Exhibit 2

Advanced Threat Prevention Appliance

Product Overview

Juniper Networks Advanced Threat Prevention Appliance is a distributed software platform that combines advanced threat detection, consolidated security analytics, and one-touch threat mitigation to protect organizations from cyber attacks and improve the productivity of security teams. The ATP Appliance detects threats across web, e-mail, and lateral traffic. Additionally, it can ingest logs from security devices to present a consolidated view of all threats in the environment.

Product Description

Organizations worldwide face security and productivity challenges every day. Zero-day malware often goes undetected because traditional security devices, which rely on signature-based detection, can't see it. Adding to the problem, security teams—overwhelmed by large volumes of alerts—often fail to recognize and act on critical incidents.

The Juniper Networks® Advanced Threat Prevention Appliance (formerly the Cyphort All-in-One system) provides continuous, multistage detection and analysis of Web, e-mail, and lateral spread traffic moving through the network. It collects information from multiple attack vectors, using advanced machine learning and behavioral analysis technologies to identify advanced threats in as little as 15 seconds. Those threats are then combined with data collected from other security tools in the network, analyzed, and correlated, creating a consolidated timeline view of all malware events related to an infected host. Once threats are identified, "one-touch" policy updates are pushed to inline tools to protect against a recurrence of advanced attacks.

The detection component of the ATP Appliance monitors network traffic to identify threats as they progress through the kill chain, detecting phishing, exploits, malware downloads, command and control communications, and internal threats. A multistage threat analysis process, which includes static, payload, machine learning, and behavior, as well as malware reputation analysis, continuously adapts to the changing threat landscape leveraging Juniper's Global Security Service, a cloud-based service that offers the latest threat detection and mitigation information produced by a team of security researchers, data scientists, and ethical hackers.

The threat analytics component of the ATP Appliance offers a holistic view of identity and threat activity gathered from a diverse set of sources such as Active Directory, endpoint antivirus, firewalls, secure Web gateways, intrusion detection systems, and endpoint detection and response tools. The analytics component looks at data from these sources, identifies advanced malicious traits, and correlates the events to provide complete visibility into a threat's kill chain. Security analysts receive a comprehensive host and user timeline that depicts how the events that occurred on a host or user unfolded. The timeline enhances the productivity of Tier 1 and Tier 2 security analysts who work on triaging and investigating malware incidents.

The ATP Appliance can integrate with other security devices to mitigate threats, giving users the ability to automatically quarantine e-mails on Google and Office 365 using REST APIs. Communications between the infected endpoint and the command and control servers are blocked by pushing malicious IP addresses to firewall devices. Integration with network access control devices can isolate infected hosts. The ATP Appliance's open API architecture also allows it to integrate with a number of third-party security vendors such as Cisco, Palo Alto Networks, Fortinet, Bluecoat, Check Point, Carbon Black, and Bradford, among others.

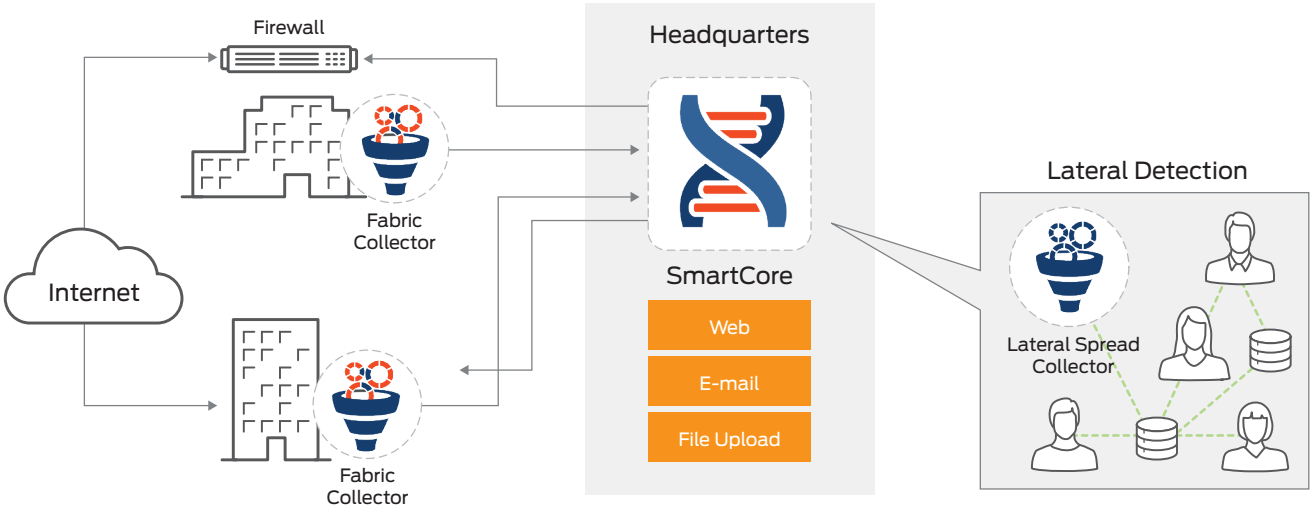

Figure 1: Juniper Networks ATP Appliance architecture

Architecture and Key Components

The architecture of the ATP Appliance consists of collectors deployed at critical points in the network, including remote locations. These collectors act like sensors, capturing information about Web, e-mail, and lateral traffic. Data and related executables collected across the fabric are delivered to the SmartCore analytics engine. Along with traffic from the native collectors, the ATP Appliance also ingests logs from other identity and security products such as Active Directory, endpoint antivirus, firewalls, secure Web gateways, intrusion detection systems, and endpoint detection and response tools. The logs can be ingested directly from third-party devices, or they can be forwarded from existing SIEM/syslog servers.

Armed with data collected from various sources, the SmartCore analytics engine performs the following multistage threat analysis processes:

- **Static analysis:** Applies continuously updated rules and signatures to find known threats that may have eluded inline devices.
- **Payload analysis:** Leverages an intelligent sandbox array to gain a deeper understanding of malware behavior by detonating suspicious Web and file content that would otherwise target Windows, OSX, or Android endpoint devices.
- **Machine learning and behavioral analysis:** Employs patent-pending technologies to recognize the latest threat behaviors (such as multicomponent attacks over time) and quickly detect previously unknown threats.
- **Malware reputation analysis:** Compares analysis results with similar known threats to determine whether a newly detected threat is a variant of an existing issue or something completely new.
- **Prioritization, risk analysis, correlation:** Prioritizes threats based on threat severity, asset targets in the network, endpoint environment, and the threat's progression along the kill chain. For example, a high severity Windows malware landing on a Mac receives a lower risk score than a medium severity malware landing on a protected server. All malware events from the ATP Appliance and other security devices are correlated based on endpoint hostname and time and then plotted on a host timeline, allowing security teams to assess the risk of a threat and whether it requires immediate attention. For example, a threat detected by the ATP Appliance but missed by the antivirus solution receives a higher risk score. This allows security teams to go back in time and review all malicious events that have occurred on an infected host.

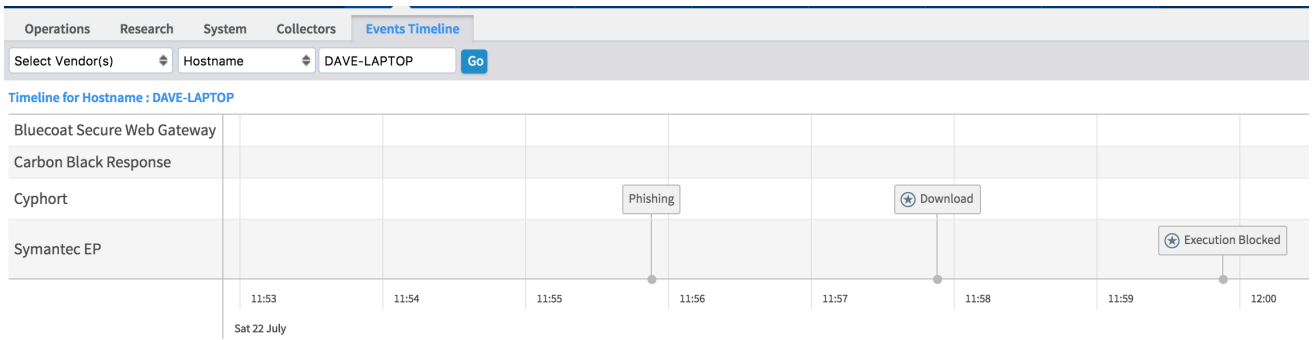

Figure 2: ATP Appliance events timeline