Application and Threat Intelligence (ATI)

Ixia Body BOLD

Ixia Body

Figure 1 – Sample Figure

Key Features

- Global Application and Threat Intelligence Research Center
- Over a decade of testing the application performance and security resilience of the world's largest service providers and manufacturers
- Round-the-clock network of threat intelligence research and validation
- Enhances the value of Ixia's Test, Visibility, and Security solutions
- Always-on cloud-based intelligence provides high-confidence threat feeds to protect your network
- Intelligence to simulate real-world applications, exploits, malware, and evasion techniques, seen on the internet today
- Evergreen application signature ensure timely tracking of application version updates

Better Data for Better Decisions

The ATI team leverages more than 10 years of experience in researching application performance and security technologies. Using advanced surveillance techniques and methodologies, it identifies, captures, and rapidly delivers the application and threat intelligence you need. Ixia's products, powered by ATI, reduce your attack surface, bring application-level visibility and context to your monitoring tools, and validate network devices with real-world threats and application conditions.

Ixia understands the unique security challenges faced by modern enterprises, network security manufacturers and service providers. The ATI program enables them to validate, secure, and improve visibility into their critical projects.

Ixia's team of dedicated application and security researchers provides everything you need for thorough measurement of the performance, security, and stability of IT infrastructures. This includes access to all application protocols, security attacks, product enhancements, and full service and support. Ixia enables granular application-level visibility and control, geolocation, and threat site blocking. This comprehensive program keeps your Ixia hardware and software continually up-to-date.

Ixia's Application and Threat Intelligence (ATI) program provides a comprehensive service and support resource for optimizing and hardening the resiliency of IT infrastructures, including:

- Over a decade of experience testing the threat detection and blocking capabilities of the world's largest service providers and equipment manufacturers
- Real-time cloud threat intelligence that enables Ixia's ThreatARMOR™ to reduce your attack surface and provide continuous protection. ThreatARMOR eliminates traffic originating from known malicious IP addresses (malware distribution, phishing sites, botnet C&C sites, SPAM distribution, BOGONs hijacked domains and unassigned IPs)
- Application insight enabling Ixia's network visibility products such as the ATI Processor to provide complete network visibility extending beyond layer 4 into granular application behaviors
- Intelligence in simulating realistic conditions and relevant attacks consolidated into a large database of exploits, DoS, DDoS, phishing, live malware and applications
- Simulation of 100+ evasion techniques
- Information to recreate real-world network traffic using more than 300+ applications
- The Evergreen feed to provide constant updates for applications that are critical in validating lawful intercept, data loss prevention, and deep packet inspection devices
- Always-on global IP geolocation database
- Application- and geography-based application filtering
- Rich contextual NetFlow / IPFIX generation

Benefits of using Ixia's Application and Threat Intelligence

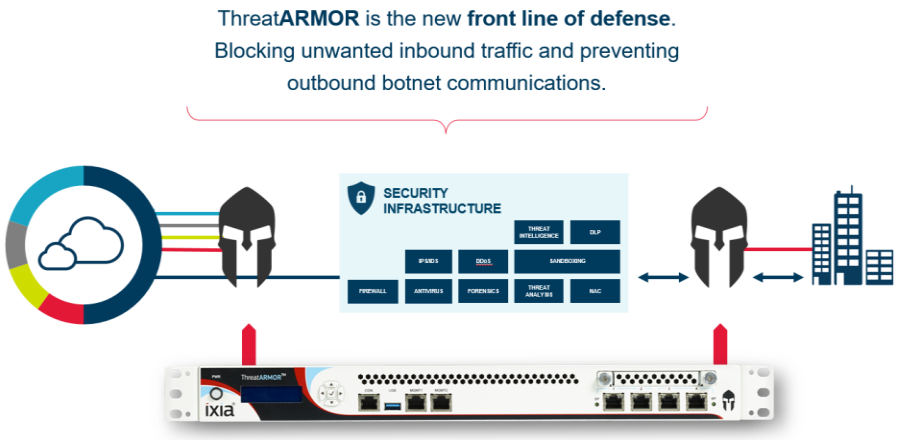
Ixia's ATI service fuels multiple Ixia products and solutions and enhances their value to:

- Reduce your attack surface by acting as your new first line of defense (ThreatARMOR™)
- Deliver real-time application data to monitoring tools (ATI Processor™)
- Provide most realistic simulation conditions of application and attack traffic (BreakingPoint™, IxLoad™ and IxNetwork™)

Ixia empowers ThreatARMOR with the intelligence required to protect your network and users by reducing the attack surface

As the complexity and intensity of Internet threats has evolved, the range of security technologies needed to secure the network has increased rapidly. New layers have been added to the perimeter to deal with these emerging threats, fortifying the existing firewalls and IPS/IDS systems with threat detection, malware inspection, content security, DLP, DDoS mitigation, and more – at great expense.

ThreatARMOR™ establishes a new front line of defense 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 load on your firewall and SIEM 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 5 minutes.

Arms your visibility infrastructure to provide better data for better decisions when using ATI Processor

The Application and Threat Intelligence (ATI) Processor delivers real-time filtered application data to monitoring tools, empowering you to make better decisions with better data. It provides rich data on behavior and location of users and applications, in any format needed – raw packets, application-filtered packets, or metadata. This allows IT teams to identify unknown network applications, mitigate network security threats from suspicious applications and locations, and spot trends in application usage to predict and forestall congestion.

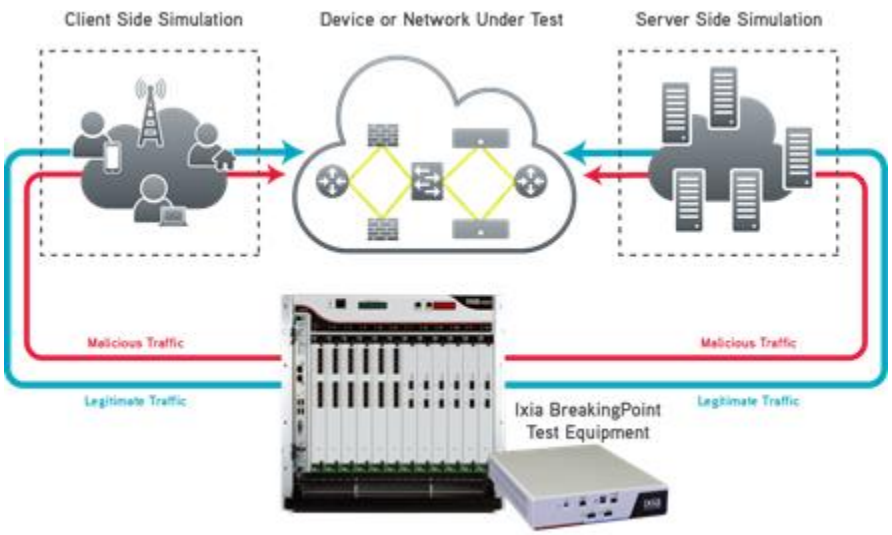
Using the ATI application feed, this product solves one of the biggest challenges facing network administrators – complete network visibility that extends past layer 4 information. Many applications today run over HTTP within your network or cloud infrastructure, and thus can be obscured. The ATI Processor provides expanded visibility that gives you deep knowledge of your network, including application bandwidth, handset and browser type, and geo-location of application traffic. The ATI Processor has patent pending ability to dynamically detect new applications without signatures. It also provides mobile device identifier and browser information.

Enables Ixia BreakingPoint to deliver most realistic simulations when validating network solution performance and security

Security threats are constantly evolving, with new vulnerabilities discovered each day. Attackers continue to evolve their methods and new attacks seek to find yet-undiscovered holes in your network defense. Your simulation conditions must reflect the latest security threats so that you can ensure your equipment will perform reliably and protect your infrastructure from the most advanced and malicious traffic. Our team of security experts does the research for you by identifying and generating security attacks that meet your needs.

With a current ATI subscription, you are assured of the most realistic simulation conditions possible with access to a large repository of 300+ application protocols and 36,000+ security attacks (exploits, malware, DoS and DDoS) while benefiting from the industry's most comprehensive Microsoft® Tuesday coverage.

In today's rapidly evolving networks, popular application protocols change on a daily basis. Content-aware network and security devices are at a severe disadvantage if they are not tested using the most current versions of the most popular application protocols. The ATI team addresses this need through the ATI Evergreen program by providing ever-current versions of popular Web and network applications for validating deep packet inspection (DPI), Lawful Intercept (LI), and Data Loss Prevention (DLP) products.



Every BreakingPoint system is designed for speed, realism, and ease of use. This allows you to recreate the good, the bad, and the ugly of any network. A key aspect of the design is the Application and Threat Intelligence (ATI) Program, a responsive and all-inclusive service and support program.