JUNIPER ADVANCED THREAT PREVENTION CLOUD SERVICES DESCRIPTION

Introduction

This Cloud Service Description ("CSD") describes Juniper Advanced Threat Prevention ("ATP") Cloud and the Juniper Care Software Advantage Services offering that is included with the Cloud Services ("Support Services") that Juniper Networks, Inc. ("Juniper") makes available as part of the Cloud Service Subscription for customers of Juniper products ("Customer") directly or through its authorized resellers. This CSD governs your purchased subscription to a Cloud Service as defined under the Juniper Purchase and License Agreement posted at https://www.juniper.net/us/en/legal-notices/juniper-networks-contracts-resource.html (or another written master services agreement signed by Juniper and the End User and covering within its scope, the terms and conditions under which Juniper will render support and maintenance services) (the "Master Agreement"). Capitalized terms used in this CSD, not otherwise defined herein, have the meaning given to them in the Master Agreement.

The Support Services are subject to the terms of this CSD and the Master Agreement.

If applicable to the Cloud Services, all license terms for Software provided by Juniper as part of the Cloud Services are subject to the Master Agreement.

The Terms of Service for Support API provided by Juniper as part of the Cloud Services are subject to the Juniper Support API Terms of Service, and a copy is posted at: https://support.juniper.net/support/legal/supportapitos (the "TOS").

In the event of any conflict between the terms of this CSD and those of the Master Agreement or TOS, the terms of the Master Agreement and TOS shall take precedence.

Cloud Service Description

Juniper Networks® Advanced Threat Prevention Cloud (ATP Cloud) is a cloud-based service providing complete malware detection and advanced threat prevention. When integrated with SRX Series Firewalls, Juniper ATP Cloud delivers threat intelligence and malware analysis capabilities leveraging static and dynamic analysis and machine learning identification to safeguard your users, data, and infrastructure.

Juniper ATP Cloud is the threat intelligence hub for the network with a litany of built-in advanced threat services that use the power of AI and ML to detect attacks and optimize enforcement. Juniper ATP Cloud finds and blocks commodity and zero-day malware within files, IP traffic, and DNS requests. The service assesses risk from encrypted and decrypted network traffic and connecting devices, including IoT, and distributes that intelligence throughout the network to stop attacks and drastically decrease the attack surface before a breach occurs.

Juniper ATP Cloud delivers SecIntel security intelligence consisting of malicious domains, URLs, and IP addresses gathered from file analysis, Juniper Threat Labs research, and highly reputable third-party threat feeds. Juniper ATP Cloud includes its own management portal configuration management, licensing, and reporting.

For purposes of clarity, all referenced Juniper Hardware or Software must be purchased and/or licensed separately.

ATP Cloud Data Licensing Entitlements and Fair Use

ATP Cloud can be purchased as a subscription license and is included as part of Juniper FLEX software licensing model. Licensing is term based and can be purchased for one (1), three (3), and five (5)-year terms. For ease-of-use, Juniper FLEX software licensing is available with Advanced or Premium software features. ATP Cloud delivers security intelligence ("SecIntel") and ATP Cloud are sold as part of the Advanced and Premium bundles, respectively. The Advanced and Premium bundles are as follows:

SRX license model	License Tier	Use Case	Detailed Features
Advanced	Advanced 1	DC Security	Application Security, IDP and SecIntel
	Advanced 2	DC Security + UTM	Advanced 1 + Cloud AV/AS + URL Filtering
	Advanced 3	DC Security + UTM (on-box AV)	Advanced 1 + On-box AV/AS + URL Filtering
Premium (Advanced + ATP Cloud)	Premium 1	DC Security + ATP	Advanced 1 + ATP Cloud
	Premium 2	DC Security + UTM + ATP	Advanced 2 + ATP Cloud
	Premium 3	DC Security + UTM (on-box AV) + ATP	Advanced 3 + ATP Cloud

Data Protection and Security

In this CSD, "Customer Data" shall mean all information submitted by the Customer to Juniper and may include third-party data that the Customer submits to Juniper. "Processed Data" shall mean information about Customer's devices or systems in connection with Customer's usage of Juniper products and services, as well as any network management information or configuration data from the use of Customer's Processed Data.

Juniper shall maintain appropriate administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of Customer Data.

In accordance with the Customer's use of the Cloud Service, the categories of personal data that may be processed are as set forth in the Juniper Privacy Notice available at: https://www.juniper.net/us/en/privacy-policy together with any Supplemental Privacy Information referenced therein, which includes Juniper's collection and use of network device logs configured by the Customer, such as the metadata from managed devices (e.g., IP address of source and destination, accessed applications, or websites).

Juniper ATP Cloud logs of inspected files may contain the following metadata: Client Host, Client IP Address, File name, Username (if User Firewall is turned on), Vendor or creator, Date/time submitted, URL, and Device name. Juniper ATP Cloud also logs command-and-control (C&C) events that have been detected, which may include: Client Host, Client IP address, IP address or URL of the C&C server, Date/time detected, and Website certificates. If the Customer configures ATP Cloud to quarantine emails, ATP Cloud may also process email data as described in the Supplemental Privacy Information available in the Juniper Privacy Notice.

Data Ownership

Customer retains ownership of Customer Data. In connection with the Customer's use of the Cloud Service, Juniper collects and uses Processed Data in accordance with the Juniper Privacy Notice. Juniper uses Processed Data to enable, optimize, and provide the Cloud Services and support to the Customer and to improve Juniper Cloud Services in general, including, but not limited to, integrating such Processed Data on an anonymized basis into our Cloud Services. By using the Cloud Service, Customer agrees to allow Juniper to use and collect Customer Data to generate Processed Data as defined in this CSD.

Data Location

Juniper ATP Cloud locations are built and hosted in top-tier data centers to meet the hosting location requirements of ATP Cloud customers. Locations are globally located in regions most typically required by Juniper ATP Cloud customers.

This widespread availability allows customers in these regions to benefit from the cloud-based threat prevention and intelligence services while addressing customers' data localization and data privacy concerns. Data submitted in a particular region will be processed in that region and will not leave its geographic boundaries. Customers have greater control over the location of the data, helping them comply with regulatory and privacy requirements.

Juniper personnel who are granted access to network management data or a Cloud Service instance may be in regions outside of the EU where data privacy and data protection laws may differ. Nonetheless, Juniper has established standard information security policies and practices that apply globally to all Juniper locations.

Data Retention

User-specific configuration and device log data — including access, network management, and service data — are stored in one or more Juniper cloud locations for the length of the subscription term (either non-commercial or commercial subscription) or as otherwise configured by Customer. Juniper ATP Cloud retains inspected files for a 60-day period in order to correlate events over time and determine which machines or hosts may be compromised or infected. When a trial subscription ends, all Customer data associated with the Cloud Service will be deleted within sixty (60) days, if the Customer does not explicitly delete such data by then.

Encryption of Data

Industry-standard encryption is utilized for the Cloud Service web interface, data communications across the service instances, data at rest, and passwords.

- Communication between customers and the Cloud Service web interface use HTTPS connections.
- Data at rest, including passwords, is protected by database storage with AES-256.

Access Controls

Access authentication and authorization can be configured using the native Role-Based Administrative capability of ATP Cloud.

Juniper provides the following access controls and restrictions to Customers:

i. Customer access restrictions and controls:
   - Customer access to the Cloud Service is based on the role assigned by the Customer.
   - Customer can leverage predefined roles or define customized roles.

ii. The Cloud Service access restrictions and controls:
   - The Cloud Service access to Customer network management data is restricted based on role or customer-granted permission.
   - Access is logged.

Security Incident Response Team (SIRT)

Juniper's Security Incident Response Team (SIRT) manages vulnerability reports and provides support for security incidents. SIRT works with the Operational Security Community, other SIRT Teams, and Customers to maintain situational awareness of threats. This information is processed and communicated to the larger SIRT Teams and Customers. To report a Potential Security Vulnerability, refer to: http://www.juniper.net/us/en/security/report-vulnerability.

Cloud Environment and Security

Servers are hosted in ISO 27001-certified data centers, which also provide SOC 2 attestation reports over their security controls and across multiple availability zones. All servers are hardened per best practices. Servers are hosted at AWS with security groups enabled. Only the required ports are opened on front-end servers. The Cloud Service is developed and maintained following Juniper Secure Development Lifecycle practices.

Security Testing

Juniper performs web security testing from development through production. Juniper periodically scans for SQL injections, cross-site scripting (XSS), and more than 700 other vulnerabilities, including the OWASP Top 10.

SLA/Performance Measures and Reporting

Cloud Service Resiliency

By leveraging the public cloud, the infrastructure components and services of the Cloud Service are deployed redundantly (across AWS clusters and zones) in an effort to provide 24 x 7 availability. In addition, the Cloud Service is divided into microservices, so issues with one microservice do not directly affect other microservices. The Cloud Service buffers data in the event of a component disaster, such as the loss of backend microservice. Once the disaster has been addressed, the data is replayed to fill in the lost analytics. System upgrades and feature introductions also benefit from microservices to avoid impact to the Cloud Service when performing either. This reduces the need for planned downtime. The Cloud Service has a scheduled downtime during the release upgrade, and Customers are notified 48 hours in advance of any such downtime. Minor updates and patches can be performed without any downtime.

Availability

Juniper Networks will use commercially reasonable efforts to make the Cloud Services fully available and operable over the internet in full conformity with the Cloud Service specifications for access and use by Customer, as measured over the course of each calendar month, an average of 99.99% of the time, calculated as follows:

$$\left[\left(\frac{total - nonexcluded - excluded}{total - excluded}\right) * 100\right] \geq \text{Available \%}$$

Where:

“total” means the total number of minutes in the calendar month; “nonexcluded” means downtime that is not excluded; and “excluded” means any planned downtime of which Juniper gives three business days or more written notice via email or banner on the Cloud Service dashboard. All scheduled maintenance work and planned downtime will be during the hours from 7:00 p.m. PST to 7:00 a.m. PST on any day. Planned downtime is not expected to occur more than once or twice per year and is not expected to exceed 120 minutes in any given month.

Note that availability of the ATP Cloud service means the service is available to accept Customer files for scanning and threat data from CPE (customer premise equipment) and Customer has properly configured its CPE to leverage ATP Clouds services.

Support Services Eligibility

A Subscription to a Cloud Service (as defined in the Master Agreement) purchased by the Customer shall be treated as a Juniper Care Software Advantage Support Services contract (the “Support Service”) for purposes of this CSD. The Support Service is available only to qualified Customers who have purchased the subscription for their own use. The Cloud Service will be supported only for the duration of the Subscription Term. In addition, if a Juniper Networks device is managed by the Cloud Service, then the Juniper device must be under an active support contract.

Support Services Features and Deliverables

Juniper will use commercially reasonable efforts to provide the Customer with Support Services. The Support Services may include access to Juniper's technical support engineers, software releases, and online tools.

JTAC Access

With Juniper Networks Technical Assistance Center (JTAC) support, the Customer will have unlimited access to JTAC engineers by phone and online 24/7/365. JTAC engineers will help diagnose system problems, configure, troubleshoot, and provide workaround solutions where necessary.

For details on the JTAC support center structure, how to access JTAC support, JTAC response time guidelines, problem reporting and escalation procedures, case workflow, and customer communication guidelines, please refer to the JTAC User Guide at https://www.juniper.net/content/dam/www/assets/resource-guides/us/en/jtac-user-guide.pdf.

Online Support

During the term of the Juniper Service Contract, Juniper provides the Customer with self-service access to the Juniper Customer Service Center (CSC) online portal, which provides information, answers, tools, and service options for the Customer's use in supporting the Cloud Service. Offerings include, but are not limited to:

- Online case management: create new cases, check the status of existing cases, update cases with new information, and search by case numbers, RMA numbers, and the Customer's own internal case reference numbers.
- Juniper Knowledge Center: the ability to search thousands of articles, including configuration assistance, known issues, interoperability, and compatibility information.
- Problem Report (PR) Search: the ability to access the most complete and up-to-date information about known Juniper's operating system defects. This tool allows you to search for defects by PR number, Junos OS release version, and keyword, providing upgrade analysis and impact information. The Customer can also subscribe to PRs of interest in order to receive automated updates as specific PRs change.
- Online Tools: various tools to help analyze hardware and software information, such as the configuration tool, translator, migration tool, etc.
- Technical Bulletins: timely notification on new features release, end of life, known product issues, etc.
- Security Advisories: provide known security vulnerability issues to help avoid network impact.

The use of online tools is subject to the following:

- Customers shall have personal, non-transferable, non-sublicensable, nonexclusive access during the term of the Support Services to Juniper's online Customer Support Center (CSC), subject to limited use terms posted at such site, all solely for the Customer's internal use in support of Juniper's product covered under Juniper's Service Contract.
- Customers shall maintain an active subscription contract to access resources on CSC related to the Cloud Service. Customers are not entitled to access CSC resources for any products that are not covered by an active Juniper support contract.

Juniper reserves the right in its discretion to limit or prohibit any Customer access if Juniper it believes that such access may give rise to a violation of export control laws, regulations, or any other violation of Juniper's rules or the limited use terms identified above.

Customer Responsibilities

For any Problem identified as a Priority 1 Problem, the Customer will provide Juniper or its authorized service representative access to the affected network environment, if required, and will assign a technical contact for Juniper. Furthermore, if Juniper determines that its technical personnel need access to the Customer's network to remotely diagnose a problem, the Customer will ensure that Juniper's personnel have the necessary level of authorized access to such network. Customer shall have the right to observe such access.

- Customer shall maintain a reasonable number of support engineers who are trained on Juniper's Products.
- All communication to Juniper's engineers of customer issues and responses will be conducted in English.
- Customer shall inform Juniper about the role changes or resignation of its support engineers so that the Customer's individual CSC accounts can be modified/deactivated as needed.
- Customer shall provide access to servers, equipment, information, logs, infrastructure, and resources necessary to deliver the service.
- Customer shall advise Juniper of any Information Juniper may reasonably request about the execution of the Services throughout the delivery of Services. If third-party participation and cooperation are required for the Customer to perform the Customer responsibilities, the Customer shall be responsible for getting such participation and cooperation.
- Customer shall provide written notice to Juniper as soon as it becomes clear or there is reason to believe that the Customer will not meet any of the Customer responsibilities.

Compliance with Laws — Export Requirements

Customer shall comply with all applicable laws and regulations and with all terms of the Export Note incorporated in the Shipping Terms Exhibit posted at https://www.juniper.net/Shipping-Terms-Exhibit. Customer warrants that it has no knowledge or reason to believe that it has received any Juniper product through any export or re-export in violation of the U.S. or other applicable laws or regulations, that it is not a Sanctioned Party (as that term is defined in the Export Note), that no Juniper product or Cloud Service is located in or controlled from a site in a Group E country (Belarus, Cuba, Iran, North Korea, Syria, the region of Crimea, Russia, and the oblasts of Luhansk and Donetsk), and that it is not using any product or Cloud Service to support activities in support of development, manufacture, or use of nuclear fuel or weapons, missiles, or chemical or biological weapons or other prohibited uses as that term is defined in the Export Note. Customer further covenants that it will immediately notify Juniper if at any time such warranties and representation become no longer accurate at such time. Regardless of any disclosure made by the Customer to Juniper of an ultimate destination of the Products. Customer will not export, either directly or indirectly, any Juniper products or Cloud Service without first obtaining any and all necessary approvals from the competent government authorities administering the U.S. and other applicable country export controls. Customer understands and agrees that Juniper may impose certain restrictions on services described herein to avoid violations of export control laws.

Availability

These Support Services are available where they can lawfully be sold and subject to applicable limitations posted by Juniper Global Support Operations on the Juniper website or the Juniper price list; Support Services are available with a Subscription for a minimum fixed duration of twelve (12) months.

Scope

Support Services shall be delivered remotely from an authorized Juniper Networks location unless specified otherwise.

All service deliverables in this offering are available in English only unless otherwise specified by Juniper.

Juniper's obligation to perform any particular Support Services hereunder is contingent upon Juniper receiving from the Customer such cooperation, network access, consents, information, and materials that Juniper may reasonably request to enable Juniper's' proper and efficient performance of such Support Services and to enable Juniper to do so in compliance with all applicable laws and regulations.

Exclusions

Juniper is not obligated to provide Support Services for any of the following:

- Third-party devices (hardware, software cabling, etc.) not provided by Juniper or problems associated with or arising directly or indirectly from such components;
- Problems with a Cloud Service that have been modified without Juniper's written consent by any person (including unauthorized modifications by Support Services Specialist);
- Problems relating to the incompatibility of the Cloud Service with third-party devices;
- Problems caused by the use of the Cloud Service other than in accordance with applicable documentation;
- Problems with the Cloud Service where Customer did not provide the required information;
- Problems caused by the misuse of the Cloud Service generally;
- Problems with Software used in connection with a Cloud Service that is not a supported release;
- Problems with a cloud-managed hardware device that is not compatible nor under a supported release of the Cloud Service.

About Juniper Networks

At Juniper, we are dedicated to dramatically simplifying network operations and driving superior experiences for customers. Our solutions deliver industry-leading insight, automation, security, and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability, and equality.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 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