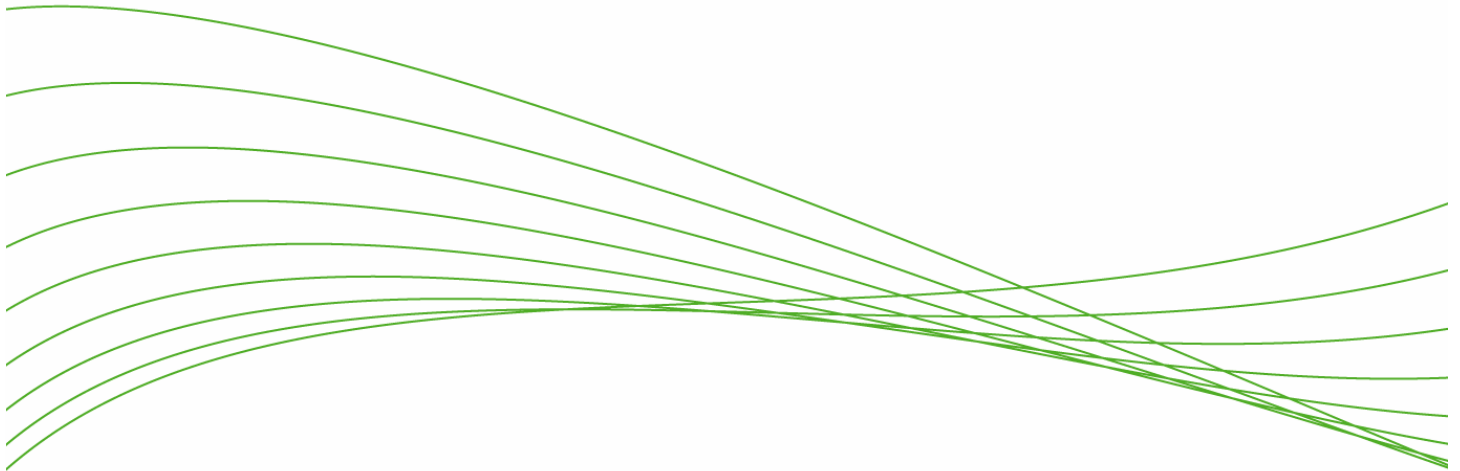


IDM and Endpoint Integrity Technical Overview



The Threats to Today's Networking Environments	2
Endpoint Integrity Defined.....	2
Endpoint Integrity Options.....	2
The ProCurve Solution: Endpoint Integrity <i>plus</i> Identity Driven Management.....	4
ProCurve and Client-based Endpoint Integrity.....	5
ProCurve and Network-based Proprietary Endpoint Integrity	6
ProCurve and Standards-based Endpoint Integrity	7
ProCurve and de facto standard Endpoint Integrity.....	7
Summary.....	8

The Threats to Today's Networking Environments

Computing in the 21st century is a different proposition from computing in the past. With the emergence of the Internet and the increased importance of email as a primary form of communication, computers are connecting, interacting and sharing information as never before. The mobile workforce has also played a part in changing the computing landscape; static, stationary computing resources are a thing of the past, replaced by laptops which move from conference room to conference room, desk to desk, and workplace to home and back again.

This new computing paradigm brings with it changes to networks and networking infrastructures. In the past, the network was just a convenient component of a productive work environment. Today, the network is a strategic corporate asset that goes beyond enabling convenient information sharing to being a fundamental component of an organization's productivity. Downtime resulting from viruses cannot be tolerated. The protection of confidential and competitive information assets and the ability to meet key government and industry compliance initiatives are mandatory requirements.

Thus it has become a business fundamental that networks be completely reliable and dependable. In the past this would have meant that the networking equipment itself would need to be of high enough quality to not break down. However, these days the dangers of failure are often not related to the reliability of the network equipment; but rather there is real and present danger from malicious or unintentional attacks on the network in the form of viruses, worms and other such external threats.

Typically, these attacks originate from outside the organization. However, with the advent of telecommuting and a mobile workforce, the actual attacks themselves frequently arise from inside the company intranet brought there by unsuspecting employees who inadvertently pick up viruses, worms and other malware from the Internet at home or on the road – outside the company's firewall. Thus the employee's endpoint¹ becomes infected via email or the internet, and when brought back to the organization, is unleashed to wreak its havoc on the internal network.

This current situation demands a solution which addresses these vulnerabilities and protects the network from such attacks. That solution is called Endpoint Integrity.

Endpoint Integrity Defined

Endpoint integrity is the functionality which examines all endpoints attempting to attach to the network and prohibits unsafe or non-compliant endpoints from gaining access. It insures that an endpoint attaching to the edge of the network is clean and meets configured criteria (e.g. antivirus program present and running with current signatures) before allowing it to inject a single packet into the network.

The basic idea is that when an endpoint physically connects to the network through a switch or wireless access point, it triggers a response from the endpoint integrity functionality, which checks to make sure that the endpoint meets certain entrance criteria before allowing it into the network. If the endpoint meets the criteria, it is granted appropriate access; if not, it is either denied or placed into a quarantine or remediation area.

Typical endpoint integrity implementations check compliance with respect to antivirus applications and signatures, operating system versions and patch levels, and any other programs that may be required or forbidden by the corporate guidelines.

There are two basic approaches to integrating endpoint integrity into your access control solution: client-based and network-based. These options are outlined below.

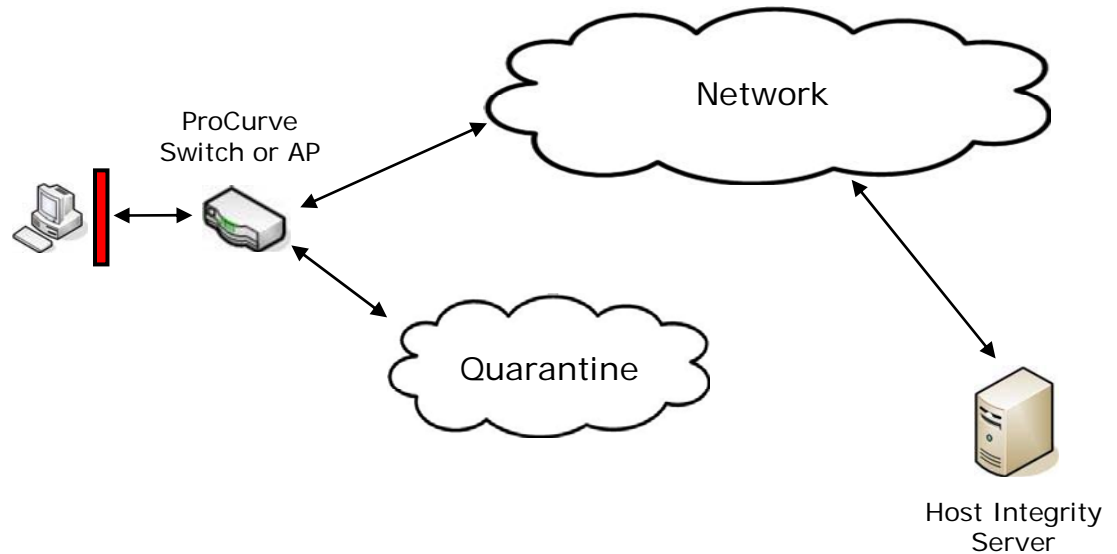
Endpoint Integrity Options

Endpoint integrity options fall into two major categories, which are described below.

Client-based solutions: In these solutions, there is an agent running on each endpoint which does the compliance checking and implements a local firewall to prohibit or limit network connectivity for non-compliant endpoints. Client-based solutions do not interact with network

¹ The term "endpoint" is used here, and in the remainder of the document, to indicate a user's PC, or any computer system connecting or attempting to connect to the network.

devices such as the edge switch or wireless access point; rather they restrict network access by using a local firewall on the connecting endpoint itself.



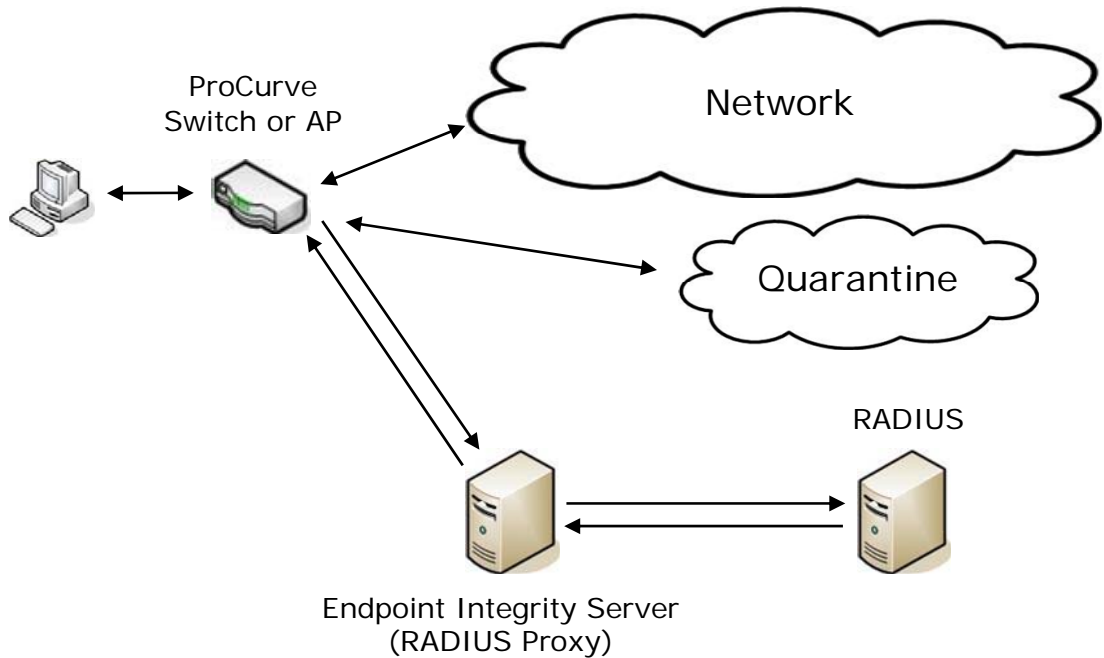
This is less secure than network-based solutions because the network port that connects the endpoint to the network is open. Any endpoint not running an endpoint integrity agent would have unrestricted access to the network.

However, running this type of solution in conjunction with an access control solution like mac-auth, web-auth, or 802.1X, provides access security for the network. The way it works is that the port connecting the user to the network is initially closed. Once the user authenticates successfully via mac-auth, web-auth, or 802.1X, the port becomes open, and at this point the agent's endpoint integrity steps in and performs its function.

Network-based solutions: In these solutions, the port (or access point) connecting the user to the network is initially closed, and the endpoint integrity function works in conjunction with the networking device to allow, deny or restrict access based on both user authentication and endpoint compliance.

Typically there is an agent running on each endpoint (although clientless solutions have been proposed). This agent works with (or includes) an 802.1X supplicant; 802.1X is used to authenticate the user and checks the compliance of the endpoint. It then utilizes capabilities in the connecting switch or wireless access point to put non-compliant endpoints into a quarantine area, typically a VLAN, using RADIUS attributes sent to the switch. Network-based solutions always utilize functionality in the edge networking device (switch or wireless AP) in order to deny, restrict or redirect traffic from a non-compliant endpoint. These solutions are more secure because the network is closed until both the user and endpoint have been authenticated and found to be compliant.

The following diagram shows a network-based solution with the endpoint integrity server running as a RADIUS proxy.



There are three subcategories of the network-based solutions.

Proprietary solutions: These solutions typically implement a RADIUS proxy, which allows the 'real' RADIUS server to authenticate the user. It then manages the user's connectivity through the configuration of the edge networking device (e.g. it's VLAN) using RADIUS, based on the result of the compliance state of the endpoint.

De facto standard solutions: Pervasive deployment to their installed base makes Cisco's NAC and Microsoft's NAP 'de facto standards'. Both solutions are open to software security vendors with products such as anti-virus and patch-level management; however, they each have limitations from a customer perspective. Cisco's NAC requires you to purchase expensive solutions that will not interoperate with other networking vendor equipment. Microsoft's NAP, however, is open to all networking device vendors but may have limited security at the point of access, depending on the type of NAP solution used. In addition, NAP is only applicable to clients running Microsoft operating systems.

Standard solutions: The Trusted Computing Group (TCG) is a consortium of companies who have agreed to create an open standard to ensure customers can choose the vendor that best meets their needs while being confident that the solution components remain interoperable. There is a standard called the Trusted Network Connect (TNC) which has defined an endpoint integrity solution and set of standard interfaces. An implementation of this standard available today is Funk Software's Steel Belted Radius EA, and other RADIUS and supplicant vendors are in the process of bringing their solutions to market. The solution uses the 802.1X and RADIUS standards to perform and communicate the compliance state of the endpoint to the policy decision point. The results of the decision (VLAN, ACL, etc.) are communicated back to the networking device in the form of RADIUS attributes.

ProCurve products operate in all of these environments. The integration of ProCurve devices and IDM with these endpoint integrity solutions is described below.

The ProCurve Solution: Endpoint Integrity *plus* Identity Driven Management

Before beginning to discuss the details of the solutions a few very important facts about ProCurve and endpoint integrity need to be understood. These are highlighted below.

ProCurve works with proprietary, de facto and standards-based solutions.

ProCurve's strategy is, and always has been, to support standards wherever they exist, and to create them where they don't. Thus the emphasis for ProCurve is to promote and support the

existing standard in this area, which is the TNC solution. ProCurve architects have been involved and have helped to drive this standard since its inception, and will continue to do so.

While working with industry leaders in support of open standards offers the best value to customers, ProCurve knows that it is not always possible or convenient for customers to move to the standards-based solution. Therefore ProCurve products can be deployed and interoperate with existing proprietary solutions, giving customers the ability to choose the solution that best fits their needs. ProCurve will participate in future de facto standards such as Microsoft's NAP as well.

ProCurve integrates Endpoint Integrity with Identity Driven Management to provide superior levels of quarantine and isolation for non-compliant users.

ProCurve's Identity-Driven Manager (IDM) product provides for the automatic and dynamic configuration of a connecting user's access rights. When a user connects to the network they are placed in the appropriate VLAN with the appropriate access rights (ACLs), as well as with the appropriate QoS and rate-limits. The initial release of IDM did this access-rights delivery based on *user, group, locatio*, and *time* information.

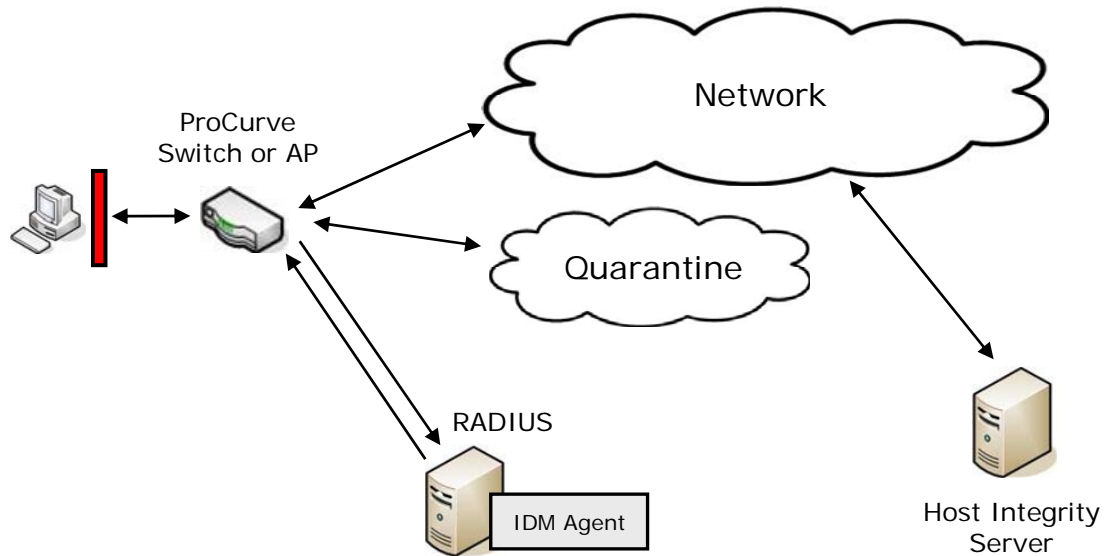
By integrating IDM with endpoint integrity, a user's access rights can now also be determined by their compliance to the endpoint integrity criteria. Thus, this extra input value, *endpoint-integrity-state*, is considered by IDM as it makes its access rights decision. This seamless integration allows for the definition of all access rights policies to be performed in a single location using a simple, intuitive interface.

Not only is there the simplicity of configuration, but also the level of quarantine and isolation available with this integrated solution is far superior to what is available with other solutions. This is because IDM brings with it the ability to set ACLs and even QoS and rate-limits for non-compliant users. Other network-based solutions can only place users on a separate VLAN where they can still infect others who are in that same VLAN. They could also potentially bring down the remediation VLAN with their malicious traffic. However, by being able to set the ACL for the user to restrict its traffic, the isolated user can only be allowed to connect to the appropriate remediation server, thus further limiting the damage that can be done until the user's endpoint is fixed.

The following sections describe how ProCurve products operate in these various solution environments.

ProCurve and Client-based Endpoint Integrity

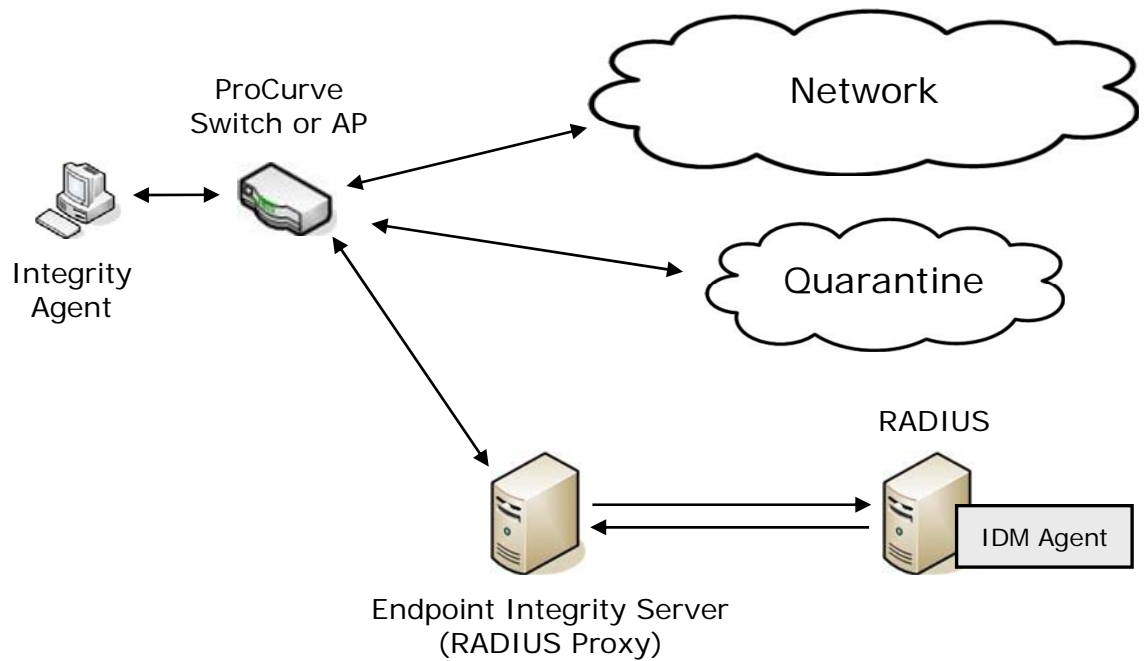
ProCurve devices work seamlessly with client-based solutions. In the most basic configuration, without access control, the network devices themselves are not even involved. With access control – mac-auth, web-auth or 802.1X – the switch will keep the network port closed until the user is authenticated, at which point the client-based endpoint integrity functionality begins to function and controls access from that system out into the network, based on compliance.



In fact, you can even use IDM in these environments in order to handle compliant users where normal user access rights are granted. And so, with this combined solution, you achieve endpoint integrity, access control and sophisticated access rights delivery via IDM. Although the overall security solution is not as comprehensive as network-based solutions, this may be the choice of customers who have either already invested in this type of solution, or who are satisfied with the level of security it provides.

ProCurve and Network-based Proprietary Endpoint Integrity

ProCurve devices and IDM work very well with existing proprietary endpoint integrity solutions, such as offered by Sygate (Symantec) and ZoneLabs (CheckPoint). These solutions operate as a RADIUS proxy for their compliance checking. They perform the checking at the time that the user attempts to connect to the network through the RADIUS server.



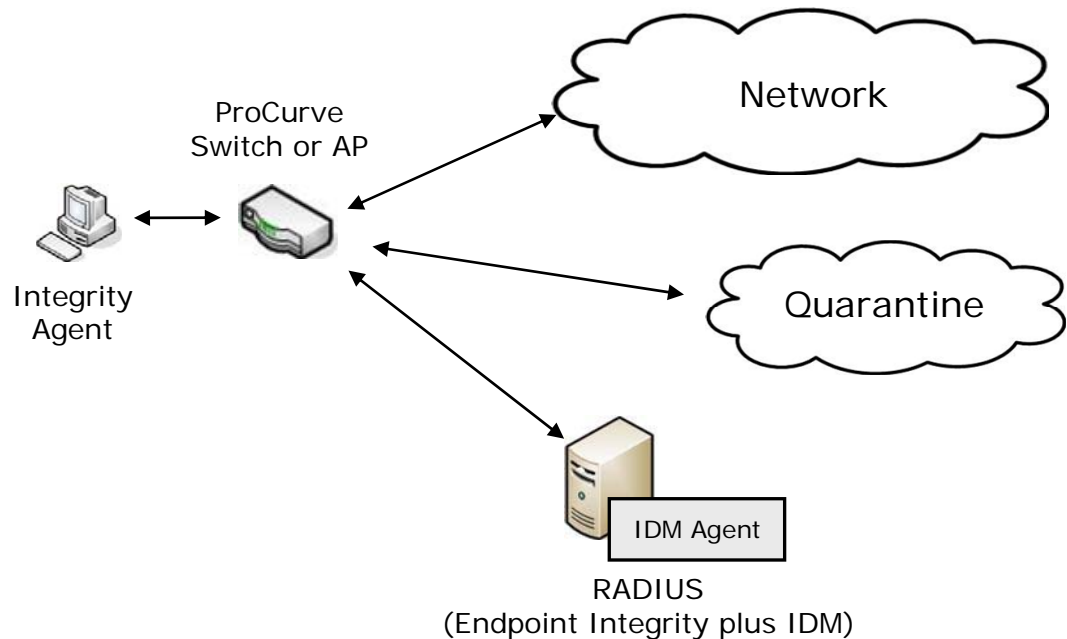
In this scenario, at the real RADIUS server where the IDM Agent is running, the user is authenticated and IDM assigns the appropriate access rights, independent of the endpoint integrity state. However, the endpoint integrity server has the last word: if the endpoint is non-compliant, the ProCurve device will be instructed to place the user into the quarantine VLAN. If the endpoint is compliant, then IDM sets the appropriate access rights for the user.

ProCurve and Standards-based Endpoint Integrity

The best solution is the standards-based endpoint integrity integrated with IDM. This allows for the rich security of an 802.1X solution, standards-based endpoint compliance checking and integrated robust access rights delivery from IDM.

The first such standards-based solution platform comes from Funk, based on their leading Steel-Belted Radius platform. It is supported with antivirus and patch management products from Symantec, McAfee, and PatchLink.

The way that this operates is that at authentication time, after the user has been authenticated, the compliance of the endpoint is verified. If the endpoint is found to be out of compliance, then IDM will take action to quarantine the user into the appropriate area, using VLAN, ACL, QoS and/or rate-limits as defined by the network access policy. At this point, the user is safely isolated into a strict isolation area with access only to the systems which can make the user's endpoint compliant with the integrity standards. When the compliance problem is remedied from within this restricted quarantine area, the user will be allowed back into the network and given the appropriate access rights from IDM for this newly-compliant user.



One of the major advantages of a standards-based solution such as this is that as time goes by the customer will have more and more chances to choose the endpoint integrity vendor, or vendors, which best suits their needs. For the first release, the choices are Symantec, McAfee, and PatchLink for the integrity applications, and Funk for the integrity platform. In the future, there will be other integrity applications and platform vendors to choose from.

ProCurve and de facto standard Endpoint Integrity

There are two de facto standard endpoint integrity architectures being proposed today by Cisco and Microsoft.

Since Cisco's Network Admission Control (NAC) solution is closed to networking vendors – all networking equipment must be from Cisco – it is not an open standard, and thus is not a candidate for interoperation with ProCurve.

Microsoft's Network Access Protection (NAP) architecture, on the other hand, is open to endpoint integrity as well as networking vendors. The architecture of NAP is consistent with the TNC standards-based solution, as shown in the diagram above. And as such, NAP will integrate with ProCurve devices as well as with IDM. So customers who are inclined to pursue the NAP solution will be able to utilize their ProCurve equipment and software with this endpoint integrity solution as well.

Summary

Why choose ProCurve?

- Works well with existing client-based and network-based solutions.
- Focused on standards so you can choose the best solution and vendors based on your needs.
- Integrated with award-winning IDM, allowing for a richer and more robust implementation of endpoint integrity.
- Future-proof: simplified product design integrates equally well with proprietary, standard and de facto standards, both now and into the future.

The following table shows the endpoint integrity options you have and some of the characteristics of each.

Solution Class	Solution Type	Security Provided	IDM Integration	Availability
Client-based	Without access control	Least	None	Now
	With access control	Moderate	Least	Now
Network-based	Proprietary	Better	Least	Now
	Standards	Best	Full	Now
	De facto standard (NAP)	Best	Full	Future

To find out more about
ProCurve Networking
products and solutions,
visit our web site at

www.procurve.com



© 2006 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA0-4385ENW, 02/2006