Exhibit 7

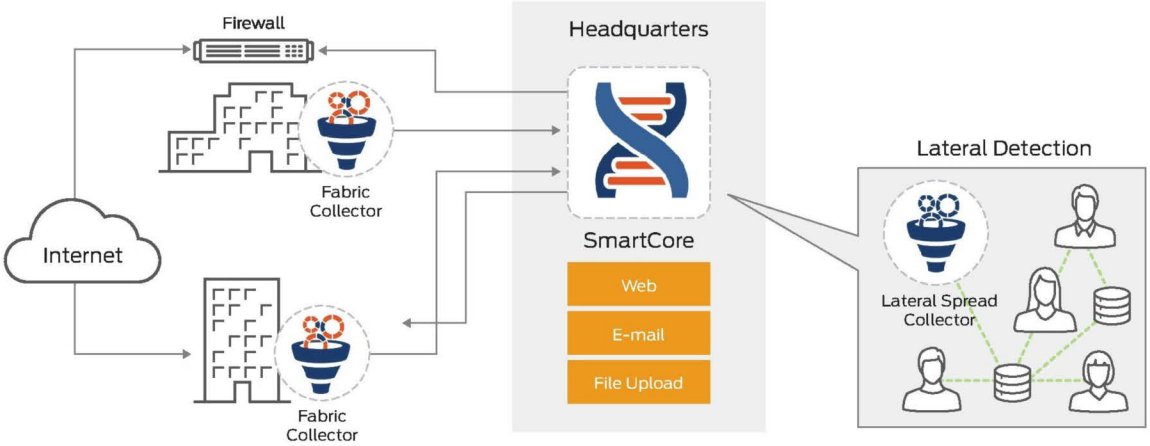

Figure 1: Juniper Networks ATP Appliance architecture

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

Features and Benefits

The ATP Appliance includes the following features and benefits:

- Inspects traffic across multiple vectors such as Web, e-mail, and lateral spread
- Uploads suspicious files through the Web UI for processing
- Supports Windows 7 and OSX 10.10 operating systems
- Analyzes multiple file types, including executables, DLL, Mach-o, Dmg, PDF, Office, Flash, ISO, ELF, RTF, APK, Silverlight, Archive, and JAR
- Includes detection techniques such as exploit detection, payload analysis, command and control (C&C) detection, YARA, and SNORT rules
- Provides comprehensive and well-documented APIs that allow easy integration with third-party security devices
- Integrates with Juniper Networks, Palo Alto Networks, Checkpoint, Cisco, Fortinet, and Bluecoat solutions to automatically block malicious IP addresses and URLs
- Automatically quarantines Office 365 and Gmail e-mails
- Integrates with Carbon Black Protect and Response (endpoint solution) to allow upload of binaries executed on endpoints
- Integrates with Cloud Access Security Broker vendor SkyHigh to protect assets in the cloud
- Manages multiple SmartCore analytics engines via Manager of Central Managers functionality
- Supports access and authentication using SAML and RADIUS
- Correlates events across kill chain stages to monitor threat progress and risk
- Visualizes malware activity and groups malware traits to help incident response teams better understand malware behavior
- Prioritizes threats based on risk calculated from threat severity, threat progress, asset value, and other contextual data
- Provides timeline host view to obtain complete context about malware events that have occurred on the host

Product Options

The ATP Appliance is available as both a physical and virtual appliance. Physical appliances can be deployed in all-in-one mode (SmartCore and Fabric Collector are installed on the same physical appliance) or in distributed mode (SmartCore and Fabric Collector are installed on separate appliances). Virtual appliances can be deployed in distributed mode only.

Physical

All in One

Model	Performance (Objects Detonated)	Performance
AIO-R430	Up to 30,000 objects/day	1 Gbps
AIO-R730	Up to 80,000 objects/day	2 Gbps

SmartCore

Model	Performance (Objects Detonated)
SC-R730	Up to 175,000 objects/day
AIO-R730	Up to 80,000 objects/day

Fabric Collector

Model	Performance
FC-R330	1 Gbps
FC-R730	4 Gbps

Virtual

Virtual SmartCore Engine

Model	Performance (Objects Detonated)	Virtual CPU	Virtual Memory	Virtual Disk
vSC-8	Up to 40,000 objects/day	8	32 GB	1.5 TB
vSC-24	Up to 140,000 objects/day	24	96 GB	1.5 TB

Virtual Fabric Collector

Model	Performance	Virtual CPU	Virtual Memory	Virtual Disk
FC-v50M	50 Mbps	1	1.5 GB	16 GB
FC-v100M	100 Mbps	2	4 GB	16 GB
FC-v500M	500 Mbps	4	16 GB	512 GB
FC-v1G	1 Gbps	8	32 GB	512 GB
FC-v2.5G	2.5 Gbps	24	64 GB	512 GB

Advanced Threat Prevention Appliance