Implementing CIS Controls Version 8 with Arista NDR

By Deborah Moreira

In 2021, the Center for Internet Security (CIS) launched the CIS Critical Security Controls version 8. These controls contain safeguards that assist organizations of all sizes assess their security posture and identify the most critical opportunities for defense against attacks. The updated CIS Critical Security Controls reflect technology trends, such as networks without fixed boundaries, increased cloud adoption, and zero trust policies. The revised controls, terminology, and grouping of safeguards resulted in a decreased number of controls from 20 to 18. Further, unlike previous versions where the safeguards were grouped by the function responsible for executing each control, in version 8 the safeguards are grouped by activities instead.

All safeguards are still prioritized into implementation groups from IG1 to IG3. IG1 defines the most critical safeguards to establish basic cyber hygiene. IG2 and IG3 are more advanced safeguards that offer a path to a sophisticated security program.

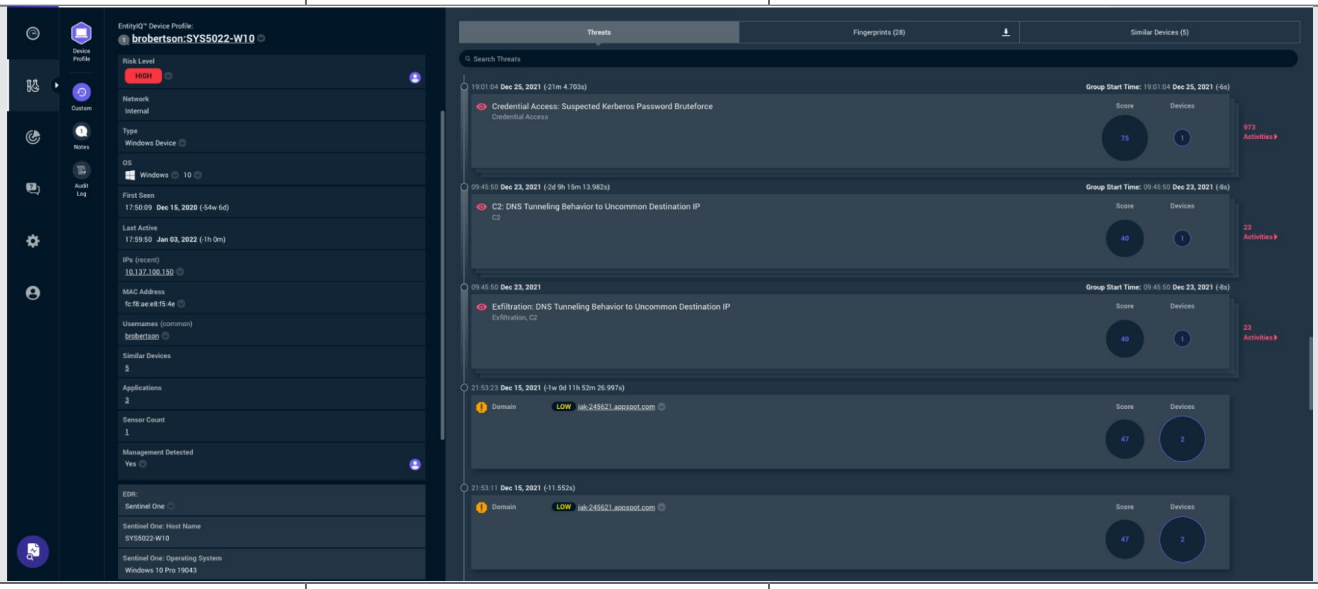
The latest CIS Critical Controls were developed based on the Community Defense Model (CDM), which is considered CIS's most data-driven approach as it takes into consideration multiple data sources, including the Verizon Data Breach Investigations Report and the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework. According to the CIS Critical Controls Version 8 report "These activities ensure that the CIS Security Best Practices (which include the CIS Controls and CIS Benchmarks) is more than a checklist of "good things to do," or "things that could help"; instead, they are a prescriptive, prioritized, highly focused set of actions […]".

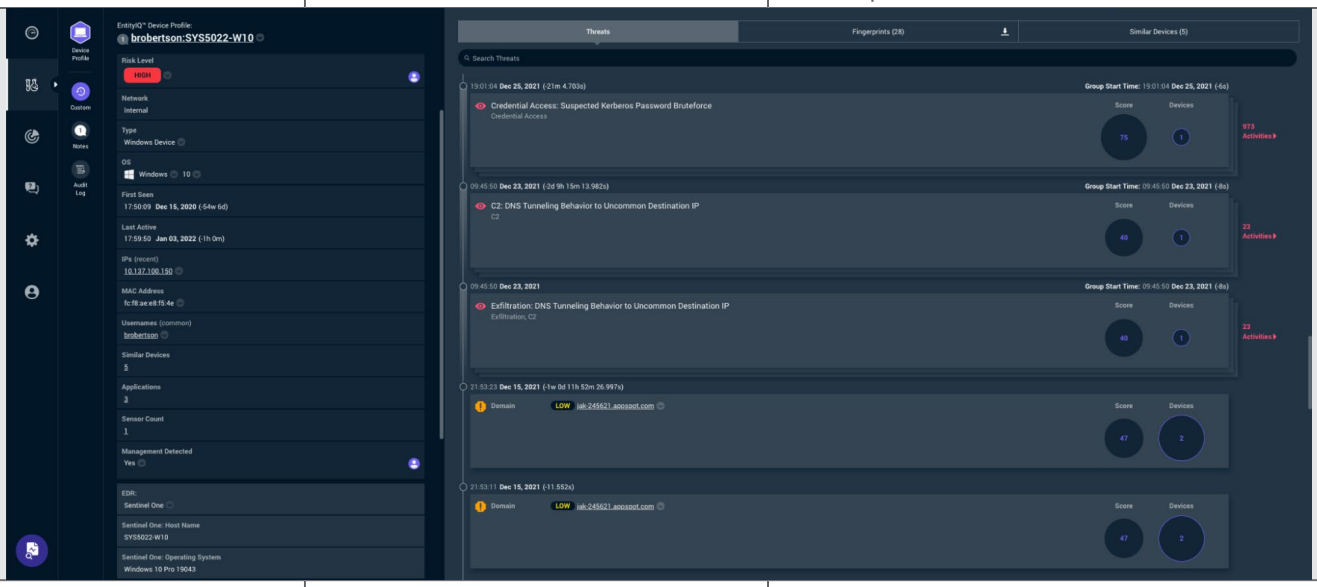
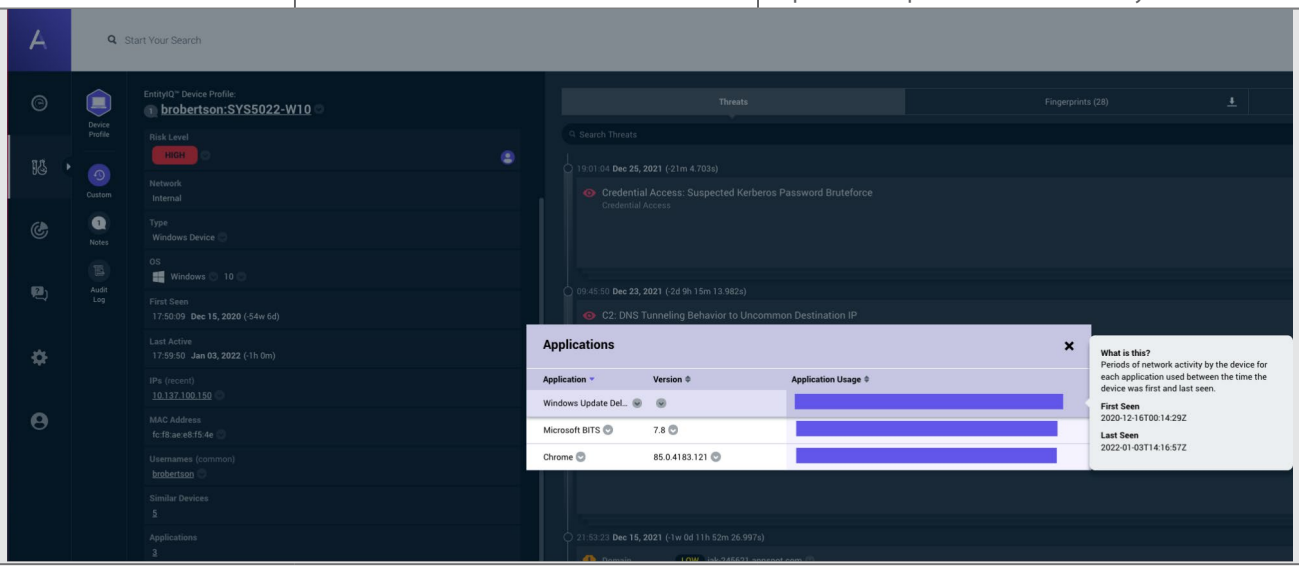
Arista NDR (Network Detection and Response) and Awake Labs can help organizations comply with multiple safeguards contained in the CIS Critical Security Controls Version 8. This includes some of the most challenging safeguards, yet some of the most effective in detecting and defending against cyber attacks, such as identifying and monitoring all network assets as well as responding to security incidents.

Arista NDR provides network visibility and observability by doing deep packet inspection and using analytics and machine learning models to monitor all network traffic and automatically hunt for malicious intent involving network assets. This includes assets that are difficult to monitor, such as Internet of Things devices that traditional endpoint security tools can not manage.

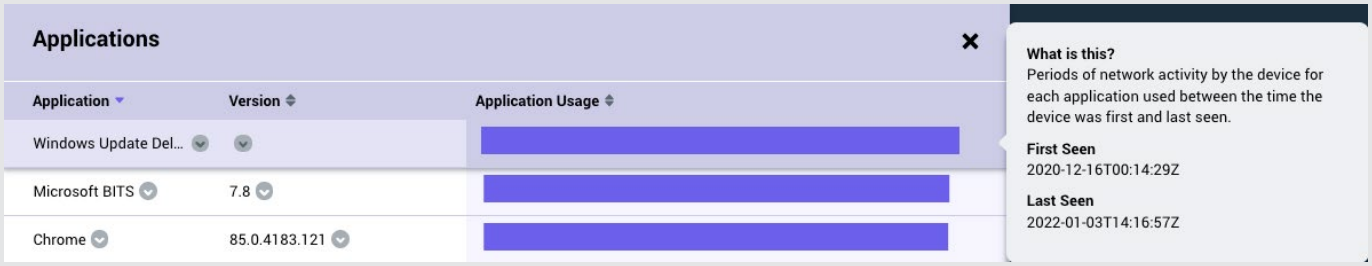
Although implementing the CIS security controls requires thoughtful planning and resources, these controls offer a guide to assess an organization's security posture and lead to a robust cyber security strategy. Furthermore, the CIS critical controls can pave the way for implementing most major compliance frameworks, such as the NIST Cybersecurity Framework, NIST 800-53 and ISO 27000 series.

The rest of this document maps specific safeguards from the CIS Critical Controls Version 8 to capability in Arista NDR and Awake Labs.

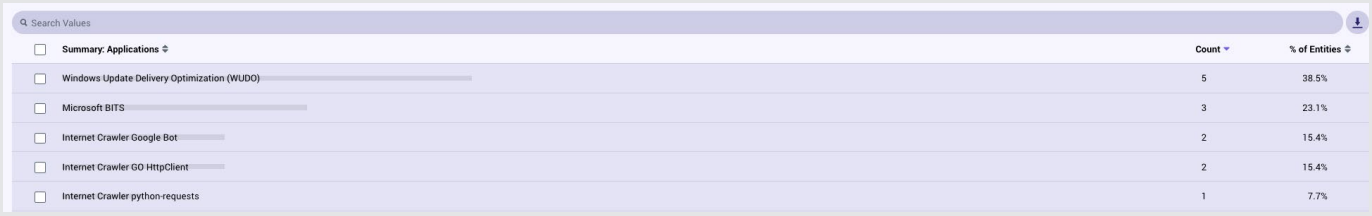
Implementing CIS Controls Version 8 with Arista NDR and Awake Labs		
Control	**Safeguards**	**Arista NDR Capabilities**
1	1.1 Establish and Maintain Detailed Enterprise Asset Inventory Implementation Groups: IG1 · IG2 · IG3	Arista's EntityIQ™ device profile can identify and keep track of all devices generating network traffic being monitored by the Arista NDR platform. For each network device, the EntityIQ profile includes associated user(s) and roles, operating system, network addresses used by the device overtime, hardware address, details on applications running on that device, a forensic threat timeline, fingerprints, as well as a listing of similar device(s) for campaign analysis. The EntityIQ device profile also shows the risk level for the device and the attributes and activities that contributed to that level. The list of risk items varies depending on the device's communications and behavior indicative of malicious intent.
		
1	1.4 Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Assets Inventory IG2 · IG3	EntityIQ monitors DHCP requests and responses to build a comprehensive device profile as described above. The platform keeps track of all the IP addresses a device has leased on the network over time.
		

Implementing CIS Controls Version 8 with Arista NDR and Awake Labs Contd.		
Control	**Safeguards**	**Arista NDR Capabilities**
1	1.5 Use a Passive Discovery Tool G3	Arista NDR passively analyzes network traffic and creates an EntityIQ device profile for each device on the network. This capability tracks devices over time, including all IPs leased by the device and the first and last time the device was seen on the network. This information can help organizations keep track of network assets and identify rogue devices connected to the enterprise.
		
2	2.4: Utilize Automated Software Inventory Tools: IG2 · IG3	Within the EntityIQ device profile, Arista NDR detects and lists software applications in use on devices, which is derived from network traffic analysis. The platform shows the time frame during which each software detected was seen on the device. Arista NDR also allows users to query the system for all applications observed from network traffic within a given time period and the results will be ordered by most to least used as observed in the image below. The results can be easily downloaded into a CSV file or copied to a clipboard for further analysis.
		

Implementing CIS Controls Version 8 with Arista NDR and Awake Labs Contd.

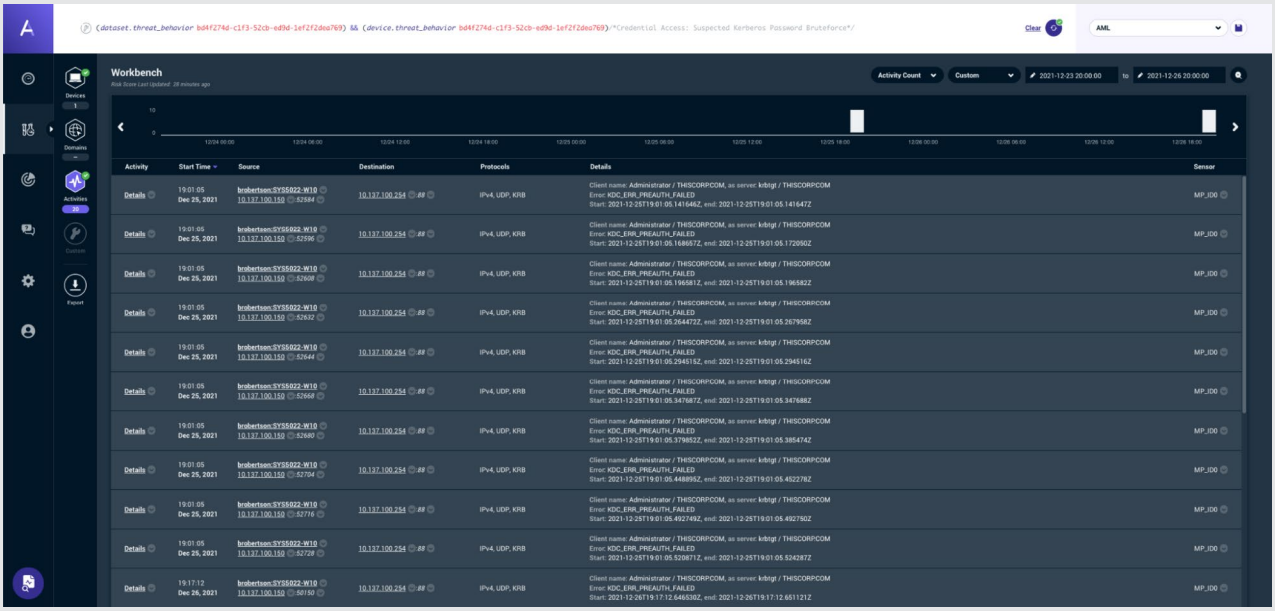


All applications observed from network traffic within a given time period:



3	3.14. Log Sensitive Data Access IG3	Arista NDR can monitor SMB activity and use machine learning models to determine when a device accesses an unusual SMB path. The security team can use the platform to monitor access, read and write actions to sensitive SMB shares and files. NDR also has multiple out-of-the-box models that alert the security team of suspicious SMB activity and signs of data exfiltration. Users can also modify these existing models or create their own

Score	Title
3	Discovery: SMB C Drive Access Discovery
0	Credential Access: Password Bruteforce Attempt for Admin Account (SMB2) Credential Access
0	Credential Access: Password Bruteforce Attempt for Non-Admin Account (SMB2)
0	Discovery: Direct To IP SMB C Drive Access Discovery
0	Discovery: SMB Admin Share Access Discovery
0	Discovery: SMB Connection To Credential Store Or Sensitive Share Discovery
0	Execution: Behavior indicative of SMBleed Kernel Memory Leakage Remote Execution
0	Impact: Possible Ransomware Files Written To SMB Impact
0	Lateral Movement: Attack Tools Via SMB Lateral Movement
0	Lateral Movement: SMB Communications To External Location Lateral Movement
0	Lateral Movement: SMBv1 Accessing Sensitive Shares Credential Access, Lateral Movement

Implementing CIS Controls Version 8 with Arista NDR and Awake Labs Contd.		
Control	**Safeguards**	**Arista NDR Capabilities**
4	4.7 - Manage Default Accounts on Enterprise Assets and Software IG1 · IG2 · IG3	Arista NDR can detect and flag network artifacts containing unencrypted credentials, including common cases of basic HTTP authentication where credentials are encoded using Base64.
5	5.1 Establish and Maintain an Inventory of Accounts IG1 · IG2 · IG3	Arista NDR treats usernames as entities that can be tracked over time based on network usage. These users are also automatically correlated to the devices that have used them over time. This visibility combined with the analytics suite allows the system to identify and alert users of high risk and malicious use of user accounts, including highly privileged accounts. The example below shows metadata associated with a trigger for model Credential Access: *Suspected Kerberos Password Bruteforce using client name Administrator:*
		
5	5.5 Establish and Maintain an Inventory of Service Accounts IG2 · IG3	As mentioned in the safeguard 5.1, Arista NDR is able to identify and analyze account usage traversing the network, including for service accounts.
8	8.2 - Collect Audit Log IG1 · IG2 · IG3	The system collects network traffic and parses packets into network metadata that are ultimately processed to provide security context. Additionally, Arista NDR has native integrations with multiple SIEM and EDR tools that can use the network audit information, metadata and NDR alerts to enrich security context.
8	8.3 - Ensure Adequate Audit Log Storage IG1 · IG2 · IG3	Arista NDR stores network security activity data for up to 180 days. Full packet storage options are also available.
8	8.5 - Collect Detailed Audit Logs IG2 · IG3	Arista NDR collects and parses network traffic containing detailed information about source and destination devices, usernames, data, timestamp, ports and protocol used, bytes transferred and other useful network metadata.
8	8.6 Collect DNS Query Audit Logs IG2 · IG3	DNS queries from network devices are monitored and stored for further analysis.

Implementing CIS Controls Version 8 with Arista NDR and Awake Labs Contd.		
Control	**Safeguards**	**Arista NDR Capabilities**
8	8.10 Retain Audit logs IG2 · IG3	The system stores network security activity data for up to 180 days. Full packet storage options are also available.
8	8.11 Conduct Audit Log Reviews G2 · IG3	Arista NDR performs network traffic analysis for automatic threat detection and alerting. Each alert has a severity score associated with it and it can be forwarded via syslog to other tools, such as SIEM and SOAR platforms.
9	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions IG2 · IG3	The system provides visibility of browser extensions communicating with external endpoints over unencrypted protocols and extensions downloaded over HTTP. As an example, Arista NDR generates alerts for Chrome extensions downloaded outside of the Chrome store and Chrome extensions connecting to risky domains. The Arista Threat Research team also uncovered a massive surveillance campaign of spyware disguised as legitimate Chrome extensions, leading Google to remove 106 extensions from the official Chrome store.
10	10.7 Use Behavior-Based Anti-Malware Software IG2 · IG3	Arista NDR tracks devices over time and applies data science and machine learning methodologies to analyze behaviors and alert security teams of chains of events that indicate malware infections, as well as malwareless "living-off-the-land" attacks.
12	12.3 Securely Manage Network Infrastructure IG2 · IG3	The system detects the use of insecure or outdated network protocols, such as HTTP and SMBv1. The network visibility provided also allows for the discovery of unencrypted credentials traversing the network and insecure network protocol configurations, such as simple LDAP authentications that expose clear-text credentials on the network.
13	13.1 Centralize Security Event Alerting IG2 · IG3	Arista NDR generates security alerts and has native integrations with SIEM and SOAR tools, such as Splunk and Palo Alto Networks' Cortex XSOAR. This forwards network alerts to these tools and centralizes security event alerting.
13	13.3 Deploy a Network Intrusion Detection Solution Network IG2 · IG3	Arista's network detection and response capabilities provide superior levels of protection compared to legacy network IDS solutions. This is achieved by analyzing network data at a deeper level than just signatures and by using a variety of data science methods. The consequence is that Arista NDR can identify more sophisticated threats including non-malware malicious activity. In addition, Awake Labs offers Managed Network Detection and Response (MNDR) services, in which industry experts monitor customer networks for threats 24x7 as well as threat hunt on their behalf.
13	13.6 Collect Network Traffic Flow Logs IG2 · IG3	The Arista NDR sensor collects network packets and does deep packet inspection on all network traffic being passively ingested. The platform applies data science and machine learning models to analyze network traffic and automatically hunt for suspicious activity at different attack stages. As the platform learns the environment, categorizes assets, and understands network behavior, Arista NDR can determine if an anomaly is malicious or expected based on who and what is involved. This helps increase true positive alerts and reduce false positives.

Implementing CIS Controls Version 8 with Arista NDR and Awake Labs Contd.		
Control	**Safeguards**	**Arista NDR Capabilities**
16	16.10 Apply Secure Design Principles in Application Architectures IG2 · IG3	Arista NDR detects ports being used to communicate internally and externally by applications, as well as default credentials being transferred over unencrypted protocols, such as HTTP. This level of visibility allows developers to identify misconfigurations, such as communication ports, unencrypted default credentials, and clear-text credentials exposed in connection URIs for example.
		
17	17.1 Designate personnel to manage incident handling IG1 · IG2 · IG3	The Awake Labs team offers incident response (IR) retainers with an SLA (Service Level Agreement) on response time. In addition to identifying an internal person(s) for incident response, customers can designate Awake Labs to manage incident handling or to enhance their existing IR programs and practices.
17	17.2 Establish and Maintain Contact Information for Reporting Security Incidents IG1 · IG2 · IG3	Awake Labs IR retainer is a key component to rapid response in the event of an incident. Having a retainer allows for contractual and compliance obligations to be resolved ahead of emergencies. Awake Labs also has experience working with cyber liability insurance providers and can therefore guide the claim process as well as work with law enforcement when needed.
17	17.4 Establish and Maintain an Incident Response Process IG2 · IG3	The Incident Response Retainer services offered include a "best of breed" incident response capabilities processes. Further Awake Labs experts can also audit existing processes and make recommendations for improvements.
17	17.7 Conduct Routine Incident Response Exercises IG2 · IG3	Awake Labs offers various forms and topics of incident response exercises. Usually called tabletops, Awake Labs does both a theoretical table discussion or a "live fire" interactive type. IR retainer hours can be repurposed into one of these engagements.
17	17.4 Establish and Maintain an Incident Response Process IG2 · IG3	Post incident reviews and reports are included in Awake Labs incident response engagements.

Arista can be a key partner in helping organizations improve security posture and decrease cyber risk by leveraging the CIS Critical Security Controls. From the most essential safeguards for security hygiene (IG1) to the most sophisticated strategies (IG2 and IG3), the Arista NDR and Awake Labs services can help organizations implement as well as maintain these controls over time.

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