CASE STUDY

# Service Provider Secures Network, Blocks Threats, and Boosts Efficiency

KEYSIGHT

## Organization

- U.K. based provider of fixed and mobile telephone, television, and broadband internet
- 4.8 million subscribers

## Challenges

- Extra layer of security without increase in budget
- Handle inspection of growing traffic volume
- Block data leakage and known threats

## Solutions

- ThreatARMOR™ 1G/10G security appliances
- Application and Threat Intelligence (ATI) subscription
- Vision ONE™ packet broker

## Results

- Traffic volume handled without device upgrades
- Outbound data leakage identified and stopped
- Security alerts reduced 30%

# Identifies And Stops Data Leakage

This company is one of the world's largest service providers with operations in more than 30 countries. To support the company's emphasis on service delivery and customer satisfaction, the security team at this broadband provider continually works to identify threats that can impact network reliability, performance, and sensitive company data. The team had a positive experience using Keysight BreakingPoint to stress test and bulletproof their infrastructure, and they were excited to hear about Keysight's other solutions for improving network security.

Since the cost of upgrading security appliances is significant and budget was somewhat limited, the security team wanted to explore ways of getting more out of their existing security infrastructure. Their local reseller suggested they look at using ThreatARMOR, Keysight's threat intelligence appliance, to drop known malicious traffic before it was processed through their firewall and IPS. While the security team believed their existing appliances were effective in protecting their network, they wanted to see if deploying a threat intelligence solution would significantly reduce tool workload and enable their existing infrastructure to handle more volume without the need for additional devices.

# Proof Of Concept Demonstrates Immediate Value

Naturally, deploying anything inline on the live network is extremely sensitive. To address this concern, ThreatARMOR was deployed and evaluated in passive mode. The team originally planned to operate the threat intelligence solution for several weeks to observe its behavior. Unlike other threat intelligence solutions, ThreatARMOR generates a “rap sheet” for every malicious IP address identified to fully explain the source of the threat and how it was confirmed. Reviewing the rap sheets allowed the company to see exactly what actions ThreatARMOR would take. And knowing each threat was verified before a rap sheet was created, eliminated concern about the risk of false positives, another possible result when appliances are deployed inline.

The ThreatARMOR appliance had been operating only a few hours when it flagged an active infection that was allowing data to leak outside the company’s firewall. Although security team had not anticipated responding so soon, they sprang into action to isolate the problem. The team was surprised to discover that the infected device was a server they thought had been decommissioned. Realizing that their existing infrastructure had not detected the leakage, the team was convinced that ThreatARMOR would indeed provide an extra layer of security against attacks that could potentially impact their services.

# Ease Of Use Gets the Team’s Attention

Even before ThreatARMOR flagged the data leakage, the team was impressed with the ease and speed of implementation. It took only fifteen minutes to connect ThreatARMOR’s power and Ethernet cables and begin generating notifications. The speed of deployment made it much easier to sell the concept to network managers.

Once the team was convinced of ThreatARMOR’s value, they began to notice additional features that would save them time and deployment effort. A post-deployment analysis showed that the number of security alerts requiring staff investigation would be reduced by up to 30% with blocking activated. Considering the difficulty of hiring and retaining experienced security staff, reducing the number of alerts was another valuable outcome.

Security managers were also pleased with the simplicity of ThreatARMOR’s drag-and-drop management interface. Unlike security appliances that required programming to make filter changes, ThreatARMOR’s interface was straightforward and could be used by the entire staff without specific training. When integrated with Keysight’s Application and Threat Intelligence (ATI) subscription feed, the ThreatARMOR appliance is automatically and remotely updated every five minutes with the latest intelligence and requires no manual maintenance or intervention.

> “Many attacks today are perpetrated in steps. Even a benign leakage must be corrected to ensure it doesn’t become a hole for future exploits and allow hackers an avenue for siphoning away sensitive data.”
>
> **Chief Security Officer**

# Advanced Threat Blocking Capabilities

ThreatARMOR also enabled the company to block traffic from specified geolocations where it did not do business, further reducing the security attack surface. Though the company's firewalls could be programmed to do this, spending the time to create the appropriate filters and maintain them had made it impractical to implement this function.

# Intelligent Packet Brokers Increase Tool Efficiency

Once the company reduced traffic from known malicious sources, it turned to selectively filtering legitimate traffic that was not central to the purpose of the specific tool. The ability to reduce the flow of unnecessary traffic reduces the risk of tool congestion, increases efficiency, and allows the existing tool capacity to handle growth in traffic volume. Although the company was currently using traffic visibility nodes from another vendor, the team decided to purchase Keysight Vision ONE packet brokers with the high-performance Advanced Threat Intelligence Processor (APPSTACK) during their next budget cycle. APPSTACK will give them the ability to identify packets by the associated application and context, giving them more control over what they send to their tools. The team estimates that advanced filtering will reduce the traffic load on the security appliances deployed by 15—30% and eliminate the need to upgrade this infrastructure over the coming year.

> "It is very rare to find a security appliance that is so easy to deploy and use. It literally took us fifteen minutes to plug ThreatARMOR in and get it running."
>
> **Network Security Engineer**

KEYSIGHT

For more information on Keysight Technologies' products, applications, or services, please visit: www.keysight.com