

White Paper

Identity and Information Security Integration

By Jon Oltsik

September, 2009

Contents

Executive Summary	3
Identity and Security: A Historical Perspective	3
The Need for Identity and Information Security Integration	4
Think Identity and Access Assurance.....	6
Identity and Information Security Integration Requirements.....	6
Real-time Business Agility.....	7
Ease of Use	8
Enhanced Protection	8
RSA and Courion are Leading the Way	10
The Bigger Truth	12

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188. This ESG White Paper was developed with the assistance and funding of RSA Security and Courion, Inc.

Executive Summary

In the past, identity management and information security solutions were often procured, implemented, and managed independently with different tools, processes, and organizational units. This separation is quickly becoming a thing of the past. Why? In this white paper, ESG concludes that:

- **New business requirements demand integrated identity and information security management.** Large organizations are rapidly bringing identity and security together in order to meet regulatory compliance mandates, address sophisticated security threats, safeguard sensitive data, and enable new network-based business processes. These changes demand integrated identity/security people, processes, and technologies.
- **Legacy identity and security infrastructure is no longer adequate.** Change is a necessity since most currently deployed autonomous identity and security infrastructure simply can't scale, map identity with data classification, or provide the central management capabilities needed to address these new demands. Over time, these limitations will inhibit business processes, create operations overhead, complicate regulatory compliance audits, or introduce new security risks to the business.
- **The new goal should be identity and access assurance.** Rather than basic interoperability, CIOs should create an identity and access assurance infrastructure. In this model, identity and information security are tightly integrated to manage and monitor access and usage rights to sensitive data – not just applications. In this way, CIOs can create more granular entitlement roles and rules to improve governance, risk, and compliance without added complexity or operations overhead.
- **Identity and access assurance delivers three components.** With network-based business processes that include external users becoming commonplace, identity and access assurance should not be thought of solely as an IT project. Rather, successful integration will provide: 1) Real-time business agility so IT can deliver proactive identity/security services for network-based business processes, 2) Ease of use for both business and IT managers, and 3) Enhanced protection in order to minimize new risks posed by external IT initiatives.

Identity and security integration is already challenging technology vendors, not just IT professionals. RSA, The Security Division of EMC, and Courion are addressing new user requirements by integrating their best-of-breed identity and security technologies in order to meet the changing needs of demanding enterprise customers.

Identity and Security: A Historical Perspective

Throughout the history of distributed computing, identity management and information security were often implemented and managed in a fairly independent fashion. Yes, security groups cooperated with software developers and IT operations on things like user authentication and password management, but overall collaboration remained fairly limited. For the most part, identity and security remained separate because:

- **Identity management focused on employee productivity.** The process for provisioning a user account was generally led by the human resources department as part of providing new employees with essential productivity tools like telephones, employee badges, and network/application access. While HR initiated the process, IT was responsible for many critical Identity and Access Management (IAM) tasks. Until fairly recently, many of these tasks were ad-hoc and manual, with IT administrators provisioning application and network accounts on a system-by-system basis. More recently, IT operations acquired more sophisticated identity management tools to automate user provisioning, workflow, and day-to-day operations, but these processes were still guided by HR and business managers.
- **Security teams focused on IT infrastructure and security attacks.** Far removed from HR, CSOs concentrated on safeguarding networks and PCs against hackers and malicious code. Security professionals were often highly focused on technologies like firewalls and antivirus software and were regarded as a niche group of specialists within IT.

With the benefit of hindsight, it is hard to believe that security and identity operations were so far removed from one another, but this separation was logical at the time. Until recently, business computing was anchored by private networks and minimal Internet access, so “trusted” employees were thought of as a minimal security risk. Sure, a few rogue workers might steal office supplies, but this type of physical threat was all that was expected. Alternatively, IT security risks were pigeonholed into known attacks like the “I Love You” and “Melissa” e-mail viruses, web site defacement, and network scanning. Identity and security were binary topics – one dealt with trusted employees and the other with untrusted network packets. These areas were distinct and disconnected within IT.

The Need for Identity and Information Security Integration

Fast forward to the last few years and there is growing IT consensus: identity and data-centric security technologies and processes must come together. Why? In 2009 and beyond, tight identity and data-centric security integration has become an enterprise requirement because:

- Regulatory compliance requires strong access and security controls.** Government and industry regulations such as Basel II, HIPAA, the EU Data Privacy Directive, and PCI DSS are forcing large organizations to implement security and identity policies and controls to restrict access to private/sensitive data (i.e., customer data, health care records, credit card numbers, etc.), log security events, and perform compliance audits on a regular basis. Since compliance violations can result in stiff penalties, costly data breaches, or even criminal charges, regulatory compliance (and associated identity and security integration) plays an extremely influential role in the data privacy/security efforts of large organizations (see Figure 1).

Figure 1. Influential Factors in Information Security/Privacy Efforts



Source: Enterprise Strategy Group, 2009.

- Costly data breaches are all too common occurrences.** There were a total of 615 publicly-disclosed data breaches in 2008 exposing more than 83 million personal records (source: datalossdb.org). Approximately 21% of these incidents are the result of stolen or lost laptops, 17% are the results of “hacks,” 14% are the results of attacks on web applications, and 7% are the result of fraud. To address the risk of a data breach

in the future, CSOs need to control access to regulated private data, detect/prevent data leakage, and monitor user activity at all times.

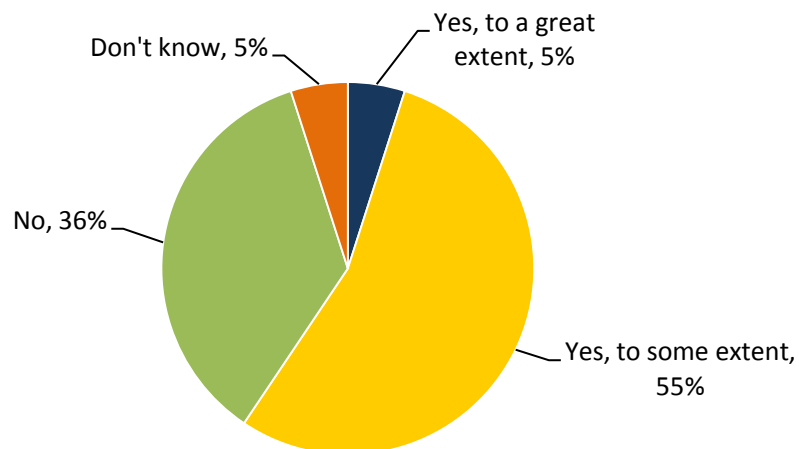
- **Internal networks are “open for business.”** New business processes are often linked to web applications and Internet technologies in order to drive new revenue streams, expand opportunities, accelerate business initiatives, and lower costs. This trend is illustrated by ESG research data, where 60% of enterprise organizations (i.e. 1,000 employees or more) say that they share confidential data with non-employees (see Figure 2).¹ Most organizations also believe that they will share more confidential data with more external constituencies like business partners, customers, or suppliers in the future as well. This trend means more and more users will live “outside the firewall.” And with more and more business conducted over the network, large organizations can’t simply block IP addresses, ports, and protocols. Alternatively, they need a clear understanding of who accessed sensitive data from which location. This demands tight identity/information security integration, constant user and network monitoring, and strong technologies for policy enforcement.

Taken together, these factors break the old model of independent security and identity islands. Today’s disparate identity and security infrastructure is anchored by multiple management platforms that can’t provide for central control, end-to-end monitoring, or common skills and processes. Protecting confidential data and meeting regulatory compliance requirements are dependent upon an army of IT administrators, manual processes, and costly fire drills. Even with this amount of effort, CSOs must piece the status of enterprise security together based upon disjointed data and personal opinions. In this scenario, enterprise information security is an educated guess at best.

Since legacy tactical identity and security tools can’t provide automation, command-and-control, or end-to-end oversight, CIOs find themselves at a technology crossroad: either proceed with identity and security integration or suffer the consequences of high costs, limited agility, and increased risk.

Figure 2. Most Large Organizations Share Confidential Data with Non-Employees

Does your organization share its confidential data with non-employees (i.e., business partners, suppliers, customers, etc.)? (Percent of respondents, N=308)



Source: Enterprise Strategy Group, 2009.

¹ Source: ESG Research Report, *Protecting Confidential Data Revisited*, April 2009.

Think Identity and Access Assurance

Most identity management tools are designed for password management, application account provisioning, and role management. To meet today's new challenges, identity management must embrace information security knowledge in order to enforce access and entitlements at a more atomic level. With this intelligence, large organizations can then lock down data access to a small group of "need to know" users, monitor activity, and change access controls on the fly when necessary.

In order to achieve these goals, identity management needs to be integrated into a common "identity and access assurance" infrastructure with leading security safeguards like:

- **Data discovery, classification, and security policy enforcement.** The identity management infrastructure should be supported by Data Loss Prevention (DLP) tools that can scan and classify data repositories and endpoint systems for sensitive data. Armed with this knowledge, identity and access management tools can be used to create small sub-groups or specific roles with confidential data access rights. In this way, information-centric identity management can help streamline regulatory compliance controls, simplify audits, and reduce information security risks.
- **Security monitoring and analysis.** Many existing compliance and security tools can only identify a user based upon an IP address, not by an actual account name. This is clearly inadequate as current and future compliance auditing and security forensic investigations demand an end-to-end review of who did what, when. To get a complete picture, identity auditing tools must align with log management and security event management data. This integration alone can greatly reduce the time and effort necessary for security event detection, root cause analysis, and emergency response.
- **Authentication management.** New demands for entitlements and role-based access controls demand a combination of automated account provisioning and strong authentication. When applied in an integrated fashion, account provisioning and authentication can make access rules far more granular to specific users, application functions, or data elements.
- **Access certification.** In order to demonstrate compliance with industry and government mandates regarding controls over access to sensitive data, organizations need a mechanism for automatically analyzing user access rights and verifying that they are consistent with corporate policy.

It is important to note that identity and information security integration must go beyond information exchange for historical reporting. Today's business and security demand rapid response capabilities for functions like provisioning a user account for an external contractor, detecting a security attack in progress, or gathering evidence for a legal proceeding. To meet these requirements, identity and information security must have integrated command-and-control, common user interfaces, and real-time monitoring and alerting.

Identity and Information Security Integration Requirements

As described above, identity and information security integration is being driven by numerous business and technology trends. Moving forward, CIOs will need to be incredibly responsive to changing requirements with an identity and security infrastructure that can meet their requirements in 3 areas (see Table 1):

1. Real-time business agility
2. Ease of use.
3. Enhanced protection

Table 1. Attributes of Identity and Information Security Integration

Attribute	Business Benefit	IT Benefit
Real-time business agility	<ul style="list-style-type: none"> • Get users productive • Extend internal applications to external constituencies to drive revenue and productivity • Customize business processes to user needs and requirements 	<ul style="list-style-type: none"> • Offer proactive support for new business processes • Accelerated deployment of new applications
Ease of use	<ul style="list-style-type: none"> • Rapid business process execution • Accelerates time to user productivity 	<ul style="list-style-type: none"> • Rapid user provisioning • Rapid integration into IT infrastructure • Enhanced IT skills with common processes and training
Enhanced protection	<ul style="list-style-type: none"> • Secure business processes • Security seen as enabler, not an inhibitor 	<ul style="list-style-type: none"> • Security from user access to back-end data • End-to-end enterprise coverage • Common view and reports for measurement, forensics, and compliance audits

Real-time Business Agility

First and foremost, an integrated identity and information security infrastructure must enable, rather than inhibit, new network-based business processes without increasing risk or complicating regulatory compliance efforts. To accomplish these goals, integrated identity and security must:

- **Get users productive—and keep them productive.** Think of automated user account provisioning as “table stakes” here. Basic identity tools must tie into HR systems, anchor workflow processes, and handle moves/adds/changes in a straightforward fashion. Superior systems will also define and manage roles/entitlements, keep users productive with enterprise password management based upon corporate policies, and tie into user access compliance tools that review access rights, detect control gaps, and guide IT administrators through remediation processes. The best identity tools will also interoperate with existing directory infrastructures rather than require a costly and complex directory overlay. Ultimately, the goal is to maintain productivity by making tasks like application authentication, password management, and management approval processes as automated and transparent as possible.
- **Accommodate non-employees.** As ESG’s research clearly indicates, moving forward, more and more users will be external constituents rather than employees. While external IT applications help the business, IT may be quickly overwhelmed if it is expected to provision external users via internal tools and processes. To align external business processes with IAM requirements, it is imperative that CIOs set up the right processes and technologies to accommodate federated identity. With the appropriate tools and support for federated standards, an integrated identity/security infrastructure can extend security, authentication, authorization, and user account provisioning to business partners and vice versa. When supported by the right contractual protection and IT/end-user training, federated identity can greatly accelerate external business initiatives without adding operations overhead or incremental risk.
- **Align access rights with business processes.** While most large organizations have standard security policies, IT utilization and risk tolerance varies greatly on a business process basis. For example, a health care facility will customize access rights and security policies depending upon whether business processes center around urgent care, prescription management, or administration. By marrying identity and information security, large organizations can create authentication and authorization policies based upon

additional factors such as location, time of day, and type of transaction. When a physician accesses patient records from the emergency room, she will be given immediate access based upon her RFI identity badge. When she prescribes painkillers for this patient, she may be asked for additional access verification before the transaction can be processed.

Ease of Use

Even in the most sophisticated IT shops, many business and IT managers would agree that current identity and security processes and tools are overly complex and cumbersome. Today's annoyances could quickly cascade into major impediments as the number of external users and network business processes skyrocket. Clearly, this must change quickly. To support growing business needs, identity and security integration "ease of use" must be drastically improved with:

- **Integrated command-and-control.** Today's patchwork identity and security infrastructure is anchored by a potpourri of management and reporting consoles that can't scale, coordinate change management, or offer common reporting. While a single management platform would be ideal, the reality in today's diverse, heterogeneous environment is that vendors must integrate disparate tools and technologies. In the short term, identity and security must be backed by integrated management tools that share information while coordinating configuration and change management operations. With identity and security integration, a security or compliance manager can evaluate user access rights or roles as they relate to sensitive data, like health information, in a common report. By viewing this data in a common report, they can easily take the necessary remediation actions like verifying access privileges with a business manager, adjusting policies, or modifying user access rights accordingly.
- **Wide support for applications and devices.** The history of IAM is plagued by limited software tools that demand complex and time consuming custom integration. CIOs should no longer put up with this burden. Rather, IAM systems designed for today's business requirement must provide "out-of-the-box" support for a wide assortment of business applications, security technologies, and hardware devices. For example, IAM tools should seamlessly plug into hard and soft authentication technologies for user provisioning as well as configuration and change management. Account and role management systems should work flawlessly with web access management systems that often control access to external applications. Internal systems should also support federated identity standards to simplify integration with external users and applications.
- **User self service.** Regardless of training efforts, many users will still need help with new identity tools, lose their security tokens, or forget their passwords. This usually ends with a help desk call carrying an associated cost of \$20 to \$50 each. Yes, it is important to provide adequate services for end-users, but user self service tools have demonstrated their value in accelerating problem solving and greatly reducing help desk call volume. The best identity tools provide an assortment of self service capabilities, such as password reset or business manager-based user provisioning. All of these capabilities bolster productivity while minimizing IT involvement.

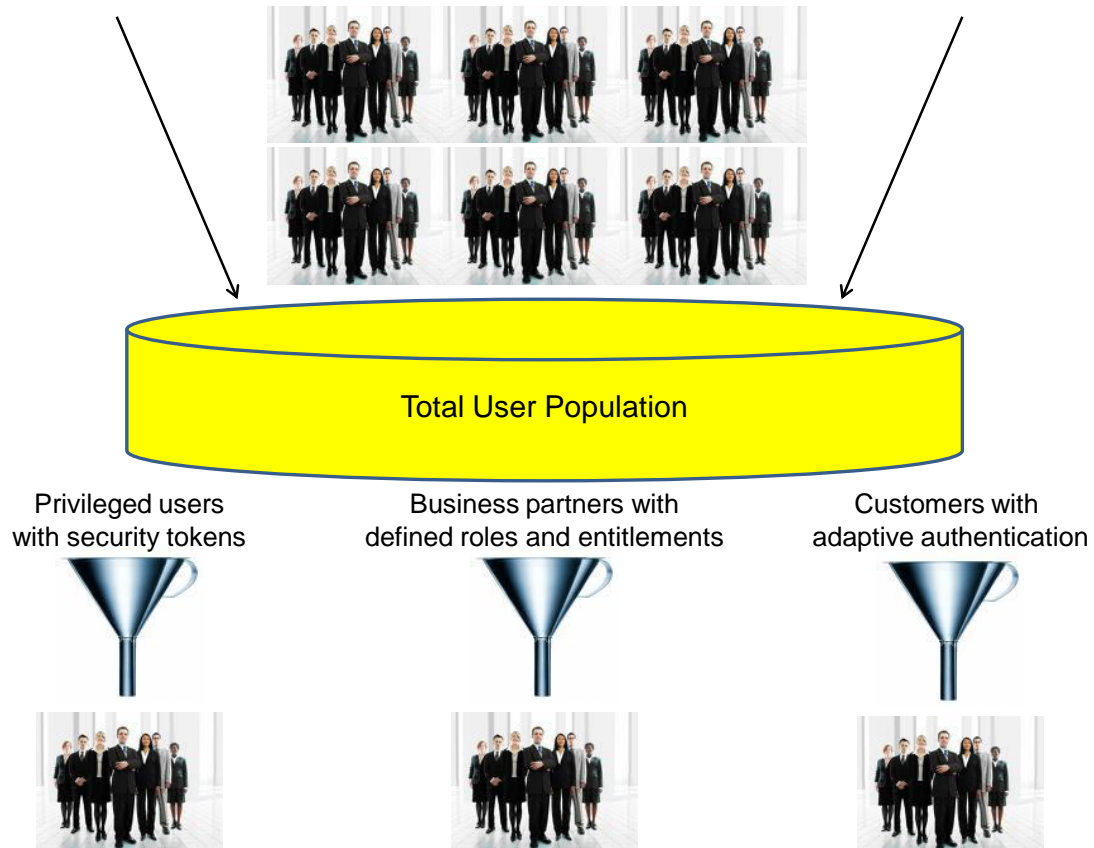
Enhanced Protection

Of course, the other side of accelerated business processes is risk management. More users, devices, network traffic, and web-facing applications have the potential to greatly increase security risk. To address these threats while supporting the business, identity and security integration must:

- **Support strong authentication and fine-grained access control.** To deal with issues around identity theft, users accessing sensitive or private data should use some type of authentication technology that offers greater security than a typical user name and password. Aside from standard account provisioning, this requires account management systems capable of provisioning one-time passwords or risk-based authentication technologies such as adaptive authentication (i.e., challenge/response systems), as well as application access-based rules based upon organizational risk posed by users, groups, or specific roles. This

functionality creates a “funnel effect” in order to segment the total population of users into more discrete, manageable, and secure sub-groups (see Figure 3).

Figure 3. Identity and Security Used to Segment Total User Population into Manageable Sub-groups



Source: Enterprise Strategy Group, 2009.

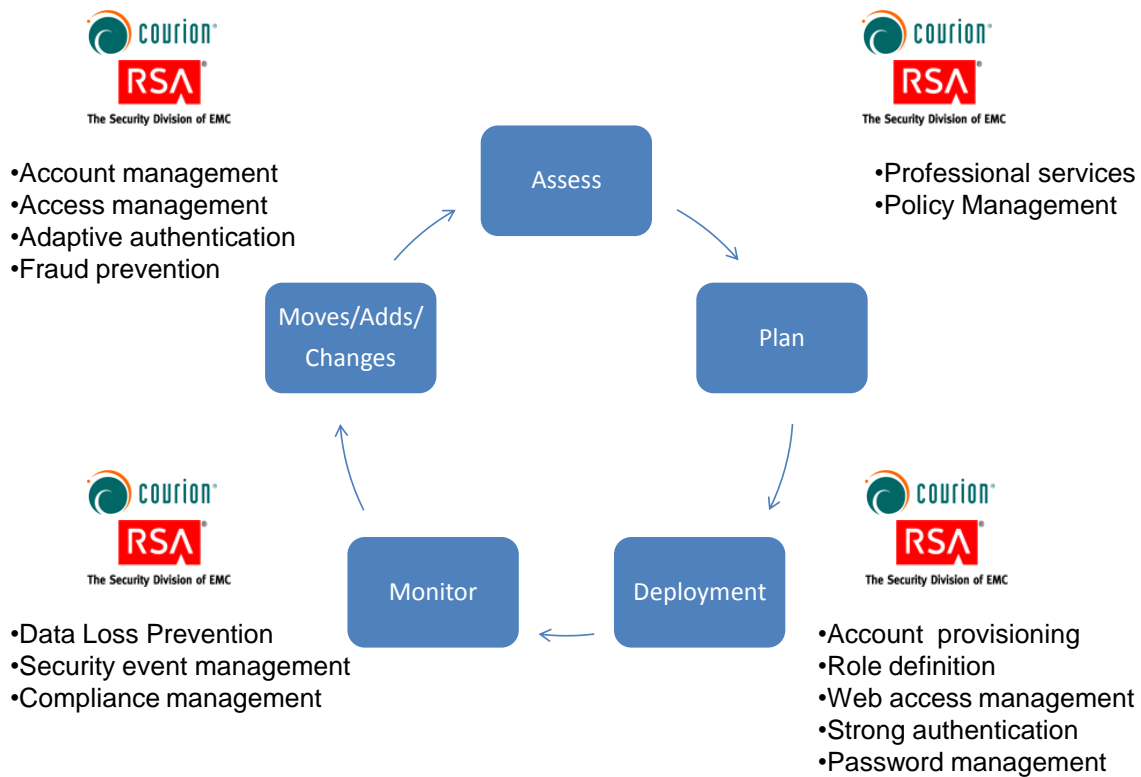
- Augment information security controls.** Entitlement management success depends upon data discovery, classification, and rights management. This is best accomplished with an integrated identity and security infrastructure that includes DLP in the data center, in the network, and on endpoints. In this scenario, DLP is used to scan and classify data repositories and apply data access rules that align with roles and security policies. In the best case, identity tools can support DLP by mapping confidential data files directly with user access rights. This helps apply a sense of context to access policies by mapping data classification with user roles. In this way, security administrators can ensure that only authorized personnel have access to sensitive data. When Margaret in HR tries to download the employee database, security administrators can quickly determine her identity and location and then take remediation actions to cut off her network access and cancel her account.
- Provide end-to-end monitoring and reporting.** Governance, risk, and compliance efforts depend upon a steady stream of real-time information to assess current status, detect anomalies or attacks, analyze events, and compile reports for management reviews or IT audits. Integrating identity and security with Security Information and Event Management (SIEM) can enhance current monitoring and reporting tools by linking security events to actual people and transactions. When Eddie in Sales suspects that he will be terminated soon and begins stealing customer information, security administrators will be able to link large file downloads to Eddie himself, rather than to a cryptic IP address. This capability is also extremely useful for security event detection and investigation. Managers can also use access certification and compliance management software to examine and validate that user access rights to sensitive data are consistent with the “least privilege” principle and that access is based on a clearly defined business purpose.

Taken together, these identity and security integration attributes can help CIOs achieve their biggest objectives: provide technology tools to accelerate the business while minimizing any incremental risks. Aside from these worthwhile goals, large organizations can experience some other significant benefits as well. First, they will be able to customize business processes and security policies based upon user or group attributes. For example, IT can create application features and provide secure access for only a handful of top customers to increase sales and customer satisfaction. This can lead to more creative and experimental applications. Finally, IT can greatly reduce the costs associated with IAM and security through greater use of automation, user self-services, and common management/reporting.

RSA and Courion are Leading the Way

Since users managed identity and security separately in the past, many technology vendors picked their battles in one area or another, so there are few integrated solutions to choose from. The story is actually worse than this, however. Many “integrated” identity and security solutions were either cobbled together through acquisition or depend upon basic interoperability between various vendor offerings. The RSA and Courion partnership offers an exception to this rule through its ability to create an end-to-end identity and access assurance infrastructure (see Figure 4).

Figure 4. RSA Security and Courion Support the Identity/ Information Security Lifecycle



Source: Enterprise Strategy Group, 2009.

Individually, the two companies offer best-of-breed identity and security products that combine to cover the full identity and access assurance lifecycle composed on user provisioning, role management, identity change management (Courion), web access management, strong authentication, federated identity (RSA), and compliance (Courion and RSA). Rather than simply partner, however, the two companies have taken their relationship to another level.

Initially, RSA and Courion integrated their identity management technologies for provisioning, access control, and strong authentication. More recently, the two companies expanded this relationship with information security integration as well. For example, RSA's Data Loss Prevention (DLP) suite and Courion's management tools can map identity information with data classification to determine who has access to sensitive data and ensure that access rights are based on business need and corporate policy. Finally, RSA enVision and Courion ComplianceCourier can be used to associate security events and sensitive data access with individual users, reducing the potential for spurious, time-consuming "false positive" alerts.

By working together on identity and information security, the RSA/Courion identity and access assurance infrastructure has become one of the most sophisticated available. Other identity firms lack information security capabilities or provide basic API or data exchange information with a variety of partners. Alternatively, RSA and Courion provide tight integration across identity and information security applications. This integration may be a blueprint for today's real-time business and stringent compliance requirements.

The Bigger Truth

Along with death and taxes, integration of identity and security is inevitable. CIOs must recognize this reality soon and address the current gaps between the two areas. While IT operations, compliance, and security groups will benefit from an integrated identity and security infrastructure, smart IT executives will make sure to work hand-in-hand on this transition with business managers as well. Use this as an opportunity for IT and the business to collaborate on things like data classification, user roles, self-service requirements, and workflow process improvements.

Smart CIOs will assess their current identity and information security tools and begin crafting a migration plan toward integrated identity and access assurance. To avoid past mistakes and move forward on a proactive basis, IT executives should:

- **Gain buy-in from the business.** As mentioned above, CIOs should use this project as an opportunity to get business managers involved. This means defining policies, data classification taxonomies, roles, and workflows and then aligning monitoring and enforcement technologies with clearly defined business processes. Make sure to define “ease of use” requirements as well, in order to deliver an identity and access assurance infrastructure that business managers will support.
- **Appoint and empower project managers.** Even if business and IT requirements are clearly defined, things will change as identity/security projects progress. Make sure that project managers have enough internal clout to manage through these changes. Savvy organizations will support project managers with business and IT executive oversight.
- **Require a proof of concept.** Make sure that identity and access assurance projects contain a proof-of-concept phase so project managers gain experience from a final test on functionality and usability by a broad group of business, IT, and security managers.
- **Look for “out-of-box” capabilities.** Even the best project can be detoured by months of custom software design, development, and testing. To avoid these interruptions, make sure to select tools that offer the broadest “out-of-box” support for application/device support, policy creation, custom reports, and information security integration. Vendors and reference accounts that provide nebulous information about multi-year implementation cycles, development tools, or vague information security partnerships should be viewed as a red flag.

Finally, software and services acquisition costs are important, but the real goal should be long-term TCO, risk reduction, and business enablement. Make sure to ask reference accounts for concrete data on how they’ve done in these areas.



Enterprise Strategy Group | **Getting to the bigger truth.**