

WHITE PAPER

Privileged Identity Management: IDC Defines an Identity and Access Management Submarket for Managing Privileged User Accounts and Meeting GRC Requirements

Sponsored by: Cyber-Ark Software

Sally Hudson

April 2008

IDC OPINION

Over the past several years enterprise IT organizations have been forced to publicly acknowledge an unsettling truth: Risk associated with insider threats far exceeds that of outsider threats. These insider threats affect organizations at many levels, serving to erode consumer trust and increase corporate costs exponentially. While identity and access management (IAM) solutions typically serve as the foundation for access control and audit, insider threat remains a critical obstacle within the IT enterprise. IDC believes that a significant portion of the insider threat problem can be alleviated by applying a specialized subset of IAM technologies, a privileged identity management (PIM) platform.

IDC defines PIM as:

- An essential building block of the larger IAM ecosystem
- A natural evolution and outgrowth of privileged password management (PPM)
- Able to provide the necessary granularity in a scalable fashion, especially in large-scale computing environments
- A core element of a comprehensive IAM platform by correlating to, and complementing, existing and established IAM practices via the creation of an identity environment tailored to the privileged user and providing audit and tracking capabilities within the privileged user environment

Enterprise organizations must look at PIM as an essential step in achieving and maintaining overall health in governance, risk, and compliance (GRC), as well as an integral source of the security of the internal organization on a continual basis. In fact, some companies are finding that starting with a firm PIM platform allows them to more easily meet compliance and audit requirements as they build out the enterprise IAM architecture and strategy.

METHODOLOGY

IDC's industry analysts have been measuring and forecasting IT markets for more than 30 years. The market forecast and analysis methodology used in this study incorporates information from five different but interrelated sources. They are:

- ☒ Reported and observed trends and financial activity.
- ☒ Product briefings, press releases, and other publicly available information. IDC's analysts around the world meet with hundreds of vendors each year to review current and future business and product strategies, revenue, shipments, customer bases, target markets, and other key product and competitive information.
- ☒ Vendor financial statements and related filings. IDC also builds detailed information related to private companies through in-depth analyst relationships and maintains an extensive library of financial and corporate information.
- ☒ IDC demand-side research. This includes thousands of interviews with business users of software solutions annually and provides a powerful fourth perspective for assessing competitive performance and market dynamics.
- ☒ Review of laws and regulations. IDC keeps track of laws and regulations that shape the regulatory framework affecting security compliance and control. International, federal, state, and local laws are accessed by IDC analysts through a network of information services.

IN THIS WHITE PAPER

IDC's research focuses on the emerging PIM market, a submarket of the overall IAM market as defined in the IDC taxonomy. PIM is the larger, contextual world where PPM resides. IDC has established the need for PPM in previous documents, but it is beneficial for IT professionals to have an overview of the larger ecosystem. Several analogies can be drawn between enterprise PIM and the traditional IAM architecture found within an organization. This document maps the analogies between IAM and PIM while explaining that the value-add of PIM goes beyond security and access management.

SITUATION OVERVIEW

Identity and Access Management: The Who, What, When, Where, and Why of Enterprise IT

IDC defines IAM as a comprehensive set of solutions used to identify users in a system (e.g., employees, customers, contractors) and to control their access to resources within that system by associating user rights and restrictions with the established identity. A typical corporation must employ some, several, or, in some cases, all of the components associated with the IAM market to achieve a comprehensive platform capable of reducing risk, increasing security, and meeting compliance standards.

IDC research shows that compliance is the major driver in the IAM market, accounting for more than 70% of all revenue. To meet regulatory requirements, both government and industry driven, most companies employ a variety of IAM technologies spanning the submarkets and including provisioning, password management, privileged password management, digital signatures, secure single sign-on (SSO), audit and reporting, and two- and multifactor authentication mechanisms. Having established a framework for IAM, enterprise organizations must consider PIM as a next logical step in reducing insider threat while achieving and maintaining compliance.

Privileged users can be either the unsung heroes or the undiscovered villains within organizations, given their exclusive usage and access rights to critical corporate systems. These privileged user accounts are the most powerful accounts defined within critical applications and the servers, operating systems, and databases on which they run. They include, but are not limited to, generic accounts such as administrator on Wintel platforms, root on Unix systems, DBA passwords, and hard-coded passwords found in application scripts throughout an enterprise. Another aspect of privileged user accounts is that controls on privileges must extend beyond the accounts themselves. A full PIM environment should track *all* privileged activity (e.g., if a privileged user logs in from a personal account or an account with more elevated privileges as opposed to SysAdmin). It is a sobering reality that not all privileged actions are initiated via a privileged user account, hence the need for monitoring and tracking all privileged activities.

A goal of the overall PIM approach would be to deliver an environment capable of addressing all privileged users and actions, with the ability to monitor and manage all privileged sessions regardless of access and account usage. This ability can substantially increase overall IT security within an organization while simplifying critical component GRC requirements.

Understandably, IT professionals who are already overburdened with constant demands for increased security mechanisms and GRC requirements often balk at the idea of adding another item to their overly long to-do lists. However, if implemented correctly, a PIM environment can make life easier for the security professional and privileged user alike by giving them the ability to automate, manage, audit, and monitor privileged identities, their life cycles, and their specific provisioning parameters within a single, manageable system — in effect creating a multitiered identity environment for the organization.

A properly deployed PIM implementation can perform the dual function of helping IT to meet security and compliance demands without adding significantly to the day-to-day tasks. GRC and security professionals can take advantage of greater efficiencies via the automated, integrated nature of a privileged identity subsystem.

Market and Technology Trends

Compliance Is the Major Market Driver for IAM

Organizations are faced with addressing compliance issues surrounding Sarbanes-Oxley (SOX), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), European Union Data Protection Directive 95/46, Japanese Personal Information Protection Act (JPIPA), and additional regulations and guidelines, not only in the United States but also in the rest of the world. Additionally, the Payment Card Industry's Data Security Standard (PCI DSS), although not a regulation, has considerable impact on companies that handle credit cards. Further impetus for executives to push their organizations to comply with these regulations includes personal liability and the threat of criminal and/or civil penalties. The ability to track user rights and privileges as well as combat authorization drift is an integral part of a strong compliance program.

Audit, Audit Everywhere ...

With compliance comes the dreaded audit. What was considered a detailed audit just two to three years ago at a large financial services organization is being employed routinely at Global 2000 midsize companies today. Once a centralized IAM environment is established within the enterprise, tools and techniques must be available that are capable of tracking systems with sufficient granularity to satisfy auditors while simultaneously (and seamlessly) integrating with existing systems. As audits are becoming increasingly detailed in their demand for fine-grained data, specialized systems, such as roles-based user provisioning, entitlements, and PIM, are needed.

Companies are putting more access controls in place to present the more detailed information now required by auditors. Who has access to what, when, and why are the questions that must be answered, at different levels, again and again and again. To answer these questions for auditors, most IAM solution suites today are complemented by the addition of audit tools and software. Their main purpose is to allow organizations to reduce liability risks and comply with government regulations. They are often tailored toward a specific regulation or corporate need and are capable of collecting data on security, systems, applications, and events — ideally to a centralized log. Collected information is typically filtered to provide real-time monitoring, triggering notifications and report generation. This ability to monitor, track, and evaluate how access rights are being used is critical to meet government regulation mandates and identify systems misuse.

PIM implementation drives this process deeper by focusing on the privileged user environment within an organization. A PIM system takes into account that while security best practices differ from company to company, employing the proper monitoring and management of privileged accounts and privileged activities is paramount to passing an audit. Corporate IT access controls must incorporate very robust controls on privileged account operations, including those at the application-to-application level. The ability to track access and usage at these levels is a vital element of corporate security.

Further, as worldwide compliance regulations proliferate, it becomes correspondingly more difficult for IT professionals to manage these processes manually. Software solutions are therefore required.

Key Components of IAM/PIM

Today, core IAM technologies include Web SSO (WSSO), federated SSO (FSSO), host/enterprise SSO (ESSO), user provisioning, advanced authentication, legacy authorization for mainframes, public key infrastructure (PKI), hardware tokens and appliances, and directory services. IDC is proposing that a new and critically important submarket is forming surrounding the implementation, restriction, and management of privileged identities. We are calling it the privileged identity management, or PIM, market.

The foundation of IAM is access control, as illustrated in WSSO/FSSO/ESSO technologies, which are pervasive in organizations and are generally the first step in laying the groundwork for a comprehensive IAM platform. These technologies often incorporate user password management technologies, which allow users to log in via username and password while also providing capabilities such as self-service password reset and registration. WSSO and FSSO offer the ability to share a user's log-in and authentication data across different Web sites and applications, both internal and external to the organization, using secure, standards-based protocols. The user is able to sign on to multiple Web sites regardless of the provider or identity domain, and organizations are able to separate employees from external parties to better meet compliance regulations.

Secure ESSO (or host SSO) enables users to log in to internal applications, databases, and other corporate systems with just one identity. ESSO solutions enforce password policies and eliminate the need for employees to remember multiple passwords. In addition to providing a high level of password security and simplifying the password management process for employees, a well-developed system also relieves the IT staff of additional burdens — freeing it to work on more urgent system matters. End users do not have to remember different credentials for different applications.

User provisioning automates the process of granting access rights, automates the process of changing those rights, and in some cases, audits the appearance of inappropriate rights in a user's profile. By automating time- and cost-sensitive manual procedures, user provisioning can sharply reduce the costs of granting new employees, customers, partners, and suppliers the necessary access.

Passwords Are Important

From a security and password policy perspective, expiration parameters and password composition rules are important. Additionally, the ability to synchronize passwords is critical because synchronization reduces the number of passwords a user must remember when accessing various applications on the corporate network. Password synchronization allows users to have a single password with which to access all of their provisioning accounts. Companies can also implement reverse/bidirectional synchronization to verify passwords between assigned target systems and applications utilizing an administration tool's password policies. These functions allow the system to automatically verify and reestablish access based on pre-established policies.

ESSO handles only the storage and autolog-in of user passwords, and most user provisioning systems end at the password management and server level. Core elements of PIM can pick up where ESSO and provisioning leave off by creating a specific SSO environment for the privileged users within any organization.

Some Passwords Are More Important than Others ...

Privileged user accounts are the most powerful accounts defined within an IT enterprise environment. Privileged passwords run on critical applications in servers, operating systems, and databases. Often generic in nature, they include, but are not limited to, generic accounts such as administrator on Wintel platforms, root on Unix systems, DBA passwords, and hard-coded passwords found in application scripts throughout an enterprise. A particularly complex situation arises with embedded application passwords. When two unattended software applications connect, they require a powerful username and a powerful password, which are often stored in clear text or embedded in the application code, configuration file, or script.

Most organizations have more privileged user passwords than personal passwords. Those with access to privileged passwords possess the power to change system data, user access, configuration, and so forth. They also have the power to easily sabotage the critical IT operations of any organization. On a nonmalicious scale, users often unknowingly place an organization in compliance violation by using the generic passwords for systems configuration and other activities. This is perhaps the greatest and most common threat today. For these reasons, privileged user accounts are the target of increased scrutiny by internal and external auditors to ensure that organizations have the proper controls over the financial IT systems and thus are in accordance with the requirements of Section 404 of the Sarbanes-Oxley regulation.

To increase security thresholds, thwart insider threats, and meet GRC requirements, organizations are implementing a PPM approach. The first step is to locate and label these passwords and then apply the appropriate security parameters for access, personalization, change, and control. Given the size and distribution of most enterprise organizations today, this task is, practically speaking, insurmountable without the aid of automation. Ideally, there should be a centralized management function, or dashboard, available to make this monitoring process easier. All of this PPM activity must be audited regularly by appropriate internal systems management and external regulatory sources.

Application Identity: The Sleeping Giant of Password Violations

A widespread and not often talked about issue in almost every company is the existence of powerful privileged identities and passwords hard-coded in clear text in the scripts that sit between applications or on the application server or that are part of an application workflow. The distributed systems approach in business today requires that applications directly access other applications on a constant basis. This includes all types of applications and software, ranging from internal proprietary systems to popular off-the-shelf systems such as SAP, Microsoft, or Oracle. This common process makes these systems vulnerable to insider threat because:

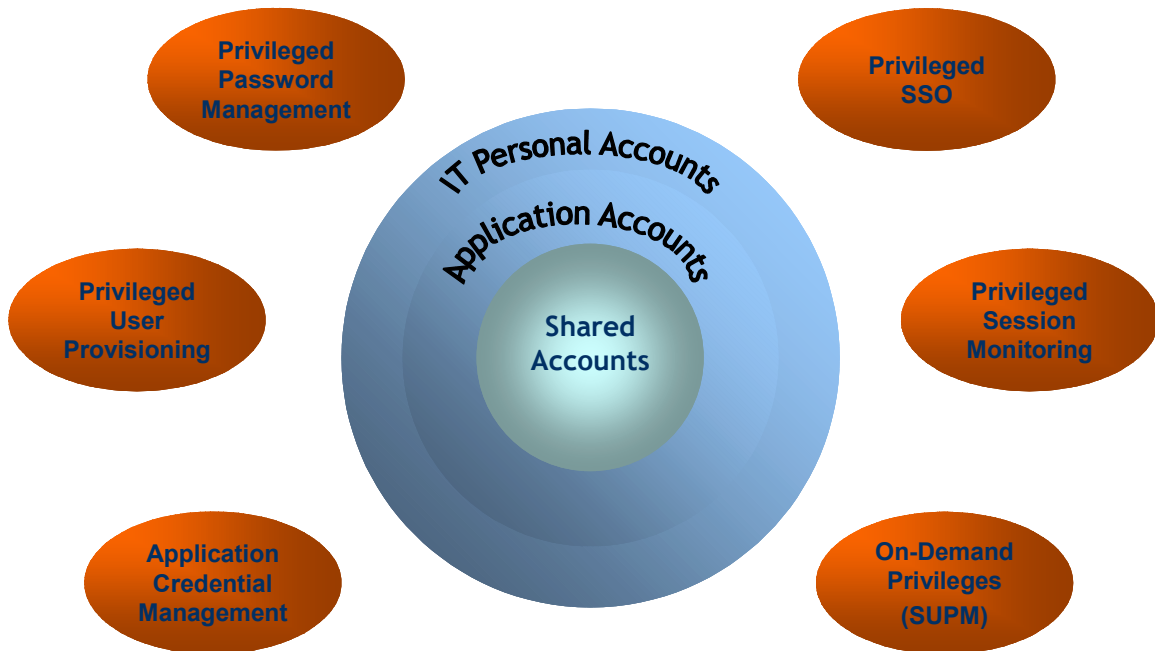
- ☒ They can be accessed by any developer with access to the scripts.
- ☒ It is difficult, if not impossible, to track user access.
- ☒ These systems cannot be easily changed or updated according to company policies.

Further, privileged users may abuse legitimate data access privileges for unauthorized purposes. For example, a user with privileges to view individual patient records via a custom healthcare application client may abuse that privilege to retrieve all patient records via a Microsoft Excel client. Unauthorized privilege elevations are also an issue, and user provisioning software is becoming more refined to eliminate this problem. However, "privilege creep" is a concern for the privileged world as well, and organizations require software capable of dealing with these issues. For example, does one always need to be a full SysAdmin to perform a specific activity on a one-time or occasional basis? The ability to do "on-demand privileges" or privileges delegation is an important element of both user provisioning systems and evolving PIM products. By granting users privileges as needed and then tracking their movements for audit purposes, companies can create a more sophisticated privilege delegation methodology and avoid the privilege elevation trap that is so easy to fall into today. Hostile attackers can also take advantage of vulnerabilities in database management software to convert low-level access privileges to high-level access privileges. These accounts provide wide-ranging access to the data within the application/system, the ability to view/copy/modify this highly sensitive information, and even the ability to change the access rights to this information.

Again, the solution lies in access control policies that apply not only to *what* data is accessible but also to *how* and *when* the data is accessed, and by *whom*. By enforcing policies for time of day, location, and application client and volume of data retrieved, companies can identify users who are abusing access privileges. If the accounts and application servers are not properly managed and secured, with the default passwords changed to a strong password, and under a trackable "change control" process/system, it leaves these critical applications and the data they contain vulnerable to deliberate or inadvertent misuse, breaches, and potential data theft. It could even allow the control of these applications to be transferred to an outside entity not under control, monitoring, or jurisdiction of the target organization (see Figure 1).

FIGURE 1

Privileged Identity Management



Source: Cyber-Ark, 2008

Escalating Need for PIM

In traditional ESSO/WSSO, it is often mandated that end users change their passwords routinely, perhaps every month, every quarter, or annually. This security policy is not routinely extended to the privileged password community, as attempting such a task manually is extremely complicated and would entail hundreds of hours and dozens of employees who are often dispersed geographically around the world. Further complicating an already complex issue is the ability to provision/deprovision systems access when employees are hired and terminated. While provisioning software today is becoming extremely sophisticated from a roles-based entitlement perspective, the deprovisioning issue is extremely critical when the former or soon-to-be-former employee is a systems administrator or developer with access to privileged passwords.

Thus, IT must look at taking the basic IAM components (ESSO/WSSO/password management/provisioning) and replicating this functionality within a privileged user environment.

IAM and PIM: Completing the Circle of Enterprise Security and GRC

A recent and dramatic example of privileged user abuse can be seen in the highly publicized case of Societe Generale, a 144-year-old financial and lending institution in France. In January 2008, it was disclosed that an insider (a 31-year-old junior trader) bilked the bank of almost US\$7 billion through unauthorized, fictitious transactions. The junior trader used the computer log-in and passwords of colleagues in both the trading unit and the technology section to bypass access controls to various computing systems.

Not surprisingly, in February, Societe Generale reported an 82% drop in net profit for the year. The results followed the release of an independent report that found Societe Generale had failed to follow up on at least 75 alerts raised by its risk control officers, compliance officers, and accountants over two years. The independent panel concluded that the accused began making unauthorized transactions in 2005, but lapses in the bank's internal controls allowed the trades to go undiscovered until January 2008! European news agencies report that the scandal has raised serious questions about the quality of risk management and oversight at Societe Generale and prompted speculation about a possible takeover bid.

Unfortunately, this type of incident is not without precedent, both internationally and closer to home. In June 2005, for example, a Federal Trade Commission (FTC) press release announced a landmark settlement in which BJ's Wholesale Club signed a consent agreement with the FTC that requires the large warehouse buying club based in Natick, Massachusetts, to establish and maintain a comprehensive information security program including administrative, technical, and physical safeguards.

The settlement requires BJ's to undergo an audit every year for the next 20 years by a qualified, independent third-party professional to indicate that its security program meets the standards of the order and that it complies with standard book and record keeping provisions. BJ's was accused of lax security measures allowing for the theft of both debt and credit card information. Following the discovery of the fraud, banks and credit unions have filed suit with BJ's and pursued bank procedures seeking the return of millions of dollars in operating expenses and fraudulent purchases. According to BJ's May 2005 SEC filings, the amount of outstanding claims was over \$13 million.

Of course, the BJ's scandal was not the last news to break in this area. Many other well-known companies and organizations, including The TJX Companies, Boeing Co., Cingular Wireless, and ChoicePoint Inc., and several large universities have had well-publicized security breaches over the past several years.

Unless more comprehensive controls are put into place, IDC believes these incidents will continue to occur. As the problem of fraud becomes more widespread, governments will steadily (and in some cases harshly) tighten the noose around the necks of careless businesses to prevent the onslaught of problems created in the wake of carelessness.

IDC recommends that businesses focus on the following strategies to avoid being in this position:

- Vigorously* limit and control access to sensitive data
- Enforce rigorous passwords/authentication
- Store consumer data for less than 30 days
- Encrypt consumer information when transmitted or stored
- Conduct regular security investigations for unauthorized access
- Watch for security compromise in new technology or in new uses of old technology (e.g., wireless devices, PDAs)

Regulations such as Sarbanes-Oxley require businesses not only to document and assess their internal controls but also to control access to financial systems. Section 404 covers internal control activities during the creation of financial reports and points to compliance risks that can be addressed by IAM and PIM solutions. Much of this can be achieved by mapping the same strategies employed in IAM to a PIM environment, as illustrated in Table 1.

TABLE 1

Mapping Strategies Employed in IAM to a PIM Environment

	Identity and Access Management	Privileged Identity Management	PIM-Specific Value-Add Administrator IDs and Application IDs	GRC Initiatives
Access Controls				
Directory-based user management	X	X	Secure, centralized vault for privileged accounts Autoprovisioning the correct privileged users to the correct target accounts	SOX, GLBA, Basel II, PCI
Cross-domain SSO	X			SOX, GLBA, Basel II, HSPD-12, HIPAA
User account provisioning/deprovisioning	X	X	Roles-based, on-demand access to shared, privileged accounts	SOX, GLBA, Basel II, HSPD-12, HIPAA
Approval workflow management	X	X	Apply policy to privileged accounts based on requestor role	SOX, GLBA, Basel II, HSPD-12, HIPAA, PCI
User access recertification	X	X	Automatic password resets for shared accounts	SOX, HSPD-12, PCI
Password synchronization	X	X	Synchronized password changes for shared accounts and between database and applications	SOX, PCI

TABLE 1**Mapping Strategies Employed in IAM to a PIM Environment**

	Identity and Access Management	Privileged Identity Management	PIM-Specific Value-Add Administrator IDs and Application IDs	GRC Initiatives
Password quality enforcement	X	X	Privileged accounts adhere to company policy on length, strength, uniqueness, and frequency of change	SOX, PCI, HSPD-12
Access management	X	X	Protects against application-to-application access abuse; access controlled to application level	SOX, GLBA, Basel II, HSPD-12, PCI
Enterprise SSO	X	X	Transparent log-in to shared accounts and strong authentication for privileged accounts that offer only user/password log-ins (i.e., single factor)	SOX, GLBA, Basel II, HSPD-12, HIPAA
Strong authentication	X	X	Encryption of both at-rest and in-transit requests	SOX, GLBA, Basel II, HSPD-12, FFIEC, PCI
Account management and user self-service	X			SOX, FFIEC, HIPAA
Shared account management		X	Personalizing, securing, and tracking usage of generic shared accounts	SOX, PCI, Basel II
Inter-application authentication		X	Management, securing (encryption), and auditing of application-to-application authentication	SOX, PCI, Basel II
Fine-grained entitlements	X	X	Privileges elevation/on-demand privileges	SOX, GLBA, HIPAA
Audit and Reporting				
Real-time activity monitoring and correlation	Add-on	X	Included	SOX, GLBA, Basel II, HSPD-12, HIPAA, PCI
Automated incident remediation	Add-on	X	Included	SOX
Compliance reporting	X	X	Included	All

Source: IDC, 2008

Benefits of PPM and PIM

Corporations are moving as fast as possible to implement automated systems that contribute to a strong security framework, and auditing, archiving, and storage become essential components for compliance purposes. Certain information (who, what, where, when, and why) must be easy to locate and produce for audit. Easy implementation of new controls is essential due to the metamorphic nature of the compliance landscape. A proactive automated system that does not permit an out-of-compliance action to occur is the goal, and systems such as those offered by PIM can reduce complexities and tracking headaches for IT executives and systems administrators alike.

Increasingly, both internal and external auditors are highlighting existing privileged password management policies, procedures, and solutions as an area of audit concern or noncompliance. For issues specific to areas under the PIM umbrella, Sarbanes-Oxley and other audits are finding problems with existing solutions, including:

- Lack of accountability (Many existing internal solutions are not able to ensure 100% accountability for shared or application privileged accounts.)
- Lack of effective, secure release controls
- Limited implementation of strong inter-application authentication
- Lack of monitoring of privileged activities and enforcement of privileged activity policies
- Lack of change controls (Too many internal solutions today deploy manual and infrequent change controls of shared privileged passwords, with many not managing application accounts at all.)
- Lack of consistency in password change policies (i.e., an enterprise may have a strong internally developed solution for Unix root privileged accounts, but not for Windows administrator or DBA accounts)
- Limited auditing of privileged activities, approvals processes, privileged account access requests, privileged password changes, and/or strength/uniqueness

Propelled by today's compliance-driven environment, including ISO 17999, ITIL, and CobiT (see Appendix), the design requirements for an administrative password management solution need to address critical issues such as password storage, password release, and password updates and changes, which also require robust auditing capabilities for reporting purposes.

THE CYBER-ARK APPROACH

Cyber-Ark Software, a privately held software security company based in Newton, Massachusetts, offers corporations a PIM suite that includes the Enterprise Password Vault (EPV), a unique privileged password management system, as well as the Inter-Application Identity Manager (IAIM) for managing generic application accounts. Both products incorporate the company's Digital Vault and Central Password Manager technologies. The PIM suite is designed to allow organizations to change privileged passwords automatically on remote machines, applications, and operating systems and store the new password securely in the Digital Vault highly secure storage. This can be accomplished without human intervention and can be completed rapidly and in accordance with corporate policy. Within the PIM suite, multiple security layers (including firewall, VPN, authentication, access control, dual control, FIPS 140-2 validated encryption module, and more) make up the core of the Vault. These layers are assembled to offer organizations a comprehensive security platform for storing and sharing privileged passwords in an enterprise environment.

Inside the Vault are storage units designated as safes, which are designed to give IT professionals flexibility and choice when organizing privileged passwords according to unique corporate requirements. Each safe is configured with a specific list of users with authorized access — all others remain unaware of its existence. Within the safe, additional security parameters enable the administrator to determine which activities each user can carry out on the passwords. Password policies define the type of password that is allowed and how frequently the password must be changed. The type of password indicates the rule that applies to the password, such as the minimum number of characters required for the password, the type of characters, and so on. The frequency of the password change indicates if the password must be changed at regular intervals or if it is a "one-time" password that must be changed after having been accessed.

The Enterprise Password Vault provides administrators the tools to manage and use privileged, administrative identities and to automate password management operations such as recycling, verification, and autodetection. The Inter-Application Identity Manager allows applications and scripts to eliminate the usage of hard-coded credentials and provides extensions to ensure that application passwords can be managed according to enterprise policies. The solution provides sophisticated SDK and application authentication capabilities to allow runtime access to application identities managed in the Digital Vault.

The PIM suite also includes compliance and policy management tools such as a dashboard application, compliance reports, and live status of potential policy violations across the entire PIM environment. Future enhancements planned in Cyber-Ark's PIM suite include the ability to fully monitor and control privileged sessions, as well as on-demand access to privileged identities by regular, personal users.

Cyber-Ark has designed the PIM suite to solve the following issues within a PIM environment:

1. **Policy management.** Companies can define and enforce life-cycle policies for privileged identities that include the requirement for access management, automated management, auditing, entitlement, and notifications. The policy defines which users and applications should use each privileged identity, when, how, and for what purpose.
2. **Password storage.** The storage of privileged passwords requires strong encryption and server security. Key management must be secure, and the system responsible for holding the passwords is hardened and firewall protected to prevent unauthorized access.
3. **Password release.** The password release mechanism can support dual control to help achieve segregation of duties for the managed accounts. In addition, the release mechanism is encrypted to support strong authentication. Granular authorization allows only required users to request the password.
4. **Password update.** The system automatically generates and updates the passwords to be managed. This ensures strong and random passwords and maintains individual accountability. Passwords can (and should) be rotated/regenerated routinely.

5. **Inter-application identity management.** Inter-Application Identity Manager provides a secure environment for applications to authenticate to databases or applications without hard-coded credentials. The solution supports leading application servers, batch scripts, and custom applications in Java, .NET, and C/C++.
6. **Auditing.** Robust auditing is essential to frequent demands for process reconciliation and reporting. Ideally, reports should detail all password changes and related activities.

Designed to be an easily integrated, plug-and-play solution for the enterprise, the PIM suite also provides the following capabilities to achieve a comprehensive PIM platform:

- Customizable privileged user and administrator profiles
- Centralized dashboard for displaying privileged user data
- Email notification
- Integration of verification and alerting system
- Bottom-up analysis and design around privileged users and their usage of PPM

Cyber-Ark's EPV and IAIM are currently used by Fortune 1000 customers such as T. Rowe Price, ING, and Deutsche Bank, as well as Global 2000 companies and government organizations throughout the world. Major verticals include government, financial services, pharmaceutical, retail, and energy.

FUTURE OUTLOOK

Government and industry regulations require not only the aggregation of data and event management but also the ability to identify and remediate internal threats based on user privileges. Privileged access and control of shared administrative accounts is a continuing area of interest and concern for the enterprise. Today's increasing compliance requirements have focused additional attention on how the enterprise manages and controls these critical accounts and passwords.

IDC research shows that IAM has emerged as a key component of a compliance platform. We predict that compliance and corporate governance initiatives will significantly drive IAM software spending in 2007 and beyond. The IAM market accounted for nearly \$3 billion in software license revenue and maintenance revenue in 2006, and IDC forecasts that it will reach \$5 billion by 2011, exclusive of services. Regulatory compliance is a strong growth factor in this market, both horizontally and vertically and on a worldwide basis.

IDC believes that increasing regulatory compliance mandates (both in the United States and internationally), combined with budgetary and staffing constraints as well as U.S. economic uncertainty, will drive organizations to look for better ways to cost-effectively manage their security infrastructures. The need to comply with specific regulations will push organizations to look for IAM and related solutions to help solve security and GRC issues, as determined by company size, revenue, and vertical industry compliance demands.

CHALLENGES/OPPORTUNITIES

Industries looking to combat identity fraud and identity theft will want to enhance current IAM solutions and establish best practices for monitoring, maintaining, and modifying these systems as necessary to effectively protect data and information from both internal and external threats. Further, as security becomes more important at the application level, new products will be introduced that are designed to assess the status of individual applications, databases, and Web servers. Organizations will demand software that is less vulnerable to external attack and/or internal compromise. Therefore, security at the application level will become a fundamental requirement for software within the enterprise. These trends will present opportunities for companies such as Cyber-Ark that offer lower-cost and easy-to-integrate solutions.

In the recent past, the biggest challenge facing companies such as Cyber-Ark was the reluctance of corporate IT to openly acknowledge that opportunists may exist among their own ranks. Ironically, thanks to the worldwide publicity attached to security breaches, such as those mentioned in this paper as well as numerous others, organizations can no longer adopt an ostrich-like posture to these situations. While historically there have been no easy answers to the privileged user problem, the emergence of technologies capable of enabling an automated, integrated PIM environment should ease the corporate workload while increasing security and meeting GRC initiatives.

The greatest challenge for Cyber-Ark and others in the PIM space will be to educate corporate IT that these solutions exist and to demonstrate that they do indeed work. Cyber-Ark will have to point to existing deployments as proof of easy integration with directories or provisioning solutions for monitoring and enforcement, as well as the ability to audit and report on user access activity within the PIM environment.

CONCLUSION

Organizations must move from a reactive compliance stance to proactive and cost-effective information protection and control. Enterprises must go beyond the minimum requirements of regulatory compliance to internal policy compliance at a higher level of assurance. The ability to perform automated checks in advance of auditing, to report on a regular basis, and to monitor employees and discern behavior patterns to stop malicious and noncompliant actions before they occur requires that steps be taken to achieve proactive and effective cost management.

The broadening of the enterprise workplace has greatly increased risk, and IT organizations are trying to manage this new environment. This will eventually require more usage of a total security framework, including security management, IAM, security information and event management (SIEM), and secure content and threat management (SCTM) solutions.

IDC believes that inadequately addressed compliance regulations will result in increased violations and subsequent legal and public relations problems for corporations over the next several years. The value of PIM is germane to all enterprise-class organizations across industries and on a worldwide basis.

APPENDIX

Definitions

- ☒ **HIPAA.** The Health Insurance Portability and Accountability Act of 1996 requires that to ensure privacy and confidentiality, all patient healthcare information be protected when electronically stored, maintained, or transmitted. It also mandates that each user be uniquely identified before being granted access to confidential information. It specifies that access to personal health information (PHI) be restricted to only those individuals who need access as part of their role.

- ☒ **Sarbanes-Oxley Act of 2002.** The Sarbanes-Oxley Act of 2002 requires public companies to validate the accuracy and integrity of their financial management. It requires businesses not only to document and assess their internal controls but also to control access to financial systems. Section 404 covers internal control activities during the creation of financial reports and points to compliance risks that can be addressed by IAM solutions.

- ☒ **Gramm-Leach-Bliley Act (GLBA).** The GLBA mandates privacy and the protection of customer records maintained by financial institutions. These security requirements include access controls on customer information systems, encryption of electronic customer information, procedures to ensure that system modifications do not affect security, and monitoring systems to detect actual attacks or intrusions.

- ☒ **California Security Breach Information Act.** This law, better known as SB-1386, requires companies to report security breaches involving private consumer information. The California law was the first of its kind but it has been replicated in over 30 states and growing.

- ☒ **European Union Data Protection Directive.** Member countries are mandated to adopt standards for the collection, storage, and disclosure of personal data, and individuals' rights concerning their personal data are outlined. This directive is described as the most ambitious and stringent data privacy initiative.

- ☒ **JPIPA.** JPIPA is a Japanese law aimed at protecting personal data and regulating the acquisition, custody, and use of personal information. The act requires the following from businesses: specify the purpose for collecting and using personal information; do not collect information by fraudulent or unfair means; promptly notify the subject of the purpose for which his or her personal information will be used; ensure securing of personal data from loss and unauthorized access/disclosure; refrain from giving personal data to third parties without subject's consent; permit individuals to access and correct personal data.

- ☒ **PCI Data Security Standard (PCI DSS).** The PCI DSS was initially adopted by major credit card companies. Its goal was to articulate clear requirements to any entity that processes or holds credit cards to ensure the protection of credit card data. The standard was intended to prevent fraud and protect consumer privacy when sensitive data is submitted to a financial institution, merchant, or vendor over the Internet and stored on its network. PCI DSS provides a single global

security standard that offers specific technical guidance for protecting cardholder interests. PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. It presents the framework and standard for protecting cardholder and sensitive authentication data with the goal of limiting access, controlling fraud, and providing financial benefits to organizations that are in compliance.

- ☒ **ISO 17799.** This detailed security standard is organized into 10 major sections: business continuity planning, system access control, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, computer and network management, asset classification and control, and security policy. The objective of ISO 17799:2005 is to provide a common basis and practical guideline for developing organizational security standards and effective security management practices.

- ☒ **IT Infrastructure Library (ITIL).** ITIL has seven sets of processes providing a framework for businesses in the following areas: service support, service delivery, planning to implement service management, ICT infrastructure management, applications management, security management, and business perspective.

- ☒ **Control Objectives for Information and Related Technologies (CobiT).** CobiT was developed as a generally applicable and acceptable standard for good information technology security and control practices for management, users, auditors, and security practitioners. It was issued by the IT Governance Institute and now is in its third edition. CobiT contains 34 processes and provides the tools to assess and measure an organization's ability to deliver on those processes. It was originally published in 1996, with versions 2 and 3 appearing in 1998 and 2000, respectively. Version 4 has just been released.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2008 IDC. Reproduction without written permission is completely forbidden.