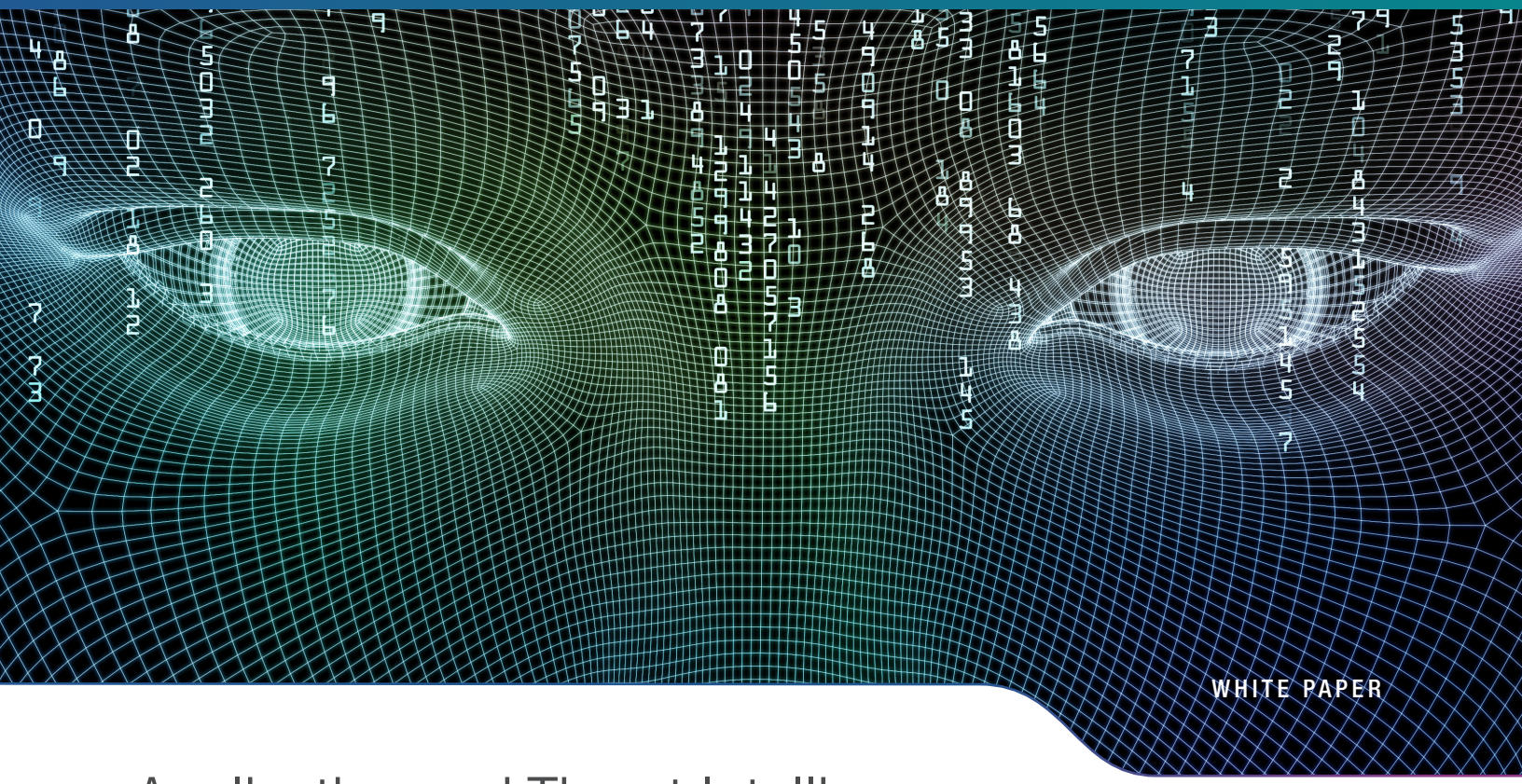


WHITE PAPER

Application and Threat Intelligence Research Center

Complexity Creates Vulnerability

Modern applications are complex. As an enterprise, you rely on your development teams to have a depth of knowledge across a wide range of technology areas, including application and threat vulnerabilities. Tracking the latest message board alerts—from operating systems, to software development environments, to threat and connectivity attack methods—requires multiple focused teams. You have one team and it is under constant pressure to fix bugs faster to meet delivery schedules. And you have a failsafe way to make sure apps rushed to completion do not introduce vulnerabilities…right?

Vulnerabilities come from many places. For instance, one operating system kernel or driver update can have ripple effects to related software elements. Did that update just create the possibility of a buffer overflow that hackers can exploit? One unpatched security vulnerability can create a pathway directly into your application database. Did you just open the door to your customer data? You need the ability to validate the entire security ecosystem to protect against breaches resulting from changes like these.

Vulnerabilites come from many places. The challenge is to find them before hackers do.

KEYSIGHT TECHNOLOGIES

Many security providers offer threat intelligence—the tracking of attacker profiles, methods, and attack vectors. Some vendors offer application intelligence—the monitoring of applications in action. Both are critical to your operation and more intertwined than they may appear on the surface.

Keysight's Application and Threat Intelligence Research Center

Keysight knows test, how applications should perform, and cybersecurity. We have deep knowledge about the challenges of maintaining a network solution that facilitates high-speed data moving through a network, along with the security and performance issues that inevitably arise. That is why, in 2005, we created the Application and Threat Intelligence (ATI) Research Center, staffed by an elite group of top application and security researchers from around the globe. Our expertise spans software development, reverse engineering, vulnerability assessment and remediation, malware investigation, and intelligence gathering.

The ATI Research Center combines proficiency in cybersecurity threats and application protocol behavior. This unique combination takes network security to a new level, looking at it the same way as a cybercriminal, from every direction. We use this application and threat intelligence across our test, visibility, and security solutions to:

- Create realistic application attacks – from protocols, loading, and threats
- Block malicious inbound and outbound communications
- Collect ongoing intelligence on new threats
- Identify unknown applications
- Detect traffic geolocation

These capabilities combine to go far beyond simple signature recognition. They proactively defend against attack patterns and reduce your attack surface by finding product vulnerabilities before and after you launch to the market. The ATI Research Center leverages the knowledge of hundreds of Keysight engineers and decades of knowledge across test, protocols, networks, and security.

Keysight's ATI Research Center combines proficiency in cybersecurity threats and applicaiton protocol behavior.

ATI Global Impact

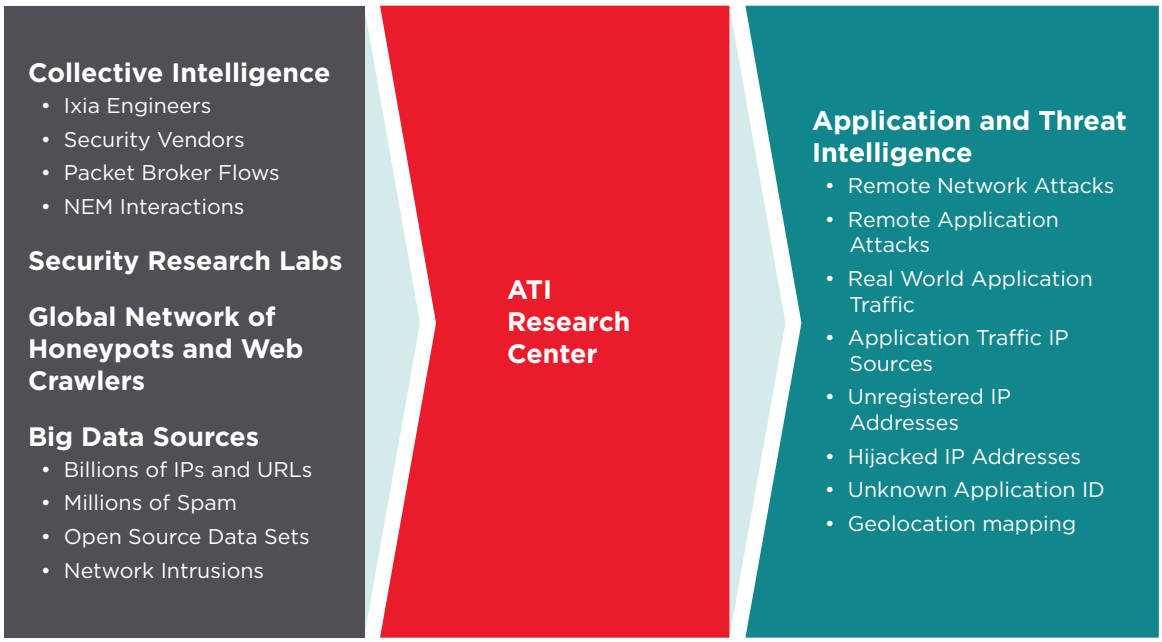
The ATI Research Center intelligence supports a wide range of Ixia products including AppStack capabilities on our network packet brokers (NPBs), ThreatARMOR, BreakingPoint, IxLoad, IxChariot, and IxNetwork. ATI data sources are used in the test products we provide to every major security vendor, network equipment manufacturer (NEM), and service provider in the industry. Top-ranked security vendors all leverage the outputs of the ATI research to verify their own products and applications run strong.

We augment the knowledge of how applications perform in service provider and enterprise networks with threat intelligence data gathered from our network security products.

The combination gives the ATI Research Center a powerful understanding of how hackers exploit vulnerabilities missed before product launch or once they are in a live network. We partner with leading developers, monitor alerts across every layer of the Open Systems Interconnection (OSI) stack, and actively research threats around the globe to keep our application and threat intelligence feeds up to date with the latest data. Our daily malware update service enables nearer-real-time malware threat intelligence that helps differentiate the most agile security systems from the rest.

The ATI Research Center operates a worldwide, distributed network of honeypots and web crawlers to actively identify known and unknown malware, attack vectors, and application exposures.

Top-ranked security vendors leverage the outputs of the ATI research to verify that their own products and application run strong.



In addition, the team regularly finds and discloses zero-day vulnerabilities. We correlate this data with real world events, validate reported findings, and then push actionable intelligence to customers with continuous updates.

The ATI data feeds produce actionable security intelligence on application vulnerabilities as well as threats across networks, endpoints, mobile devices, virtual systems, web, and email. The ATI feeds automate the gathering and analysis of a wide range of threat intelligence data from sources including:

- Billions of IPs and URLs
- Millions of spam
- Millions of malware attacks
- Open source data sets
- Millions of network intrusions

The majority of NEMs and service providers validate their hardware and systems by leveraging our application intelligence, which includes:

- Programming methods of communication protocols, common practices to introduce weaknesses, and loading profiles of the widest range of traffic types
- Deconstructing application protocols and packaging them for use in real-world user simulation testing
- Using a deep knowledge of protocols to fuzz applications and look for specific types of weaknesses as well as find unknown, zero-day vulnerabilities

The unique combination of application plus threat intelligence ensures resilient networks, and better performing and secure applications.

The uniqe combination fo application plus threat intelligence ensures relilient networks.

More Resilient Security and Better Performance With ATI

Threat intelligence providers and security vendors typically focus on the symptom, not the disease. They address how to identify and block the high-level threat without addressing the door that the threat exploited to originally enter, typically from a vulnerability in the network or application. Stronger applications lead to better performance and just as importantly, more resilient security.

You need to know if the application or service you are providing is stable and secure. You need expertise to fully assess your application's stability as well as its security. Testing massive scale at high speeds across multiple data types requires breadth of application expertise. Knowing the latest threat attacker exploits, identities, and methods requires a depth of threat intelligence that only comes from years of experience and millions of man hours.

The combination of application plus threat intelligence expertise can mean the difference between delivering a product that significantly grows your market share versus one that fails.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES