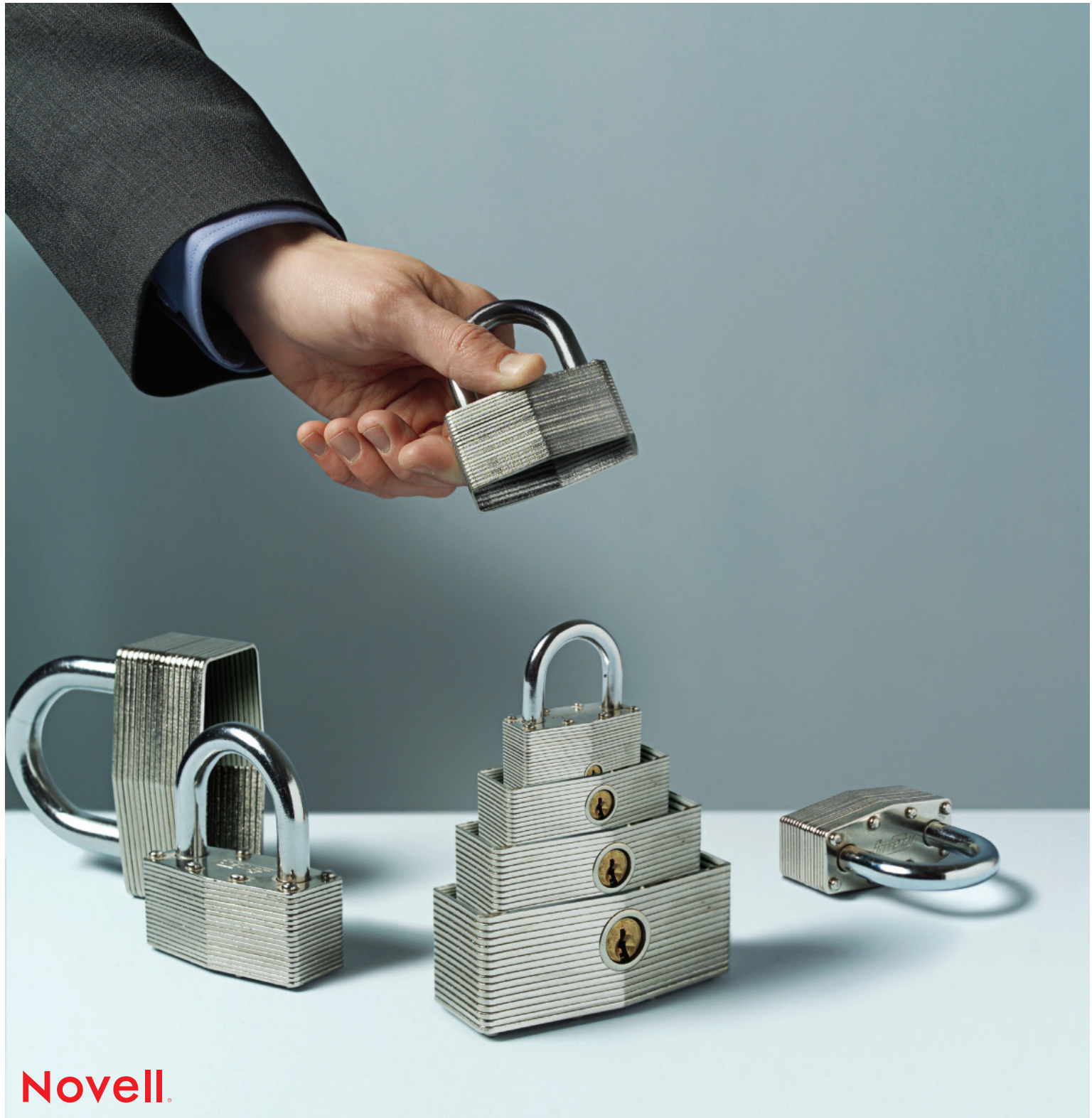


IDENTITY AND SECURITY SOLUTIONS

Build a trusted environment



Novell.

N

Trust

Trust should be at the core of every good identity and security management solution. Just having the management and security procedures written down is not enough—you need to trust that the solution you choose will allow you to conduct business as usual and ensure that policies are being enforced and regulations are being met. In short, **it's making IT work as one.**



novell.com/security

Built-in Security

Novell® Compliance Management and Identity and Access Management solutions manage identities, automate provisioning, manage access to applications, and enforce and prove regulatory compliance. **We deliver all this in a way that interoperates and integrates with your current applications and operating systems.**

Solving your identity and security challenges is at the top of our agenda. Novell offers two comprehensive solutions—one for Compliance Management and one for Identity and Access Management. These solutions offer the following capabilities:

Compliance Management

1. **Compliance Automation and Validation**
2. **Access Governance**
3. **Security and Vulnerability Management**

Identity and Access Management

1. **Identity Lifecycle Management: User Provisioning**
2. **Identity Lifecycle Management: Role Management**
3. **Identity Lifecycle Management: Storage Management**
4. **Access Management**
5. **Enterprise Single Sign-On**
6. **Password Management**





COMPLIANCE MANAGEMENT



Visibility from every angle. Compliance Management solutions deliver on the promise of infrastructure software to simplify business governance, mitigate risk and ensure compliance throughout the enterprise.

We offer technologies that inspect and enforce activities relative to business policies and processes, thus reducing the risk of security vulnerabilities, improving response time and increasing the transparency of compliance tasks. With Compliance Management solutions from Novell, customers can demonstrate compliance with both internal and external regulations, while reducing costs and freeing resources to drive top-line growth.

Scenario 1:
Compliance Automation and Validation

Scenario 2:
Access Governance

Scenario 3:
Security and Vulnerability Management



“We have a much greater ability to manage user identities, and especially to ensure the removal of access rights from former employees who no longer work for the company. With help from Novell, we can now protect our assets and simplify identity management.”

Walter Mondino
IT Security Manager
Grupo Arcor

1

Scenario 1: Compliance Automation and Validation

In today's complex enterprise, it is extremely difficult to centrally track who has access to what. However, without this insight, you cannot correctly report on enterprise activity to meet your regulatory compliance obligations and mitigate risk. Novell technologies monitor your compliance and security status in real time, so you can take corrective action immediately—while a violation is in progress—instead of discovering it after it's too late.

Customer Situation

A large financial services firm in Asia has to deliver 24x7x365 access to its systems and data without violating a growing number of industry and government regulations. This was becoming increasingly difficult in the firm's IT environment, which included Linux, UNIX, Windows and mainframe operating systems. Because of the volume of data produced, only high-priority systems could be fully monitored—even with a full team of analysts—and the log files remained separate, which complicated the process of reporting to auditors and regulators.

The difficulty of collecting and analyzing data also forced the IT staff into reactive mode—responding to suspicious events months after they occurred. Furthermore, the manual processes of gathering and analyzing data were costly and error-prone, and the firm's written security policies were not followed consistently.

The Solution

The firm deployed compliance automation and validation capabilities to deliver centralized, real-time monitoring and event source management for networks of every size. And due to the complexity of the firm's existing systems, it chose to work with a trusted Novell partner to implement its new Novell technology. This global Consulting Systems Integrator (CSI) helped the firm leverage Novell products in the most efficient way.

The firm's CxOs now get a complete picture of security and compliance status, even in a mixed IT environment with widely dispersed network components. Our software collects and correlates security event data from all across the network and standardizes it to make it usable. Instead of having dozens of logs in different formats, the firm's analysts now have easy-to-use logs in a uniform format, which cuts the time and costs involved in proving compliance.

These technologies have also increased the firm's agility. Because of the complexity of its systems and the regulatory requirements it had to follow, the firm could not react quickly to changing regulations or security threats. Now, however, IT administrators can implement new policies and automate their enforcement almost immediately, using a single console. The capabilities that come in compliance automation and validation automatically alert administrators and take predefined, customizable actions when they detect a policy violation or network threat, storing all activities in a central log file for easy access and reporting.

Because the firm's IT administrators were staffed in various locations across the continent, instructing them on how to monitor and administer the capabilities was a daunting task. However, by using a remote Novell training instructor and virtual classroom technology, all the IT staff were efficiently trained in a single training engagement regardless of location, saving the firm both time and money during deployment.

With Novell technology, IT administrators can now work proactively to prevent problems and can intervene immediately to stop violations before they endanger the firm. And if a problem does occur, the firm has a Dedicated Support Engineer on site to help get everything back on track quickly.

2

Scenario 2: Access Governance

In a complex enterprise, governing access to information resources can be an uphill battle. You need to make sure that users can do their jobs, but roles change so quickly that granting access is increasingly risky and costly. If time-consuming manual processes are leaving you vulnerable, access governance can help. You can eliminate error-prone manual processes, support compliance and bring access management costs under control with Novell Access Governance Suite.

Customer Situation

A leading global financial services firm was struggling to comply with government and industry regulations such as SOX, PCI DSS and Basel II. It needed a way to replace its error-prone manual processes with automated processes, so it could manage access and prove compliance. The firm needed a new system for access certification and compliance reporting. It also needed better processes for separation-of-duties review and certification between departments.

Automation and scalability were also important factors in the firm's decision for a solution. It realized that automation was needed to ensure that user access was limited to what each user actually needed to perform his or her job, that any access violations were identified and eliminated, and that the entire system could scale as the enterprise evolved and grew.

As a financial services firm, it needed to prove to its customers that their personal data was safe. The value of its brand depended on its ability to protect that information and maintain that trust. If the firm failed to reduce access-related business risks, those risks could ultimately harm its reputation and success.

The Solution

The firm decided to implement access governance as part of a broader Compliance Management solution. By leveraging Novell Access Governance Suite, the firm was able to enforce access policies, streamline certification processes and prove compliance. With this comprehensive product, the firm now has the ability to see who has access to what, and who authorized that access. Novell Access Governance Suite provides an automated review and certification process for all users' access. It also validates that entitlements have been granted or revoked.

With our technologies, the financial services firm can now confidently manage user access, lowering cost, complexity and risk, while proving compliance with industry regulations. And to ensure that it knows how to best manage its new technologies, the firm decided to work with Novell Technical Training. Novell Technical Training met with the IT department, assessed the situation and skills of the staff, and trained them on how to use the new products. With this system in place, the firm is now free to focus on projects that will grow and improve business. It can provide users access to information they need while governing their roles and maintaining compliance.

3

Scenario 3: Security and Vulnerability Management

Threats to your business can come from inside and outside. But no matter where a threat is coming from, our technologies can help you manage that risk more effectively. We are a leading provider of security information and event management (SIEM)—a service that allows for continuous monitoring of all enterprise activity, evaluating what is normal activity and what is anomalous, risky activity. When this service is coupled with the other capabilities we deliver through our Compliance Management solutions, you can trust that your systems are secure and compliant.

Customer Situation

A prominent financial brokerage firm in Europe was concerned about preventing fraud and protecting its consumers and itself from financial loss. However, when the firm looked for compliance and security solutions, they tended to be fractured and made SIEM even more complicated. In addition, industry security and compliance regulations continued to multiply and become more complex. Among other requirements, the industry specifications insist that the firm maintain a secure network, protect stored data, implement strong access management measures, regularly monitor and test networks, and maintain a comprehensive information security policy.

With millions of customers, thousands of internal users and hundreds of applications and databases, the firm was spending significant time and effort compiling reports to prove its compliance. Compliance was managed on a departmental basis, which was inefficient and made it difficult to ensure that the same approaches and policies were being applied uniformly across the company. To reduce the cost and effort of compliance and improve security reporting, the firm needed an automated, centralized resource for monitoring and managing security, information and events.

The Solution

By using Novell technologies to centralize and rationalize its network security monitoring and reporting capabilities, the firm has strengthened its protection against intrusion. The company worked with a local Novell partner to smoothly and efficiently implement and manage the new Novell solution.

We replaced the manual, department-led monitoring of distinct network elements with automated, enterprise-wide software for real-time monitoring and reporting of security issues—all managed from a single point of control. In addition to improving security metrics, Novell is helping to reduce security and compliance costs by releasing departmental staff from monitoring duties.

Most important, we enabled the firm to simplify the process of security reporting while enriching the information itself. Now the firm can more easily demonstrate compliance with industry regulations. The Novell offering is the only technology based on a SIEM product that delivers incident response management. It has automated and formalized the firm's process of tracking, escalating and responding to incidents and policy violations from the moment they occur through final resolution. Our technology has also provided two-way integration with leading trouble-ticketing systems as well as end-to-end tracking of system activity for audit purposes.

“Novell offers the unique ability to proactively address business needs for a real-time, comprehensive compliance solution that integrates people, systems and processes.”

Chris Christiansen
Program Vice President
Security Products and Services Group
IDC

“Using the Novell solution, we have optimized our security workflows, saving time by eliminating the need to manually check log files on hundreds of systems.”

Oliver Eckel
Head of Corporate Security
bwin International Ltd.

IDENTITY AND ACCESS MANAGEMENT



Trace every click. Identity and Access Management solutions encompass a range of enterprise technologies that automate business-driven processes to manage the security of and access to enterprise applications and resources.

We offer solutions that deliver identity lifecycle management, access management, enterprise single sign-on and password management. With these solutions, you can manage your entire identity infrastructure and securely manage who has access to your mission-critical applications—cost effectively and easily.

Scenario 1:

Identity Lifecycle Management: User Provisioning

Scenario 2:

Identity Lifecycle Management: Role Management

Scenario 3:

Identity Lifecycle Management: Storage Management

Scenario 4:

Access Management

Scenario 5:

Enterprise Single Sign-On

Scenario 6:

Password Management





“The automated user provisioning enabled by Novell Identity Manager saves us considerable time and effort, and also reduces delays for users.”

Henrik Jordt
Enterprise Architect
Central Denmark Region

1

Scenario 1: Identity Lifecycle Management: User Provisioning

With Novell Identity and Access Management solutions, you can manage user access rights throughout their lifecycle—from the day users are hired to the day they leave the company. By enabling the right combination of provisioning, deprovisioning, roles management and automated policies, you can optimize business efficiency, improve productivity and minimize the risk associated with manual processes.

Customer Situation

The parent company of a large, international manufacturer frequently makes new acquisitions, and the manufacturer itself works with many partners both inside and outside the group. Both factors contribute to a continuously changing set of users who require access to a variety of different resources. Without a standardized solution for identity management, it has been difficult for the company to ensure that the right people—whether employees, partners or customers—have access to the resources and systems they need.

The company needed to simplify the process of provisioning new users and granting access rights without compromising security. The existing identity management procedure was a manual process that required the IT staff to respond to requests from area managers to set up new users. Additionally, the lack of clear, centrally managed security policies made it difficult to audit user activity and demonstrate regulatory compliance.

The Solution

The company used Novell Services to assess its current infrastructure. Then, once the company had a detailed accounting of its assets, it worked with a low-cost, offshore CSI provider to implement and manage the technology. The company's user provisioning capability—as part of a larger identity lifecycle management system—manages user information across multiple systems, creating a central point of management over access to corporate information and applications. User provisioning enables faster, more efficient creation and deletion of user accounts, supporting the company's rapidly growing business.

As the second stage in the solution, the joint CSI and Novell Services team delegated user administration from specialist IT staff to area managers. In addition to freeing up skilled IT staff to work on higher-value projects, user provisioning has empowered business managers to provision their own users. Now, instead of waiting on centralized IT staff to provision users throughout the entire company, area managers can set up new employees or create new partner relationships independently. This significantly increases the speed of user provisioning and makes the company more agile and responsive.

The next stage in the process was to create workflows to automate user provisioning and role-based access to resources. When a manager sets up a new user with a particular profile, the Novell solution automatically and seamlessly provides access to all relevant resources. The removal of access rights is also automated, creating greater certainty that confidential information and systems are only accessible by authorized users.

User provisioning has given the company a central point of control for identity and access management. The company can now connect employees, partners and customers to the systems and information resources they need, rapidly, and with minimal administrative effort. Managers can quickly create, administer or remove their own users, enabling them to respond immediately to new business requirements.

2

Scenario 2: Identity Lifecycle Management: Role Management

If your organization is going to be successful, ensuring your users have access to the resources they need, when they need them, is vital. Novell delivers technologies that are based on your users' roles and on your business policies, so you can be sure that security procedures are consistently followed. With identity lifecycle management capabilities, you can grant access quickly and consistently and easily collect data to prove compliance—cutting management costs while improving security and productivity.

Customer Situation

The IT system for a manufacturing company in the United States serves a large number of employees, partners and vendors who need access to the company's systems. With a frequently changing population and heightened identity and security challenges, the company needed an IT solution that would allow it to automatically assign users rights based on their roles within the system, in addition to managing access and monitoring and reporting on security incidents. The company lacked centralized management, which meant IT staff had to take a manual approach to provisioning. This approach was costly and time consuming, and increased risk to the entire company.

The Solution

By more tightly managing roles through identity lifecycle management capabilities, the company achieved a complete, integrated solution for meeting security, governance, risk and compliance requirements—without placing additional burdens on users. Because the company has such a dynamic user base, it needed to be sure its new system would provide the right access to the right users. Working directly with Novell IT Consulting, the company discovered which assets it already had and how the new solution would affect those components already in place. In addition, Novell worked with the company to ensure it had the right business process model in place. This collaboration led to a Novell solution that worked specifically to answer the needs of the company.

With access to sensitive information based on users' roles, and with system and monitoring tools that report security incidents in real-time, the company's systems are no longer vulnerable. It allows the company to automate complex provisioning processes so its users have immediate—and appropriate—access to resources. Our technology enables the company to assign resources to its users based on business roles and policies. New employees and partners are granted access to all the resources they need on their first day. We also make it easy for departments to manage their own users' access needs instead of having to rely on a network administrator. When roles change, access rights are updated automatically. And when an employee or vendor leaves, access is revoked in real time. With roles-based provisioning, systems are never vulnerable, and the company can maintain visibility into how information and resources are being used.

In addition, the company now has a cost-effective way to show compliance with state and federal regulations, and it can maximize the value of its existing IT hardware and software investment through seamless interoperability with Windows, UNIX and Linux.

With 24x7x365 unlimited access to the Novell Support Center, the company has confidence that any technical questions will be quickly resolved, optimizing the user experience. In addition, the company has an invaluable resource: an assigned support engineer (ASE). The ASE, while off site, is familiar with the company's deployment and is well equipped to answer the company's unique questions. Role management, as part of the larger Identity and Access Management solution, provides solid confirmation that only authorized users have access to sensitive information and systems.

“Our large and dynamic user base of employees, students and parents all have varying levels of access to different applications in our IT environment. In our previous system, it took hundreds of employees to manually manage and secure user accounts, while still ensuring adequate access and the flexibility to scale with population changes. Novell Identity and Security Management solutions gave us the ability to automate our identity infrastructure.”

Ted Davis

Director of Enterprise Information Services
Fairfax County Public Schools



“Controlling access to confidential information and intellectual property is vital to our business. With Novell, we can secure our data, while making sure our users have easy access to information, regardless of location.”

Marguerite Whited

Enterprise Client Services Manager
Fairchild Semiconductor

3

Scenario 3: Identity Lifecycle Management: Storage Management

Every networked organization has storage. It's where everyone—users, IT personnel and executives—saves critical files and information. Unfortunately, even in today's technology-savvy world, storage can't manage itself. That's why the Novell approach to storage management automates the complete lifecycle of user and group storage through identity-based policies stored in the directory.

Customer Situation

A growing school district in the United States had limited IT staffing and funding to solve its identity and storage management challenges. The district had more than 3,500 students, teachers and staff members across multiple campuses. And if that wasn't bad enough, the district was also running disparate systems, which meant it had to manually enter, update and manage more than 3,000 student accounts—a process that often required a great deal of time and paperwork. The district needed to automate the management of users' identities and storage needs to simplify administration and reduce unnecessary IT costs.

The Solution

To automate user provisioning and synchronize user information across its enterprise and to provide its students, teachers and staff with identity-based storage capabilities, the district chose Identity and Access Management solutions from Novell. The district had been using Novell eDirectory™ and wanted to leverage it across all its systems. With eDirectory and other Novell technologies, it was able to unite distributed systems and quickly introduce new applications into its environment.

Novell eDirectory integrates with the district's student information system to provide a central repository for user identity information. And Novell Identity Manager automatically synchronizes this user information across multiple applications and automates user account provisioning, which eliminates the need for manual updating.

Another benefit for students and IT staff is the easy management of electronic student portfolios with Novell Storage Manager. Now when a student moves grades, or a teacher transfers to another site, they can continue to access their data. And students can easily and securely access their e-portfolio from grade school to graduation.

And by taking advantage of identity-driven storage, the district was able to automate the complete lifecycle of user and group storage through policies stored in Novell eDirectory. User identity, events in the directory, and these policies determine the storage action that takes place. For example, if a new teacher is provisioned for a particular campus, the storage system looks to the policy for that campus to see how much storage to create for the instructor, which access rights to set up to shared storage areas, and even what documents to copy into the teacher's home directory on the day he or she starts.

The district plans to integrate more applications, such as its library and transportation systems, to further reduce administration time. Freeing up the IT staff from routine administrative tasks—such as identity and storage management—allows them to spend more time on value-added activities, such as classroom computer instruction.

4

Scenario 4: Access Management

To meet compliance standards, you need to know who is accessing your system at all times—even if you have a mixed environment. You need to secure access to Web applications every time, even for employees or partners outside the firewall, without increasing complexity for users. And you need to intelligently enforce security policy enterprise-wide based on accurate information.

Customer Situation

A South American health care organization focuses on specialized services. In any health care organization, timely and secure access to data is critical to providing efficient patient care. With many disparate systems, the organization's physicians and staff often had to remember many different user names and passwords to access clinical applications.

The organization wanted to make its technology solutions transparent to users and quickly get the right information in the hands of the right people when they needed it. The organization also wanted to extend convenient and secure access to its remote users—whether they were working from another office, from a patient's home or while traveling.

The Solution

The organization analyzed several software vendors before selecting a complete Novell system. To reduce costs, the organization wanted to implement the products itself; however, to ensure quality, it looked to Novell to provide periodic delivery excellence reviews. And once the access management technology was implemented, the organization turned to Novell for custom connector development. The Novell Custom Development team, as part of Novell Services, built identity management connectors unique to the organization to ensure that our solution met its specific needs.

Once the portal was created, Novell Identity and Access Management solutions gave the organization secure, identity-based access to the new portal. This, in turn, gave users fast access to a number of applications such as hospital administration, finance, calendars and e-mail.

With an identity-based portal, the organization can now provide personalized views of information to users based on their roles and responsibilities. This gives users access to critical information nearly 90 percent faster. Furthermore, a single user ID and password for each employee speeds access and has reduced password-related helpdesk calls by 80 percent. This means that the right people have the information they need, when they need it—all so they can make the best decisions possible for patients.

Novell solutions make efficient use of the organization's IT staff and allow it to get more done with the same level of resources. Without a cumbersome application delivery process, the IT staff can easily keep their organization up to date.



"With the number of applications we have, we absolutely needed single sign-on. Many of our users were required to remember 8–12 passwords. Now they can get much of what they need with a single ID and password."

John Jahne

Vice President of Network Services
Webster Bank

5

Scenario 5: Enterprise Single Sign-On

Is your IT department straining to handle all of its password-related work? Is user productivity suffering at the expense of password-related issues? Spending a few extra seconds or minutes logging in to various systems might not seem like much, but those seconds and minutes can quickly turn into hours and days of lost productivity. That's when it's time for Enterprise Single Sign-On.

Customer Situation

A credit company based in Asia needed to ensure that its users' and customers' identities were safe and that it wasn't spending too much to keep them that way. Following an enterprise-wide audit, the company realized that its identity management system was in need of an overhaul. Employees had multiple identities with different formats and often used up to eight passwords to access order entry, credit management and finance applications. The IT staff was seriously concerned that the company's fragmented identity management system could pose a major security risk.

In addition, the company feared that its reputation for quality service was at risk. Customer service representatives were spending more time trying to resolve IT issues than focusing on customers, and IT staff members were spending about 20 percent of their time attending to password- and identity-related issues—time they could have used to focus on more strategic initiatives, such as customer relationship management.

The Solution

To address its security and productivity needs, the company implemented a Novell identity management and single sign-on solution using Novell SecureLogin. With these capabilities, the company's users only have to log in to one application—and that happens when they log in to their workstations every morning. Once users are logged in, SecureLogin recognizes when they are inputting passwords and asks them if they would like to remember that password for the next login. If the user agrees, SecureLogin takes care of the rest and users are freed from remembering multiple passwords.

This process gives employees single sign-on access to corporate resources, when and where they need them, in a secure environment. Now, instead of providing one generic login for all corporate applications, the company can easily and efficiently give users the power to create their own secure passwords. This innovative feature has enabled the company to decrease administration costs and enhance user productivity—not to mention dramatically improve security and compliance.

Working in conjunction with Novell Identity Manager, enterprise single sign-on, as part of the larger Identity and Access Management solution, enables users to reset lost or forgotten passwords through a self-service password reset feature. It has also helped the IT team simplify user administration. The team can easily grant application access according to user or group, and can set viewing and editing capabilities for each user.

Since implementing its Novell resources, the company has received excellent reviews from employees who no longer have to remember multiple passwords to access applications. It has reduced the number of passwords per user from eight to one. And with our products, the company is decreasing time and money spent on password-related issues while increasing productivity and return on investment. In fact, the company is estimating that it will recover its full investment in about 10 months. Not only that, but its savings over the next year could be as high as US\$440,000.

6

Scenario 6: Password Management

As the need for trust increases, so does the need to strengthen authentication requirements. This can result in more complex password policies that require users to change passwords more frequently. And with so many passwords to remember for so many different applications, users are bound to forget at least one. These forgotten passwords lead to a loss in productivity and higher administration costs as users call the helpdesk to reset them. With Novell technologies, organizations can enforce password policies throughout the enterprise, empower users with self-service password management, reduce costs and improve productivity.

Customer Situation

A large medical center in North America was having difficulties with its users' logins. Employees needed to log in to multiple applications throughout the day, each with a different password. Users became frustrated trying to remember passwords, and helpdesk calls related to password requests exceeded 800 per month. In addition, generic logins were reducing the security of the entire system, since Web access and workstation usage could not be monitored effectively. Automating identity and password management would allow the IT staff to decrease administration time while better securing sensitive information.

The center also implemented the solution to manage user information across its directory services. For example, the center transformed its human resources (HR) system into the main database for user identity information. This implementation opened the door for the center to automatically manage HR changes throughout other systems, eliminating the need for manual updating. The center has eliminated the manual processes associated with granting and revoking users' access and can set up new user accounts quickly and efficiently. The IT staff can also revoke access as soon as employees leave the center to safeguard the security of its network, as well as access to its 1,500 critical infrastructure control rooms.

The center has also been able to easily and securely provide users with access to important network resources from any location. That way, when employees are working off site or traveling, they can still update and access vital information, and the center does not experience delays or downtime.

Between the password management capabilities of the Novell solution and the on-site, custom training for the IT staff, the center now has centralized and automated identity and password management. The IT staff has reduced time spent on user provisioning by 60 percent and can provision new users 90 percent faster. Users now have secure, single sign-on access to applications, which has improved security as well as employee productivity. Automating identity management and providing end-user training has already reduced helpdesk calls and their associated costs by approximately 70 percent and allows the IT staff to focus more on value-added projects and less on routine administration.

The Solution

The center quickly realized it needed to upgrade its systems to include password management capabilities to eliminate user frustration and reduce support time and costs. It would also minimize lost productivity since employees could reset passwords without making calls to the helpdesk.

After setting up a selection committee to evaluate several password and identity management vendors, the center chose Novell Identity and Access Management solutions, which included password management capabilities. The solutions were a complete package of products and services that would allow the center to get all the technology and support it needed in one place. The deployment allows the center to give its users single sign-on to applications, which reduces user frustration and increases security. With the new system in place, if users forget a password, they can use password self-service to reset it.

“Having one common method for accessing the network improves security and reduces the complexity of what users are required to do.”

Carl Vercio
WHS Program Manager
OSD

“Before implementing the Novell solution, we provisioned users in a hundred different ways. We didn't think we could streamline this process without substantially increasing our staff. With the Novell solution, we have a high-quality, yet cost-effective solution that actually frees up much of our staff to work on other projects.”

Eric Leader
Chief Technology Architect
Catholic Healthcare West

Through our infrastructure software and ecosystem of partnerships, Novell harmoniously integrates mixed IT environments, allowing people and technology to work as one.

Mixed IT environments are a reality for almost all organizations, and we understand that you can't let this reality undermine your ability to compete. We enable businesses around the world to manage their mixed IT environments, helping them reduce cost, complexity and risk. Whatever solutions you're looking for—Identity and Security, Data Center or End-User Computing—we have the tools to connect people to performance and business possibilities. Let us make IT work as one for you.

novell.com/security

**Novell®
Making IT Work
As One™**

Novell.

Novell, Inc.
404 Wyman Street
Waltham, MA 02451

Tel: (781) 464-8000
Toll-free: (800) 453-1267
www.novell.com