

## V8100 Network Monitoring Appliance

### Benefits

A crucial component for enterprises and service providers looking to achieve real time network situational awareness

Provides early detection of cyber attacks using real time traffic analysis without reliance on external databases or feeds

Detects single and double fast flux botnet activities before day zero

Accurate alerting of suspected botnet command and control communications

Detects botnets that use DNS servers outside your network

Enables rapid response to detected threats, based on real time network information

### Key Features

Provides a scalable and dedicated hardware platform to help ensure the network is always secure by reporting suspicious behavior instantly

Processes all incoming traffic at 10 Gigabit line-rate speed

Supports in-line and network-tap deployment with port mirroring capabilities

Supports a web GUI to simplify control and management

Supports user authentication and access control levels for data privacy protection

### Overview

For enterprises and service providers, the V8100 stand-alone appliance is ideal for cloud high bandwidth monitoring and analysis. Its intelligent technology continuously monitors Domain Name Service (DNS) network traffic and helps suppress various botnet cyber attacks, such as denial of service or spam, by performing early detecting and reporting of suspicious network behavior. This scalable solution supports multiple 10 Gigabit Ethernet ports, has built-in storage, and is securely managed remotely without any additional client software.

#### Why traditional defense mechanisms don't work.

**Timing.** One of the typical approaches to dealing with botnets is to inspect Internet traffic in a network and identify communications occurring with a database of known or suspected botnet command and control hosts (e.g. blacklisting). Typically, an organization will receive periodic database updates from its central processing division (or third-party data feeds) that have taken the time to analyze and announce the latest cyber threat. These list-classification methods are limited by the accuracy and timeliness of the list, and may introduce an unnecessary time lag in implementing protective measures. Furthermore, sophisticated botnets, utilizing fast flux techniques to obfuscate their location are not amenable to fixed list identification approaches.

**Technique.** Another standard approach to detecting botnet activity is to examine network traffic for specific activities coming out of suspected infected PCs. While this approach may catch the botnet as it is involved in performing an attack, it is deficient in detecting botnets as they are still forming.



# V8100

## Network Monitoring Appliance

**Location.** Some DNS servers have software features to help detect suspected botnet traffic passing through them. Even if the DNS servers in your network have these features, botnets may simply be bypassing them and using other DNS servers outside your network.

**Response.** If you are relying on traditional techniques, by the time botnet activity is detected on your network, your ability to mitigate infection is greatly reduced, if not already too late. While you may be able to contain the attack or prevent its spread beyond the local network/segment, the local resources are still consumed by the attack.

**The V8100 network monitoring solution provides an innovative, scalable approach to network security.**

The best defense against botnets and other malicious software is rapid, early detection that enables a swift response. The V8100 network monitoring appliance gives you the ability to do this in a powerful, scalable way that the traditional list-classification methods can't match. Take action to secure your network by using the V8100 network monitoring solution. Its main features and benefits include:

- **On-the-fly botnet activity detection and alerting** — inspects traffic in real-time at 10 Gigabit Ethernet line-rate on multiple 10Gbps links at once. No waiting for database or third-party updates. Your rapid response can begin before day zero of the threat, and can include sending out live alerts in real-time.
- **Detects botnets while they are still forming** — use your valuable resources to “sniff” out the specific characteristics of traffic coming from suspected servers. This ensures only those local PCs that may be potential botnet members are flagged and analyzed before they become active.
- **Detects botnets that use DNS resources outside your network** — captures all DNS traffic, enabling detection of botnets that bypass DNS servers on your network.
- **Contains botnet attacks that use zero-day exploits** — the real-time detection capabilities can provide on-the-fly updates to blacklists or ACLs helping to limit botnet recruitment that uses zero-day exploits.

## Technical Specifications

### NETWORK INTERFACE

12 10GBASE-SR or 10GBASE-LR SFP+ optical ports  
12 10/100/1000BASE-T ports

### MANAGEMENT INTERFACE

10/100/1000BASE-T RJ-45 port for secure remote control and management

### STORAGE

2 500GB hard drives for storing SQL database files

### COOLING

Two hot-swappable cooling units  
Temperature controlled fans with smart fan control

### POWER REQUIREMENTS

Maximum power consumption: 600W  
Input voltage: dual redundant -48V DC inputs  
Maximum input current: 18A

### COMPLIANCE

PICMG MTCA.0 R1.0 for MicroTCA  
IEEE 802.3ae 2002 10GBASE LAN  
RoHS Directive 2002/95EC  
FCC 47 CFR Part15 Class A (USA)  
ICES-003 Class A (Canada)  
EN 55022 Class B (EU)  
UL/EN 60950-1  
NEBS Level 1

### DIMENSIONS

26.3cm (H) x 48.2cm (W) x 25.7cm (D)  
Standard 19” rack-mountable

### ENVIRONMENTAL

Operating Temperature: 4° C to 45° C  
Storage Temperature: -40° C to 85° C

#### FOR MORE INFORMATION ON OUR PRODUCTS:

www.advancedio.com  
contactus@advancedio.com  
595 Howe Street, Suite 502  
Vancouver, BC V6C 2T5  
Canada

Phone 604.331.1600  
Fax 604.331.1800  
Toll Free 1.877.331.7755



**ADVANCED**io