

**Net**VISION



*Access Rights*  
*Reporting & Monitoring*

The Business Value of Effective Audit

## The Problem

### *Your Biggest Threat is Your Most Trusted Employee*

Numerous industry sources tell us that insiders represent an enormous potential risk to information security. **But it's not always malicious.** In fact, most security breaches occur by accident (someone loses a briefcase) or in an effort to perform typical employee duties. To be more efficient, meet deadlines, and make the best decisions possible, employees often breach security policies and put organizational information at risk.

#### **Insider Threat**

Insiders are the biggest threat not because they're out to get you but because they have the most power, the most opportunity, and often find themselves in the wrong place at the wrong time. Every day, system administrators stumble across sensitive information such as Human Resource records and company financial information. Human nature all but compels us to satisfy our curiosity and look through information that we know should be off-limits.

The combination of intentionally-granted access, human error, and constant opportunity proves to be too great a force against security controls that are mostly designed to keep outsiders away.

#### **Segregation of Duties**

Humans are not designed or hired for individual tasks. We wear many hats and perform various roles that sometimes conflict. This creates *Segregation of Duties* (SOD) issues where the people who are responsible to approve certain actions are also the people performing those actions. The introduction of checks and balances assures that processes run efficiently and resources are not squandered or mis-spent.

#### **Administrative Audit Trail**

In many environments, the responsibility for management of access rights is spread across numerous individuals. This makes it more efficient for rights to be granted quickly. But, it also presents a challenge for record keeping. As changes occur, help-desk calls come in from frustrated employees who want to understand why access rights were revoked or how certain individuals were granted access to sensitive resources. Given the complexity of today's network systems, you probably either can't get the information you need or it takes way too much time, effort, and cost to get the real answers you want.

#### **The Bottom Line**

All of these issues lead to loss of efficiency, employee downtime, data loss, data exposure, security breaches, and loss of trust among employees, partners, and customers. Without a doubt, you've already experienced some level of frustration associated with these challenges.

# 53%

of employees need to work around their company's security policies and procedures just to get their job done.

– RSA Insider Threat Survey 2008

## The Solution

*The best way to manage the insider threat is through effective, easy-to-use **AUDIT***

The challenges presented by the insider threat are widely recognized. In an effort to protect sensitive information, various mandates and regulations have been enacted that require organizations to protect critical information. Whether it's HIPAA, SOX, PCI-DSS, or other, the goal is to *identify sensitive information, control access to it, and provide audit trails* of access rights changes and access attempts. Many unregulated organizations have taken the hint and also implement controls to protect sensitive information in a way that's consistent with the leading standards and regulations.

### **Preventative, Detective, Reactive**

In analyzing and responding to various regulations, industry experts have recommended three audit control types:

*Preventative* controls are designed to prevent policy violations from occurring. This could be via a deterrent or an obstacle that actually disallows the event from happening.

*Detective* controls enable after-the-fact automatic identification and reporting on security events. Most audit controls are considered to be detective.

*Reactive* controls work with detective controls to enable real-time event response providing alerts and/or remediation of security events.

### **Who Has Access to What**

The best way to mitigate the insider threat is to fully understand how people get access to information, lock down that access, and track permission changes over time. Given the three audit control types above, answering these access rights questions adequately really requires two technical capabilities:

- Be able to report on what permissions exist right now. This essentially answers the 'who has access' question and ensures that preventative controls are functional.
- Monitor user activity and administrative changes in real-time. This provides details such as who granted access rights, when permissions change, and an audit trail of changes over time. This also enables real-time alerts and policy enforcement as events occur.

You can't revoke all access to sensitive information at the expense of business efficiency. But you can audit access rights and monitor for changes over time. These basic audit and reporting capabilities enable a comprehensive response to the complex challenge of the insider threat.

“Most security against crime comes from audit.”

Of course we use locks and alarms, but we don't wear bulletproof vests. The police provide for our safety by investigating crimes after the fact and prosecuting the guilty: that's audit.”

“...Audit helps ensure that people don't abuse positions of trust.”

- Bruce Schneier

# The NetVision Approach

NetVision has been solving access rights challenges since 1995. NetVision solutions answer the question of **Who has access to what?** while also enabling real time monitoring of user activity and administrative changes across Novell and Microsoft networks.

Information Technology professionals are already struggling with demanding schedules and unexpected issue response on a daily basis. A solution that enables effective audit should also have a minimal negative footprint in terms of management and maintenance requirements. It needs to be easy to use and easy to own.

NetVision helps organizations to manage the insider threat via effective audit with simple-to-use tools for access rights reporting and monitoring. Our priority is to ease the pain. We know that audit and monitoring of access rights is important, but it's not where you want to spend your time or resources. It would be ideal if it were just done for you. NetVision makes that a reality.

NetVision's one-click reporting console enables quick access to reports through an extensible and flexible web-based interface powered by BusinessObjects' CrystalReports™.

## Holistic Approach

NetVision's combined solutions help with all three audit control types. On core network systems, preventative controls are built-in requiring authentication to the network and authorization via file and folder security permissions. Often, these permissions are granted or denied via security group memberships. Sometimes, access rights are based on user attributes or account location within the network directory. Accounts, groups, file system permissions, authentication rules, and access attempts are intertwined in a complex web of permissions.

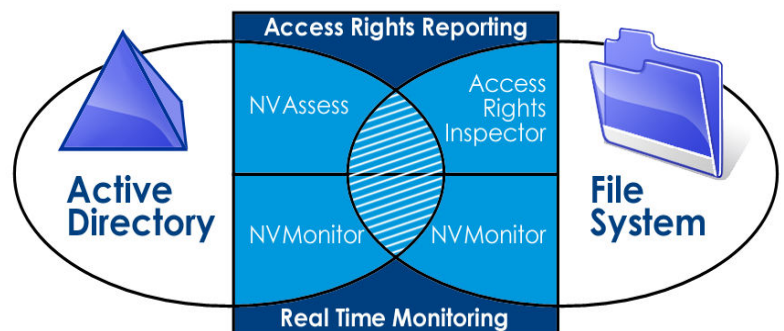
NetVision enables reporting on *preventative* controls while also providing a *detective* audit trail of user and administrative activity and *reactive* controls that can immediately alert and remediate events that breach security policy.

## NetVision Products

NetVision's products work together to provide a comprehensive solution for access rights reporting and monitoring. NetVision covers both the network directory and file systems, which have tightly integrated security models. Permissions and security groups that are stored within the directory enable access to resources across the file system.

NetVision's product line includes:

- **NVAssess** – enables periodic, query-based reporting on the network directory, including any combination of user accounts, groups, and/or attributes.
- **NVMonitor** – enables real-time monitoring of directory and file system activity, including authentication attempts, file access, permission changes, and account/group changes.
- **Access Rights Inspector** – enables flexible, on-demand and scheduled reporting of file system access rights, including complete reporting on *who has access to what?*



## NVASSESS

---

### Easy Reporting on [User Accounts](#) and [Security Groups](#)

NVAssess enables automated reporting of user accounts and group memberships in the network directory. These accounts and groups enable access to sensitive information across the network. Understanding accounts, account status, attributes, and group memberships is a key aspect of answering audit questions about access rights.

NVAssess enables you to report on any combination of object and attribute in the directory. This includes answers to common questions such as:

- What Accounts Exist?
- Which Accounts are Enabled or Disabled?
- Which Accounts are Dormant or Unused?
- Which Accounts have Specific Attributes (job titles, departments, etc.)?
- What Groups Exist?
- Which Accounts are Members of Which Groups?

## NVMONITOR

---

### Real-Time Monitoring enables [Continuous Audit](#).

NVMonitor enables real time monitoring of access rights, administrative activity, and user behavior. Based on policies, which can filter by affected object or who is making the change, NVMonitor can send alerts, remediate changes, disable attacker accounts, create helpdesk tickets, and more.

NVMonitor event information is collected directly from the source for immutable, non-repudiable, and complete reports. Events are filtered and analyzed in real time to ensure extremely high relevance in reports and alerts.

Some of the activities that NetVision NVMonitor Monitors include:

- Account Creations
- Account Deletions
- Account Status Changes
- Account Attribute Changes
- Group Membership Changes
- File or Folder Permission Changes
- File or Folder Reads, Writes, or Deletes
- User Authentications
- User File or Folder Activity



## ACCESS RIGHTS INSPECTOR

### Effective Rights on File System & Directory Objects

Access Rights Inspector calculates permissions across file systems and directory objects to provide effective rights reports. This essentially answers the question "Who has access to what?"

Directory and File System rights are complicated to capture. Actual permissions are often granted or denied based on a combination of explicitly assigned rights, group memberships, inherited rights, network share permissions, object ownership, denied permissions, and more.

NetVision's Access Rights Inspector enables you to get detailed answers on access rights across Active Directory and Windows file system environments. Reports can then be scheduled and emailed in multiple formats.

Report Types Include:

- **Effective Rights:** Reports on calculated rights accounting for group memberships, inheritance, direct assignments, and other factors.
- **Explicit Rights:** Reports on explicit permission assignments.
- **Direct User Assignments:** Reports on instances where a user account has been granted access directly to a resource.
- **Deny Entries:** Reports on instances of explicitly denied permissions.
- **Group Memberships:** Reports on group membership assignments.

With Access Rights Inspector, the department head is emailed weekly with a PDF of all accounts that have access to the department's sensitive documents. So, they always know who has access.

## SIMON MANAGED SERVICE

### Hands-Off Service Delivery Reduces Cost & Effort.

NetVision's managed service makes life easier and reduces operational costs. With SIMON, NetVision delivers monitoring and reporting of access rights with none of the typical hassles associated with traditional software solutions.

SIMON Includes:

- ☑ *All related hardware and software (inc. licenses, installation, configuration, security hardening)*
- ☑ *Setup and configuration of best-practice policies, filters, and reports*
- ☑ *Immediate and touch-free upgrades*
- ☑ *Creation and management of custom scripts and report templates*
- ☑ *Remote system health monitoring*
- ☑ *Guaranteed availability of trained staff*

*Recover time. Improve efficiency.  
Reduce costs.*

Since 1995, NetVision has provided access rights reporting & monitoring of both network user accounts and file systems. NetVision's flexible, web-based reporting console, real-time alerts, remediation capabilities, and extensibility enable dramatically reduced audit costs, improved security over critical network resources, and complete visibility into user and administrative activity.