

# Novell® Compliance Management Platform

# Rising Risk, Rising Compliance Costs

**By blending its award-winning identity, access and security technology, Novell has created the Novell Compliance Management Platform, an innovative solution that ensures that business policy becomes automated IT practice.**

---

1 [www.cnn.com/2008/BUSINESS/01/24/societegenerale.fraud/index.html](http://www.cnn.com/2008/BUSINESS/01/24/societegenerale.fraud/index.html)

2 IDC, "Identity and Security Management and Strong Information Technology Governance: Novell's Solution Suite Automates the Approach to the Perfect Union," Sally Hudson, February 2008

For millions of people around the world, Jan. 24, 2008, began like any other day—an ordinary Thursday in the middle of an average week. But for Societe Generale, the second-largest bank in France, that particular day was one of sobering revelation. It was on that day that the bank announced it had been the victim of a US\$7 billion crime.

In an announcement reported around the world, bank officials revealed that, over the course of several years, a rogue trader executed fraudulent transactions that cost the bank billions of dollars. According to company executives, it was the trader's knowledge of internal policies and process controls that had allowed him to hide the fraud for so long. Though Societe Generale reacted quickly to the discovery, dismissing related personnel and addressing recovery plans with investors and the media, the staggering losses significantly diminished the company's profits, shook customer and investor confidence and left the bank in the unenviable position of being the victim of the single largest act of fraud by an individual in the history of the securities industry.<sup>1</sup>

Although the fraud discovered at Societe Generale is one of the most dramatic examples of what can occur when corporate policy is breached, it is certainly not unique. Today companies around the globe struggle to achieve compliance with internal policies and external regulations—expending enormous resources only to end up with a piecemeal solution that may get them through this year's audit but will likely be woefully inadequate at tackling tomorrow's threats. Even as compliance spending continues to increase dramatically year after year, analyst firms like IDC report that "inadequately addressed compliance regulations will result in increased

violations and subsequent legal and public relations problems for corporations over the next several years."<sup>2</sup>

Further complicating the matter, business executives must now take personal responsibility for compliance issues. An organization's failure to comply with established policies—whether internal or regulatory—could be damaging not just to the company's brand and image, but also to the personal credibility of the management team.

Amid such a challenging business climate, executives are left to ponder several pressing questions:

- *Will the costs required to achieve compliance continue to escalate?*
- *Do we know with confidence our compliance status at any given moment?*
- *Have we automated the key business processes upon which compliance depends?*
- *Do our IT policies and infrastructure support our business goals and governance requirements?*

Fortunately, as companies around the world have already discovered, the tools and expertise to solve many of these challenges can be found in a solution offered by a company with decades of experience tackling the issues of security and policy enforcement. By blending its award-winning identity, access and security technology, Novell has created the Novell® Compliance Management Platform, an innovative solution that ensures that business policy becomes automated IT practice—so company executives can not only be confident in their compliance posture, but also trust that their image, brand and reputation are safe.

To understand the urgency of deploying such a solution, it is first important to consider why compliance is so difficult to achieve in the first place, and why thousands of companies are at risk from internal and external threats despite spiraling budgets.

## A Simple Matter of Communication

IT has become the cornerstone of most organizations' efforts to achieve compliance, with the primary goal being the automation and enforcement of policies originally developed on paper. And the most important product categories to emerge in the fight to enforce policy are identity and access management and security information and event management (SIEM). It is identity and access management products that determine users' identities and then grant and revoke appropriate access to corporate applications, while SIEM solutions provide an enterprise-wide view of perimeter security and other products, including intrusion prevention systems and firewalls. In short, identity and access management defines who *should* have access to corporate resources, and SIEM identifies who *is* accessing corporate resources—both of which are integral components of policy and regulatory compliance. Yet despite an enormous investment in these technologies—IDC expects the identity and access management market alone to reach US\$5 billion by 2011 as companies continue to struggle to make achievable, scalable, forward-looking compliance a reality.<sup>3</sup> But why? The answer, it turns out, is a simple matter of communication.

While modern identity and access management products are extremely adept at validating identity, provisioning resources and enforcing access roles, and SIEM solutions do an excellent job of aggregating security data from across the enterprise, in most cases, these two technologies are not very good at talking to each other. What exists in most organizations is two silos of information—

one that holds identity and access management policies (who gets access to corporate applications) and another that contains security data (who is accessing corporate applications). As in the case of Societe Generale, it is this “gap” between what should be happening and what is happening that provides an opening for criminal activity.

Consider this illustration to understand why the integration of identity and security management is so vital to achieve compliance: A typical financial transaction may need to touch an identity management system, an end-user terminal and a transactional database before it is complete and funds are dispersed. The identity management system verifies the identity of the user. In turn, both the end-user terminal and the database generate log data that is tracked by a SIEM system every time an action is executed on those applications. If, however, an employee has administrator access to the end-user terminal, the employee could conceivably circumvent the established process—the process that external customers are forced to follow—and initiate an unauthorized transaction, the result of which could be criminal fraud. With no common framework to tie together the elements of identity and security, a perpetrator could commit a crime by taking advantage of his or her access privileges or knowledge of internal processes.

### A Real-time, Holistic View

Bridging the gap between identity and security, the Novell Compliance Management Platform provides a real-time, holistic view of the enterprise and its compliance posture. The Platform cross-validates identity, access and policy information in real time, so the business always knows who is accessing what, when they are doing it and if they are authorized. In turn, if situations arise that are out of the norm—such as the illustration above where terminal access was not preceded by authentication—the Platform takes appropriate action in real time, from sending simple

**Identity and access management defines who *should* have access to corporate resources, and security information and event management (SIEM) identifies who *is* accessing corporate resources—both of which are integral components of policy and regulatory compliance.**

---

<sup>3</sup> IDC, “Identity and Security Management and Strong Information Technology Governance: Novell’s Solution Suite Automates the Approach to the Perfect Union,” Sally Hudson, February 2008

## To learn more about the Novell Compliance Management Platform and how it can help organizations bolster security, boost performance and lower operating costs, go to: [www.novell.com/cmp](http://www.novell.com/cmp)

**By combining user provisioning, access control and security monitoring, the Novell Compliance Management Platform delivers business process automation that gives users the appropriate resources, validated in real time, to ensure compliance with company policies—eliminating the gaps that have left so many companies at risk.**

notifications to initiating full remediation (e.g., revoking access to the user). The actual ‘remedy’ for the violation is determined by the policy of the organization and how it wants to manage a given situation.

By combining user provisioning, access control and security monitoring, the Novell Compliance Management Platform delivers business process automation that gives users the appropriate resources, validated in real time, to ensure compliance with company policies—eliminating the gaps that have left so many companies at risk. Rather than a piecemeal solution made up of complex (and expensive) product silos, Novell Compliance Management Platform delivers an enterprise-wide view and enforcement of policy as defined by corporate governance.

At the heart of the Novell solution is its ability to operate in real time. No other company delivers a comprehensive solution that addresses both identity and access management and SIEM in real time. While most identity management products take a periodic assessment of policy changes—creating a lag time between administrator actions (like revoking a disgruntled employee’s access to a financial database) and policy enforcement—the Novell solution affects policy changes as they occur, without lag time. In similar fashion, the Novell Compliance Management Platform tracks and correlates security and application logs as they are generated. This real-time approach allows the Platform to take appropriate action (the action can be as minimal an e-mail notification to an administrator or as proactive as

automating the immediate deprovisioning or revocation of access to resources) whenever something unusual—that is, something that could violate company policy—occurs.

Next, as policy and security data are gathered in real time, the Novell Compliance Management Platform correlates the information to identify legitimate threats. For instance, a user who legitimately logs in (i.e., has a valid username and password) to a financial application may simply be doing business as usual. However, if that user’s role within the company does not warrant access to the financial application, that login could present a serious threat. The Novell Compliance Management Platform can correlate the application log data with provisioning policies to catch this kind of security risk, which could easily go undetected by a piecemeal compliance solution—that is, until the auditors decide to take a closer look.

### ***Process Automation***

In addition to correlating identity and security, automation is also a key factor in the Novell solution’s ability to ensure compliance. Organizations are placing themselves at risk if they are depending on administrators and line-of-business managers to view and make sense of reports outlining user access to applications or waiting for the attestation of users themselves regarding compliance. Any time a business process becomes manual, the possibility of human error is introduced, not to mention the possibility of willful misconduct and increased expense. The ability of Novell Compliance Management Platform to pinpoint areas of concern and notify the appropriate individuals about those concerns takes the guesswork out of evaluating compliance. The Platform can even automate the process of provisioning access to corporate applications, based on a user’s self-service request, if the request is in line with company policy. Again, the need for manual intervention, with all of its associated risks, is eliminated.

Finally, the Novell Compliance Management Platform is a complete solution, built not only upon award-winning technology, but also on the culmination of years of experience deploying identity and security management software. Other compliance-related offerings claim to be comprehensive solutions with strong returns on investment, but in reality they are little more than a bundle of products, often without any consideration for the unique requirements of various industries and operational structures. In contrast, the Novell Compliance Management Platform encompasses integrated software as well as preconfigured identity and security policies and innovative success practices documentation—giving companies a significant head start on developing compliance solutions that fit their unique business needs. Indeed, deploying the piecemeal “solutions” is not unlike purchasing a bicycle that comes disassembled in a hundred different pieces. It may get you where you need to go, but you’ll have to do a lot of work before it’s ready. On the other hand, deploying the Novell Compliance Management Platform is like purchasing a bicycle that is not only fully assembled and road ready, but that also comes with a set of detailed directions to your destination. Naturally, the return on investment in the second example is much higher—in addition to offering a much smoother ride.

### ***Benefits of the Novell Compliance Management Platform***

As the ultimate governance solution, the Novell Compliance Management Platform delivers many compelling benefits:

1. The Platform minimizes the anomalies, uncertainties and violations that can ruin a company’s reputation. Its real-time capabilities provide the information needed to instantly remediate any divergence from business policy, assuring that little or no damage is actually done. Further, the Platform is built on battle-tested technologies that protect more than 6,000 customers worldwide.
2. The Platform can reduce the costs of ensuring and proving compliance by cross-validating data throughout the enterprise, rather than requiring identity and security management products to be managed and evaluated individually.
3. The Platform enables organizations to take advantage of new business opportunities without compromising security, integrity or a company’s reputation. For instance, users can be granted secure access to business partner applications without jeopardizing any unrelated systems or data from either company. Plus, the Platform has the flexibility to quickly bring on board employees of new subsidiaries (or acquisitions) while restricting their access to only the data they need.
4. User interactions with the Platform will promote trust. Rather than requiring a call to the helpdesk for password support, the Platform’s self-service password maintenance lets users manage their passwords for all corporate resources via a user-friendly graphical interface that will visually indicate which systems were affected by the change. In addition, users can initiate a self-service request to be provisioned access to a key application; that request can then be automatically approved if the user’s identity and role match the corporate policy for access to the application.

With these high-level benefits in mind, it’s now valuable to take a closer look at how the Novell Compliance Management Platform can be applied to several typical scenarios throughout the enterprise.

### **The Platform in Action**

A comprehensive approach to compliance addresses both inadvertent breaches of policy as well as acts of willful misconduct, as in the following illustrations:

#### ***Rogue Administration***

The Novell Compliance Management Platform guards against changes made by

**At the heart of the Novell solution is its ability to operate in real time. No other company delivers a comprehensive solution that addresses both identity and access management and SIEM in real time.**

**Using the Novell solution, administrators gain an additional level of inspection and validation—providing them visibility into not just which users have access to corporate applications, but also how often those employees log in to and use those applications.**

administrators that overtly or accidentally violate policy. For instance, a new accounting employee is assigned to work with the marketing department and is granted appropriate access to the company's finance application. Then a system administrator—either intentionally or inadvertently—grants the new accountant additional access inside the finance application, giving him visibility into the finances of not just the marketing department, but the entire organization. With the Novell Compliance Management Platform in place, the inappropriate access is not only immediately revoked, but the action is also correlated with relevant security data to determine who it was that granted the additional access, so the appropriate security personnel can be alerted. Certainly, given the employee's job function, it is quite possible that the provisioning error was simply a mistake—but the Novell Compliance Management Platform gives companies the insight they need to make that determination for themselves before a more serious security breach can occur.

### ***Streamlined Access***

The Novell Compliance Management Platform maximizes user efficiency because it automates the process of requesting application access. For example, a salesperson attempts to log in to a new lead management system but is denied because access has not yet been provisioned. The Novell solution automatically determines if the salesperson should have access to the application, and if so, creates a workflow request. The request is sent to an appropriate administrator, and if approved, the user is provisioned to the application and notified. This self-service model not only improves the experience and the productivity of users, but it also serves as an additional layer of automation to ensure policy compliance is maintained, and that it reduces the associated costs.

### ***Identity-enriched Security***

By mapping security information to identity profiles, the Novell Compliance Management

Platform enables organizations to be much more effective at identifying and investigating security breaches. Without this correlation, if a user were to attempt to access a sensitive customer database by overriding security protocols, database administrators would know little more than the fact that someone tried to break in. Using the Novell solution, those same administrators could quickly turn to an easy-to-read, real-time dashboard to determine who attempted the security breach, what else he or she has been doing recently and what other accounts that user has across the enterprise. This clear graphical overview of identity and security concerns throughout the organization enables administrators to make sense of mountains of security data, identifying legitimate threats while eliminating false positives.

### ***Provisioning vs. Utilization***

Identity management systems can identify which users are provisioned to which applications. But are those employees actually using the applications? That's a question that can only be answered when identity management and security management are correlated, as they are with the Novell Compliance Management Platform. Using the Novell solution, administrators gain an additional level of inspection and validation—providing them visibility into not just which users have access to corporate applications, but also how often those employees login to and use those applications. Tracking application usage is an excellent way to gauge whether corporate policies and role definitions actually line up with day-to-day operations.

### ***Role-based Provisioning***

Role-based Provisioning from Novell automates the process of granting appropriate access to resources, which reduces the complexity and cost of identity and security management. Our solution quickly and easily grants or denies access based on a user's role within an organization. Furthermore, it manages permissions according to depart-

ments, jobs or the specific tasks assigned to a person, minimizing the amount of IT administration required to add, delete or maintain system users' access rights. If your company is in a high-security industry, such as health care or financial services, you can ensure that access rights for role memberships are managed properly so you will always be in compliance with internal and external regulatory standards. Because access to resources is based on roles and policy that is consistently enforced, Role-based Provisioning from Novell increases the security of your valuable IT resources while making it easy to prove compliance with government and industry standards.

While these illustrations are in no way a comprehensive list of the capabilities of the Novell Compliance Management Platform, they do serve to demonstrate the scope of the Novell solution. Only by addressing such a broad range of challenges can the Platform actually ensure enterprise-wide compliance.

## Why Novell?

Like the example of the recent fraud at Societe Generale and hundreds of other similar situations, companies around the world continue to struggle with issues of policy compliance. Security and business policy violations continue to multiply and evolve, even as spending increases—leaving many organizations with a feeling that they have little recourse but to spend more. And that is why the Novell Compliance Management Platform is different from the piecemeal offerings that are in the market today. By blending its award-winning identity, access and security technology, Novell has delivered

**By combining user provisioning, access control and security monitoring, the Novell Compliance Management Platform delivers business process automation that provides users with the appropriate resources, validated in real time, to ensure compliance with company policies—eliminating the gaps that have left so many companies at risk.**

the ultimate governance solution—a platform that provides a real-time, holistic view of the enterprise to mitigate the risk posed by internal and external threats, and ultimately, to ensure an organization's image, brand and reputation are safe.

Novell expertise in compliance-related solutions is second to none. The company is not only an established leader in identity and security management, but is also a solution provider to thousands of organizations around the globe. That deployment experience allows Novell to go beyond just installing a patch-work of products. The Novell Compliance Management Platform combines powerful technology with preconfigured policies and documented best practices to provide a comprehensive approach to policy compliance—plus the most impressive return of investment available anywhere.

To learn more about the Novell Compliance Management Platform and how it can help organizations bolster security, boost performance and lower operating costs, go to: [www.novell.com/cmp](http://www.novell.com/cmp)

**Novell expertise in compliance-related solutions is second to none. The company is not only an established leader in identity and security management, but is also a solution provider to thousands of organizations around the globe.**

By blending its award-winning identity, access and security technology, Novell has delivered the ultimate governance solution—a platform that provides a real-time, holistic view of the enterprise to mitigate the risk posed by internal and external threats, and ultimately, ensure an organization's image, brand and reputation are safe.

[www.novell.com](http://www.novell.com)



Contact your local Novell Solutions Provider, or call Novell at:

1 800 714 3400 U.S./Canada  
1 801 861 1349 Worldwide  
1 801 861 8473 Facsimile

**Novell, Inc.**

404 Wyman Street  
Waltham, MA 02451 USA