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 The principles of market competition often described by the big eating the small has been replaced by the fast beating the slow with technology as a catalyst.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 (AI)’s impact on today’s 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.

Mist Systems’ AI-driven enterprise platform is deployed across leading Fortune 500 companies, which only validates IT’s growing dependence on AI today. These leading companies have relied on Mist’s modern cloud-based architecture of delivering predictable, reliable and secure wireless services with AI to meet the challenging management and performance requirements for their digital transformation.

When you choose Mist, a Juniper Company, you gain the speed, experience, expertise, and reliability that has been synonymous with the networking innovations from Juniper Networks. Mist’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, Mist 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 architecture 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 the Mist Customer’s network. Customers who deploy Mist products should review their activities for compliance with applicable laws and regulations. This brief explores how security and privacy are embedded throughout Mist’s solutions.

RESILIENT AI IN A SECURED CLOUD

Protecting our Customers’ data is mission critical to Mist. The 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.

Mist cloud-based solutions offer 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 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. Secured Interfaces Diagram on Page 2 provides additional security details from the datacenter to data-at-rest and data-in-transit.
Snapshot of Mist Cloud Security Features:

- Servers are hosted in an ISO 27001 certified datacenter, which datacenter 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).
- Mist performs web security testing from development to production stages. Mist 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.
- 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 Mist Cloud, while stored data is block-encrypted.

Mist secures Customer data by implementing various controls, such as encryption and obfuscation, including:
- **AP to Mist Cloud:** Communication between the Mist cloud and the AP 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. A 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
Mist 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.
  - AP access to cloud — Based on role.
- **Access Controls**
  - Role based for org/site changes.
  - Mist adheres to the principle of least privilege in granting its personnel access to Customer data, including Device Data.

MIST’S PRIVACY REGIME
Supporting our privacy-driven architecture and internal administrative and procedural safeguards, Mist by default only collects certain Device Data (Please reference ‘Device Data’ section for details) and does not collect the payload data of applications or individual device end users by default. In addition, Device Data is encrypted with a Customer-specific key.

The collection and analysis of Device Data allows Mist to provide insights to its Customers into a specific 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 Mist 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.

Device Data
Device Data collected from users by default to help our Customers efficiently optimize the performance and security of their Mist APs includes, for example:
- 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

Customer Choices and Control
The Mist solution is designed to give Customers options for how much Device Data Mist may access. For example, Mist Customers have the option within the Mist Dashboard to temporarily authorize Mist personnel to access and view the Customer’s Device Data processed by Mist. Using this access authorization feature, Customers have more control over when Mist personnel have access to the Customer’s Device Data. When first implementing the Mist Dashboard, this authorization and access is configured to be “on” in order to provide a better support experience.

Manual PCAP
If a Customer wishes to configure Manual PCAP for more detailed troubleshooting or security management, the Customer may collect certain data that might, depending on whether the underlying transmission was encrypted, include payload. In such cases, Customers may permit Mist 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 Mist 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). The Customer may elect the retention period for this information as well as allow end users to opt out of having the Customer (and Mist) to store such information.

Location Data
If a Customer elects to subscribe to Mist location-services, Mist will process a device’s precise location information. Less-precise location information may be collected by default for devices connecting to a Mist AP using Wi-Fi even if such location services are not enabled. Depending on the device and the protocol used to connect to the Mist AP, the 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 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 Mist AP network – whether the device is communicating through connected or unconnected Wi-Fi, Bluetooth Low Energy, assets such as RFID 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. If a Customer requests that Mist turn on visibility for unconnected devices, Mist 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., within 1-3 meters). Specific location tracking is not enabled 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.
EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (GDPR)

Under the GDPR, Mist Customers are data controllers and Mist is a data processor. When a Customer decides to deploy the Mist solution in its offices, retail business, or other environment, the Customer deploys a wireless local area network (LAN) using Mist 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. 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 Mist, generally are obligated to process personal data only as instructed by the data controller.

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

Data Protection Principles

- Data Minimization: The Mist system by default collects the information required to provide and maintain the service, anticipate and address network performance and connectivity issues, and troubleshoot support requests. Customers are generally able to configure the type and quantity of data collected from data subjects for select Mist services when their end users connect to a Mist AP.
- Data Retention: Mist deletes Customer data (including Device Data) from Mist’s systems on a 60-day rolling basis and upon a Customer’s written request. Packet data is retained and available for seven (7) days. Mist APs regularly purge data.
- Data Portability: Customers may download a copy of selected data through the Mist Dashboard or by using Mist’s API.
- Data Subject Requests: including access and erasure/deletion: Mist is committed to assisting Customers who need to respond to certain data subject requests regarding Device Data processed by Mist on the Customer’s behalf, for example, to receive a copy of, delete, or correct, certain data through the Mist Dashboard. In addition, Customers can directly manage any data downloaded by Customer from the Mist Dashboard. By minimizing our collection and retention of personal data, we help simplify the data subject response process.
- Notice and Consent: Mist 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: Mist enables Customers to determine which tracking technologies to use and how to configure them, for example, whether to enable location services for more precise geolocation tracking of users.

EU Hosting of Customer Data

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

Data Processing Agreement (DPA)

Our Data Protection and Privacy Exhibit (“DPA”) is our data processing agreement for Customers and is available here. The Juniper DPA incorporates the European Commission’s Standard Contractual Clauses (SCC) and other provisions applicable to Mist. The DPA provides Customers with greater clarity as to how Mist will process and store any personal data.
CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

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

Generally, Mist 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 Mist. This means that, in addition to other exceptions under the CCPA that may apply (including for employees, contractors and business contacts), Mist’s processing of data as a service provider may not involve a sale of personal information of a consumer.

To the extent that Mist 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, Mist 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 Mist’s legal rights, to protect security, or to improve the products and services of Mist provided under a contract with a Customer, Mist is prohibited from:

(i) “selling” (as defined in the CCPA) personal information received by Mist in connection with the processing of personal data under the Customer’s contract;
(ii) retaining, using or disclosing personal data received by Mist under the Customer’s contract for any purpose other than providing products or services of Mist under the Customer’s contract; and
(iii) retaining, using or disclosing such personal data outside of the direct business relationship between Mist 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, Mist 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 Mist under the Customer contract, where such processing is not otherwise exempt under the CCPA.

CONCLUSION

Mist 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 Mist in our role as a data processor, and to empowering and assisting our Customers.