CloudVision as-a-Service: Security and Data Protection

Introduction

Cloud-based software delivery has increasingly become the norm in today's world, owing to the elasticity, scalability, and economy of cloud architectures. Arista has established a leadership position in the delivery of reliable and secure cloud networking and services management through the introduction of CloudVision®, a single unified AI/ML-enabled network management platform supporting every place in the cloud – and CloudVision is now available in an "as-a-Service" delivery model in the cloud.

Arista CloudVision as-a-Service is architected from the ground up with security in mind, taking proactive measures to deliver a robust security architecture suitable for cloud delivery. The cloud-native architecture of the CloudVision platform, whether delivered as an on-premises server application or as a cloud-managed service, is identical and provides an operational foundation for automation of provisioning and change management with network-wide visibility. Our site reliability engineers support the CloudVision cloud service with modern operational controls in accordance with industry best practices and subject to third-party certifications.

Also, the Arista CloudVision as-a-Service platform comprises multiple security pillars and safeguards to protect users and their data as described in this document. Considering the increasing pressure on IT teams to ensure that the necessary security and compliance policies, procedures, and technologies are in place with any cloud-based service, this document describes the architecture, operational and regulatory aspects at the core of CloudVision as-a-Service, as well as steps that we take for protection and defense of the cloud services and data from malicious actors.

Architecture

Architectural cloud principles that form the foundation of CloudVision as-a-Service and establish the core of its security and data protection model include strong authentication, strong data encryption (for data-in-transit and data-at-rest), secure device onboarding, secure encryption keys, and integrated key management.

CloudVision as-a-Service is hosted as a shared-services Kubernetes cluster in multiple regions of a tier-1 public cloud provider. Its cloud-native approach allows it to utilize many providers, enhancing its resiliency and flexibility, though the actual provider in use within a particular region is not visible to the customer of the service.

CloudVision's architecture builds on the distributed EOS state-data model, called NetDB®, which is extended to a central data repository through the streaming of state and telemetry data from Arista devices to the CloudVision service. Arista NetDB shares state over the network by adding network-wide actions, including state-sharing mechanisms for control, replication, network analytics, and a central time-series store for network state. Within each cloud cluster, NetDB provides logically isolated environments for different customers' data.

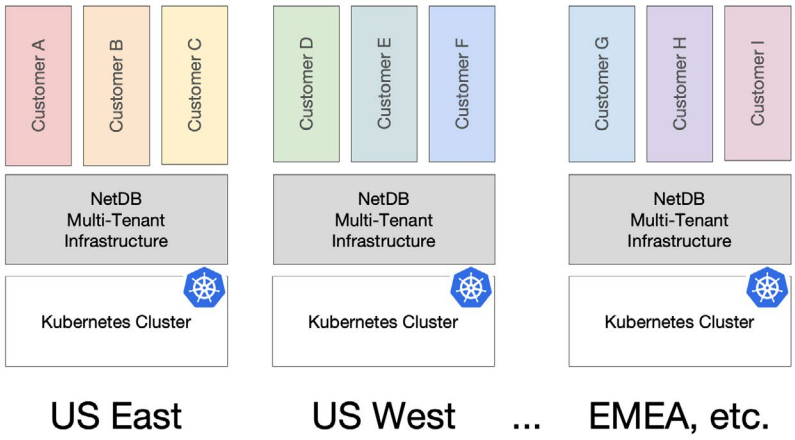

Figure 1: CloudVision Multi-Tenant Architecture

While Arista relies on default Kubernetes constructs, such as network policies and namespaces, to secure the internal cluster communication, customer-specific details such as device configurations and streaming data are isolated from each customer tenant using the NetDB service layer.

Separation of Local Control Plane, Data Plane, and Management Planes

In the CloudVision as-a-Service architecture, the control plane and data plane traffic is always kept local to the on-premises network, while the ability to access the management plane lives in the cloud.

The control plane refers to all of the functions and processes that determine which path to use; routing protocols (such as OSPF, IS-IS, EIGRP, etc.), spanning tree, LDP, and controller functions for services like VXLAN EVPN overlays are examples.

The data plane is for the transport of user and application data and comprises the most sensitive and confidential enterprise data. The management plane includes all of the functions that you use to provision, control, and monitor devices and services.

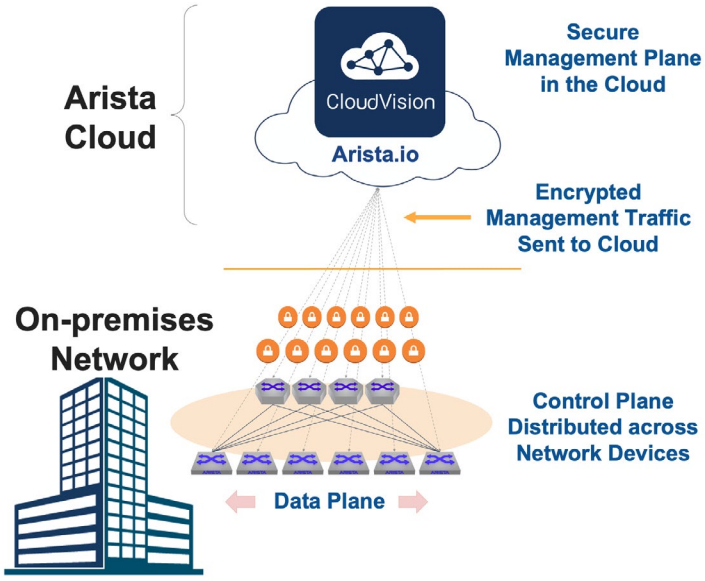

Figure 2: Separation of Local Control, Data, and Management Planes

Network packet data and control plane data transiting through Arista EOS® devices never flows to or from the CloudVision service, rather, it remains local to the enterprise network. Device telemetry is streamed from the network devices to CloudVision securely and data in both directions is encapsulated and encrypted.

The CloudVision service is designed so that services at the customer premises continue to operate even when the CloudVision service is unavailable, such as during a network or cloud outage. Arista devices provide network access in the customer network using the last known configuration when they are disconnected from the cloud service, and devices can be accessed and managed locally at any time. However, cloud applications may be inaccessible or impaired while the service or network connection is unavailable.

Remote Access from Anywhere

The CloudVision web management console and APIs, used to configure and monitor the on-premises network, are securely accessed from anywhere by customer administrators and their authorized users using HTTPS. HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses and provides secure client-to-service access.

CloudVision as-a-Service client authentication and authorization utilizes standard authentication and authorization mechanisms such as OAuth 2.0, while others may be added in the future including OpenID and SAML. These mechanisms allow customers to use their own identity platform to authorize users in the CloudVision service and do not require Arista to retain any actual user credentials for access to the service, such as a username and password.

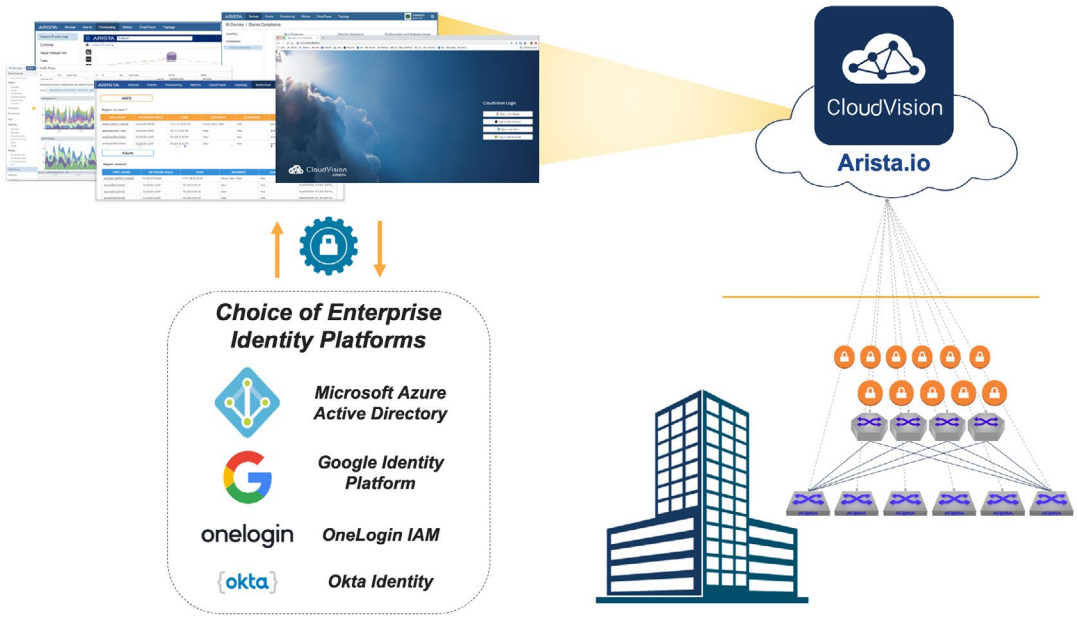

Figure 3: Secure Remote Access from Anywhere

Admins can log in to the CloudVision service using their preferred enterprise identity provider to onboard devices and users into the service and empower them with all of the capabilities that CloudVision as-a-Service offers, or just those capabilities that are appropriate for their roles. This approach also allows customers to take advantage of their selection of single sign-on (SSO) and multi-factor authentication (MFA) solutions. Popular enterprise identity providers supported currently include Microsoft Azure AD, Google Identity Platform, OneLogin, and Okta.

Device-to-Cloud Communication

Arista EOS devices (switches and routers) use gRPC to communicate with CloudVision, either on-premises or in the CloudVision service. Standardized under the auspices of the Linux Foundation and the Cloud Native Computing Foundation, gRPC is a modern high-performance open-source RPC framework that uses standards-based HTTP/2 over TLS 1.3 as the secure transport protocol.

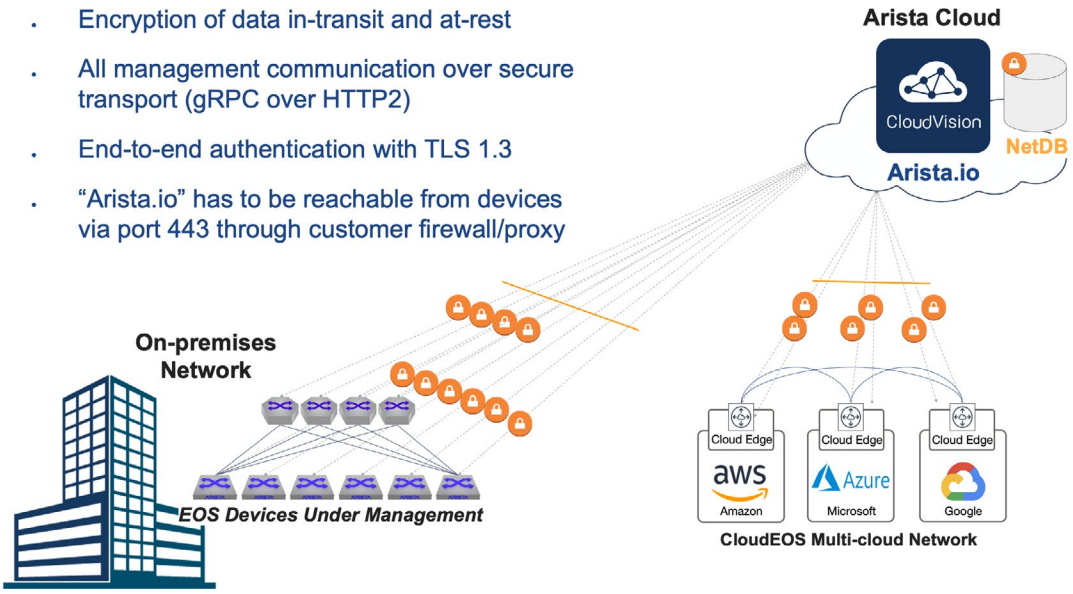

Figure 4: Secure Device-to-Cloud Communication

The HTTP/2 transport allows gRPC to easily traverse enterprise proxies and firewalls using standard ports (e.g., port 443), while SSL/TLS is used to authenticate the service nodes and the devices and to encrypt all of the data exchanged between them. Mutual TLS (mTLS) authentication is used in which both sides authenticate each other using x.509 v3 digital certificates to permit data exchange.

Device Onboarding

To communicate with the CloudVision service, each new device must be securely onboarded to the customer's unique CloudVision service tenant before it can be managed by CloudVision. Network admins can add EOS devices to their service tenant simply and securely using ZTP-as-a-Service* or manually.

ZTP-as-a-Service establishes the secure identity of an EOS device being on-boarded in CloudVision as-a-Service and is used to obtain the client-side x.509 v3 certificates required for further secure communications without having to manage pre-shared keys. This is the certificate that will also be used to encrypt the communication channel using TLS 1.3 and mTLS.

Only devices whose identity has been authenticated can join the customer's CloudVision service tenant. The establishment of device identity in ZTP-as-a-Service is done using a unique cryptographically signed enrollment token assigned to each device.

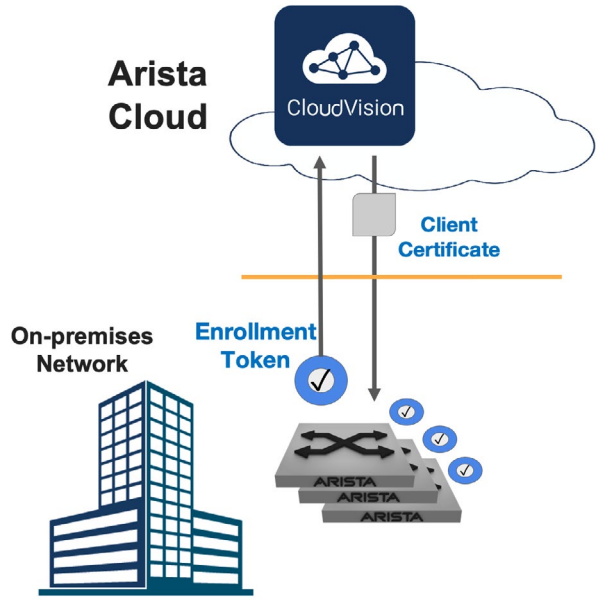

Figure 5: Secure Device Onboarding

Enrollment tokens authenticate that the device and hardware are genuine and that they belong to the customer. Onboarding multiple new devices with ZTP-as-a-Service can be as simple as point-and-click with this process, and rogue devices can be easily excluded. For newer Arista devices, the CloudVision enrollment token will be embedded during the manufacturing process. For brownfield deployments, the customer has the option to generate the token on-demand from the CloudVision as-a-Service web portal.

The Arista secure device enrollment process will become increasingly automated as the service is rolled out, reducing the burden on IT for securely rolling out new or replacement infrastructure across the enterprise.

Data Protection

In CloudVision as-a-Service, Arista has defined additional security, confidentiality, usage, and retention policies for data collected and stored in the CloudVision service at the NetDB service layer. NetDB data includes the entire state for enrolled customer devices (i.e., running configuration, topology, protocol state, monitoring counters, connected peer devices, etc.) as well as the aggregated state of all the Arista EOS-based devices across the network.

If any customer data is used by Arista for any purposes other than to provide direct customer support and service, it will only be used in an anonymized and aggregated form to improve the service. For example, aggregated historical data can be used with machine learning algorithms to improve anomaly detection, identify devices prone to early failure, or to analyze how customer use of the service has changed over time.

Credentials: Arista does not retain any customer login credentials or passwords that are used to access the service. Device login credentials within the device configurations are stored in an obfuscated manner in secure storage.

Data in-Transit: Arista encrypts all data in transit, as described above. This includes web management access, communication between the Arista devices and the service, and all interactions between different Arista servers and applications in the cloud.

Data at-Rest: Data at rest is automatically encrypted as it is being written to disk using AES256, which relies on the Advanced Encryption Standard (AES) algorithm with a key size of 256 bits. Each encryption key is itself encrypted with a set of master keys within the cloud service provider. This encryption uses shared keys that are only known to the CloudVision service cluster and are not published or shared externally.

Obfuscation: Any sensitive fields in the configuration that are used for control-plane authentication or routing protocols on the customer network are obfuscated by EOS before being collected and stored in the cloud service where it is encrypted as described above.

Type of Data Collected: CloudVision as-a-Service collects and stores a range of control plane state, including but not limited to (a) Media Access Control (MAC) addresses and Internet Protocol (IP) addresses of devices in Customer's network(s), or seen by, or advertised to, the devices deployed within the customer network, (b) additional information about these devices such as information about device activity, configuration, operating system, and login identities used from the devices, (c) metadata about devices, such as their serial numbers, model numbers and types (OS, hostnames), and potential communication activity (applications usage).

Data Ownership and Use: The customer owns all of the data that is stored in the service associated with their service tenant and their connected devices. Arista personnel may need to access this customer data for provisioning, maintenance, and troubleshooting the customer's environment. Arista implements access control mechanisms to limit Arista personnel access to customer data to a basic minimum, and Arista's use of this data is limited to providing agreed support services, as requested by the customer. Privilege escalation for any task that requires a higher level of access is subject to the customer's permission and is made available for a temporary period.

Data Retention and Backup: Arista has a customer data retention policy to address specific data retention concerns from our customers. Backups of customer data taken to facilitate disaster recovery are automatically deleted after a defined period. Data may be retained indefinitely while the customer remains subscribed to the CloudVision service. Customers may request all data associated with their use of the service be deleted permanently at any time by contacting Arista a dataprivacy@arista.com.

Operational Security

Protection and defense of the confidentiality, integrity, and availability of CloudVision services and data from malicious actors and other risks are provided by regularly scheduled vulnerability scanning and penetration testing of the service as well as limiting access to the service clusters by authorized maintenance personnel. Further, preventative activities based on the results of risk and security assessments lower the number of incidents by security systems, but not all incidents can be prevented. Therefore, our commitment to incident response and reporting capability is a critical resource for security operations.

Access Controls

Access to CloudVision as-a-Service at all levels follows the principle of least privilege, whereby a "need-to-know" basis is used as a rule of thumb regarding access to and sharing of information and control. Employees who might work with sensitive customer data must pass background screening first.

Vulnerability Scanning

Arista regularly performs different types of vulnerability scans on the cloud-hosted applications as follows:

Port scans: As compute instances are launched in different parts of the data center, it is essential to validate that access to them is restricted to only those ports necessary for accessing the application functionality. This reduces the attack surface considerably. Arista performs regular port scans on its cloud environment.

Web Application Security (WAS) scans: WAS scans focus on finding vulnerabilities at the web application level. Since CloudVision as-a-Service is publicly accessible over HTTPS (port 443), a WAS scan's objective is to ensure there are no exploitable vulnerabilities if an unauthorized user attempts to access the application. Another important objective is to prevent an authorized (authenticated) user from breaching application security controls, such as injection attacks, privilege levels, multi-tenancy, and so on. Arista deploys automated WAS scanning using WhiteHat Security services and complements it with penetration tests by third-party WhiteHat Security experts.

Software components scans: These scans are performed to audit software modules in the application for any missing security patches, stale versions, and misconfigurations. Arista performs software component scans on all its cloud applications using different types of scanning tools.

Penetration Testing

Arista engages third parties to perform periodic penetration testing on the external-facing interface of the cloud service. These attack simulations closely model the techniques of real-world adversaries through a matrix of approaches in which security experts perform tests to find exploitable weaknesses in the system's workflow, configuration, and implementation.

Incident Response

Arista has established an Incident Management (IM) process to provide a consistent and organized approach for handling customer support issues, and security and availability incidents. Customers can report security incidents by logging the issue with customer support personnel by phone or email. Monitoring tools are in place to continuously monitor the capacity, availability, and performance of the services. Alerts may get automatically escalated to an on-call team based on their severity. Cloud operations personnel analyze incidents and implement mitigating actions. The incident patterns are periodically analyzed to identify root causes and any corrective actions.

Disaster Recovery

Arista maintains a Disaster Recovery (DR) plan to be prepared for recovery of services in case of a disaster affecting the CloudVision service. Semi-annual testing is performed for the DR plan. During the testing, steps are followed as they would be during a disaster situation. The results are analyzed to ensure the validity of the DR plan and to estimate the recovery time objective (RTO).

Change Management

Arista has a formal change management process for CloudVision application components and infrastructure. We follow it to ensure that all changes to the service are peer-reviewed, approved, tested, and logged. Our operational controls include well-documented procedures for a change request, approval, planning, testing, rollback, notifications to affected parties, and steps to be taken to implement planned and emergency changes. Customers can monitor the CloudVision services live status and review recent changes via https://cloudvision.statuscast.com. This service also provides email/text notifications and RSS/Web integrations.

Data Backups

Data backups are periodically taken and encrypted according to a documented schedule using an automated process. During a disaster event, these backups are available to promptly bring up the service in another availability zone within the cloud region. An inventory of cloud servers and access keys is maintained using an automated process that can serve as a reference point for restarting failed servers in the event of a disaster. The inventory keeps detailed information about the configuration of servers and the applications running on the servers.

Regulatory Compliance and Certifications

Arista, our subprocessors, and our customers must comply with various international regulations and policies. Our operational policies and practices are designed to allow you to comply with your country's specific laws. Arista also achieves compliance with international privacy regulations by maintaining a comprehensive, written information-security program that contains technical and organizational safeguards designed to prevent unauthorized access, use, or disclosure of sensitive customer data.

Further, Arista pursues compliance certifications that include third party audit and validation of the Arista cloud service security controls geared towards confidentiality, integrity, and availability (the CIA triad). Together, these three principles form the cornerstone of any organization's security infrastructure.

Data Confidentiality and Privacy

Arista is committed to protecting the confidentiality and privacy of all customer information. However, it is important to note that because Arista CloudVision manages network infrastructure devices, the NetDB data that it processes do not generally include Personally identifiable information (PII) that can be used to identify a specific individual.

Within CloudVision as-a-Service, all customer data is treated as confidential and sensitive. Confidential information includes information about devices such as MAC and IP addresses and other metadata from the customer networks. Sensitive data includes network secrets in the customer's environment such as control-plane passwords that are configured on devices. Confidential data is protected with various controls described in this document. Access to sensitive data is subject to additional access restrictions and controls. For example, Arista provides an option to disable access to customer data by Arista customer support personnel, and sensitive data is cryptographically hashed before it is received by the service.

Data Processing Agreements (DPA) are in place with third-party processors that may be able to access any potential personal or sensitive data. Arista does not share any customer data with third parties that are not Arista's agents and are not bound by data confidentiality obligations through executed DPAs.

Applicable Privacy Law(s)

Privacy laws have now been enacted in over 80 countries around the world. Arista will comply with the requirements of all applicable privacy laws, including the European Union's General Data Protection Regulation (GDPR).

The GDPR is a data privacy regulation that imposes certain data protection obligations on "data controllers" (i.e., companies that decide how your information will be used) and "data processors" (i.e., companies that process information on behalf of data controllers) and makes the protection of "personal data" (e.g., your name and email address) a fundamental right for residents of the European Union ("EU"). We act as a data processor with respect to data related to CloudVision as-a-Service with respect to GDPR.

Although not a GDPR requirement, some companies may require that their data reside within a specific country or region. CloudVision as-a-Service is currently hosted in multiple regions, including the US, EU & APAC regions of a tier-1 cloud provider. Planned expansion to further regions will be timed based on global customer demand.

Request to Delete Data

Arista will comply with any requests to remove specific personally identifiable information (PII), as required by GDPR. However, it is important to note that because Arista CloudVision as-a-Service manages networking devices and not users, the data that it processes does not generally include PII. More information with regard to GDPR compliance can be found in the Arista Customer Data Privacy Addendum posted on our website.

External Audits

The operations, policies, practices, and procedures at Arista are assessed and attested in line with guidelines provided by the American Institute of Certified Public Accountants (AICPA), SSAE 18 (Statements on Standards for Attestation Engagements no. 18) by an independent third party. Arista Networks has both the SOC 2 Type 1 and Type 2 attestation assessment reports for the security, availability, and confidentiality of the CloudVision as-a-Service.

SOC 2 Type 1 details the suitability of the design controls to the service organization's system at a single point in time, Whereas SOC 2 Type 2 covers the assessment of control effectiveness over an active operational period, typically ranging from 6 to 12 months. Ongoing SOC 2 Type 2 attestation assessments will be conducted regularly by an independent third-party auditor, and reports will be made available to customers or prospects upon their completion.

*Indicates features planned for a future release

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office
1390 Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062