Sector Insight

Aberdeen Group
A Harte-Hanks Company

November 2011

Stronger Authentication for Small and Mid-Sized Business

Small and Mid-Sized Businesses (SMBs) authenticate their end-users primarily with passwords, in spite of the fact that passwords are *less secure*, *inconvenient*, and in fact *more expensive* than stronger forms of authentication. Compared to larger organizations, SMBs on average spent 38% less per user on identities and authentication – but this was a false economy, as they also incurred an average of 87% more cost per user as a result of security-related incidents. Aberdeen's analysis of drivers, inhibitors and technology adoption trends among SMBs indicates that stronger authentication solutions which are especially well-designed to address the needs of SMBs include **heuristic / adaptive / risk-based authentication**, **out-of-band / phone-based authentication** and verification, and multi-purpose **smart cards**.

Business Context: Recap – The Case Against Passwords

A number of events in 2011 combined to lead many enterprises to proactively re-evaluate their strategies for authenticating end-users, in particular with methods that are stronger than traditional passwords. As Aberdeen noted in *The Case Against Passwords: Re-evaluating Stronger User Authentication* (August 2011), this is a very good idea – because the research confirms that traditional usernames and passwords are *less secure*, *inconvenient*, and in fact *more expensive* in comparison to stronger forms of end-user authentication. Aberdeen's analysis of responses from 32 organizations relying exclusively on traditional usernames and passwords (the "Passwords" group) and 69 organizations using one or more forms of stronger user authentication (the "Stronger Authentication" group) provided several useful insights with respect to security, convenience and total cost, which are recapped here.

Passwords are Less Secure

Aberdeen asked respondents about the number of incidents – including *unauthorized access* to enterprise resources, *audit deficiencies*, and *data loss or data exposure* – their organization experienced in the last 12 months related to identities and authentication. On average, the Stronger Authentication group experienced **about 5% fewer incidents** than the Passwords group. This may seem modest, but assuming an average total cost per incident of just $640K – a figure which itself is modest in comparison to several widely circulated industry figures – this actually works out to an annual savings of **between $4 and $5 per enterprise end-user**.

Sector Insight

Aberdeen's Sector Insights provide strategic perspective and analysis of primary research results by industry, market segment, or geography.

Basis for the Research Findings

In 1Q2011, Aberdeen examined the use, the experiences and the intentions of more than 160 enterprises from a diverse set of industries with respect to their approach to managing identities, authentication and access. Responding enterprises had the following demographics:

Geography

√ Americas: 56%

√ Europe / Middle East / Africa: 30%

√ Asia / Pacific: 14%

Company size (annual revenue)

√ >$1 billion: 32%

√ $50M to $1 billion: 36%

√ < $50 million: 32%

Company size (users)

√ < 2,500: 55%

√ 2,500 - 10,000: 18%

√ > 10,000: 27%

For additional information, see Aberdeen's benchmark study on *Managing Identities and Access* (March 2011).

Passwords are Inconvenient

A majority of all respondents have taken steps to strengthen the security of traditional passwords, for example:

- Requirements for length (87%), complexity (80%), frequency of change (85%), and restrictions on re-use (84%)
- Exclusion of standard dictionary terms (shockingly, only 53%)

All of these steps enhance the security of passwords by making them more difficult to guess, but at the same time they make passwords more cumbersome for end-users to use and remember. The sheer number of passwords amplifies the problem. Natural coping mechanisms include writing them down (which increases risk) and relying on calls to the help desk (which increases cost).

Ironically, the Stronger Authentication group proved on average to be **about 25% more efficient** than the Passwords group across virtually all aspects of the identity management lifecycle – from initial provisioning of identities and access; to resets and emergency access; to eventual suspension, revocation and de-provisioning – which translates directly to greater convenience for all enterprise end-users. The takeaway is that the Stronger Authentication group applied the business processes and discipline necessary for successful implementations of their stronger authentication solutions to their lifecycle management processes for traditional passwords as well.

Passwords are Actually More Expensive

Aberdeen asked respondents to approximate the total annual cost of managing identities and authentication – including all associated people, process and technology, hardware, software, services, training and support. On average, the total annual cost per enterprise end-user was **$12.60** for the Stronger Authentication group, an **annual advantage of about 8%** compared to the finding of **$13.70** for the Passwords group. Again, this represents the average annual cost across *all* enterprise end-users, not just those that are using stronger authentication.

Taken together, Aberdeen's research showed that the Stronger Authentication group reported both greater *efficiency* (lower total annual cost per user) and greater *effectiveness* (fewer annual security-related incidents per user) – for **a combined advantage of between $5 and $6 per enterprise end-user per year** for enterprises deploying stronger authentication.

Aberdeen's Research Findings: Current End-User Authentication Practices in Small and Mid-Size Business

Aberdeen analyzed responses from 81 Small and Mid-sized Businesses (SMBs, defined as fewer than 2,500 users) to better understand current practices in end-user authentication, current drivers and inhibitors for

Sector Definitions

For purposes of this analysis:

√ **Small and Mid-Sized Businesses (SMBs)** are defined as fewer than 2,500 end-users

√ **Large** enterprises are defined as 2,500 end-users or more current investments, and the effectiveness and efficiency of existing implementations. Responses from 66 Large enterprises (defined as 2,500 end-users or more) were also analyzed to provide a point of comparison.

How are SMBs Currently Authenticating?

Small and Mid-Size Businesses are currently authenticating primarily with passwords, but responses for planned use in the next 12 months and current evaluations indicate very high market interest in stronger forms of end-user authentication (Figure 1). Relative to current use, the strongest levels of market interest are seen to be in *heuristic / adaptive authentication* solutions, *smart cards*, and *out-of-band, phone-based* solutions:

- **Heuristic / adaptive authentication** solutions – also referred to as **risk-based authentication** – operate transparently to end-users, by monitoring and analyzing online activities in real-time to generate a risk-based assessment of identity assurance. Correlation of information about devices, end-user patterns of behavior, and data feeds from external fraud monitoring services are used to determine if stronger levels of authentication than username and password are warranted for a given transaction. Widely used and proven for several years in large-scale, transaction-oriented consumer environments, these technologies are more recently being packaged by leading solution providers for use in traditional enterprise authentication scenarios.
- **Smart cards** – typically used with **digital certificates** – are multi-purpose in nature, supporting a range of enterprise use cases including *authentication* (e.g., to the endpoint / desktop, for network access, for remote access, for privileged administrative accounts), *signatures* (e.g., signed email), *encryption* of sensitive data (e.g., encrypted email, secure file transfer), *building entry* (e.g., integration with physical access control systems), and *photo identification* and *corporate badging*. Leading solution providers have been actively addressing historical inhibitors to broader investments in smart cards by introducing streamlined issuance and credential management solutions; for additional detail, see Aberdeen's Analyst Insight on *The Case for Smart Cards* (July 2011).
- **Out-of-band, phone-based** solutions are typified by end-users entering their traditional username and password on a web site, then receiving and responding to a phone call or text message (i.e., in a different band, or channel) as an integral part of the authentication process. Similarly, out-of-band solutions can be used to ask the end-user to verify the legitimacy of an online transaction. In its supplement (June 2011) to its earlier guidance on *Authentication in an Internet Banking Environment* (October 2005), the agencies of the **Federal Financial Institutions Examination Council (FFIEC)** noted that out-of-band solutions can be used not only to provide higher assurance for end-user authentication and

Definitions

In the United States, the **Federal Financial Institutions Examination Council (FFIEC)** consists of the following federal agencies:

√ The Board of Governors of the Federal Reserve System

√ Federal Deposit Insurance Corporation

√ National Credit Union Administration

√ Office of the Comptroller of the Currency

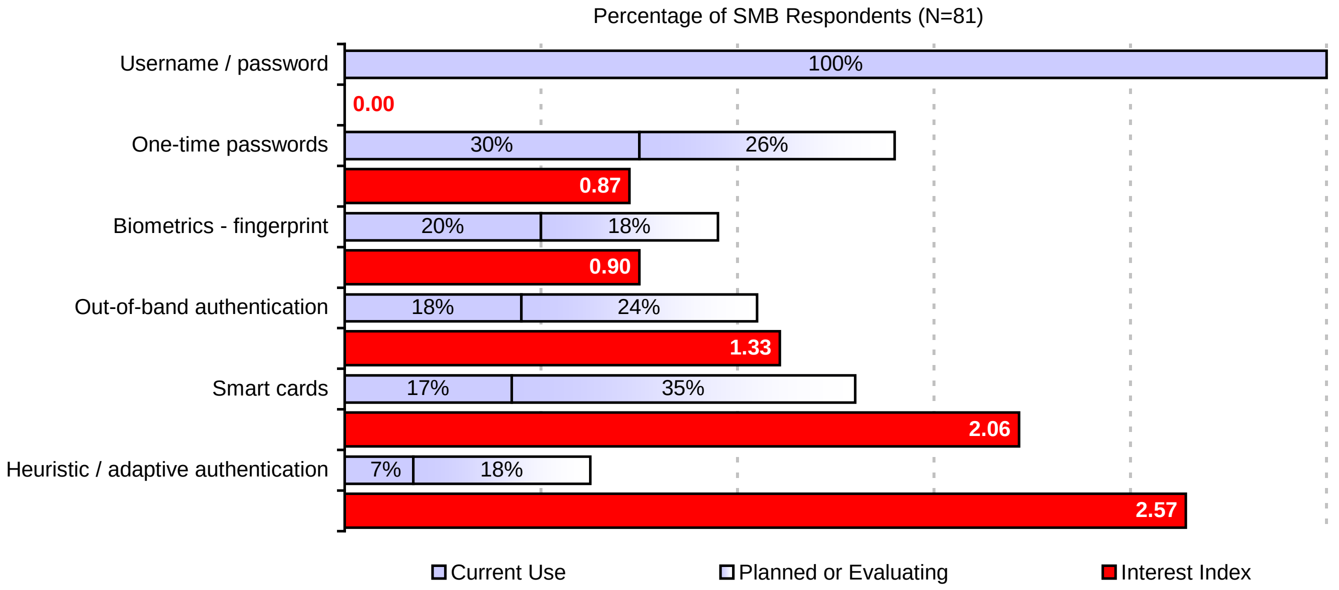
√ Office of Thrift Supervision

Man-in-the-middle / man-in-the-browser attacks refer to scenarios in which the attacker hijacks the online session by transparently inserting himself between the end-user and the financial institution.

Electronic signatures are designed to increase transaction security and protect end-customers against Man-in-the-Middle attacks, by incorporating unique factors such as transaction amount and destination, source account information, time values and counter values to allow the bank to verify that a transaction was initiated by a legitimate end-user. If the transaction can not be validated, the e-signature will be rendered useless, the bank can flag the transaction as suspected fraud, and the end-user can have confidence that the transaction was not intercepted or altered in transit.

verification of transactions, but also as an effective protection against *man-in-the-middle* attacks.

Figure 1: SMBs and End-User Authentication – Current Use, Planned / Evaluating, Interest Index

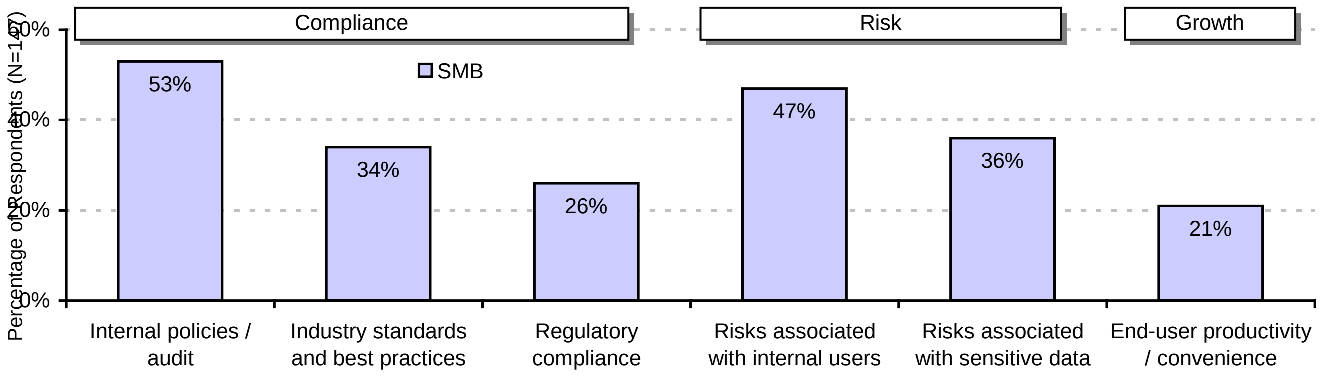


Note: multiple responses accepted; does not add to 100%
Interest Index is calculated as (Planned or Evaluating) / (Current Use), i.e., a measure of market interest relative to current use
Source: Aberdeen Group, November 2011

What Pressures are Driving Current SMB Investments?

Current SMB investments in end-user identities and authentication are more strongly driven by **internal policies** than by external requirements for **compliance** (Figure 2). SMBs also indicate that their investments are strongly driven by **risk** (particularly risks associated with internal users, and sensitive data), but less strongly by **end-user productivity** or convenience.

Figure 2: Leading Drivers of Current SMB Investment in End-User Identities and Authentication

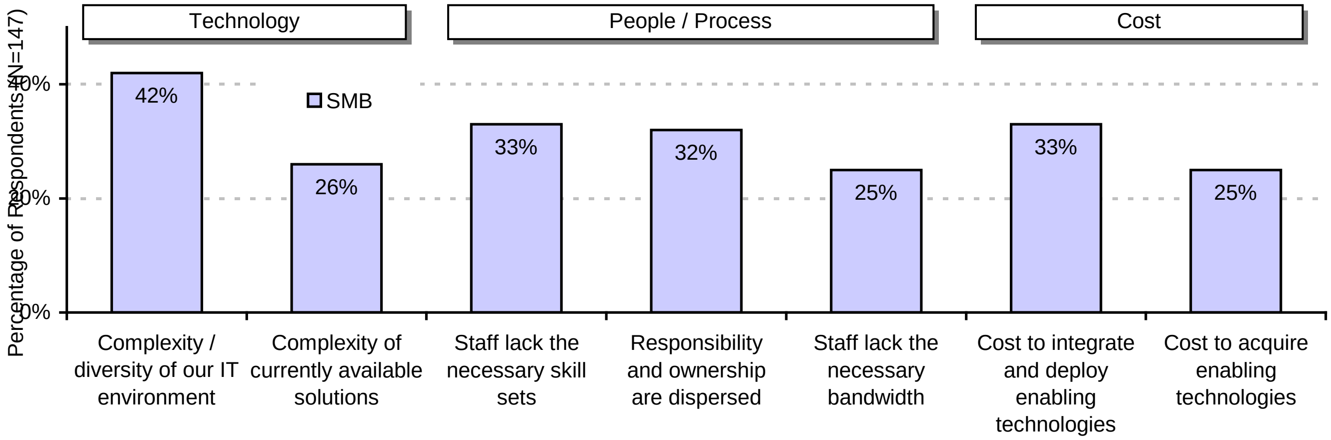


Note: multiple responses accepted; does not add to 100%. Source: Aberdeen Group, November 2011

What Factors are Inhibiting Current SMB Investments?

Perceived **complexity** – of the SMB's IT environment, and of currently available stronger authentication solutions – combines with internal staff lacking necessary **skill sets** and **bandwidth** as the leading inhibitors of current SMB investments in end-user identities and authentication (Figure 3). These factors align logically with **cost to integrate and deploy** being viewed as an even greater inhibitor than initial **cost to acquire**. Taken together, the current SMB environment favors stronger authentication solutions that are easy to integrate, use and manage.

Figure 3: Leading Inhibitors of Current SMB Investment in End-User Identities and Authentication



Note: multiple responses accepted; does not add to 100%. Source: Aberdeen Group, November 2011

Analysis: SMBs are Getting the Security They Pay For

Compared to Large organizations, SMBs on average spent $5.70 (38%) less per user on managing identities and authentication – but this was a false economy, as they also incurred an average of $73 (87%) more cost per user as a result of security-related incidents, in spite of their current investments (Table 1). Stated another way, Large organizations realized a return of *12.8-times on their incremental investments* in stronger end-user authentication in comparison to SMBs – confirming that typical SMBs have a compelling opportunity not only to enhance security, but also to reduce total cost.

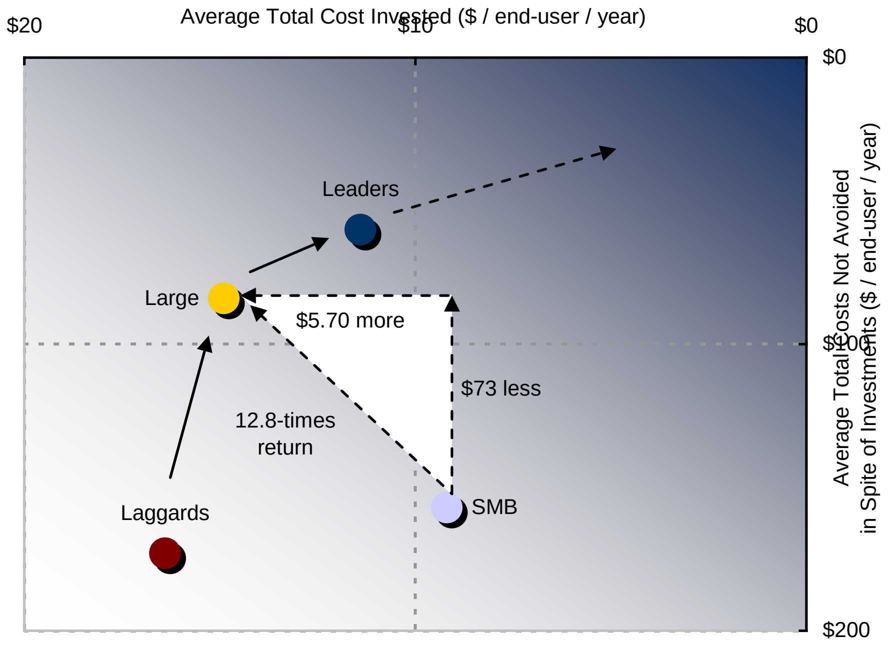
Table 1: Average Total Costs Invested, Average Total Costs Not Avoided, by Group ($/user/year)

Average $ / end-user / year	Leaders	Laggards	SMBs	Large	Large vs. SMBs
Total cost for managing identities and authentication	$11.40	$16.40	$9.20	$14.90	$5.70 more
Total costs incurred as a result of security-related incidents	$60	$173	$157	$84	$73 less
Total cost	**$71**	**$189**	**$166**	**$99**	12.8-times return on incremental investment

Source: Aberdeen Group, November 2011

To provide a more visual perspective, the findings from Table 1 are also represented graphically in Figure 4. Note that the Leaders (top 20%) in the study not only spent less than the Laggards (bottom 30%) in terms of average total costs invested (i.e., they were more *efficient*), but also incurred fewer costs as a result of security-related incidents (i.e., they were more *effective*). Given that the upper-right quadrant represents the most desirable direction, Figure 4 again makes it clear that typical SMBs have an immediate opportunity for improvement.

Figure 4: Average Total Costs Invested, Average Total Costs Not Avoided in Spite of Investments ($ / end-user / year), by Group



Source: Aberdeen Group, November 2011

Solutions Landscape (illustrative)

Based on the research findings outlined above, high-level solution selection criteria for SMBs include the following:

- Address concerns and costs related to risk, with stronger authentication than traditional username and password
- Provide the flexibility to support internal policies, as well as address external requirements for audit and regulatory compliance
- Integrate easily within the diversity and complexity of existing IT infrastructures, without adding complexity or additional burden on end-users or existing IT staff
- Support demonstrable business value, by being affordable to acquire, integrate and deploy, and manage

Defining Maturity Classes

Aberdeen's research methodology defines all study respondents as falling into one of three groups, with three corresponding levels of practices and performance:

√ *Leaders* or *Best-in-Class* (top 20%) – Practices that are the best currently being employed and result in the top overall performance

√ *Industry Average* (middle 50%) – Practices that represent the industry average or norm, and result in average performance

√ *Laggards* (bottom 30%) – Practices that are behind the industry average, and result in below-average overall performance

For additional information, see Aberdeen's benchmark study on *Managing Identities and Access* (March 2011).

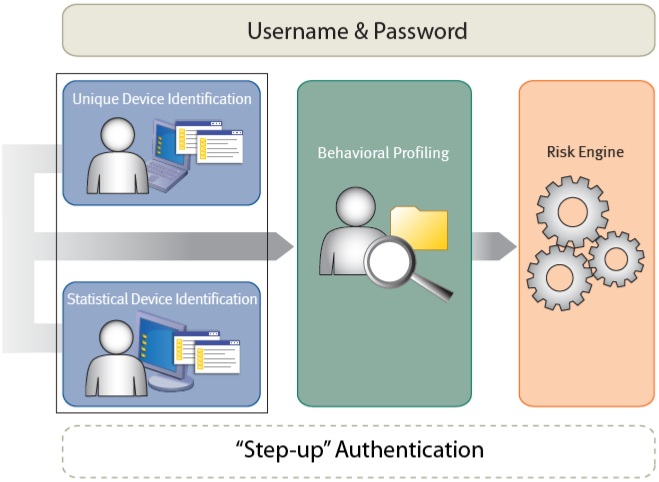
With these in mind, stronger authentication solutions that are especially well-designed to address the particular needs of SMBs include the following three examples, selected based on the three highest Interest Indexes from Figure 1:

- **Heuristic / adaptive / risked-based authentication** – For SMBs looking to augment their existing username and password implementations with multi-factor authentication, *RSA Authentication Manager Express* integrates with existing IT infrastructure with no change to the end-user experience in typical situations.
- **Smart cards** – For SMBs looking for flexibility in augmenting or replacing their existing username and password implementation with smart cards and other stronger forms of authentication, *Entrust IdentityGuard* integrates with existing identity infrastructure and manages a broad range of stronger authentication methods from a common platform.
- **Out-of-band authentication via phone call or SMS** – For SMBs looking to augment their existing username and password implementations with two-factor authentication, *PhoneFactor* integrates with existing IT infrastructure and leverages the mobile phones most end-users already carry and use.

Solution Provider Case-in-Point: RSA Authentication Manager Express

RSA Authentication Manager Express (RSA AMX) is a relatively new offering for the small and mid-sized enterprise, but it is based on the proven *RSA Adaptive Authentication* solution which is currently in use by more than 8,000 organizations to protect more than 250 million end-users worldwide.

Figure 5: Heuristic / Adaptive / Risk-Based Example – RSA AMX



Source: RSA, The Security Division of EMC, November 2011

RSA Authentication Manager Express is designed to provide SMBs with stronger, multi-factor authentication in a solution that is completely transparent to end-users – i.e., no change to the existing username and password authentication experience in typical situations, with optional "step-up" authentication challenges when the risk engine identifies higher-risk, higher-assurance scenarios (Figure 5). For example, RSA AMX includes support for on-demand delivery of one-time passcodes to end-user mobile phones via SMS or email as one option for step-up authentication.

Packaged for convenience as a hardware appliance platform, RSA AMX is designed to be simple for SMB IT organizations to implement and use, featuring out-of-the-box integration with existing IT infrastructure, and nothing to deploy to end-users.

Summary and Key Takeaways

Aberdeen's research and analysis shows that Small and Mid-Sized Businesses (SMBs) authenticate their end-users primarily with passwords, in spite of the fact that passwords are less secure, inconvenient, and in fact more expensive than stronger forms of authentication.

Compared to Large organizations, SMBs on average spent 38% less per user on identity management – but this was a false economy, as they also incurred an average of 87% more cost per user as a result of security-related incidents, in spite of their current investments. Stated another way, Large organizations realized a return of *12.8-times on their incremental investments* in stronger end-user authentication in comparison to SMBs – confirming that typical SMBs have a compelling opportunity not only to enhance security, but also to reduce total cost.

Aberdeen’s analysis of drivers, inhibitors and technology adoption trends among SMBs indicate that high-level solution selection criteria for SMBs include the following:

- Address concerns and costs related to risk, with stronger authentication than traditional username and password
- Provide the flexibility to support internal policies, as well as address external requirements for audit and regulatory compliance
- Integrate easily within the diversity and complexity of existing IT infrastructures, without adding complexity or additional burden on end-users or existing IT staff
- Support demonstrable business value, by being affordable to acquire, integrate and deploy, and manage

With these in mind, stronger authentication solutions that are especially well-designed to address the needs of SMBs – and align with the highest levels of market interest seen in Aberdeen's research – are exemplified by:

- **Heuristic / risk-based / adaptive authentication** – e.g., RSA Authentication Manager Express

- **Multi-purpose smart cards**, among a broad range of stronger authentication methods managed from a common platform – e.g., Entrust IdentityGuard
- **Out-of-band authentication via call or SMS to mobile phones** – e.g., PhoneFactor

Small and Mid-Sized businesses that are investigating stronger forms of end-user authentication than traditional username and password should consider putting these three classes of enterprise solutions at the top of their respective short lists.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research

The Case Against Passwords: Re-evaluating Stronger User Authentication; August 2011

The Case for Smart Cards; July 2011

Q1 2011 Aberdeen Business Review; May 2011

IAM Integrated: Analyzing the Platform versus Point Solution Approach; June 2011

Managing Identities and Access; March 2011

The Zen of Network Access; Dec. 2010

Logon Once, Access Many: The Pursuit of Single Sign-On; March 2009

One-Time Passwords for Two-Factor Authentication; January 2009

Managing Privileged Users; Nov. 2008

Strong User Authentication: Best-in-Class Performance at Assuring Identities; March 2008

Author: Derek E. Brink, Vice President and Research Fellow for IT Security (Derek.Brink@aberdeen.com)

For more than two decades, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.5 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen's research provides insight and analysis to the Harte-Hanks community of local, regional, national and international marketing executives. Combined, we help our customers leverage the power of insight to deliver innovative multichannel marketing programs that drive business-changing results. For additional information, visit Aberdeen http://www.aberdeen.com or call (617) 854-5200, or to learn more about Harte-Hanks, call (800) 456-9748 or go to http://www.harte-hanks.com.

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc. (2011a)