

## ProCurve Network Immunity Manager 1.0

The ProCurve Network Immunity Manager is a plug-in for ProCurve Manager Plus that detects and automatically responds to threats, such as virus attacks, inside the network. This security management tool monitors devices across the network for internal network attacks and allows administrators to set detection and response security policies. It leverages security and traffic-monitoring features built into ProCurve switches with the ProVision ASIC, such as sFlow, Virus Throttle, and remote mirroring technologies, and it performs NBAD (Network Behavior Anomaly Detection) to detect attacks. Optionally, it remotely mirrors suspect traffic to an IDS/IPS/UTM appliance for virus signature file matching to provide administrators with broad coverage against malicious attacks and a rich set of attack-mitigation and offender-tracking capabilities. This easy-to-use security management tool provides visibility into virus activity on the network and helps administrators maximize network availability f

# ProCurve Network Immunity Manager 1.0

## Features and benefits

### Addition Information

#### • **Intrusion detection:**

- **Network visibility:** monitor traffic for internal network threats across wired and wireless networks using sFlow data from ProCurve devices
- **Multiple intrusion detection methods:** detect intrusions using virus throttle alerts from select ProCurve switches, NBAD (Network Behavior Anomaly Detection) performed by Network Immunity Manager, and security alerts from virus signature-based third-party IDS/IPS security devices
- **Remote monitoring for deeper analysis of traffic:** mirrors suspect traffic to select third-party IDS/IPS/UTM devices for virus signature file matching for high-confidence detection of known viruses; leverages one IDS/IPS/UTM device across the network
- **Offender tracking:** identifies the offender (username, IP, and MAC and DNS name) responsible for the network attack and displays their location; additional information can be displayed, such as the offender's name and network access information when Identity Driven Manager is installed
- **Security heat map:** real-time view of security activities across the network; displays devices where attacks occur using visual color-coding

#### • **Intrusion response:**

- **Internal threat protection:** discover the switch port where the offender connects and mitigate the attack at the port where attack originates (Per-Port-Response)
- **Location-based policy enforcement:** set and enforce security policies based on the network location of the offender and the time of attack
- **Multiple threat mitigation responses:** mitigate internal network attacks by putting the offender in a Quarantine VLAN or using offender bandwidth rate limiting, offender MAC lockout, offender port shutdown, or IT administrator e-mail alert notification only
- **Chain of actions:** provides a prioritized list of mitigation actions, so when a response to the

attack fails, an alternate response can be triggered

- **Wireless support:** mitigate threats from wireless LAN by blocking offender MAC address

#### • **Security management:**

- **Policy management:** create and manage mitigation policies based on event source, location, time, action, and other alert parameters
- **Security event collection and suppression:** collect and display internal threat alerts and suppress duplicate alerts to trigger one action for a flood of alerts
- **Security dashboard:** real-time view of security activities, mitigation actions taken, and offender details across the network over various time intervals
- **White list (exempt list):** set of IP address and MAC and DNS names that are exempt from mitigation actions
- **Configuration cleanup:** automatic rollback response configurations from ProCurve switches and wireless access points after the policy expires

#### • **Reporting:**

- **Data mining:** generate network-based, offender-based, and alert-based tabular reports

#### • **Flexible deployment:**

- **Network Behavior Anomaly Detection and response:** detect attacks using NBAD analysis of sampled traffic and Virus Throttle attack alerts from select ProCurve switches, and mitigate threats at the ProCurve network edge using intrusion-response capabilities
- **Passive intrusion prevention and response:** remotely mirror suspect traffic identified by NBAD analysis to an offline IDS/IPS/UTM device for a virus signature file match to detect attacks and mitigate threats at the ProCurve network edge using Network Immunity Manager's intrusion-response capabilities
- **Active intrusion prevention and response:** prevent attacks using inline IDS/IPS/UTM device and mitigate threats at the ProCurve network edge using Network Immunity Manager's intrusion-response capabilities

# ProCurve Network Immunity Manager 1.0

- **Third-party IDS/IPS/UTM device support:**

- **Cisco:** Cisco IPS 4200 series sensor
- **Fortinet::** Fortinet UTM appliances (estimated support date: June 1, 2007)
- **Sonicwall:** Sonicwall UTM Pro series appliances (estimated support date: July 1, 2007)

- **Industry-leading warranty**

- 90-day media warranty (software)

# ProCurve Network Immunity Manager 1.0

**ProCurve Network Immunity  
Manager 1.0 50-device license  
(J9060A)**

**ProCurve Network Immunity  
Manager 1.0 +100-device  
license (J9061A)**

**ProCurve Network Immunity  
Manager 1.0 unlimited-device  
license (J9062A)**

---

## Specifications

---

### Notes

For system requirements, please refer to the ProCurve Manager specifications list.

For system requirements, please refer to the ProCurve Manager specifications list.

For system requirements, please refer to the ProCurve Manager specifications list.

---

# ProCurve Network Immunity Manager 1.0

## Accessories

---

### **NEW ProCurve Manager Plus v2.2 50-device license (J9057A)**

PCM+ provides a starter license for advanced device management of up to 50 ProCurve devices, including integration with OpenView's Network Node Manager product.

### **System requirements**

For networks having 50 to 250 managed devices, ProCurve recommends the following:

#### **Minimum hardware**

2.0 GHz Intel Pentium 4 or equivalent processor  
2 GB RAM memory  
10 GB storage  
1000 MB NIC

for PCM+ as a standalone application, assuming a dedicated server

#### **Recommended hardware**

3.0 GHz Intel Pentium 4 or equivalent processor  
3 GB RAM memory  
40 GB storage  
1000 MB NIC

for PCM+ assuming a dedicated server, and including Identity Driven Manager, ProCurve Mobility Manager, and Network Immunity on the same server

#### **Recommended software**

Microsoft Windows 2000 Server, Advanced Server or Professional with SP4 or better  
Microsoft Windows 2003 Server  
Windows XP SP2  
Windows XP Professional SP2

For networks having 250 to 2,000 managed devices, ProCurve recommends the following:

#### **Minimum hardware**

3.0 GHz Intel Pentium 4 or equivalent processor  
3 GB RAM memory  
40 GB storage  
1000 MB NIC

for PCM+ as a standalone application,

assuming a dedicated server

#### **Recommended hardware**

Intel Xeon or equivalent processor  
4 GB RAM memory  
80 GB storage  
1000 MB NIC

for PCM+ assuming a dedicated server, and including Identity Driven Manager, ProCurve Mobility Manager, and Network Immunity on the same server

#### **Recommended software**

Microsoft Windows 2000 Server, Advanced Server or Professional with SP4 or better  
Microsoft Windows 2003 Server  
Windows XP SP2  
Windows XP Professional SP2

#### **Browsers**

Microsoft Internet Explorer version 5.0 or later

#### **Supported platforms**

HP OpenView Network Node Manager version 6.41 or 7.01 or 7.5

#### **Additional requirements**

NOTE: Network Immunity Manager when loaded on PCM+ 2.2 can sample up to 500 managed ports using sFlo

#### **Notes**

Unlimited license means that ProCurve does not impose a limit on the number of devices attached to the network as a condition of the license. Some degradation in performance may be expected the greater the number of devices attached to the network.

---

# ProCurve Network Immunity Manager 1.0

## **NEW ProCurve Manager Plus v2.2 upgrade +100-device license (J9058A)**

PCM+ 2.2 +100-device license gives the customer an additional 100-device license for companies with growing managed device counts.

## **System requirements**

For networks having 50 to 250 managed devices, ProCurve recommends the following:

### **Minimum hardware**

2.0 GHz Intel Pentium 4 or equivalent processor  
2 GB RAM memory  
10 GB storage  
1000 MB NIC

for PCM+ as a standalone application, assuming a dedicated server

### **Recommended hardware**

3.0 GHz Intel Pentium 4 or equivalent processor  
3 GB RAM memory  
40 GB storage  
1000 MB NIC

for PCM+ assuming a dedicated server, and including Identity Driven Manager, ProCurve Mobility Manager, and Network Immunity on the same server

### **Recommended software**

Microsoft Windows 2000 Server, Advanced Server or Professional with SP4 or better  
Microsoft Windows 2003 Server  
Windows XP SP2  
Windows XP Professional SP2

For networks having 250 to 2,000 managed devices, ProCurve recommends the following:

### **Minimum hardware**

3.0 GHz Intel Pentium 4 or equivalent processor  
3 GB RAM memory  
40 GB storage  
1000 MB NIC

for PCM+ as a standalone application,

assuming a dedicated server

### **Recommended hardware**

Intel Xeon or equivalent processor  
4 GB RAM memory  
80 GB storage  
1000 MB NIC

for PCM+ assuming a dedicated server, and including Identity Driven Manager, ProCurve Mobility Manager, and Network Immunity on the same server

### **Recommended software**

Microsoft Windows 2000 Server, Advanced Server or Professional with SP4 or better  
Microsoft Windows 2003 Server  
Windows XP SP2  
Windows XP Professional SP2

### **Browsers**

Microsoft Internet Explorer version 5.0 or later

### **Supported platforms**

HP OpenView Network Node Manager version 6.41 or 7.01 or 7.5

### **Additional requirements**

NOTE: Network Immunity Manager when loaded on PCM+ 2.2 can sample up to 500 ports using sFlow.

### **Notes**

Unlimited license means that ProCurve does not impose a limit on the number of devices attached to the network as a condition of the license. Some degradation in performance may be expected the greater the number of devices attached to the network.

**NEW ProCurve Manager Plus v2.2 unlimited-device license (J9059A)**

PCM+ 2.2 unlimited license provides a PCM+ license that does not limit the number of devices managed (It does NOT require the 50-device license).

**System requirements**

For networks having 50 to 250 managed devices, ProCurve recommends the following:

**Minimum hardware**

2.0 GHz Intel Pentium 4 or equivalent processor  
2 GB RAM memory  
10 GB storage  
1000 MB NIC

for PCM+ as a standalone application, assuming a dedicated server

**Recommended hardware**

3.0 GHz Intel Pentium 4 or equivalent processor  
3 GB RAM memory  
40 GB storage  
1000 MB NIC

for PCM+ assuming a dedicated server, and including Identity Driven Manager, ProCurve Mobility Manager, and Network Immunity on the same server

**Recommended software**

Microsoft Windows 2000 Server, Advanced Server or Professional with SP4 or better  
Microsoft Windows 2003 Server  
Windows XP SP2  
Windows XP Professional SP2

For networks having 250 to 2,000 managed devices, ProCurve recommends the following:

**Minimum hardware**

3.0 GHz Intel Pentium 4 or equivalent processor  
3 GB RAM memory  
40 GB storage  
1000 MB NIC

for PCM+ as a standalone application,

assuming a dedicated server

**Recommended hardware**

Intel Xeon or equivalent processor  
4 GB RAM memory  
80 GB storage  
1000 MB NIC

for PCM+ assuming a dedicated server, and including Identity Driven Manager, ProCurve Mobility Manager, and Network Immunity on the same server

**Recommended software**

Microsoft Windows 2000 Server, Advanced Server or Professional with SP4 or better  
Microsoft Windows 2003 Server  
Windows XP SP2  
Windows XP Professional SP2

**Browsers**

Microsoft Internet Explorer version 5.0 or later

**Supported platforms**

HP OpenView Network Node Manager version 6.41 or 7.01 or 7.5

**Additional requirements**

NOTE: Network Immunity Manager when loaded on PCM+ 2.2 can sample up to 500 managed ports using sFlo

**Notes**

NOTE: unlimited license means that ProCurve does not impose a limit on the number of devices attached to the network as a condition of the license. Some degradation in performance may be expected the greater the number of devices attached to the netw