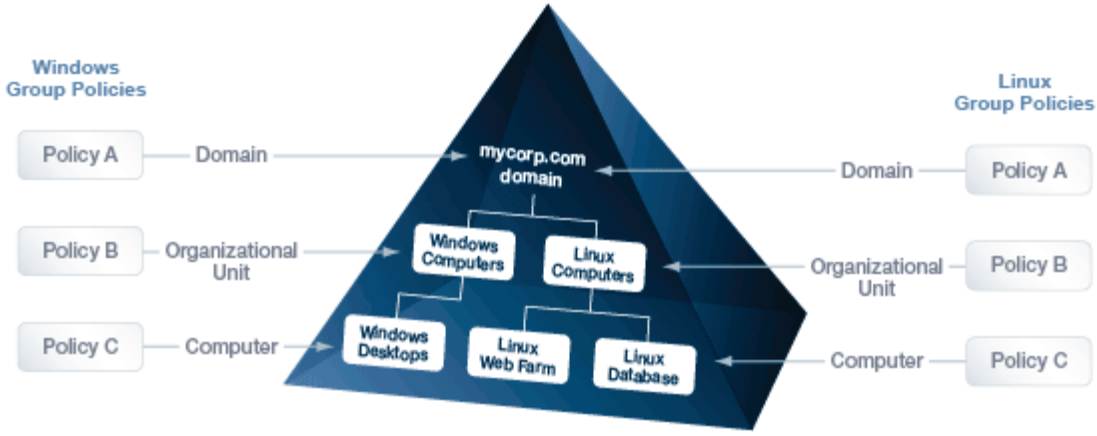
This approach eliminates the need to have multiple local user IDs on different UNIX systems, to have administrators to log as root and/or struggle with the limitations of sudo.[1] Users can log on the system with AD domain credentials, while having appropriate UIDs and GIDs to control user access to specific resources on the local node.

BeyondTrust cell technology provides custom mapping of a unique and identifiable Active Directory user to their UIDs (user identifiers) and GIDs (group identifiers):



[1] For a definition and explanation of sudo, see: http://en.wikipedia.org/wiki/Sudo

After being securely authenticated, non-Windows users have uniform policies applied to their computers. The policies are stored in Active Directory, managed by easy-to-use Windows tools, and can be applied on at the level of the organizational unit in the same way that Active Directory applies group policies to Windows systems:



Altogether, with BeyondTrust technology, compliance requirements are fulfilled in the following fashion:

Requirement	Method of Compliance
Assignment of unique ID to a unique user	With the use of use Active Directory, administrators can provision each non-Windows user with a unique ID, which will work on all UNIX, Linux, and Mac systems. When users are migrated from NIS domains to Active Directory, BeyondTrust uses cell technology to preserve the user NIS information.
Encryption of data transfer	Encryption of all non-console administrative access is accomplished by switching to protocols like SSH, VPN, or SSL/TLS (for web-based management) with Kerberos authentication to Linux, UNIX, and Mac OS X against credentials stored in Active Directory. And, unlike NIS, AD clients cannot retrieve the whole password database for offline inspection.
Password strength	Password strength, history, lifetime, and lockout threshold are enforced on all non-Windows nodes by global policy.
Role-based access control. Linking administrative access to individual users	RBAC is implemented by mapping AD users to non-Windows resources with BeyondTrust cell technology. Cells provide a custom mapping of AD user names to UIDs and GIDs on Linux systems. This establishes granular access control and limits users to the systems that they need to access for business reasons and – within the system – to the commands that they are allowed to execute with sudo. As a result, access to computing resources and to customer data is limited on a need-to-know basis. In the same fashion, time-based access to resources can be implemented.
Simple provisioning and deprovisioning	This is implemented by associating BeyondTrust cells with AD OUs for fast and efficient privilege granting, role change, or termination. All user access to all systems can be effectively terminated by disabling the appropriate AD account.
Computer lockdown after pre-set inactivity interval	Inactivity timeout and screen locking is controlled by the Screen saver policy.
Log rotation	BeyondTrust policies allow fine-grain control of the log rotation daemon.

Requirements	Method of Compliance
System security hardening	This is implemented by configuring AppArmor, SELinux, or the Mac OS X firewall by group policies. Removal of all unnecessary artifacts (such as scripts, driver subsystems, and more) is implemented with group policies.
Access tracking d	PowerBroker Identity Services Enterprise allows administrators to create custom reports about Linux and UNIX users, groups, computers, forests, and domains within Active Directory, search for duplicates, and generate permission or access reports. The BeyondTrust syslog group policy allows administrators to configure the logging daemons on UNIX and Linux nodes. The BeyondTrust event log subsystem provides administrators and security managers with an event viewer that shows denied authentication and access attempts. This implements an automatic audit trail for all system components to reconstruct the user behavior in case of an investigation. An inactivity report can list unused or infrequently used accounts that could be marked for possible deletion.
Alerting	Cron scripts alert administrator to changes in files or policies.

Summary

In today's information security regulatory environment, maintaining compliance with computers running a mixture of Windows, UNIX, Linux, and Mac operating systems can be complex. PowerBroker Identity Services Enterprise seamlessly integrates Linux, UNIX, and Mac computers with Active Directory and enables migration of non-Windows users to AD while maintaining their identities and permissions.

The combination of Windows' AD framework, Windows' management, and monitoring tools along with BeyondTrust technology allows administrators to comply with multiple industry regulations on data protection while also simplifying system management and increasing the security posture of the network.

Contact Information

For more information about this report or if you have any questions, please contact:

BeyondTrust
Corporate Headquarters
2173 Salk Avenue Carlsbad, CA 92008

+1 818-575-4000 (tel)
info@beyondtrust.com