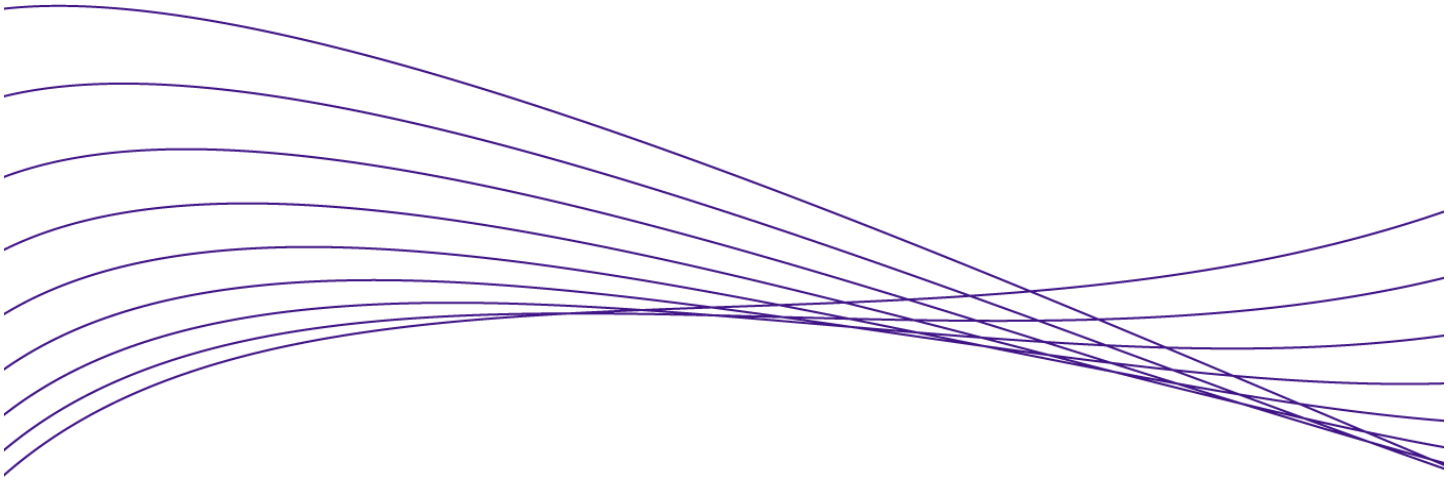
ProCurve Networking by HP

# ProCurve ProActive Defense: A Comprehensive Network Security Strategy



# Introduction

Security issues are not going away.

More networks are being attacked and threatened, in more devious and creative ways, than ever before. Incidents range from viruses and worms to Trojan horses and internal sabotage.

According to the 2006 CSI/FBI Computer Crime and Security Survey of U.S. corporations, government agencies, financial institutions, medical institutions and universities, the majority of organizations experienced computer security incidents during the previous year. Of those that experienced incidents, nearly one-quarter reported six or more attacks during the year.

At the same time, the information technology (IT) industry itself is evolving in ways that make it both more important and more difficult to secure networks. Some important factors include:

- Openness driven by the Internet, and the need to make resources available – securely – to more people;
- An increasingly mobile workforce, and the challenge of making the network available whenever and wherever people want to connect; and
- The convergence of voice, video and data over a single network, which can deliver greater efficiency if they can be run over a single network, thus overcoming the hassle and expense of running multiple networks.

Take just the example of increasing mobility. In 1999, one in five PCs were mobile; in 2005, it was one in three. In the next few years, laptops will outnumber desktops. While wireless networks and collaborative communication are a huge boon to users everywhere, they create equally huge security challenges for those who design and manage networks: People take their mobile devices away from the office and use them in potentially harmful and hostile environments. The mobile devices can get infected while in these environments, introducing the infections into the mission-critical enterprise when they return to the office. And with mobile devices, there is a greater tendency to mix personal and business use, which can jeopardize the security integrity of the device.

## The Impact of Network Security on Companies

The costs of security are rising, as are the costs of failing to provide effective network security.

Among the respondents in the 2006 CSI/FBI survey, reported losses due to network security incidents totaled nearly $52.5 million for the previous year. Almost 35 percent of respondents spent more than 5 percent of their IT budget on security measures. Nearly all the organizations invest in firewalls and antivirus software, and most have other security products in place, as well.

Unfortunately, focusing only on defending against external threats risks misses the large number of network attacks originating inside an organization.

And beyond actual attacks, compliance requirements – for regulations such as Sarbanes-Oxley, HIPPA, GLBA, FISMA, PCI and NERC – are becoming an immense burden and enormous expense. Companies are forced to demonstrate compliance with security requirements, both from regulatory bodies and internal mandates. For many organizations, compliance has become a top security concern.

In general terms, taking control of network security means companies must do the following:

- Control access to the network and enforce appropriate use;
- Eliminate viruses/worms and unwanted network traffic;
- Understand both the internal and external threats;
- Make sense out of the enormous amount of security intelligence available and turn it into actionable items; and
- Understand and demonstrate regulatory compliance to internal auditors, government agencies and supply chain partners.

To enable companies to achieve these goals, security solutions must be:

- Based on a trusted network architecture and a sound strategy that mitigates risk and returns control to the organization;

- Easy to deploy and use; and
- Standards-based, interoperable and reliable.

### The Security Approach Matters

Traditional core-centric network architectures are not up to the task for today's more frequent and potentially destructive assaults and challenges. These networks lack the scalability and dynamic capabilities required to handle current network security needs or meet rapidly changing business and technological requirements.

This paper describes a better alternative for network security: a comprehensive security vision and strategy that arises directly from the revolutionary ProCurve Adaptive EDGE Architecture™ (AEA), which embraces distributed intelligence at the network edge and takes a holistic approach to networking. The new security vision, called ProCurve ProActive Defense, is the first approach that combines proactive security offense techniques with steadfast traditional defense security techniques, simultaneously, at the edge of the network where users connect. As such, ProCurve ProActive Defense is expected to change dramatically how network security is deployed from now on.

## What is Network Security?

The first step in implementing network security is to define the characteristics and conditions of a secure network.

People often think of network security as defending against worms or viruses, or preventing access to the network by unauthorized users or protecting the privacy of network information and resources. In fact, network security is all these things, and more.

Some networking vendors have tried approaching security by focusing only on the perimeter, guarding against external threats using firewalls, virtual private networks (VPNs), intrusion detection systems (IDSs) and intrusion prevention systems (IPSs). Such a perimeter-only focus, however, does not address threats from inside the organization, and it creates an expensive and complicated management framework.

Other networking vendors focus their enforcement on core switches or core router blades, far from the network edge. While centralized enforcement might be easy to manage, it operates at a considerable distance from the "action" of points of attack and the network resources being attacked. This approach is analogous to stationing a building's security guard in the middle of the building, instead of near the entrances. By the time the security guard notices a problem, it's too late.

ProCurve takes a different – and far more effective – approach. By moving important access and policy enforcement decisions to the edge of the network where users and applications connect, ProCurve's ProActive Defense frees core resources to provide the high-bandwidth interconnect functions they are designed to perform. The result is not only better network security, but also better-performing, more scalable networks.

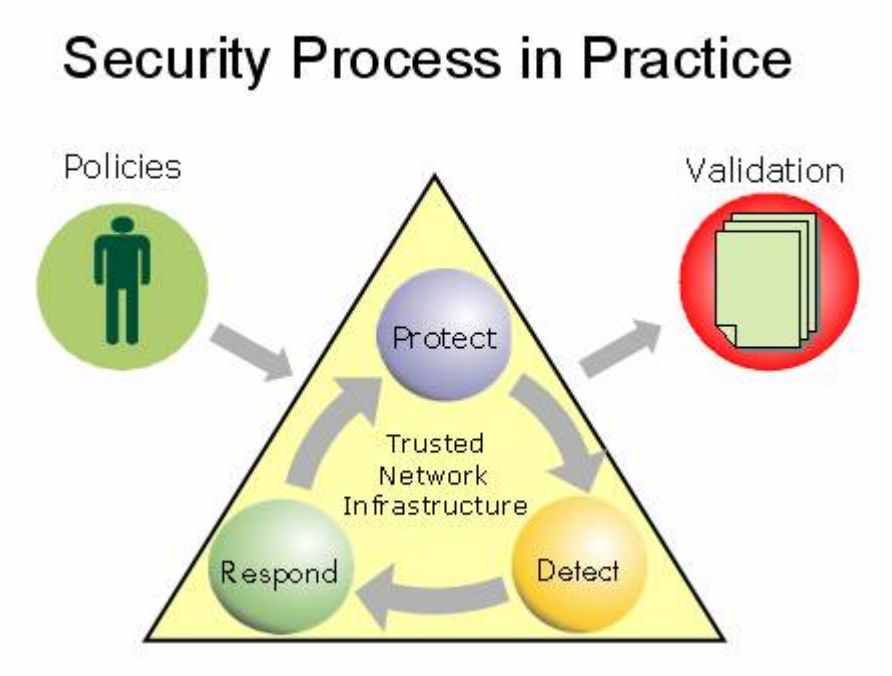
### Security is a Process, Not a Product

Many myths surround network security, including that there is a single shrink-wrapped "solution" to network security and that network security can be fully "achieved" and then crossed off the list.

Unfortunately, the network paradigm delivered by many vendors today does more to support than dispel these notions. Despite well-intentioned efforts to provide network security "solutions," the vast majority of networking vendors at best come up with "bolted-on" approaches that do nothing to relieve the complexity of managing network security.

Instead of believing the prevalent myths about security, it's important to recognize that effective network security is a process, not a product or the latest patch. The dynamic nature of network security means that security should be automated – so that the network itself can react to and repel threats.

But such automation works only if it arises within a trusted network infrastructure. In other words, the *process* of network security must begin with the network architecture itself – and that network architecture must be founded on trustworthy technologies.




As illustrated above, the ProCurve security architecture – with management tools that "command from the center" the network edge devices – is designed to:

- Prevent security breaches and protect the network before a breach occurs; prevent unauthorized users from accessing or eavesdropping on the network; prevent hosts and applications from being deployed on the network without authorization.
- Automatically detect external and internal security threats; detect attacks during a security breach.
- Respond automatically and appropriately to a security breach; correlate network threat events and dynamically respond to mitigate attacks.

## ProCurve Adaptive EDGE Architecture

The ProCurve Networking Adaptive EDGE Architecture (AEA) departs dramatically from the prevalent networking paradigm, which forces companies to adopt and manage a "network of networks" in which features are afterthoughts or exist in isolation. Instead, the AEA encompasses a holistic, comprehensive view of the network and distributes intelligence to the edge, where users connect.

The main tenets of the AEA are "control to the edge" with "command from the center." These two tenets are achieved because intelligence – defined as the ability for the network to respond and react – is located at the edge, where users and resources connect with the network. At the same time, the policies and rules governing the network's intelligence reside conveniently and centrally in the hands of the network administrators.

It is this dynamic configuration of the edge (control to the edge) from the management center (command from the center) that enables automation of functions including network security. This automation is essential for reducing both the costs and the complexity of the network.

### AEA is the Basis for ProCurve's Security Strategy

The cohesiveness and distributed intelligence of the AEA enable ProCurve to offer a security vision and strategy unlike previous approaches. Importantly, the AEA establishes the trusted network infrastructure necessary for security automation.

The AEA's *control to the edge* of the network means that decisions about security happen automatically, at the point where users connect. This approach leads directly to more efficient, less complex and more flexible network and security management.

The AEA's *command from the center* – the ability for ProCurve management tools to set security policies and report alerts and information about the security of the network – provides unified access to critical network resources based on policies enforced at the individual user level. As a result, organizations can more effectively protect secure data while making sure that authorized users gain access to the network resources they need to be most productive.

An important aspect of the AEA is that it is built on industry standards. In fact, ProCurve not only supports standards in its products, it also takes a leading role in the creation and adoption of networking industry standards.

As a result of this standards leadership, ProCurve can ensure that its products interoperate with third-party solutions and provide long-lasting choice and flexibility for companies using these products. With standards-based security, companies avoid being locked into proprietary schemes that may or may not work with other equipment or under conditions that arise in a year or five years.

## ProCurve ProActive Defense

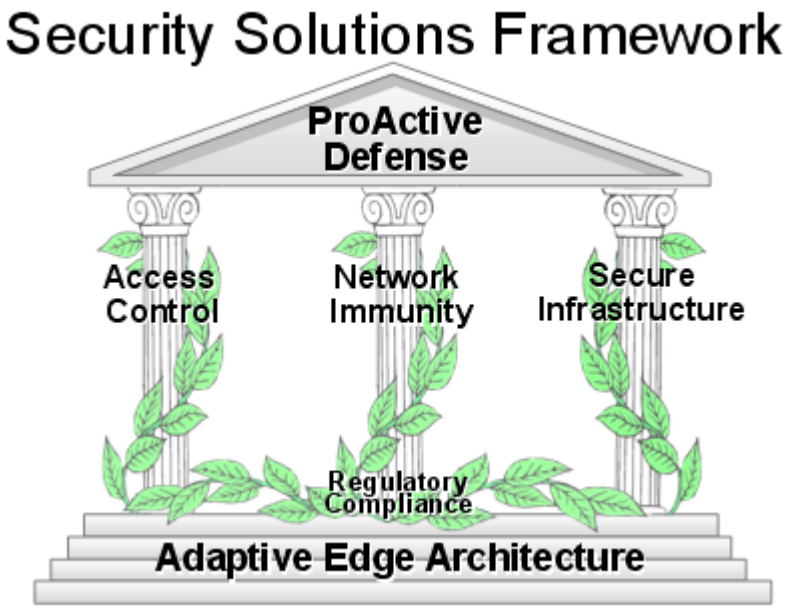
ProCurve's comprehensive security vision and strategy – ProCurve ProActive Defense – delivers a trusted network infrastructure that is immune to threats, controllable for appropriate use and able to protect data and integrity for all users.

The three main pillars of the ProActive Defense strategy are as follows:

*Access Control:* Proactively prevents security breaches by controlling which users have access to systems and how they connect in a wired and wireless network.

*Network Immunity:* Detects and responds to internal network threats such as virus and worm attacks; monitors behavior and applies security information intelligence to assist network administrators maintain a high level of network availability.

*Secure Infrastructure:* Secures the network for policy automation from unauthorized extension or attacks to the control plane; includes protection of network components and prevention of unauthorized managers from overriding mandated security provisions; also includes privacy measures to ensure the integrity and confidentiality of sensitive data: protection from data manipulation, prevention of data eavesdropping, end-to-end VPN support for remote access or site-to-site privacy, and wireless data privacy.




Together, the three pillars of Access Control, Network Immunity and Secure Infrastructure work to secure the network while making it easier for companies to comply with – and verify compliance for – regulatory and other requirements.

## Simultaneous Offense and Defense

A unique aspect of the ProCurve ProActive Defense vision and strategy is that it combines both the security offense and security defense at the same time and, most importantly, at the network edge. This combined offense and defense is possible only because ProActive Defense is based on Adaptive EDGE Architecture principles, which drive intelligence to the network edge while retaining centralized control and management.

### Offense

The ProActive (offense) piece, which is primarily about access control, is a comprehensive way of managing access to the network, dealing with all types of users: everything from an uncontrolled user to an authenticated user to a fully trusted user.

Today, a multitude of devices connect to the network, including laptops, IP phones, peripherals, PDAs and various wireless devices as well as traditional desktop computers. It is essentially impossible for IT departments to mandate a specific operating environment for all devices that access the network. As a result, it is vital to employ a proactive access control solution that is comprehensive and capable of identifying and controlling access for all users and device types. The access control solution must be capable of proactively validating the integrity and operating state of all users and devices.

### Defense

The defense piece of the ProCurve ProActive Defense starts with a trusted network infrastructure that is reliable, self-identifying and fully authenticated.

At the same time, the infrastructure must remain plug-and-play and easy to manage. Security is not effective if it is too complex to implement or if it degrades the performance of the overall system. For that reason, the ProCurve trusted network infrastructure includes built-in threat management and anomaly detection. These capabilities are embedded features that promote the defensive security posture of the trusted network infrastructure.

# How ProCurve Implements ProActive Defense

Recognizing that network security is a process rather than a discrete solution, and that it must arise holistically from the network infrastructure itself, ProCurve weaves security capabilities throughout its network infrastructure and offerings.

Here are some highlights of how ProCurve implements its ProActive Defense strategy:

- ProCurve builds defensive security features into its switches, access points and other hardware, enabling the creation of a trusted network environment.
- ProCurve-designed network processor chips – notably, the fourth-generation ProVision™ ASIC – embed policy enforcement capabilities into the Adaptive EDGE Architecture. The ProVision ASIC is built into the recently introduced ProCurve Switch 5400/3500 Series products and will be included in future products, as well.
- Integrated security and performance management, via ProCurve Manager (PCM) network management software and ProCurve Network Immunity Manager (NIM), allows network security to be automated as well as pervasive, and it takes the complexity out of security management.
- Distribution of intelligence to the edge of the network enables effective proactive access control, which is enacted by ProCurve Identity Driven Manager (IDM) 2.0, a software module for ProCurve Manager Plus (PCM+). IDM allows organizations to define network access policies that enforce secure access to the network and provide dynamic security and performance configuration to network ports as users connect. IDM lets network administrators proactively control access to the network based upon user or device identity, location, time of day and an end point's integrity.
- Virus Throttle technology and anomaly detection are provided as embedded threat defense capabilities.

## ProActive: Access Control and the Intelligent Edge

ProCurve's delivery of advanced access control capabilities predates the ProActive Defense strategy. In fact, it is rooted in ProCurve's initiation of key industry standards activities – notably, the IEEE 802.1X standards for port-based network access control – almost a decade ago.

Since then, ProCurve has added to and refined its access control offerings, culminating in comprehensive access control through its IDM 2.0 software module. Importantly, ProCurve's approach to user-based access control, as exemplified by IDM 2.0, also includes *usage*: Once users are admitted to the network, IDM determines what resources they gain access to, where they can go in the network and what boundaries will be imposed on their movement through the network.

With IDM, network administrators can set policies for both performance and security management. Additionally, IDM assists with reporting for regulatory compliance.

A number of ProCurve products are designed specifically for secure access, including secure wireless access. The ProCurve Secure Access 700wl Series provides seamless secure roaming and session persistence, centralized security configuration and policy management, and automatic enforcement of user authentication and access rights for both stationary and mobile users. Its flexible authentication modes – with customizable Web-based authentication screens and ability to authenticate uncontrolled clients (i.e., end points that do not have specific authentication agents) – enables guest access and greater overall authentication control.

Similarly, the ProCurve Switch xl Access Controller Module (ACM), a blade for the ProCurve Switch 5300xl Series, delivers a unique approach to integrating identity-based user access control, wireless data privacy and secure roaming with the flexibility of a full-featured intelligent edge switch.

For controlling policies at the network edge, ProCurve products incorporate standards-based IPsec VPN security, as well as wired and wireless authentication via 802.1X, Web-based authentication and Media Access Control (MAC) authentication.

Industry standards important to the ProActive part of ProCurve ProActive Defense include:

- IEEE 802.1X (a port authentication protocol that ProCurve initiated and for which it serves as a key technical contributor).

- TNC (Trusted Network Connect) from the Trusted Computing Group (end device compliance authorization; ProCurve initiated this standard, served as interim chair and edited the IF-PEP protocol).
- IETF RADIUS Extensions (ProCurve served as Internet-draft editor and technical advisor for these protocols).
- IETF NEA[1] (network endpoint assessment); ProCurve is championing the TCG/TNC liaison and contributing to this standard).
- In addition, ProCurve's access control solution is compatible with the Microsoft NAP architecture.

### Defense: Network Immunity and Command from the Center

ProCurve Manager (PCM) management software provides a complete platform for management of all aspects of network security, including advanced policy-based device and traffic management. Importantly, because it is part of the comprehensive Adaptive EDGE Architecture framework, PCM both simplifies and boosts the effectiveness of network management.

ProCurve ProActive Defense also encompasses embedded virus detection and response that includes:

- Virus Throttle software – an algorithm embedded within the ProVision ASICs that rapidly detects and quarantines a virus or worm, preventing its ability to spread and disarming its ability to harm the network.
- ICMP throttling – defeats denial-of-service attacks by enabling any switch port to automatically restrict Internet Control Message Protocol (ICMP) traffic.
- Control protocol detection – software that prevents Address Resolution Protocol (ARP) spoofing, rogue Dynamic Host Configuration Protocol (DHCP) servers and Spanning Tree root protection.
- Device authentication – enables ProCurve switches and access points to authenticate to one another using 802.1X to form a trusted infrastructure.
- Network Immunity Manager – a security management tool that monitors wired and wireless networks for internal network threats and allows administrators to set security policies for threat detection and response.

Industry standards important to the Defense aspects of ProCurve ProActive Defense – and for which ProCurve is a voting member and contributor in each case – include IEEE 802.1AE-2006 (MAC security and Ethernet encryption); IEEE 802.1af (encryption key agreement protocol); and IEEE 802.1AR (secure device identity).

## The Future of Network Security

While predictions are necessarily uncertain, it's likely that the future of network security will be one of evolution rather than revolution: There will be further integration of the security offense and defense, with ever easier-to-deploy solutions that allow security protection to be always enabled.

For instance, ProCurve's roadmap for its ProActive Defense strategy includes characteristics such as the following:

- Additional enhancements to Identity Driven Manager, such as clientless and agent-based endpoint integrity with flexible remediation and a vulnerability assessment framework.
- Additional enhancements to Network Immunity Manager, such as increased network behavior anomaly detection (NBAD) capabilities.
- Enhanced policy control at the edge, including Web-Auth with clientless endpoint integrity authentication.
- Standards-based endpoint integrity, with trusted agent access for LANs, WANs and WLANs.

[1] Working group pending approval

- Further enhancements to ProCurve Manager to create a platform that combines access and secure network infrastructure management.
- Continued and increased embedded threat management and infrastructure authentication capabilities.
- Additional new products and solutions that fit into the ProActive Defense framework and that provide solutions to security issues not yet identified, as they arise.

## Final Advice

The first step in network security is to realize the importance of combining the offense and defense into a single comprehensive system. You must understand the threats to your network assets – as well as the risks to your business if those assets are compromised. Remember, there are both internal and external threats to consider. Businesses need to know how attacks are going to occur so they can understand what to do about them.

To deliver more security with less complexity, security practices must be automated and auditable. The business policies that represent how the network service is supposed to behave need to be entered into an automated network system of enforcement that is capable of reporting on those policies to make sure they are working. This automation must be founded upon a trustworthy network infrastructure.

ProCurve ProActive Defense, arising from the ProCurve Adaptive EDGE Architecture, is the only approach offered today that has the built-in flexibility to meet not only today's security challenges, but tomorrow's, as well. By uniquely melding offense and defense into a cohesive, easily managed and comprehensive architecture, the ProCurve ProActive Defense is the best way to harness the full potential of networks, now and in the future.

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

**www.procurve.com**


© 2007 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.

4AA1-0786ENW Rev. 1, 7/2007