The Hillstone and Trend Micro Joint Solution  
Advanced Threat Defense Platform

Overview

Hillstone and Trend Micro offer a joint solution – the Advanced Threat Defense Platform – by integrating the industry leading Hillstone NGFW/iNGFW with Trend Micro’s leading breach detection technology. The Advanced Threat Defense Platform provides automatic threat identification, threat warning, and threat blocking. It dramatically reduces threat response time by taking rapid remedial action following any security breach, thereby reducing human resource costs and significantly improving a timely response.

The Advanced Threat Defense Platform provides high performance of NGFW features, industry-leading breach detection rates and zero false positives. With comprehensive attack protection, this platform detects and prevents known as well as unknown threats in real-time.

Malware

The main malware threats are Trojans and Viruses, pieces of software stealthily installed onto application servers, endpoints, and smart phones in your network, with the intent to steal critical user data or damage the IT system. An attacker implants new variants of malware that hide longer term in the network, awaiting an opportunity to attack.

Botnet

Once infected by a Botnet, enterprise endpoints are hijacked and subsequently controlled as the bot computer. Attackers often leverage these bot computers to launch a DoS/DDoS attack from your company’s network onto one of your partners’ systems, not only resulting in stolen data or service failures, but also damaging your enterprise’s reputation and trust with your partners.
**C&C Attack**

A Command and Control (C&C) attack is a typical Botnet breach where the attackers control the internal host to stealthily communicate with external C&C servers. C&C messages are furtively hidden in normal traffic, or use a mediating agent to send messages. For example, some attacks use Web applications where the C&C messages are transmitted in the SSL tunnel – a traditional security device is unable to detect these malicious messages inside the encrypted traffic.

**Advanced Persistent Threat (APT) Attack**

APT attackers intrude into the core enterprise network by evading security devices, then targeting intellectual property and customer information. They use unknown malware and zero-day vulnerabilities to infiltrate the network in steps. Once they obtain administrator credentials, they search the entire network for a target from where to steal user data or damage the IT system.

Today’s enterprise network infrastructure is changing fundamentally in response to the accelerating impact of virtualization and mobile technologies. These trends have expanded the boundaries of security defense. New types of APT attacks leverage the vulnerability of business systems and mobile devices, stealthily intruding into the system and causing serious risk to online services and critical user data. As cyber-attacks continue to evolve, APT attackers no longer use a single method, but adopt hybrid methods for network infiltration.

**Deficiencies of Existing Security Solutions**

Existing security solutions result in high rates of false positives and are ineffective at continuous monitoring and the identification of unknown threats. Traditional threat detection tools are based on signature matching, which allows only the detection of previously identified threats. In some defense systems, the firewall and breach detection devices are not integrated, so that when a threat is detected, a mitigation policy must be configured manually. This response is slow, consumes human resources and is unable to protect the system from the first strike of the threat.

**Advanced Threat Defense Platform: Accurate Unknown Threat Prevention**

To achieve accurate threat prevention of unknown threats, the integration of Hillstone’s NGFW/iNGFW and Trend Micro’s Deep Discovery Inspector (DDI) technologies offers a sophisticated Advanced Threat Defense Platform. DDI uses sandboxing technology to analyze dynamically, and accurately identify, unknown threats: the results of which are synchronized with the Hillstone NGFW/iNGFW. DDI enables the Hillstone NGFW/iNGFW to augment its defense capacity by automatically configuring the mitigation policy to block these unknown threats more accurately. The Hillstone NGFW/iNGFW provides security protection from the network to the application layer, complementing DDI’s capabilities.

The Advanced Threat Defense Platform, depicted in Figure 1, effectively prevents malware, Botnet, C&C and APT attacks from either Internet or Intranet sources, and provides security protection for enterprise core networks.
and APT attacks from either Internet or Intranet sources, and provides security protection for enterprise

The Advanced Threat Defense Platform, depicted in Figure 1, effectively prevents malware, Botnet, C&C protection from the network to the application layer, complementing DDI's capabilities. Hillstone NGFW/iNGFW provides security policy to block these unknown threats more accurately. The Hillstone NGFW/iNGFW provides security by automatically configuring the mitigation of unknown threats: the results of which are synchronized with the Hillstone NGFW/iNGFW. DDI enables the

To achieve accurate threat prevention of unknown threats, the integration of Hillstone's NGFW/iNGFW is unable to protect the system from the first strike of the threat. A mitigation policy must be configured manually. This response is slow, consumes human resources and systems, the firewall and breach detection devices are not integrated, so that when a threat is detected, DDI protects against DDoS attacks, SQL injection, XSS attacks, protocol vulnerability attacks, as well as offering IP blacklist, URL filter and web server protection.

Advanced Threat Defense Platform Features

Figure 2 shows the primary features of the Advanced Defense Platform. These include:

- **Threat Visibility:** Trend Micro DDI inspects and analyzes more than 80 L2-L7 protocols to detect traffic threats in real-time, and clearly exposes suspicious behavior in servers and endpoints.

- **Identification Accuracy:** Trend Micro DDI is based on contextual analysis, multi-level correlation analysis and sandboxing. This enables it to expose infected hosts, identify threat types accurately, and issuing threat warnings.

- **Real-time Blocking:** The Hillstone NGFW/INGFW automatically synchronizes analysis data, dynamically updates the global blacklist, and blocks attacks from threat sources in real-time.

- **Comprehensive Protection:** The Hillstone NGFW/INGFW provides L2-L7 threat prevention to protect against DDoS attacks, SQL injection, XSS attacks, protocol vulnerability attacks, as well as offering IP blacklist, URL filter and web server protection.

![Figure 2: Features of the Advanced Threat Defense Platform](image-url)
Advanced Threat Defense Platform Operation

The Advanced Defense Platform offers the following operational characteristics:

- **Integration:** The Hillstone NGFW/iNGFW and DDI integrate by using a standard API which allows DDI to mirror the traffic of the NGFW/iNGFW.

- **Threat Identification:** DDI monitors and analyzes all data traffic, identifies suspicious communication and hidden attacks, and generates an IP/URL reputation of a threat.

- **Data Synchronization:** The Hillstone NGFW/iNGFW periodically synchronizes the IP/URL reputation information from DDI via a service API once it gets access permission from DDI.

- **Threat Visibility:** The Advanced Threat Defense Platform provides a web UI to configure the integrated solution, and to display graphic reports of threat types, threat source IP addresses, blocking logs and more.

- **Threat Blocking:** The Hillstone NGFW/iNGFW adds the IP/URL reputation information to the local IP blacklist and URL filters, allowing it to block in real-time attack packets from this threat source.

Use Case

The Advanced Threat Defense Platform enables protection for financial enterprises by deploying the platform at the Internet entry point to guard against social engineering APT (malware mail). The sandbox analyzes suspicious attachments and identifies malicious contents, communications and behaviors. The NGFW prevents unknown attacks in real-time, and guarantees the reliability and availability of the enterprise network.

Governments and educational establishments are primary targets of APT and malware. Deploying the Advanced Threat Defense Platform in front of the service zone enables accurate identification of data stealing behavior, either from/on servers or from/on endpoint devices, and also prevents malware from accessing sensitive data. Simplified deployment management reduces operational costs.

Summary

The Hillstone and Trend Micro joint solution enables integration between the most innovative NGFW device and the most innovative deep breach detection device, combining the advantages of both. The Advanced Threat Defense Platform automatically blocks unknown threats upon first encounter, thereby protecting critical business systems and data, and guaranteeing business continuity for the enterprise.

Hillstone Networks

As a leading provider in network security, Hillstone Networks’ security products are widely used by carriers, government agencies, large enterprises and universities. With its innovative Intelligent Next-Generation Firewall, Hillstone Networks is recognized by the Gartner firewall report as a vendor providing continuous innovation efforts in the China market. In 2014, Hillstone Networks was positioned in the Gartner Magic Quadrant for Enterprise Network Firewalls due to its outstanding innovative capabilities and competitiveness, surpassing many other global vendors in terms of “completeness of vision” of network security technology.
Advanced Threat Defense Platform: Accurate Unknown Threat Prevention

Deficiencies of Existing Security Solutions

Today’s enterprise network infrastructure is changing fundamentally in response to the accelerating impact of virtualization and mobile technologies. These trends have expanded the boundaries of security systems, the firewall and breach detection devices are not integrated, so that when a threat is detected, monitoring and the identification of unknown threats. Traditional threat detection tools are based on types accurately, and issuing threat warnings.

Stealthily Intruding into the System and Causing Serious Risk to Online Services and Critical User Data

Advanced Persistent Threat (APT) attackers intrude into the core enterprise network by evading security devices, then targeting access to infiltrate the network in steps. Once they obtain administrator credentials, they search the entire network for a target from where to steal user data or damage the IT system. They use unknown malware and zero-day vulnerabilities to infiltrate the network stealthily intruding into the system and causing serious risk to online services and critical user data. As new types of APT attacks leverage the vulnerability of business systems and mobile devices, the impact of virtualization and mobile technologies. These trends have expanded the boundaries of security

Use Case

The Advanced Threat Defense Platform enables protection for financial enterprises by deploying the Advanced Threat Defense Platform in front of the service zone enables accurate identification of data as offering IP blacklist, URL filter and web server protection. The Advanced Threat Defense Platform, depicted in Figure 1, effectively prevents malware, Botnet, C&C attacks from either Internet or Intranet sources, and provides security protection for enterprise

Advanced Threat Defense Platform

Trend Micro

As a global leader in IT security, Trend Micro offers innovative security solutions that deliver top-ranked client-server, network, virtualization and cloud-based protection. Trend Micro is recognized as the “Top one vendor in global virtualization security market”, the “Top one vendor in global server security market”, and the “Top one vendor in global cloud security market”.

In the testing conducted by NSS labs, Trend Micro’s DDI provides outstanding results of the highest detection rate and zero false positives, making it a leader compared to other tested vendors.

Trend Micro Deep Discovery

TOP SCORE
in breach detection

NSS Labs
RECOMMENDED

2014 Breach Detection Tests