

# Network Immunity Solution



## Technical White paper

Introduction .....	2
Current Security Threats .....	2
Solutions for Internal Threat Protection .....	2
Network Immunity Solution: What It Is and How It Works.....	2
Benefits of Network Immunity Solution.....	3
How It Works .....	4
Security Management .....	5
Reporting.....	5
Flexible Deployment .....	6
Scalability .....	6
Third-party IDS/IPS/UTM device support .....	6
Industry-leading warranty .....	6
Competitive Advantages.....	6
Summary.....	7

## Introduction

### Current Security Threats

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, more than half of the organizations surveyed – U.S. corporations, government agencies, financial institutions, medical institutions and universities – experienced computer security incidents during the previous year. Of those that experienced incidents, nearly 25% reported six or more attacks during the year.

The reported losses are significant: \$52 million for the 313 respondents, an average of \$167,000 per respondent. Importantly, only half of the total survey respondents actually reported their losses – there appears to be significant concern about public reporting of attacks and losses – and so it's difficult to accurately gauge the actual losses. One thing is certain: network attacks are far more widespread than had been imagined.

Over the past decade, the primary network security strategy for many IT managers has been to invest in perimeter security defenses to protect against external threats. They believed that all threats were external, and that the network with the biggest moat at its network perimeter was the safest. Packet-filter routers, firewalls, applications proxies, and VPNs are all technologies that came of age during that time.

Vendors and customers came to see their network design as having a “hard crunchy shell with a soft chewy center.” That is, security strategies intentionally disregarded internal network edge security, assuming that (somehow) the internal network was inherently more secure. For many organizations, this assumption has backfired painfully.

Without adequate protection from internal threats, networks are susceptible to viruses, worms, user sabotage and other attacks that can cause significant downtime, revenue loss, end user dissatisfaction and an increase in IT management bandwidth.

### Solutions for Internal Threat Protection

Current options available for customers to comprehensively detect attacks inside their network are usually costly, performance limited and/or marginal in security value.

Many customers today are protecting their networks by putting firewalls at the periphery of their network and anti-virus software on client PCs. Unfortunately, their networks are vulnerable to advanced security threats, such as viruses and worms, since most firewalls are incapable of performing the deep inspection to look for virus signatures. Nor do firewalls perform Network Behavioral Anomaly Detection (NBAD) to look for network behaviors indicative of attacks. Likewise, PC anti-virus software does not protect against zero-day virus attacks, not to mention the fact that many customers permit network access even to end users whose anti-virus files aren't up-to-date.

Other organizations have installed expensive technologies such as IPS (intrusion prevention system) devices inline on many distribution switch uplinks. Given the higher cost and lower performance of IPSs compared to the switch networking infrastructure, it's obvious that customers need a more efficient and affordable solution to gain visibility into internal threat activity.

ProCurve Network Immunity Manager is a cost-effective software solution for managing internal network threats. Network Immunity Manager brings security and the network together by leveraging internal attack detection in conjunction with external network and security information to monitor the network for internal threats. It can pinpoint the source of security events and then leverage the network to mitigate those threats.

## Network Immunity Solution: What It Is and How It Works

ProCurve Network Immunity Manager is a plug-in module for ProCurve Manager Plus that provides a rich toolset to manage internal network threat detection and response. Together, ProCurve Manager Plus and the Network Immunity Manager plug-in constitute the ProCurve Network Immunity Solution.

ProCurve Network Immunity Manager monitors access points and switch ports across the network for internal network threats and allows administrators to set detection and response security policies.

By leveraging security traffic monitoring technology built into ProCurve switches, such as sFlow and Virus Throttle, ProCurve Network Immunity Manager performs NBAD (Network Behavior Anomaly Detection) to detect and respond to internal threats in both wired and wireless networks. Optionally, the Network Immunity Manager can remotely mirror suspect traffic to an IDS/IPS/UTM appliance for high-confidence detection of known viruses, using virus signature file matching. With Network Immunity Manager, IT managers enjoy broad coverage against internal attacks and a rich set of mitigation and offender tracking capabilities.

This easy-to-use security management tool turns access points and switch ports into security sensors, provides visibility into internal threat activity on the network and helps administrators to maximize network availability.

## Benefits of Network Immunity Solution

### Business Benefits

Businesses need to maintain maximum network availability, meet regulatory compliance requirements, protect their investment in network hardware and management tools, and deploy affordable efficient solutions. For companies that have invested in ProCurve switches, the Network Immunity Manager meets these critical needs.

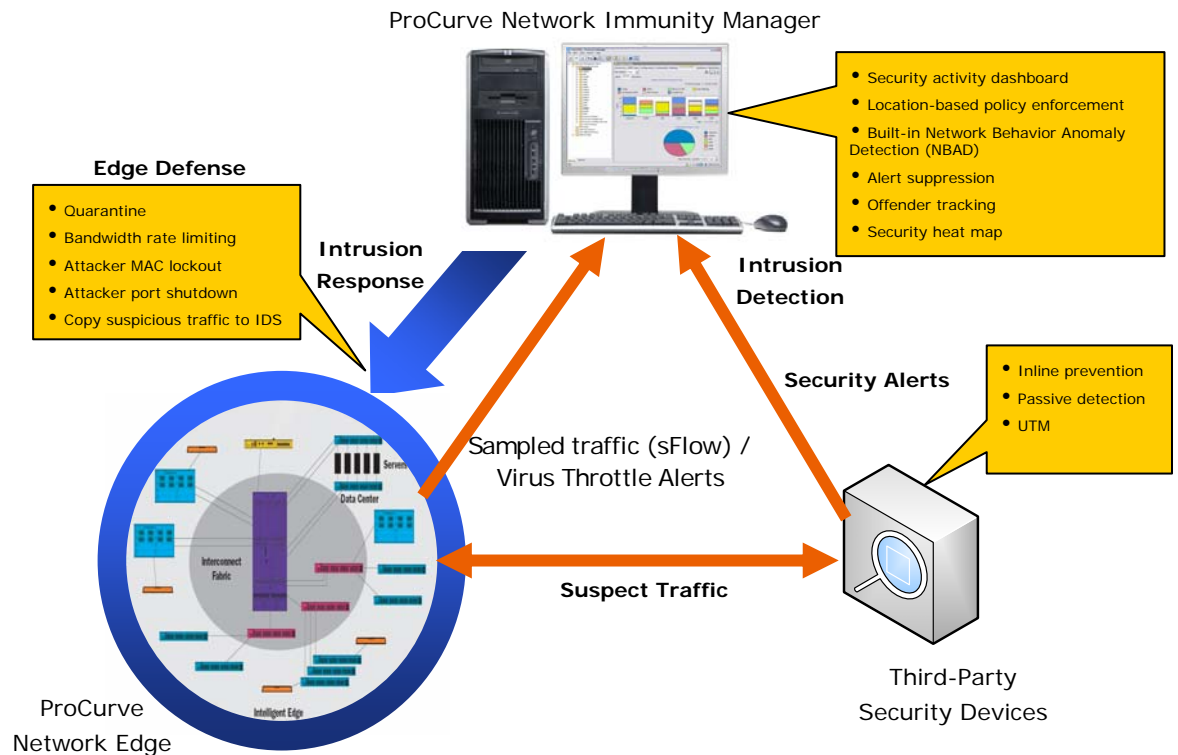
Business Needs	ProCurve Network Immunity Manager
Maximum Network Availability	Detects and automatically responds to internal network attacks
Regulatory Compliance Assistance	Provides security attack policy and action reports
Investment Protection	Leverages built-in ProCurve switch technology to make each port a security sensor
Affordability and Efficiency	Provides broad coverage of internal attacks with few components

### IT Manager Benefits

IT Needs	ProCurve Network Immunity Manager
Internal Threat Protection	Detects known and zero-day attacks inside the network
Automated Threat Response	Provides a rich set of automatic network attack mitigation actions on the offender that initiated the attack including: <ul style="list-style-type: none"> <li>Quarantine VLAN</li> <li>MAC lockout</li> <li>Port shutdown</li> <li>Port bandwidth rate limit</li> <li>IT administrator email notification</li> </ul>
Offender Tracking (forensics)	Displays the offender's IP address, MAC or DNS name, offender network access details (requires Identity Driven Manager), and username (requires Identity Driven Manager)

# How It Works

## Architecture



ProCurve Network Immunity Manager is a plug-in to the ProCurve Manager (PCM) management suite. Both the Network Immunity Manager and PCM are delivered as software packages.

### Attack Detection

There are two ways to deploy attack detection with the Network Immunity Manager: in standalone mode, or in conjunction with third-party security devices.

Network Immunity Manager standalone scenario (NBAD detection)

- ProCurve switches send sampled traffic using sFlow technology to the Network Immunity Manager, which performs NBAD (Network Behavior Anomaly Detection) on the data to detect internal attacks.
- The Network Immunity Manager can accept virus alerts from ProCurve switches running Virus Throttle software that detect IP Fan Out virus behavior.
- The Network Immunity Manager can detect the following types of internal threats:
  - Zero-day and known viruses or worms, similar to: SQL Slammer, CodeRed, Sasser, MSBlaster, etc.
  - Protocol anomalies, similar to: Land attack, UDP Flood, UDP Bomb, etc.
  - Reconnaissance scans, similar to: port scanning, fPing, superscan, nmap, etc.
  - Network-based attacks, similar to: DNS tunneling, Smurf, IP spoofing, etc.
  - Anomalous packet sizes, similar to: Ping-of-death, Nmap, Netcat
- The Network Immunity Manager's NBAD capability doesn't rely on signature file matching in the same manner as anti-virus or IPS, but rather detects behaviors symptomatic of viruses, worms, or malicious users.

### Third Party Security Devices scenario

- ProCurve Network Immunity Manager can accept security attack alerts from select third-party devices, such as IDS/IPS and UTM appliances, that have already been deployed in strategic locations. This allows organizations to leverage existing security infrastructure without having to do more than send security alerts to the Network Immunity Manager.
- The Network Immunity Manager can bring suspect traffic to a security device for inspection by leveraging ProCurve's Intelligent Remote Mirroring feature, present on ProVision-based switches. This allows the security device to be virtually deployed anywhere within the network on a moment's notice. The security device can then inspect the traffic and generate alerts that are subsequently consumed by the Network Immunity Manager for correlation, mitigation and logging purposes.

### Response

- As security events occur, the Network Immunity Manager can be configured at multiple response levels, from just quietly recording events as they unfold to taking multiple active mitigation actions against the threat.
- The Network Immunity Manager can be configured to send emails when one or more events of interest occur.
- The Network Immunity Manager can respond to attacks on a per-access point or per-port basis, based on the policies set by the IT administrator. The spectrum of responses include:
  - Quarantine the attacker on a VLAN
  - Bandwidth rate limit the port that originated the attack
  - Lock out the attacker's MAC address
  - Shut down the attacker's port
  - Mirror suspicious traffic to security device
  - Alert the IT administrator of the attack via email

### Security Management

The ProCurve Network Immunity Solution (ProCurve Manager Plus with the Network Immunity Manager plug-in) supports these security management features:

- **Policy Management** – Utilizes the PCM Automation Manager to create and manage mitigation policies based on event source, location, time, action and other alert parameters.
- **Security Event Collection and Suppression** – Collects security alerts from anomaly detection, ProCurve switches and third-party security devices in a single management tool, and suppresses duplicate alerts to trigger a single action for a flood of alerts.
- **Security Dashboard** – Provides a real-time view of security activities, mitigation actions taken, and offender details across the network over various time intervals.
- **White List (Exempt List)** – Allows you to create a set of IP addresses, MAC and DNS names that are exempted from mitigation actions.
- **Configuration Cleanup** – Provides automatic rollback response configurations from ProCurve switches and wireless access points after the policy expires.
- **Security Auditing** – Utilizes PCM Audit Logging to log any changes to policy configurations and network devices.
- **ProCurve Manager Integration** – Has built-in capability to manage ProCurve switches, routers and wireless access point configurations, and understand network topology.

### Reporting

The ProCurve Network Immunity Solution can provide reports that include security policy reports and offender tracking reports for forensics. The Network Immunity Solution supports these reporting features:

- **Data Mining** - Generate network-based, offender-based and alert-based tabular reports with various degrees of information granularity.
- **Custom Reports** – Generate reports from the PCM database schema to assist with regulatory compliance. See the ProCurve white paper "Sustainable Compliance" ([www.procurve.com](http://www.procurve.com)) for information about regulatory compliance reporting.

## Flexible Deployment

To provide flexibility in deployment, ProCurve Network Immunity Manager supports several use models:

- **Network Behavior Anomaly Detection and Response** – Use Network Immunity Manager to detect unknown or zero-day attacks and mitigate threats at the ProCurve network edge.
- **Active Intrusion Prevention and Response** – Prevent attacks using an inline IPS/UTM appliance; mitigate threats at the ProCurve network edge using Network Immunity Manager.
- **Passive Intrusion Detection and Response** – Detect attacks using an offline IDS/UTM appliance; mitigate threats at the ProCurve network edge using Network Immunity Manager.

## Scalability

The ProCurve Network Immunity Solution provides broad coverage for small or large switch and access point coverage.

- **Monitoring** - Monitor up to 10,000 edge nodes across the wired and wireless network.

## Third-party IDS/IPS/UTM device support

Network Immunity Manager supports these third-party IDS/IPS/UTM devices:

- Cisco IPS 4200 series sensor
- ISS Proventia G Series IPS appliances (estimated support date: June 2007)
- Fortinet UTM appliances (estimated support date: July 2007)

## Industry-leading warranty

- 90-day media warranty (software)

## Competitive Advantages

ProCurve Network Immunity Manager has a simple, efficient, and affordable architecture that provides broad coverage of internal threat protection for wired and wireless networks, with several components utilizing security monitoring technology built into ProCurve switches.

ProCurve Network Immunity Manager differentiates itself from the competition by:

- Providing wired and wireless support. Other solutions are designed to function only in a wired *or* wireless environment, but not both.
- Making full use of the security capability of the switch and access point infrastructure. Many ProCurve infrastructure devices include built-in sFlow sampling technology and/or Virus Throttle.
- Offering a rich set of response options, as compared with most competitors' limited set of response actions.
- Supplying more security with less complexity. ProCurve has always differentiated itself through easier and more intuitive technologies.

## Summary

ProCurve Network Immunity Manager is the Defense piece of the ProCurve ProActive Defense security strategy to build a trusted network infrastructure. Together with ProCurve Access Control solutions such as Identity Driven Manager, ProCurve Network Immunity Manager provides security at the edge of the network where users connect. ProCurve Network Immunity Manager defends the network against internal threats by detecting and responding to internal threats.

**The ProCurve Network Immunity Solution provides significant value by:**

- Maximizing network availability
- Providing an affordable and efficient scalable solution with few components
- Providing internal threat management
- Providing zero-day attack protection
- Maximizing the current investment in ProCurve switches
- Providing offender tracking capabilities
- Providing internal threat coverage for both wired and wireless networks

ProCurve Network Immunity Manager helps customers deploy the right security solutions based on their individual needs.

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

[www.procurve.com](http://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.

4AA1-0788ENW, 02/2007