Data sheet

HP TippingPoint Advanced Threat Appliance family

Stop advanced persistent threats from spreading in your network

HP TippingPoint Advanced Threat Appliance overview

Targeted attacks, advanced threats, and advanced persistent threats continue to penetrate traditional network security solutions with evasive techniques like slow detonating malware, compromised mobile devices, and hidden payloads. Using multiple scanning techniques, the software from Trend Micro helps the HP TippingPoint Advanced Threat Appliance (ATA) family carefully watch malware behavior as it runs in a safe, sandboxed environment. When malware infiltrates your network, the sophisticated detection technology of ATA identifies the suspicious behavior giving you the visibility to respond quickly to stop it before it can cause damage.

Advanced Threat Appliance highlights:

- Lock down patient zero, stop the spread, and neutralize the attack at the initial point of infection before it spreads laterally
- Increased protection against advanced persistent threats with static and dynamic detection techniques
- Leverage the HP TippingPoint Security Management System (SMS) to coordinate responses with HP TippingPoint Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (IPS) in-line enforcement appliances
- Enhance security intelligence as the NGFW and NGIPS “learn” from attacks and feed the HP TippingPoint Threat Digital Vaccine (ThreatDV) service

HP TippingPoint ATA family

HP TippingPoint ATA family offers two solutions: the ATA - Network and the ATA - Mail. For broad network malware protection, the ATA - Network detects advanced persistent threats on all ports, over 80 protocols, and across a broad spectrum of OSs. The ATA - Mail works with your mail gateway to identify and block malicious emails including spear-phishing emails that are the initial phase of most targeted attacks. It reduces your risk of a successful attack by adding a transparent inspection layer that discovers malicious content, attachments, and URL links that pass unnoticed through standard email security.

Figure 1. The host severity reports provide a numerical value and example of the threat, giving better insight into the attack

Host severity of affected hosts

Host severity		Examples
Critical Host exhibits behavior that definitely indicated host is compromised.	10	• Host with detections(s) of files, IP addresses, URLs, or domains associated with known Advanced Persistent Threat (APT). • Host with evidence of data exfiltration or compromised database.
	9	• Host with detection(s) of files, IP addresses, URLs, or domains indicating a targeted attack is underway.
	8	• Host with connection(s) to URLs, IP addresses, FTP accounts, email addresses, and others associated with known data-stealing activities. • Host is propagating or sending malicious files to other hosts.
Major Host is targeted by known malicious behavior or attack and exhibits behavior that likely indicated host is compromised.	7	• Host with inbound malware download(s); no evidence of user infection.
	6	• Host with inbound high-risk potentially malicious file download(s); no evidence of user infection.
	5	• Host with inbound medium- or low-risk potentially malicious file download(s); no evidence of user infection.
	4	• Host with inbound phishing email message; no evidence of user action and/or stolen credentials.
Minor Host exhibits anomalous or suspicious behavior that may be benign or indicate a threat.	3	• Host with repeated unsuccessful logon attempts or abnormal patterns of usage. • Host downloads or propagates packed executables or suspicious files. • Host uses IRC, TOR, or outbound tunneling software.
	2	• Host uses rogue services.
Trivial Host exhibits normal behavior that may be benign or indicate a threat in future identification of malicious activities.	1	• Host uses Remote Access tools (RDP, telnet, VNC). • Host with normal database access.

HP TippingPoint ATA - Network

Features and benefits

Custom sandboxing

Precisely match your system configurations to detect the targeted attacks threatening your network. The custom sandbox can emulate your environment allowing you to detect threats targeted to your organization and react accordingly.

Attacker forensics

Use specialized detection engines, correlations rules, and custom sandboxing to detect all aspects of an advanced persistent threat, not just malware. Advanced threats are multifaceted and require many methods of detection for command and control, malware, and unique attacker activity.

Detect and enforce

Detection is only half the solution, enforcement is the other half. By integrating with the HP TippingPoint SMS, you can easily leverage detection data to create new rules and policies to block existing and future attacks.

Broad system malware protection

Detect threats on your network regardless of OS. Today's networks are made up of a number of different OSs. You need protection across Android, Linux®, Mac OS X, Windows®, and others. Your security shouldn't dictate what OSs you could run in your network; it should be able to detect threats across the spectrum.

Comprehensive advanced persistent threat detection

Monitor all ports and more than 80 protocols to identify attacks anywhere on your network.

Software by Trend Micro

HP has partnered with Trend Micro, an industry leader in advanced persistent threat detection, to create the HP TippingPoint ATA family. In the NSS Labs Breach Detection Tests, this product recorded the highest score in breach detection (99.1 percent) with zero false positives and low total cost of ownership—over 25 percent below the average of all products tested.[1]

HP TippingPoint ATA - Mail

Email attachment analysis

Examines email attachments using multiple detection engines and sandboxing. Attachments analyzed include a wide range of Windows executables, Microsoft® Office, PDF, Zip, Web content, and compressed file types.

Document exploit detection

Malware protection is done by specialized detection and sandboxing techniques, which can discover malware and exploits delivered in common office documents.

Embedded URL analysis

URLs contained in emails are analyzed using reputation, content analysis, and sandbox simulation.

Password intelligence

Unlocking of password-protected files and Zip files is attempted using a variety of heuristics and customer-supplied keywords.

[1] nsslabs.com/reports/breach-detection-system-bds-product-analysis-report-trend-micro-deep-discovery-inspector

Table 1. HP TippingPoint ATA family

	ATA - Network 250	ATA - Network 500	ATA - Network 1000	ATA - Network 4000	ATA - Mail 6000
Capacity	250 Mbps	500 Mbps	1 Gbps	4 Gbps	400,000 emails/day
Form factor	1U rack-mount, 48.26 cm (19")			2U rack-mount, 48.26 cm (19")	1U rack-mount, 48.26 cm (19")
Weight (max.)	16.78 kg (36.99 lb)			23.6 kg (51.5 lb)	16.78 kg (36.99 lb)
Dimensions (w x d x h)	43.47 x 69.85 x 4.32 cm (17.11 x 27.5 x 1.7 in.)			44.55 x 67.94 x 8.73 cm (17.54 x 26.75 x 3.44 in.)	43.47 x 69.85 x 4.32 cm (17.11 x 27.5 x 1.7 in.)
Management ports	10/100/1000BASE-T RJ45 x 1			10/100/1000BASE-T RJ45 x 1	10/100/1000BASE-T RJ45 x 1
Data ports	10/100/1000BASE-T RJ45 x 4			10/100/1000BASE-T RJ45 x 4, 10GbE SFP+ x 2	10/100/1000BASE-T RJ45 x 4
AC input voltage	100 to 120 V ac 200 to 240 V ac			100 to 120 V ac 200 to 240 V ac	100 to 120 V ac 200 to 240 V ac
AC input current	2.78 A (100 V) to 1.15 A (240 V)			4.58 A (100 V) to 1.88 A (240 V)	2.78 A (100 V) to 1.15 A (240 V)
Hard drives	600GB 12G SAS 15k rpm 2.5" x 2			600GB 12G SAS 15k rpm 2.5" x 8	600GB 12G SAS 15k rpm 2.5" x 2
RAID configuration	RAID 1			RAID 10	RAID 1
Power supply (hot swap)	500 W Redundant			800 W Redundant	500 W Redundant
Power consumption (max.)	276.9 W			456.1 W	276.9 W
Heat (max.)	944 BTU/hr			1,556 BTU/hr	944 BTU/hr
Frequency	50/60 Hz			50/60 Hz	50/60 Hz
Operating temperature	10 to 35°C (50 to 95°F)			10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)

Learn more at
hp.com/go/tippingpoint

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-6202ENW, December 2014