

CUSTOMER NEEDS AND STRATEGIES

Enterprise IT Shops Attack Single Sign-On and Authentication Challenges with Secure Appliance Platform from Imprivata

Sally Hudson

IDC OPINION

Recent trends show that IT security professionals are increasingly adopting appliance-based solutions as a method of protecting the enterprise. There are few pure-play appliance offerings in the identity and access management (IAM) market space. Imprivata is one of the exceptions. In this document, IDC profiles international customer experiences with the Imprivata OneSign appliance, as presented by the customers at a recent Imprivata customer forum held in the greater Boston area. IDC research shows the following:

- Customers are looking for security-based solutions for regulatory and internal policy compliance.
 - If given a choice, customers prefer an integrated approach as opposed to implementing a series of point products.
 - There is a movement away from software and toward appliances in the security space.
-

IN THIS STUDY

In this study, IDC examines the deployment of appliance technology in an identity and access management (IAM) environment through the experiences related by IT customers at a recent Imprivata user and partner event.

SITUATION OVERVIEW

The following customer profiles are extrapolated from presentations and interviews at the Imprivata Partner Conference, October 17, in Waltham, Massachusetts. Almost 100% of Imprivata sales are channel driven. There were a variety of industries represented, including healthcare, finance, manufacturing, and the public sector. The audience was able to learn from a worldwide perspective because customer presentations included representatives from the United Kingdom, Italy, Belgium, and the United States.

Imprivata, based in Lexington, Massachusetts, is a privately held company that manufactures and sells the OneSign platform, a purpose-built appliance providing several common IAM and security components in a single, easy-to-use deployment scenario. OneSign includes the following:

- ☒ Single-management UI
- ☒ Intuitive user policy implementation and management
- ☒ Support and integration for strong authentication devices (e.g., RSA SecurID, VASCO DigiPass), finger biometrics, smart cards, proximity cards, and building access cards
- ☒ Comprehensive user access monitoring, logging, and reporting
- ☒ Built-in failover and redundancy

The OneSign appliance includes three modules that can be licensed as needed with a simple upgrade key:

- ☒ **OneSign Authentication Management** replaces Windows and remote access VPN passwords with a broad range of strong authentication options, whether accessed through the network locally, via remote VPN, or while working offline.
- ☒ **OneSign Single Sign-On** enables SSO access to enterprise applications — legacy, client/server, Windows, Java, and Web — without requiring any custom scripting or modifications to directories.
- ☒ **OneSign Physical/Logical** integrates network and building access systems to provide a single consolidated user identity. This allows organizations to map identities between physical access systems and IT directories to enable one converged policy for allowing or denying network access based on a user's physical location, organizational role, and/or employee status.

The Imprivata appliance provides integrated and centralized user access monitoring and reporting capabilities in order to better demonstrate regulatory compliance. The following excerpts from customer presentations demonstrate how the Imprivata technology is applied today.

Customer Experience with Appliance-Driven ESSO

IT organizations represented at this year's event included BJC Healthcare, Bridgestone Europe, Coface, ING Bank Wholesale Banking, United Kingdom, and Tayside Royal Fire and Rescue.

BJC Healthcare

BJC Healthcare, a nonprofit healthcare organization, based in St. Louis, Missouri, manages 13 hospitals in the Midwest, 3,500+ beds, and over 70 other healthcare locations. BJC has more than 25,000 employees. The centralized IT group employs 550 people. Patrick Heisinger, senior technical specialist at BJC, addressed the conference about the organization's primary drivers for SSO technology — repeated physician complaints concerning the number of passwords they were forced to remember and time-consuming log-in requirements.

According to Heisinger, Imprivata OneSign was selected after a lengthy RFI based on several criteria. This included previous experience in healthcare settings, support for shared workstations, and support for a wide variety of authentication technologies. (BJC uses Windows Userid/Password, RSA SecurID, and Xyloc RFID/fingerprint technology.) One of the most important features leading to selection of OneSign was that external consulting and services were not required to profile new applications to the system. The unique nature of many healthcare applications presents a problem for many external solutions providers, but the BJC IT team was able to easily profile applications for the Imprivata appliance. Not all of the BJC's 550 applications will be SSO enabled, and Heisinger states that there will be "no true SSO in our lifetime." But, BJC has SSO enabled all critical applications and is very happy with the reduced sign-on and integration capabilities provided by Imprivata. The system provides the benefits that BJC has hoped for. Nurses and physicians are happy that they don't have to remember passwords. According to Heisinger, "Imprivata has proven to work."

Bridgestone Europe

Bridgestone Europe, based in Brussels, is a division of the global tire manufacturer. The European division has 11,743 employees, 17 fully owned sales subsidiaries, 6 factories, and a large technical center that oversees many diverse technologies and vendors, including SAP, Microsoft, Citrix, Siebel, Navision, Cognos, Vignette, and others. The organization manages 5,500 PCs. According to Paul De Vroede, manager of office automation and telecommunications at Bridgestone Europe, it was the company's employee portal that initially drove the IAM investment. In 2006, it was apparent that the company needed an SSO solution capable of accessing the primary applications portfolio. After conducting an extensive proof of concept with three vendors, Bridgestone Europe selected Imprivata OneSign.

The selection matrix was composed of 28 weighted criteria, which included check boxes for integration, support, maintenance, ease of use, stability of product, vendor reputation, and price. OneSign was selected and implemented initially for SSO only. De Vroede noted that it is nonintrusive to end users and no training was necessary. Since December 2006, the company has purchased 5,000 OneSign licenses. In January 2007, a rollout was completed in headquarters through group policy with a pure focus on SSO. De Vroede reports that there were no issues and that the rollout received a great response. It has also been determined at Bridgestone Europe that password-only protection is inadequate. Based on its previous success with the Imprivata product, the company evaluated OneSign as a component of a strong authentication strategy. Based upon OneSign's solid integration with third-party authentication devices, the tire manufacturer rolled out 95 UPEK fingerprint readers to European subgroup companies and has purchased 3,000 additional fingerprint readers and 2,000 Vasco One Time Password tokens. Bridgestone is planning to upgrade to OneSign 4.0 in 2Q08 in order to take advantage of the new distributed architecture, delegated administration, and other features. According to De Vroede, Imprivata provided the company with the "360 degree solution needed" to solve SSO integration issues and password problems and provide a platform for strong authentication.

Coface

Coface, founded in 1946, is a subsidiary of Natixis, a key player in the banking sector. The company provides worldwide expertise in trade receivables. It is directly present in 64 countries, and through its partner, Credit Alliance, it is in 93 countries. The company has more than 6,000 employees worldwide and 105,000 clients.

Coface in Italy has 17,000 clients and 400 employees. It is currently ranked as number 1 in the bond market and number 2 in the credit insurance market. Gianni Fasciotti, deputy director of information systems at Coface Italy, manages a complex environment of HP-UX, Linux, and WIN2003 servers, numerous applications (both client server and Web based), and 40 remote sites. There is also an Oracle database and application server centralized in Milan and Paris. Until recently, users were required to log into each application with a username and password. This presented problems with the authentication phase, and Coface Italy determined that it must rearchitect its access mechanism to increase security, simplify the log-on process for users, and improve the current access process to the correct information with authorization. Users could not cope with more than one password, nor could they cope with multiple password change requirements for security purposes. This led Fasciotti and his team to look at an SSO solution. Using the OneSign appliance, the company adopted a solution that spans 16 applications and 350 users. It relies on an authentication strategy with log-in and password or biometric fingerprint. The company uses Windows AD as primary authentication in this setup.

Fasciotti lists many benefits realized by this implementation. First, users are happier because they need to remember only one password for log-in. The application password is safer because it is now more complex and managed by the SSO. "The appliance-based approach makes the maintenance phase much simpler," Fasciotti said, "and the product provides good integration with Windows AD and easy

integration with RADIUS for the company's VPN." The next step will be to add more applications and to extend the fingerprint technology to the remote sites.

ING Bank Wholesale Banking, United Kingdom

ING Bank Wholesale Banking, United Kingdom, is part of the ING Dutch-headquartered financial services company. It is ranked thirteenth by revenue in the Fortune 500 for 2006 and currently has 115,000 employees worldwide. Damian Atkinson is the CIO for the United Kingdom's wholesale banking division. Noting that there is a "constant wind of change blowing through our industry," Atkinson added that SOX compliance has emerged as a major driver for analyzing, testing, and understanding controls around systems and data. He also observed that the internal and external audit bar is going ever higher as new threats emerge in financial services and banking communities.

Passwords have proved notoriously inefficient because users tend to have trouble remembering anything complex enough to be truly useful. "Going forward, simple, secure solutions are key," said Atkinson, "and ease of deployment and maintenance are critical to the success factor of any solution." An important criteria at ING, United Kingdom division, is that the solutions must work, with minimal customization, for all technologies. The financial institution decided that biometric fingerprint technologies would provide several benefits, including the elimination of password sharing and weak passwords, nonrepudiation claims, and users writing down passwords. Additionally, it was determined that the biometric authentication approach would significantly reduce help desk costs.

The SSO solution from Imprivata has helped ING discover more about the unique ways applications deliver their authentication mechanisms. The product keeps track of authentication failures and recognizes how applications indicate user lockout. It also recognizes (where possible) privilege-level modification and additional group membership. All this leads to better security monitoring, said Atkinson, which will contribute to meeting auditing requirements. ING's philosophy is not to reengineer applications but to surround them with security, compliance, monitoring, and auditing capabilities. Atkinson's advice to others is, "Keep it simple. Don't over-engineer a solution, and avoid customization wherever possible."

Tayside Fire and Rescue

Tayside Fire and Rescue provides 24 x 7 services to a population of almost 400,000 in the Tayside region of Scotland. There are approximately 800 staff members at Tayside Fire and Rescue, wholetime, retained, and volunteer staff. Having access to the correct information is truly life critical, as opposed to mission critical, in this business. Gary Bellfield, Information and Communications Manager (ICT) for Tayside Fire and Resuce is responsible for providing IT services to the roughly 800 end users needing access to systems.

The department supports a wide range of systems, from traditional green screen applications to Web-based systems, and needed a flexible SSO solution. It was determined that given the critical nature of the user base, complex password policies were a core requirement, so a simple and direct solution was needed. The company uses Citrix Presentation Server with Windows embedded thin clients, with the

requisite high-availability technology required in this field. With an IT staff of three people, there was lack of revenue for IT, and "big vendors just weren't interested" as the company moved toward its SSO strategy, said Bellfield. He and his staff evaluated the Imprivata appliance in June 2005 and used it to profile six of their key applications. Tayside Fire and Rescue also wanted to deploy biometrics to all access points and integrate their existing token system.

Since the initial rollout, the user password situation has improved considerably, and access is no longer an issue. Users can now reset their own passwords, a process that used to take the help desk up to two weeks to resolve. In the future, Bellfield and his staff have a full plate. The Fire and Rescue unit will be evaluating token integration (they are even looking at waterproof tokens), integrating IT access with building access control, more transparent VPN integration, and possible use of native UPEK devices. "All of this ease of access breeds confident users," said Bellfield, who has learned how to manage in an environment where needs are many and resources are few.

Other attendees who contributed content for this report via interviews and commentary include the following:

- Christopher Paidhrin, Security Compliance Officer, HIPAA & IT Security Officer for ACS/Southwest Medical Center
- Mary Pat Weiss, Group Manager, BCJ Healthcare

FUTURE OUTLOOK

The worldwide IAM market realized almost \$3 billion in revenue in 2006. We expect this market to increase at an overall 10.7% compound annual growth rate (CAGR) through 2011 based on the following assumptions:

- Regulatory compliance is a strong growth factor in this market, both horizontally and vertically, on a worldwide basis.
- Demand for consumer authentication will grow, driven by both increasing regulations and an increase in reported ID thefts and compromised identities.
- The need for enterprise single sign-on (ESSO) and Web single sign-on (WSSO) will steadily increase, driven by needs for secure access with strong systems management and administration capabilities.
- Provisioning and deprovisioning solutions will see gains beyond the United States and Western Europe, reaching into the Japanese and Asia/Pacific markets over the next several years.
- There will be more partnerships among the major players and other technology and service providers to provide customers with total end-to-end solutions.

In the future, IDC believes the trend will be for new security software to be sold and delivered as a service and/or a security appliance rather than purchased as shrink-wrapped products.

Finally, the unification of physical and logical security access via a single secure, seamless set of solutions has become the paramount goal of many IAM and other security vendors. IDC believes that significant progress is being made in this area and expects a continued uptake and evolution of this technology over the next several years.

ESSENTIAL GUIDANCE

IDC believes that security appliances will continue to grow in popularity as an easy way to distribute software security solutions to customers. Appliances will continue to be popular with customers and distributors. There will be a replacement cycle associated with this market. Software vendors that can partner with or license to appliance vendors will have an advantage in the market.

It is becoming apparent that there is a shortage of IT security personnel. With a limited supply of trained security personnel, easier solutions are required. This need will drive the purchases of security solutions that are easy to use, reduce the need for trained security personnel, and add value to other IT solutions. We believe these needs are among those addressed by the Imprivata solution as outlined by the customer experiences in this document.

LEARN MORE

Related Research

- ☒ *Worldwide Identity and Access Management 2007–2011 Forecast with Submarket Segments* (IDC #208060, August 2007)
- ☒ *Worldwide Identity and Access Management 2007–2011 Forecast and 2006 Vendor Shares* (IDC #207609, July 2007)
- ☒ *IDC's Software Taxonomy, 2007* (IDC #205437, February 2007)
- ☒ *Worldwide IT Security Software, Hardware, and Services 2006–2010 Forecast: The Big Picture* (IDC #204736, December 2006)
- ☒ *Worldwide Security Products and Services 2007 Top 10 Predictions* (IDC #204678, December 2006)

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2007 IDC. Reproduction is forbidden unless authorized. All rights reserved.