

iNetSec



The Next Step in Network Visibility and Access Control



Internal Visibility and Security for Today's Network

iNetSec Smart Finder is a next-generation network access control appliance providing comprehensive security features for the internal network. It incorporates wired and wireless device discovery and network access control policies, application usage management and the industry's most advanced behavioral APT (Advanced Persistent Threat) malware detection. These features directly address the growing mobility and IoT trends and secure networks from intrusions and attacks.



Key Features

Device Visibility and Network Access Control

- Discovery and classification of wired and wireless devices connected to LAN and WLAN
- Up to 6,000 devices supported per sensor appliance (3,000 concurrently)
- Blocking of unauthorized devices via ARP spoofing technique
- Set-and-forget approval policies, captive portals and authorization workflow features
- Device whitelisting and blacklisting
- Independent access control policies for different IP segments

Application Visibility and Usage

- Layer 7 application visualization and network bandwidth usage
- Visibility of application usage per device
- Blocking policies for unauthorized applications
- Media-streaming, P2P file sharing, social networking, email and others

Behavioral APT (Advanced Persistent Threats) Malware Detection

- Detection of advanced persistent threat (APT) attacks via remote access Trojans (RAT)
- Automatic and immediate blocking of infected devices
- Behavioral analysis of internal network traffic, no signatures based, no sandboxing

Ease of Use

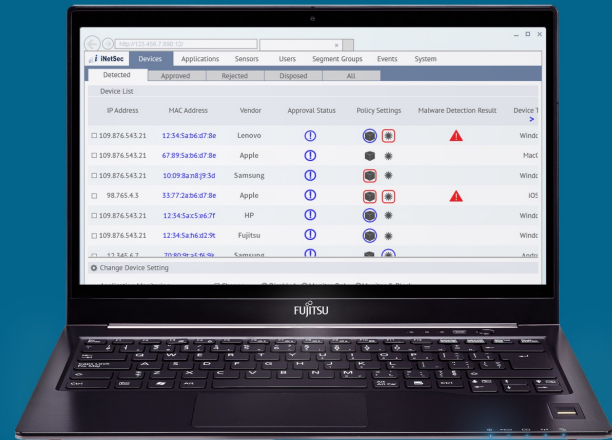
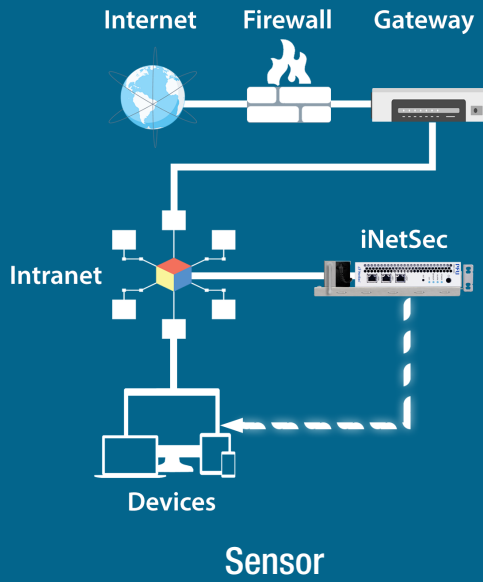
Centralized Policy Management

- Central graphic interface management supporting remote locations deployment
- Web-based interface management for ease of access
- Notifications via E-mail/SMTP for selected events

Fast Deployment

- ~2 hour deployment time
- No agent software required on devices
- Not in-line installation means no network downtime
- No network disruption
- Multiple VLAN management per single sensor to cover wider networks
- Two operation modes: Monitoring and Blocking to facilitate phased deployment





Sensor

Manager UI

Appliance Specifications	
Model Number	PD-APSS02A
LAN Ports	3 ports (for 1000base-T/100base-TX/10base-T)
Dimensions	42.5 (W) x 198 (D) x 180 (H) mm 1.7 (W) x 7.8 (D) x 7.1 (H) in.
Weight	1.3 kg / 2.9 lb (excluding accessories)
Power Supply	Supplied AC adapter
Input voltage (frequencies)	100-240 VAC (50/60 Hz)
Power consumption	28 W
Temperature of Installation Location	5° to 35° C / 41° to 95° F
Max Capacity per Appliance	6,000 devices (3,000 concurrent)
Number of Managed IP Segments	Up to 3 segments when port VLAN is used Up to 30 segments when tagged VLAN is used
Number of Segment Groups	Up to 5

Manager Interface System Requirements					
CPU	1 or more cores, 2 GHz or faster for less than 10,000 devices 2 or more cores, 2 GHz or faster for more than 10,000 devices				
Memory	1 GB or more for less than 10,000 devices 2 GB or more for more than 10,000 devices				
Free Disk Space	<table border="1"> <tr> <th>Static disk space</th> <th>Dynamic disk space</th> </tr> <tr> <td>Installation drive: 150 MB System drive: 2 GB</td> <td>Installation directory: 1 GB or more</td> </tr> </table>	Static disk space	Dynamic disk space	Installation drive: 150 MB System drive: 2 GB	Installation directory: 1 GB or more
Static disk space	Dynamic disk space				
Installation drive: 150 MB System drive: 2 GB	Installation directory: 1 GB or more				
OS Support	Windows Server 2008 SP2 32 bit 2008 R2 w/ SP1 64 bit 2012 w/ No SP 2012 R2 w/ No SP				
Required Software	Internet Information Services (OS bundled version) with ASP.NET .NET Framework 4.5.1 or higher .NET Framework 3.5 or .NET Framework 2.0 (For Windows Server 2008) Microsoft SQL Server 2008 R2 Express Edition SP2 (Bundled) Visual C++ Redistributable Packages for Visual Studio 2013 (Bundled)				

Manager Interface Specifications	
Total MAC Address	50,000
Maximum Manageable Number of Sensors	500
Maximum Manageable Number of Segments	1,000
Maximum Manageable Number of Segments per Group	75

Learn More at [iNetSec.com](http://inetsec.com)

PFU Ltd. is a wholly-owned subsidiary of Fujitsu that designs, sells and maintains computer hardware, networking and security systems.