

To ensure compliance with regulations, two groups of solutions either help manage workstations/servers or help manage network devices, says **Nathan Ouellette**.

Configuration weaknesses and missing patches for servers, workstations and network devices continue to make their way into the information security headlines. Like many other well-publicized events that tend to whip people into action, IT and security stakeholders are inundated with

reactive mandates to patch quicker without breaking applications, deploy faster with less resources, and to provide more protection without impacting productivity.

As companies experience growth, acquisition or even expansion to different lines of business, the configuration of workstation,

server, network and security devices becomes more difficult to manage.

By no means is implementing technology to help you manage policies a panacea, but some of the features that are creeping into the policy management space can help alleviate some of the pain points associated with these tasks.

## SCM 5.7



**Vendor** NetIQ  
**Price** starts at \$1,100 per server  
**Contact** [www.netiq.com](http://www.netiq.com)

NetIQ's Secure Configuration Manager (SCM) is a combination of client server and web-based components to help organizations manage

configurations of workstations and servers. The tool is primarily made up of a central administrative console, which controls policy dissemination through software agents deployed to hosts running Windows, UNIX, Linux and iSeries operating systems.

The SCM server components are typically installed on Windows 2000 or Windows 2003 and use

an MS SQL 2005 database. We had a little bit of trouble with the solution not recognizing a database during one install attempt, but it recognized it when we chose a different installation option. Agents for individual hosts (branded as NetIQ VigilEnt) that are managed through SCM can be deployed by the console using a deployment wizard. We did not have any trouble deploying various test agents throughout our lab environment. Hosts can also be part of the reporting and monitoring process without an agent installed, they simply won't have policies pushed to them.

Unlike policy management solutions that strictly push configuration files to network devices, there is a little bit more overhead associated with managing agents installed on Windows, UNIX and other operating systems. Overall, the performance was good, however. SCM approaches policy management by comparing known vulnerabilities and threats with the configuration of the managed assets in the environment.

Pricing starts at \$1,100 per server that reports through SCM and this

price includes basic support. In addition to phone and email support, customers can also access the online user forums and the NetIQ knowledge base. Premium support is available for an additional cost. Overall, we find that this is a pretty good value for organizations who really struggle with compliance and configuration management across multiple platforms. NetIQ customers will benefit from framework integration with other products.

### SC MAGAZINE RATING

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★☆

### OVERALL RATING ★★★★★

**Strengths** Solid feature set. Risk-based scoring mechanisms to help prioritize remediation efforts.

**Weaknesses** May get pricey as more assets are managed.

**Verdict** Overall, a good risk-based approach for managing known weaknesses in configurations, patches and other host-level vulnerabilities. We recognize the product as this month's SC Magazine Best Buy.



Solid feature set. We recognize the product as this month's SC Magazine Best Buy.

– Nathan Ouellette



**NetIQ Corporation**  
 An Attachmate Business  
 1233 West Loop South, #1800  
 Houston, TX 77027  
 713.548.1700 • 888.323.6768 sales  
[www.netiq.com](http://www.netiq.com)