



Access Risk Management Suite

Benefits

- **Reduce Access Risk:** Automatically protect sensitive data and other vital assets from inappropriate user access, simplifying access risk policy enforcement.
- **Strengthen Compliance:** Deliver improved compliance with corporate security policies, industry standards and government regulations.
- **Achieve fast time to value and lower total cost of ownership:** Rapid deployment methodology and modular architecture have you up and running quickly, with fewer resources to manage and maintain over time.
- **Improve business alignment:** Non-technical business users are easily engaged in the security and compliance process.
- **Provide flexible, interactive tools:** Extensive analytical capabilities automatically evaluate and monitor user access, and enterprise risk trends.
- **Deploy on-premise or in the cloud:** Choose the deployment option that makes the most sense for your business.

Courion's comprehensive approach to Access Risk Management is based on the premise that every organization has a unique, globally distributed environment – on-premise, outside the fire-wall, in the cloud, and mobile and virtual environments.

Courion's new Access Risk Management Suite provides a single platform for managing user access to vital information by automating and integrating key IAM functions such as identity and access governance, user provisioning and password management. Our unique, rapid deployment methodology combined with our flexible, modular architecture and the fact that our solutions are not dependent on any proprietary infrastructure, enable us to leverage your existing infrastructure and eliminate technology prerequisites – delivering faster time to value and a lower total cost of ownership.

By streamlining the user access process, Courion solutions help companies easily reduce the risk of intellectual property theft, loss of reputation and regulatory penalties by automatically identifying, quantifying and managing access risk.

Access Risk

An integral part of Courion's Access Risk Management Suite is **Access Insight™**. Access Insight helps organizations identify, quantify and manage their access risk – seeing not only where their risk resides, but the level of risk as well.

Access Insight constantly analyzes IAM and other security data to identify and quantify risks to vital information such as intellectual property, medical records, personally identifiable information and customer data – recognizing associations and patterns in user access privileges that might violate compliance guidelines of company policies.

Using predictive analytics to manage business, people, assets and security risks, Access Insight automatically creates near-real-time graphical profiles of the most critical security risks to information – replacing manual data sorting and risk scoring that lacks context, and a connection to business priorities.

The result – quicker identification of security or risk issues, fewer resources needed to manage compliance and audit requests and, ultimately, a more secure environment for your entire organization.

Access Governance and Compliance

Streamline Access Certification, Ensure Compliance

Courion's **Compliance Manager** automates the access certification and compliance management lifecycle. By automating these processes, you will quickly and easily streamline access certification, improve security, reduce access risk and ensure compliance with relevant regulations.

With Courion's Compliance Manager, authorized business managers can review access rights for users they supervise, using business-friendly entitlement definitions as part of a complete access compliance strategy. The **Access Certification Portal** enables the business user to certify appropriate access or take immediate action to protect the enterprise by revoking access that violates enterprise security policy.

Compliance Manager provides users with automated discovery, validation and reporting capabilities that deliver a comprehensive view of access risk caused by inappropriate user access rights and behavior. Policy violations can be addressed by automatically triggering appropriate actions to initiate corrections; indirectly by generating an email notification or help desk trouble ticket, directly through Courion's powerful built-in remediation capabilities, without requiring deployment of a provisioning solution, or via connectors to installed third-party provisioning solutions.

Detective and Preventive Controls

Designed with vendor-neutral architecture, Courion's **Sensitive Data Manager** and **User Activity Manager** solutions integrate seamlessly with enterprise-class data loss prevention (DLP) and Security Incident and Event Management (SIEM) products on the market today.

Sensitive Data Manager reduces access risk by enabling organizations to identify who has access to sensitive data and certify that their access is consistent with policy. When a data loss prevention (DLP) solution identifies sensitive data, Courion organizes, filters, and synthesizes this data, identifies the users who have access to the sensitive data and puts this information into the hands of business users who are in the best position to determine whether their access is appropriate. If needed, Courion provides the manager with the ability to remediate inappropriate access by modifying or disabling user entitlements according to policy.

User Activity Manager improves security by providing managers with user activity data combined with identity profile data. Managers can view and compare actual activity with access policy, allowing the business to uncover inappropriate activity. For example, User Activity Manager may uncover situations where a user is engaged in suspicious activity, such as after-hours access. Providing a comprehensive identity profile to the manager reviewing this data enables the manager to choose the most appropriate action to resolve the situation. The ability to see which applications are being used is beneficial in avoiding "over-provisioning" or paying user license fees or maintenance on systems and applications that users are not accessing regularly as part of their job.

"It is the better-managed organizations that are using IT as a competitive advantage to generate more capital to invest in acquiring new customers and markets, reduce capital and operating costs, while significantly reducing operational and strategic risks related to the use of IT."

"How High Performance Organizations Manage IT"
IT Policy Compliance Group, 2011

Simplify and Optimize Access Risk Policy Enforcement

The often complex, cumbersome and inefficient process of role creation and role lifecycle management is now automatic. Embedded within Courion's unique access risk management platform is Courion's **Role Manager**. This solution empowers organizations, helping them to simplify and optimize security and access risk policy enforcement by automatically creating roles that align IT accounts and access rights with business functions.

Courion's Role Manager effectively manages the entire enterprise role lifecycle, including the ability to modify or delete role attributes, enable or disable roles and manage role hierarchies. Role Manager provides role history analysis, an important capability for compliance analysis and reporting, while role comparison and consolidation enables organizations to iteratively examine their role definitions and identify opportunities to simplify security policy management and administration by reorganizing, creating nested roles or merging similar roles.

Courion's dynamic role definition process reduces the potential for role proliferation by creating a single role with localized attributes that are dynamically assigned at provision time. "What-if" role modeling examines a candidate role against security policy to determine if changing access rights would create a policy violation, or to detect attribute-level conflicts across multiple roles.

Now, organizations can readily adapt to changes in today's business environment, such as mergers, acquisitions, and reorganizations – making it easy for managers to assign or revoke user access privileges, ensure least privileged access and manage segregation of duties in accordance with their roles.

User Account Provisioning

Maximize Savings, Accelerate Service Delivery

Courion's **Provisioning Manager** is essential for organizations seeking to: improve alignment with business needs; cut costs and improve productivity; proactively enforce compliance with internal security policies, industry standards and government regulations; and reduce the risk of security incidents.

Provisioning Manager enables organizations to manage the user provisioning lifecycle – from policy definition to granting application access through end-user termination. Business managers can easily create, modify, disable or delete user accounts – enforcing security policy based on operating knowledge of the business. By automating the process of creating, changing and terminating access rights, your organization is immediately protected against the risk of unauthorized access by employees whose roles have changed, or have been terminated.

Using Courion's exclusive PolicyLink™ technology, Provisioning Manager gives organizations the flexibility to leverage existing policy information and dynamically generate new policy in accordance with changing business needs. A secure, reusable framework makes periodic or ad hoc access verification, reporting and attestation simple.

Business-Friendly, Streamlined Provisioning

Courion's Access Request Manager presents a business-friendly, streamlined user interface that enables organizations to offer provisioning capabilities to its user community by delivering a shopping cart approach to provisioning, providing users with a familiar experience when requesting access.

An integral part of Access Request Manager is the access catalog, which shows the entire inventory of all the access choices available to an organization. The access catalog provides authorized users with a simple way to browse through the access rights assigned to individual users in an organization with the convenience of being able to sort by a number of categories including role, person, category and application.

Using business-friendly terms and an easy-to-use interface, authorized users are guided through the access request process, allowing them to easily define access for users in their organization. Requesting access and viewing access, as well as viewing outstanding requests for access is simple and fast.

Access Request Manager expands upon the dynamic approval mechanisms in Courion's Provisioning Manager by offering line-item veto capabilities during the dynamic approval process – giving authorized users the ability to approve some requests while denying others.

“The findings show the best performers are using IT to grow top-line revenue, increase profit, gain customers, retain customers, and minimize the business risks associated with the use of information systems.”

“How High Performance Organizations Manage IT”
IT Policy Compliance Group, 2011

Ease of Transfer of Access Approval and Request Authority

Managers no longer need to worry about how access requests and approval will be accomplished while they're on vacation or on extended leaves of absence. **Access Request Manager** provides the capability for managers to easily delegate access approval and access request authority to direct reports while managers are away. In the case of a security breach or an emergency termination scenario where time is of the essence, Access Request Manager offers a simplified UI to immediately disable access to all of a user's associated accounts.

Self-Service Password Management

The Simple, Secure, Cost-Effective Solution

Courion's **Password Manager** is the industry standard solution for secure, self-service password management for organizations seeking to deploy self-service password reset and synchronization for users, as well as to enforce secure password policies. This feature-rich solution offers multiple access options, robust service desk integration and the ability to enforce consistent password policies for any system, application, or web portal.

With its powerful policy engine, organizations can apply a wide variety of password rules to all systems and applications, selected groups of systems and applications (e.g. all UNIX systems, all z/OS systems, all web portals), or individual systems and applications. A sample of rules that can be put into effect include: minimum/maximum password length, history and dictionary checking, required mixed case, and numeric or special character use.

Flexible, Easy-to-Use Password Management Options

Administrators have flexible options for managing password synchronization. Active Synchronization enables end-users to choose individual accounts for reset from an eligible list. Transparent Synchronization enables password changes to be propagated to all systems. Courion's synchronization technology enforces native target password requirements, making it simple for end-users who only have to remember one password for multiple platforms.

A Connector Library with Hundreds of Options

Courion's rich connector library contains hundreds of connectors for a wide range of platforms, including operating systems (desktop PCs, servers, mainframes), directories, networks, databases, security systems, help desks, middleware, and packaged enterprise applications, such as ERP (SAP, Oracle, JD Edwards. etc.), industry-specific (McKesson, Metavante, MEDITECH, Epic, etc.), and many more. Connectors are available from Courion at a low fixed price, or customers can use Courion's Rapid Development Kit to create custom connectors where no standard connector is available.

Enterprise Architecture

Courion's Access Risk Management Suite runs on a multi-tier platform implemented using industry standard, service-oriented architecture (SOA). Three logical tiers deliver reliability, scalability and performance since they can be deployed on a single machine or distributed across multiple servers for high throughput or improved availability. Communications between the logical layers utilize secure, encrypted web services protocols.

On Premise or in the Cloud Best-of-Breed Solutions

As a natural extension of Courion's industry-leading architecture, Courion now delivers its portfolio of solutions from the cloud as well as an on-premise solution. The **Access Risk Management Suite** allows customers to manage access to applications in the cloud just as easily as they execute their existing identity and access management programs on premise – whether provisioning user access changes, certifying user access, remediating access violations or generating audit and compliance reports.

CourionLive™, Courion's SaaS offering, delivers feature-rich functionality with the benefits of low start-up, operational and maintenance costs, and quick time to value, bringing its best-of-breed IAM solution to organizations of all sizes. This means you can now make informed business decisions by being able to immediately identify the critical risk areas in your organization, and then focus your efforts on those high impact areas to reduce the risk.

Courion's innovative solutions combine out-of-the-box functionality and best practices based on hundreds of successful implementations to provide the intelligence to identify, quantify and manage access risk in your organization – by ensuring the right people have the right access to the right information.

Backed by Industry-Proven Services

Every solution in Courion's Access Risk Management portfolio is backed by world-class, expert services delivered directly by the Courion Professional Services organization or by our Certified Solution Partners. Courion's unique technology platform combined with our comprehensive discovery and implementation methodology enables us to offer the optimal combination of products and services to meet our customers' ever-changing business needs while demonstrating strict compliance with mandatory regulations, rules and policies.

About Courion

Courion, the leader in identity and access (IAM) management solutions that effectively and securely manage user access risk, helps companies manage risks associated with information access. More than 14 million users in 500 organizations worldwide rely on Courion's solutions to align user access privileges with corporate and regulatory governance policies.

Courion's best-of-breed solutions enable organizations to identify, quantify and manage access risks to vital information including intellectual property, medical records, personally identifiable information and customer data, while demonstrating regulatory compliance. Courion's cloud and on-premise solutions offer full arrays of IAM functions, including identity and access governance, user provisioning and password management – delivering the industry's fastest time to value and lowest total cost of ownership.

For more information, please visit our website at www.courion.com, our blog at blog.courion.com, or on Twitter at twitter.com/Courion.



World Headquarters

COURION CORPORATION
1900 West Park Drive
Westborough, MA USA 01581
Phone: +1 508-879-8400
Toll-free: 1-866-COURION

APAC

COURION IT PRIVATE LTD
305, Pride Purple Accord,
S. N. 3/6/1 Baner Road,
Pune, Maharashtra, India 411 045
Phone: +91(20) 6687-9100