# Reduce Your Network's Attack Surface

Ixia's ThreatARMOR Frees Up Security Resources and Personnel

## The Threat Landscape

When you're dealing with network security, one of the primary measurements of risk is the size of your "attack surface." The attack surface is every way that an attacker can either enter or try to sneak data out of your network.

One way to think about the size of your attack surface is to look at the size of your internal network times the size of the Internet. Everywhere there is a "touch point" between any host on the Internet and any host on your internal network, there is a possible path for unwanted intrusion into your network or for data to leak out.

There was a time in network security history when a firewall was all you needed to be "secure." But as attacks have become more persistent and sophisticated, and new regulatory requirements have expanded, security vendors have responded with new, very impressive technologies and products. The evolution of security over the last several years evolved in response to new and emerging threats.

Currently, we deploy additional solutions like DLP, sandboxing, anti-virus software, deep packet content inspection, and more to ensure network security. These extended security solutions are necessary, and designed to tackle specific threats that your network faces. But with these new solutions comes a networking overhead. The processing requirements, the storage requirements, the number of security alerts, and the requirements on your security team have all gone way up.

With this increase in resource consumption comes an increase in cost. A new goal of security teams is minimizing the costs associated with increased security complexity. Effectively and completely protecting your network should be cost-effective as well.

Another way of thinking about reducing the load on your security solution is shrinking the size of your network's Internet exposure—in other words, reducing your network "attack surface."

ThreatARMOR™

Your New Front Line of Defense.

## What is an Attack Surface?

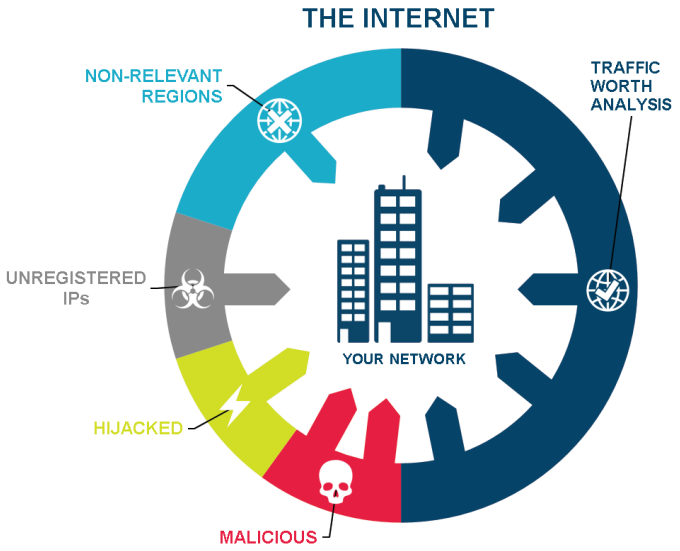
To do this, first we need to think about the make-up of today's Internet. Most hosts on the Internet are "good" or "safe." They are just people and companies going on about their business.

However, many sites out there don't belong on your network. For instance, there are sites that:

- Distribute malware
- Conduct phishing attacks
- Serve as botnet command and control (C&C) locations
- Are hijacked for nefarious purposes

There are also unallocated IP addresses that don't belong to anyone and shouldn't have access to your network. And there may very well be regions or countries in the world where you just don't do business (and therefore traffic from these hosts have no business on your network).

**When you're dealing with network security, one of the primary measurements of risk is the size of your "attack surface."**

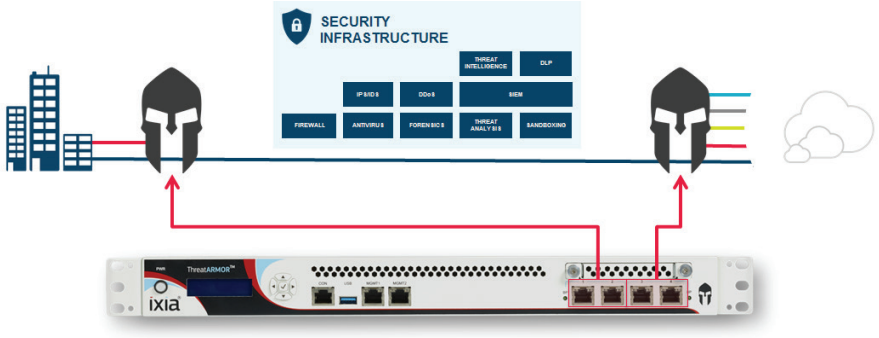



All the categories shown in the left-hand side aren't really worth firewall and IPS resources. They're certainly not worth creating a flood of security and event management (SIEM) alerts—knowing they're "bad," you don't really need IT security teams investigating them. What you need is a way to filter out these known issues, and save security resources for inspecting the truly "unknown" traffic. This results in fewer attackers and fewer SIEM alerts. The result is a smaller attack surface, and a security infrastructure that focuses on what's important, not what is already known.

Ixia used this insight to develop a new product: ThreatARMOR.

# ThreatARMOR: Your New First Line of Defense

When deployed in your security infrastructure, ThreatARMOR lowers your attack surface by blocking unwanted traffic from the Internet, and it blocks outbound connections to malicious sites from inside your network.




**What you need is a way to filter out these known issues, and save security resources for inspecting the truly "unknown" traffic.**

For example, if someone was to click on a phishing email, or an infected host tries to connect to an external botnet controller, ThreatARMOR will block those outbound connections.

So one question you might be asking yourself is: "Doesn't my firewall already do that kind of stuff?" It turns out that next-generation firewalls are very good at deep packet inspection (DPI). They're also very good at user-based policies, content inspection, and URL filtering. And some even are even very good at sandboxing and anti-malware.

But they're not very good at blocking really large numbers of IP addresses.

Why would you want to do that? The answer: lowering your attack surface. Here are some statistics:

- 18% of DDoS attacks come from China
- Russia, Ukraine, Pakistan, China, and Turkey are in the top ten botnet command and control (C&C) countries
- China, Brazil, Russia and India together account for 26% of web application attacks

The typical organization receives almost 17,000 malware alerts in a week and spends $1.27 million annually tracking down false positives. You may want to block countries where you don't do business because you know that a very large percentage of DDoS attacks or malware or phishing sites originate in some of these countries. So by simply blocking traffic from these countries you can reduce your attack surface and reduce your overall risk.

By reducing your attack surface, you're making your network safer by letting your security devices focus on traffic that is more likely to be legitimate and is therefore more worth inspecting. Another example is blocking phishing sites. This requires blocking a many thousands of hosts or IP addresses.

A firewall will usually run out of capacity somewhere around 10,000 rule sets at most (about 30,000 objects). So it's not able to cope with blocking the very large list of IP addresses required to block the IP ranges for multiple individual countries, or to block all of the malicious IP addresses that are out there.

## Operation

Now the key to the success of ThreatARMOR is the security research and resulting threat intelligence that feeds the device and keeps it continuously up to date!

**Ixia's Application and Threat Intelligence (ATI) program has been doing deep security research for over ten years.**

Ixia's Application and Threat Intelligence (ATI) program has been doing deep security research for over ten years. In fact, major security equipment manufacturers use Ixia's ATI program to test their own security devices. Major service providers also use it to test the security of their networks.

One of the ways we express this threat intelligence is through a "Rap Sheet." We provide a Rap Sheet for each and every blocked IP address to clearly demonstrate and document the malicious activity executed at that host. It provides clear proof of why that site is blocked. It will show you:

- What malicious activity is happening at that site
- What date it was last validated
- Screen shots of the malware downloader or a phishing site or other evidence.

You can override the blocking action with a whitelist entry if you really need to access that site.

ThreatARMOR leverages our years of threat intelligence and applies it directly to your network, to immediately to reduce your attack surface. It keeps ThreatARMOR apprised of the most current threat information, every five minutes.

ThreatARMOR is different from other traditional inline security products in that it performs strictly IP-based security. It only focuses on IP- or packet-based blocking. It is built to maintain line rate performance no matter how many IP addresses or IP address ranges are entered. It could actually filter on every IP address on the Internet, with a simple "Yes / No" flag beside that IP to determine whether or not it gets blocked.

And of course, because this is an inline device, it is built for maximum up-time and reliability. It's designed with built-in redundant, hot-swappable power supplies. It has a field-replaceable solid state drive (SSD). With its integrated bypass NICs, ThreatARMOR continues to let traffic flow uninterrupted even in the event of a complete power failure.

## Set Up

In addition to being extremely reliable, ThreatARMOR is extremely easy to set-up. We've designed it so the entire rack, stack, and configuration process takes only 30 minutes:

1. Take it out of the box, cable it up.
2. Select either Report Only Mode, or Blocking Mode.
3. Then walk away. The device automatically starts getting its regular threat intelligence feeds.

ixia

Blocking Mode automatically blocks all "flagged" sites. Because the ATI program provides evidence of the criminal behavior in the Rap Sheet, there are no false positives. Unlike many other behavioral security devices, no tuning is required.

Geographic-based blocking is optional. However, you can quickly select individual countries to block or disallow from connecting into your network. Once those countries are specified, inbound traffic from them is automatically stopped from entering the network (although you can still connect from inside the network to locations in those countries).

Once you're done, there's nothing else you need to do. The ThreatARMOR device queries the cloud for an update every 5 minutes.

## Conclusion

ThreatARMOR is "Your New Front Line of Defense." It is the fastest and easiest way to block lots of unwanted traffic from entering or leaving your network—reducing your overall attack surface. You can get much more out of your security team and your security tools because ThreatARMOR reduces the number of incidents they need to investigate by blocking known problem IP addresses and reducing your attack surface. It is a great way to quickly operationalize Ixia's leading ATI threat intelligence in your network.

Contact Ixia for a live demonstration of ThreatARMOR in your network, so you can quickly see what it can do for you and your security team.

**When deployed in your security infrastructure, ThreatARMOR lowers your attack surface by blocking unwanted traffic from the Internet.**

**Ixia Worldwide Headquarters**
26601 Agoura Rd.
Calabasas, CA 91302

**(Toll Free North America)**
1.877.367.4942

**(Outside North America)**
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

**Ixia European Headquarters**
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750
(Fax) +44 1628 639916

**Ixia Asia Pacific Headquarters**
101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
Fax +65.6332.0127

915-6786-01 Rev. A, October 2015