Portal Authentication: A Balancing Act Between Security Usability and Compliance

An Osterman Research White Paper
Published February 2014

SPONSORED BY

PortalGuard
EXECUTIVE SUMMARY

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 Microsoft SharePoint and other solutions. Importantly, SharePoint is among the leaders in Gartner’s 2013 Magic Quadrant for horizontal portals.

Maintaining robust security has become essential, as evidenced by the large and growing number of major data breaches, the most recent of which have been major incursions affecting Target, Neiman-Marcus, Michaels Stores, the internal Web site of the US Federal Reserve, LivingSocial and many other organizations that retain and manage customer and other sensitive data. These breaches underscore the critical importance of a multi-layered security approach that includes continuing user education, updates to operating systems and firmware, robust anti-virus and anti-malware defenses, real-time alerts, monitoring and other measures – in essence, going well beyond passwords as the bare minimum for security.

However, security is increasingly becoming a key legal issue. 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 examples in the United States:

- The Health Insurance Portability and Accountability Act (HIPAA) and the more recent changes brought about by the Health Information Technology for Economic and Clinical Health (HITECH) Act.
- The Gramm-Leach-Bliley Act
- The Payment Card Industry Data Security Standard
- Various state data breach notification laws

In addition, there are numerous laws in other nations focused on data security, such as the following:

- Personal Data Ordinance Code of Practice on Consumer Credit Data (Hong Kong)
- Information Technology Act 2000 and Amendment Act 2006 (India)
- The Personal Information Protection and Electronic Documents Act (Canada)
- Personal Data Protection Act: Telecommunications Act (Spain)
- Electronic Communications Act (Sweden)
- Postal and Electronic Communications Code (France)
- Data Protection Code (Italy)

A failure to comply with these requirements can be quite costly, totaling in the millions of dollars in some cases. For example, the Ponemon Institute determined that the cost of a data breach in 2012 was anywhere from US$42 per record compromised in India to as much as US$199 per record in Germany.

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 simply will 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.
ORGANIZATIONS MUST SATISFY THE COMPETING INTERESTS OF HIGH SECURITY AND EASE-OF-ACCESS

What organizations need, therefore, is the best of both worlds: 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 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 focuses on 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.

THE ENTERPRISE IS CHANGING

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 16.8 different applications or systems to do their work on a daily basis. A survey that we conducted in 2009 found that a mean of 12.3 password-protected systems were accessed on a typical day.

The problems that this number of access credentials creates include the fact that most users report that they have too many usernames and passwords 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. In the Osterman Research survey cited above, we found that there are numerous problems with current authentication methods:

- 83% of users employ the same username/password for more than one application or system they must access
- 75% of users forget their username/password at least once each year and must contact IT or an automated system to have it reset. In fact, 33% do so more than once per quarter.

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.

The bottom line is that users and organizations are dissatisfied with current access methods: 82% of users in our survey feel that access methods need improvement.
IT'S A CLICHÉ, BUT IT'S TRUE
Keeping up with “the speed of business” may be a bit of a cliché, but it is a critical necessity, particularly in a fluctuating economy. 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 organizations like IBM, Boeing and the US federal government do not have a fixed location from which to work because of a growing emphasis on telework initiatives, 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.

On the other hand, becoming more mobile and flexible is not without its consequences. 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 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 or an automated system.

• 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 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.

SECURITY CHALLENGES ARE BECOMING MORE DIFFICULT TO MEET

PREVENTING UNAUTHORIZED PARTIES FROM GAINING ACCESS TO YOUR SYSTEMS
It 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 critical 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 a November 2013 Osterman Research survey, we found that decision makers are concerned or seriously concerned about a variety of issues:
• 58% are concerned that malware that could be introduced through employee Web surfing.

• 56% are concerned about malware introduced from employees’ personal Webmail accounts.

• 53% are concerned about phishing attacks.

• 36% are concerned about breaches of sensitive internal data.

• 35% are concerned about breaches of sensitive customer data

• 32% are concerned about direct hacker attacks

In short, preventing 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, malware and other external Web-borne threats.

However, these activities 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, Osterman Research has found that most 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 IS ESSENTIAL

Decision makers are concerned about preventing incidents of password fraud and data theft, and so must reduce the risk of exposure through external attack. However, hackers exist both internally and externally and are becoming more sophisticated, clever and better funded over time. Cybercriminals 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 must do a variety of things:

• Meet the data security standards that have been established by government, industry and corporate mandates.

• Prevent data breaches and mitigate against the rising level of risk in the enterprise because of the increasing number and variety of vulnerabilities.

• 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.

• Finally, 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.
THE NEED FOR IMPROVED AUTHENTICATION

AUTHENTICATION IS REQUIRED 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 often forget passwords or they lose passwords and must contact the help desk to retrieve them. This happens a mean of 6.8 times per year.
- They have too many passwords to remember. As noted earlier, the typical user must access a mean of 16.8 different applications or systems on a daily basis.
- Help desk costs are driven up by the need to reset forgotten passwords. The average cost of a help desk call is $6 to $8 according to one study.

THE REQUIREMENT 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.
MANAGING THE TENSION BETWEEN SECURE ACCESS AND EASE OF USE

WHAT THE AUTHENTICATION SOLUTION MUST PROVIDE
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 the number of help desk calls and the overall cost of providing help desk services.

- 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
So that the organization can 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 should include:

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

- 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.

- 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 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 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 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 – as noted, 83% of users will sometimes employ the same username and password for multiple systems. Doing so creates an enormous security vulnerability, since a hacker or other unauthorized user that gains access to one set of login credentials will then have access to a number of other systems.
• Protection of self-service password reset functionality with two-factor authentication to further verify the user before a password change can be completed.

BYOD MEANS USERS HAVE MORE CHOICES
The Bring Your Own Device (BYOD) phenomenon that has taken significant hold in most organizations further complicates authentication management because users simply have more devices and applications available to access corporate applications, systems and data resources. Similarly, the Bring Your Own Credentials (BYOC) problem that is part and parcel with BYOD also makes things more tricky for IT and business decision makers because, as with devices and applications, users have more control over authentication practices than perhaps they should.

BYOD and BYOC can result in a reduced level of governance that comes from IT’s loss of control over personally owned devices and how users access corporate systems, the data that is sent from and stored on these devices, and the potential loss of intellectual property that can result from the physical loss of a device that cannot be wiped. BYOD and BYOC clearly complicate the issue of authentication management, but it is an issue that decision makers must address.

MONITORING OF USER LOGIN BEHAVIOR AND ACCESS CONTROL
IT should also have the ability to monitor users’ login behavior as part of a robust access control capability. This should include things like:

• Tracking each user’s last successful login and login attempt(s).
• Determining the time they last logged into the system or attempted to do so.
• Tracking any password changes that users might have made.
• Monitoring 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
US 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:

• 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.

• HITECH
Although HIPAA was enacted in 1996, it was considered by many to be a poorly enforced requirement. However, the Health Information Technology for Economic and Clinical Health (HITECH) Act, followed by the HIPAA Omnibus Rule that became effective as of March 2013, significantly increased the scope of HIPAA and the consequences for its violation. The US Department of Health and Human Services (HHS) has raised the requirements for protection of confidential and sensitive information, increased the number of organizations that are subject to HIPAA, and it can be expected to levy fines and penalties with greater frequency than it has in the past. The Omnibus rule now allows HHS to impose
fines ranging from $100 for a "Did Not Know" breach of Protected Health Information to $50,000 for a single, uncorrected and willful violation. However, fines can reach $1.5 million per year or more.

- **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.

- **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.

**REGULATIONS IN OTHER COUNTRIES**

- **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.

- **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.

- **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.

- **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.

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

- **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”.

- **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.

- **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).

There are also a growing number of US state laws that address data breaches – as of late January 2014, 46 of the 50 US states – as well as the District of Columbia, Puerto Rico, the US Virgin Islands and Guam – have enacted data breach notification laws.

**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.

**ABOUT PORTALGUARD**

PistolStar, Inc. makers of PortalGuard is offering an affordable turnkey user authentication solution-set designed for any company providing external customer-facing web applications to their employees, contractors, suppliers, and vendors. PortalGuard is an ideal on premise turnkey solution-set providing a balance between security and usability. Its five layer integrated design includes eight flexible two-factor methods, four single sign-on methods, centralized self-service password reset and unlock, password synchronization, and contextual authentication to create transparent barriers that block unauthorized access by validating the user’s location, device, IP, and Wi-Fi encryption access.
PortalGuard’s SAML Identity Provider (IdP) acts as a SAML-based portal that uses a single set of credentials for the portal login itself and then grants access to your web-based applications whether cloud-based, private, on-premise, or behind the firewall. For example Outlook Web App (OWA), BlackBoard, Google Apps, Concur, and Salesforce are all easily integrated using the SAML protocol.

PortalGuard’s PassiveKey provides the security of two-factor authentication by leveraging the end-users device, which abolishes the need for hardware tokens or using your cell phone. This approach minimizes negatively impacting end-users while addressing the problem of network attacks by hackers worldwide.
Portal Authentication: A Balancing Act Between Security, Usability & Compliance

© 2014 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader’s compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, “Laws”)) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

i http://www.gartner.com/technology/reprints.do?id=1-1KH0XVB&ct=130917&st=sg&submissionGuid=41e7b22f-a66d-4cc3-a136-2dca31b5d6c0
iii Source: Osterman Research survey, June 2013
v Source: Osterman Research survey results, June 2013
vi Source: UK Service Desk Benchmarking Report 2011, Service Desk Institute
vii Source: National Conference of State Legislatures