



# PRODUCT EVALUATION GUIDE

## NAC Products

Insight's Technology Assessment Services (TAS) team has evaluated the following products. Please e-mail [tas@insight.com](mailto:tas@insight.com) for specific information on any of these:

- Symantec™ Network Access Control
- McAfee® Policy Enforcer
- Vernier Networks

## NETWORK ACCESS CONTROL

Today the boundaries of a safe and secure corporate network are becoming less and less definitive. The old strategy of protecting only the perimeter of your network no longer applies now that more and more workers are using wireless devices. Those endpoints may be functioning inside the safety of the corporate LAN by day, but by night they are attached to a strange and unsecured network at employee homes or public Wi-Fi hotspots. The typical laptop lacks fire-wall protection and is vulnerable to viruses and malicious attacks. When users connect back to the corporate LAN, the worms and malware they picked up in the cloud begin running wild on the “secure” network.

Computers with out-of-date Microsoft® Windows® security patches can also contribute to corporate LAN vulnerabilities. Patches are typically offered as monthly downloads from the Microsoft website. But if the user doesn't make the effort to download these patches, they may become vulnerable to a number of threats.

Network access control is quickly becoming a priority as IT departments look for ways to keep vulnerable, virus-infested, out-of-date laptops and desktop computers from accessing the corporate network. Microsoft and Cisco have proprietary solutions that are still evolving, but if you're searching for a non-proprietary, stand-alone solution that will work in your environment, look to companies like Symantec, McAfee, Vernier Networks, Mirage Networks, Caymas Systems and others.

## KEY CONSIDERATIONS

### Infrastructure

Network access can be controlled via the 802.1x infrastructure, when it exists, which tells an Ethernet switch or wireless access point to validate a user to a RADIUS server before allowing access to the network. When an 802.1x LAN doesn't exist, a special purpose access device is required. These solutions typically consist of a policy server, an access controller and, depending on the solution, a client loaded on the endpoint.

### Policies

Server access policies determine whether users are quarantined, dropped or allowed access. Once allowed on the server, users may then have full access to the network or only to certain applications. Your company will need to develop these policies, based on who users are or how they access the network.

### System mitigation

When users' systems have been quarantined or blocked, you must give them the ability to bring their system up to date or solve the policy issue that has been violated—otherwise you will end up with a lot of unproductive computers and frustrated users trying to access the network.





## KEY FEATURES

- **Unmanaged device scanning** – Scan and block not only the managed devices you already know about, but also unmanaged ones belonging to visitors, vendors or partners. When an unmanaged device is detected, most NAC solutions offer the user the option to download a Web application that performs a quick system scan to verify that it adheres to company policies.
- **Desktop firewall** – Offer users a defense-in-depth approach to security. Instead of just protecting the perimeter of your network, desktop firewalls protect each system from attacks that may originate from within the corporate firewall. They are also critical for users using their laptops remotely.
- **Vulnerability monitoring** – Continually monitor endpoints for vulnerabilities. Solutions that have a client installed may have an IDS/IPS module that detects, logs and blocks malicious behavior.
- **Load-balancing and failover** – High-volume environments may require load-balancing and failover capabilities to provide optimal user throughput.
- **Self-remediation** – Offer blocked or quarantined devices limited access to a secured segment of the network where they can update operating system and virus definitions, eliminating IT department involvement.
- **Containment** – In situations where a worm is able to infiltrate your network, segment or zone off your network to contain the worm until it is removed.

## CONCLUSION

Many IT departments have tried to control the use of their company computers and most have failed. Employees will always use company laptops for personal use and because of this, malware has a good chance of finding its way back to your corporate network. Inspecting and mitigating problems before devices connect to your network is critical. The network access control solution you choose plays an important role in protecting the security of your network and enforcing your security policies.

Insight has sales specialists ready to discuss NAC solutions, and a supporting staff of technical resources. We can be a valuable resource when you're faced with the issues that may arise in your effort to control access to your network.

**For more information, contact your account representative, or the Insight Technology Assessment Services team at [tas@insight.com](mailto:tas@insight.com).**

Insight and the Insight logo are registered trademarks of Insight Direct USA, Inc. All other trademarks, registered trademarks, photos, logos and illustrations are the property of their respective owners. ©2007, Insight® Direct USA, Inc. All rights reserved.