

White Paper:

Securing Sensitive Information with Identity and Access Assurance



Table of Contents

1. IAM Business Drivers	3
1.1 Compliance	3
1.2 Security	3
1.3 Operational Efficiency And Productivity	3
1.4 Cost Containment	4
1.5 User and Manager Convenience	4
1.6 Business Effectiveness	4
2. Access Assurance – Extending the Identity Management Lifecycle	5
2.1 Define Policy	5
2.2 Apply Policy	7
2.3 Detect Activity	7
2.4 Remediate Violations	9
2.5 Validate Compliance	10
3. The RSA/Courion Solution	10
3.1 Policy Definition	10
3.2 Managing Access & Authentication	11
3.3 Compliance Management	12
4. The Benefits of Access Assurance	14

1. IAM Business Drivers

Identity and access management (IAM) is a combination of business and information technology (IT) practices designed to ensure that only the right people have the right access to the right resources and are doing the right things.

While different organizations may place varying emphasis on different business drivers for implementing an IAM solution, in general, there are six principle factors underlying their reasons for doing so.

1.1 Compliance

Government and industry regulations, such as Sarbanes-Oxley, HIPAA, GLBA, Basel II, European Data Protection Act, Data Privacy Act (UK) and PCI DSS, have all had a significant impact on organizations worldwide. What these and other regulations have in common is a requirement to develop and implement policies and controls to ensure only authorized users are provided access to certain classes of sensitive data (financial records, personal health information, Social Security numbers, credit card numbers, etc.)

Organizations seeking to address the challenge of complying with these requirements need a way to:

- Discover and classify sensitive data
- Define policies as to how sensitive data can be handled and by whom
- Secure access to sensitive data
- Monitor for compliance on a regular basis

1.2 Security

For many years the focus of security personnel was to protect the network perimeter. However, increased awareness concerning the risks posed by insiders who have the ability to expose sensitive data, whether out of malice or ignorance, has become a core focus for many IT departments.

According to a study conducted by the Ponemon Institute, insiders caused 75 percent of all data breaches in the U.S. As a result, defining policies and establishing controls to both access and data has become a focal point for organizations seeking to protect against insider security threats.

Implementing stronger identity and access and data controls to ensure that the right people have the right access to the right resources and are doing the right things can help organizations maintain the integrity of their sensitive information.

1.3 Operational Efficiency And Productivity

Automating identity and access management (IAM) processes provides substantial return on investment due to improvements in operational efficiency and enhanced productivity. Most large organizations suffer from a plethora of heterogeneous automated systems, which can impact productivity as users struggle to deal with different sign-on mechanisms.

- New hires can be automatically provided with secure access to the resources and systems they require to become useful on day one;
- Self-service password management enables those who have forgotten their account password to reset them without calling the help desk for assistance;
- Transparent password synchronization enables users to use a single user ID and password combination to access heterogeneous systems, which speeds up log on time and reduces the temptation for users to resort to insecure practices, such as writing down passwords and sticking them on a computer monitor or under a keyboard.

1.4 Cost Containment

Companies report a variety of ways that costs are reduced by implementing key IAM technologies, such as self-service password management or user account provisioning. One way is that identity-related calls to the help desk plummet by as much as 80% or more, which can very quickly translate into large, ongoing cost savings. A major Fortune 100 manufacturing firm, for example, estimates that it is avoiding 70,000 help desk calls per month, resulting in a reduced help desk staff and approximately \$8.4 million in annual, recurring savings.

Other firms report huge savings resulting from automation that enables them to dedicate fewer personnel to provisioning, managing and terminating user accounts.

1.5 User and Manager Convenience

Users who find themselves locked out of their systems because of a forgotten or expired password find it much more convenient to use a self-service solution to reset the password, rather than phoning the help desk and waiting for either the help desk or a system administrator to reset the password. This can be particularly problematic if the help desk isn't open all hours, if the user is located at a remote facility, or if the system administrator isn't available because he or she is handling some other problem.

Managers who have tools to automatically establish, modify or revoke user identities and access rights on business systems for users under their control, greatly appreciate no longer needing to fill out and submit multiple paper forms and wait for days to provision a new hire. Automated compliance reporting and attestation tools can make life significantly easier for busy professionals by reducing the amount of time and effort required to review, validate and attest that employee access rights are consistent with corporate policy and industry regulations.

1.6 Business Effectiveness

Most companies go through three stages of process maturity as they become more familiar with IAM.

In the *efficiency* stage, companies are primarily looking to cut costs or pass an audit. However, as their IAM programs mature and as more and more companies become subject to regulatory compliance, greater attention is paid to the *effectiveness* benefits of adopting IAM. Moving to the

effectiveness stage implies incorporating security deeper into business processes and delivering stronger automation of access management and compliance controls. Finally, in the most mature programs, the focus shifts from efficiency and effectiveness to business performance and *enablement*. Achieving the enablement stage means that IAM and security technologies are driving business process optimization and acceleration, resulting in greater security transparency.

2. Access Assurance – Extending the Identity Management Lifecycle

Traditional IAM has been perceived as the process of managing users' identities and access rights. Access Assurance has emerged as a broader concept that extends the traditional IAM lifecycle to include user activity and compliance management.

Access Assurance is ensuring that only the right people have the right access to the right resources and are doing the right things.

Delivering Access Assurance involves managing the interactions between people (or automated systems), their access rights to various systems, and the activity they engage in on those systems, all governed by corporate security and compliance policies (See figure, below.)

The five key stages of the Access Assurance lifecycle are:

- Define policy
- Apply policy
- Detect actions or access activity that violates a policy
- Remediate any misuse or non-compliance with policy
- Validate and attest that policy has been implemented effectively

2.1 Define Policy

Organizations looking to define their Access Assurance policies need to consider a complex array of factors such as their business requirements, security maturity, company size, and industry profile, and regulatory drivers.

Some of the core elements that drive policy definition include:

- Discovering and classifying sensitive information and determining its business value;
- Establishing who has access rights to certain data, based on principles such as least privilege or segregation of duties;
- Determining who has authority to grant/revoke access rights.

Data Loss Prevention (DLP) technology is focused on identifying where sensitive data resides and classifying that data according to its business value.

While specific industry requirement, government regulations, and corporate standards determine what information is considered sensitive, proprietary or protected, common examples include:

- Personally identifiable information such as name, maiden name, mother’s maiden name, date/place of birth, Social Security number, passport number, driver’s license number, taxpayer ID number, patient or identification number
- Personal financial information such as bank account number, PIN, or credit card number
- Protected health information such as medical history, hospitalizations, medications, treatments, procedures or diagnosis
- Information identifying personal property such as vehicle registration or identification number, title numbers and related information
- Proprietary business processes, trade secrets, formulas, customer lists, product plans and roadmaps, company financials and schematics

Upon discovery and classification of data, policies must be defined – the rules for 'appropriate handling' of the data – including which users and applications are authorized to access this data and how, when, and from where they are allowed to access it.

Once data policies have been established, organizations must consider a number of principles to define access rights. One of the most basic is the principle of least privilege, which states that users should hold the minimum access rights necessary to complete effectively perform their business function.

Another core principle to consider is segregation of duties (SoD) which ensures that no single person can complete all the steps of a vital business process.

Most examples of SoD are related to finance, such as the notion that the person who creates a purchase order cannot also have the authority to approve it or sign the check. However, SoD principles are also being used in other areas of the business, such as the IT department. For example, some organizations are establishing policies that a software developer cannot also have the right to validate an applications security profile or install it into a production environment.

Another policy area is defining who may approve, manage and monitor access to sensitive data, as well as creating processes to ensure only the appropriate personnel can approve and enable access rights. For example, a manager of a new hire may have the authority to approve that person’s access to email or the network, but will need VP-level approval before access to systems containing sensitive data is enabled.



Figure 1 The Access Assurance Lifecycle

Finally, the organization should consider how various business roles are aligned with specific IT accounts and entitlements. What applications and access rights should a senior teller in a bank have that a junior teller does not? Which roles in the finance department should be able to perform certain business functions, such as accounts payable/receivable, general ledger, or checking account reconciliation? While a role management lifecycle solution is not *required* in order to implement an Access Assurance strategy, defining business roles and their associated IT applications makes it easier to determine and enforce policies concerning access rights and entitlements.

2.2 Apply Policy

Once policies are defined, the organization can begin to apply policy according to the user and the resource. It is important for organizations to implement policies that combine both data and access controls to ensure the most comprehensive protection. For example, if access rights are provided to resources where sensitive data is contained, yet the organization is not aware of its existence, the opportunity for exposure increases.

For data, applying policy means specifying the usage and handling rules based on the sensitivity of data. Policies are important for determining when a violation has occurred and how that violation should be handled (alerting, blocking, encryption, etc.). For access, organizations can apply policy through provisioning which is the creation of IT accounts and access entitlements on various systems.

2.2.1 Provisioning and Entitlements

The provisioning process can be relatively simple or complex, depending on who is being provided access rights, the sensitivity of the system being accessed, and the procedures required to authorize the creation of the accounts.

Manually provisioning accounts is a slow, cumbersome process that requires the manager to fill out a paper or email form, send it to the IT help desk or system administrator, who then creates the account (user name and password), and reports back to the manager. In large organizations, this process can literally take days to complete and the potential for error is very high.

Automating access to corporate assets (email, network servers, databases, devices, etc.) can be performed by a workflow initiated by an authorized requester (such as a manager) or as part of a lights-out process initiated by a trigger event, such as a new hire record being added to a PeopleSoft system. An automated process can complete in minutes, and delivers a higher level of assurance that the account has been correctly established.

2.2.2 Role Management

Some organizations have embraced role-based access controls (RBAC), and use roles to determine the entitlements that the new user will have on various systems. The combination of role management and provisioning delivers faster service, at lower cost, and with a higher level of assurance that the user's access rights are consistent with the needs of the business and relevant regulations.

2.2.3 Authentication & Authorization Mechanisms

Once accounts have been established, along with their respective entitlements, the organization relies on authentication technology to ensure that the user is who they say they are before granting access.

Almost all organizations rely on the authorization system of a target system (such as a desktop PC, network operating system, database, or enterprise application) to challenge the user with a user-name and password prompt, which they must satisfy before they are granted access to the system.

Many organizations rely on an enterprise repository which can be used by multiple systems for authentication. Others deploy a single sign-on system which can transparently manage the user's access to multiple systems, reducing the number of times a user is required to re-authenticate.

Web access management solutions are essential for organizations with web-based mission-critical applications that require users to authenticate their identity through a browser. Other organizations rely on federation solutions in order to provide external users, such as business partners or customers, with secure access to data.

Multi-factor authentication is essential for organizations that require stronger security controls than a username/password combination. Some of the more common multi-factor authentication solutions used by organizations today to assure user identities are one-time password authentication and risk-based authentication. One-time password authentication is based on something the user knows (such as a PIN number) and something the user has (an authenticator). Risk-based authentication analyzes a series of factors such as device forensics, IP geo-location, and user behavioral profiles to authenticate a user.

2.3 Detect Activity

While traditional IAM solutions stop at the authentication and authorization stage, Access Assurance goes beyond IAM to include mechanisms for detecting and analyzing user activity to ensure users are not engaged in prohibited or insecure practices.

2.3.1 Compliance Management

A complete description of compliance management in a large complex organization is beyond the scope of this document, but there are steps commonly used by compliance managers who are concerned with protecting sensitive data from unauthorized access and disclosure.

Most large organizations give line-of-business managers the primary responsibility to review, manage, attest, and report on access rights for the employees or users within their sphere of operations. Some organizations place the responsibility for compliance management with specialized functions, such as IT Audit or a Security Office, however, these organizations often lack the business acumen and operational knowledge required to effectively determine if a particular user's access rights are legitimate and consistent with policy.

Enabling operational managers to apply their specialized business expertise to the compliance management process also leverages their interest in ensuring the business unit runs smoothly and efficiently.

2.3.2 Monitoring Activity and Access

Data loss prevention (DLP) and security incident and event management (SIEM) technologies play an increasingly important role in the compliance management and attestation process by allowing ongoing monitoring of user activity and access.

Just as DLP solutions are designed to identify and classify sensitive data on a variety of systems, they also enable organizations to be proactive in protecting sensitive data from unauthorized access or use by applying various remediation options if a policy is violated. For example, an IT administrator can be alerted when highly sensitive data is sent outside the network by a user.

SIEM systems enhance security and data protection by monitoring user activities and capturing the data in log files as a record of security events, information access and user activities which can be used in both real-time or for forensic analysis should a high-risk event occur.

Identity and access management systems complement DLP and SIEM systems by adding an identity component that enriches the DLP/SIEM system with detailed, specific information about users who have potentially, or actually, accessed sensitive data and what they did with the data. Access Assurance combines data from DLP, SIEM and IAM systems, giving managers and administrators the ability to quickly and efficiently determine that only authorized users have accessed sensitive data and take remedial steps in the event an unauthorized user accesses sensitive data unwittingly.

2.4 Remediate Violations

Evaluating user activity and access rights provides managers with the data they require to determine if user rights are not aligned with corporate policy or best practices (such as least privilege), and take the appropriate steps to bring those rights back into alignment. Remediating access violations entails modifying, suspending or revoking a users access rights to systems, applications or data.

Most remediation scenarios result from a change in a user's status or a change in policy. If a user changes roles (for example, a promotion or transfer), it is appropriate to evaluate the rights the user will require in the new position, and whether the user should retain some, or all, of the entitlements they held in the previous one. Not remediating rights as users move from one role to another can result in rights accumulation with potentially serious consequences. In one notorious case, Jérôme Kerviel, a trader at Société Générale, used rights he retained from a previous position in the compliance group to cover up unauthorized trades, which resulted in the bank eventually losing €4.9 billion.

Another common scenario arises when there is a major restructuring due to a merger or reorganization. All too often, companies forget to re-evaluate and remediate user access rights, either for new users entering the workforce as the result of a merger or for employees whose roles are changing in a reorganization.

Finally, when an employee (or other user) leaves the organization, their ability to access corporate assets should be immediately suspended or terminated, depending on the circumstances of their departure.

A zombie account (also called a dormant or orphan account) is an account that remains active after an employee leaves the organization. Automatically removing or disabling zombie accounts

eliminates the potential for terminated employees to engage in malicious behavior. In one particularly brazen example, a former auditor at the California Water Service Company in San Jose used a zombie account to log on to a financial system the evening after he was terminated to transfer \$9 million to an offshore bank account.

2.5 Validate Access

The final step in the Access Assurance lifecycle is the ongoing validation and attestation of user access rights.

Despite the recent economic downturn, auditors and regulators are not reducing their demands for compliance attestation and reporting. In fact, many industry observers expect that demands by government and other regulators will likely increase in certain industries, such as financial services, as a direct result of the recent increase in bank failures and corporate bankruptcies.

Validation of compliance with relevant regulations is becoming increasingly important as various industry organizations and government bodies mandate that companies periodically attest that internal access controls are both appropriate and adequate. Automating the compliance validation process brings two major benefits.

First, it enables managers to quickly and easily confirm that employees have entitlements that are appropriate to their business function. A properly implemented compliance validation process enables managers to reliably report to auditors and other concerned stakeholders that controls are in place to restrict individuals from accessing sensitive data or performing business operations that violate corporate policies, such as segregation of duties.

Second, the amount of effort required to create reports for auditors and regulators can be significant. For a large entity with thousands of employees, the expense of collecting, consolidating, analyzing and reporting on compliance with Sarbanes-Oxley or HIPAA access requirements, for example, can literally run into millions of dollars.

Even beyond the need to meet the demands of auditors, the true spirit of compliance validation is to make compliance a seamless, transparent part of routine business activities. Automated compliance eliminates the disruption caused when managers must focus their attention on compliance reporting and attestation.

Making compliance and validation reporting an ongoing, transparent part of business operations that automatically ensure users only have access rights appropriate to their specific job functions, reduces wasted time and effort and enables the business to run more effectively.

3. The RSA/Courion Solution

RSA®, the Security division of EMC, and Courion® Corporation have teamed up to deliver a complementary array of industry-leading products and services that deliver the benefits of Access Assurance to enterprise customers.

3.1 Policy Definition

The Courion **Access Assurance Suite™** includes a number of products that combine seamlessly with RSA solutions to implement the Access Assurance lifecycle.

AccountCourier® is Courion's user provisioning solution that automates the process of creating and managing user accounts and access rights across a wide range of host-based and web-based systems, platforms and applications. **RoleCourier®**, also from Courion Corp., is a role management solution that simplifies security and access policy enforcement by creating user roles that align business functions with IT accounts and access rights. AccountCourier and RoleCourier are used to define access policies that ensure users only have the access rights to sensitive information necessary to perform their job duties, and both products work seamlessly with RSA's authentication and authorization products to enforce those rights.

RSA Access Manager is designed to enable organizations to manage large numbers of users while enforcing a centralized security policy that ensures compliance, protects enterprise resources from unauthorized access and makes it easier for legitimate users to do their jobs. The **RSA Data Loss Prevention Suite** provides a policy-based approach to securing sensitive data, enabling customers to classify their sensitive data, discover that data across the enterprise, enforce controls, and report and audit to ensure compliance with policy.

3.2 Managing Access & Authentication

PasswordCourier®, Courion's password management solution, provides self-service password reset and synchronization across a wide variety of enterprise systems. PasswordCourier is the industry standard for secure, self-service password management, featuring multiple access options, robust service desk integration, and the ability to enforce consistent password policies on any system, application, or Web portal. PasswordCourier features include: multiple user access options for password reset, comprehensive password synchronization options, strong enterprise password policy enforcement, integration with popular service desk applications.

RSA Access Manager delivers secure access to Web applications in intranets, extranets, portals and exchange infrastructures. With RSA Access Manager, organizations assign access privileges to ensure that only authorized individuals (e.g. employees, contractors, citizens) can access sensitive information within web-based applications – ensuring the right people have the right access at the right time. These privileges can be determined by select attributes, such as job function and responsibilities, and can be readily turned off if a person is terminated or takes on a new job role that does not require access to sensitive information. In addition, end users benefit from single sign-on (SSO) to multiple resources while the enterprise protects access to mission-critical Web resources.

RSA SecurID® two-factor authentication is based on something you know (a PIN or password) and something you have (an authenticator). The authenticator generates a new one-time password code every 60 seconds, making it very difficult for anyone other than the genuine user to input the correct code at any given time.

To access resources protected by the RSA SecurID system, users simply combine their secret personal identification number (PIN) with the unique one-time code displayed on their authenticator at that particular time. RSA SecurID authentication offers a wide array of one-time password authentication form factors including hardware authenticators, software authenticators for mobile devices and a software toolbar. Courion's AssetLink™ technology, part of the Courion Access Assurance Suite, is used to provision and de-provision users with the RSA SecurID system.

RSA® Adaptive Authentication is a strong authentication and fraud detection platform that offers cost-effective protection for an entire user base. Adaptive Authentication secures access to:

- Websites & portals
- SSL VPN applications
- Web Access Management applications

Adaptive Authentication leverages risk-based authentication technology to conduct a risk assessment of all users behind-the-scenes. Adaptive Authentication measures over one hundred risk indicators, including a user's device, IP geo-location, and behavioral patterns, to positively assure a user's identity. A unique score is assigned to each activity. If the activity falls below the risk threshold established by the organization, the user is permitted to proceed without interruption. If an activity exceeds a predetermined risk threshold (as customized by each organization), the user is prompted to provide an additional authentication credential to be granted access.

RSA Federated Identity Manager is an enterprise-ready, flexible identity federation solution that enables enterprises to securely exchange user identities between disparate internal business units and with customers and partners, utilizing the latest industry standards. It allows organizations to unlock the true potential of business relationships while maintaining consistent and centralized control over the policies associated with users and applications. Designed to be fully standards-based and compatible with other systems, it is based on the latest web services standards, including XML, SOAP, and SAML 1.1, SAML 2.0, and WS-Federation 1.0. With RSA Federated Identity Manager, organizations can easily integrate, configure and use, and obtain more options for securely federating both employee and consumer identities.

Courion's Access Assurance Suite acts as the control center that, based on business policy, enables or disables user access through the various RSA authentication and authorization solutions for a wide variety of computing systems and applications.

3.3 Compliance Management

The **RSA Data Loss Prevention Suite** offers a comprehensive data loss prevention solution that discovers, monitors and protects sensitive information whether at rest in a data center, in motion over the network or in use on a laptop or desktop. The RSA DLP Suite provides a policy-based approach to securing sensitive information data, enabling organizations to classify their sensitive data, discover where it resides, enforce appropriate controls, and report and audit appropriately as mandated.

The RSA Data Loss Prevention Suite is offered in three distinct modules:

Module	Functionality
RSA Data Loss Prevention Datacenter	Identifies personal information and other sensitive data stored across file shares, SAN/NAS, databases, and other data repositories such as content management systems. Once sensitive data is discovered, RSA DLP Datacenter allows organizations to apply policy-based remediation actions, such as quarantining or moving a file to a secure location.
RSA Data Loss Prevention Network	Identifies and controls sensitive data as it is transmitted throughout the network and enables policies to be enforced across areas such as corporate email systems, web-based email systems, instant messaging, and web-based protocols. RSA DLP Network can identify sensitive information through the analysis of the data inherent in a transmission and prevents data loss by blocking or encrypting such transmissions should they violate a defined security policy.
RSA Data Loss Prevention Endpoint	Identifies and controls sensitive data on endpoints such as laptops and desktops. RSA DLP Endpoint has the capability to monitor the usage and movement of sensitive data on laptops and desktops, even as it is moved to external media such as USBs or CD/DVDs. RSA DLP Endpoint can enforce and control end user actions that violate policy through blocking, encryption or other file control mechanisms.

In addition to a range of DLP solutions, RSA offers RSA enVision®, a SIEM solution that turns raw log and event data into actionable information to help organizations identify and respond to high-risk events and simplify reporting requirements. The RSA enVision platform offers comprehensive correlation, analysis, monitoring and alerting capabilities to make it easy to consolidate and review daily logs from different systems, including logs from all critical intrusion detection, authentication, authorization, and accounting protocol servers.

RSA enVision establishes a centralized point for tracking and monitoring access to sensitive information and systems – from the users that access it to the activities they perform – and if those attempts are valid. With the RSA enVision platform, organizations can create custom watch lists to look for multiple login failures or other security-related events that may be deemed potentially suspicious, whether successful or not.

In the case of a high-risk event, RSA enVision delivers automatic notifications to assigned security personnel in real-time, who can then use identity information available through the Courion Access

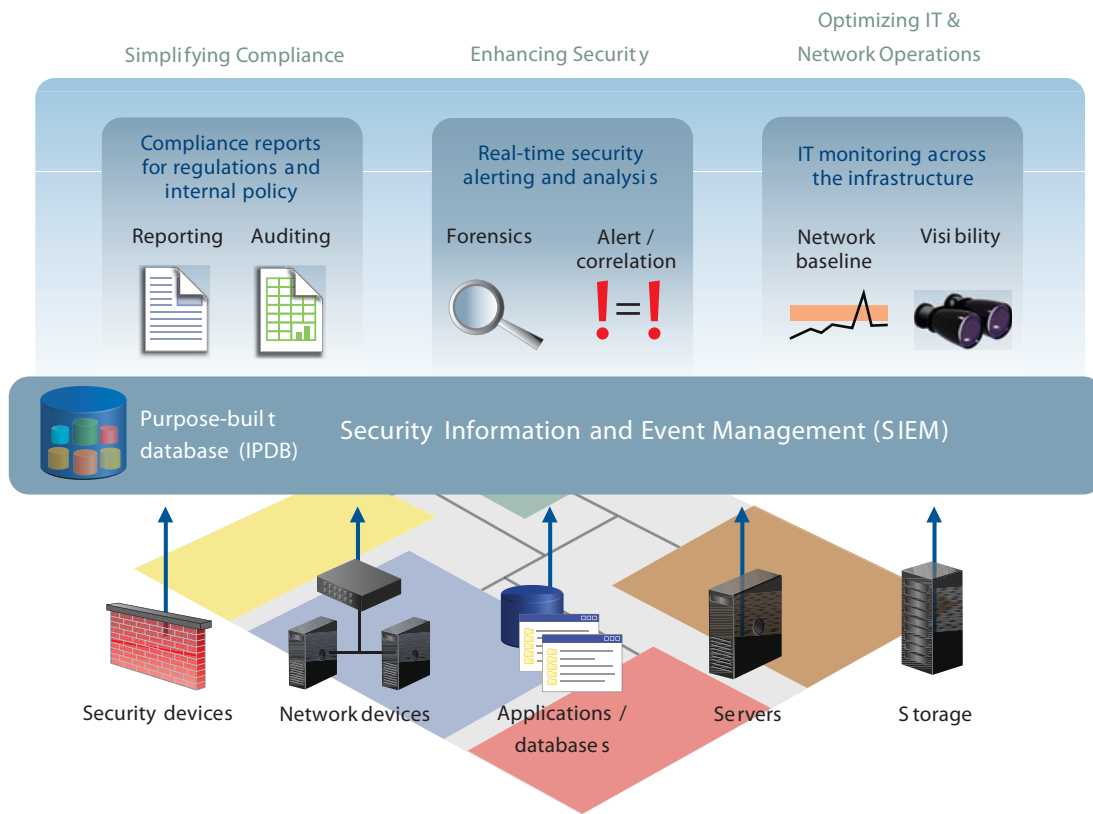


Figure 2 SIEM Architecture

Assurance Suite to quickly and easily assess which users are engaged in activities that are not consistent with the business and security policies of the enterprise. They then can take the appropriate measures to resolve these issues by, for example, remediating the individual's access rights.

Finally, **ComplianceCourier™**, Courion's access, audit and policy compliance software, provides a solution for automating the analysis of user access rights, as well as tying critical application access to passing policy awareness tests as ways to proactively meet regulatory requirements.

ComplianceCourier enables business managers to periodically engage in audit compliance by reviewing and verifying employee access rights and attesting that employee access rights are consistent with policy and regulatory requirements. Automating policy verification helps ensure compliance with key mandates, such as industry or government regulations, while simultaneously reducing operational costs.

4. The Benefits of Access Assurance

Organizations looking to ensure only the right people have the right access to the right resources and are doing the right things need to take a close look at the value of adopting an Access Assurance strategy. Adopting an Access Assurance strategy that fits the needs of your business and implementing the solutions described above allows you to:

- Personally identifiable information such as name, maiden name, mother's maiden name, date/place of birth, Social Security number, passport number, driver's license number, taxpayer ID number, patient or identification number
- Personal financial information such as bank account number, PIN, or credit card number
- Protected health information such as medical history, hospitalizations, medications, treatments, procedures or diagnosis
- Information identifying personal property such as vehicle registration or identification number, title numbers and related information
- Proprietary business processes, trade secrets, formulas, customer lists, product plans and roadmaps, company financials and schematics

About RSA

RSA offers enterprises a wide range of user authentication options to help positively identify users before they interact with mission-critical data and applications. With more than 20,000 customers worldwide and a 20-plus year history of outstanding performance and innovation, RSA's authentication solutions remain an industry standard for organizations looking to protect their key business data assets. For more information, please visit our website at www.rsa.com.

About Courion

Courion's award-winning Access Assurance solutions are used by more than four hundred organizations and over 7.5 million licensed users worldwide to quickly and easily solve their most complex identity and access management (password management, provisioning, and role management), risk and compliance challenges. Courion's business-driven approach results in unparalleled customer success by ensuring users' access rights and activities are compliant with policy while supporting both security and business objectives. For more information, please visit our website at www.courion.com.



The Security Division of EMC

US Headquarters
RSA, The Security Division of EMC
 174 Middlesex Turnpike
 Bedford, MA 01730
 phone +1 877 RSA-4900
 fax +1 781 515-5010
www.rsa.com



Worldwide Headquarters
Courion Corporation
 1881 Worcester Road
 Framingham, MA 01701 USA
 phone +1 508 879-8400
 fax +1 508 879-8500
www.courion.com

© 2009 RSA Security. All rights reserved. RSA, The Security Division of EMC, provides Secure Data, Compliance, SIM, SEM, SIEM, PCI, Consumer Identity, Two-Factor Authentication, Custom Applications, Consulting, Assessment, and other security solutions and services to over 90% of the Fortune 500.

Copyright © 2009 Courion Corporation. All rights reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Courion, the Courion logo, RoleCourier, Enterprise Provisioning Suite are registered trademarks or trademarks of Courion Corporation. All other company and product names may be trademarks of their respective owners.