



## Case Study

# Stopping Attacks in Their Tracks: A Manufacturing Company's Network Threat Detection Triumph

A well-known textile manufacturer in southeast Asia deployed Hillstone Networks to stop threats in their tracks.



## Customer Profile

### Customer

Textile manufacturer

### Sector

Manufacturer

### Location

Southeast Asia

### Scope

Over the past 40 years, the company has grown into a publicly-traded entity, won numerous awards, and now calls some of the largest brands in the world its customers

### Size

800 employees

### Challenges

- Insufficient visibility into network traffic, and activity
- Vulnerabilities from botnets and cyberattacks in web application services

### Requirements

- A network monitoring solution with real-time detection and analysis of advanced threats.
- A turnkey solution without the burden of significant onboarding or management overhead.

### Results

The solution from Hillstone delivers real-time alerts that are prioritized for action. Additional context, including geo-location of hosts and events accelerate and improve threat triaging. In addition the built-in threat monitoring keeps security admins informed on suspicious and malicious events



## Background

The customer is a Manufacturer in the garment and textile industry, with nearly 800 employees in Southeast Asia. Over the past 40 years, the company has grown into a publicly-traded entity, won numerous awards, and now calls some of the largest brands in the world its customers.

As the company has matured, legacy technology solutions have lost their potency, and certain systems have been forgotten and left vulnerable. The company found itself in need of a modern security solution that could rapidly address its network security challenges, while delivering rapid time to value and low cost of ownership.

## The Challenges

The company had insufficient visibility into its network traffic, vulnerabilities, and activity. This left their security and network teams flying blind to potential threats, so they needed a network monitoring solution that provides real-time detection and analysis of advanced threats.

The company's web application service was at risk for botnet and other attacks. They needed a visual representation for the topology of attacks, command and control server relationships, host risks and kill chain mapping.

With these new security capabilities to be brought online, the company also needed a turnkey solution that comes without the burden of significant onboarding or management overhead.

## The Solution

Hillstone Networks' Breach Detection System (BDS) was called into service for its comprehensive capabilities in defending against network attacks.

### Continuous Real-time Monitoring for Enhanced Security

Hillstone BDS capabilities include detecting unknown and recent threats based on abnormal network and application-level activities on servers. With a baseline modeled across L3-L7 behaviors, Hillstone BDS is continuously trained to detect unknown and known threats such as DDoS, HTTP scanning, flooding, deception and more.

### Threat Analysis and Visualization

Hillstone BDS features several dashboards and visualization modules to enable threat analysts and administrators to clearly see the kill chain and related entities involved in an attack. This additional context includes threat maps, threat tags, user agents, service types, server risk index, trends and much more.

### Effective Threat Mitigation

Once threats are detected, Hillstone BDS enables administrative status actions and one-click cleanup of threat evens on servers for posture reevaluation. In addition, BDS integrates seamlessly with Hillstone's industry-leading next generation firewall (NGFW) devices for preemptive blocking and policy synchronization.



## Reduced Total Cost of Ownership

Finally, Hillstone BDS is designed to enable rapid time to value and deployment. There is no need for specialized training or dedicated resources to quickly get value from Hillstone BDS. Once it is brought online, it quickly begins learning, mapping and analyzing networks for risk and threats.

## The Results

Hillstone Networks BDS delivered value to the organization right away. The ease of deployment and simple management meant that no specialized training was required to onboard their security team, resulting in lower total cost of ownership from less overhead.

Threats against the organization are now visualized in real time and alerts are prioritized for action. Geolocation of hosts and events provides additional context in triaging threat, and Hillstone BDS' built-in threat monitor enables the company to know exactly what types of suspicious or malicious events are taking place at any given time. Events are responded to quicker, and the organization is more confident in their overall security program.

“ Hillstone gives us peace of mind. It helps us detect attacks before they spread out on the network. We can now stop the hosts that have been compromised and who are scanning our networks attempting brute force access to our datacenters.

IT Director





## About Hillstone Networks

Hillstone Networks is a leader in cybersecurity, delivering both depth and breadth of protection to companies of all sizes, from edge to cloud, and across any workload. Hillstone Networks' Integrative Cyber Security approach brings coverage, control, and consolidation to more than 26,000 enterprises worldwide.

Hillstone Networks is uniquely positioned with a platform that's future-proof to enable digital transformation and business continuity. For more information and to find your Integrative Cybersecurity solution, please visit [www.hillstonenet.com](http://www.hillstonenet.com)

### Learn more about Hillstone products mentioned in this case study

[Hillstone Breach Detection System \(BDS\) ⇒](#)



### Read about Hillstone solutions

[Cloud Workload Protection \(CWPP\) ⇒](#)

[Extended Detection & Response \(XDR\) ⇒](#)

[Zero-Trust Network Access \(ZTNA\) ⇒](#)

[Secure SD-WAN ⇒](#)

[Micro-segmentation ⇒](#)

[Network Detection & Response \(NDR\) ⇒](#)