Juniper Networks | Driven by Experience™

CONTRAIL SERVICE ORCHESTRATION TECHNICAL BRIEF ON PRIVACY AND SECURITY

Introduction

Contrail® Service Orchestration (CSO) software designs, creates, and coordinates a secured WAN service. CSO is highly available, scales easily, and supports multitenancy with role-based access. Furthermore, starting in June 2021, with the availability of our newest cloud-managed CSO deployment hosted in the European Union, customers have the ability to elect to have CSO provisioned from the United States or the European Union (see section below on European Union Data Hosting and Data Protection). Multitenancy separates customer tenancies and creates a more personalized experience. For communication service providers (CSPs), multitenancy is fundamental to building out SD-WAN and enterprise services, increasing competitiveness, and enabling real profits.

As managed service providers look to deliver SD-WAN services, and as enterprises seek assurances that these services can be delivered across all locations, the resulting platform must be agile and capable of scaling cost effectively. While simpler SD-WAN systems offer single tenancy scale and basic reliability, CSO's foundational microservices architecture ensures cloud-grade reliability and scalability to enable multitenancy and ensure high availability and high performance.

Contrail Service Orchestration includes a web-based management interface for defining policies, managing locations, visualizing performance behavior, and automating the provisioning and management of devices running within the SD-WAN environment. With Juniper's cloud-managed SD-WAN, customers do not need to run or maintain the CSO component of the SD-WAN solution.

This technical brief focuses on the many privacy and security features relating to Juniper's cloud-managed CSO deployment. At customer's election, CSO may also be deployed using an on-premises version.

Network Management in a Secured Cloud

Protecting our customers' data is mission critical to Juniper. Network traffic traveling through a customer's SD-WAN (referred to as "network traffic data") does not travel through CSO, and customers who procure Contrail Service Orchestration in the cloud control the touchpoints of their network data.

While CSO provides powerful analytics regarding websites and applications that a customer's users are employing on its SD-WAN, it does not process those data transmissions or inspect any packets. Customers can rest assured that CSO does not process any data its users send or receive via the SD-WAN. Information regarding websites and applications is derived from logs generated by the network device (also called "network management data").

Juniper's cloud-managed CSO offers customers peace of mind that they are always using the latest version of the software. This enhances our ability to innovate and apply the latest improvements based on evolving technology. We can respond to security threats quickly by pushing security updates to our entire customer base and ensuring common security standards. Most importantly, CSO is hosted in a top-tier Amazon Web Services (AWS) data center in the United States and European Union with industry-standard certifications. AWS data centers feature state-of-the-art physical and cybersecurity with highly reliable designs.

Juniper Contrail Service Orchestration includes the following security features:

- Servers are hosted in an ISO 27001-certified data centers.
- 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.
- Industry-standard encryption is utilized for data in transit and data at rest (see the Data Security section later in this document for more details).
- 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.
- Logs, including access, incident, and device, are captured at a centralized location in AWS and retained for one to 30 days or, in select cases, based on the duration of the customer's tenancy, and are available to customers via API or the CSO platform.
- Customers can apply principles of granting minimal privileges, minimal access, and minimal services. User access is restricted through customer-granted role-based access control.

- CSO access authentication can be configured for single sign-on (SSO) and authenticated using customer authentication controls (such as through Active Directory, LDAP, and Okta).
- CSO is developed and maintained following Juniper's Secure Development Life-Cycle practices.
- Juniper employs robust key management processes via the AWS Key Management Service.
- Customer network devices are located on customer premises and are configured and managed by the customer using CSO.

Further information about security provided by AWS is available from the AWS Security Website, including AWS's overview of security processes.

Data Security

Cloud-Managed by Juniper Networks

Customers can leverage the Juniper SD-WAN solution using Contrail Service Orchestration. Customer access to the CSO management interface uses a management plane that separates network management data from user WAN and LAN data traffic. While management details are provisioned and maintained in CSO, network traffic data does not route through or to CSO. Instead, such data is directed to its destination over the LAN and WAN between source and destination within the customer's SD-WAN infrastructure. This architecture ensures that any loss of management connectivity to the cloud-managed Juniper SD-WAN service does not impact the customer's network flows or end-user experience.

Juniper's cloud-managed SD-WAN service also provides strong security protections for CSO, including:

- CSO's perimeter is secured with network access control lists, managed distributed denial of service (DDoS) protection, and security groups for all public IPs.
- Web application firewalls and https secure user access.
- Strong firewall policies deny malicious traffic.
- Secure firewalls serve as Operation, Administration, and Maintenance (OAM) hubs for control plane traffic from devices.
- Device access is secured through firewalls and IPsec tunnels.

Encryption

- Data in transit:
  - HTTPS connections are used for customer access to the CSO Web interface.
  - SSH is used for the SD-WAN network device console.
  - Data traveling from SD-WAN network devices to CSO is encrypted with AES-256 through secured IPsec tunnels.
- Data at rest is protected by whole-disk encryption with AES-256.
- Passwords are encrypted.

Service Reliability

- CSO is hosted in data centers across multiple availability zones designed for physical redundancy and resiliency, providing uninterrupted performance following a power outage or natural disaster.
- On-demand scaling of resources is provided transparently to the customer.
- Management continuity is provided with controller redundancy and daily backups. System failover and recovery capabilities are tested annually.

Access Controls

Juniper provides the following access controls and restrictions to customers and follows its own access procedures:

- Customer access restrictions and controls:
  - Customer access to CSO cloud is based on role assigned by the customer.
  - Customers can leverage predefined roles or define customized roles.
- CSO access restrictions and controls:
  - CSO access to customer network management data is restricted based on role or customer-granted permission and is based on the principle of least privilege. Access is logged.
  - There is no CSO access to network traffic data.

Contrail Service Orchestration Privacy Regime

Supporting our privacy-driven architecture and internal administrative and procedural safeguards, Juniper does not process the customer's network traffic data. This supports two key privacy principles: data minimization and data retention. By design, Juniper reduces to zero the network traffic data CSO processes and therefore is unable to process any personal information that may be contained in a customer's network traffic. As a result, there is no such data to retain or manage going forward.

The minimal network management data CSO processes allows Juniper to provide customers with insight into a specific device's network usage. This is key for baselining and monitoring trends, and later identifying macro issues early so that customers can proactively address any possible networking issues.

For example, CSO can analyze network management data to enable customers to monitor the top websites or Web applications that a particular device accesses to determine which websites and applications consume the most bandwidth, or whether certain websites or applications should be disallowed pursuant to the customer's policies. Additionally, depending on the customer's network architecture, CSO enables customers to identify the top IP addresses by name, provided there is an Active Directory integration if elected by the customer. This network management

data is not collected from network traffic data; rather, it is derived from logs generated by the network device and is under the customer's control.

Customers can configure the information provided to CSO through the customer's device logs. CSO only processes the data transmitted by the customer's network devices.

Compliance

- CSO is backed by a cloud infrastructure with industry-standard certifications.
- CSO is supported by Juniper with proactive monitoring, regular vulnerability scans, and penetration tests performed by reputable third-party providers. Any open items are prioritized and addressed based on their Common Vulnerability Scoring System (CVSS) score.

Account Protection and Privacy

- User accounts are password-protected with secured access as described above in the Access Controls section.
- SSO authentication is supported.
- System logs are monitored for authentication failures, with instant alert notifications.

Network Management Data

Network management data processed to help customers efficiently optimize the performance and security of their SD-WAN includes:

- Network device information such as name, device type, model, and operating system
- Depending on the customer's network architecture, IP addresses connecting to the network device
- Websites and applications accessed by an IP address through a network device

Network management data is derived from logs generated by the network device. Other personal data processed by CSO includes login information of customer administrators such as e-mail and password ("CSO user information"). Customers also control the specificity of site location information.

Customer Choices and Control

To support the principle of data protection by default, Contrail Service Orchestration allows customers to choose whether Juniper may access the customer's CSO network management data for support or troubleshooting purposes. For example, CSO customers have the option to temporarily authorize Juniper personnel to access and view the customer's network management data processed by Juniper to respond to support requests.

Supporting Global Privacy Compliance

Juniper is committed to helping our customers address global privacy compliance requirements, including locations where the customer operates and from which it collects personal data. Based on the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), customers are provided with the information they need regarding data processing. Implementing privacy tools and security features with CSO empowers customers to make their own decisions about what data they want to process to enhance the performance and security of their SD-WAN.

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

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

European Union Data Hosting and Data Protection

CSO provides the ability for customers to deploy their instance from Juniper's European Union data center. In doing so, customers can focus the processing of personal data within the European Union. This may provide customers with certain advantages in supporting their compliance programs and initiatives.

Juniper strenuously protects customer data, including from any government requests. Any government requests submitted to Juniper will be stringently evaluated and scrutinized. Juniper will seek to appropriately challenge or narrow requests which, among other reasons, are not necessary nor proportionate. We will also seek to challenge requests that prohibit notification to our customers. Juniper's standard practice is to only produce information to an agency with appropriate authority under applicable law to demand the information, and we will only provide the information within the specific scope of the request after exhausting any available challenges. Every government request, however received, goes through this strict evaluation process. For additional details regarding governmental requests and our processes and procedures for transferring EU personal data, see Juniper's Post-Schrems II International Personal Data Transfers FAQ. Juniper closely monitors and analyzes developments in the global regulatory and legislative landscape and adjusts its data protection and data privacy practices accordingly. Options such as European Union data hosting demonstrate our continuing commitment to providing our customers valuable additions to their compliance toolbox.

European Union General Data Protection Regulation (GDPR)

Under the GDPR, Juniper customers are data controllers and Juniper is a data processor. When a customer deploys CSO in a cloud-managed service, the customer subscribes to a cloud-based network management solution hosted and provided by Juniper to better manage its SD-WAN. Under the GDPR, end users located in the EU who access the customer's SD-WAN are data subjects. The GDPR defines certain requirements for data controllers and data processors alike when handling the personal data of data subjects. Data processors, like Juniper, are generally 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 network management data that may contain the personal data of end users.

Data Protection Principles

- **Lawfulness, Fairness, Transparency:** A number of legal bases for processing may be available to customers under the GDPR. Customers can rest assured that Juniper will only use the data in a manner related to the provision of CSO, which allows customers to maintain transparency regarding CSO's personal data processing activities by providing them with information regarding the solution's data privacy and data security features. Customers may use this detailed information to notify appropriate parties regarding CSO's personal data processing operations.
- **Data Minimization:** By default, CSO processes only the information required to provide and maintain the service, anticipate and address network performance and connectivity issues, and troubleshoot support requests. Customers can control the information related to data subjects contained in their network device logs and transmitted to CSO. CSO does not collect or otherwise process any network traffic data.
- **Data Retention:** CSO retains network management data, logs, and any other user information for one to 30 days or, in select cases, based on the duration of the customer's tenancy. Customers may purge some of the network management data earlier.
- **Data Portability:** Customers may download a copy of selected data through CSO or by using CSO's API or other tools dependent on the applicable service.
- **Purpose Limitation:** Juniper developed CSO with flexibility in mind and built-in tools that allow customers to only process the personal information required for their SD-WAN management activities. Customers can remain confident that the network management data and logs processed by CSO are not used in a way that is incompatible with provisioning of CSO itself. If customer administrators elect to share such data with Juniper, Juniper will only use the data in the context of providing and supporting CSO. Juniper's use of network management data is restricted to the purposes set forth in applicable Juniper agreements, including the Juniper Data Protection and Privacy Exhibit, explained in greater detail in the Data Processing Agreement (DPA) section. Customers also control what they do with the information presented to their CSO administrators and can ensure its uses align with its own policies or employee terms.
- **Accuracy:** CSO promotes data accuracy by only processing network management data that is automatically produced by devices as configured by customers, reducing the occurrence of human error. Data is protected in secured environments designed to prevent it from being modified and rendered inaccurate through any unauthorized or unlawful access. Please see the Data Security section for additional security information.
- **Accountability:** CSO allows customers to demonstrate compliance with data protection principles by providing them with information regarding CSO's data privacy and data security features. Juniper uses a data protection and privacy exhibit that incorporates the European Commission's Standard Contractual Clauses (SCC) and other provisions applicable to Juniper. Please see the Data Processing Agreement (DPA) section for information regarding the Juniper DPA. In accordance with applicable laws, Juniper assists customers with data protection impact assessments and other data protection-related queries. Juniper also conducts its own data protection impact assessments where needed and follows other accountability principles.
- **Integrity and Confidentiality:** CSO implements features designed to ensure appropriate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage. Personal data is stored in Juniper's AWS data center in accordance with access and security protocols designed to maintain the privacy and confidentiality of personal data. Please see the Data Security section for additional security and confidentiality information.
- **Notice and Consent:** Juniper is committed to helping customers learn about CSO's features to support the deployment of any notices and collection of any consents they deem necessary in accordance with applicable laws or internal policies. Customers are responsible for managing and implementing any required notices or consents.

Hosting of Customer Data

The CSO public cloud instance is hosted in top-tier AWS data centers in the United States and European Union. Depending on customers' data compliance or data governance preferences, customers can elect the data center location. Juniper personnel who are granted access to network management data or a CSO instance may be located in regions outside of the EU where data privacy and data protections laws may differ. Nonetheless, Juniper has established standard information security policies and practices that apply globally to all Juniper locations, and this Technical Brief on Privacy and Security provides details regarding how CSO protects customer data. Please see the Data Processing Agreement (DPA) section for information regarding Juniper's practices, processes, and contractual obligations for transfers of personal data to third countries.

Data Processing Agreement (DPA)

Our Data Protection and Privacy Exhibit (available here) incorporates the European Commission's Standard Contractual Clauses (SCC) and provides customers with greater clarity regarding how CSO will process and store any personal data.

California Consumer Privacy Act (CCPA)

Juniper is committed to protecting our customers' confidential data, including personal information, under the California Consumer Privacy Act (CCPA). For our customers' convenience, 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 employing Juniper products or services. 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:

- "Selling" (as defined in the CCPA) personal information received by Juniper in connection with the processing of personal data under the customer's contract
- 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
- 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 a 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 understands and shares our customers' concerns about data security and privacy protection. With Juniper's cloud-managed SD-WAN service and Contrail Service Orchestration, we are fully 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 manage their network data in a secured cloud.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. 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.
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: +31.207.125.700

Juniper Networks | Driven by Experience™