Identity and Access Intelligence: How Big Data and Risk Analytics Will Revolutionize IAM

Applying business intelligence to simplify audits and tighten security

By Nick Berents
Director of Product Marketing

www.courion.com

Table of Contents

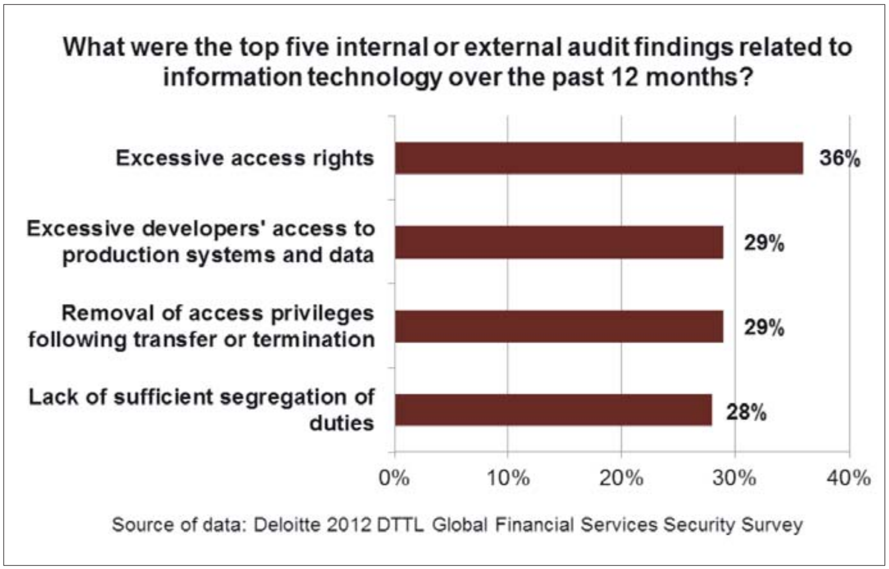
Why IAM is Incomplete Without Identity and Access Intelligence

In recent years Identity and Access Management (IAM) solutions have made great advances in helping enterprises increase the efficiency of user account provisioning and more effectively manage IT audits.

Yet in too many cases these enterprises still discover orphan accounts, people with inappropriate or excessive access to confidential and sensitive data, "privileged users" with unnecessary permissions, employees with toxic combinations of entitlements (violating segregation/separation of duty rules), and individuals violating corporate policies.

Statistics confirm the prevalence of these problems. When security executives from 250 financial institutions were asked for the top five audit findings related to information technology, they most often cited excessive access rights, excessive developers' access to systems and data, failure to revoke access after employees were transferred or terminated, and lack of segregation of duties (Figure 1).

These issues have a big impact on security as well as compliance: according to Verizon's 2013 Data Breach Investigations Report, 76% of network intrusions exploit weak or stolen credentials.[1] They also have implications for how IT departments operate. Administrators are forced to react to problems and crises, rather than anticipating risks and continuously improving IAM processes. IT executives find themselves unprepared for audits, and worried about access-related vulnerabilities.



Source of data: Deloitte 2012 DTTL Global Financial Services Security Survey

Figure 1: Most common audit findings at financial institutions.

Many of these issues can be traced to three shortcomings of existing IAM solutions:

- To identify policy violations, they rely on infrequent and time-consuming access certification exercises and simplistic audit checklists.
- Their reporting capabilities are incapable of processing and analyzing the masses of identity and access data generated by today's enterprises.
- They lack any mechanism to correlate identity and access data with user activity, and therefore miss many opportunities to alert administrators to policy violations and suspicious activities.

Fortunately, a new type of technology called *Identity and Access Intelligence* addresses these problems. It employs continuous monitoring of identities, access rights, policies, and user activities to identify and remediate vulnerabilities quickly. It provides data warehousing tools to process and interpret huge volumes of complex data. It includes business intelligence tools to pinpoint policy violations and focus attention on high risk areas. And it enhances traditional IAM functions such as provisioning and governance, so those functions can more effectively reduce risk and focus attention on issues critical to the business.

[1] Verizon 2013 Data Breach Investigations Report

In this white paper we will:

- Explain where today's provisioning and identity and access governance solutions fall short.
- Provide an overview of an Identity and Access Intelligence System.
- Discuss how an Identity and Access Intelligence System can help enterprises detect and remediate threats and vulnerabilities, feel confident at audits, and improve provisioning and governance processes.

Shortcomings of Today's IAM Systems

Identity and Access Management systems have helped many enterprises automate routine tasks, reduce costs, improve security, and evaluate various controls for auditors. (See table)

Identity and Access Management Successes	
User Account Provisioning *Automate account creation, modification, and disablement for user provisioning and de-provisioning processes*	• Reduce administrative costs • Detect and modify or delete inappropriate access rights • Improve security by enforcing policies (give the right people the right access)
Password Management *Self-service password reset, unlock and synchronization*	• Enhance service for employees • Reduce help desk costs
Identity and Access Governance (IAG) *Define access policies and certify identity and access compliance*	• Enable business managers to review and verify access rights • Simplify compliance with SOX, HIPAA, PCI DSS, FISMA and other regulations and standards • Provide data and metrics to improve security processes.

Yet even when these systems have achieved considerable success within their respective domains, from a broader perspective a number of shortcomings are visible.

Problem #1: The "Governance Gap" and Accumulating Violations

Most enterprises today suffer from a "governance gap" with two major causes.

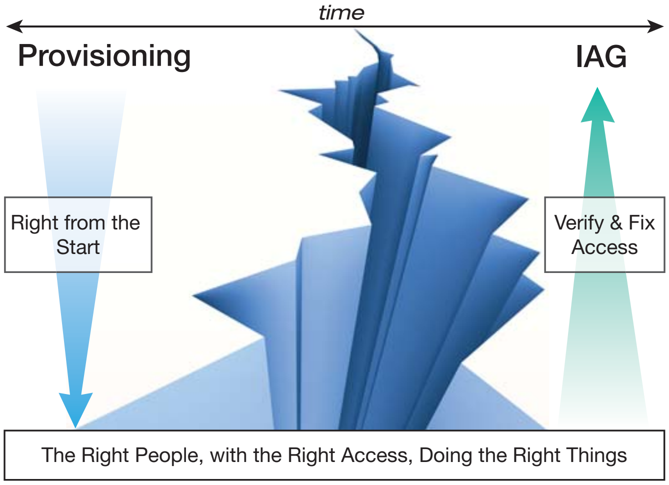

time
Provisioning
IAG
Right from the Start
Verify & Fix Access
The Right People, with the Right Access, Doing the Right Things

Figure 2: The IAM "Governance Gap"

The first cause of the governance gap is the accumulation of access events that occur between account provisioning and periodic certifications, leading to vulnerabilities and policy violations.

User account provisioning systems are designed to give IT system users access to the right resources, with the right permissions, "right from the start." But change inevitably causes policy violations. Managers make mistakes when employees are promoted, transferred and terminated. Errors are made when new applications and resources are brought online, and when roles are created or modified.

Most Identity and Access Governance systems attempt to find these policy violations by periodically gathering reams of entitlements data and asking managers to certify the access rights of their reports. But since most organizations cannot afford to ask administrators and managers to perform these time-consuming certifications more than quarterly or semi-annually, a large number of violations build up over time. Often, busy managers turn certification reviews into "rubber stamp" exercises without making real efforts to detect inappropriate or unnecessary permissions.

Some of these violations give employees (and potentially outside cybercriminals who capture employee credentials) access to key systems and confidential data. Enterprises are exposed to these accumulating vulnerabilities during the three months or six months between certifications. In many busy organizations, the certification review is out of date within days of the attestation.

The second cause of the governance gap comes from inevitable flaws in provisioning and governance processes. Managers and privileged users make exceptions to the provisioning rules, or completely bypass established processes for granting access. Administrators make changes related to transfers, promotions and other events directly to applications and enterprise directories, without the controls and oversight of provisioning systems. Certain applications and systems are not connected to provisioning systems at all.

In addition, identities and roles are not always perfectly understood, leading to access rights that subtly (or not-so-subtly) violate policies.

These hidden flaws give some IT executives and compliance managers a false sense of confidence about their compliance posture, and others a well-founded anxiety about their audit preparedness.

Problem #2: Information Hidden by Complexity

The volume of identity and access-related data is immense and growing rapidly. A few years ago administrators could focus on corporate employees, with one device each (a laptop or desktop PC), accessing a handful of corporate applications in the data center. Today, they must assign and monitor access rights for employees, contractors, business partners and customers, each of whom uses an average of 2.9 mobile devices (including smartphones, laptops and tablets),[2] to access applications in data centers, private clouds and public clouds.

A quick calculation illustrates the magnitude of this challenge. An organization with 1,000 system users, 5,000 user accounts, and 1,000 rights or entitlements would need to keep track of **5 billion** combinations.[3]

Moreover, information that might provide clues about policy violations resides not only in IAM systems, but also in directories, databases, logs and security applications.

Conventional Identity and Access Management systems simply cannot produce useful, timely intelligence from these volumes of disparate data.

In addition, although many current solutions can look for pre-determined violations such as segregation of duties (SoD) and orphan accounts, many policy violations are too subtle to be caught by simple rules. These include:

- Access rights derived from inherited and nested permissions.

[2] SecurityWatch: Everyone is Carrying Too Many Mobile Devices

[3] 1,000 x 5,000 x 1,000 = 5,000,000,000

- Unnecessary privileges granted through poorly designed roles.
- Users possessing excessive rights compared to others in their peer group.
- Administrative privileges for non-administrative users.
- Temporary changes to access privileges.

Finally, complexity makes it extremely difficult to assess relative risks and identify high-priority issues. IAM and security specialists end up responding to the most recent issue or the loudest complaint, rather than focusing on the areas that would yield the greatest improvements in security and compliance.

Problem #3: Correlation between Identity Data and User Activity

Sometimes the “right people,” with “the right access” to “the right resources,” do unauthorized things with that access, often unintentionally, but other times with malicious intent. Employees use valid credentials to violate policies (or commit crimes). “Privileged users” abuse their status to create new accounts, view confidential information they have no right to see, and grant themselves unnecessary permissions. (See the section below on “Doing Bad Things with Valid Credentials”)

Also, activities like multiple failed logins and privilege escalation can be vital clues for spotting malicious insiders, and also cybercriminals on the outside who have captured legitimate credentials through spear phishing or social engineering techniques.

Doing Bad Things with Valid Credentials

Hospital employees fired for viewing Kim Kardashian’s medical records

Three doctors at a Los Angeles Hospital gave their login credentials to six lower-level employees, who viewed 14 confidential patient records, including those of reality show star Kim Kardashian.

Shared passwords expose 4 million customer records

Employees of Vodafone in Australia gave acquaintances shared passwords that could have provided access to four million customer records, including credit card information.

Students in New Jersey change price of school lunch to $9,000

A board of education administrator posted administrative credentials on an online bulletin board. Students used the credentials to log on, change the price of a school lunch to $9,000, and make all classes electives.

Employees give outside lending companies access to customer files

Employees of a financial firm gave outside lending companies passwords to systems with customer data, including social security numbers and income information. The lending firms used the information to market loans to the customers.

Insurance firm baffled by illegal employee access

A former employee of a life insurance company illegally accessed customer accounts with social security numbers and bank account information. Unfortunately, the company could not determine which accounts had been accessed.

Sources: SC Magazine: Six employees fired at LA hospital for accessing patient records; Dark Reading: A Glaring Lesson in Shared Passwords; PC World: Hackers “School” a New Jersey School Data System; CNET News: LendingTree sues mortgage firms over security breach; Dark Reading: Penn Mutual Says Employee Might Have Disclosed Customer Data.

Unfortunately, today's IAM systems have no ability to correlate identity and access data (identities, policies, rights and resources) with security and user activities (such as logging on to sensitive applications, creating accounts, granting rights and downloading files). This means that patterns and clues are missed that could have identified vulnerabilities, and even attacks in progress.

No Easy Fix

To sum up the weaknesses in today's IAM systems, they:

- Allow policy violations and vulnerabilities to accumulate between periodic, labor-intensive, single-point-in-time certification processes.
- Lack tools to collect and process large volumes of data and to identify patterns that can pinpoint subtle violations and identify high-risk areas.
- Cannot use the "context" provided by identity data to separate legitimate from suspicious user actions.

Because of the tremendous volumes of data involved, these shortcomings cannot be addressed simply by adding a few database tables and reports to a provisioning or an IAG system.

Today's security and compliance initiatives demand something more: Identity and Access Intelligence.

Overview of an Identity and Access Intelligence System

An Identity and Access Intelligence System employs data warehouse and business intelligence technologies, tailored to analyze the connections in identity and access data, in order to produce meaningful, timely intelligence for IAM, compliance and security teams.

The basic components are illustrated in Figure 3.

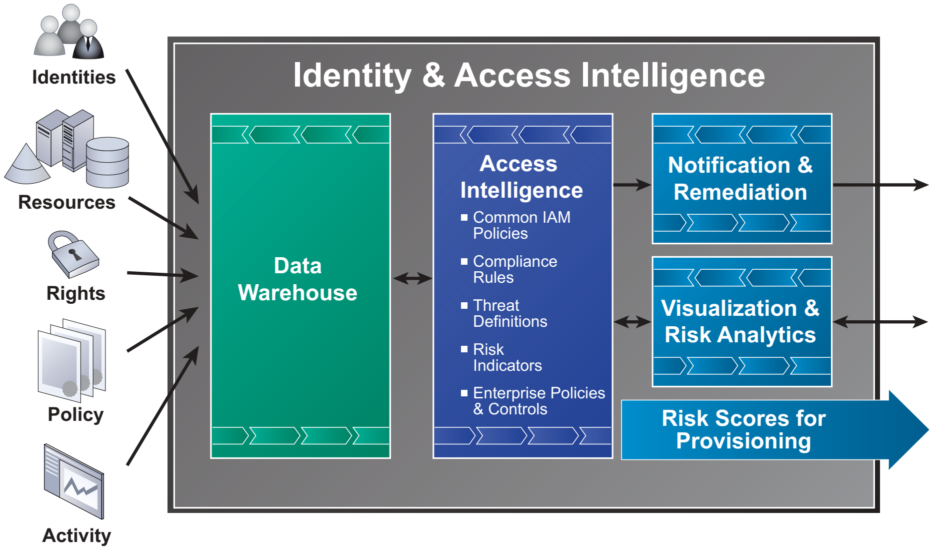


Figure 3: Components of an Identity and Access Intelligence System

Data Types and Sources

An Identity and Access Intelligence System works with data about:

Identities, information about employees, contractors, business partners and customers, as well as groups and roles. Aspects of identity include: Who are they? Where are they located? What job function do they perform?

What is their title? What projects are they working on?

Resources, such as applications, file shares, cloud-based services and hardware systems (ranging from mainframes and servers to mobile devices).

Rights, including permissions to access resources, perform add, change and delete transactions, and create and change users and accounts.

Policies, specifying who should have access to what, who is allowed to grant rights, how rights should be mapped to identities and roles, how rights should be requested, reviewed and approved, and how identities and rights should be certified. Policies can also include business rules, such as limitations on who can access protected data, requirements to prevent toxic combinations of access and ensure segregation of duties (SoD), and restrictions on who can approve transactions over a specific amount.

Activities, including security-related actions such as creating accounts and creating and modifying rights, and user actions, such as accessing resources, performing transactions, and downloading files.

These data elements reside in enterprise directories, account provisioning systems, identity and access governance systems, application databases, server and firewall logs, and Security Information and Event Management (SIEM) and Data Loss Protection (DLP) systems.

Data Warehouse

As noted earlier, an organization with 1,000 users might need to deal with several *billion* data interrelationships. That number might reach hundreds of billions for a very large enterprise with hundreds of thousands of identities and rights, thousands of applications and systems, and hundreds of policies and regulations. Moreover, traditional governance systems were architected to provide point-in-time data dumps, not ongoing access to key information.

To work with these massive quantities of data, an Identity and Access Intelligence System must utilize data warehouse technology. Enabling the ability to gather and correlate data in real-time is a crucial aspect of identity and access intelligence systems.

The data warehouse uses “connectors” and “collectors” to gather data continuously from enterprise directories, provisioning and governance systems, and other sources, then employs ETL (extract, transform and load) technology to transform information from disparate systems into a common format so it can be correlated and analyzed together.

Access Intelligence

The payoff for the enterprise comes in the “access intelligence” component of the Identity and Access Intelligence System. This combines IAM-specific knowledge with business intelligence and advanced analytic tools.

Business intelligence and analytic tools go far beyond simple ad-hoc reporting. They perform tasks such as:

- Data mining
- Statistical correlation and clustering
- Data visualization
- Determination of deviations from normal behaviors and trends
- Predictive analytics

With these tools, analysts and managers can sift through billions of pieces of interrelated data to detect patterns, pinpoint anomalies, and perform "what-if" analyses.

In an Identity and Access Intelligence System these analytic tools are enhanced by identity and access-specific information such as common IAM policies, compliance rules, threat definitions, and risk indicators.

In addition, identity and access data can be mapped against the policies and controls of a specific enterprise. For example, a financial institution could configure the tools to look for violations of regulatory rules concerning access to customer account numbers and credit card information.

Because Identity and Access Management concepts are embedded in the system, administrators and analysts can start taking advantage of advanced analytics quickly, without a long learning curve or an extended period defining relationships between the IAM data types.

Notification and Remediation

The output from an Identity and Access Intelligence System can include alerts that notify key IT and line of business personnel when potential policy violations are detected. These can trigger actions such as contacting users to determine if questionable actions were legitimate, and initiating immediate re-certification "mini-cycles."

In other cases remediation actions can be launched automatically, for example disabling or modifying user access. This automation speeds up remediation, and also lowers administrative costs.

Visualization and Risk Analytics

One of the biggest shortcomings of conventional Identity and Access Management solutions is that they are almost exclusively reactive. Administrators can respond to violations after they have been detected, but rarely anticipate problems or determine the areas of highest risk.

An Identity and Access Intelligence System can help IAM staff become proactive and focus on mitigating risks rather than fighting fires. Data visualization and risk analytic tools make it easier for administrators and managers to perform tasks like:

- Determining normal behavior patterns.
- Identifying individuals who deviate from group norms, and groups that deviate from company norms.
- Highlighting the policy violations that occur most frequently.
- Pinpointing the individuals and groups who cause the most violations.
- Sorting out which policy violations combine the greatest potential impact with the highest likelihood of occurrence, and therefore pose the greatest risk to the organization.
- Gaining insight into why some events are perceived to be higher risk than others.

In a moment we will look at examples of how these visualization and risk analytics can be applied.

Provisioning with Risk Scoring

An Identity and Access Intelligence System can also be linked directly to an account provisioning system to provide real-time risk scoring on provisioning requests. As illustrated in Figure 4, instead of relying on static policies, the Access Intelligence engine can supply the provisioning system with a multi-dimensional risk analysis in real time. Different approval workflows can be triggered based on the risk score.

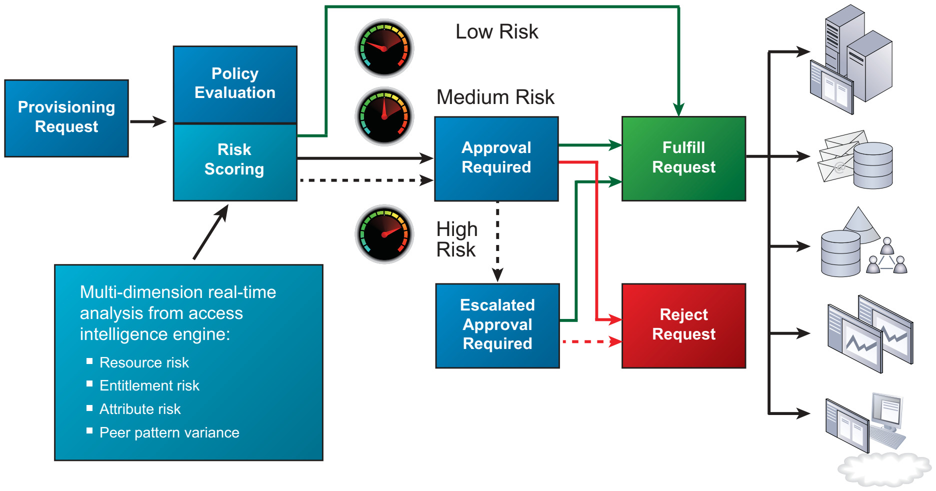


Figure 4: Intelligent Provisioning with Risk Scoring

This "intelligent provisioning" has the potential to significantly improve security, increase insight and visibility into risk, and increase confidence in the accuracy of the provisioning system.

How Identity and Access Intelligence Fixes the Shortcomings in IAM Solutions

An Identity and Access Intelligence System can help organizations overcome the "governance gap," the problem of identity information hidden by complexity, and the inability of traditional IAM solutions to correlate identity data with user actions.

Avoiding the Governance Gap with Continuous Monitoring

An Identity and Access Intelligence System can continuously monitor and assess identity and access data. For example, it can immediately alert IAM and operations staff when it finds policy violations, including:

- Orphan accounts (accounts belonging to employees who have been terminated).
- Individuals who retain rights associated with their former position after being transferred.
- People gaining unnecessary privileged or administrative access.
- Factors associated with vulnerabilities, such as shared passwords, weak passwords, and very old accounts.

Continuous monitoring prevents the accumulation of vulnerabilities and policy violations. It allows IT staff members to take immediate corrective actions without waiting three or six months for the next major certification exercise.

An Identity and Access Intelligence System can also close gaps caused by flaws in the provisioning and governance processes. For example, it can highlight:

- Rights granted through exceptions, or outside of the approved corporate workflow.
- Excessive numbers of accounts or permissions granted by an administrator or other privileged user.

With access to this continuous flow of intelligence, the IAM staff can address vulnerabilities proactively, rather than merely reacting to complaints or waiting for policy violations to be turned up in periodic audits.

Defeating Complexity with Access Intelligence and Risk Analytics

An Identity and Access Intelligence System provides the data warehouse and business intelligence tools to collect and correlate information from billions of related data points, as well as analytic and data visualization tools to discover patterns in that mass of information.

Correlation can uncover policy violations that would be difficult or impossible to discover with conventional IAM tools, such as:

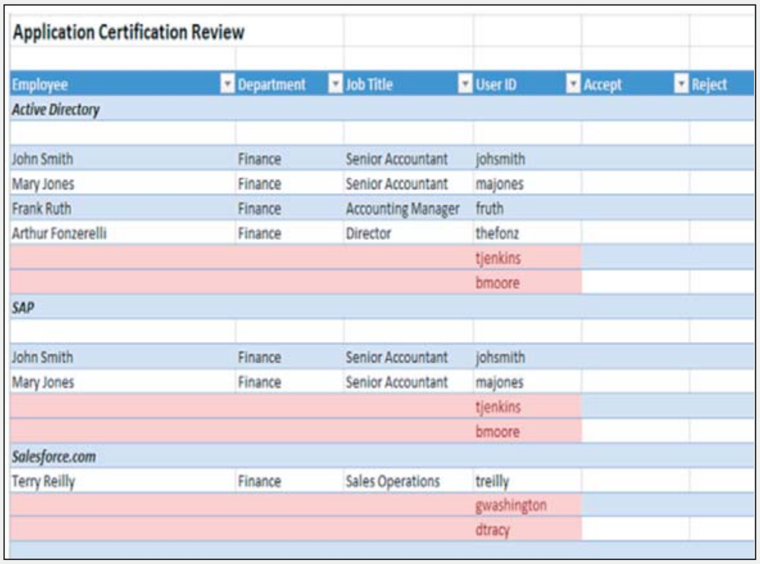
- Rights granted via inherited permissions or nested groups.
- Individuals with rights in excess of those granted to peers doing similar jobs.
- Excessive access rights for applications containing confidential data or data covered by regulatory requirements (often a symptom of “privilege escalation” associated with an advanced persistent threat or a malicious insider).

Other types of violations can be discovered as they are created, instead of waiting for periodic reviews, for example one person being granted rights to issue and approve purchase orders, in violation of segregation of duties rules.

An Identity and Access Intelligence System can provide risk analytics that help analysts focus on the greatest risks, as illustrated in Scenario 1.

Scenario 1: Finding High-Risk Orphan Accounts

This screen is part of a traditional orphan account analysis showing active accounts that are no longer (or were never) associated with a valid identity. This information is useful, but there is no context to help the analyst understand which of the hundreds or thousands of orphan accounts identified represent serious risks and which are trivial.



Application Certification Review

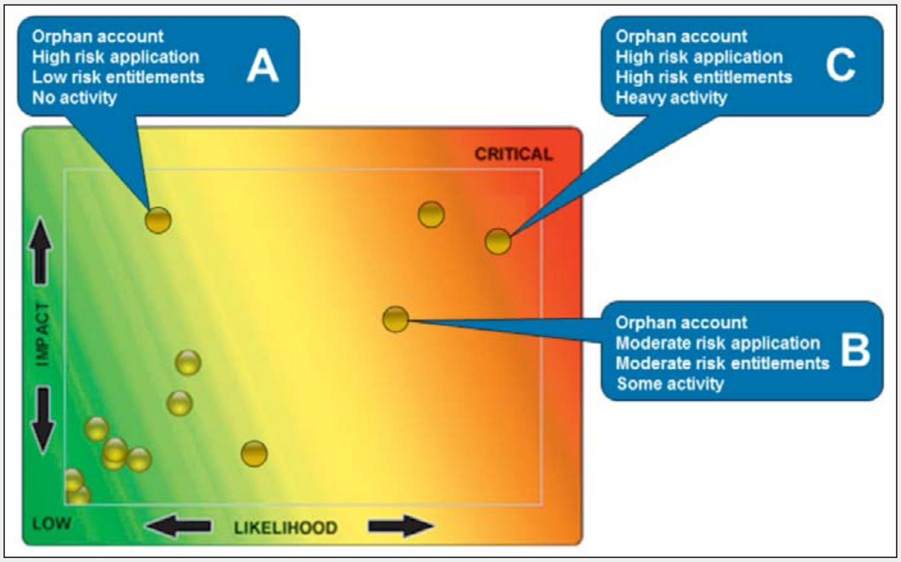
Employee	Department	Job Title	User ID	Accept	Reject
Active Directory					
John Smith	Finance	Senior Accountant	johsmith		
Mary Jones	Finance	Senior Accountant	majones		
Frank Ruth	Finance	Accounting Manager	fruth		
Arthur Fonzerelli	Finance	Director	thefonz		
			tjenkins		
			bmoore		
SAP					
John Smith	Finance	Senior Accountant	johsmith		
Mary Jones	Finance	Senior Accountant	majones		
			tjenkins		
			bmoore		
Salesforce.com					
Terry Reilly	Finance	Sales Operations	treilly		
			gwashington		
			dtracy		

Scenario 1: Continued

This “heatmap” plots individual orphan accounts based on the potential impact of a violation, and on the likelihood of that violation occurring.

The heatmap is produced by correlating:

- Orphan accounts.
- The risk of the application accessed by the orphan account (e.g. does the application contain confidential data, intellectual property, or security files).
- The risk of the entitlements granted to the orphan account (e.g. does the account have rights to edit or delete files or initiate major transactions).
- The level of activity of the orphan account.



Without analytics, an analyst might be tempted to first investigate orphan account A, because it has access to the highest-risk application.

But with the heatmap, the analyst can see that orphan account C should be the priority. Not only does Account C involve a high risk application, but the orphan account has powerful entitlements, and has been engaged in heavy activity.

The heatmap shows that even orphan account B is a greater risk than orphan account A. Although the application contains fewer risks, account B has more entitlements, and has been more active.

Figure 5 shows two more examples of the advantage of analytics. One chart shows trends in Segregation of Duties (SoD) violations, and the other shows, in real time, individuals who are being granted excessive access rights compared to peers in the same role.

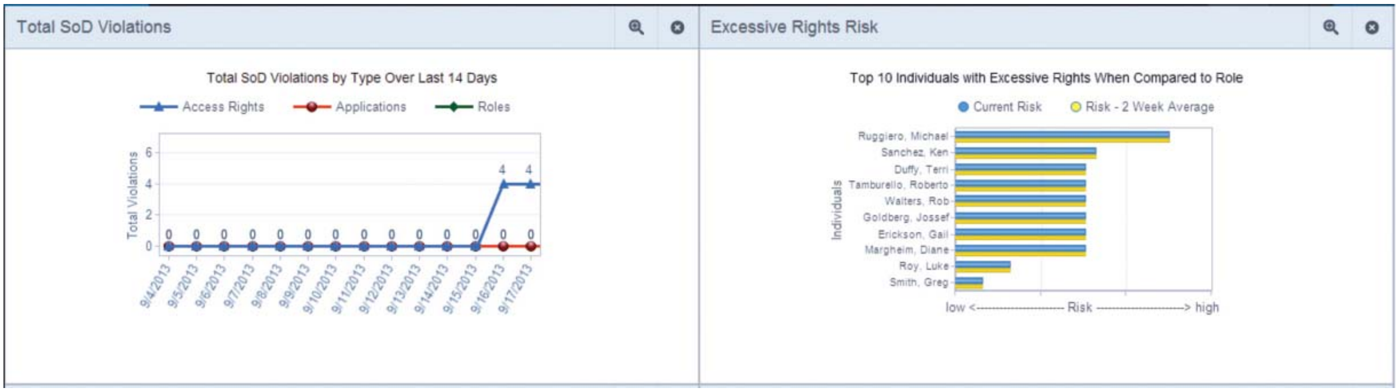


Figure 5: More Analytics - SoD Violations and Excessive Rights Compared to Peers

Business intelligence and risk analytics tools allow administrators to get to the heart of identity and access management problems by identifying policy violations that otherwise would have been lost in the sea of data, and by allowing them to focus first on high-risk issues.

Catching More Violations by Correlating Identity Data and User Actions

As discussed, today's Identity and Access Management solutions have no way to correlate identity and access data with user actions. Security tools like SIEM systems are good at correlating data, but they have limited views and understanding of identity and access issues.

An Identity and Access Intelligence System can identify many policy violations and malicious activities by observing activities such as:

- Several failed logins, followed by a successful login (often an indicator of an advanced persistent threat or other attack by cybercriminals).
- Multiple privileged accounts created and deleted within a short period, or multiple privileged accounts created for the same user (signs of suspicious activity by an insider).
- Creation of privileged accounts for a user in a non-administrative position.
- Large numbers of files downloaded outside of work hours or from a remote IP address.
- User activity that varies from others with similar job functions, locations, or titles.

Administrators alerted to these conditions can block insiders from taking unauthorized or inappropriate actions, and outsiders from probing web applications and using "privilege escalation" to penetrate critical systems.

Scenario 2 illustrates another technique: observing patterns that predict malicious activity, and detecting those patterns in real time.

Scenario 2: Flagging Risky Patterns of Activity

Several departing sales representatives are suspected of taking customer lists and confidential product information with them to competitors.

An analyst conducts a post-mortem analysis of their activity and notices several behaviors:

- Accessing the CRM system after hours.
- Downloading large volumes of customer data.
- Connecting via IP addresses different from their usual office location.

The analyst can specify these behaviors as suspicious when performed by sales representatives, account managers, sales directors and regional managers.

When the Identity and Access Intelligence System detects one of these behavior patterns, it immediately disables the individual’s access to key systems and notifies the appropriate sales manager.

In this scenario, correlating identity data and user activity allows the system to thwart harmful actions.

An Additional Benefit: Feedback and Process Improvement

An Identity and Access Intelligence System can provide yet another benefit: feedback to improve provisioning and governance processes. For example:

- If the same right is frequently requested by people with a given role, then that right can be added to the role, and if a right granted to members of a group is rarely or never used, then it can be removed from the group.
- If the Identity and Access Intelligence System detects one business unit where a high volume of access rights are granted outside of the approved process, then administrators can focus on training managers in that unit to use the process.
- If the system uncovers an unexpected number of policy violations by privileged users, efforts can be made to improve their training and monitor their actions.
- If an increasing number of violations of segregation of duties policies are detected, those policies can be better defined and more vigorously enforced.

In short, an Identity and Access Intelligence System can help organizations gradually reduce inefficiencies and errors in provisioning and governance processes.

The Ultimate Goals

Although this white paper has delved into details about the components of an Identity and Access Intelligence System, it is important not to lose sight of the broader goals. By gaining timely, complete identity and access information, enterprises obtain:

- Tools to better identify and manage risk.
- Information to simplify audits.
- Features to improve the effectiveness of existing provisioning and governance systems.
- A reduction in vulnerabilities, so they can better protect the privacy of their customers and their own intellectual property.

Readers are invited to learn more about Identity and Access Intelligence by calling 1-866-COURION or email us at info@courion.com.

About Courion

With deep experience and more than 600 customers managing over 10 million identities, Courion is the market leader in Identity and Access Management (IAM), from provisioning to governance to Identity and Access Intelligence (IAI). Courion provides insight from analyzing the big data generated from an organization’s identity and access relationships so users can efficiently and accurately provision, identify and minimize risks, and maintain continuous compliance. As a result, IT costs are reduced and audits expedited. With Courion, you can confidently provide open and compliant access to all while also protecting critical company data and assets from unauthorized access.

Worldwide Headquarters
Courion Corporation
1900 West Park Drive
Westborough, MA 01581 USA
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
Telephone: +91(20) 6687-9100

www.courion.com