WHITE PAPER

Adaptive Access Management: An ROI Study

Sponsored by: Oracle

Sally Hudson Randy Perry

September 2010

EXECUTIVE SUMMARY

Enterprise computing infrastructures — on premise, hosted, or in the cloud — demand rigorous attention to who, what, where, when, and how a person or an entity accesses data. Security solutions must verify and provide assurance that those requesting access are indeed who and what they say they are. In order to increase security and comply with industry compliance regulations, organizations are looking for solutions that allow them to proactively:

- Prevent fraud
- Authenticate identities
- Increase compliance

While enterprises are carefully scrutinizing the cloud deployment model to achieve economies of scale and reduced capex, to evaluate the cloud platform without carefully considering the security and compliance capabilities is to invite disaster. Identity issues are now pervasive in all areas of security, and IP addresses are no longer deemed sufficient. Stricter compliance regulations and reporting are now driving non-IT people (CEOs, CFOs, compliance officers, legal staff, HR staff, auditors) to demand reports with names and locations, and the move to a cloud platform does not release enterprises from their responsibilities in legal liability and privacy matters. This is true whether or not they use private clouds or public clouds, or a mixture of both, creating a hybrid model. At present, IDC is seeing more adoption of the latter.

The impending collision of cloud platforms and traditional systems is pressuring enterprises to better and more efficiently manage identity and access management (IAM). As we see increasing mixtures of SaaS with internal applications, such as ERP and CRM, organizations that fail to implement comprehensive identity access and antifraud solutions risk not only damaging their reputations and losing customers but hefty legal penalties and fines as well. Fortunately, much of this can be addressed by implementing a comprehensive IAM strategy. IAM technology can by deployed to determine, defend, and protect critical corporate resources, as well as private customer data (e.g., financial, healthcare) while in transit and at rest.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

SITUATION OVERVIEW

Business computing models are changing rapidly, expanding beyond traditional business-to-employee to business-to-consumer, business-to-business, and increasingly, government-to-citizen. Many retail, insurance, and banking organizations now enjoy a large Web presence, and government sites (e.g., motor vehicle registries) are following suit. As the volume and number of people and entities interacting via the Internet increase exponentially, so does the risk of fraud and misuse. Organizations need to be proactive to prevent becoming tomorrow's headline. For example, it was recently reported by several national news agencies that the Financial Industry Regulatory Authority (FINRA) fined brokerage firm Davidson & Co. $375,000 over a 2007 data breach in an action that highlights the growing attention regulators are paying to the controls companies have in place for protecting customer data. The breach resulted in the exposure of customer names, account numbers, addresses, Social Security numbers, dates of birth, and other confidential information belonging to about 192,000 customers. For Certegy, a wholly owned subsidiary of Jacksonville, Florida–based Fidelity National Information Services (FIS), a 2007 breach resulted in bad press and huge fines. The company recently had to pay $975,000 in fines to the Florida attorney general after it was discovered that a malicious insider at the company exposed 5.9 million customer records. The actual $850,000 fine was levied by Florida to pay its investigative costs and attorney fees, and the additional $125,000 was demanded to help fund a statewide crime prevention program. This is just the beginning for Certegy: Because of the breach, the company was forced to settle a $4 million class-action lawsuit and is now required by the state of Florida to conduct a yearly security assessment.

The regulations for stemming the tide of online fraud and identity theft are well known across industries: Sarbanes-Oxley (SOX) and Section 404 of same, HIPAA, PCI, GLBA, HITECH, FFIEC, HSPD-12, and others. Perhaps one of the most visible U.S. cases that drew attention to the need for enforcing these regulations came with the famous TJX Companies breach. During the investigation, it was determined that 45.6 million credit and debit card numbers were stolen over an 18-month period ending in 2007. This incident, as well as numerous others such as Societe Generale and Hannaford, points to the absolute requirement for strong authentication and fraud prevention.

While finance and banking have historically been the focus of fraud prevention and privacy protection, regulators for the healthcare industry are rapidly ramping up as well. In the United States, the federal government has recently expressed concerns surrounding Medicare fraud and increased activity by criminals looking to defraud senior citizens. Secretary of Health and Human Services Kathleen Sebelius has stated that the mandate is to use the new tools and resources to further crack down on fraud. The most recently publicized case involved a group of pharmacists in the Tampa, Florida, area fraudulently using client identities to bilk the government of millions of dollars. Secretary Sebelius' goal is to cut the improper payment rate, which tracks fraud, waste, and abuse in the Medicare Fee for Service Program, in half by 2012.

Private citizens are also now taking action. In September 2009, it was reported that the U.S. District Court for the Northern District of Illinois allowed a couple whose home equity loan account was looted to bring a negligence claim against Citizens Financial Bank after determining the bank had not employed adequate controls.

IDC advocates that organizations adopt a multilayer approach for security and compliance to avoid these situations and take a proactive stance. A fundamental portion of this approach rests with risk-based authentication, authorization, and identity authentication.

As threats multiply and increase in number and severity, organizations must go beyond "front door" security to provide specific protection for all high-value services, applications, events, and transactions. The severity and financial impact of security, fraud, and identity exposure can have enormous impact on an organization, C-level executives can be held accountable, and the fines can be hefty as demonstrated in the preceding examples.

A securely configured cloud model can provide organizations with:

- Reduced cost through process automation, lower head count, and no expense for on-premise equipment and maintenance
- Ease of deployment, reducing the need for internal IT, external consultants, and help desk calls
- Minimized administration overhead, providing current updates and checks for access control
- Consistent and continual policy enforcement, which increases both security and compliance

A nonsecure cloud or internal platform can lead to increased risk and exposure to fines, bad publicity, and loss of both current and future business.

The Foundation: Identity and Access Management

Applying identity and access management technology serves to ensure that company data, applications, documents, and Web services are protected from intruders both inside and outside the organization.

The industry has defined identity and access management as a set of solutions used to identify users in a system (employees, customers, contractors, and so on) and control their access to resources within that system by associating user rights and restrictions with the established identity. Subcategories of the IAM market include Web single sign-on (WSSO) and federated single sign-on (FSSO); host/enterprise SSO; and user provisioning, including granular authorization and policy rights. Given the evolution of advanced threats and the development of technologies to combat these threats, the traditional definition has been expanded to include solutions that profile behaviors, track devices, authenticate identities, assess risk, and dynamically challenge users based on the level of risk. This is done while capturing an exceptionally rich audit trail of user behavior.

Constant change across corporations, organizations, and industries is driving the enterprise to demand greater integration of security and management technology, with an eye toward cost/benefit analysis and compliance.

Preventing Fraud and Utilizing Risk Mitigation

No one wants to be tomorrow's media headline. To avoid those situations and the resulting fines, loss of consumer faith, and perhaps even criminal penalties, organizations should employ a risk-based access management solution to thwart malicious acts and misappropriation of sensitive information. Additionally, the ability to detect aberrant behaviors and anomalies in real time serves to create a rich forensics profile.

Creating a strong risk management profile is critical today. A better risk posture has been proven to be instrumental in helping organizations proactively avoid situations that cost time and money to repair. (It is easier to fix a vulnerability than to spend hours retroactively patching a problem.) Identity and security is no longer just "who had access"; rather, it has expanded to include the what, how, and why of any interaction. Customers looking to save time and money by implementing a holistic solution should look for mature enterprise-class software that allows security and compliance to be done in tandem and to be fused with overall business operations.

Risk-based decision making must be dynamic to be effective today, and it must be continually monitored/evaluated. A comprehensive security and compliance profile includes fraud prevention measures such as real-time risk analysis to drive authentication and authorization decisions. A risk-based approach addresses the gray areas of access management in a way traditional solutions cannot. For example, with traditional means, if a user enters John Smith's valid username and password, the solution must assume that it really is John accessing the protected resources. However, with a risk-based approach, behavioral profiling can be used to dynamically determine how likely it is that the user is indeed John and take action accordingly. Such measures are effective in preventing fraud and misuse during log-in and at any time during a session. Risk analytics provides the ability to identify anomalies in user access patterns (current versus historical) and take action. Risk analytics and fraud detection software can also identify anomalies nonspecific to an individual. For example, if John Smith logs in to a computer and conducts a transaction with a company in Australia, and one hour later, Jane Doe logs in to the same computer and conducts a transaction with a company in Houston, Texas, the software could immediately flag this incompatibility because the device and the locations are tracked and compared between sessions, regardless of the user. Investigation tools in this area allow an organization to shift gears from reactive to proactive. In this way, fraud and misuse not detected through traditional means can be prevented, saving money directly and indirectly.

The one-two punch delivered by the combination of strong authentication and fraud prevention greatly increases the likelihood of stopping malicious activity at the gate — and if not at the gate, then *very* soon after entry. From a cost perspective, it is much better to make a minor repair to the lock on the gate than to replace stolen valuables.

An Active Approach to Compliance

Identity and access management is proven to be a key technology set in achieving compliance. Regulatory compliance regulations (e.g., SOX, PCI, GLBA, HITECH, HIPAA, JPIPA, and NERC) are increasing on a worldwide basis. To meet many of these criteria, companies are implementing IAM frameworks. In fact, IDC estimates that 85% of all strategic IAM purchases in 2009 were compliance driven. Enterprises increasingly require automated workflows that incorporate strong security, auditing, archiving, and storage for compliance purposes. Data must be easy to locate and produce for audit. The technology must allow for easy implementation of new controls because the compliance landscape is always changing. A proactive automated system that does not permit an out-of-compliance action to occur is the goal. Advanced offerings that profile behaviors and track application, device, and location usage capture a uniquely rich audit trail not available through traditional means. Such solutions go beyond the compliance of current regulations, making businesses ready for future compliance measures today, which could mitigate the need for costly future upgrades.

Taken together, these elements — IAM, fraud prevention, and risk mitigation — can provide essential pieces of an end-to-end security strategy. By fusing these capabilities, whether on premise or in the cloud, organizations can hope to achieve:

- Stronger security posture and increased customer trust; lack of trust decreases business opportunity (e.g., customer churn)
- Cost savings through consolidated software functionality, less system administrative overhead
- Cost savings through automation, which reduces manual error while increasing overall system productivity
- Cost savings through better reporting and ability to more quickly meet audit requirements
- Protection against inadvertent regulatory violation and the resulting fines
- Increased overall time to value

Oracle Adaptive Access Manager

Oracle Corp., based in Redwood Shores, California, has led the IAM market in leveraging industry consolidation to achieve a comprehensive product suite extending from IAM to governance, risk, and compliance (GRC).

The Oracle Adaptive Access Manager (OAAM) is not a point solution but a robust component of Oracle's proven Identity Management platform. OAAM is integrated with Oracle Access Management software. The software is designed to offer customers end-to-end IAM functionality, including:

- Risk-based authentication and SSO
- Fraud prevention

- Federation
- Authorization and entitlements
- Web services security
- Information rights management

OAAM can be both a consumer-facing and employee/partner-facing solution. This flexibility allows the enterprise to more completely protect itself and its users as well as save money through centralization of security. Its broad set of capabilities includes real-time risk analysis, strong authentication, risk-based authentication, device and location tracking, and event/transaction monitoring. For compliance purposes, OAAM offers tracking and auditing of and visibility into user actions to allow organizations to proactively determine risk and deny access before a security event occurs. The software utilizes virtual authentication devices that provide users with mutual authentication and protection from various types of malware and other online threats.

One example of the virtual authentication devices offered by OAAM is KeyPad. The time-stamped KeyPad uses simple but elegant Web technologies to protect passwords from keyloggers and other types of malware and can be customized to include a user's personalized image and phrase antiphishing protection. Rather than a user's password, a random data string is generated each and every time it's used. The authentication strengthening provided by the virtual authentication devices is becoming a necessity and not a nice-to-have extra in access management today, as username/password is widely perhaps the weakest link in the overall computing environment. The virtual authentication devices combine with risk-based authentication and behavioral profiling. One of the advantages of OAAM is that there is no chance of an end user losing it; therefore, an organization has no replacement costs or lack of productivity issues to deal with in that area. In addition to strong authentication, OAAM provides autolearning capability. The software analyzes current user behaviors versus recorded behaviors and dynamically adjusts risk evaluations based on the results in real time. The software includes investigation tools, which allow IT professionals and security analysts to link suspect sessions to a case in order to quickly determine and relate fraudulent activity. Case workflow features provide case expiration management and customer case escalation.

Within the security and IAM space, IDC advocates that IT vendors and service providers develop tools that bring together event records, efficiently prioritize incidents, separate real security violations from false alarms, and aggregate security events from different locations, devices, and manufacturers.

Another significant advantage derived from OAAM is that the product secures single instances for Web applications, Web services, and mobile devices, creating a more cost-effective overall approach through a proactive, up-front approach to increased security and simplified end-to-end implementation. As enterprise IT moves toward a more Web services–driven approach, it should be noted that IAM software inherently has many of the standards and technological requirements for supporting Web services implementations. Companies are migrating toward Web services. IAM inherently supports SSO, SAML, LDAP, certificate authority, etc., all of which are a natural fit for Web services.

The software incorporates an easy-to-use dashboard for security professionals and systems administrators. The dashboard displays performance statistics, historical trending, and expanded activity aggregates. Out-of-the-box templates for BI Publisher can be used to create and manage custom reports. OAAM comes with a simplified administration console to provide business users with easy-to-use policy administration, transaction definition, and data mapping capabilities. The software provides in-depth transaction analysis and detailed audit trails of related data. OAAM can be applied successfully in all inline, non-inline, and offline transactions.

In summary, OAAM offers a comprehensive, proactive approach to security and compliance within the enterprise by providing:

- Strong authentication
- Real-time anomaly detection
- Interdiction mechanisms
- Reporting and forensics

As part of Oracle's overall Fusion Middleware family of products, OAAM also offers customers the benefit of rich IAM functionality found within the Oracle Access Manager SSO and Oracle Identity Manager's self-service password management. Taken together, these proven and tested components and their features provide a comprehensive platform for strong authentication, risk analysis, and fraud prevention. The reporting and analytics serve to support ongoing compliance mandates and initiatives within an organization.

The Business Case for Oracle Adaptive Access Manager

IDC conducted in-depth interviews with three companies that had deployed OAAM to counter significant threats from fraud. From the research, we determined that prior to the implementation of OAAM, the companies experienced average annual losses of $2.4 million from fraud. Reducing fraud generated the following benefits:

- **Reduced fraudulent credit applications.** Fraudulent credit applications lead to significant costs associated with unpaid bills and the labor to investigate and prove fraud. Reducing fraud by 13% saved millions annually.
- **Chargeback avoidance.** On average companies saved $33,600 annually by avoiding chargeback fees.
- **Decreased customer churn**. Even when fraud does not result in direct loss of revenues or fees, high fraud rates undercut the value of a company's services and cause customers to change providers. Reducing churn from 6% to 4% saved nearly $3 million annually (see Table 1).
- **Reduced IT staff costs.** In addition to reducing the lost revenue from fraud, the companies were able to reduce their internal labor costs for dealing with fraud. These IT labor tasks included authentication, risk analysis, investigation, password management, and policy administration.

TABLE 1

Benefits — Fraud Reduction

	Before	After	Savings	Average % Savings
Fraud rate				34%
Customer churn rate related to fraud	6%	4%	3%	45%
Annual lost revenue due to churn	$13,561,600	$10,580,480	$2,981,120	22%
Savings as a % of revenue				3%

Note: Companies did not provide before and after data for fraud rate and savings as a percent of revenue because they considered this information too confidential.

Source: IDC, 2010

ROI Analysis

Overall, the companies in the study recognized total benefits of over $6 million from an investment of $2.9 million over three years in the OAAM platform. IDC accounts for the opportunity costs realized by not having invested the initial amount in some other instrument yielding a 12% return. This results in a net present value (NPV) for the three-year benefits of $3.1 million (see Table 2). Based on the total benefits, the payback period from deploying OAAM averaged 12.1 months for the companies surveyed, yielding an average return on investment of 106%.

TABLE 2

Three-Year ROI Analysis

Metrics	Value
Benefit (discounted) — benefits at a 12% discount factor	$6,007,641
Investment (discounted) — investment at a 12% discount factor	$2,912,513
Net Present Value (NPV) — discounted benefits – discounted investment	$3,095,129
ROI = NPV/Investment	106%
Payback = Investment/NPV	12.1 months
Discount Rate (cost of capital plus a risk factor)	12%

Source: IDC, 2010

IDC'S ROI METHODOLOGY

IDC's extensive research on IAM technology was recently validated by in-depth interviews with companies that have had IAM installed for more than one year. The IDC ROI methodology is based on gathering data from current IAM users. IDC performs a three-step process to calculate the ROI and payback period:

1. Measure the financial benefits from reduced costs (operations and infrastructure), increased user and IT staff productivity, and increased revenue.

2. Ascertain the investment made in deploying the IAM solution and the associated training and support costs.

3. Estimate the costs and savings over a three-year period and calculate the ROI and payback for the deployed solution.

Because the full benefits of the solution are not available during the deployment period, IDC prorates the benefits on a monthly basis and subtracts the appropriate amount for the deployment time from the first-year savings.

IDC uses a discounted cash flow methodology to calculate the ROI and payback period. ROI is the ratio of the net present value (NPV) and discounted investment. Payback period is the point at which cumulative benefits equal the initial investment. IDC uses a standard 12% discount factor (allows for risk and the missed opportunity cost that could have been realized using that capital).

FUTURE OUTLOOK

Today, compliance regulations are driving the need for flexible roles-based access and delivery models, fine-grained entitlements, and advanced authentication mechanisms across all industries, but especially in finance, banking, insurance, and healthcare.

Furthermore, the ability to proactively assess fraud threats and risk levels based on time, date, geographic location, and usage patterns is essential to strong corporate security and compliance postures. As the scope of fraud and threats has expanded past its traditional usage point in banking and finance, research shows that risk-based authentication is superior. Customers give strong marks to products and/or services that are capable of integrating with existing enterprise access management systems for monitoring and compliance purposes.

Fraud prevention is becoming a requirement across many industries, including government, healthcare, manufacturing, and education. Healthcare is particularly vulnerable due to the comprehensiveness and sensitivity of information associated with patient histories and accounts. This goes beyond protecting Social Security numbers and includes preventing access to personal healthcare history and treatments. Healthcare organizations, like banking and government organizations, are realizing that that fraud detection is not enough; fraud prevention and blocking are critical. While deep protection and prevention are critical, having them incorporated within a nonintrusive, integrated system is the ideal.

Brand protection is critically important as well. As one interviewee put it, "…our brand is strong and we have been around such a long time. Every time fraud occurs, it weakens the brand. Risk Manager is our main way to automatically guard against fraud. If we didn't have it, we might suffer brand damage and customers not coming back."

Finally, the ability to monitor, track, and report on activities will greatly simplify the audit process while giving real-time views into system activity.

CHALLENGES/OPPORTUNITIES

Challenge: Oracle must quickly demonstrate that OAAM offers an easier-to-use, cost-effective strong authentication and comprehensive fraud prevention solution. This is a growing and crowded market space. Many products are available today from both large and small technology vendors.

Opportunity: IDC research shows that advanced authentication/strong authentication is an area poised for growth over the next several years. Many organizations and government entities are currently evaluating the myriad options available today. Vendors such as Oracle can provide not only mature, proven products but also the channels and delivery mechanisms necessary to make the process easier to administer and deploy. The number of applications, both internal and Web facing, requiring strong authentication will continue to increase over the next several years. The ability for these solutions to provide proven scalability is essential.

The ability to provide not only strong authentication but also sophisticated fraud prevention and reporting capabilities within a single solution set should prove appealing to customers. Software tokens offer many advantages to customers looking to avoid the hardware-oriented authentication approach. Software tokens do not get lost, do not need to be physically present with the person requesting access, and are generally a less cost-intensive solution. Help desk calls and management tasks are also reduced when users don't have to call in to report missing authentication devices.

Achieving cost savings while increasing security is important to organizations today. One of the interview candidates pointed out that the company was able to reduce headcount within its security auditing staff by half while increasing security via automation: "We get 24-hour-a-day protection because my staff doesn't have to be at their desks."

CONCLUSION

Security has emerged as a critical component in risk management and business operations. Demand is strong because of increased threat levels, increased incidence of identity fraud, data misuse, and tougher regulations. Lastly, organizations are implementing comprehensive access management tools to protect their customers, business, and shareholders.

As articulated by one of the ROI study participants, Oracle's OAAM authentication software meets critical customer needs by providing an "invaluable resource for fraud analysts" to do research based on the output of the tool and, in conjunction with other security mechanisms, to obtain a portrait of certain aspects of user behavior.

With worldwide, 24 x 7 access to information, it's easy for companies to be more vulnerable these days. Moving to cloud platforms increases compliance complexities. Businesses are beginning to realize that security measures are never final solutions in and of themselves; security for the organization must be a proactive and continual process. Companies must create and maintain risk profiles and continually raise flags. In the rush to get products or services to market, it is sometimes too easy for businesses to ignore good security practices. However, those that do will be increasingly addressed by regulations and fined heavily for noncompliance.

Companies must remember that although the cloud promises cost savings, threat and risk assessments must still be part of the equation. Cloud platforms will be increasingly targeted as their use grows, and the need for business-proven, cost-effective security and compliance will increase as well.