Portal Authentication: A Balancing Act Between Security, Usability & Compliance

An Osterman Research White Paper

Published August 2009

Sponsored By  PISTOLSTAR

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com • www.ostermanresearch.com

Why Strengthening Authentication is Critical

Virtually every organization maintains highly sensitive information to which it must control strict access. These data sources might include customer databases, CRM systems, repositories of financial information and the like. Increasingly, these content sources are accessed through portals built in IBM® WebSphere® Portal, the leading portal software provider[1], and Microsoft SharePoint.

Maintaining robust security is not just a good idea; it is also increasingly becoming the law. For example, there is a large and growing number of state, provincial, federal and international regulations focused on maintaining the integrity of sensitive and confidential information. These requirements include, but certainly are not limited to, the following:

- S.B. 1386 (California)
- The Gramm-Leach-Bliley Act (US)
- The Payment Card Industry Data Security Standard (US)
- The Health Insurance Portability and Accountability Act (US)
- The Personal Information Protection and Electronic Documents Act (Canada)
- Personal Data Ordinance Code of Practice on Consumer Credit Data (Hong Kong)
- Information Technology Act 2000 and Amendment Act 2006 (India)
- Personal Data Protection Act: Telecommunications Act (Spain)
- Data Protection Code (Italy)
- Electronic Communications Act (Sweden)
- Postal and Electronic Communications Code (France)
- S 93 Telecommunications Act (Germany)

A failure to comply with these requirements can be very costly, totaling in the millions of dollars in some cases.

However, maintaining highly secure and usable access to corporate systems is difficult using native tools. For example, a highly secure authentication mechanism that requires very strong, unique passwords for access to each system will often be defeated by users who will simply write them down in non-secure locations, or users will forget their passwords and make frequent calls to a help desk to recover them, driving up help-desk and IT costs. On the other hand, relaxing the strength of passwords, allowing the same password to be used for multiple systems or requiring only single-factor authentication will make life easier for users – as well as for hackers and rogue internal users – thereby decreasing the security of sensitive applications and information.

WHAT ORGANIZATIONS NEED: SECURITY, USABILITY, AUDIT AND COMPLIANCE

What organizations need, therefore, is the best of both words: highly secure access to corporate resources to maintain their integrity, and ease-of-use for individuals accessing these systems. Ideally, an authentication system will provide robust and granular capabilities

[1] http://www.eweek.com/c/a/Web-Services-Web-20-and-SOA/Report-IBM-Number-One-in-Portal-Software-333186/

for IT to manage the security of corporate resources, and it will allow users the ability to recover or reset their own passwords.

ABOUT THIS WHITE PAPER

This white paper discusses the problems with current authentication systems and the drivers that should be motivating organizations of all sizes to improve their access controls. It also discusses PortalGuard, an offering from PistolStar that enables IT to provide secure and granular authentication to corporate resources while maintaining the ease of use that individuals require.

Changing Circumstances in the Enterprise

THE GROWING NUMBER OF ENTERPRISE WEB APPLICATIONS

There are a large and growing number of Web and enterprise applications that users access on a regular basis. In fact, just about every corporate application is either designed as a browser-based application or has an HTML interface to a backend application. Key to the utility of these applications is their integration so that data from one application can be passed to another and all relevant applications updated in real time. However, integration is not an easy task in many organizations because the majority of Web-focused applications maintain a unique database, they may not share information in standard ways, they require different access methods, and so on.

Compounding the problem is simply the sheer volume of applications that individuals employ on a daily basis. For example, in the primary research survey conducted for this white paper we found that users access a mean of 12.3 password-protected systems on a typical day at work, including tools like their corporate network, email, CRM systems, Web portals, Twitter and other tools that they use for work-related purposes.

The problems that this number of access credentials creates include the fact that most users report that they have too many usernames and password to remember, they use the same password for accessing more than one system, they forget passwords periodically, and they must call the help desk all too frequently to have their passwords reset.

Further, the situation is not getting better or easier over time. There are a growing number of portals being implemented to access corporate applications, raising the number of password stores that must be managed. This, in turn, increases the sets of password policies that need to be managed, further complicating the entire password management problem that organizations face and decreasing the overall level of security for corporate applications.

KEEPING UP WITH THE SPEED OF BUSINESS

Keeping up with "the speed of business" may be a bit of a cliché, but it is a critical necessity, particularly in a difficult economy in which demand is softer and competition is more severe. By keeping up with the speed of business, we mean providing globally and remotely based employees, customers, partners and vendors with streamlined – yet secure – access to corporate intranets, extranets and portals. This is particularly important for any organization

that wants to realize the benefits of a distributed workforce. For example, a large proportion of employees at companies like IBM and Boeing do not have a fixed location from which to work, but instead work from home and come into the office only on an as-needed basis. This can save a large organization millions of dollars each year on rent, power, taxes and other costs – savings that are even more appealing during an economic downturn.

However, becoming more mobile and flexible is not without its problems. For example, instead of walking down the hall to a departmental meeting, some employees will log into an online meeting space to participate in a shared whiteboard session or a videoconference. Remote team members, partners or consultants that are brought into a project will need to be given access to various corporate applications so that they can do their work.

The implications for keeping up with the speed of business are several and impact groups across the enterprise in various ways:

- For IT staff, it means more work in managing access to various corporate systems, in addition to the tasks associated with deploying, configuring and maintaining these systems.

- For help desk staff, it means more calls to recover more passwords as users forget them and need to have them reset.

- For users, it means more difficulties in accessing corporate systems that they need to do their work and more time spent being unproductive while waiting for passwords to be reset by the help desk.

- For organizations in general, it means a loss of employee productivity and higher overall costs if access to systems is not seamless.

In general, then, organizations must provide easy to access to a growing variety of backend systems, Web tools and other capabilities while imposing the least impact on users, IT and help desk staff.

Increasing Complexity of Security Challenges

THWARTING UNAUTHORIZED PARTIES FROM GAINING ACCESS

It virtually goes without saying that unauthorized parties should be prevented from accessing corporate systems and data sources. Preventing hackers and others from gaining access to these resources is of paramount importance to protect against the loss of sensitive and confidential information and the consequences that can arise from data breaches. The consequences of data breaches can be quite severe in some cases, resulting in the loss of millions of dollars in lost business and remediation, not to mention less tangible consequences like loss of reputation.

Keeping out hackers and others is a problem that has not been lost on those charged with managing their organizations' IT infrastructure. In the survey conducted for this white paper,

we found that 53% of these individuals are concerned or very concerned about potential data breaches from external sources like hackers. Further, 27% of these individuals are more concerned about the problem of unauthorized access than they were just 12 months ago, while only 5% are less concerned.

In short, prevent unauthorized access to corporate portals and other resources needs to focus on detecting fraud patterns and usage anomalies from inside sources, such as disgruntled employees, as well as protecting business applications from phishing, Trojans and other external Web-borne threats. However, it also must focus on enabling IT to implement business policies and automate business processes, but then push policy decisions and compliance monitoring to business owners. For example, an Osterman Research survey published in mid-2009 found that 63% of IT decision makers would like a way to enable other parts of their organization to manage the enforcement of policies for acceptable use and regulatory compliance. The same survey found that one-half of those in IT feel that C-level line of business managers should be more involved in managing policies for confidential information protection and regulatory compliance.

PREVENTING INCIDENTS OF PASSWORD FRAUD AND DATA THEFT

Clearly, decision makers are concerned about preventing incidents of password fraud and data theft, and so need to reduce the risk of exposure and of being hacked or attacked. However, hackers exist both internally and externally and are becoming more sophisticated and clever over time. They have become stealthier in their practices and they are being rewarded: they are achieving greater success at capturing passwords and breaking authentication methods.

In short, IT has its work cut out:

- It must prevent data breaches and exposure and mitigate against the rising level of risk in the enterprise because of the increasing number and variety of vulnerabilities.

- It must meet the data security standards that have been established by government, industry and corporate mandates.

- It must meet customers' demands for the protection of personal data. This may, in fact, be the worst problem associated with data breaches given the high level of customer churn that can occur after a breach. For example, a study by SafeNet UK found that nearly one-half of those in Britain would not buy from a company that had suffered a data breach[2].

- Finally, IT must deploy the right technologies and achieve the correct balance between authentication security and usability. If authentication is made too difficult or cumbersome for end users – by requiring very strong, unique passwords for each application or portal, for example – users will simply circumvent this system by writing passwords in non-secure areas, defeating the work that IT has done.

[2] http://is.gd/25GJD

Portals Need Stronger Authentication

USERS MUST AUTHENTICATE MULTIPLE TIMES

Portals are growing in popularity because they offer organizations the ability to create customized experiences for different groups of users within or outside an organization. For example, an IT department can create a portal for financial users that consists of a mashup of access to various financial applications deployed on internal corporate servers, external Web-based applications, Web-based data sources and feeds, a document repository, notifications, calendars, and the like. Using the same underlying technology, IT could create a separate portal for its manufacturing operation, a portal for each region in which it operates, etc. The portal content could be based on the roles of users inside an organization or other parameters. Among the leading corporate portal and mashup offerings currently available are IBM® WebSphere® Portal Server and Microsoft SharePoint Portal Server.

Despite the utility of portals, one of the key drawbacks with them is that users must authenticate to access the portal itself, and must then authenticate again for each of the application servers or data sources they want to access through the portal. The drawbacks of requiring users to authenticate to several different applications include the fact that users regularly forget passwords or they lose passwords and must contact the help desk to retrieve them, they have too many passwords to remember, and help desk costs are driven up by the need to reset forgotten passwords. As noted earlier, the survey conducted for this white paper underscored the quite serious problems that users have with too many passwords.

THE NEED FOR PORTAL ACCESS CONTROL IS MUCH MORE IMPORTANT

With the entrance to so many applications, data sources and other content and resources through one access point so easily facilitated by a portal, the need for access control is that much more important compared to traditional methods of accessing these applications and content sources. Further, corporate portals and social networking capabilities are converging as part of a larger move to collaboration. By integrating portal and social networking capabilities, content can be integrated with the ability to collaborate in more meaningful and faster ways than if a separate backchannel, such as email, must be used for collaboration.

Among the capabilities that organizations must deploy to ensure the integrity of the applications and data accessed through the portal are:

- The need to secure the authentication process so that users access only the applications and data sources they are authorized to access.

- The need to monitor user login behavior so that IT can determine where and with whom there are security risks.

The latter point is particularly important to prevent rogue users – either inside the organization or among business partners – from causing data breaches that could compromise corporate security, violate regulatory requirements and otherwise create trouble for an organization. While some studies suggest that inside threats are the primary

source of data breaches and other research suggests that external threats are most prevalent, even the latter reveal that insider threats are a major source of data breaches. Maintaining appropriate access control, therefore, must be a key consideration as portals become more widely deployed.

The Need: Simplify, Yet Secure Access and Authentication

WHAT A SOLUTION MUST PROVIDE

Clearly, IT must deploy an authentication capability that is both sufficiently robust to protect corporate applications and content sources, and easy enough to use so that users will not defeat the steps that have been taken to secure access. Specifically, an authentication solution should provide:

- Strong, multi-factor authentication beyond just the simple username/password combinations that are commonly used. The use of multiple authentication factors can provide an additional level of security beyond what is provided by the use of a single method.

- Self-service password recovery and reset so that users can recover their own forgotten passwords without having to call the help desk for assistance. This will speed users' access to systems, making them more productive, and it will reduce help desk calls and costs.

- Browser-based access with secure functionality in order to increase the versatility of access for users. This is particularly important as more users work from home or other remote locations.

AUTHENTICATION AND PASSWORD SECURITY FUNCTIONALITY

In order to maintain robust security for corporate applications and data assets, an authentication solution should possess a number of features that can be configured and easily managed by IT staff members. These features include:

- Password expiration intervals that will require users to create a new password at predetermined times defined by IT. Obviously, the more sensitive or critical the asset that is being accessed, the more frequently that IT might want passwords to change.

- Password strength rules that will enforce minimum corporate standards for password strength.

- The ability to define strikeout limits by person, group or hierarchy. The most sensitive assets, for example, might allow just two password-entry errors, while less sensitive ones might have no limits. This feature is particularly important, since IT might want to allow inside users more leeway than the external users over which IT has less confidence or control.

- The ability to limit multiple, concurrent logon sessions. For example, this will allow IT to impose controls over users who might log into an application and then walk away from their desk, and then open the application again on another computer, leaving access to the application unattended on the first computer.

- The ability to lock out inactive users after a specified number of days. This allows IT to limit access to an application or content source only to active users.

- The ability to impose password limits that will restrict the frequency with which passwords can be re-used. This feature is critical to prevent the very common occurrence of users employing the same password for multiple applications. Doing so creates an enormous security vulnerability, since a hacker or other unauthorized user that gains access to one password will then have access to a number of other systems.

ACCESS CONTROL AND MONITORING OF USER LOGIN BEHAVIOR

IT must also have the ability to monitor users' login behavior as part of a robust access control capability. Tracking users' access events include things like each user's last successful login and login attempt(s), the time they last logged into the system or attempted to do so, any password changes that users might have made, and their use of weak passwords. This monitoring capability will ensure that IT has the information it needs to maintain the appropriate levels of security for each asset, and will allow IT to identify individual users who might pose a risk, such as through their use of weak passwords.

Regulations Focused on Security

NEW REGULATIONS FOCUSED ON SECURITY

There are a large number of regulations worldwide that require holders of personal, consumer and employee information, as well as other sensitive content, to protect that information from unauthorized access. Among these regulations are the following:

- **S.B. 1386**
  California's SB1386 (the Database Security Breach Notification Act) is a far reaching law that requires any holder of personal information about a California resident to notify each resident whose information may have been compromised in some way. This requirement makes it very important to retain and transmit records in an encrypted form, since doing so exempts an organization from the reporting requirement in the event of a breach.

- **PCI DSS**
  The Payment Card Industry Data Security Standard (PCI DSS) encompasses a set of requirements for protecting the security of consumers' and others' payment account information. It includes provisions for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.

- **GLBA**
  The Gramm-Leach-Bliley Act (GLBA) requires that financial institutions protect information collected about individuals, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers.

- **Regulation S-P**
  Regulation S-P has been adopted by the US Securities and Exchange Commission (SEC) in accordance with Section 504 of the GLBA. This section requires the SEC and a variety of other US federal agencies to implement safeguards to protect non-public consumer information, and to define standards for financial services firms to follow in this regard. The rule applies to brokers, dealers, investment firms and investment advisers.

- **HIPAA**
  The Health Insurance Portability and Accountability Act (HIPAA) of 1996 addresses the use and disclosure of an individual's health information. It defines and limits the circumstances in which an individual's protected health information (PHI) may be used or disclosed by covered entities, and states that covered entities must establish and implement policies and procedures to protect PHI.

- **Federal Trade Commission's proposed security breach notification law**
  In April 2009, the Federal Trade Commission proposed a security breach notification law focused on electronic health information. The rules, covering notification to individuals and federal regulators, would apply to vendors of personal health records and entities that offer products or services through Web sites of such vendors.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)**
  The Family Educational Rights and Privacy Act of 1974, which is focused on protecting the privacy of students' education records, includes provisions for how states can transmit data to Federal entities.

- **Red Flag Rules**
  Part of the Safeguards Rule, the Red Flag Rules requires financial institutions and creditors to implement a program to detect, prevent, and mitigate instances of identity theft.

- **Canada**
  The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian privacy law that applies to all companies operating in Canada. Like many other privacy laws, it requires that personal information be stored and transmitted securely.

- **United Kingdom**
  The UK's Information Commissioner issued The Employment Practices Data Protection Code in June 2005, which includes, among other things, limits on the extent to which employee communication can be monitored.

- **Japan**
  Japan's Personal Data Protection Law is designed to protect consumers' and employees'

personal information. It includes provisions for ensuring the security and disclosure of databases that contain this information, among other provisions.

- **France**
  The French Data Protection Act, Article 34, requires those who control data to protect the security of the data under their care. A failure to adequately protect data can result in a fine of €300,000 and five years in prison.

- **Italy**
  Legislative Decree no. 196 (the Personal Data Protection Code) requires the protection of personal data, managed by the Garante Per La Protezione Dei Dati Personali.

- **Germany**
  The German Federal Data Protection Act (Bundesdatenschutzgesetz) has passed an amendment that will take effect on September 1, 2009 requiring data breaches to be reported to customers. However, the German law is less restrictive than those in many other countries, requiring notification only if a particular data breach represents an "imminent threat".

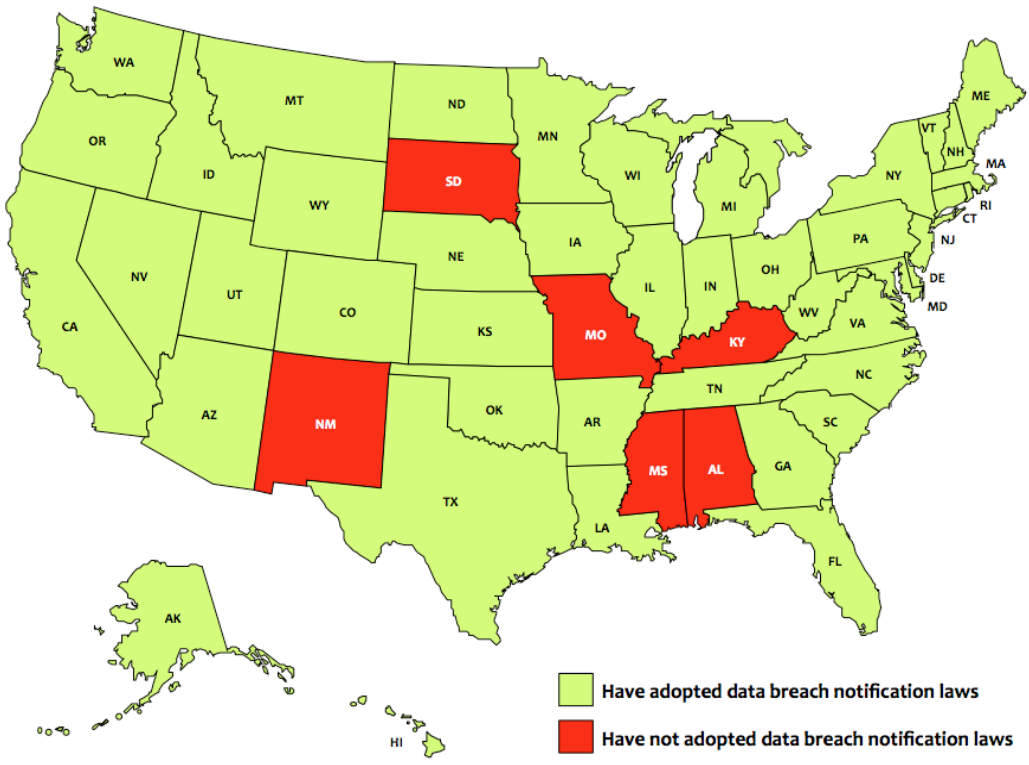
- **Hong Kong**
  The Code of Practice on Consumer Credit Data was first published in 1998 with revisions in 2002 and 2003. The Code was issued by the Hong Kong Privacy Commissioner in response to Part III of the Personal Data (Privacy) Ordinance (Cap. 486).

- **Australia**
  Australia has not passed any laws requiring the report of a data breach despite the 2008 recommendation by the Australian Law Reform Commission that such notification be required.

- **EU Regulations**
  Directive 95/46/EC (the Data Protection Directive) was originally implemented in 1995 and reflects a strong European focus on privacy rights. The Directive provides for a number of different protections on personal data, including restrictions on the transfer of data to countries outside of the EU whose data protection standards are determined not to meet the EU's standards.

There are also a growing number of US state laws that address data breaches – 44 of the 50 US states have enacted data breach notification laws, as shown in the following figure.

Status of Breach Notification Laws at the US State Level



Data Source: National Conference of State Legislatures

The bottom line is that data breaches are serious and laws against them are growing in number and the severity of the consequences for violating them. Organizations must protect access to the data sources that contain this information and the systems that process and create this data. There will definitely be more regulations and greater controls as a result of an increased level of corporate oversight over the next several years.

About PistolStar's PortalGuard

PistolStar's PortalGuard is an authentication solution that allows robust authentication management in Lotus Domino, IBM WebSphere Portal and Microsoft SharePoint environments. It satisfies organizations' key business drivers for authentication management, including usability, security, compliance and auditing. Among the many features of PortalGuard are:

- **Strong authentication**
  PortalGuard provides much stronger authentication than traditional, simple usernames and passwords. It does this by optionally requiring not only a username and password to gain access to an application or resource, but also the answer to a challenge question,

thereby significantly improving security and minimizing the ability for hackers to guess passwords or use dictionary-style attacks.

- **Highly configurable and secure self-service password recovery/reset**
  A feature of PortalGuard that IT and help desk will particularly appreciate is the ability for users to securely recover and reset their own passwords using multiple challenge question-and-response functionality. This capability permits faster recovery of passwords and significantly reduces help-desk costs.

- **One-time password (OTP)**
  This functionality offers a strong two-factor approach to authentication, which avoids the typical issues associated with static passwords. PortalGuard creates a password valid for one session that adds a layer of security to any access point. The OTP is sent to the user's mobile phone instead of requiring a proprietary hardware-based token.

- **Verbal authentication**
  PortalGuard allows the Help Desk to easily prove the identities of users calling in. This is done with the use of a highly configurable challenge question and answer functionality. This functionality uses a different set of challenge questions and answers, than would be used to allow the user to reset their own Active Directory password. This is a way to minimize the associated risk of the Help Desk.

- **Powerful passwords and authentication security features**
  PortalGuard also offers a number of important features for maintaining the security of access to corporate resources, including the ability to:

  - Set intervals between password changes
  - Define the grace period during which expired password notifications are displayed
  - Define rules for the strength of passwords
  - Define strike-out limits as well as intervals for automatic unlocks
  - Limit the number of multiple, concurrent logon sessions
  - Lock out inactive users after a specified number of days
  - Place limits on password reuse

  For added flexibility, all the rules above can be configured for specific individuals, groups or roles in an organization.

- **Auditing and logging of user activity**
  PortalGuard also provides robust and granular auditing and logging of user activity, including the last login date and time for each user, if invalid usernames are provided during authentication, when individual users change or perform self-service recovery for their passwords, and when they use weak passwords.

BENEFITS OF PORTALGUARD

PortalGuard offers benefits to a number of different constituencies with the organization. For example:

- Users can maintain high levels of productivity through their ability to self-manage their own passwords and perform their own password resets instead of needing help-desk staff for assistance. This is especially advantageous when the help desk is closed or overburdened with other tasks or when users are remote.

- IT and help desk staff members benefit by being relieved of the burden to help users recover or reset their passwords. They also benefit by reducing the number of multiple password stores and user accounts, allowing them to synchronize password policies across the enterprise much more easily than if multiple passwords are required for each user.

- The entire organization benefits through dramatically improved security. For example, a password stolen by a hacker will not compromise the security of a resource, since more than one factor is needed to gain access to it. Further, easy-to-guess passwords are not an option, IT can limit the opportunity for hackers to guess passwords, IT can restrict attempts to access resources during off-hours, and the use of credentials that are already in use or that are inactive is prevented, all of which dramatically enhances the security of access.

APPLICABLE ACROSS MULTIPLE INDUSTRIES

While certain industries and organizations maintain more sensitive information than others, virtually any organization will have sensitive applications and content sources for which it must maintain strict access control. As a result, PortalGuard is applicable in any industry, including banking, financial services, government, military and other industries that deal with highly sensitive data. Further, as government oversight and control increases over the next few years – such as through the application of stricter, more expansive and more punishing HIPAA requirements, to name but one example – almost every organization will have sensitive data to which it must carefully control access.

Summary

Web-focused portals are becoming increasingly popular as a method to give employees, business partners, consultants and other access to a growing variety of databases, backend applications and other tools. Further, social networking capabilities are increasingly being integrated into corporate portals as a means of allowing better and faster collaboration capabilities.

One of the most important issues facing organizations that are increasingly reliant on portals is maintaining their security of access. A failure to maintain adequate security can have a variety of negative consequences, including violation of the law, the requirement to report data breaches to affected parties, lost business, lost reputation and other problems.

What organizations need is the ability to deploy access to corporate resources through portals and maintain the security of this access from internal and external threats. Further, IT needs the ability to bolster the strength of authentication for access to portals, make access

as easy as possible, and push policy compliance management and enforcement to line-of-business decision makers.

PortalGuard from PistolStar is designed to offer robust authentication management in Domino, WebSphere Portal and SharePoint environments while also offering end user self-service and other capabilities for security management.