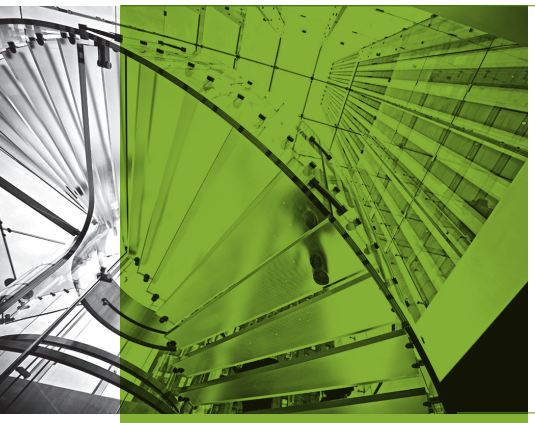

UNCOVER AND MITIGATE THE MOST SOPHISTICATED CYBER ATTACKS

The Power of Threat Intelligence Sharing: Juniper ATP Cloud and Carbon Black Cb Response

Challenge

Today's rapidly evolving threat landscape is outpacing the abilities of many security solutions. The increasing volume of threat data, combined with a lack of data correlation, means businesses have limited protection across advanced threat vectors.

Solution

When integrated with Carbon Black Cb Response, Juniper ATP Cloud offers a cloud-based malware defense service that effectively protects enterprise networks and endpoints from the most destructive, hard to detect attacks by identifying and blocking lateral threat propagation from compromised hosts.

Benefits

- *Quickly detect attacks in progress and respond immediately*
- *Prevent lateral threat propagation from compromised hosts*
- *Gain rich APIs and modern threat intelligence sharing capabilities*

Businesses moving their network infrastructures and applications to distributed multicloud architectures are facing a growing number of increasingly sophisticated cyber attacks sponsored by organized, well-funded hacking groups. This trend, combined with limited visibility beyond the perimeter and a lack of data correlation between network, servers, and endpoints, means the tools used to find and eradicate these advanced threats and malware must adapt and get smarter.

Juniper Advanced Threat Prevention Cloud uses real-time information from the cloud to defend your business against malware and sophisticated cyber attacks such as advanced persistent threats and ransomware. Juniper ATP Cloud is designed from the ground up to address the most sophisticated threats with a rich set of APIs and the ability to consume threat intelligence from multiple resources.

When hunting for threats, enterprises also need a solution that can "roll back the tape" to understand an attack's root cause. Working together, Juniper ATP Cloud and Carbon Black Cb Response hunt for threats, accelerate threat discovery, respond in seconds when a threat is discovered, and proactively prepare businesses for a breach. By adopting the latest technologies and an open integration ecosystem, you can reduce the risk to your business and align security with your organization's key initiatives.

The Challenge

The rapid growth of emerging technologies, combined with an increasing number of connected devices running business-critical applications in highly distributed environments, is producing an unprecedented amount of security event data. Having the right tools in place is critical for quickly detecting and mitigating threats. The ability to recognize advanced threats across the network, quickly share threat intelligence, and take immediate remedial action is an absolute requirement for security teams to keep their environments safe.

The Juniper ATP Cloud and Carbon Black Solution

Through its comprehensive open APIs, Juniper ATP Cloud shares threat intelligence with Carbon Black Cb Response to deliver a comprehensive, cloud-based, dynamic anti-malware solution that is tightly integrated with Juniper Connected Security. This joint solution quickly correlates threat intelligence, identifies unknown threats, and blocks impending attacks.

Because today's highly mobile workforce frequently resides outside the corporate network, the endpoint has become a highly targeted attack point. Hackers employ compromised endpoints to move laterally throughout an organization, gaining access to critical assets in order to disrupt operations.

Juniper ATP Cloud maintains a list of compromised endpoints as data feeds (also called information sources) that include the IP address or IP subnet of the infected host, along with a threat level and recommended action. You can create security policies that automatically perform enforcement actions on traffic entering or leaving these infected hosts. Juniper ATP Cloud uses multiple indicators of suspicious behavior, such as a client attempting to contact a Command and Control (C&C) server or a client attempting to download malware, and applies a proprietary algorithm to determine the infected host's threat level.

When integrated with Carbon Black, Juniper ATP Cloud allows security teams to share threat intelligence between the two platforms, improving your security posture by identifying infected hosts across the network and allowing you to proactively hunt advanced threats, detect attacks, and investigate and respond immediately.

The following section describes the various solution components and explores two key use cases for Juniper ATP Cloud integrated with Carbon Black Cb Response.

Solution Components

Carbon Black Cb Response

Carbon Black Cb Response, purpose-built for enterprise security operations center (SOC) and incident response (IR) teams, can run on-premises or in the cloud. It offers a streamlined UI built for speed, unlimited historical data retention, and unlimited scaling, enabling it to support even the largest enterprises. Cb Response proactively discovers the most advanced threats that make it past your defenses, leveraging open APIs to integrate with Juniper ATP Cloud for automatic threat remediation. Cb Response includes the following key components:

- Threat Intelligence Feeds
  - Preconfigured threat intelligence feeds contain threat intelligence data and come from various sources, including Carbon Cb, Cb customers, open-source feeds, and Cb partners such as Juniper ATP Cloud.
  - Cb threat intelligence feeds provide a list of Indicators of Compromise (IOCs) and contextual information based on binary/process attributes and events. These attributes and events are scored, rated, and correlated with matching files in the customer environment. Threat intelligence feeds from third parties such as Juniper Networks can be enabled from the Cb Dashboard under the Threat Intelligence Feed page.
  - The Cb Response 6.1+ server supports the following types of indicators: Binary Message Digest 5s (MD5s), IPv4 addresses, Domain Name System (DNS) names, process queries (searches), binary queries (searches), and IPv6 addresses.
  - The IOCs contained in the feeds are compared to the sensor data as it arrives on the Cb Response server. Any activity matching an IOC is tagged; users can search for the tags and, optionally, register for e-mail alerts.
- Watchlists
  - Watchlists are fully customizable saved searches. They are visible to all users and contain lists used to track specific IOCs. Watchlists can be used to search either processes or binary executable files.
- Alerts and Log to Syslog
  - For each watchlist, you can generate alerts and/or send the logs to a system logging server. Alerts are generated when conditions matching the watchlist occur. Triggered alerts are reported on the Alert Dashboard page and the Triage Alerts page. Enabling Log to Syslog records all hits that match the search in a specific watchlist.

Cb Sensor

The Cb Sensor is installed on endpoint devices, where it continuously captures unfiltered data and analyzes each event stream in context to uncover emerging attacks that other solutions miss. The Cb Sensor then sends this information to the Cb Response server for analysis.

Because the Cb Sensor is always on and collecting, it records and stores the complete data record of every endpoint, even if it is offline. A Cb Response query determines the responsible host, the process, and all activity related to that process, allowing you to visualize every stage of the attack.

Carbon Black TAXII Connector

The Carbon Black TAXII Connector retrieves and converts Structured Threat Information Expression (STIX) information from the TAXII server on Juniper ATP Cloud into Cb Feeds. The connector can be downloaded at https://github.com/carbonblack/cb-taxii-connector.

STIX and TAXII: The STIX provides a formal way to describe threat intelligence, while TAXII (client/server) provides a method for delivering that intelligence—a free and open transport mechanism that standardizes the automated exchange of cyber threat information. To learn more about STIX and TAXII, visit https://oasis-open.github.io/cti-documentation.

Juniper Cloud Advanced Threat Prevention

Juniper ATP Cloud is a service provided by Juniper on its Juniper Networks® SRX Series Services Gateways to assist in the detection and remediation of advanced threats. Juniper ATP Cloud includes several service elements, including malware detection, C&C identification, infected hosts remediation, and geographic IP (GeoIP) control. Integrated with SRX Series Services Gateways, Juniper ATP Cloud delivers a dynamic anti-malware solution that adapts to an ever-changing threat landscape. To learn more about Juniper ATP products, visit www.juniper.net/us/en/products-services/security/advanced-threat-prevention/.

Juniper ATP Cloud Connector

The Juniper ATP Cloud Connector, installed on the Cb Response server, is configured to monitor one or more watchlists. The watchlists on a Cb Response server are created to match specific criteria. The Juniper ATP Cloud Connector submits infected host IPs detected by Cb Response to the Juniper ATP Cloud infected hosts database. Download the Juniper ATP Cloud connector at https://github.com/carbonblack/cb-skyatp-connector.

SRX Series/vSRX Next-Generation Firewall Services

SRX Series physical gateways and the next-generation vSRX Virtual Firewall services provide an array of cyber defenses to reduce your attack surface. With the SRX Series/vSRX firewalls at their foundation, Juniper Next-Generation Firewall Services allow the safe operation of critical applications, preventing advanced malware from entering your network. Available on all SRX Series/vSRX platforms, NGFW Services stop cyber criminals before they can breach your organization's defenses.

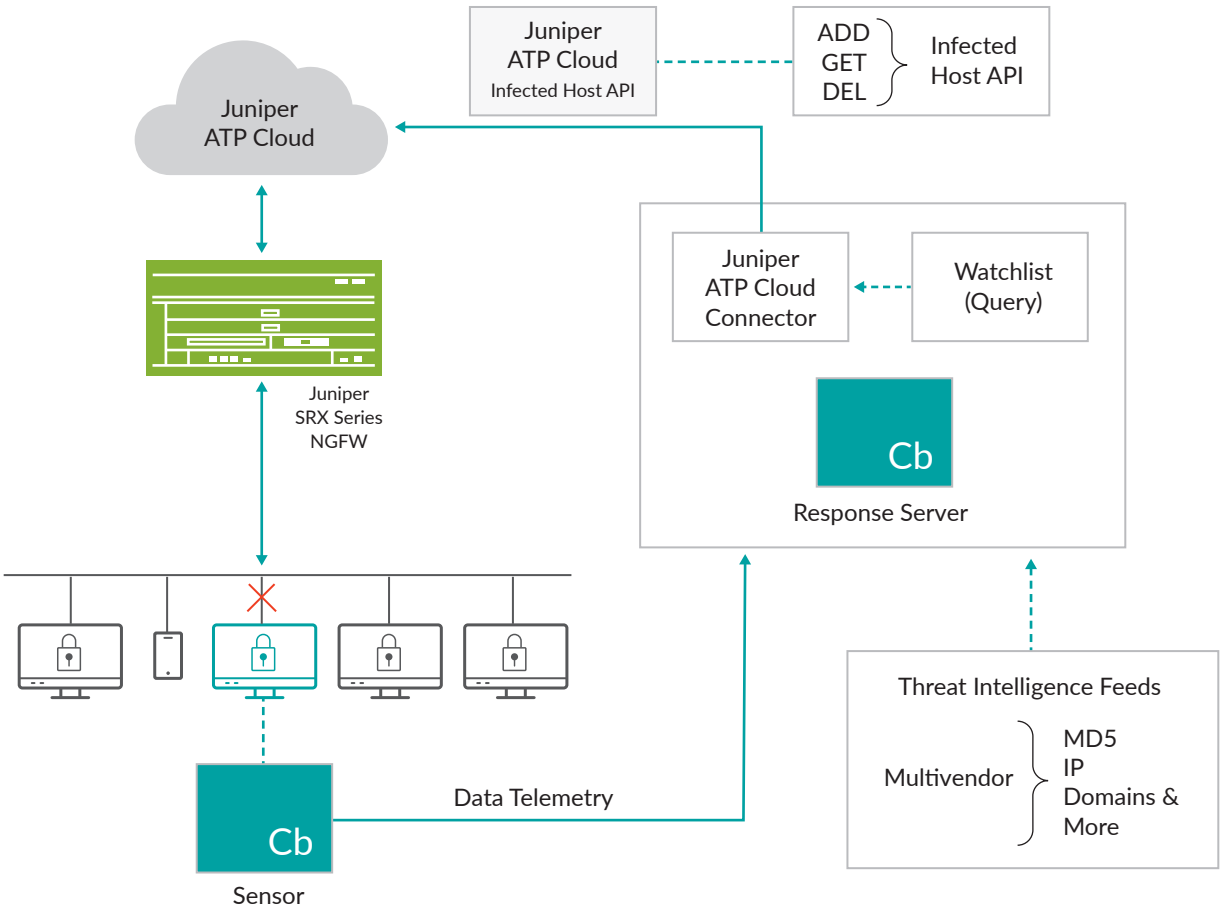

Figure 1: Juniper ATP Cloud and Carbon Black Cb Integration—infected host feed

To learn more about SRX Series/vSRX NGFW services, please visit www.juniper.net/us/en/products-services/security/next-generation-firewall-services.

Use Cases

Identify and Block Compromised Hosts: Juniper ATP Cloud Receives Threat Intelligence from Carbon Black to Protect Users

Juniper ATP Cloud's rich set of APIs and integration ecosystem can automate the ingestion of threat intelligence and IOCs from multiple resources, including Carbon Black Cb Response, to uncover the most sophisticated attacks.

Cb Response continuously monitors and records all activity on servers and endpoints to detect and stop cyber threats that evade traditional security defenses. It identifies compromised endpoint devices and shares infected host information with Juniper ATP Cloud for threat remediation.

Threat intelligence imported by Juniper ATP Cloud from Carbon Black is automatically ingested and distributed to Juniper Policy Enforcer, enabling enforcement on SRX Series/vSRX NGFWs and third-party switches. This allows enterprises to quickly identify unknown threats and block impending attacks.

Required components:

- Carbon Black Cb Response
- Carbon Black Cb Sensor
- Carbon Black Cb Response Juniper ATP Cloud Connector
- Juniper ATP Cloud
- SRX Series/vSRX NGFWs

Key benefits:

- Quickly detect attacks in progress and respond immediately
- Deploy a commit-less, dynamic, automated workflow
- Gain complete endpoint visibility

Use Case 1 Workflow

Infected host IP is identified on Carbon Black Cb Response server	1. Cb Sensor is installed on the endpoint and observes malicious endpoint behavior. The endpoint data/telemetry is sent to the Cb Response server for analysis. 2. The Cb Response server receives IOCs from one or more configured threat intelligence feeds. 3. The Cb Response server compares endpoint "Process" and "Binary" activities against these threat intelligence feeds (Cb-owned and third-party). 4. When a monitored watchlist is matched on the Cb Response server, an alert is triggered based on the enabled alerts for a specific watchlist. Note: • You can create one or more watchlists for each IOC feed. • You can enable or disable alerts for each IOC feed.
Cb Response server sends infected host IP to Juniper ATP Cloud	1. Juniper ATP Cloud Connector on the Cb Response server is configured to continuously monitor existing alerts on CB Response server. 2. When a new alert is triggered from a watchlist (meaning there is a specific IOC feed that matches the endpoint data), the Juniper ATP Cloud Connector will collect the infected host IP from the Cb Response server and call the Juniper Infected Host API to pass the IP to Juniper ATP Cloud.
Infected host IPs are added to Juniper ATP Cloud	• Juniper ATP Cloud adds the received infected host IP(s) to the infected host feed.
Juniper ATP Cloud updates network enforcement elements	• The infected host IPs are pulled into the SRX Series firewalls in near real time.
SRX Series firewalls and Policy Enforcer isolate the infected host	• Infected host feeds pass from Juniper ATP Cloud cloud to the SRX Series firewalls. • SRX Series firewalls block traffic from infected hosts.
Infected host IP is removed from the Juniper ATP Cloud infected host database when the issue is resolved	• As alerts generated from the watchlists are marked as resolved on the Carbon Black Cb Response server dashboard, the Cb Juniper ATP Cloud Connector will remove the host from the blacklist/infected hosts feed from the Juniper ATP Cloud IH database. • The SRX Series firewalls are updated to unblock the previously isolated endpoint.

Threat Intelligence Sharing and Remediation: Cb Response Receives Threat Intelligence Feed (IOCs) from Juniper ATP Cloud to Detect and Investigate Infected Endpoints Across the Network.

Juniper ATP Cloud shares threat intelligence in STIX format over TAXII. Carbon Black Cb Response has the ability to pull feeds from multiple sources, including Juniper ATP Cloud. In this integration, the TAXII service running on Juniper ATP Cloud is configured to share threat intelligence when a threat threshold set on Juniper ATP Cloud is exceeded. The indicators of compromise (IOCs) contained in this feed can be compared to sensor data as it arrives via the Cb Response server. Matching IOCs are tagged and can be added to watchlists to identify other compromised hosts.

Required components:

- Carbon Black Cb Response
- Carbon Black Cb Sensor
- Carbon Black TAXII Connector
- Juniper ATP Cloud
- SRX Series/vSRX NGFW services

Key benefits:

- Utilize shared threat intelligence to identify infected hosts and protect endpoint devices
- Gain visibility into all endpoints and identify compromised hosts across your network
- Identify and prevent malware spread and lateral threat propagation from compromised hosts

Use Case 2 Workflow

Juniper ATP Cloud analyzes files for malware and generates a STIX report when threats are detected	• The IOCs are packaged in the STIX format. The STIX package is accessible via the TAXII service on Juniper ATP Cloud. It is also downloadable on the Juniper ATP Cloud management UI.
TAXII Connector downloads a STIX threat report from TAXII server	• Cb TAXII Connector runs on the Cb Response server and is configured to connect to the TAXII service on the Juniper ATP Cloud. Cb TAXII Connector downloads the STIX report for the latest detected threats every few minutes (the interval is configurable). • The MD5, IP, and domain are the supported IOCs.
Solution identifies infected (host) end-point	**Identify infected endpoint:** • Carbon Black Cb Response server compares threats from the STIX report with the data received from the endpoint devices. If there is a match, it means that another endpoint within the network is infected with the same malware. **Identify lateral propagation of malware:** • If the malware has reached other endpoint devices and other endpoints are infected, the joint Juniper ATP Cloud and Cb Response solution will detect them all.
Users react to and investigate compromised host	**Generate alerts from previously created watchlists:** 1. Cb Sensor observes malicious endpoint behavior and sends data/telemetry to Cb Response for analysis. 2. Cb Response receives IOCs from one or more configured threat intelligence feeds. 3. Cb Response server compares endpoint “process” and “binary” activities against these threat intelligence feeds (Carbon Black-owned and third-party). 4. When a monitored watchlist is matched on Cb Response, an alert is triggered based on the enabled alerts for a specific whitelist. **Manual investigation:** • There is also an option to review a specific IOC feed manually from the Cb Response dashboard. From the dashboard, you will be able to trace host behavior and determine whether there is a potential threat on the endpoint—for example, you can see process calls, file changes, registry changes, etc.
Organization takes action	• From the results of the investigation, an alert can be cleared, or the endpoint can be banned (hash) or completely isolated.

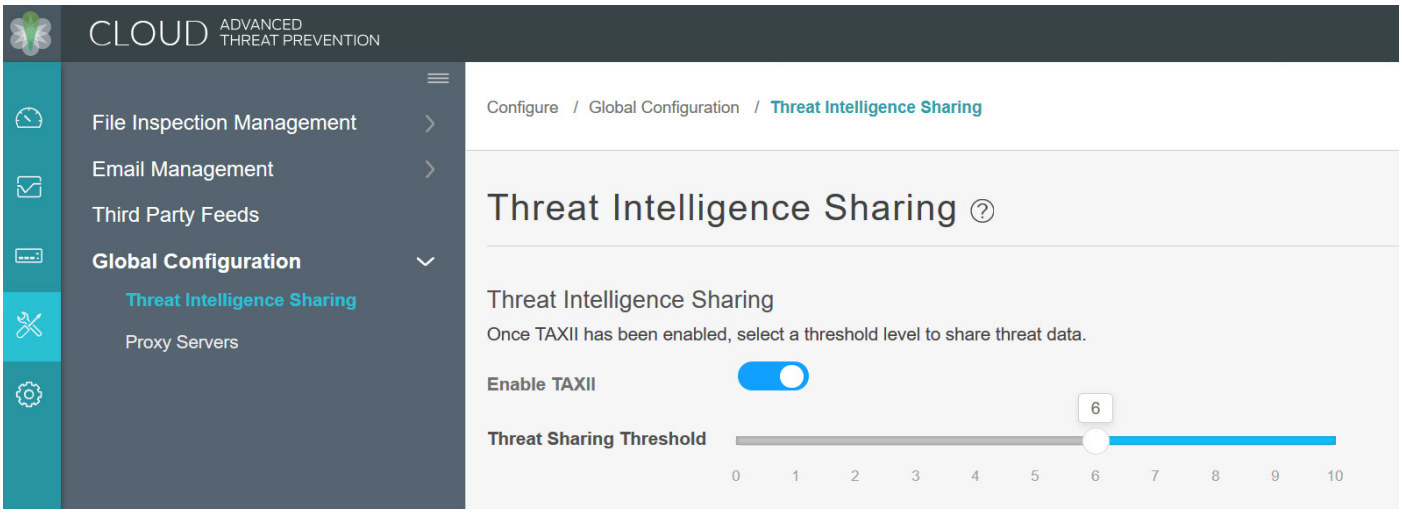

Figure 2: Juniper ATP Cloud enables Threat Intelligence Sharing (TAXII)

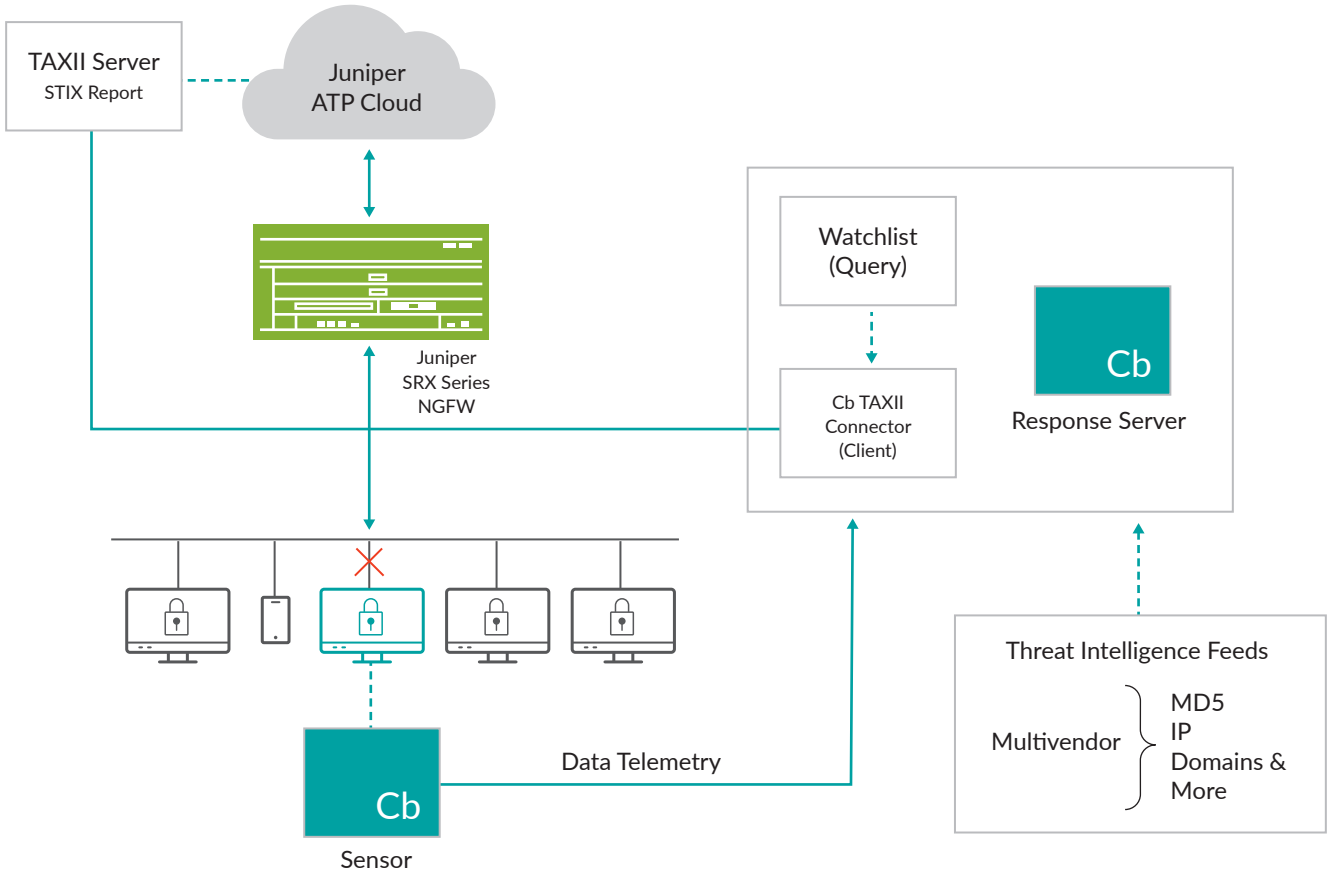

Figure 3: Juniper ATP Cloud and Carbon Black Cb integration—Threat Intelligence Sharing (STIX/TAXII)

Summary—Quickly Correlate and Identify Unknown Threats to Block Impending Attacks

Juniper ATP Cloud and its integration with Carbon Black Cb Response offers a cloud-based malware defense service that effectively protects enterprises from the most destructive, hard to detect attacks, as well as detecting and blocking lateral threat propagation from compromised hosts. This level of protection is crucial; firewalls, antivirus, and other traditional security solutions are simply not designed to defeat unknown and hyper-evasive exploits used by criminals. The joint solution brings together advanced detection, analytics, and mitigation techniques to deliver truly advanced methods for preventing these breaches to secure the network from known compromised hosts at the edge and at the access layer.

Next Steps

For more information about Juniper Networks security solutions, please visit www.juniper.net/us/en/products-services/security and contact your Juniper Networks representative.

About Carbon Black

Leveraging its newly introduced big data and analytics cloud platform, the Cb Predictive Security Cloud, Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus. To learn more, visit www.carbonblack.com.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701