



PLAY NICE WITH OTHERS: McAfee applies your mother's advice to network access control.

Network and system security at your organization is a top priority. You've spent considerable time and expense defining comprehensive policies. You have the latest virus, spyware and spam controls; you deploy patches as soon as they are issued; you've invested in intrusion prevention devices and bullet-proof firewalls.

So why do you continue to come across security breaches?

The answer, of course, is compliance and enforcement. All the policies and protection in the world won't help you if they're not being followed or used. And human nature doesn't always make things easy for the IT security manager. Your most valued employee might inadvertently pick up a worm while working from home one evening. When he connects his laptop to the corporate network the next morning— presto destructo!—your precious network is infected.

Network access control (NAC) was a big focus at the RSA® conference in February and everyone, it seems, has a different idea of how to do it. Overlay or embedded? Switches or standards? Frameworks or software?

McAfee's NAC strategy, according to McAfee group product marketing manager Michelle Johnson Cobb, has been to study customer IT environments and develop technology that works in the real world. The new McAfee Policy Enforcer is a natural outgrowth of McAfee's own Blackuster technologies, ePolicy Orchestrator (ePO) and Foundstone. But its approach is hardly proprietary. The software-based solution is designed to work in a multi-vendor infrastructure and features comprehensive compliance checks that include third-party security applications. "It really gives enterprises with heterogeneous environments the ability to deploy NAC today," says Cobb.

Read more about McAfee Policy Enforcer: software.spectrum.com/spectrum/mcafee

"We've pulled together proven McAfee systems and network technology to create an integrated solution that keeps noncompliant or dirty systems off the network."

Michelle Johnson Cobb,
McAfee Group Product Marketing Manager

"Software Spectrum works closely with McAfee Security Alliance partners, as well as McAfee, to help customers deploy Policy Enforcer quickly and effectively."

Pete Oliver,
Software Spectrum Director of Partner Programs

[Callout quotes:]
"We've pulled together proven McAfee systems and network technology to create an integrated solution that keeps noncompliant or dirty systems off the network."

-- Michelle Johnson Cobb,
McAfee Group Product Marketing Manager

"Software Spectrum works closely with McAfee Security Alliance partners, as well as McAfee, to help customers deploy Policy Enforcer quickly and effectively."

-- Pete Oliver,
Software Spectrum Director of Partner Programs

Play Nice with Others: McAfee applies your mother's advice to network access control.

Network and system security at your organization is a top priority. You've spent considerable time and expense defining comprehensive policies. You have the latest virus, spyware and spam controls; you deploy patches as soon as they are issued; you've invested in intrusion prevention devices and bullet-proof firewalls.

So why do you continue to come across security breaches?

The answer of course, is compliance and enforcement. All the policies and protection in the world won't help you if they're not being followed or used. And human nature doesn't always make things easy for the IT security manager. Your most valued

employee might inadvertently pick up a worm while working from home one evening. When he connects his laptop to the corporate network the next morning—presto destructo!—your pristine network is infected.

Network access control (NAC) was a big focus at the RSA® conference in February and everyone, it seems, has a different idea of how to do it. Overlay or embedded? Switches or standards? Frameworks or software?

McAfee's NAC strategy, according to McAfee group product marketing manager, Michelle Johnson Cobb, has been to study customer IT environments and develop technology that works in the real world. The new McAfee Policy Enforcer is a natural outgrowth of McAfee's own blockbuster technologies, ePolicy Orchestrator (ePO) and Foundstone. But its approach is hardly proprietary. The software-based solution is designed to work in a multi-vendor infrastructure and features comprehensive compliance checks that include third-party security applications. "It really gives enterprises with heterogeneous environments the ability to deploy NAC today," says Cobb.

Read more about McAfee Policy Enforcer:
www.softwarespectrum.com/spectrum/mcafee

----- End of print piece – Online continuation follows -----

McAfee Policy Enforcer is built on top of the ePO platform, which manages integrated system security policies for over 40 million end points. If you're one of the more than 30,000 organizations that have already implemented ePO, this NAC solution is ready-made to integrate with your management infrastructure and operational processes.

Vulnerability assessment for McAfee Policy Enforcer is accomplished with Foundstone technology, which McAfee purchased in 2004. Policy Enforcer offers extensive risk mitigation, says Cobb. "The capabilities we've put together are second to none in terms of ability to assess and determine system compliance. We've pulled together Foundstone technology as well as other proven McAfee systems and network technology to create an integrated solution that keeps noncompliant or dirty systems off the network."

How it works.

McAfee Policy Enforcer checks any system trying to connect to your network to make sure it is compliant with the security policies defined by your organization. Say one of your sales people turns off her anti-virus for some reason while she's on the road, or misses a DAT update while she's disconnected. The next time she connects to the corporate network, Policy Enforcer detects a policy deviation and directs her to take the necessary steps to bring her system into compliance.

But McAfee Policy Enforcer doesn't stop with compliance checks. It also scans the system for high-risk infections. So that employee who picked up the worm while he was working from home will be alerted the next morning when he tries to plug his laptop back into the network. He'll be prompted to correct the problem, but the rest of your organization won't know the difference.

So what about those system assessments? Won't extensive system checking every time you log onto the network slow everyone in your organization down? Will frustration levels skyrocket?

According to Cobb, this isn't really a concern with McAfee Policy Enforcer. Systems under the management of your organization run a combined ePO/Policy Enforcer agent, which streamlines the process by running the checks right on the host system (your laptop, for example), without ever touching the network. Normal checking and scanning is typically unnoticed by the user, depending on the number of checks you do and the number of infections you're looking out for.

Unmanaged systems—consultants logging onto the corporate network temporarily, for example—are scanned remotely without the use of an agent. "Our Foundstone technology," says Cobb, "does very quick, thorough scans of those systems. Typically the system scan is going on in the background while the user is typing in his password. But before he can log in, we've already determined whether or not the system should be allowed on."

As for those systems found to be non-compliant, a web page provides instructions that tell the user what remediation steps need to be taken so they can be up and running again on the network.

McAfee Policy Enforcer is a reflection of your company's own security policies, so the number of checks and scans done when users log on is controlled by your organization. The average user doesn't need to do an extensive vulnerability scan each time he or she accesses the network. While a thorough Foundstone vulnerability scan checks for over 4000 threats, Policy Enforcer users can choose from approximately 600 of the most critical threats—automatically updated with the latest threat intelligence from McAfee AVERT Labs.

Simplified deployment.

Network access control is a fairly new area of technology, not without its challenges. Chief among them is figuring out how to deploy a product that combines system and network protection. Getting all the people necessary to discuss a NAC solution in one room can be a challenge, says Cobb.

Different organizations require various types of network access control integration and deployment scenarios, so services are a key component of this product. According to Pete Oliver, Software Spectrum's director of partner programs, "Software Spectrum works closely with McAfee Security Alliance partners, as well as McAfee, to help customers deploy Policy Enforcer quickly and effectively."

The deployment of McAfee Policy Enforcer is simplified because of its tight integration with ePO—and because Policy Enforcer is built to work with whatever network infrastructure you already have in place. Once McAfee Policy Enforcer is integrated into your network, management couldn't be easier.

When it comes to network access control: security policy definition, discovery, assessment, enforcement and remediation, McAfee makes sure all the networks, systems and organizations involved work supremely well together—which makes things a whole lot easier. Wouldn't your mother be proud.

Download a McAfee white paper: "Enforcing Endpoint Policies for Network Access with Policy Enforcer: Selecting the Right Solution for Your Environment."