

Securing and Managing Your Enterprise: An Integrated Approach

Table of Contents:	2 Simplifying Management Across the Enterprise
	2 Choosing Integration
	4 Realizing the Potential of Policy-driven Automation
	4 Addressing Governance, Risk and Compliance
	6 Using Key Capabilities
	9 Planning Your Deployment: Best Practices and Project Milestones
	10 Growing Your Enterprise through Integration and Automation



Simplifying Management Across the Enterprise

Many IT administrators see security and systems management as separate functions. Most IT departments still reflect this division.

Your organization has a dizzying number of platforms, directories, systems and applications—all requiring your attention and administration. You know you need to manage this complex infrastructure correctly, or your diverse resources will cease to be assets, and instead become a serious drain on administrative time and budget. And even worse, if the management program you deploy isn't comprehensive, unsecured devices can expose your systems to significant security issues.

So how can you integrate and automate fragmented management tasks while addressing a full range of governance, risk and compliance (GRC) issues? You can choose the security and system management solution from Novell®. It's a solution that helps you secure and manage your enterprise from the desktop to the data center—and you benefit almost immediately as you lower costs, reduce complexity and mitigate risk.

In theory, the formula for achieving these benefits is straightforward:

$$\text{Integration} + \text{Policy-driven Automation} = \text{Simplicity}$$

In reality, such a formula can be difficult to deploy—and this is where Novell can help. We implement the formula through a common, enterprise policy store that ensures uniform execution and consistency. Then,

we provide a set of policy-driven components to automate routine security and resource management issues.† These components are completely integrated, working together to address the management challenges your IT department faces. It's a solution that allows you to spend your time and resources on what really matters—growing your business.

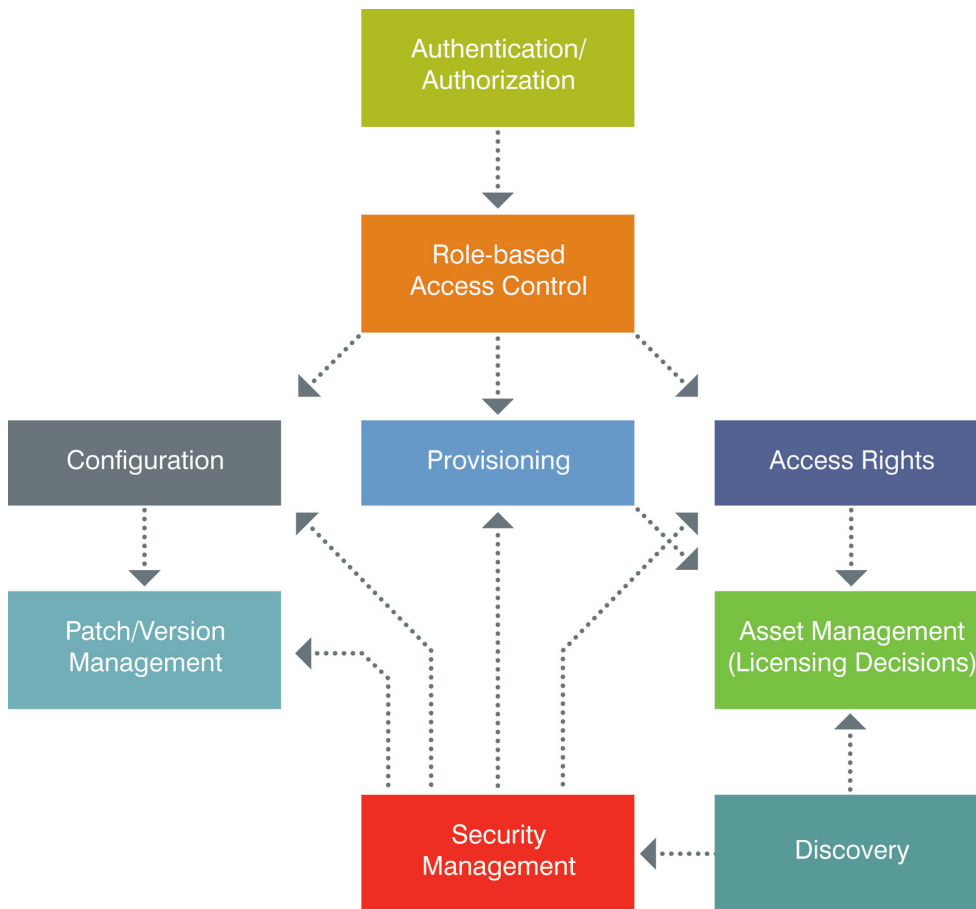
Choosing Integration

Many IT administrators see security and systems management as separate functions. This is because, in the past, systems management has included tasks such as physical device inventory tracking, device configuration and provisioning, software license monitoring, patch installation and upgrade deployment; whereas, security management has included identity access management and the ability to prevent threats, intrusion and malware.

Most IT departments still reflect this division. One group is concerned with system management questions such as, "How do I deliver application X to device Y?" and a separate group is concerned with security management questions like, "Which users of device Y should be granted access to application X?"

This two-group approach doesn't reflect the dependencies that exist between security and systems management. The following diagram shows the intricacy of these dependencies:

† These components are listed at the end of this paper.



In an integrated system, the upgrade would be deployed automatically in response to the security warning, keeping both teams productive and protecting the system at the same time.

Figure 1. Historically, system management and security have been viewed as separate functions, but as this diagram shows, there are numerous dependencies—a strong argument for the superiority of an integrated approach.

Failing to address these dependencies can lead to situations where both the security and systems management teams are doing their jobs, but many problems are not addressed because the groups don't work together effectively. For example, an intrusion detection tool operated by the security management group notes anomalous activity at a user endpoint, indicating a potential security breach. The security team is completely unaware, however, that the systems management group already has an upgrade available to prevent the breach. The systems management group, in turn, has the upgrade, but is delaying its deployment in favor of other tasks

because they are unaware of the potential breach. In an integrated system, the upgrade would be deployed automatically in response to the security warning, keeping both teams productive and protecting the system at the same time.

Another example of the efficiency of an integrated system is a security monitoring system detecting a user, without clearance, attempting to access sensitive data. In this case, business policy would be automatically enforced to modify the user's access pending an internal review.

Identity and system management from Novell provides a comprehensive solution for addressing governance, risk and compliance (GRC).

Identity-driven Security and Resource Management reduces the burden on your IT staff, helping them stay focused on building your enterprise.

Realizing the Potential of Policy-driven Automation

The absence of integrated security and systems management programs is not the only challenge your enterprise faces. Your IT department may be spending valuable resources manually performing tedious, time-consuming processes that could be automated easily with an identity-based security and system management solution.

Transferring a user to a new group is a typical example. Often, when users are moved to new assignments, they must be granted new access rights, have their previous rights removed and be provided with a new seat license. Since security management must remove previous rights and systems management must provide a new license, setting up new group members involves an e-mail exchange between the group leader and two separate IT departments. But that's just the minimum—transferring users might also require higher-level approvals, either for the access rights or the license. And an administrator might have to manually change the access list and activate the seat license, which adds more time to the process (in addition to any delays experienced if an approving manager is too busy to reply or is out of the office).

The costly manual elements of this process can be eliminated by integrating security and systems management. When an employee changes departments, the new manager simply submits a request via the company portal, a workflow sequence is initiated and the employee can become productive almost immediately.

Addressing Governance, Risk and Compliance

Identity and system management from Novell provides a comprehensive solution for addressing governance, risk and compliance (GRC):

- **It puts governance in the hands of the people who know what their employees need.** *You will no longer have IT departments creating business policies for your users based on software parameters instead of company objectives.*
- **It mitigates risk.** *With automated workflows in place, steps aren't forgotten and resources are secure and accessible. Disgruntled employees won't be able to cause system damage because access was terminated in one database but missed in another.*
- **It transforms corporate and regulatory compliance.** *Automated policies and reports can change compliance from an overwhelming, seemingly impossible job, into a set of processes that are simple to implement and track.*

Governance

With the right governance system in place, you can simplify IT management and reduce overall costs.

Simplify IT Administrative and Maintenance Burdens

Identity-driven Security and Resource Management reduces the burden on your IT staff, helping them stay focused on building your enterprise. By making access rights dependent on your business policies, governance is no longer restricted by software capabilities. Business units can make decisions about which individuals have access to which resources, allowing IT to function as it should—in the role of implementer.

Since rights can be assigned based on policy with Identity-driven Security and Resource

Management, the rights-distribution process can be automated (with the option for semi-automated or manual workflows). This eliminates an enormous amount of tedious and error-prone manual labor. And when security management and systems management are integrated, workflows can provide the appropriate machine images and capabilities to users' desktops, laptops or mobile devices. An integrated system also provides their access rights, which eliminates even more work. The end result is enhanced IT efficiency and a better experience for your end users.

To further simplify administrative processes and reduce the governance burden, an inheritance feature is available to automatically grant a specific set of resources and rights to all the employees in a particular supervisor's work group or business unit.

Reduce Costs

Eliminating manual tasks translates directly into cost savings for IT organizations by reducing the number of hours required to equip users with the correct machines and the appropriate access rights.

Improved visibility into asset usage, specifically the usage of software licenses, can also save your business money. Armed with reports that integrate licensing, installation and usage data in one place—and with detailed information about desktops, servers and other network assets enterprisewide—IT managers can precisely tailor licenses to real needs, avoiding unnecessary fees for software that isn't used.

Costs associated with password management can also be reduced via Identity-driven Security and Resource Management. Through a combination of single sign-on (which reduces the likelihood that users will forget their password) and self service (which allows users to reset their own pass-

words), helpdesk calls associated with password resets can be reduced anywhere from 30 to 90 percent.

Risk

Today's organizations don't want to assume unnecessary risk. That's why many of them are turning to Identity-driven Security and Resource Management.

Improve Risk Management

Security is a huge component of risk management for IT organizations, with sensitive data protection and disruptive exploit prevention topping the list of challenges. But Identity-driven Security and Resource Management ensures a fully coordinated response to all types of security-related exploits.

To protect sensitive data, Identity-driven Security and Resource Management automatically ensures that access to sensitive data, applications and other computing resources is granted only to authorized individuals.

It can also help you improve risk management through integrated security and event monitoring. It aggregates and correlates the masses of security-related data that are continuously generated by network devices, displays an integrated real-time view of network status and triggers automated responses by other system components such as deprovisioning an account or upgrading software.

Finally, Identity-based system management eliminates security loopholes. It can retire unused software and hardware resources, and protect your system's many endpoints. Endpoint security management protects data through whole-disk encryption for laptops and prevents users from transferring sensitive data to USB or Bluetooth-based memory devices.

Eliminating manual tasks translates directly into cost savings for IT organizations by reducing the number of hours required to equip users with the correct machines and the appropriate access rights.

Identity-based security and system management provides an integrated, automated, secure solution for the day-to-day administration and management of your IT resources. It provides reliability, flexibility and scalability for your IT department, business units and individual users enterprisewide.

Compliance

When it comes to security, you can't just assert that your systems are safe, you have to be able to prove it. And that's why you need Identity-based Security and Resource Management.

Enhance Regulatory Compliance

Regulatory compliance, as it relates to security, has two components:

- *Implementing security policies and procedures such as access control, integrated security/event monitoring and endpoint security management.*
- *Providing documented proof that the organization is complying with its stated policies and procedures*

When access requests and other security matters are handled via e-mail, not only can providing proof of compliance be difficult, but simply documenting the process can seem impossible. In contrast, when you automate security-related procedures with a centralized, policy-driven engine, you can easily track employees and resources, ensure consistent enforcement of laws and regulations (such as HIPAA and SOX) and provide full documentation as part of the process.

Additional Benefits

There are many other reasons to deploy identity-based security and system management.

Increase User Productivity

Manual provisioning and lack of integration can create downtime for users, which depletes your organization's profit margins. Your enterprise needs to ensure that users have fast, uninterrupted access to the data and functions they need. Both the automated provisioning and single sign-on (SSO) features enhance user productivity.

Automate Data Center Management

System management can help you look forward to increased virtual machine use and a compelling "do-more-with-less" scenario. When data center management is automated, it is possible to reconfigure physical and virtual machines to meet demand. For example, servers can be reconfigured to handle the requirements of a financial system at the end of the month, or to handle higher-than-average Web traffic during a sales promotion.

Ensure Consistency Across Systems and Processes

You can achieve consistency across processes—one of the central principles of the Information Technology Infrastructure Library (ITIL). ITIL is a collection of best practices for IT management in 11 functional areas: helpdesks, incidents, problems, change, configuration, releases, availability, capacity, finance, service level agreements (SLAs) and continuity. And because Identity-driven Security and Resource Management adheres to the ITIL standards, you can be sure you will get optimum performance from your IT resources.

Identity-based security and system management provides an integrated, automated, secure solution for the day-to-day administration and management of your IT resources. It provides reliability, flexibility and scalability for your IT department, business units and individual users enterprisewide. Implementing the Identity-driven Security and Resource Management solution doesn't require a "big-bang" initiative—it can be achieved in small, manageable steps. The following section outlines the key capabilities required for success in the various functional areas.

Using Key Capabilities

We recognize organizations may already have some of these capabilities in place;

however, we have built our own offerings based on open standards, including connectivity with Web services functionality. This approach enables Novell products to integrate with pre-existing tools and legacy systems. But regardless of the systems you are currently running, the capabilities listed below are central to your success.

Discover

Discovery/Asset Management

An IT team cannot manage a device if it doesn't know the device exists. Visibility into assets, and particularly into licensed applications, can enable you to make better decisions regarding licensing needs and can result in significant cost reductions. The first step for improving security and resource management is discovering which systems within your network need to be secured and managed. Key capabilities in the Discovery/Asset Management category include:

- *Automatic network device recognition and discovery*
- *Routine application discovery*
- *Application suite recognition*
- *Continuous machine image and application version visibility*
- *Software reconciliation licensing and purchasing data importation*

Manage

Configuration Management

In an optimized system, device application delivery is integrated with user access rights provisioning. Key capabilities in the Configuration Management category include:

- *Change control for remote management and application update deployment*
- *Patch control for remote security patch management*
- *Integration with security monitoring system to enable automated responses to exploits*

Visibility into assets, and particularly into licensed applications, can enable you to make better decisions regarding licensing needs and can result in significant cost reductions.

Provision

Centralized Policy Engine

A centralized engine ensures consistency across your enterprise and reduces your IT department's administrative burden. Key capabilities in the Centralized Policy Engine category include:

- *Association of access rights with user roles as defined by business units*
- *Dynamic assignment and automatic modification of access rights based on changes in user roles*
- *Automatic, manual or mixed assignment of roles and rights*
- *Reports organized by roles, by rights associated with specific roles, and by users associated with specific roles*

Integrated Identity Store

The authoritative-source approach Novell assumes when multiple data sources are involved helps resolve political disputes over data ownership. Most systems take a last-commit approach that allows critical data to be controlled by whatever source last wrote to the database. In contrast, the authoritative source approach mandates that data can only be changed by a single, designated source. This ensures that line-of-business and data owners are certain their data is accurate. Key capabilities in the Integrated Identity Store category include:

- *Connectivity with multiple data stores to build "one view" of the user*

The authoritative source approach mandates that data can only be changed by a single, designated source. This ensures that line-of-business and data owners are certain their data is accurate.

Compliance auditing is becoming a part of everyday IT administration. You need to ensure you have the functions required to meet regulators' demands and facilitate compliance.

- *Authoritative-source approach to resolving conflicting data*
- *Bi-directional connection with systems (so business processes can be integrated, and IT departments can have flexibility in designating authoritative data sources)*
- *Real-time detection and response to enable a proactive (preventive) approach to security issues*
- *Policy violation detection involving the inappropriate use of two or more connected systems by one individual*
- *Total enforcement of business policy, even on super administrators and other trusted users*

Password Management

To deploy a single sign-on system, your company needs enterprisewide password management. Key capabilities in the Password Management category include:

- *Availability of user self service through the Web without logging into the network*
- *Ability to implement password policies on an enterprisewide basis*
- *Password synchronization on an enterprise-wide basis (including legacy systems)*
- *Single sign-on using advanced authentication options, such as biometrics, smart cards and tokens*

Workflow

Efficient, user-friendly workflow that automates processes as much as possible (while allowing human intervention) can significantly increase productivity and reduce your IT department's administrative burden. Key capabilities in the Workflow category include:

- *User-friendly design tools for creating and managing workflow requests*
- *Detailed, automated documentation tool*
- *Dynamic routing of workflow and approvals to the right role/person based on defined organizational information*
- *Ability to delegate approval authority*
- *Automatic escalation of requests to an alternative approver if time elapses*

- *Integrated management console for administration of identity and access management administration*

Access

Access Management

Sophisticated access management is crucial for reducing security risk and achieving regulatory compliance. Key capabilities in the Access Management category include:

- *Web- and client-based single sign-on*
- *Endpoint device authentication that includes desktops, laptops and mobile devices*
- *Support for federation to internal and external partners*
- *Adherence to industry/open standards*
- *Protection of private user information*
- *Secure processes for transmitting changes in access rights over the Internet*
- *User access events and changes in access rights reporting*

Secure

Security Management

The security data you need is available, but for you, the challenge is evaluating that data and effectively responding to the threats it presents. Key capabilities in the Security Management category include:

- *Data aggregation from multiple, disparate sources*
- *Data correlation based on time, location, user, group and process—or more complex needs*
- *Pre-designed and custom reporting*
- *Event-based design*
- *Automated response to security exploits*

Compliance, Dashboard, Reports and Auditing

Compliance auditing is becoming a part of everyday IT administration. You need to ensure you have the functions required to meet regulators' demands and facilitate compliance. Key capabilities in the Compliance, Dashboard, Reports and Auditing category include:

- *Active dashboards that show compliance and risk status*
- *Focus on policy violations and anomalies, not all data*
- *Reports for both business and IT managers*
- *Integration of siloed data to enable understanding of true system status*

Endpoint Security Management

You can now protect your systems' most vulnerable areas—the endpoints. Endpoint security management provides integrated security at the endpoint for USB, wireless, data and application control. Key capabilities in the Endpoint Security Management category include:

- *Ability to prevent unauthorized USB devices*
- *Data encryption on endpoints to protect against theft*
- *Location awareness for wireless security*
- *Policy-based management for security policies*

Orchestrate

Data Center Automation

When you automate the provisioning of data center resources, you can better meet the constantly changing needs of your business. Key capabilities in the Data Center Automation category include:

- *Ability to adapt to workload requirements, hardware health and business policies*
- *Integrated management of physical and virtual machines*

Planning Your Deployment: Best Practices and Project Milestones

To simplify deployment, your IT department needs definitive goals. With the following best practices and suggested milestones, you can begin to implement Identity-driven Security and Resource Management and transform your vision of an integrated, efficient enterprise into a reality.

Align IT to Business

- Adopt a process model to govern the project, such as ITIL or Cobit.
- Obtain executive sponsorship.
- Involve IT executives in business discussions.

Evaluation and Design

- Determine if pre-existing conditions need to be addressed before the project launches.
- Develop a solution roadmap of what the enterprise will look like after the project is completed.
- Include line-of-business units (such as HR or accounting) that own applications in the request for proposal (RFP) creation.
- Define the business processes to be automated.
- Map your existing enterprise data model.

Proof of Concept

- Focus on access to legacy or siloed applications.
- Identify vendor customization requirements.
- Consider paying for a more detailed proof of concept (POC) proposal—with the price credited toward the final purchase.
- Define success factors based on business requirements, not technical minutiae.

Production Preparation, Pilot and Rollout

- Set realistic organizational timeline expectations.
- Make sure the solution you choose can support roll-back.
- Create a centralized identity vault.
- Find project champions within user groups and train them first.

Installation Sequence

- Install software.
- Set up connected systems.
- Activate the software.
- Configure password management.
- Configure entitlements.

When you automate the provisioning of data center resources, you can better meet the constantly changing needs of your business.

- ❑ Configure audit and reporting.
- ❑ Configure workflow and user applications based on business policies.

Documentation

- ❑ Ensure documentation addresses audit and compliance needs.
- ❑ Automate documentation production.

Additional Comments

- ❑ Identity and access management projects will succeed if taken in stages.
- ❑ Not all technologies may be initially required; most are ultimately used, with very little shelfware.
- ❑ Avoid solutions that disrupt existing systems during deployment.
- ❑ Align early-stage deliverables with primary business drivers to achieve quick-win

return on investment (ROI) and to build internal support for the project.

- ❑ Focus on the total cost of the project over time, not just the cost of software or support.

Growing Your Enterprise through Integration and Automation

Governance, risk and compliance are major challenges for today's IT organizations. The Novell approach to this challenge, Identity-driven Security and Resource Management, provides an integrated, automated, policy-driven solution. In addition to specifically addressing GRC issues, the Novell solution can reduce costs, support business goals, enhance user productivity and promote consistency across your entire enterprise.



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

Identity-driven Security and Resource Management Components

Novell ZENworks Asset Management	Provides discovery for all enterprise resources, with reports that integrate licensing, installation and usage data
Novell ZENworks Configuration Management	Provides policy-driven automation for software setup, updates, healing and migration
Novell Identity Manager	Translates business policies into IT controls and compliance mandates across all connected systems
Novell Access Manager™	Secures corporate Web resources while providing for a consistent policy-based authentication and access experience
Novell Sentinel™	Integrates identity-managed systems with other IT resources to ensure business policy is followed
Novell ZENworks Orchestrator	Automates provisioning of physical and virtual data center resources to meet changing needs

Learn more about how Novell can help you secure and manage your enterprise at: www.novell.com/innovationline