courion®

Courion Perspective

Access Assurance

Ensuring only the right people have the right access to the right resources and are doing the right things.

In the face of a worldwide economic slowdown, companies and other organizations are increasingly challenged to improve efficiency and effectiveness. At the same time, the impact of government regulations and industry requirements is not lessening. The identity and access management market has evolved from its early focus on password management to today's focus on Access Assurance.

Access Assurance is a unique approach that ensures only the right people have the right access to the right resources and are doing the right things. This white paper defines the Access Assurance lifecycle and identifies three core components—Access Governance, Access Provisioning and Access Compliance—which enable companies with even the most complex, heterogeneous environments to increase operational efficiency and transparency, strengthen security and improve compliance, while delivering lower total cost of ownership.

www.courion.com

Table of Contents

Business Challenges

It’s become almost a cliché that businesses are increasingly challenged by the need to improve efficiency and effectiveness in today’s difficult economy.

Cost Pressures

Organizations—large and small—in multiple industry sectors are under tremendous financial pressure. According to the Bureau of Economic Analysis, “Real gross domestic product – the output of goods and services produced by labor and property located in the United States – decreased at an annual rate of 6.2 percent in the fourth quarter of 2008.”[1]

Sectors that have been particularly hard hit by the downturn include financial services, manufacturing (especially automotive), construction and retail. For example, insurance giant AIG reported a net loss of $61.7 billion for the fourth quarter of 2008 (the largest single quarterly loss in American history), while once-mighty General Motors and Chrysler are facing bankruptcy.

Many organizations are responding to these challenges by reducing head count through layoffs or employee attrition. As a result, the US and other major economies are grappling with unemployment rates approaching levels that haven’t been seen in decades. U.S. unemployment rose to 7% in 2008 and in January 2009 the U.S. Bureau of Labor Statistics reported, “Since the recession began in December 2007, 3.6 million jobs have been lost, with about half of the decrease occurring in the last 3 months.”[2]

Given these economic pressures, many companies are struggling to do everything they can to maintain fiscal stability and remain viable. Different companies are taking differing approaches to respond to the recent economic downturn, but one thing all these strategies have in common is the need to do more with less.

Regulatory Pressures

At the same time, the regulatory environment continues to impact businesses, requiring them to exert significant effort to comply without necessarily delivering greater business value. These regulatory pressures are converging from two different sources: government regulations and industry requirements.

Government regulations in the United States are affecting businesses at the local, national and international level. States like Massachusetts and California have enacted legislation mandating that organizations collecting personal information about their citizens take specific steps to protect that data from unauthorized exposure. At the national level, organizations are affected by the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act (SOX). And, as companies extend their business operations into international markets, they need to meet data privacy and protection requirements promulgated by the interna-

[1] http://www.bea.gov/newsreleases/national/gdp/gdpnewsrelease.htm

[2] http://www.bls.gov/news.release/pdf/empsit.pdf

tional banking regulators (BASEL II), the United Kingdom (Data Privacy Act), the European Union (European Data Protection Act), and other relevant authorities. Meeting the requirements of these mandates is essential, since many of them carry serious penalties, including civil fines and penalties or even criminal prosecution in the event of a breach.

Industry-specific requirements are also driving organizations to spend large sums of money and energy to deliver infrastructure that enables them to be compliant. Probably the most widely known example is the Payment Card Industry Data Security Standard (PCI DSS), which affects any organization that accepts credit or debit cards. Similarly, the electric power industry is affected by rules published by the North America Electric Reliability Corp. (NERC).

Regulation	Scope	Requirement
BASEL II	International – financial institutions	Requires financial institutions to install internal systems of control, including authorization and authentication, activity controls, segregation of duties, compliance checking, etc.
Data Protection Act 1998	International – all companies doing business in the UK	Establishes principles protecting personal data against unauthorized or unlawful processing, loss, destruction or damage.
European Data Protection Act	International – all companies doing business in the European Union	Establishes principles protecting personal data against unauthorized or unlawful processing, loss, destruction or damage.
The Federal Information Security Management Act	U.S. – federal agencies	Requires agencies of the U.S. Federal government to implement programs to protect the information systems and data required to support the agency.
Gramm-Leach-Bliley Act	U.S. – financial institutions	Requires implementation of information security policies that protect clients' nonpublic personal information.
Health Insurance Portability and Accountability Act	U.S. – organizations controlling protected health information, such as providers and insurance companies	Organizations handling protected health information must establish procedures controlling access authorization, establishment, modification and termination.

Regulation	Scope	Requirement
North America Electric Reliability Corp.	U.S. and Canada – electric power utilities	Requires power utilities to document and implement a program for managing access to protected information, and perform an annual review to confirm that employee access privileges are correct and correspond with appropriate roles and responsibilities.
Payment Card Industry Data Security Standard	International – all companies accepting payment cards	Requires that each person with computer access be assigned a unique ID. Access to cardholder data is restricted to those with a business need-to-know. Access to cardholder data must be tracked and monitored.
Sarbanes-Oxley Act	U.S. – public companies	Requires companies to establish and attest to access controls over financial systems.

What these regulations all have in common is that they require organizations to implement processes and procedures designed to protect sensitive information from compromise. While each act or regulation comes at the data protection problem from a different perspective, they all strive to ensure that only the right people have the right access to the right data and are doing the right things with it.

The Role of IAM

Virtually all modern organizations depend on various computer systems to perform vital business activities. These include a heterogeneous array of desktop and mobile computers, servers, databases, networks, file shares, middleware, collaboration tools, web sites, enterprise portals, and a host of enterprise applications (HR, finance, manufacturing, healthcare, logistics, etc.)

In order to perform their functions, employees (including temps, contractors, partners, and even customers) need access to accounts on relevant systems with privileges that govern what data the user can access, what they can do with the data, which application modules they can utilize, etc.

Identity and access management (IAM) includes the processes, procedures and technologies required to define, create, manage and terminate these accounts. It has become clear that automating IAM is fundamental to cutting costs, while simultaneously improving compliance with relevant security mandates.

The IAM marketplace has been a distinct, recognizable segment of the enterprise software marketplace for over a decade. As is the case with most information technology markets, it has evolved during that time from relatively modest beginnings to a significant market that has developed its own ecosystem.

During the mid-1990s, IAM began with password management. Companies developed technologies that made it possible for network and system administrators, help desk operators and, eventually, users to manage users' access to systems. Password management software reduces the time, effort and cost of managing user passwords and helps ensure that passwords were consistent with security polices (i.e., password length, strength, password expiration, reuse, use of dictionary words, etc.)

While password management software helped reduce the amount of effort and time required to manage passwords, the initial accounts still had to be created manually. Eventually, around the 2000 timeframe, the market expanded to include automated provisioning, which helps companies to define enterprise access management policies and simplify the process of creating accounts using those policies. Provisioning not only helps ensure consistent access policies, it also cuts costs by enabling organizations to add, edit, and delete end user accounts using fewer personnel than were required to perform these functions manually.

Over the past few years, new capabilities have emerged. One is role management, which helps accelerate the provisioning process, making it more repeatable and consistent and reducing the time and effort required to provision accounts. Now, managers can provision a new employee quickly by simply assigning the new employee to a pre-defined role.

Another is compliance management, which has emerged in response to the increased emphasis on enforcing compliance with industry requirements and government regulations. Companies that install an automated compliance reporting and management solution find they can meet auditor demands for data, while significantly reducing the effort and cost required to collect, analyze and report on compliance.

Access Assurance

As the market has evolved, its identity has also been evolving: from password management to a broader security management and compliance focus. However, this has led to some confusion about what the market has become. IAM is evolving in a way that touches on policy management, security management, or governance, risk and compliance (GRC), leading to even greater confusion on the part of some as they try to figure out where the various vendors deliver value. As one analyst recently put it, "Is it a provisioning play, a role-management play, a password-management play, a compliance play, or all of the above?"[3]

[3] Steve Coplan, The 451 Group, Jan. 15, 2009.

The bottom line, for many organizations, is that they want IAM solutions to help them reduce overhead expenses, enhance productivity and improve the user experience. They also recognize the role IAM has in improving security and compliance management, recognizing that it is far more efficient to make compliance a seamless, transparent part of the business, rather than treating the audit process as a once a year event.

At the heart of any organization's rationale for purchasing an identity and access management solution is the desire to ensure that *only the right people have the right access to the right information and are doing the right things*.

What they are looking for, in other words, is *Access Assurance*.

What is Access Assurance, what are the benefits of adopting an Access Assurance strategy, and what elements should companies be looking for in order to ensure that they achieving them?

Access Assurance Components

Access Assurance is based on the interaction of three complementary pillars that combined, enable organizations to fully automate the management of users' identities and access rights. They are:

- Access Governance
- Access Provisioning
- Access Compliance

Together Access Governance, Access Provisioning and Access Compliance (see Figure 1) provide the basis for designing, implementing, managing, monitoring and remediating user access rights and entitlements.

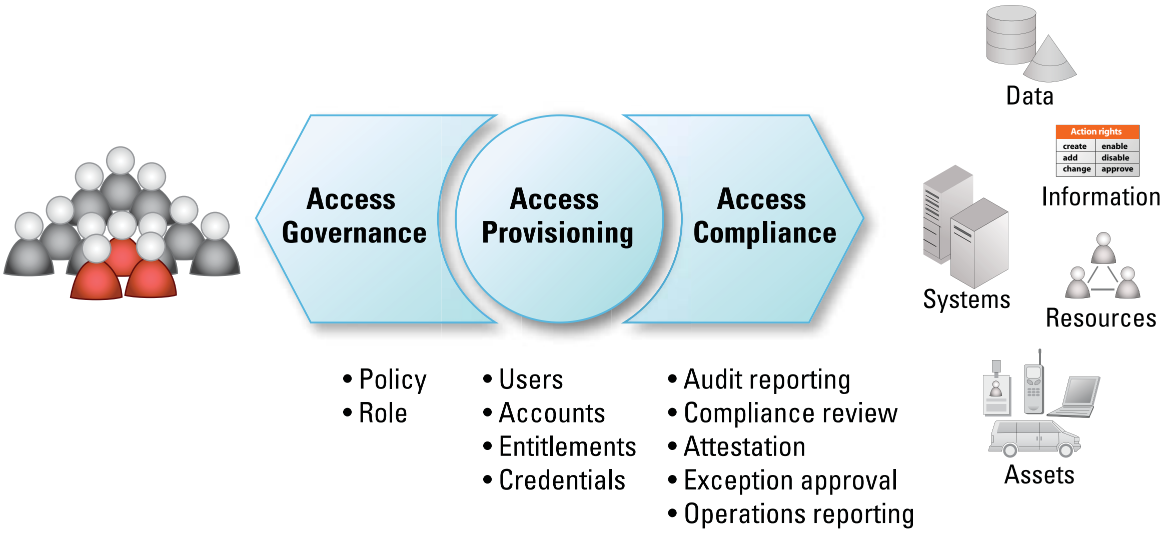

Figure 1. Access Assurance Components

Access Governance

Access Governance is the process of defining corporate access management policies and roles.

Policy

Access Governance policies can vary considerably from one organization to another. However, most typical organizations define some or most of these policies:

- Open versus restricted access rights – which users have access to which applications and/or data, and at what level of privilege. For example, most organizations provide all users with email and general purpose file share access, but restrict access to financial applications (general ledger, accounts receivable/payable, payroll) to members of the finance group.
- Authorizations – policies that govern who can approve what. Examples: purchase orders greater than $10,000 must be approved by a VP, or only a department manager or supervisor can originate a new hire.
- Information classification – differentiating non-critical information from sensitive or proprietary data (such as protected health information).
- Principles of least privilege – defining the minimum level of privileges users require to perform their function.
- Segregation of duties – polices intended to minimize the potential for fraud or abuse. Authorization and authentication are essential to enforce SoD policies.
- Password integrity – policies that influence password robustness, such as minimum length, password strength (i.e., mix of alpha, numeric and special characters), expiration, prohibiting reuse, not allowing common dictionary words, etc.

Roles

Roles are another core element of Access Governance. Every organization, regardless of size or complexity, employs the concept of roles in its organizational design.

Roles (senior teller, sales manager, customer service specialist, etc.) help to define the business operations that users can engage in. From an information technology perspective, roles govern the systems and access rights that individual users should be granted. For example, all users may be given access to a corporate email server and file server. However, only certain roles in the human resources (HR) department may have access to the HR functions within a Peoplesoft system, while only senior tellers may have access to certain banking operations, such as cash drawer reconciliation.

Business Alignment

By understanding the linkage between business roles, on the one hand, and IT accounts and access rights on the other, information technology becomes aligned with the business. Without understanding the business role a user plays within an organization, it becomes very difficult for IT to effectively determine which applications that user should be able to access or what rights and entitlements the user should have within the application. This often results in over-provisioning, wherein users are granted excessive access rights beyond what they actually require.

Similarly, as users shift from role to role (for example, as the result of a promotion or reorganization), IT needs to understand how a new role affects accounts and access rights (see sidebar).

Access Governance, therefore, is essential for a business to align the core components of its IT security infrastructure and strategy with specific business requirements. Without this alignment, there can be no practical association between access rights and corporate security guidelines and best practices, industry requirements or government mandates.

Impact of Changing Roles

According to published reports, Jérôme Kerviel, a trader at Société Genérajé, engaged in unauthorized trades totaling as much as €49.9 billion, an amount larger than the bank's total market capitalization. He concealed the scope of his activities by using access rights he acquired when he worked in the compliance department which were not revoked when he became a trader. The bank lost approximately €4.9 billion as a result.

Access Provisioning

If Access Governance is where roles, access policies and rights are defined, Access Provisioning is where they are put into practice. Provisioning is the process of establishing accounts for users, along with their respective access rights, on selected target systems.

Provisioning requires, at a minimum:

- Integration with one or more target systems.
- The ability to define accounts on those systems, in a way that is supported by the native security system of the target platform.
- Granting appropriate entitlements and access rights to a user, which can be enforced by the target platform security system.

In addition to establishing accounts on various systems, provisioning may also include configuring a variety of other access management and authentication systems. These include:

- Password management – provides a mechanism for users or IT support personnel to manage passwords. For example, if a user forgets their password, or the password expires, a password management system enables the user to reset it.
- Web access management (WAM) systems – WAM is used to control access to internal and external-facing web sites. These sites can be used to support of a wide variety of business activities,

such as employee portal, customer support, business partners, e-commerce, etc.

- Single sign-on (SSO) systems – many organizations have a wide variety of systems that various users need access to. SSO systems make it possible for a user to be authenticated once and then access other systems without having to re-enter their credentials.
- Privileged account management (PAM) systems – manages access to highly privileged accounts, such as a network or database administrator. PAM systems reduce or eliminate the potential threat that a privileged account password might fall into the wrong hands.
- Multi-factorial authentication – using multiple forms of identification to authenticate a user, based on something you know (a password or PIN) and something you have (an authenticator)—providing a much more reliable level of user authentication. Multi-factorial authentication system may require the user to use an authentication token, like a RSA SecurID® device, or pass a biometric scan, as part of the authentication process.

Benefits

Automated provisioning and password management deliver a number of useful benefits. They provide improved security, by ensuring that user privileges and password profiles are consistent with policy. Automation also reduces overhead costs by enabling fewer personnel to manage user access and accounts. And, there is increased convenience for users who don't have to wait idle for long periods of time, waiting for access to their systems.

The Zombie Account Problem

An account that remains active after an employee leaves the organization is a zombie account (also called a dormant or orphan account).

In an era of large layoffs, the number of zombie accounts remaining can be potentially overwhelming, because of the number of systems employees and other workers typically use. It is typical at a large enterprise for a user to have access to as many as 15 or 20 accounts.

For example, in late 2008 a major financial institution announced plans to terminate 50,000 employees. If the institution has an average of 20 accounts per employee (which is not unusual), that means as many as one million zombie accounts could be live, waiting for a disgruntled former employee to log on and do something malicious with that access.

The problem is that manually disabling or eliminating this many accounts is extremely challenging. At a conservative estimate of 5 minutes per account, removing 1,000,000 accounts requires more than 83,000 man-hours or approximately 9.5 man-years.

A key benefit of a strong Access Provisioning system is the ability to quickly and easily disable or terminate accounts, whether initiated by an authorized manager or by an automated “lights-out” process triggered by updates to a HR system of record. This eliminates the potential for terminated employees to access their former accounts and engage in malicious behavior.

Access Compliance

The third pillar of Access Assurance is Access Compliance, which enables the organization to monitor, detect and verify that users have access rights and entitlements that are consistent with corporate security policy, relevant industry guidelines and government regulations.

User Activity

Effectively monitoring users requires integrating identity and access rights with applications that capture specific information concerning user activity, including what data users have access to and what they are doing with that access.

Two major categories of software have emerged that help organizations understand what users are doing with data: data loss prevention (DLP) and security incident and event management (SIEM) software.

DLP alerts organizations when sensitive data may be vulnerable to exposure and provides the ability to take steps to protect it. Sensitive data can take many forms, such as protected health information (PHI), personal employee information (social security, salary, date of birth), corporate trade secrets and formulas or customer data (such as credit card numbers).

Initially, DLP technologies were deployed at network endpoints to block sensitive data in motion, such as an email attachment or on a laptop hard drive. More recently, DLP has been employed to identify sensitive data at rest, stored on internal systems in a data center, such as a network server.

SIEM software evolved from network logging and is typically used for compliance reporting, threat management or a combination of both. SIEM focuses on monitoring networks, identifying potential security incidents, and alerting security personnel to investigate.

What both DLP and SIEM lack is an identity context that makes it easy for managers, security or IT administrative personnel to understand which users have access to the data and whether those access rights are appropriate or consistent with policy.

For example, when a DLP tool highlights sensitive data on a SharePoint server, it is relatively difficult for a security administrator to know what remediation steps are appropriate without knowing who has access to that data. The administrator can go a step further by leveraging SIEM data to identify which employees have actually accessed the data. However, simply knowing the network user ID of the individuals who have accessed the data doesn’t go far enough. What’s needed to complete the circle is information about who the individuals are, what department they work for, who their manager is, what roles they occupy, etc.

Integrating DLP and SIEM data with identity-related information provides the business context that makes it feasible for a business manager or security administrator to understand who the user is, whether or not it’s appropriate for them to be accessing the data, and if further steps should be taken to protect the data against unauthorized access. Adding this additional business context to the alert information generated by a DLP or SIEM tool, effectively puts the power to understand and address the risk of the situation into the hands of the individuals who know the business.

Compliance Validation

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 many industries, such as financial services, as a direct result of the recent increase in bank failures and company bankruptcies.

Access Compliance 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. Implementing Access Compliance within the organization brings two major benefits.

First, it enables managers to quickly and easily confirm that employees have entitlements that are appropriate to their role or function. This is particularly important in environments where segregation of duties (SoD) is essential.

Classic financial examples of SoD include not allowing an individual to both originate and sign a corporate check or to create and approve purchase orders. SoD practices are also being adopted by IT to ensure that no individual can introduce fraudulent or malicious code or modify sensitive data without detection.

A properly implemented Access Compliance process enables managers to reliably report to auditors and others that controls are in place to restrict individuals from accessing sensitive data or performing business functions that would violate segregation of duties or other business policies.

Second, the amount of effort required to collect data and 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, for example, can literally run into millions of dollars.

Even beyond the need to meet the demands of auditors, the true spirit of Access Compliance is to make compliance a seamless, transparent part of routine business activities. Automated Access Compliance eliminates the need to periodically disrupt managers performing their usual activities and force them to focus a significant amount of effort on compliance reporting and attestation.

Making Access Compliance an ongoing part of routine business operations that automatically ensure users only have access rights which are appropriate to their specific job functions reduces wasted time and effort and enables the business to run more smoothly and efficiently.

The Access Assurance Lifecycle

The three pillars of Access Assurance provide the foundation for organizations to implement a comprehensive, policy-driven lifecycle which ensures that people (users) are provided with the rights they need to access and use information resources, and that their activity is consistent with the organization's business goals and objectives.

The Access Assurance lifecycle (see Figure 2) encompasses five core processes based on the Access Assurance pillars:

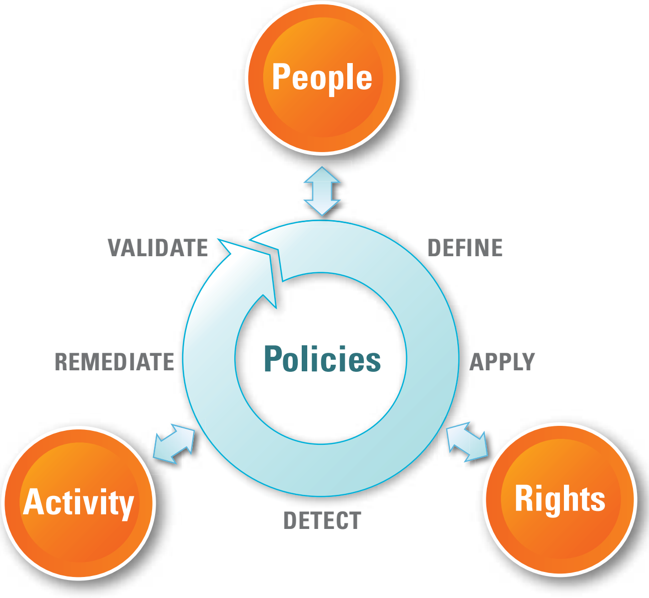

Figure 2. Access Assurance Lifecycle

- **Define** (Access Governance) – defining access policy, which includes roles and user profiles, along with their associated entitlements and access rights, enabling alignment between IT and the business.
- **Apply** (Access Provisioning) – creating user accounts and entitlements on target systems, providing users with the appropriate credentials to access and utilize corporate resources, such as applications, databases, networks, and devices.
- **Detect** (Access Compliance) – monitoring user activity on critical systems to ensure that user access is consistent with corporate security policies, guidelines and best practices, and alerting authorized personnel to potential security issues. Integration with user access and activity systems provides an identity context that enables business managers, security administrators, or other authorized personnel to effectively enforce security policies.
- **Remediate** (Access Provisioning) –making adjustments to the identity and access management environment to bring users' back into compliance with policy, or potentially modifying policy to bring it in line with actual business practice.

- **Validate** (Access Compliance) – providing ongoing assurance and verification that user rights and entitlements are consistent with policy and delivering reports that can be provided to auditors and other interested parties charged with ensuring compliance with government regulations, industry requirements, corporate policy or best practices guidelines.

Courion's Access Assurance Solutions

Courion Corporation is a leading provider of Access Assurance solutions to more than 400 organizations worldwide, including more than 25% of the Fortune 100, with more than 7.5 million licensed users.

Courion's approach to Access Assurance is based on an integrated suite of products focused on access governance, provisioning and compliance. These include:

- AccountCourier® –user provisioning and de-provisioning solution.
- PasswordCourier® – password management and user self-service.
- RoleCourier®– used to define and manage access managements and entitlements for user roles.
- ComplianceCourier™ – attestation and reporting that enables managers to quickly and easily validate that the users within their organizations have appropriate access rights to business resources.

Flexible Approach

Courion's Access Assurance approach is grounded in the principle of "start anywhere/go anywhere." Courion enables customers to focus where they it makes more sense first, be it password management, provisioning, or compliance reporting. Some customers decide to begin with the area of the greatest business pain, while others choose to begin in an area that will provide a quick win with rapid payback.

Because Courion's technology is based on a comprehensive shared framework, customers can begin with the solution that addresses a key business driver first, without having to divert precious resources to implement a complete stack of vertically integrated software before they can begin to enjoy the benefits of Access Assurance.

Courion's products all work together on a powerful, scalable workflow engine. The Courion architecture includes a standards-based and distributable Connector Framework with hundreds of predefined connectors that link Courion's workflow engine with a wide variety of operating systems, networks, servers, databases, middleware, web portals, and enterprise applications.

Strong Partnerships

Through strong relationships with companies like RSA (the security division of EMC^2), Citrix Systems, Symantec, Imprivata, Cyber-Ark and others, Courion offers complete end-to-end Access

Assurance solutions that includes:

- Enterprise single sign-on – enabling users to log onto a single system, which then transparently manages their access to a wide variety of enterprise IT resources.
- Web access management – providing secure access to web-based applications.
- Security Incident and Event Management (SIEM) and Data Loss Prevention (DLP) integration –delivering the identity context that these access intelligence systems require in order to intelligently discover and manage access to sensitive data wherever it may be located.
- Federated identity – to securely extend access rights to external users across multiple business domains, such as customers, distributors or suppliers.
- Privileged password management – enabling organizations to secure, manage and monitor activities associated with privileged passwords, such as the administrator of a server, network or database.

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.

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