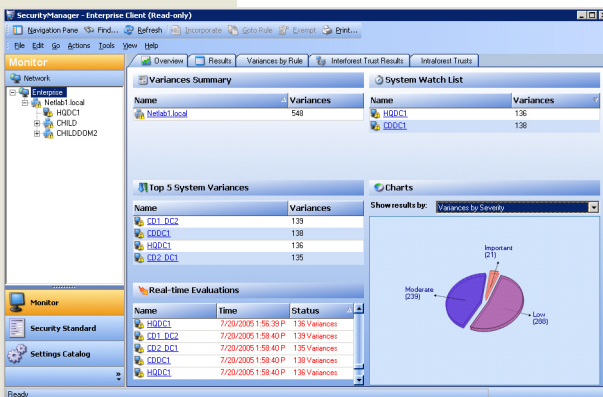


SecurityManager™

Harden Active Directory Security and Policy Management

Active Directory is critical to your overall network security. It allocates rights and protects systems and applications through highly integrated rules and policies shared enterprise wide. As such, it can also be the access point for malicious users to wreak havoc on your network, or the vehicle by which simple mistakes create gaping security holes.

Choose not to pay attention to Active Directory security and you're taking a huge risk. Yet, companies often take the path of least resistance with regard to locking down Active Directory. After all, Active Directory's complex and widely distributed nature makes potential security vulnerabilities difficult to identify. Manual methods for securing Active Directory are extremely time consuming. And even the most experienced Active Directory administrators are challenged to provide anything but reactive, inefficient protection for their business-critical directories.



SecurityManager enforces security and policy management across your entire enterprise and prevents business-crippling security breaches.

NetPro's SecurityManager ushers in a whole new breed of security for Active Directory. Using a foundation of Microsoft Security Best Practices, SecurityManager is the only solution that monitors corporate Active Directory security policies in real-time. Leveraging NetPro's auditing and configuration solution, ChangeAuditor, SecurityManager works 24x7 to ensure that critical Active Directory configurations are correctly defined, proactively reducing the risks

of costly security breaches while enforcing corporate compliance to government regulations such as Sarbanes-Oxley and HIPAA.

Through security tests and baselines, SecurityManager

- Examines AD configuration settings that could expose your network to security vulnerabilities such as Multi-forest trusts without SID Filtering enabled
- Monitors domain settings such as password policies and audit settings
- Examines policies on each Domain Controller to ensure that settings are aligned with corporate policy

SecurityManager catches vulnerabilities like these, and many more, instantly, providing the comprehensive protection your organization requires.

SecurityManager enforces security and policy management across your entire enterprise.

SecurityManager embraces the security best practices and recommendations made by Microsoft and other top industry security consultants to deliver a fully-formed security methodology for your environment. Going far beyond the functionality found in basic benchmark solutions, SecurityManager:

- Automates the enforcement of Active Directory security configuration
- Provides real-time visibility into security and policy compliance in a single interface
- Delivers a customizable, best practice baseline
- Provides security tests and baselines
- Notifies operators of policy violations
- Includes in-depth, detailed descriptions of security best practices and processes
- Integrates with ChangeAuditor to maintain a secure Active Directory environment
- Integrates with MOM

Enforce Security Best Practices

SecurityManager's highly-scalable framework was developed using Microsoft's best practices methodology for deploying and managing a secure Active Directory environment. For each step outlined by Microsoft, SecurityManager provides the automated testing and enforcement of the associated best practices.

For example, using SecurityManager, you can assess the configuration of your domain controllers and the corresponding Group Policy Objects (GPOs) to ensure that Microsoft best practices are being maintained. Further, while SecurityManager ships with the recommended best practice security baselines provided by Microsoft, it also enables you to customize policies for your environment using baseline testing.

Casting a Wide Net with NetPro's Active Directory Security and Compliance Suite

Real-time security of your environment is absolutely critical, but it's only part of the solution. Also vital is maintaining control of your environment through proactive configuration auditing and automating the workflow around directory changes.

SecurityManager is a key component of NetPro's Security and Compliance Suite (SCS), which also features ChangeAuditor and ChangeManager, NetPro's change control and work flow management solution for Active Directory.

When Active Directory security is breached through an escalation of rights scenario or a configuration change that opens a gap in the system, the entire network is at risk. SCS prevents the spread of unauthorized changes (including GPO changes) through proactive monitoring and auditing, ensuring that the directory is protected at all times through best practices, auditing and security standards enforcement.

The following example illustrates how SCS builds in critical controls and hardens security around Active Directory.

As the enterprise administrator, you ensure that the default domain controller policy is set up correctly and strictly enforced. But, when a new administrator links an unauthorized policy to the default domain controller's OU, it applies incorrect settings, causing the your DC settings to become non-compliant.

NetPro's SecurityManager reports this policy violation, not only notifying the security officer of the violation, but showing the "Actual" and "Expected" values side by side. The security officer launches NetPro's SecurityManager client, which promptly shows the misconfigured DCs along with the change that caused the compliance issue. Using NetPro's integrated ChangeAuditor solution, the security officer identifies the who,

SecurityManager at a glance...

- *Delivers a customizable, intuitive best practices-based baseline*
- *Provides security tests and baselines*
- *Alerts on security vulnerabilities instantly*
- *Includes in-depth, detailed descriptions of security best practices*
- *Integrates with ChangeAuditor, to ensure constant Active Directory security*
- *Ensures that all external and forest trusts are monitored according to user defined trust permissions*
- *Includes the ability to monitor non-Microsoft services for security conformance*
- *Integrates with MOM*

what, where and when details of the unauthorized, high-risk change, including the name of the unauthorized policy and the settings. He then refers to SecurityManager's knowledgebase to determine the potential impact of the change. Armed with this information, either the security officer or the enterprise administrator can roll back the change using NetPro's ChangeManager solution, thereby ensuring that all changes are properly documented and comply with both corporate and government regulations.

Used together, the solutions that make up NetPro's SCS provide closed loop security and control for the directory, dramatically reducing the risk of security breaches and performance concerns. Deploying the solution in your environment also eliminates the need for time-consuming manual processes designed to ensure just a fraction of the protection SCS does.

NetPro . . . the experts behind SecurityManager

NetPro sets the Gold Standard for distributed infrastructure management. We build decades of experience into every enterprise solution, ensuring that our customers can manage the health, security and control of their Active Directory, DNS, MIIS, and eDirectory environments with total, unparalleled confidence. Our solutions enable organizations to increase access availability, prevent costly disruptions, improve security and policy compliance, and enhance management efficiencies. NetPro counts Bank One, the U.S. Army and General Motors among its many customers.

For more information, visit our web site at www.netpro.com/products/securitymanager. Or call NetPro at 800.998.5090, Fax 602.346.3610. Outside the U.S. call +31 36 540 5959. Email requests to: info@netpro.com.



4747 North 22nd Street, Suite 400 Phoenix, Arizona 85016

NetPro® and NetPro Computing®, are registered trademarks of NetPro Computing, Inc. SecurityManager and the NetPro logos are trademarks of NetPro Computing, Inc. Microsoft®, Windows® 2000 Server and Active Directory™ are either registered trademarks or trademarks of Microsoft Corporation. 072805