IXIA ThreatARMOR

The amount and sophistication of cyber-attacks is increasing exponentially and many enterprises are finding their security systems are wilting under the pressure. Malware, ransomware, botnets, zero-day attacks - they're all on the up, and overworked support staff trying to cope with the daily barrage of alerts are taking too long to respond and investigate.

ThreatARMOR from network performance specialist Ixia takes the load off their shoulders by the simple expedient of blocking malware beyond the network perimeter. Instead of analysing each attack, ThreatARMOR checks their IP launch source address against a constantly updated list and blocks them, if they are on it.

The key advantage is that it doesn't use signature-based analysis, so there are no false positives. By greatly reducing the amount of incoming traffic and alerts, ThreatARMOR also improves firewall performance and IT support productivity.

The IP address source list is maintained by Ixia's Application and Threat Intelligence (ATI) Research Center, which has over a decade of experience. It gathers intelligence on threats including malware, botnets, hijacked IP address ranges and more and makes it available to ThreatARMOR as a constantly evolving database, with updates occurring every five minutes.

ThreatARMOR is an appliance-based solution and we reviewed the 1G model, which has four Gigabit data ports and a dedicated management port. Ixia offers other models with 10-Gigabit ports and one thing they all have in common is a stunningly simply deployment.

We logged into the appliance's web portal and were presented with a well-designed and intuitive interface. The home page provides an overview, showing a global map with blocked countries highlighted in red and a scorecard below of total and blocked connections and traffic.

The Dashboard shows a smaller map, plus a list of the last four blocked countries and the detected threats alongside, while below is a summary of the top and bottom allowed countries. To deploy the appliance in our live environment, we simply connected our Internet feed to the first Gigabit data port and the second to our firewall's WAN port.

And that's all we had to do, as from this moment onwards the appliance started transparently checking and blocking traffic with the maps and counters rapidly (and rather alarmingly) filling up with data on detected threats. The appliances support passive monitoring using network taps and can have data ports placed in-line behind the firewall, where they can also monitor internal traffic.

The appliance starts in a passive reporting mode and, when you're happy with its findings, you can switch it to full blocking mode with two clicks. Along with dual redundant PSUs, the appliance's data ports also have hardware bypasses, so a system failure won't interrupt Internet access.

The Dashboard is very informative and selecting a blocked country entry, or one of the last blocked IP addresses, takes you to the cloud rap sheet page. This leaves you under no illusions that ThreatARMOR knows what it's doing, as the rap sheet provides undeniable evidence about why an IP address was blocked.

Different icons are used to denote malware, exploits, phishing sites, plus hijacked IP addresses. Select an entry in the list and the rap sheet window shows details such as the threat URL, credentials used by a brute force attack, file checksums, a breakdown of attempted Trojan activities and, where appropriate, a screenshot of the offending web site.

Enterprises with overwhelmed security services should seriously consider augmenting them with ThreatARMOR, as it lightens the load significantly by stopping most threats at the network border. Ixia's cloud-based ATI feed keeps it constantly updated, the rap sheet feature provides detailed reporting, and we found that the appliance can be deployed and protecting the network in a matter of minutes. CS

Product: ThreatARMOR
Supplier: Ixia
Web site: www.ixacom.com
Phone: +44 (0)1628 408 750
Price: ThreatArmor 1G, from $19,995