



Protect The Enterprise with User Activity Manager

Benefits:

- **Improves security** – by highlighting instances where people may be abusing access rights and engaging in risky behavior.
- **Reduces risk** – by enabling organizations to quickly choose the most appropriate remediation.
- **Streamlines business** – by allowing managers to evaluate user activity, knowing who the user is, and respond quickly and efficiently.
- **Improves productivity** – by improving the ability of managers to quickly and easily filter, identify and monitor activities that represent the highest level of risk to the organization.

As companies grow increasingly complex, so does the complexity of protecting the enterprise from inappropriate behavior which can create risk. As a result, organizations are concerned with what employees are doing, whether or not they are abusing their access to corporate assets and data, and how they can reduce the risk that security may be compromised. Security incident and event management (SIEM) and identity and access management (IAM) technologies in combination can help with identifying, remediating, and reducing risk.

SIEM technology is used for broad-based monitoring and analysis of events. This can be particularly useful for compliance reporting, breach detection and uncovering potential incidents of fraud or inappropriate access.

When a SIEM analysis uncovers patterns of inappropriate user activity, it can be difficult for the data owner or security manager to know who the individual user is, what role they play in the organization, and what impact the pattern of activity may have on the risk to the organization.

IAM, on the other hand, contains information about who the user is, what other systems the user has access to, and who authorized those access rights.

IAM and SIEM Synergy

Until recently, SIEM and IAM solutions worked separately. SIEM solutions were designed to focus more on IT security, while IAM solutions were focused on enabling business users to manage identities. As a result, IT and security managers were unable to leverage their complementary capabilities in a unified solution.

Today, Courion is addressing this problem by delivering **User Activity Manager**, a solution that integrates **ComplianceCourier™** – Courion's Access Compliance and Certification solution – with leading SIEM solutions from vendors like RSA and others. Courion's SIEM integration architecture is vendor-neutral and designed to combine data from any SIEM vendor with user identity and access information contained in the Courion system.

User Activity Manager combines data from SIEM with user identity information to enable your organization (or your business) to answer the questions:

- Who is engaging in risky or unauthorized behavior?
- What are they doing that violates security policy or industry regulations?
- When did they do this?
- How should I reduce these risks?

Courion User Activity Manager adds detailed identity-based context to the SIEM event, such as: name, role, title, department, manager, location, entitlement, group memberships, etc., and presents this data in a business-friendly format that enables the manager to better evaluate the level of risk associated with this access and determine/suggest the best way to remediate.

Integrated Remediation Strategy

User Activity Manager's integration with ComplianceCourier enables managers to select the most appropriate remediation strategy, based who the user is and what activity he or she has been engaged in. These steps may include:

- Approving appropriate user access rights and activity, or approving an exception, where warranted
- Modifying the SIEM alert level
- Creating an email message or help desk trouble ticket
- Modifying user access rights
- Blocking access for individuals or groups of users
- Escalating or requesting research

If access rights to enterprise resources need to be changed, ComplianceCourier can automatically trigger the appropriate actions to initiate corrections, using a variety of remediation options. An audit trail tracks all review and remediation transactions undertaken by authorized managers.

Routine Access Certification Review

ComplianceCourier automatically manages the access compliance and certification process by notifying authorized managers when it is time to review employee access rights and activities, and enabling them to confirm that the employee's access complies with corporate policy or relevant industry/government regulations (SOX, PCI DSS, HIPAA, GLBA, etc.). Integration with SIEM technology enables Courion customers to ensure not only that end user access rights are consistent with policy, but that their activity is as well.

Features of the combined User Activity Manager and ComplianceCourier solution include:

User Activity Manager and ComplianceCourier Features	
Compliance and Attestation	Effectively respond to auditor and regulator requirements for ongoing compliance monitoring and management to ensure compliance with corporate policies or key industry and government regulations.
Review Unusual Events	Enable business managers to receive a SIEM alert and review and verify user activity.
Designed for Business Users	Provide security and business managers with a business-friendly view of activities and user entitlements to confirm or remediate improper access rights.
Comprehensive Data Integration	Identify users engaged in potentially risky behavior along with other user IDs that the individual is associated with, to identify all systems they can access.
Integrated Remediation	Enable business users to automatically initiate corrective actions, without the need to install a provisioning solution.
Audit Tracking	Capture decisions in a transaction database for ongoing analysis, audit tracking or forensics analysis.

For more information on the benefits of integrated DLP and IAM, contact Courion at info@courion.com.

About Courion

Courion, the leader in access risk management, helps companies identify, quantify and manage the risks associated with information access. Used by nearly 500 organizations and over 14 million 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 can help your company win in today's mobile, always-on, cloud-based business environment. For more information, visit our website at www.courion.com.

