Hillstone™ NETWORKS | KEYSIGHT TECHNOLOGIES

SOLUTION BRIEF

# Deep Data Visibility to Protect against Advanced Threats

Hillstone Networks’ Network Traffic Analysis (NTA) Solution and Keysight Visibility Fabric

## The Challenge

Today’s networks are increasingly complex and require advanced security for their critical assets. Perimeter security is no longer adequate to protect against advanced threats, exfiltration attempts and user misbehavior.  In addition, exploits are increasingly moving within the network itself. Deep visibility into network data and traffic is therefore required in order to fully inspect and analyze potential threats and exploits.

## The Solution

Hillstone Networks’ Network Traffic Analysis (NTA) solution, coupled with Keysight Visibility Fabric, provide in-depth visibility with strong defenses and mitigation to protect against malicious threats and breaches. Keysight Visibility Fabric provides both physical and virtual taps for full visibility even into encrypted traffic, as well as traffic management for optimized and efficient operation. Hillstone’s NTA solution detects and protects against advanced threats, secures critical servers and data against leakage and theft, and gives security admins highly granular and effective security tools.

## Joint Solution Benefits

- Provides comprehensive Next-Gen Firewall (NGFW) protection against advanced threats including ransomware and cryptomining malware
- Real-time threat monitoring of mission-critical servers, hosts and traffic
- Detects Indicators of Compromise (IOCs), identifies risky hosts and servers, and determines and restores cyberattack kill chains
- Multiple threat detection technologies including traditional signature-based detection as well as data modelling and user behavior analytics
- Deep visibility to data via both physical and virtual taps, including SSL-encrypted traffic
- Aggregates, optimizes and streamlines data to ensure efficient and cost-effective operation

## Introduction

As attackers become ever more sophisticated, network security must also evolve to protect critical business assets. A strong perimeter security remains a requirement, but it is increasingly important to examine and secure data and resources within the network itself. The challenge, however, is to deploy technologies in a way that is seamless and nondisruptive, while providing full visibility into all traffic for effective, efficient protection.

## The Hillstone and Keysight Joint Solution

Hillstone's Network Traffic Analysis (NTA) solution is comprised of the I-Series Server Breach Detection System (sBDS) and the T-Series iNGFW. They both detect and protect against a wide variety of internal and external threats, including advanced exploits like ransomware and cryptomining. Keysight Visibility Fabric interfaces to Hillstone's NTA solution using physical and virtual taps to provide full visibility into the network. The joint solution provides high efficiency and deep visibility into the network for enhanced security and protection of vital assets.

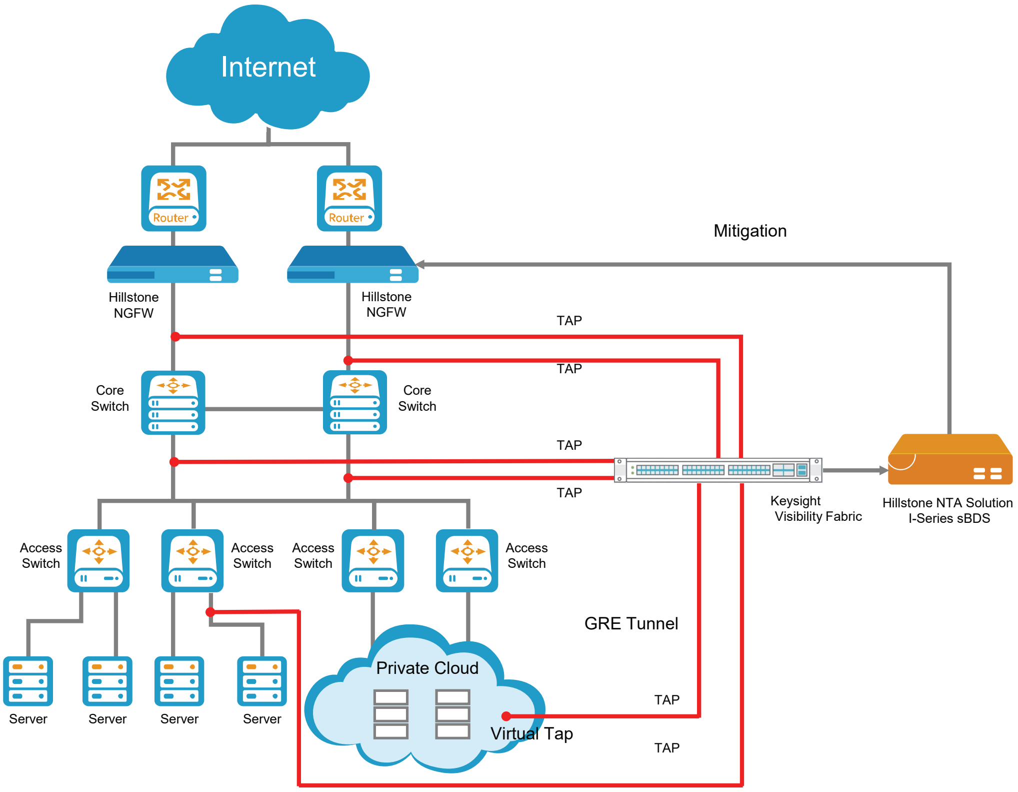
## Key Benefits of the Joint Solution

### Agile, Effective Threat Detection

- Detects advanced persistent threats, advanced malware, ransomware, cryptomining malware and other exploits
- Real-time threat monitoring for critical servers and hosts to protect against data leakage or theft, as well as to pinpoint abnormal application and network activities
- Detection of indicators of compromise, identification of compromised hosts and servers, and restoration of attack kill chains
- Multiple threat detection technologies, including traditional signature-based detection as well as large-scale intelligent data modelling and user behavior analytics to detect unknown or zero-day threats
- Threat correlation analytics to dive deep into suspicious threat events and provide accurate and effective threat detection
- A full arsenal of security capabilities, including intrusion detection (IDS/IPS), antivirus, abnormal behavior detection, advanced threat detection (APT and advanced malware), application identification, anti-spam, cloud sandbox and deception threat detection (honeypot), botnet C&C and attack detection
- Supports threat mitigation ranging from simple blocking of traffic to admin intervention
- Rich forensic information and preemptive mitigation through interworking between the Hillstone sBDS and NGFW

## Deep Visibility and Efficiency

- Physical and virtual taps provide full network visibility, far beyond simple SPAN ports
- Aggregates data from Keysight Visibility Fabric before sending to Hillstone NTA solution
- Zero packet loss to ensure that all packets are presented for inspection and analysis
- Optimizes the number of NTA interface ports required by aggregating network links
- De-duplication and filtering optimizes network traffic before forwarding to the Hillstone NTA appliance
- SSL decryption and re-encryption to ensure that all traffic is analyzed and protected
- Load balancing across multiple Hillstone NTA solutions ensures efficient operation



Visit www.hillstonenet.com to learn more
or contact Hillstone at inquiry@hillstonenet.com