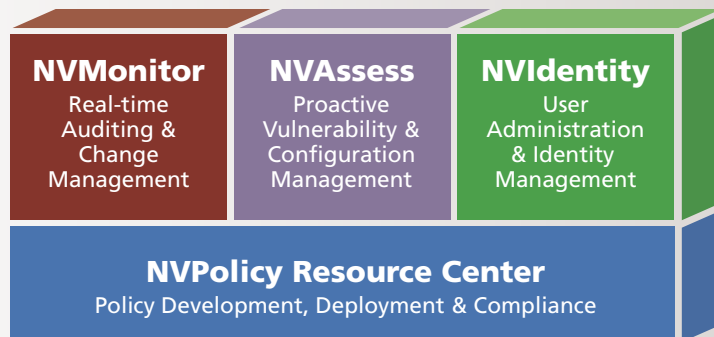




NetVision Security Administration Framework

THE SOLUTION—WHAT IT DOES

- ▶ **NVPolicy Resource Center**—
Policy Development, Deployment & Compliance
- ▶ **NVMonitor**—Real-time Auditing & Change Management
- ▶ **NVAssess**—Proactive Vulnerability & Configuration Management
- ▶ **NVIdentity**—User Administration & Identity Management



The NetVision Security Administration Framework (NSAF) delivers an IT security solutions package that fundamentally changes the way enterprises achieve policy enforcement. Based on a business-level policy approach, it enables organizations to leverage their enterprise directories to significantly simplify security management and enforcement for consistent authentication and access control across the entire organization. It provides real-time auditing and change management that not only detects attempts to breach enterprise security, but also automatically intercepts and stops attacks before they can do any damage. It proactively scrutinizes enterprise servers, directories, applications, and other services for security vulnerabilities and then automatically corrects any identified problems.

NVPolicy Resource Center

Policy Creation & Management

NVPolicy Resource Center integrates a security knowledge base with a policy creation and management system enabling organizations to build security policies from templates and then implement specific security controls to support policy objectives.

- Robust Portfolio of Security Best Practices including detailed policies, standards, technical standards, procedures and processes.
- Policies, standards and technical standards are mapped to exact regulatory requirements for GLBA, HIPAA, ISO 17799, FERC / NERC and Sarbanes-Oxley
- Workflow management for policy creation, implementation and life-cycle management

Security Awareness, Compliance, & Training

NVPolicy Resource Center provides turnkey, automated processes for security policy distribution, training and awareness.

- Tracks, records and verifies that employees have viewed, read and understood policies, standards, procedures, processes and/or awareness information in accordance with regulatory mandates.
- Quizzes and trains employees / administrators

Vulnerability Alerting & Tracking

NVPolicy Resource Center's Vulnerability Alerting and Tracking system helps security managers understand the impact of new vulnerabilities and prioritize remediation through automated alerts, reporting and analysis capabilities.

- Personalized vulnerability and malicious code alerting service for new threats
- Customizable pager and e-mail alerts
- Color-coded threat ranking and prioritization including task workflow automation and reporting
- Dynamic database of 9300 known vulnerabilities for 6,550 vendor products updated with new vulnerabilities as they occur
- Profile-based alerting capability informs system and network administrators of only those security holes relevant to their particular systems.

Change Detection, Alerting & Reporting

Based on pre-defined policies and configuration standards, NVMonitor continuously monitors enterprise directories and network operating systems and identifies unauthorized changes or access behaviors that violate policies.

- Sends an immediate alert to specified IT security managers when access attempts or changes to monitored objects or files are made that don't conform to policy.
- Through the VisionView™ reporting console NVMonitor provides clear and concise reports on the who, what, when and where audit data captures an audit trail of changes to servers and directories.

Response Automation & Remediation

Based on pre-determined policies and threshold levels, unauthorized directory and server activity can be stopped in its tracks and reversed through automated controls. Customizable responses can be escalated as monitored activity moves from innocent, to suspicious to outright malicious.

- Automated responses include: Immediate termination of access rights, reversal of unauthorized changes, deletion of offending files, or any other pre-scripted and customizable response.

Intrusion Protection / Behavior Management

As the foundation for a layered security strategy, NVMonitor delivers host-based intrusion protection by monitoring from the inside out, immediately detecting and pinpointing unauthorized change—whether malicious or accidental, initiated externally or internally.

- Whether it's a legitimately authenticated user or an outsider who has penetrated perimeter security all behavior is monitored and any attempt to gain inappropriate privileges is blocked.

Applications Management

Active auditing and monitoring functions provide versatile capabilities for managing directory-aware applications.

- The eDirectory events or processes of ZENworks, DirXML, GroupWise and more can be proactively monitored ensuring the health and integrity of directory-enabled applications.
 - ▶ **Example:** NVTao Monitor provides DirXML administrators early detection when a DirXML driver has stopped and facilitates recovery quickly without data corruption.

Directory / Server Health Monitoring

With improved visibility into the directory structure administrators can monitor partition activity with more information, and cut troubleshooting from hours to minutes.

- Remedies obituaries faster and turns reactive fire-fighting into proactive directory management.
- Unique capability to monitor even the extended schema provides monitoring for all upgrades to the OS and directory including: Schema, File system, OS, NLMs, Objects, and Rights.

Vulnerability Scanning / Reporting

Performs extensive interrogations of operating systems, applications and directories from a single console.

- Presents a comprehensive picture of the state of the enterprise by identifying and eliminating network vulnerabilities across disparate platforms.

Server Configuration Management

Simplified configuration management protects against downtime and revenue loss by identifying and ensuring that appropriate versions, service packs and hot fixes are loaded.

- Service configuration—audits servers to check for proper configuration and that only approved services are installed and properly configured.

Policy / Standards-Based Assessment

Ready-to-run query templates apply policy-based standards exported from best-practices database (NVPolicy Resource Center), including queries specific to government regulations (HIPAA, GLBA).

- With built-in knowledge, NVAssess audits and documents compliance with corporate policies and provides ability to build custom queries specific to particular corporate policies and procedures.

Disc Space Analysis & Remediation

Performs enterprise-wide disk space analysis showing the space available and space in use for all volumes, including identifying duplicate files, old files, and more.

- Identifies abuse of disc space by finding (and deleting if desired) inappropriate files such as JPG and MP3 in users' home directories.

Account / Rights Management

Performs enterprise-wide effective rights analysis on directory objects, whether via security equivalencies, group membership, trustee assignments or inherited rights filters.

- Provides critical information about hidden objects
- Locates and deletes stale or unused accounts
- Helps identify who has inappropriate rights to files, directories, applications and other assets
- Identifies and corrects password policy violations

Directory Structure Analysis

Provides ability to analyze and optimize directory tree structure and partitions.

- Facilitates disaster recovery by providing detailed documentation of directory structure and user account information.

Automated Problem Resolution

Provides customizable, automated responses to discovered vulnerabilities for closed-loop resolution.

- Flexible, pre-scripted responses automatically enforce predefined security policies.
- Automated responses include actions like: deletion of offending files, removal of dormant accounts, modification of weak passwords, or resetting a configuration to a known good standard.

NVIdentity

User Account Provisioning / De-provisioning

NVIdentity automates the process of account creation and synchronization among connected directories.

- Automates the creation and deletion of user accounts throughout the enterprise
- Upon creation, adds users rights, permissions, and group associations to multiple enterprise directories automatically
- Ensures user productivity by providing immediate secure access to proper resources
- Decreases liability associated with orphaned accounts by automating the revocation of network access rights of terminated employees
- Manages additions and deletions from groups by updating new rights and revoking previous rights automatically
- Assures passwords and password reset intervals are established for all account creations

Password Synchronization

Non-intrusive bi-directional synchronization that occurs transparently in the background.

- Predictable, automated password synchronization between eDirectory and: Active directory, NT Domains, Exchange, Lotus Notes, GroupWise and LDAP directories
- Single password authentication for users across multiple disparate directories

Password Strengthening

NVIdentity enables the implementation and enforcement of password-strengthening policies that are automatically enforced throughout the enterprise.

- Require minimum password lengths, upper/lower case letters, numbers or special characters
- Disallow certain words and usernames
- Eliminate easily cracked passwords in enterprise directories and applications
- Enforce password-strengthening policies for users resetting their own passwords

Password Self-Service

Reduces the cost of password management by giving users the power to manage and even reset their own passwords through its browser-based password management interface.

- Allows users to set passwords from any location using only a Web browser
- Quickly and efficiently reset forgotten passwords using challenge questions
- Supports context-less login, eliminating need for full distinguished name
- Enforces password strengthening rules and policies for self-service users
- Administrator configurable user attribute for login credentials

Directory Integration / Migration

Facilitates co-existence and migration strategies allowing accurate identity data to exist in multiple directories.

- Provides ability to extend rather than replace existing directory infrastructures
- Minimizes risk of lost data associated with migration initiatives and provides flexibility in migration timing and future strategic directory choices

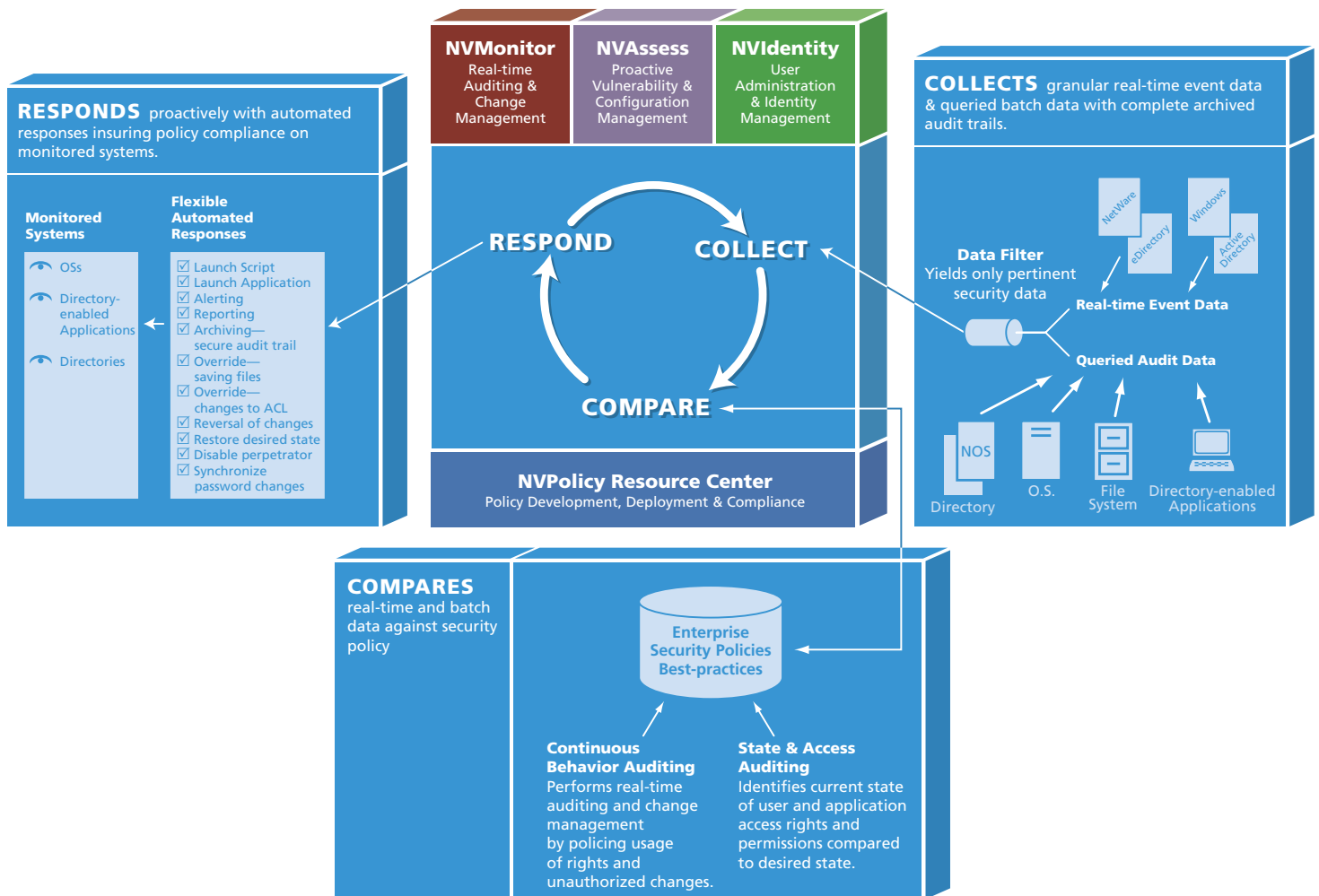
Interaction of ISPM Components

- ▶ NVMonitor and NVAssess work together to act as a configuration and change-management system. Both solutions watch for security anomalies across the enterprise. NVMonitor watches in real-time for atypical behavior (like users logging in at non-standard times) and NVAssess queries to discover vulnerabilities or misconfigured systems.
- ▶ After NVIdentity creates a directory account, NVMonitor can report that activity to an ODBC database and/or Web page, send the report via e-mail to the administrator, and/or page the administrator with immediate notification of any violations.
- ▶ When a user is moved from one group to another, NVIdentity and NVMonitor work together to automatically update the individual's new rights and revoke previous rights.
- ▶ NVAssess can uncover any accounts that don't currently adhere to password strengthening policies, while NVMonitor can automatically enforce password restrictions such as number of failed attempts allowed, required change interval, and password profile.
- ▶ NVAssess can search for and locate any file sizes or types (MP3, JPEG) that violate file saving policies, then report the violation, notify the user of the violation and automatically delete the offending file. NVMonitor can work in real-time to prevent further non-policy conforming files from being stored on the network.

CAPABILITIES AT A GLANCE

NSAF FEATURES / FUNCTIONS	BENEFITS
Systems-level integration operates at the host directory—not an application	Non intrusive, operates in the background requiring no proprietary database, enables ongoing use of native, familiar management tools
Integrated set of security management tools	Common mgt interface and interoperability among components, allows end-to-end policy management from a single administration point
Web-based management console	Provides anytime/anywhere access and consolidated view of the operation and deployment of the security solution
“Active auditing” system that is always watching and listening	Allows security administrators to prevent security compromises, rather than just responding to them
Delivers multiple security tools within a single solution	Facilitates vendor consolidation and reduced total cost of ownership
Achieves “layered security” strategy	Host-based monitoring and assessment provides additional security beyond traditional perimeter defenses
Lightweight architecture	Automates security/performance data collection across the enterprise without impacting system operations
Automated Policy Enforcement	Actually prevents and stops attacks or malicious changes rather than just providing alerts or alarms
Policy-driven security management	Built atop the Policy Resource Center and Policy Enforcement Engine, All product components are policy based and enabled

HOW IT WORKS



NetVision
Policy Driven Security

www.netvision.com or info@netvision.com
 US TOLL FREE 1.877.828.9180 FAX: 801 764-0600
 OUTSIDE US 801.764.0400
 1500 N Technology Way D-3300, Orem, UT 84097 USA

©2004 NetVision, Inc. All rights reserved. US Patent No 5,721,825 and No. 5,794,232 protect NetVision's Global Event Services with additional patents pending. GES and Global Event Services are trademarks of NetVision, Inc. All other products not listed are the property of their respective owners