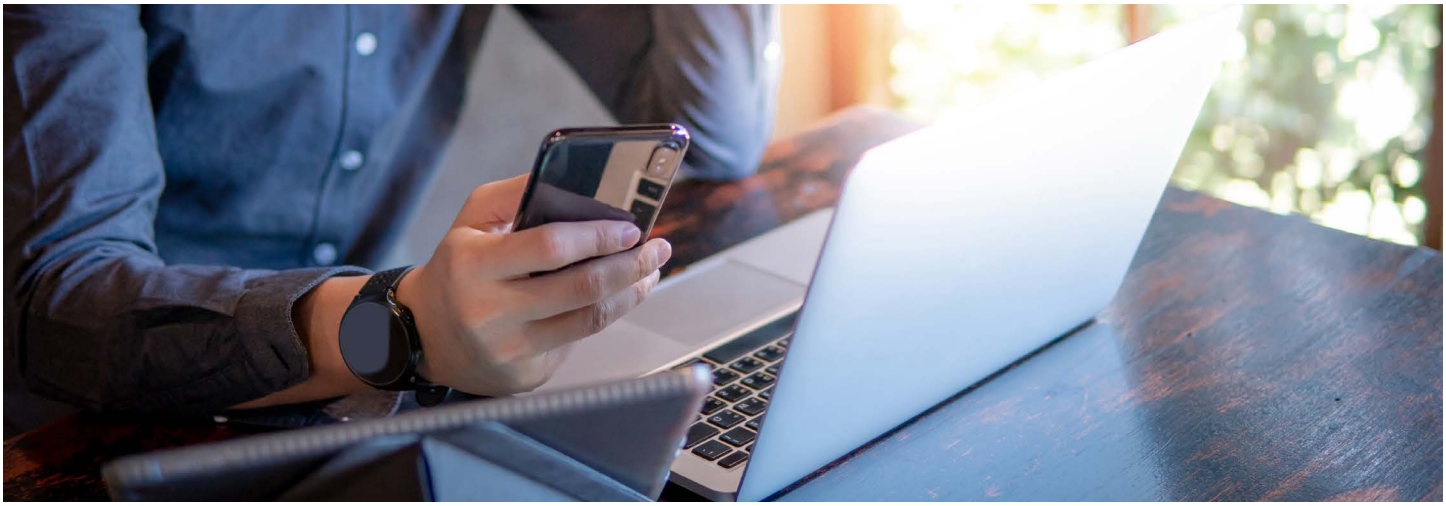
PRIVACY AND SECURITY: AI-DRIVEN TRUST



Today's digital transformation is spearheaded by the proliferation of mobile devices and applications, increasing penetration of IoT and rapid adoption of cloud services. The principles of market competition often described by the big eating the small has been replaced by the fast beating the slow with technology as a catalyst. Along with faster processors and advances in big data, artificial intelligence's (AI) impact on todays IT initiatives is becoming core to the company's success as the demand of synthesizing, processing and analyzing large data sets continue to increase along with the resources to automate the recommended actions.

Juniper Networks, driven by Mist AI™, delivers an AI-driven enterprise solution deployed across four of the Fortune 10, 25+ of the Fortune 500, and ten of the top 40 retailers, a validation of IT's growing dependence on AI today. These leading companies rely on the Juniper Mist™ Cloud Architecture to deliver predictable, reliable, and secure networking services with Mist AI across the WLAN, LAN, WAN, and security to meet the challenging management and performance requirements for their digital transformation.

With Juniper, you gain the speed, experience, expertise, and reliability that has been synonymous with networking innovations. Juniper's trust philosophy on AI and its modern cloud-based architecture is inherent across its solution portfolio as the effectiveness of AI is heavily dependent on good quality data. Thus, Juniper treats data security, integrity, and privacy as our highest priority obligation to our Customers. For additional information on our commitment to privacy, see our Privacy Policy.

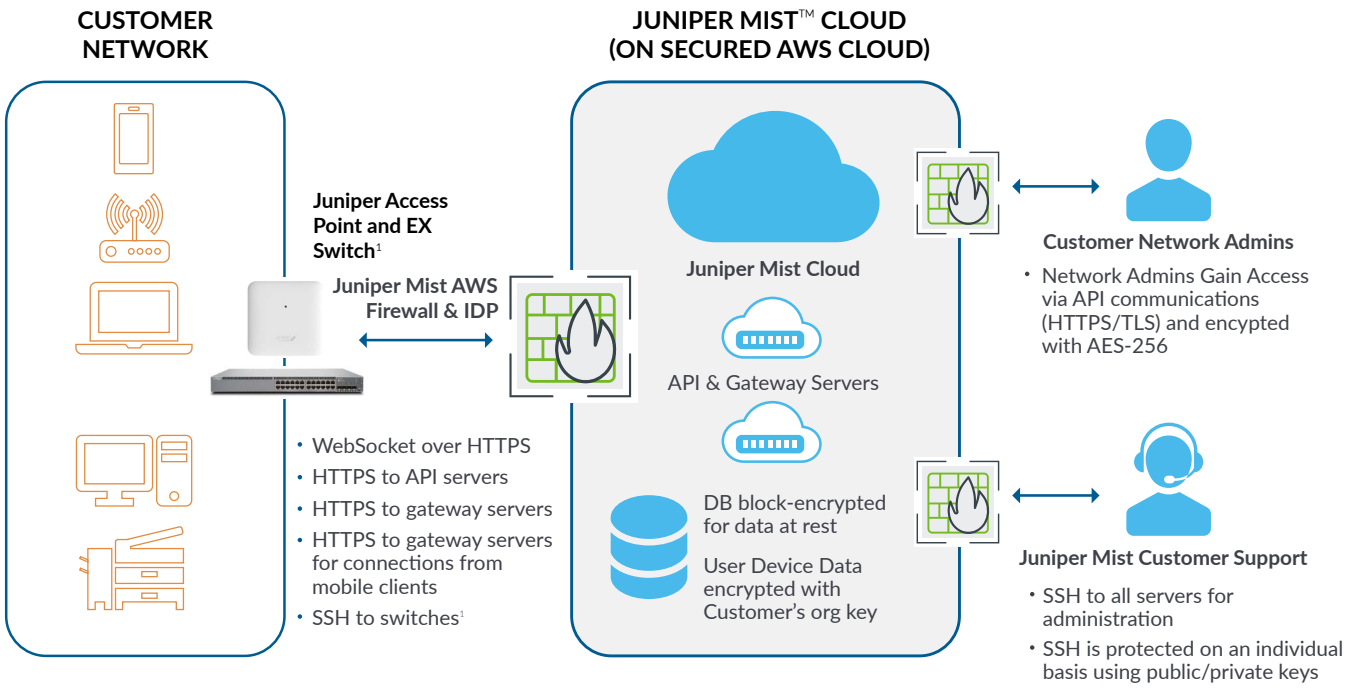
We understand that Customers use our AI-driven solution in environments that must meet industry-specific security requirements. As such, Customers determine the legal terms of use or other policies presented to individual device users prior to granting such users access to their network. Customers who deploy Juniper products should review their activities for compliance with applicable laws and regulations. This brief explores how security and privacy are embedded throughout Juniper's solutions.

RESILIENT AI IN A SECURED CLOUD

Protecting our Customers' data is mission critical to Juniper. The Juniper Mist cloud typically does not store or access the contents of any individual device, end user communications, browsing history or other content created, transmitted, or received by the device user unless directed to do so by the Customer.

The Juniper Mist cloud offers our Customers the peace of mind that they are always on the latest version of our software. This enhances our ability to innovate and protect our Customers' data with evolving technology. We can respond to security threats rapidly by pushing security updates to our entire Customer base and ensuring common data handling standards. Most importantly, the Juniper Mist cloud is co-located in tier-1 datacenters with industry standard certifications. These datacenters feature state of the art physical and cyber security with highly reliable designs. These services are replicated across multiple availability zones per AWS services, so that Customer-facing services fail over rapidly in the event of a catastrophic failure. Diagram 1 shows additional security details from the datacenter to data-at-rest and data-in-transit.

DIAGRAM 1.
JUNIPER MIST WI-FI AND WIRED ASSURANCE SECURED INTERFACES



[1] EX Access Switches–EX2300, EX3400, EX4300, EX4600

Snapshot of Juniper Mist Cloud Security Features:

- Servers are hosted in an ISO 27001 certified datacenter, which data center also provides SOC 2 attestation reports over its security controls, across multiple availability zones.
- All servers run Linux OS and are hardened per best practices.
- Servers are hosted at AWS with security groups. Only the required ports are opened on front end servers or terminators that need to communicate directly with Access Points (APs) or APIs from outside.
- Industry standard encryption is utilized for data in transit and data at rest (Please reference 'Data Security' section for details).
- Performs web security testing from development to production stages. Juniper periodically scans for SQL injections, XSS and 700+ other vulnerabilities, including the OWASP Top 10.
- Audit logs, such as access and incident logs, are captured at a centralized location in AWS and retained for six months.
- Principles of granting minimal privileges, minimal access, and minimal services are used; user access is restricted.
- Juniper employs robust key management processes.
- Juniper switches are located on Customer premises where they are configured and managed by the Customer.
- Further information about security provided by AWS is available from the AWS Security Website, including AWS's overview of security processes.

DATA SECURITY

Industry standard encryption is utilized for data communications across network administrators, infrastructure hardware/software, end users and the Juniper Mist cloud, while stored data is block-encrypted.

Juniper secures Customer data by implementing various controls, such as encryption and obfuscation, including:

- **AP and switch to Juniper Mist cloud:** Communication between the Juniper Mist cloud and Juniper APs and switches uses HTTPS/TLS with AES-128 encryption, and mutual authentication is provided by a combination of digital certificate and per-AP shared key created during manufacturing. 4096-bit key is used for certificate signature.
- **UI or API:** API communication (including UI access) uses HTTPS/TLS and is encrypted with AES-256.
- **Internal to cloud:** Data within the cloud is stored using AES-256 encryption.
- **Management/infrastructure console:** Accessed over HTTPS connection, using 2048-bit RSA key.

Access Controls

Juniper controls access to various resources involved in delivering the service to our Customers, including as follows:

- Access Restrictions
  - Access to APs—No user accessible interface.
  - Access to switches—User interface managed by Customer.
  - AP access to cloud—Based on role assigned by Customer.
- Access Controls
  - Role based for org/site changes
  - Juniper adheres to the principle of least privilege in granting its personnel access to Customer data, including Device Data (Reference 'Device Data' section below for details).

AI-DRIVEN ENTERPRISE PRIVACY REGIME

Supporting our privacy-driven architecture and internal administrative and procedural safeguards, Juniper by default only collects certain Device Data (Reference 'Device Data' section below for details) and does not collect the payload data of applications, network devices, Internet of Things (IoT) devices, or individual device end users by default. In addition, Device Data is encrypted with a Customer-specific key as indicated in Diagram 1.

The collection and analysis of Device Data allows Juniper to provide insights to its Customers into a specific network, IoT, or user device's behavior (and location information if enabled) along with analytics across device types. This is key for baselining and monitoring trends, and later identifying macro issues early so that Juniper and its Customers can proactively address any possible networking issues. For example, user device roaming time, hardware radio performance, and device throughput can all be analyzed to identify system issues, such as a performance degradation when a new mobile device operating system version is released. For wired network and IoT devices, Customers can set, monitor, and enforce Service Level Expectations (SLEs) for key wired experience metrics such as throughput, network, and switch health which, when combined with Marvis, can deliver proactive anomaly detection.

Device Data

Here is a description of the data elements processed in the Juniper Mist cloud and which may also be considered personal data under applicable data protection laws.

Juniper Mist Wi-Fi Assurance

- Device name
- Device type, model, family, and operating system
- MAC address
- IP address
- User agent
- Username
- Generic, or specific, location
- Dynamic PCAP (packet capture)—limited data such as header information, IP address of sender and recipient

Juniper Mist Wired Assurance

Device Data collected by default from network and IoT devices such as switches, laptops, desktops, printers, and Access Points to help our Customers efficiently optimize the performance and security of their networks and devices includes, for example:

- IP address
- MAC address
- Hostname
- Username
- Group
- LLDP information

Juniper Mist Premium Analytics

Customers using Juniper Mist Wi-Fi Assurance, Wired Assurance, and Location services may also subscribe or otherwise elect to enable Premium Analytics, a service that offers insights to support enterprise digital initiatives. With Premium Analytics, Customers may authorize Juniper to retain Customer's Wi-Fi and Wired data for longer periods to display trends, analysis and a more comprehensive view of network operations using Device Data and other data collected through the Juniper Mist cloud.

Customer Choices and Control

Customers may configure their Juniper APs to collect additional Device Data depending on the desired implementation and level of support. In order to provide support to our Customers when needed, our Customer success team is able to access a Customer's Device Data. However, Customers have options for how much Device Data Juniper may access. For example, Customers have the option within the Juniper Mist cloud to temporarily authorize Juniper personnel to access and view an organization's Device Data processed by Juniperin order for Juniper to provide support services. Using this access authorization feature, Customers have more control over when Juniper personnel have access to the Customer's Device Data. When first implementing the Juniper Mist cloud service dashboard, this authorization and access is configured to be "on" in order to provide a better support experience.

Below, we describe the different Juniper Mist cloud services and the configuration options that Customers have to manage the Device Data Juniper collects and processes in the Juniper Mist cloud.

Juniper Mist Wi-Fi Assurance

Juniper Mist Wi-Fi Assurance is the core cloud service all Customers must use in connection with their Juniper access points. Wi-Fi Assurance includes the following features and functionality:

Manual PCAP

If a Customer wishes to configure Manual PCAP (packet capture) for more detailed troubleshooting or security management, the Customer may decide to collect certain data that might, depending on whether the underlying transmission was encrypted, include payload. In such cases, Customers may permit Juniper to utilize Manual PCAP data to assist Customers in addressing support requests.

Captive Portal

Customers may, at their election, implement and configure a "captive portal" that guest users must enter in order to access the Customer's Juniper APs. Captive portals require some Device Data to operate but Customers may determine the extent of any additional user data collected by such captive portal, such as contact information for the guest user (for example, the user's name and email address).

Location Data[2]

If a Customer elects to subscribe to Juniper Mist location-services, Juniper will process a device's precise location information. Less-precise location information may be collected by default for devices connecting to a Juniper AP using Wi-Fi even if such location services are not enabled. Depending on the device and the protocol used to connect to the Juniper AP, the individual connecting to the AP ("data subject") may be prompted to opt-in to location sharing. For example, device users generally would not be prompted to opt-in to location sharing for passive Wi-Fi (when the device is not connected to the Wi-Fi network), Bluetooth devices, like activity trackers, but could be prompted to opt-in to location sharing of their mobile phone through Bluetooth Low Energy via an app developed and configured by the Customer. Once the Customer enables device location services, the Customer will have access to the location of all devices within range of its Juniper AP network – whether the device is communicating through connected or unconnected Wi-Fi, Bluetooth Low Energy, assets such as Bluetooth Low Energy badges, and passive Bluetooth, among others. Mist generally does not store the location history of devices and by default provides only real-time non-specific location information, or as aggregated statistics for delivering zone visitation/dwell time analytics to Customers. If a Customer requests to turn on visibility for unconnected devices, Juniper generally would process the MAC Address and approximate location for the device (typically within 10 meters of accuracy).

If a Customer subscribes to location services, the following settings are configured by default:

- **Devices communicating via Wi-Fi:** location information is made more accurate (e.g., within5-10 meters dependent on network design). Specific location tracking is not enabled by default if the device is not connected.
- **Mobile phones communicating via BLE application:** location tracking is not enabled by default. The user must opt in for location sharing in the mobile application.
- **Assets (named) communicating via BLE:** specific location tracking is not enabled by default.
- **Assets (passive) communicating via BLE:** specific location tracking is not enabled by default.

Location Data[2] and Mist Premium Analytics

If a Customer orders or otherwise chooses to participate in Mist Premium Analytics, and subscribes to a location service[2], Juniper will store location history of devices for the period as determined by the Customer and confirmed in writing with Juniper. Custom reporting, available with Premium Analytics service, may also be configured to provide more complete analytics regarding location information.

Additional Location Data[2] Use Cases

Customers may leverage location services[2] and Premium Analytics for additional use cases such as journey mapping, proximity tracing, and hot zone alerting to support business continuity practices such as proximity tracing and social distancing. Such business continuity initiatives can assist Customer employees return to the workplace after a pandemic such as COVID-19. By implementing certain location data-related solutions, Customers can better understand the movement, traffic patterns, and congestion areas of devices with the goal of reducing further exposure to individuals who have reported testing positive for a virus such as COVID-19.

Without enabling the aforementioned location solutions, Juniper offers real-time, non-specific device location with an accuracy of 5-10 meters. Use of BLE assets, such as Bluetooth-enabled ID badges, can also increase accuracy to 3-5 meters. Likewise, the use of a mobile application via the Mist SDK also leverages the BLE capabilities of the Juniper AP, which can offer improved accuracy to 1-3 meters. Meanwhile, devices with Wi-Fi enabled but which are not connected to the Wi-Fi network can be located with accuracy of 10 meters.

[2] Mist Systems Location Services constitutes Mist User Engagement and Mist Asset Visibility Subscription.

Enabling Premium Analytics provides historical location data information and reporting far exceeding the real-time only information provided in standard storage. Juniper's location services also do not utilize a device's GPS location and are dependent on presence within the network's signal area, so once the device leaves the area of a Customer's Wi-Fi network, location services cease, helping to support our Customers' privacy and trust commitments.

For additional information, please visit Juniper Contact Tracing Solution.

SUPPORTING GLOBAL PRIVACY COMPLIANCE

Juniper is committed to helping our Customers address global privacy compliance requirements, including for example and as may be applicable based on the locations in which such Customers operate and from which they collect data related to data subjects, the EU General Data Protection Regulation (GDPR) requirements and the California Consumer Privacy Act (CCPA) by providing the information that Customers need regarding data processing, and by implementing privacy tools and security features with Juniper to empower Customers to make their own decisions about what data they want to process in order to enhance the performance and security of their Wi-Fi and Wired networks.

As part of our commitment to help Customers address their global privacy compliance requirements, Juniper provides the below information for reference by Customers, who are encouraged to consult with their own data protection and privacy compliance counsel regarding any particular laws or regulations that may apply to them and to develop a compliance program that best aligns with their business needs.

Please visit our Privacy Policy for additional information regarding Juniper's commitment to privacy.

EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (GDPR)

Under the GDPR, Juniper's Customers are data controllers and Juniper is a data processor. When a Customer decides to deploy Wi-Fi Assurance in its offices, retail business, or other environment, the Customer deploys a wireless local area network (LAN) using Juniper Access Points that collect and process Device Data in order to better manage that wireless network and offer additional services (e.g., way-finding and other location-based services) at the Customer's election. When Customers deploy Wired Assurance, they implement a tool to provide insights and management capability for their Juniper EX Switches. Under the GDPR, device end users located in the EU who access the Customer's LAN are data subjects. The GDPR creates certain requirements for data controllers and data processors alike when handling the personal data of data subjects. Data processors, like Juniper, generally are obligated to process personal data only as instructed by the data controller.

Juniper has developed and adopted information security policies designed to protect the confidentiality, integrity and availability of Device Data.

Data Protection Principles

- Data Minimization: The Juniper Mist platform by default collects the information required to provide and maintain the services, anticipate and address network performance and connectivity issues, and troubleshoot support requests. Using the captive portal in the Juniper Mist cloud, Customers are generally able to configure the type and quantity of data collected from data subjects for select Juniper Mist services when their end users connect to a Mist AP.
- Data Retention: Juniper deletes Customer data (including Device Data) from the Juniper Mist cloud on a 60-day rolling basis and upon a Customer's written request. Packet data is retained and available for seven (7) days. Juniper retains certain other data for longer periods as determined by Customer if Customer orders Premium Analytics. See applicable product documentation for further details on retention of information on Juniper devices.
- Data Portability: Customers may download a copy of selected data through the dashboard or by using Juniper's API or other tools dependent on the applicable service. Reports produced from the Premium Analytics services can be downloaded by Customers.
- Data Subject Requests – including access and erasure/deletion: Juniper is committed to assisting Customers who need to respond to certain data subject requests regarding Device Data processed by Juniper on the Customer's behalf, for example, to receive a copy of, delete, or correct, certain data through the dashboard. In addition, Customers can directly manage any data downloaded by Customer from the cloud service dashboard. By minimizing our collection and retention of personal data, we help simplify the data subject response process.
- Notice and Consent: Juniper provides functionality enabling Customers to present a notice to data subjects and consent to or decline terms. Customers are responsible for managing and implementing any consents provided.
- Tracking Technologies: Juniper enables Customers to determine which tracking technologies to use and how to configure them, for example, whether to enable location services for more precise location tracking of users.

EU Hosting of Customer Data

Customers with headquarters (or main address provided to Juniper) located in the EU are automatically set up for hosting in an EU data center. This means the Customer's Device Data and the rest of its Juniper cloud instance will be hosted in the EU. Additionally, Customers may elect EU-based hosting even if their headquarters or main address provided to Juniper are not located in the EU. However, Juniper personnel who are granted access to a Customer's Device Data or cloud service dashboard may be in regions outside of the EU where data privacy and data protections laws may differ. Nonetheless, Juniper employs the same security measures no matter the location of its personnel.

Data Processing Agreement (DPA)

Our Data Protection and Privacy Agreement ("DPA") is available here. The Juniper DPA incorporates the European Commission's Standard Contractual Clauses (SCC) and other provisions applicable to Juniper. The DPA provides Customers with greater clarity as to how Juniper will process and store any personal data.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

Juniper is committed to protecting the confidential data of our Customers, including any such data that is personal information under the California Consumer Privacy Act ("CCPA"). For the convenience of our Customers, our CCPA Confirmation is available here.

Generally, Juniper processes data as a service provider for our Customers, many of which are organizations that have a direct relationship with individual end users using products or services of Juniper. This means that, in addition to other exceptions under the CCPA that may apply (including for employees, contractors and business contacts), Juniper's processing of data as a service provider may not involve a sale of personal information of a consumer.

To the extent that Juniper processes any personal information of any consumer covered by the CCPA under our contract with a Customer, and that such processing is not otherwise exempt under the CCPA, Juniper confirms it is generally acting as a service provider under such contract.

Except to the extent permitted under the CCPA, or otherwise required by applicable laws or regulations, to protect Juniper's legal rights, to protect security, or to improve the products and services of Juniper provided under a contract with a Customer, Juniper is prohibited from:

(i) "selling" (as defined in the CCPA) personal information received by Juniper in connection with the processing of personal data under the Customer's contract;

(ii) retaining, using or disclosing personal data received by Juniper under the Customer's contract for any purpose other than providing products or services of Juniper under the Customer's contract; and

(iii) retaining, using or disclosing such personal data outside of the direct business relationship between Juniper and the other party to the Customer contract (or, in the case of a Partner, the Customers or Partners to whom such Partner distributes the products or services provided under the Customer contract).

Pursuant to the CCPA, Juniper certifies that it understands these restrictions and will comply with them with respect to any personal information of any consumer covered by the CCPA that is processed by Juniper under the Customer contract, where such processing is not otherwise exempt under the CCPA.

CONCLUSION

Juniper shares our Customers' concern for data security and privacy protection. We are committed to complying with the provisions of data protection and privacy laws that apply to Juniper in our role as a data processor, and to empowering and assisting our Customers.