DATA SHEET

ThreatARMOR™

Key Features

- Reduces attack surface by eliminating known-bad traffic
- Stops traffic from unwanted countries
- Quickly identifies compromised internal systems
- Stops connections, both inbound and outbound, involving known malware, botnet and phishing sites
- No false positives – clear proof of criminal behavior for all blocked sites
- Always-on cloud update service from Ixia's ATI Research Center
- Dual redundant power supplies and integrated bypass for maximum reliability

Your New Front Line of Defence

With the evolution of Internet threat complexity and intensity, comes the rapidly increasing range of security technologies needed to secure the network. New layers have been added to the perimeter to deal with emerging threats, fortifying the existing firewalls and IPS/IDS systems with threat detection, malware inspection, content security, DLP, DDoS mitigation, and more - at increasing expense. Constant probes and automated attacks flood SIEMs and overwhelm security teams with false negatives and positives that must be tracked down.

ThreatARMOR™ establishes a new front line of defence in your network, removing threats from your network and improving your security ROI by eliminating unwanted traffic before it hits your existing security infrastructure. A single ThreatARMOR security appliance can be deployed on both the inside and outside of your perimeter, identifying infected internal systems and blocking communication with Botnet controllers while reducing inbound firewall load from known bad sites and countries you don't do business with. Even encrypted connections from those sites are automatically banned.

ThreatARMOR doesn't use signatures and there are no false positives. Any blocked sites are supported with clear on-screen proof of malicious activity such as malware distribution or phishing, including date of most recent confirmation and even screen shots. The site list is kept constantly up to date by Ixia's Application and Threat Intelligence (ATI) Research Center that individually validates every site and provides a cloud-based update every five minutes.

Since network availability is critical to your business, ThreatARMOR is built for resilient and failsafe operation. Features such as dual-redundant power supplies and Ethernet interfaces with built-in bypass modes ensure network availability on both the 1GbE copper and 10GbE fiber interfaces.The ThreatARMOR security appliance:

- Reduces attack surface by eliminating traffic from unwanted geographies and known bad sites
- Blocks outbound Botnet communication from infected internal systems
- Improves the ROI and effectiveness of your security architecture

Key Features

- 1U Security Appliance
- In-band or passive deployment
- Full line rate across all ports with blocking enabled
- Reporting, blocking, or fail-safe bypass operation
- Always-on ATI cloud security service

Management

- Serial console interface
- Front-panel LCD display and push-button controls
- Future option for dual management Ethernet interfaces

Physical Specifications **Size and Weight**

- 1U high 19” chassis
- Dimensions: 16.9W x 16.7L x 1.7H (inches)
- Weight: 22.0lb (10 kg)

Power for ThreatARMOR 1G Appliance (AC)

- Dual AC power supplies
- Operating input voltage: 100 to 200 VAC
- Idle current: 0.5A @ 120VAC, 0.25A @ 240VAC
- Max. operating input current: 1.3A @ 120 VAC
- Heat/power dissipation for module at 100% traffic load: maximum 156 W / 532 BTU/hour

Operating Specifications

Operational Environment

Temperature

- Operating: 5°C to 40°C
- Storage: -20°C to 75°C

Humidity

- Operating: 10% to 85%, (non-condensing)