



I D C T E C H N O L O G Y S P O T L I G H T

Integrating Identity and Access Management with SIEM to Enable Continuous Controls of User Activity

September 2010

Adapted from *Worldwide Governance, Risk, and Compliance Infrastructure 2010–2014 Forecast: Increased Regulatory Oversight, Privacy, Cloud Computing, and Smart Cities Drive Emerging GRC Obligations* by Vivian Tero, IDC #222214 and *Securing Identities Is Key to Success in the Cloud* by Sally Hudson and Vivian Tero, IDC #223639

Sponsored by Novell Corporation

This paper examines the role of IT continuous controls monitoring (IT CCM) solutions in operationalizing an organization's governance, risk, and compliance (GRC) objectives. It specifically looks at the value of solutions that provide out-of-the-box process and technology integration between identity and access management (IAM) and security information and event management (SIEM) applications, such as those offered by the Novell Compliance Management Platform (NCMP).

The Evolving Governance, Risk, and Compliance Landscape

A confluence of developments is compelling business organizations to reevaluate their existing compliance and risk management approaches and transition from static compliance measures to a continuous controls posture.

Chasing siloed compliance and risk management programs is neither a sustainable nor an economically efficient strategy.

In 2008, 22% to 33% of the digital universe was high-value information — data and content that are governed by security, compliance, and preservation obligations. IDC forecasts that high-value information will make up 35% to 45% of the digital universe by the end of 2012. Examples of high-profile events that drive the ongoing transition to more stringent legal, security, and regulatory regimes worldwide include the overhaul of existing global financial regulations (such as the U.S. Dodd-Frank Act and Basel III) and rising concerns over online data privacy and cybersecurity. In this environment, siloed and regulation-specific compliance programs can become costly to manage and maintain. Siloed GRC programs also increase the probability of policy conflicts and hyperenforcement.

Concerns over the pace of the global economic recovery also mean that IT budgets will continue to face constraints. Consider this sobering fact: While the amount of information is expected to grow by a factor of 44 from 2009 to 2020, IDC forecasts that the number of IT professionals will grow by only a factor of 1.4 during that period. Organizations therefore need to be smart and take advantage of opportunities to leverage their IT investments across security, compliance, and risk management projects.

Organizations continue to face data breach challenges. Failure to control excessive access rights and permissions within the datacenter's security perimeter underpins this problem.

The 2009 Deloitte Annual Global Security Survey reported "excessive access rights" as the top external and internal audit finding. The study also indicated that "unauthorized access to personal



information" was the number one finding from a privacy perspective. A 2009 IDC research study found that organizations averaged 14.4 unintentional data losses in 12 months, where 52% were considered unintentional data losses through employee negligence. The respondents also noted that excessive and/or out-of-date privilege and access rights were considered to have the most financial impact on organizations.

Organizational failure to resolve orphaned accounts in combination with the increased use of contractors and temporary employees underpins these audit failures. When an employee account and/or groups are deleted, the files associated with the associated user IDs are orphaned. In many instances, inactive and orphaned folders can be as high as 70% to 85% of the data in the distributed systems. IDC also finds that up to 60% of accounts on most systems are expired. A separate Ponemon Institute study concludes that approximately 90% of organizations have no process to identify the owner of files and 76% are unable to determine which individuals and roles are authorized to access the data.

Organizations could reduce their access control vulnerabilities and excess entitlements if they had the ability to monitor and correlate the functional and process dependencies across user activities, entitlements, and access rights with the data and applications. The ability to expose this intelligence in near real time instead of "after the fact" and kick off the appropriate remediation activities would mitigate insider-led data breaches. Automating the monitoring and remediation process typically requires the integration of traditionally siloed IAM and SIEM solutions. Integrating these point solutions can be a painful and expensive exercise. Today, organizations are considering solutions that have preintegrated business rules, workflows, analytics, and reports across these two systems.

The aggressive growth in digital data combined with the increased use of cloud computing and virtualization poses IT management complexity and underscores the need for dynamic risk, security, and compliance management.

IDC estimates that the digital universe will total 1.2 million petabytes by the end of 2010. By 2011, 50% of companies will have critical components of their production environments virtualized. By 2020, as much as 15% of the information in the digital universe could be part of a cloud service, and more than one-third of the digital universe will either live in or pass through the cloud. The introduction of new technologies and nontraditional devices into corporate networks creates new information that must be evaluated for security, risk, and compliance profiles. In addition, organizations should also assess how the new technologies alter the security, risk, and compliance profiles of existing information and computing assets. They should then update the associated technical controls and processes accordingly. Organizations should plan on having the ability to consistently manage and enforce their security, risk management, and compliance activities across increasingly complex and dynamic environments.

Cloud computing and virtualization provide additional use cases for solutions that dynamically manage user activities through integrated identity and access management and SIEM solutions.

The on-demand, self-service nature of cloud services makes it relatively easy to circumvent traditional IT governance processes for the provisioning of IT assets. Organizations also continue to face potential data leaks due to their inability to detect and delete orphaned accounts and compare user access rights against policy and operational knowledge. As such, extra care must be taken to manage and track identities, access, and entitlements across the organization's physical, virtualized, and cloud environments.

The increasing sophistication of emerging threats, as well as demand for greater security efficiency and automation of compliance and risk management activities, continues to underpin demand for SIEM. The Cloud Security Alliance notes that the lower down the stack the cloud provider stops, the

more security the consumer of the services is tactically responsible for implementing and managing. For example, in the cloud infrastructure-as-a-service scenario, organizations would still need SIEM to monitor events and activities across the workload (the OS, the applications running, storage, and some of the networking components such as the host firewalls).

Understanding the dependencies between the data, the workloads, and the underlying IT infrastructure is critical to ensuring and demonstrating adherence to a broad range of business, legal, regulatory, security, and operational requirements. Addressing user activity by integrating IAM with SIEM helps monitor and track these critical dependencies and enforce compliance with policies.

Enforcing Continuous Controls on User Activity

Foundational Technologies for IT Governance, Risk, and Compliance

Technical controls for risk management and compliance are articulated in the context of the following:

- Data confidentiality, including controlled access and data provenance
- Assurances on process and infrastructure integrity
- Application and data availability

Organizations have obligations to ensure that compliance and security policies are adhered to consistently across their on-premise and cloud environments. But there are obvious challenges. First, the highly abstracted nature inherent in cloud services poses challenges in instrumenting the dependencies across the technology stacks. Second, self-service provisioning capabilities make it easy to circumvent IT governance processes for provisioning assets and access to resources. Backward-looking (and static) audit reporting is a good first step for compliance purposes. However, preventing increasingly sophisticated attacks requires equally sophisticated real-time capabilities. Therefore, organizations should consider transitioning from backward-looking audit reporting to forward-looking continuous compliance and risk management approaches.

Context is critical to successfully executing a compliance and risk management program. Organizations need the ability to quickly reassess their risk appetites and the associated controls as their IT environments evolve. Organizations must also understand the trade-offs between security and business agility (e.g., availability requirements, operational budgets). Building out the capabilities to understand and monitor dependencies across IT infrastructure stacks is critical. To do this, organizations should have the following foundational capabilities:

- **Policy management and controls libraries.** The ability to define legal, regulatory, business, and operational policies and map them to control requirements and objectives as well as to technical controls and standards (such as ITIL/ITSM, CobiT, ISO 27001/27002/27005, CMMI, UCF/IIA). Granular security control requirements are defined in the context of confidentiality, integrity, and availability. These controls, in turn, are mapped to the compliance and risk management regimes that govern the organization. Ideally, organizations should strive to find the gaps across their IT architecture, security architecture, and risk and compliance frameworks. The analysis enables organizations to identify potential compliance conflicts, facilitate scenario planning for cloud services, define cloud service agreements (CSA), and create audit questions for cloud service providers.
- **Identity management.** The ability to define and enforce policies related to identities, access rights and permissions, and entitlements of authorized actors and business transactions.

- **Security information and event management.** The ability to securely and continually monitor security incidents and events increases in criticality when moving to the cloud or virtual platforms. This is driven by the more nebulous nature of these environments and the unpredictability of usage and access demands. The ability to track, alert, monitor, and immediately modify, if necessary, will allow organizations to maintain strong security and meet GRC requirements.
- **IT operations and incident management.** The ability to monitor, manage, and enforce policies and remediation actions for processes that support the availability and resiliency of the data and the application — including patch management, configuration management, change management, capacity and volume management, and storage management.
- **Information management.** The ability to define the value of the information (content, data, and metadata), the types of computing assets and resources, as well as the conditions under which activities (creation, capture, access, storage, archiving, data destruction, data protection) and business transactions can happen.

Getting Started on Continuous Controls of User Activity

Getting the identity house in order is a critical first step toward a comprehensive and continuous compliance program. The following components are core to this process:

- **Access certification.** First, business and IT stakeholders should collaborate and agree on a framework and a common language to define roles and requirements. This should include the following policies, controls, and processes to define:
 - "Who" owns and creates the information
 - "What" information and IT resources specific roles have access to
 - "Who" has permissions to access and perform transactions
 - Under "what conditions" the role can perform certain tasks and transactions
 - "How" the roles, permissions, and entitlements change over the life cycle of the data

It should also include a framework for mapping these controls to internal and regulatory mandates that affect user access. Second, the organization should consider automating these activities. Automation will document workflows (critical for investigation and audit purposes), identify potential compliance conflicts, facilitate scenario planning, and improve business responsiveness and agility. Features that enable discovery, role-based provisioning and access management, security monitoring, validation, compliance audits, and remediation are critical to access certification.

- **Access management.** Access management establishes secure access to corporate network resources across technical and organizational boundaries by using a combination of advanced access tools and technologies, including multifactor authentication, data encryption, Web SSO, and clientless SSL VPN.
- **Policy management and controls libraries.** Controls libraries maintain information on how the organization interprets internal and external policies into business processes and technical controls. Controls define the baseline for the organization's desired state of compliance and encapsulate an organization's risk tolerance. Maintaining the controls libraries facilitates the life-cycle management of controls and control objectives. Ideally, the controls libraries should also enable the organization to identify and rationalize common controls across security and compliance requirements. These capabilities expose potential compliance conflicts, overlapping compliance activities, and areas of hyperenforcement.

- **Log management.** Log management applications collect, manage, and archive large volumes of computer-generated event logs and audit data across security, systems, networks, and applications. Data is used for compliance and audits as well as to support IT operations. Log management tools are valuable in filtering and forwarding critical log data to SIEM, which in turn correlates events and logs against policies and controls; highlights critical security and compliance exposures; and triggers the appropriate alerts and risk mitigation and remediation actions.

Enabling continuous controls in the IT infrastructure stack hinges on the ability to dynamically enforce policies and automate remediation of key technical and process controls. Managing identities and user activities is core to building out this architecture so that risk management, security, and compliance protocols are embedded in the organization's business and technical processes. Organizations should consider solutions that would enable the management of user activities across their on-premise physical, virtual, and cloud-based deployments.

The dynamic and highly abstracted nature of cloud services and increasingly complex physical IT environments demand that organizations transition from static and periodic assessments of their compliance posture to an approach that continuously controls and monitors the IT environment. At a foundational level, solutions that facilitate continuous controls of user activity should be able to dynamically expose the dependencies between user identities and entitlements with their activities (from data supplied by log management/SIEM) and acceptable behavior and conditions (defined as baseline metrics in the policy and controls libraries). In addition to exposing the security and compliance posture of the organization, business rules could also be employed to trigger the appropriate alerts and risk mitigation and remediation activities.

Novell Compliance Management Platform for Continuous Controls of User Activity

The Novell Compliance Management Platform combines identity management (Identity Manager) with security and event management (Sentinel) in a single preintegrated solution with the following features:

- Identity Manager offers solutions that securely manage identity and access across physical, virtual, and cloud environments. Identity Manager automates provisioning and password management, supports self-service and user self-registration, automates approval workflows, enforces password policies, provides role-based identity administration, enables bidirectional password synchronization, and automates compliance documentation.
- Sentinel consolidates security event and incident logs from multiple sources (devices, systems, and applications) into a normalized data store; at the same time, it performs automated and continuous monitoring of security and compliance events. Sentinel's integration with Identity Manager is a key differentiator because it allows end-user and security compliance to be managed (in real time) via an integrated architecture.

The Novell Compliance Management Platform cross-validates identity, access, and policy information in real time. Policy changes and enforcement are done in real time. At the same time, NCMP tracks and correlates security and application logs as they are generated. Business rules and process automation allow for these logs to be continually checked against policies, thus allowing the application to trigger the appropriate actions whenever policy violations are detected. With this approach, the organization is able to continuously control and monitor user activity and take immediate, appropriate action.

Using the Novell Compliance Management Platform to enable continuous controls of user activity provides the following benefits:

- Process automation enables the organization to document that it is consistently enforcing its compliance and risk management policies. Inconsistent enforcement of compliance policies carries dormant legal and regulatory liabilities that most organizations would want to avoid.
- It enables the organization to respond to and mitigate potential violations in real time, as well as quickly adjust policies in response to business opportunities, while mitigating potential breaches to access and security policies.
- The integration with SAP BusinessObjects Access Control allows for tighter integration of separation-of-duties and access-compliance requirements across the business process and IT infrastructure stacks. This integration is a critical step in aligning enterprise and IT GRC compliance policy enforcement and reporting. It also offers opportunities to incorporate financial management with IT risk and security compliance activities.

Challenges

Customer Maturity and Budget Constraints

Deploying a solution to monitor and enforce continuous controls on user activity requires a degree of process and IT maturity. Organizations will need to rationalize policies and processes, as well as discover and audit for gaps across their IT architecture, security architecture, and risk and compliance operations. Most organizations will need guidance on the appropriate transition paths.

In addition, customers continue to face budget constraints and are therefore looking for solutions that provide them with the most immediate, quantifiable benefits.

Novell recognizes the process, IT, and budgetary challenges and recommends a phased approach. An organization could begin by cleaning up its access management, log management, and policy and controls management activities, as outlined earlier in the Getting Started on Continuous Controls of User Activity section. While these core capabilities are being deployed, and depending on the improvements in process and IT maturity and the immediate needs of the organization, it could then plan for the next stage.

Tracking Dependencies Across Information Infrastructure and IT Infrastructure

Organizations are better able to prioritize their security, compliance, and risk mitigation efforts if they have visibility into the value of the information and an understanding of the dependencies between roles, users, systems, and applications. Having the ability to be information aware, device and system aware, and identity aware is very critical in distributed, virtualized, and cloud-based environments. Novell's integration with SAP provides some level of information awareness for structured information (in databases and applications).

However, content (unstructured information) in endpoints, mobile devices, collaborative applications, and social networking sites is the fastest-growing information category. As information volume grows, organizations need to have a way to fine-tune their approaches for prioritizing their security compliance and risk mitigation efforts. Novell has a portfolio of products in its end-user computing business unit that could provide the necessary intelligence on the value of the information (content and its associated metadata). At some point, it would need to expose this intelligence to the Compliance Management Platform. Doing so will enable the organization to correlate user activity with the value and risk profile of the information across the database, application, and distributed endpoint environments.

Conclusion

IDC believes that the combination of increasingly stringent global security and compliance regimes, continued budget constraints, and rising use of virtualization and cloud services will compel organizations to adopt continuous controls of user activity. Doing so will enable organizations to execute their risk management and compliance programs more effectively.

Integrating identity management with security information and event management in a single, unified architecture is a critical differentiator for Novell Compliance Management Platform. Providing this real-time, enterprisewide view in a single console means that an organization does not have to log on to different applications to understand the true risks of an event. Also, the policy-based workflows ensure that responses are enforced in real time. Real-time policy adjustments and responses are critical to managing risks in dynamic, self-service, and highly abstracted environments.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests, contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC, visit www.idc.com. For more information on IDC GMS, visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com