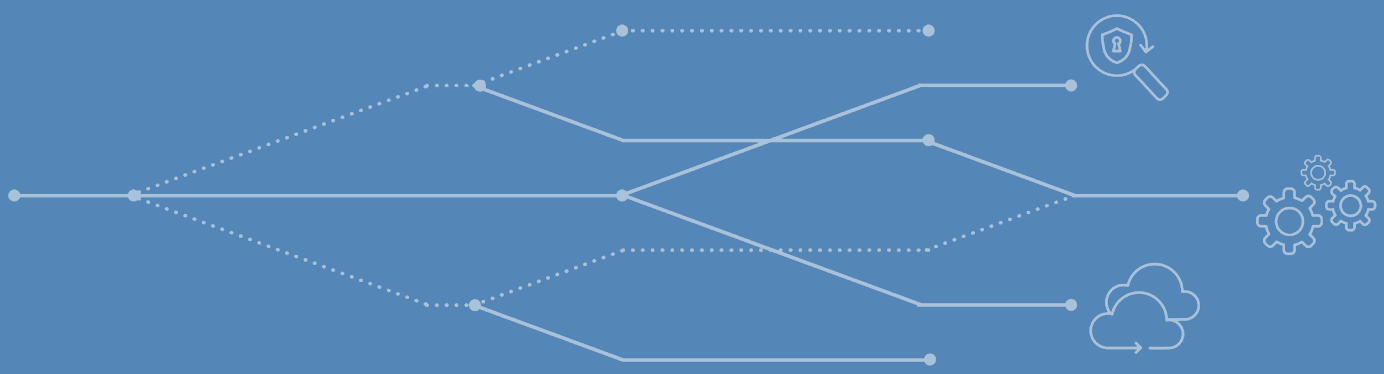


Arista NDR

Traditional security solutions struggle with a landscape where attacks continue to evolve beyond malware: supply chain threats, insider attacks, and living off the land tactics, among others. At the same time, a new network has emerged with unmanaged Internet of things, cloud infrastructure, contractor and third-party devices, and shadow IT. While the new network continues to gain precedence and transcend enterprise perimeters, it has become vital for organizations to address the cascading attack surface and to build an integrated cybersecurity strategy that delivers holistic visibility and control.

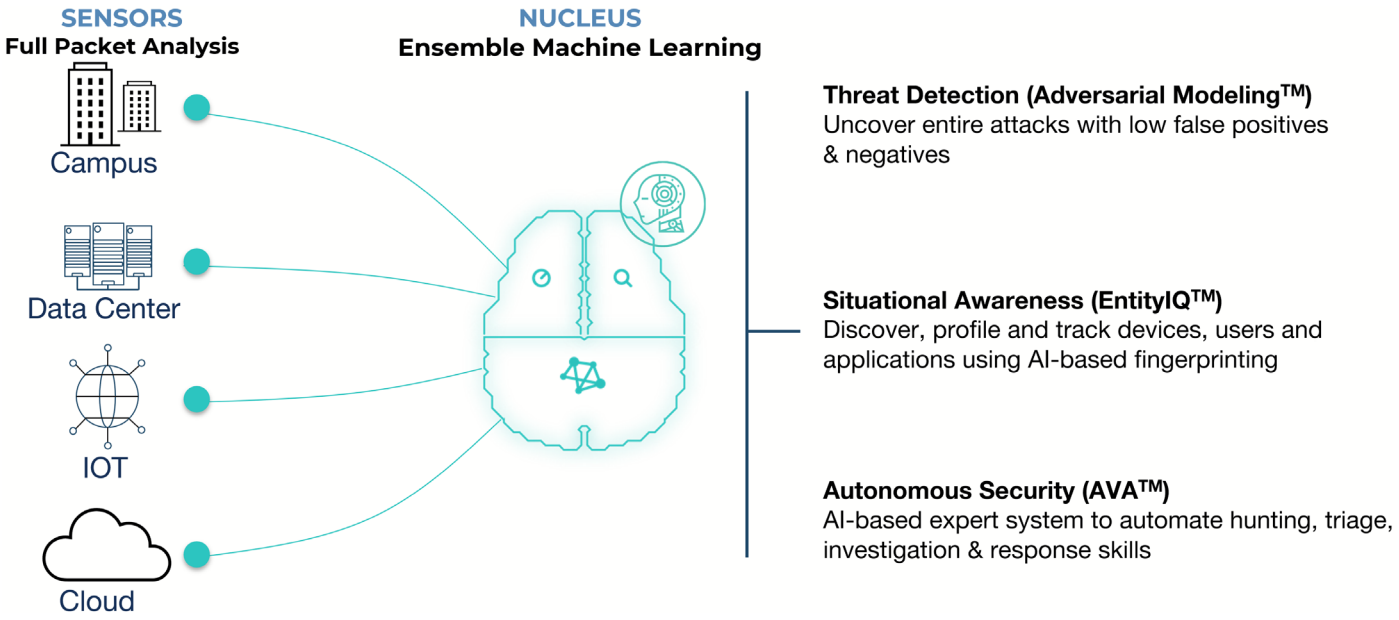
Arista is uniquely situated to address the security gap given its position at the foundation of the network. Implementing security at the network layer, eliminates the need for layer over layer of network security technologies and thus reduces operational costs and complexity. This approach represents the most effective way to track and successfully manage threats given the wider attack surface.

The Arista NDR platform is built on a foundation of deep network analysis from **AVA Sensors** that span the "new network"—including the data center, campus, IoT as well as cloud workload networks, and SaaS applications. These sensors come in various form factors from being built into Arista switches as well as standalone hardware, virtual, and cloud sensors.

Unlike other network detection and response solutions, Arista NDR parses over three thousand protocols and processes layer 2 through layer 7 data. The platform also analyzes encrypted protocols to identify important context such as the nature of traffic (file transfer, interactive shell, etc.), the applications communicating, and the presence of remote access, all without forcing data decryption. Arista's **EntityIQ™** technology uses this information to autonomously profile entities such as devices, users, and applications while preserving these communications for historical forensics.

Only Arista NDR

- Delivers EntityIQ™ to autonomously discover & profile every device, user & application (managed or unmanaged) in the organization.
- Delivers visibility into encrypted traffic using AI to identify network applications, remote control, file transfers, etc.
- Enables Adversarial Modeling™ that exposes attacks including insider threats, credential misuse, lateral movement & data exfiltration.
- Can deploy directly on network switches to deliver granular visibility while eliminating the operational overheads of additional hardware.
- Automates triage and investigations through AVA™ AI, providing a decision support system to analysts.
- Requires no agents, manual configuration, or lengthy training periods.



Extracted activity data feeds into the **AVA Nucleus** that uses a combination of detection models to uncover malicious intent. An ensemble of machine learning approaches avoids reliance on simplistic and noisy anomaly detection or unsupervised learning. The AVA Nucleus can run entirely on-premises or in the Arista cloud as a SaaS offering.

Arista's **Adversarial Modeling™** language enables the uncovering of even the most complex attacker tactics, techniques, and procedures (TTPs), with extensible AI-driven models that first zero in on the suspicious activity and then gather corroborating evidence to support conviction. The modeling language delivers rich data analysis capabilities and a vocabulary to express attacker TTPs so that even a relatively junior analyst can now hunt for sophisticated threats. The AVA Nucleus provides a single sign-on and role-based user experience and a full API for extensibility, notifications, and integrations with other IT and security solutions for automated response and remediation.

AVA, Autonomous Virtual Assist, is Arista's AI-driven decision support system that performs threat hunting and incident triage. AVA automatically connects the dots across the dimensions of time, entities, and protocols, enabling the solution to present end-to-end **Situations** to the end user rather than a plethora of meaningless alerts. Analysts thus see the entire scope of an attack along with investigation and remediation options on a single screen while avoiding the effort of piecing it together themselves. Importantly, federated machine learning allows Arista customers to gain these capabilities while keeping their private data firmly within their infrastructure.

"Arista NDR has exceeded our expectations and empowered us to secure our connected workplace more effectively and autonomously than ever."
– Rich Noguera, Fmr. CISO, Gap Inc.

Use Cases

Detection

The platform uses AI to detect & prioritize mal-intent & behavioral threats from both insiders & outside attackers while mapping these to the MITRE ATT&CK framework.

Response

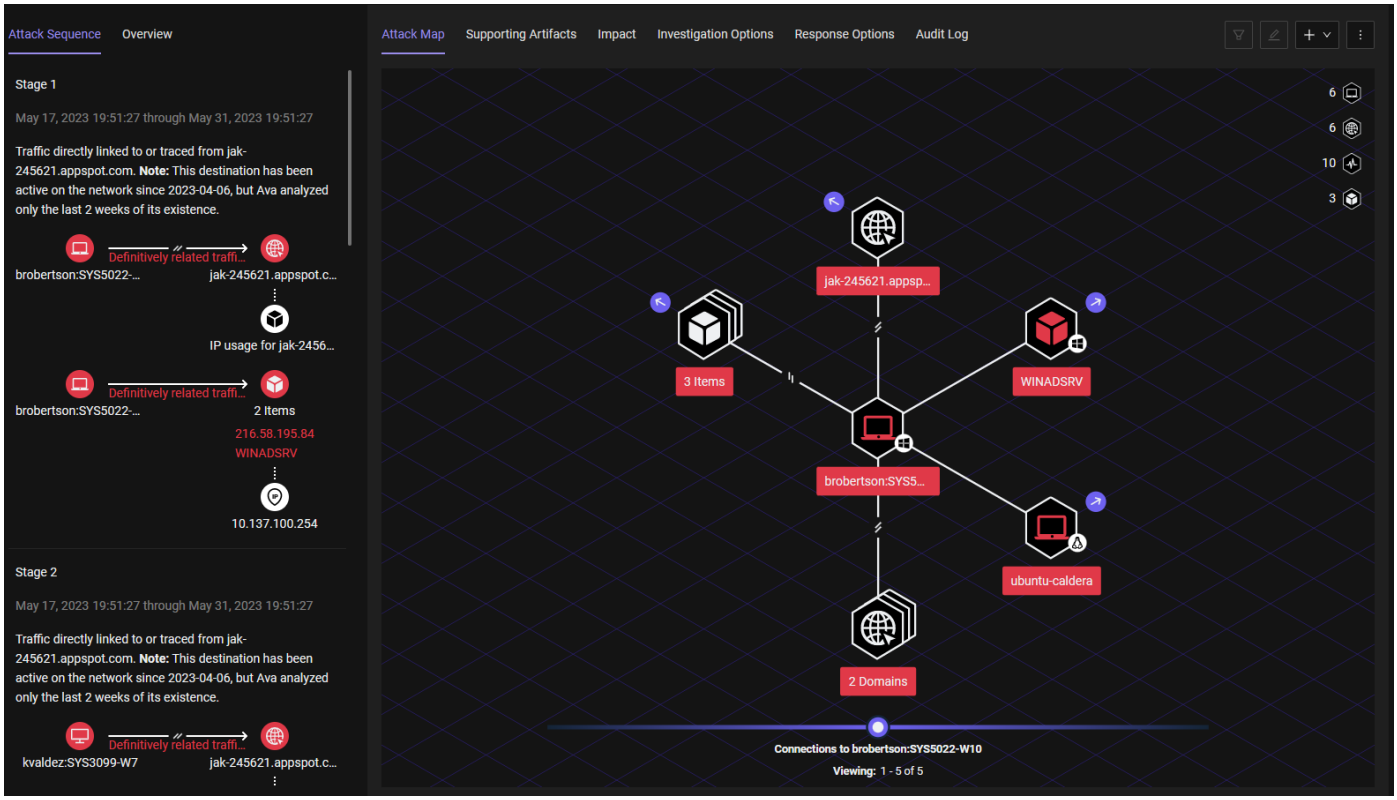
AVA forensically correlates incidents across entities, time, protocols, and attack stages, surfacing Situations with all the decision support data necessary to respond rapidly to any threat.

Situational Awareness

Arista NDR learns & tracks entities across IT, OT, or IoT environments, whether on-premise, cloud, or SaaS, and managed or unmanaged, including contractors and other third parties.

Threat Hunting

The platform's rich data set and query capabilities enable powerful threat hunting workflows. AVA can take a single trigger from a human analyst and autonomously expose the entire kill-chain in a matter of minutes.



Integrations

The Arista NDR platform integrates with and amplifies existing solutions through integrations into industry-leading SIEM, business intelligence, ticketing and analytics, endpoint detection, and security orchestration tools. In addition, the platform supports a full API for custom workflows and integrations. For instance, the SIEM integration allows an analyst to pivot from an alert containing an IP or email address to a device profile with associated user(s) and roles, operating system and application details, a forensic threat timeline as well as a listing of a similar device(s) for campaign analysis. Similarly, endpoint integrations allow one-click quarantining of compromised devices or retrieval of endpoint forensic data.

Deployment Modes

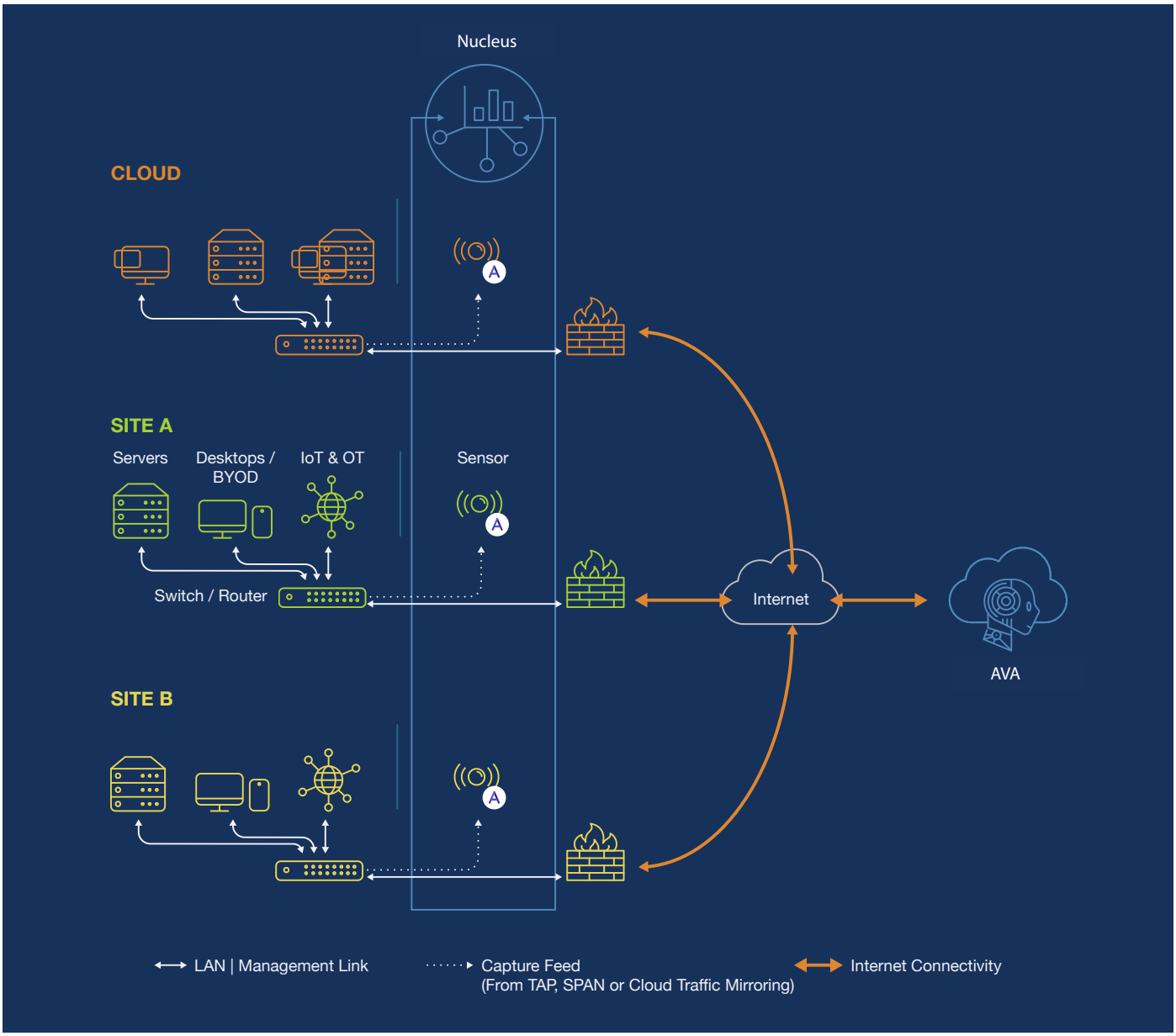
Arista NDR can be deployed in two modes depending on customer requirements and network architecture:

All-in-one

The AVA Sensor and AVA Nucleus in this case are deployed on a single appliance. This deployment is ideal for customers who deploy a single instance of Arista NDR or would like to maintain an isolated view of their deployment.

Split

In this mode, the AVA Sensor and AVA Nucleus are deployed separately. AVA Sensors can be deployed in a variety of form factors including on Arista switches, physical or virtual appliances and within Amazon Web Services (AWS) or the Google Cloud Platform (GCP). The AVA Nucleus is offered as on-premises hardware which can be configured in cluster mode to support higher performance requirements. It is also available as a SaaS service from Arista. A central console provides a unified analyst portal with complete role-based access control across multiple Nucleus deployments.



Awake Security Platform Hardware Specifications

Model #	DCA-NDR-S100	DCA-NDR-S1	DCA-NDR-S5	DCA-NDR-S10	DCA-NDR-NB10	DCA-NDR-A5	DCA-NDR-CC
PERFORMANCE & CAPACITIES							
Function	Sensor Only	Sensor Only	Sensor Only	Sensor Only	Nucleus Only	All in One	Central Console
Network Performance	Up to 100 Mbps	Up to 1 Gbps	Up to 5 Gbps	Up to 10 Gbps	Up to 10 Gbps[1]	Up to 5 Gbps	N/A
Meta Data Storage	N/A	N/A	N/A	N/A	90 days	90 days	N/A
HARDWARE SPECIFICATIONS							
Rack Unit	1U	1U	2U	2U	2U	2U	2U
CPU Cores	8	32	64	64	96	96	96
RAM	64 GB	512 GB	512 GB	512 GB	1 TB	1 TB	1 TB
Disk Storage	4x6 TB	4x10 TB	12x 6 TB	12x 18 TB	10x 8 TB	10x 8 TB	10x 8 TB
SSD	-	-	2x 480 GB	2x 480 GB	2x 480 GB	2x 480 GB	2x 480 GB
Non-volatile Memory	1x 480 GB	1x 1 TB	-	-	2x 3.2 TB PCIe NVME	2x 3.2 TB PCIe NVME	2x 3.2 TB PCIe NVME
Network	2x 1Gbps Onboard Ethernet 4x 10 Gbps Intel SFP+ 1x Out of Band Management Interface	2x 1 Gbps Onboard Ethernet 4x 10 Gbps Intel SFP+ 1x Out of Band Management Interface	2x 1 Gbps Onboard Ethernet 4x 10 Gbps Intel SFP+ Ports 1x Out of Band Management Interface	2x 10 Gbps Onboard Ethernet 4x 10 Gbps Intel SFP+ Ports 1x Out of Band Management Interface	4x 1 Gbps Onboard Ethernet 2x 10 Gbps Intel Ethernet 1x Out of Band Management Interface	4x 1 Gbps Onboard Ethernet 4x 10 Gbps Intel SFP+ Ports 1x Out of Band Management Interface	4x 1 Gbps Onboard Ethernet 2x 10 Gbps Intel Ethernet 1x Out of Band Management Interface
Power Supply	2x 750W – Redundant and Hot Swappable	2x 750W - Redundant and Hot Swappable	2X 1400W- Redundant and Hot Swappable	2X 1600W- Redundant and Hot Swappable	2X 1400W- Redundant and Hot Swappable	2X 1400W- Redundant and Hot Swappable	2X 1400W- Redundant and Hot Swappable

Model # (Switch Sensors)	SS-NDR-G-SWITCH-1M	NDR SS-NDR-G-T1-1M	NDR SS-NDR-G-T2-1M
Tier	Up to 149 switches	150-499 switches	500+ switches
Function	Sensor Only	Sensor Only	Sensor Only
SYSTEM REQUIREMENTS			
Supported Arista Switches	Please refer to https://www.arista.com/en/support/product-documentation/supported-features. Pick one or more switch models and then select "Campus Features" under Product Features and look for the "AVA switch sensor" checkmark.		

Model # (Virtual Sensors)	SS-NDR-SVV.5-1M	SS-NDR-SVV1-1M	SS-NDR-SVV5-1M
PERFORMANCE & CAPACITIES			
Function	Sensor Only	Sensor Only	Sensor Only
Network Performance	Up to 500 Mbps	Up to 1 Gbps	Up to 5 Gbps
SYSTEM REQUIREMENTS			
Supported Hypervisors	VMware ESX/ESXi 6.7+	VMware ESX/ESXi 6.7+	VMware ESX/ESXi 6.7+
Supported vCPUs	8	12	36
Minimum Memory	128 GB	128 GB	384 GB
Minimum Disk Drive	500 GB	500 GB	500 GB
Network Connectivity	2x 1 Gbps Ethernet (including 1 Management Interface)	2x 1 Gbps Ethernet (including 1 Management Interface)	1x 1 Gbps Ethernet for management, Up to 4 Intel DPDK-compatible NIC
PCAP Storage Disk Drive	Additional 500 GB	Additional 500 GB	Additional 10TB[2]

Model #	SS-NDR-SCA1-1M	SS-NDR-SCA5-1M	SS-NDR-SCG1-1M
PERFORMANCE & CAPACITIES			
Cloud	Amazon Web Services	Amazon Web Services	Google Cloud Platform
Function	Sensor Only	Sensor Only	Sensor Only
Network Performance	Up to 1 Gbps	Up to 5 Gbps	Up to 1 Gbps
SYSTEM REQUIREMENTS			
Minimum Instance Size Supported	r5.4xlarge - 16 vCPU	r5.16xlarge - 64 vCPU	n1-highmem-16 - 16 vCPU
Minimum Disk Drive	160 GB	500 GB	160 GB
Minimum Memory	128 GB	512 GB	104 GB

Model # (SaaS AVA Nucleus)	SS-NDR-NCA2-1M	SS-NDR-NCA5-1M	SS-NDR-NCA10-1M
PERFORMANCE & CAPACITIES			
Cloud	Arista VPC in Amazon Web Services (customer preferred region)	Arista VPC in Amazon Web Services (customer preferred region)	Arista VPC in Amazon Web Services (customer preferred region)
Function	Nucleus Only	Nucleus Only	Nucleus Only
Network Performance	Up to 2 Gbps average aggregate sensor throughput	Up to 5 Gbps average aggregate sensor throughput	Up to 10 Gbps average aggregate sensor throughput
Meta Data Storage[3]	30 days	30 days	30 days

[1] Cluster mode supported for higher throughputs and metadata retention.

[2]The amount of storage is determined during the deployment and is a function of the configuration and the capability of the underlying VMware host server

[3] Additional days of meta data storage available as an add-on

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