

WHITE PAPER

Identity and Security Management and Strong Information Technology Governance: Novell's Solution Suite Automates the Approach to the Perfect Union

Sponsored by: Novell Inc.

Sally Hudson
February 2008

EXECUTIVE SUMMARY

This IDC White Paper examines Novell's identity and security management (ISM) solutions and how these integrated offerings can play a key role in enforcing security compliance for enterprise organizations. When properly implemented and deployed, these solutions help companies to:

- ☒ Avoid violations of government and industry regulations
- ☒ Avoid the leakage of intellectual property
- ☒ Drive down the cost of compliance through integration, consolidation, and automation

Strong security and governance programs should be symbiotic in nature. A total identity and access management (IAM)-driven governance, risk, and compliance (GRC) solution should ensure foolproof and accurate measurements of policies and practices across the enterprise. This ideally includes creation and life-cycle support for policy and standards development, solid and integrated access and identity administration, security and vulnerability scanning, and audit and remediation capabilities.

METHODOLOGY

IDC has incorporated elements of the following categories into the research methodology for this document:

- ☒ Reported and observed trends and financial activity within the industry
- ☒ IDC's Software Census interviews (IDC interviews all significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.)
- ☒ Product briefings, press releases, vendor financial statements, and other publicly available information
- ☒ IDC's extensive demand-side research initiatives

INTRODUCTION

IT and business professionals in enterprise organizations, generally acknowledge that GRC issues generate large amounts of confusion across organizations. The primary source of this confusion is the rapidly multiplying and increasingly complex U.S. and international regulatory environments.

Organizations worldwide are facing compliance issues mandated by Sarbanes-Oxley (SOX), Basel II, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Financial Institutions Examination Council (FFIEC), and the Payment Card Industry Data Security Standard (PCI DSS), as well as other government regulations and guidelines, such as the IT Infrastructure Library (ITIL) best-practices framework.

Executives must push their organizations to comply with these regulations or face personal liability and the threat of criminal and/or civil penalties. The ability to track user rights and privileges as well as combat authorization drift is an integral part of a strong compliance program.

IDC research shows that IAM has emerged as the foundation for a solid, secure compliance platform. IAM is the who, what, where, when, why, and even how of the IT infrastructure. It is a comprehensive set of solutions used to identify users in a system and control their access to resources by associating user privileges and restrictions with their established identity. This is accomplished via implementation of some or all of the following technologies:

- Web single sign-on (WSSO)
- Federated single sign-on (FSSO)
- Enterprise single sign-on (ESSO)
- User provisioning
- Advanced authentication (which includes public key infrastructure [PKI])

Where applicable, legacy authorization and personal portable security devices (PPSDs) such as secure smart cards, traditional hardware tokens, and security USB devices (see the Definitions section) are used. Additionally, fine-grained access mechanisms and capabilities for enterprise role management have emerged as critical functions in provisioning and deprovisioning users on the systems and subsequently enforcing compliance and providing better overall GRC capabilities.

To effectively achieve an enterprisewide ISM-driven environment, organizations must couple IAM capabilities such as those outlined earlier with security information and event management (SIEM) software. SIEM solutions include software designed to aggregate data from multiple sources to identify patterns of events that might signify attacks, intrusions, misuse, or failure. Event correlation simplifies and speeds the monitoring of network events by consolidating alerts and error logs into short, easy-to-understand reports. This also includes activities that collect and disseminate threat intelligence, provide early warning threat services, and can provide information on

countermeasures. The ability to automate these functions goes beyond better security; it can help ensure accuracy as well as aid IT organizations in saving both time and money in integration and manual efforts.

IDC research shows that the IAM market accounted for \$2.99 billion in worldwide software license and maintenance revenue in 2006. Compliance and corporate governance initiatives will significantly drive IAM software spending in the coming years. IDC expects this market to reach \$5 billion by 2011. Regulatory compliance is a strong growth factor here, both horizontally and vertically.

Government and industry regulations require aggregation of data and event management, coupled with the ability to identify and remediate internal threats based on user privileges. To meet these needs, vendors are releasing software products that combine SIEM and IAM to assist enterprises in producing compliance measurements that drill down to the individual user.

Adding to this is growing customer demand for analytical tools that allow user activity data to be combined with traditional peripheral security data. Ideally, the ability to collect data from an IAM platform, enrich it with data from SIEM systems, and do this within a fully integrated, automated, and real-time environment will allow companies to greatly increase security, aid in compliance, and help ensure corporate GRC initiatives.

SITUATION OVERVIEW

IDC research shows that regulatory compliance initiatives are rapidly becoming part of larger corporate GRC strategies. Security compliance and control solutions play a key role in enforcing corporate governance — a relationship that would seem obvious but often goes unrecognized.

In addition to the widely publicized Sarbanes-Oxley, Basel II, and HIPAA regulations, a number of other important government mandates continue to evolve worldwide, creating a dizzying maze of regulations and IT implementations that are difficult to assess, manage, and maintain on a global basis. When individual industry and corporate policy regulations are added to the mix, we can see why enterprises are often overwhelmed by the situation. Enterprises need to implement flowing, automated systems designed to accommodate strong security frameworks that provide auditing, archiving, and storage for compliance purposes. A wish list would include the following:

- Data must be easy to locate and produce for audit.
- The technology must allow for easy implementation of new controls because the compliance landscape is always changing.
- A proactive automated system does not permit an out-of-compliance action to occur.

Vendors that provide SIEM and IAM and combine industry best practices and internal policy requirements by controlling and automating their daily IT environments will be at the forefront of the ever-evolving compliance landscape.

Benefits of a Strong IT Governance Solution

IDC takes the position that the increasing complexities surrounding compliance have created a new class of vulnerabilities. The majority of security problems are caused by known vulnerabilities that the customer has not patched. IDC believes that inadequately addressed compliance regulations will result in increased violations and subsequent legal and public relations problems for corporations over the next several years. (See *Worldwide Security Products and Services 2007 Top 10 Predictions*, IDC #204678, December 2006.)

Compliance can be viewed as the natural by-product of good, integrated IT governance. Strong IT governance is by nature interwoven into all aspects of the enterprise. Risk assessment and risk remediation, as well as fraud prevention and detection, are also essential. The ability to perform these tasks in a timely manner and to view and act on data in real time is crucial to achieving GRC. This can be achieved with a solid ISM offering.

IDC recommends that a comprehensive ISM solution be evaluated based on answers to the following questions:

- How does it improve overall governance?
- How does it reduce risk, increase risk management, and facilitate remediation?
- How well does it utilize existing IAM solutions?
- How does it contribute to streamlining operations?
- Does it provide automated reporting and auditing functions?
- Does it provide real-time views and remediation if something falls outside the established policies for the IT infrastructure?

The last question is critical because events often deviate from the expected, so the system needs to be flexible. Furthermore, an ISM solution should fundamentally require integrating security management while simultaneously enabling and supporting evolving business goals. These in turn must be easily mapped to both government and industry-specific regulations.

Provisioning is key, especially due to regulations such as SOX, as auditors may demand reports on personnel policies, job descriptions, performance evaluations, training and development, and even succession planning. All must be accounted for within the IT infrastructure. Roles are groups of tasks that can be assigned to an individual, a group, or even an organization within an enterprise. They can be defined functionally (i.e., who does what within a business context) or structurally as related to IT processes such as application and resource access. Roles determine access parameters within the enterprise. The ability to define, manage, and effectively integrate roles based access control within the IT and business infrastructure can make or break a compliance implementation.

Coupled with the demand for a comprehensive identity and roles management capability is the need for a documented IT risk assessment and management process that adheres to an IT control framework. IDC believes that enterprises will seek to implement a flowing automated system that allows for a strong security framework including auditing, archiving, and storage for compliance purposes. Data must be easy to locate and produce. The technology must allow for easy implementation of new controls because the compliance landscape is always changing. A proactive automated system that does not permit an out-of-compliance action to occur is a key enterprise and system goal. By combining SIEM, IAM, control, and automation within the daily IT environment, enterprises will be able to achieve these goals.

Traditional Approaches to ISM and Compliance

Historically, efforts to collect and assemble the correct information in order to meet regulatory compliance have often been manual. These efforts are incredibly labor-intensive, painstaking, time-consuming, and prone to omissions and errors. The manual process is hindered further by the lack of tools and methods for reporting and auditing data once it is, in fact, collected. Any manual process is highly prone to error, and these endeavors translate into huge costs and distractions for the IT organization and the company as a whole.

IDC believes that 70% of all serious incidents are sparked by insiders (personnel with privileged access). As corporate perimeters are increasingly expanded, more nonemployees (e.g., contractors, consultants, customers, and partners) have greater access privileges than ever before. In universities, this group includes students and visiting professors. In healthcare, outsiders include doctors with patient privileges at multiple hospitals and other healthcare personnel working on a contractual basis.

Consider the following all-too-common scenario: Compliance regulations (e.g., SOX, Basel II) demand that Company A have a process that ensures that all relevant credentials, user accounts, passwords, and log-ins are removed whenever an employee or a contractor leaves the company. This process is called deprovisioning, and it typically must be enacted across dozens of applications within the enterprise. In today's environment, this often includes physical security, such as office access and building entry badges. Corporate credit cards and telephone calling cards must also be terminated. Timeliness is critical here, and individuals within the organization require access to the termination information almost immediately, along with the subsequent proof that it was done correctly in order to meet compliance standards.

While in theory this represents a relatively straightforward and linear process, it is no easy feat in practice, primarily due to lack of comprehensive, integrated tools and solutions to automate the process. Certain IAM software products such as WSSO and host SSO can (and do) provide a certain level of access management, but they must be coupled with provisioning tools to guarantee the correct access to the correct resources scattered throughout the enterprise. Assuming that this integration across the organization is complete — and this is often a *huge* assumption — Company A now finds it needs mechanisms to audit and report on these actions to close the compliance loop. When normal organizational boundaries and political barriers found within any company are added to this scenario, the entire effort can be overwhelming for any organization.

A seemingly obvious solution would be to automate these processes to achieve greater accuracy and economies of time and scale. Until recently, very few options have been available to alleviate the pain and streamline this tedious process.

Novell ISM Software Solutions

Novell Inc. has consistently been a leader in the IAM market space. Founded in 1983, the company employs more than 5,000 people worldwide and is headquartered in Waltham, Massachusetts, with key facilities located in Provo, Utah, and Nürnberg, Germany. Novell serves customers in varied market segments and offers a wide range of solutions in the datacenter, security and identity, resource management, workgroup, and desktop market spaces. Novell's ISM product line includes several products that focus on compliance-related functions. This section details each product and its key functions.

Novell Identity Manager provides a foundation for solid identity integration within an organization and ties this to a rules-based, automated provisioning capability. The software provides delegated administration functions (including user self-service). User provisioning automates the process of granting and changing access rights and, in some cases, audits the appearance of inappropriate rights in a user's profile. By automating time- and cost-sensitive manual procedures, user provisioning can sharply reduce the costs of granting necessary access to new employees, customers, partners, and suppliers.

The *Roles Based Provisioning Module for Novell Identity Manager* reduces the complexity and cost of identity and security management by helping IT managers establish access privileges to resources — including computer applications, telephone systems, and building security systems — based on role membership within an organization. Permissions are managed according to departments, jobs, or the specific tasks assigned to a person, minimizing the amount of IT administration required to add, delete, or maintain system user access rights. High-security organizations, such as hospitals and financial institutions, can ensure that access rights for role memberships are managed properly for both internal and external regulatory compliance purposes.

Roles based provisioning capabilities are increasingly in demand by organizations today. IDC estimates that provisioning software accounted for almost \$500 million of the overall \$3 billion IAM market for 2006 and forecasts that it will reach \$997 million by 2011. We believe the strong growth in provisioning software is due to several factors, chief among them are the Fortune 2000's need to meet regulatory compliance on both industry and government levels and their growing reliance on sophisticated, more granular IAM products. A large part of this growth projection is based on IT enterprise acknowledgement of roles based identity management as a key component in a secure, adaptable business process management environment. In fact, roles based access control is extending beyond the IT level and being recognized increasingly by the business side of organizations as essential in achieving security and adaptability while meeting regulatory compliance demands.

By providing a tightly integrated identity and role management solution, the module provides IT managers with greater transparency and flexibility in managing permissions. The software includes support for tactical decision making, segregation of duties, and attestation. The module is built into Identity Manager's metadirectory and therefore can take advantage of Identity Manager's real-time capabilities and comprehensive set of connectors. The result is that enterprise customers can use roles to provision, monitor, and record user access to protected information and resources and easily provide documented evidence to meet strict regulatory requirements.

Novell Access Manager is the company's WSSO product that allows trusted users to gain secure authentication and access to portals, Web-based content, and enterprise applications. The product provides IT administrators with centralized policy-based management of authentication and access privileges for Web-based environments and enterprise applications. It also offers customers strong authentication and identity FSSO. FSSO is the ability to share a user's log-in and authentication data across different Web sites and applications, both internal and external to the organization, using secure, standards-based protocols. The user is able to sign on to multiple Web sites regardless of the provider or identity domain, and organizations are able to separate employees from external parties to better meet compliance regulations. Access Manager is designed to help streamline this process. The software supports a wide range of platforms and directory services.

Novell Sentinel is the company's SIEM offering that provides real-time event monitoring and correlation, automated incident response handling, and compliance reporting. Sentinel automates the process of monitoring for policy violations, identifying and responding to violations, and delivering compliance metrics to demonstrate the effectiveness of critical IT controls. It consists of several modules that enable IT professionals to collect, correlate, monitor, and display data from thousands of events per second in real time. This software allows enterprises to address IT controls across multiple regulations while closing the knowledge gap between what should happen and what is actually happening in a networked environment. IDC believes this real-time capability is a significant value-add for enterprise organizations looking to increase security while addressing compliance demands.

Novell SecureLogin is the vendor's ESSO product and is designed to provide users with easy access to network and Web resources via a single, secure log-in. It reduces IT administration and cost by significantly reducing the number of help desk calls related to password resets and lowers the risk of data breaches by helping companies enforce consistent password policies. This can simplify compliance with internal and industry regulations. When the product is deployed with other components of Novell's ISM suite, enterprise customers have access to a complete, integrated identity and security management stack for supporting IT compliance, risk management, and governance requirements. SecureLogin enables integration with smart cards, biometrics, and proximity cards in conjunction with usernames and passwords. This aids organizations in their efforts to meet guidelines, such as FFIEC for online banking, that require more than one factor of authentication. The product currently supports Windows Vista, Windows XP, Internet Explorer, and Mozilla Firefox.

Novell Storage Manager is an identity-based file system management product with storage policies (i.e., size, file types, naming enforcement) and document retention capabilities, which are all very important features in meeting compliance regulations today. Storage policies are set in the directory based on users' identities and roles. Storage Manager then automates many common storage-related tasks, including quota management, directory renaming, migration, storage triage, and archiving. It can be used to manage storage on Microsoft Windows, NetWare, or Novell Open Enterprise Server–Linux platforms by leveraging their underlying directories.

Novell Identity Assurance Solution is Novell's modular offering for identity-based physical/building security, where the physical credential (i.e., building access badge) management is linked with IT systems for access and verification. It is especially important in meeting government HSPD-12 regulations. Novell's modular solution ties together Novell Identity Manager, Novell Sentinel, and third-party content from Honeywell for physical access control systems (PACS) and utilizes ActivIdentity software for life-cycle card management systems.

Novell ZENworks is from Novell's Systems and Resource Management (SRM) business unit and focuses on providing policy-enforced endpoint and wireless security software solutions, addressing the demands for securing the increasing number of enterprise mobile workers. Evolving in part from the Senforce acquisition in 2H07, the full product suite is designed to address critical endpoint security issues such as endpoint management, encryption, location-aware wireless control, personal firewall, removable media control, and network access control. A key feature is its central management console, which dynamically enables policy-based implementation of endpoint security, ensuring the enforcement of security policies for all employees regardless of location. In addition, the software offers a common log, providing enterprises with critical reports necessary for adhering to compliance regulations such as GLBA, HIPAA, and SOX.

The Big Picture: Bridging Identity and Security

The ability of Novell's identity management and SIEM products to function in an overreaching, integrated fashion by connecting directories, databases, and applications to achieve a full enterprise provisioning scenario for GRC is an important advantage for customers. Novell's individual products in IAM, SIEM, and security management can be effectively combined to create solutions to solve business problems (see Figure 1). Companies will find that this approach can be very effective in meeting regulatory compliance demands.

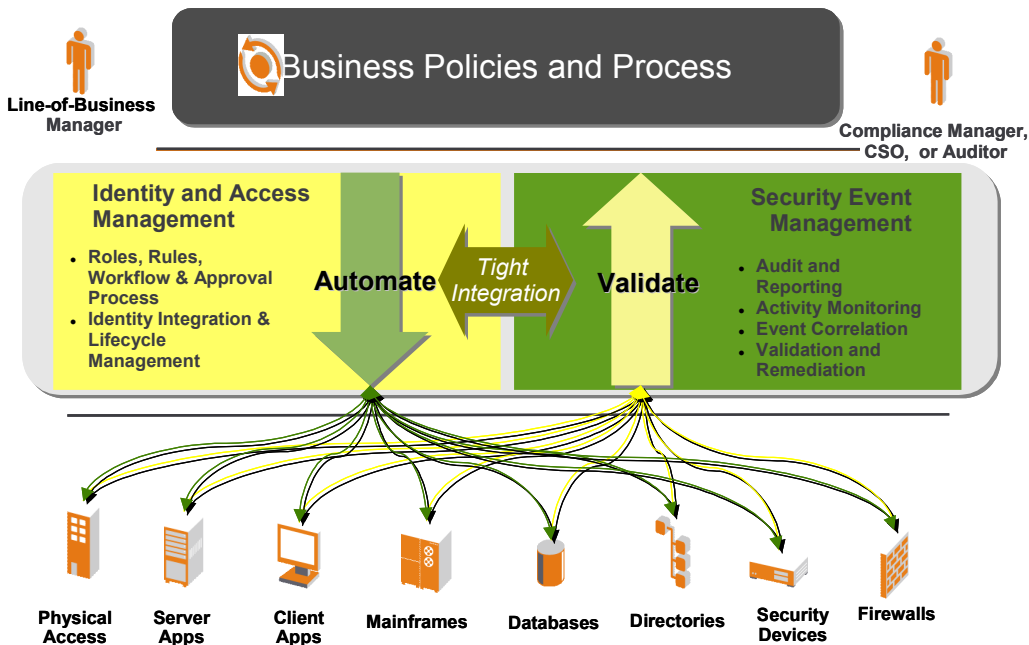
By utilizing Novell's Identity Manager as a foundation, companies can elect to add the Roles Based Provisioning Module. This module is designed to help people understand why they have access to what they do within an organization and can be configured to be very granular to go beyond just listing job functions and reporting structures. The Roles Based Provisioning Module can provide rules-based provisioning (e.g., where you are located and which print queue you use) and create approval workflow-based provisioning as an exception-handling mechanism.

The Sentinel real-time event monitoring system can trigger remedial workflows. When it is used in conjunction with the Identity Manager and provisioning functions, customers get a comprehensive identity-enabled security and compliance monitoring solution. This provides IT professionals with real-time information about events and threats and allows them to detect who did what in what context, and why it happened. These efforts, when properly executed, result in compliance recognition. The PCI DSS is a primary example of the necessity of combining IAM and security management with fraud detection and SIEM to achieve compliance with the established standard. PCI regulations demand that organizations (e.g., retail) must detect and immediately respond to actions that relate to identity theft or credit card misuse. Obviously, the financial industry cannot allow unauthorized three-day spending sprees, and this common real-world scenario illustrates the criticality of real-time capabilities. It also illustrates the importance of using identity as a context for overall activities. While many products today provide audit trails, the ability to look at identity and respond in real time within one product set can offer IT customers advantages in both security and integration economies of scale.

Finally, the convergence of physical and logical security is increasingly important to organizations. This is particularly critical in HSPD-12, which provides specific requirements for employee access and verification. Credentials can now be tied to a physical device, such as a smart card, to grant access to both IT systems and different parts of the building. While this is especially beneficial for government and government contractors, it is also important to other industries, such as manufacturing, financial, and banking.

FIGURE 1

Automation and Validation Supporting Governance, Risk Management, and Compliance



Source: Novell, 2008

Compliance and Customer Scenarios

Every year, standards are amended and refined, and organizations must continually scramble to keep pace with the evolving nature of regulations. Novell has architected its ISM products to respond to situations in real time. The goal is to allow customers to act/react in a matter of seconds versus a matter of days and to correct problems in real time rather than on a reconciliation basis. This is a key differentiator in Novell's approach. Many companies worldwide use Novell ISM technologies to address elements of their compliance needs. The following examples illustrate the application of ISM in different industries:

Standard Life (United Kingdom): Roles Based Provisioning

Standard Life is affected by several different regulations. The company found that it could meet a major requirement of all these regulations by implementing Novell's solution. Key elements are the ability to define business-oriented roles, assign users to these roles through rules or by exception (via approval workflow), and thereby grant access to various resources associated with those roles. The ability to enforce separation of duties and to report at any time on users' current access rights ensures that policies are followed. Standard Life has now achieved its compliance goal by managing approximately 12,000 users via 4,500 roles.

ABN AMRO: Compliance-Driven Access Management

Three major requirements drew ABN to Novell's solution: FFIEC strong authentication requirements for its Web-based banking applications; inability to provide consistent access control and delegated administration for its 40,000 business customers; and lack of agility in integrating third-party Web applications into its flagship CashPro Web Business Treasury and Cash application. By implementing Novell's solution, ABN achieved its regulatory goals, federated access with its third-party partners, and decreased administration costs.

bwin (Austria): Identity-Driven Security and Compliance Monitoring

To meet PCI regulatory requirements, bwin needed to get real-time information about fraudulent credit card activity. Other solutions it considered were not fast enough to keep up with the high credit card transaction load it experienced. By implementing Novell's solution, the company was able to save millions of euros in credit card transaction fees (which would be imposed if it failed to meet the regulations).

Northrop Grumman Corporation: Convergence of Physical and Logical Access

Northrop Grumman has two pressing business and compliance issues: to issue HSPD-12-compliant smart cards to over 125,000 associates and to reduce the costs associated with issuing badges for the many PACS it must maintain. Northrop Grumman is meeting both needs by issuing what it calls a "One Badge" that can be used for both physical and logical access. Novell's solution ties physical and logical access together by automating the HSPD-12 provisioning processes and handling the complexity of binding the smart card credentials to user accounts in both the PACS and enterprise computing systems.

Matrix of Compliance Capabilities by Customer Solution

Many government and industry regulations have common requirements with regard to their IT controls. Novell focuses most of its efforts on addressing these common requirements. These provide customers with building blocks to address their compliance strategies. Some of these common requirements are shown in Table 1, along with an indication of which Novell solutions address them.

TABLE 1

Matrix of Compliance Capabilities by Customer Solution

Capability	Customer Solution			
	Roles Based Provisioning	Compliance-Driven Access Management	Identity-Driven Security and Compliance Monitoring	Convergence of Physical and Logical Access
Directory-based user management	X			
Business-driven authoritative data sources	X			
User account provisioning/deprovisioning	X			
Approval workflow management	X			
User access recertification	X			
Password synchronization	X			
Password quality enforcement	X	X		
Access management		X		
Enterprise single sign-on		X		
Strong authentication		X		
Account management and user self-service	X			
Identity-driven document and file management	X			
Real-time activity monitoring and correlation		X	X	
Automated incident remediation			X	
Compliance reporting	X	X	X	X
Site/building/room access provisioning/deprovisioning				X

Source: Novell, 2008

FUTURE OUTLOOK

IDC has forecast the following trends as primary factors contributing to growth and shaping the development of the IAM market over the next several years:

- ☒ Regulatory compliance is the strongest growth factor in this market, both horizontally and vertically, on a worldwide basis.
- ☒ The need for ESSO and WSSO will increase steadily, driven by needs for secure access with strong systems management and administration capabilities.
- ☒ Provisioning and deprovisioning solutions will see gains beyond the United States and Western Europe, reaching into the Japanese and Asia/Pacific markets over the next several years.
- ☒ There will be more partnerships among the major players and other technology and service providers to provide customers with total end-to-end solutions.
- ☒ The unification of physical and logical security access via a single secure, seamless set of solutions has become the paramount goal of many IAM and security vendors. IDC believes that significant progress is being made in this area and expects a continued uptake and evolution of this technology over the next several years.

Additionally, given the rising importance of risk management, government regulations, and exposure through vulnerabilities, IDC forecasts other factors shaping the future market as follows:

- ☒ **SIEM/IAM convergence.** The demand for real-time security visibility is increasing. Products that deliver network intelligence must identify high-priority and suspect traffic. The ability to use behavioral profiling to catch noncompliant actions before they occur is becoming a necessity. The convergence of SIEM and IAM products is a natural evolution of this demand.
- ☒ **Application and software security vulnerability assessment.** As security becomes more important at the application level, new products will be introduced that are designed to assess the status of individual applications. There are tools that look at operational products such as databases and Web servers.
- ☒ **Unified security management.** Combined security resources are now being offered that couple security, storage, and systems management (3S). IDC's vision of 3S represents the convergence of storage, security, and systems management. 3S can provide a proactive way of avoiding regulatory compliance failures and also policy compliance failures. Business process-intensive regulations such as Sarbanes-Oxley and infrastructure-intensive regulations such as SB1386 (and similar state regulations) are requiring companies to provide assurances on the integrity of the information from its creation to its eventual disposition.

CHALLENGES AND OPPORTUNITIES

Novell is unquestionably a leader in the IAM market. The company's solid reputation for quality products and innovation has withstood the onslaught of competition in this area. The challenge for Novell is to concisely articulate the value-add of its products and services in IAM/SIEM and rise above the clamor created by multiple players in an increasingly confusing market space.

Historically, Novell has been weak in its approach to partnerships. The company has been working to correct that over the past 12 months by underscoring its role as a software company and dismantling a large portion of its services organization. Novell is now focused on developing healthy partnerships with integrators and is working diligently to ensure that it is on track with this plan.

Within the security and IAM space, IDC advocates that IT vendors develop tools that bring together event records, efficiently prioritize incidents, separate real security violations from false alarms, and aggregate security events from different locations, devices, and manufacturers. Moreover, vulnerabilities must be viewed as part of an overall security management infrastructure that takes into account security policy and compliance and risk management. In general, security software offerings for GRC must be able to provide a more aggressive and positive security model and not just respond to events. This is an opportunity for Novell to leverage with its ISM approach.

ESSENTIAL GUIDANCE

Customers with proper implementation of an ISM-related solution for IT governance and achieving compliance should realize the following benefits:

- ☒ Increased user productivity
- ☒ Increased predictability
- ☒ An automated datacenter, resulting in greater accuracy and efficiency
- ☒ Consistency across systems and processes within the organization

Achieving true enterprise security means that solutions need to be complete, not just tick marks on a compliance report. Enterprise customers are increasingly aware of the fact that satisfying compliance does not yield a secure environment. Likewise, a secure environment may not be compliant. Organizations must require that both compliance and security be present. IDC believes that internal and external compliance requires security management, but we caution customers not to ignore critical threat management issues that fall outside compliance concerns.

CONCLUSION

Increasing regulatory compliance mandates both in the United States and internationally, combined with budgetary and staffing constraints, will continue to drive organizations to look for better ways to cost-effectively manage their security infrastructures. It has become evident in the IT industry that IAM and SIEM products are key components of a compliance platform. When these two elements are properly implemented and deployed, the combination synergistically produces a strong GRC platform for organizations.

DEFINITIONS

- ☒ **Security software** covers a wide range of technologies used to improve the security of computers, information systems, Internet communications, networks, and transactions. It is used for confidentiality, integrity, privacy, and assurance. Through the use of security applications, organizations can provide security management, access control, authentication, virus protection, encryption, intrusion detection and prevention, vulnerability assessment, and perimeter defense. All these tools are designed to improve the security of an organization's networking infrastructure and help advance value-added services and capabilities.
- ☒ **Compliance** can be defined as conforming to any type of rule or requirement mandated by a law, regulation, or policy, whether the rule is being enforced by an external governing body or an internal best practice. Security compliance is defined as the products and services that have security as their primary function yet also allow companies to enforce compliance, which represents a combination of complying with both external regulatory requirements and internal corporate policies and best practices.
- ☒ **Security information and event management (SIEM)** solutions include software designed to aggregate data from multiple sources to identify patterns of events that might signify attacks, intrusions, misuse, or failure. Event correlation simplifies and speeds the monitoring of network events by consolidating alerts and error logs into a short, easy-to-understand package. This market also includes activities that collect and disseminate threat intelligence, provide early warning threat services, and can provide information on countermeasures.
- ☒ **Identity and access management (IAM)** is a comprehensive set of solutions used to identify users in a system (i.e., employees, customers, contractors, and so on) and control their access to resources within that system by associating user rights and restrictions with the established identity. Subcategories of the IAM market include Web single sign-on and federated single sign-on; host/enterprise SSO; user provisioning, including granular authorization and policy rights and risk and entitlement management; and advanced authentication software (e.g., PKI).
 - ☐ **Web single sign-on (WSSO)** enables companies to administer and consistently enforce user access to Web applications and provides SSO services to users. WSSO software enables companies to administer and consistently enforce user access to Web applications. WSSO provides Web application security and identity management to employees, customers, partners, and contractors.

- ❑ **Federated single sign-on (FSSO)** technologies are derived from this market as well. FSSO is the ability to share a user's log-in and authentication data across different Web sites and applications, both internal and external to the organization, using secure, standards-based protocols. The user is able to sign on to multiple Web sites regardless of the provider or identity domain, and organizations are able to separate employees from external parties to better meet compliance regulations.
- ❑ **Enterprise single sign-on (ESSO)** enables users to log in to internal applications, databases, and other corporate systems with just one identity. ESSO (sometimes known as host SSO) enforces password policies and eliminates the need for employees to remember multiple passwords. ESSO is a core component of a successful enterprise IAM architecture. A strong ESSO platform should provide a standards-based, secure approach to systems sign-on by eliminating the need for multiple passwords and allowing customers to leverage their IT existing investments while further expanding their identity management infrastructure.
- ❑ **User provisioning** automates the process of granting access rights, automates the process of changing those rights, and in some cases, audits the appearance of inappropriate rights in a user's profile. By automating time- and cost-sensitive manual procedures, user provisioning can sharply reduce the costs of granting new employees, customers, partners, and suppliers the necessary access.
- ❑ **Advanced authentication** includes software tokens and software designed to support hardware authentication solutions (tokens, smart cards, biometrics). It also covers many services associated with the creation, dissemination, validation, and protection of digital certificates. A portion of this market also includes PKI technologies.

Additional IAM categories include **legacy authorization**, such as RACF and ACF-2, and **software licensing and authentication tokens (SLATs)**. These are parallel/serial port tokens or USB keys that authorize the use of software on a particular device.

**As of 2008, IDC is adding personal portable security devices (PPSDs) to the IAM market, which includes smart cards, traditional authentication tokens, card management systems, and secure USB devices.*

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2008 IDC. Reproduction without written permission is completely forbidden.