WHITE PAPER

Know Your Adversary: Strengthen Security with Application and Threat Intelligence

Network security is essential, but it is not easy. Attackers are tenacious, opportunistic, and always looking for vulnerable misconfigurations to exploit. Staying a step ahead is vitally important, but it's easy to fall behind.

Many security providers offer "threat intelligence" to overworked security teams — tracking attacker profiles, methods, and vectors. But threat intelligence is only half of the equation. To stay secure, organizations also need to monitor known vulnerabilities and misconfigurations within their applications. This "application intelligence" is just as critical as threat intelligence, yet often overlooked.

In this white paper, you will discover how application and threat intelligence work together to help security operations (SecOps) and development teams improve resiliency and minimize risk. Using Keysight's Application and Threat Intelligence (ATI) Research Center as a real-world example, you will learn what types of information these teams gather, how it's applied to different tools, and how it fortifies your security posture.

Security teams work tirelessly to protect their networks, but that task is not getting any easier. Attack surfaces are growing, and a single misconfiguration can be the difference between a safe network and a compromised one. When the margins are this thin, application and threat intelligence can make all the difference.

KEYSIGHT TECHNOLOGIES

What You Don't Know Can Hurt You

Despite rapid technological advancement, modern applications are not getting any simpler. Enterprises count on SecOps and development teams to understand the latest application and threat vulnerabilities, but that is asking a lot. Operating systems, software development environments, and new attack methods all require constant attention — and multiple teams often find themselves continuously scouring message boards for new threats.

However, vulnerabilities come from many places. For instance, one operating system kernel or driver update can have ripple effects on related software elements. A single unpatched security vulnerability can create a pathway directly into your application database.

Did that update create the possibility of a buffer overflow that hackers can exploit? Did I just open the door to your customer data? These are just a couple of the questions SecOps and development teams ask themselves every day.

You need to validate your entire security ecosystem to prevent attackers from capitalizing on your system's weaknesses. But there is only so much time — and budget — to go around. Development teams are under pressure to fix bugs and meet delivery schedules, while SecOps is working to secure an ever-expanding attack surface. Something has to give, and many teams struggle to keep up.

Ignoring risk is a surefire way to open your network up to attack. That's why so many organizations turn to professionally curated threat intelligence feeds to take control of their security posture. With crucial insights like attack signatures, malicious IP addresses, and emerging threats, SecOps teams can stay a step ahead of cybercriminals.

However, threat intelligence is not enough on its own. Staying ahead of the latest attacks is a good start, but SecOps and development teams need to be aware of risks within their applications as well. "Application intelligence" like this isn't as commonplace as threat intelligence, but it's no less important. While new exploits and attack vectors get the most attention from the media, nearly half of all breaches stem from human error, system glitches, and misconfigurations.[1]

Both application and threat intelligence are paramount to staying secure. Dual intelligence streams can help you efficiently minimize risk, improve resiliency, and protect your most sensitive applications and data.

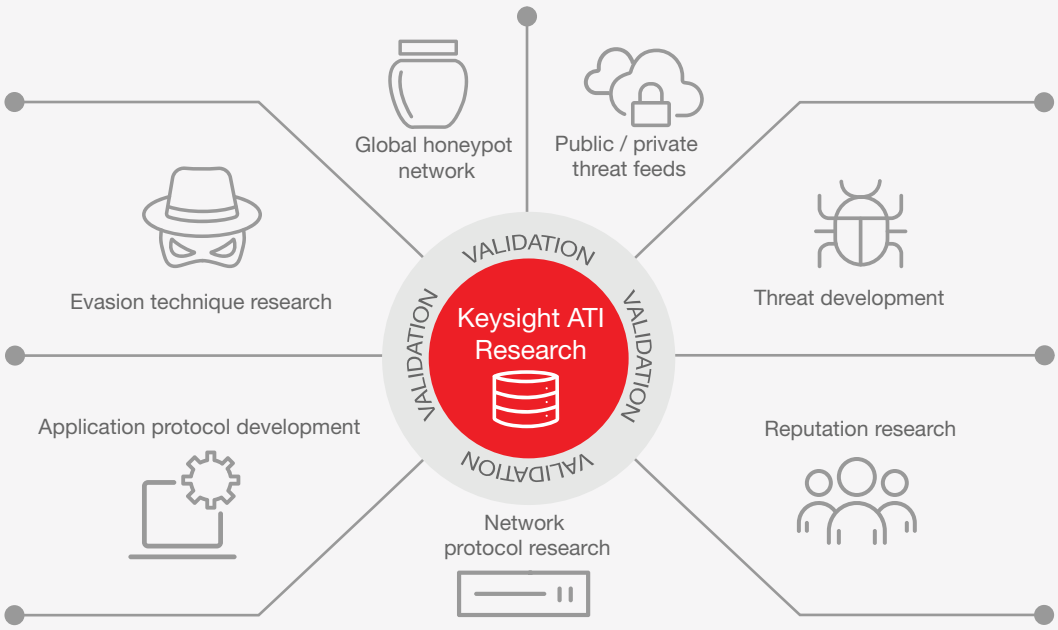
[1] "Cost of a Data Breach Report", 2019, Ponemon/IBM

Keysight ATI: A Real-World Example of Application and Threat Intelligence

Keysight knows networks. From test to application performance, visibility to cybersecurity, we know the challenges of maintaining a network firsthand. After all, when data is traversing at high speeds, security and performance issues are bound to arise.

That's why we created the Keysight Application and Threat Intelligence (ATI) Research Center, an elite group of top application and security researchers from around the globe. With knowledge spanning software development, reverse engineering, vulnerability assessment and remediation, malware investigation, and intelligence gathering, their collective expertise helps Keysight deliver industry-leading insight to security teams around the world.

Drawing on decades of leadership in network validation and test solutions, the Keysight ATI team synthesizes data gathered from our network security products with known application behaviors in multiple network environments (such as enterprises, service providers, and network equipment manufacturers). This combination gives the ATI Research Center a robust understanding of how hackers exploit vulnerabilities before a product launches and after its release on a live network



The ATI Research Center operates a distributed, worldwide network of honeypots and web crawlers to identify malware, attack vectors, and application exposures continuously. The team regularly identifies and discloses zero-day vulnerabilities. All findings are correlated against real-world events, validated against reported results, and then pushed to clients via continuously-updated feeds.

ATI feeds deliver actionable insight on critical application vulnerabilities — as well as threats across networks, endpoints, mobile devices, virtual systems, web, and email. These continuously updated feeds give SecOps teams access to a wide range of intelligence, including:

- open-source data sets
- billions of IPs and URLs
- millions of spam records
- millions of malware attacks
- millions of network intrusions

Minimize Risk and Fortify Your Defenses

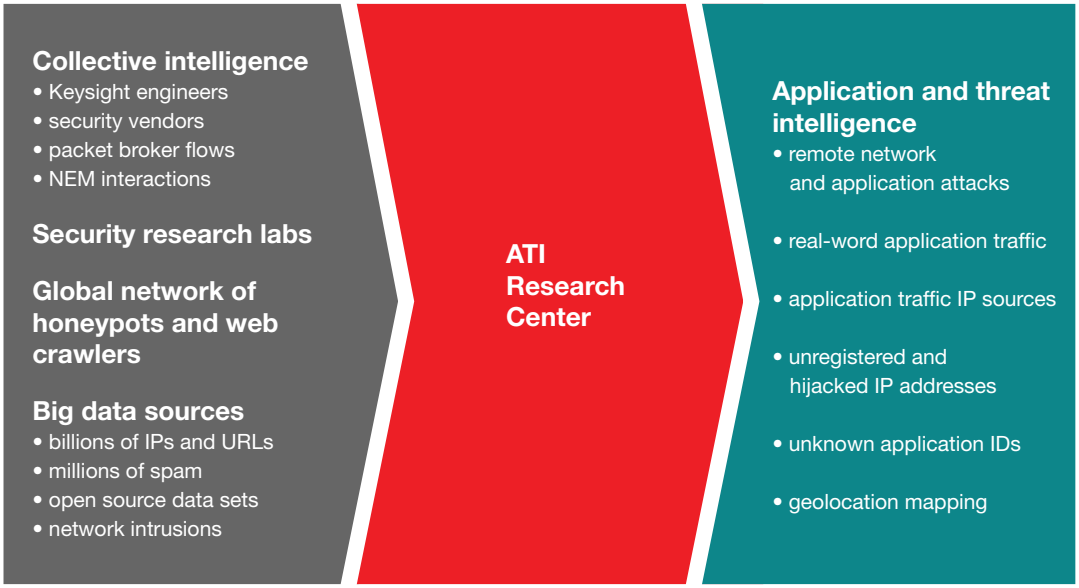
Combining deep knowledge in cybersecurity threats and application protocol behavior, the ATI team looks at threats and vulnerabilities in the same way as a cybercriminal, from every possible direction. This unique combination of intelligence enables security teams to assess their risk and vulnerability holistically — making it easy to take proactive, informed actions to shore up their defenses.

Security is never static, however, and the threat landscape is always changing. That's why ATI partners with leading developers to monitor every layer of the Open Systems Interconnection (OSI) stack and actively research threats around the globe. Furthermore, daily malware updates deliver actionable insight in near real time — helping the most agile security systems stand out in a crowded marketplace.

Empowering security teams is a crucial function of ATI's mission, but it is only a fraction of the work they do. At Keysight, we also rely on ATI's collective output to bolster our test, visibility, and security solutions — enabling us to:

- create realistic application attack simulations that emulate the entire kill chain
- block malicious inbound traffic and outbound communications
- collect ongoing intelligence on new threats
- identify unknown applications
- pinpoint traffic via geolocation

These capabilities go far beyond signature recognition. With Keysight's ATI feed, you can proactively defend against attack patterns, reduce your attack surface, and pinpoint product vulnerabilities — before and after release. By combining specialized security knowledge with decades of industry leadership in network test, protocols, and security, it's never been easier to verify, validate, and fortify your defenses.



ATI's Global Impact

In addition to application and threat intelligence feeds, Keysight's ATI Research Center supports a wide range of our products, including:

- Threat Simulator: Breach and Attack Simulation platform
- ThreatARMOR: Threat Intelligence Gateway
- BreakingPoint: application and network security testing
- Vision Series network packet brokers (equipped with AppStack visibility intelligence)
- IxLoad: L4-7 performance testing
- IxChariot: pre- and post-deployment network validation
- IxNetwork: L2-3 performance testing

However, a mere list of products does not tell the whole story. Top-ranked security vendors depend on the outputs of ATI research to ensure their products and applications work as intended. Moreover, enterprise SecOps teams count on ATI's continuous updates to ensure Threat Simulator can emulate the latest attacks, and ThreatARMOR can block them.

Additionally, almost every major network equipment manufacturer (NEM) and service provider relies on ATI data when they validate their hardware and systems with Keysight's network test products. The unique combination of application and threat intelligence enables a wide variety of advanced validation techniques, such as:

- Emulating communication protocol programming methods, common practices to introduce weaknesses, and wide-ranging traffic types.
- Deconstructing application protocols and packaging them for use in real-world user simulation testing.
- Executing application fuzzing, probing for specific weaknesses, and pinpointing undetected zero-day vulnerabilities in security tools

Smarter Security Makes Applications Stronger — and More Resilient

Threat intelligence providers and security vendors typically focus on the symptom, not the root cause. They address how to identify and block high-level threats — but often ignore the vulnerabilities attackers exploit to gain access to your network in the first place.

More robust applications mean better performance — and more resilient security. That's why you need to know if the applications you are using are stable and secure. But knowing the latest attacker exploits, identities, and methods require a depth of threat intelligence that only comes from years of experience and millions of working hours. The same is true for your applications. Understanding a churning sea of vulnerabilities — and the myriad ways they can affect downstream tools — also requires considerable time, effort, and investment.

Security teams work tirelessly to protect their networks, but that task is not getting any easier. Attack surfaces are growing, and a single misconfiguration can be the difference between a safe network and a compromised one. When the margins are this thin, application and threat intelligence can make all the difference.

SecOps teams need every edge they can get. It's time to help them work smarter, not just harder.

Learn more at https://www.keysight.com/us/en/products/network-security/ati-application-threat-intelligence.html. For more information on Keysight Technologies' products, applications, or services, please contact your Keysight representative.

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