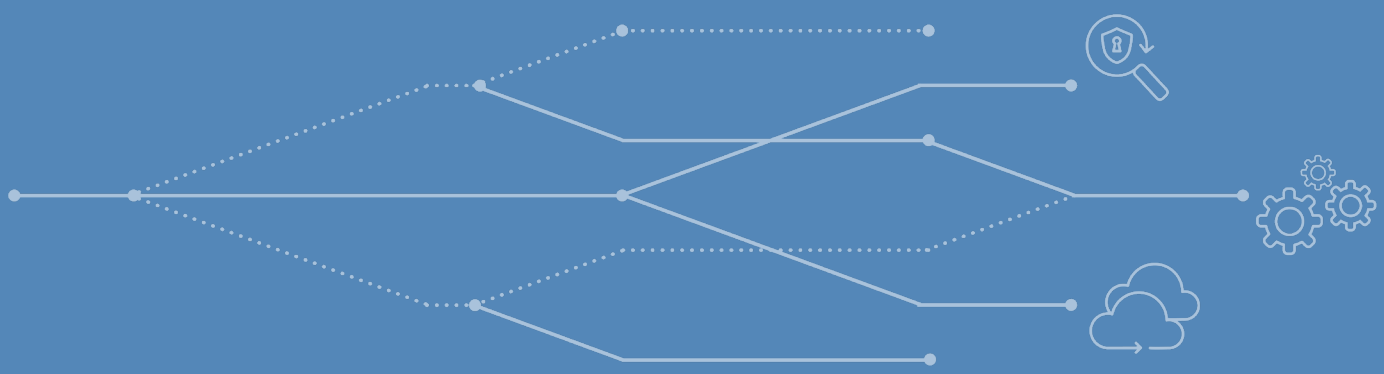


Awake Security Platform

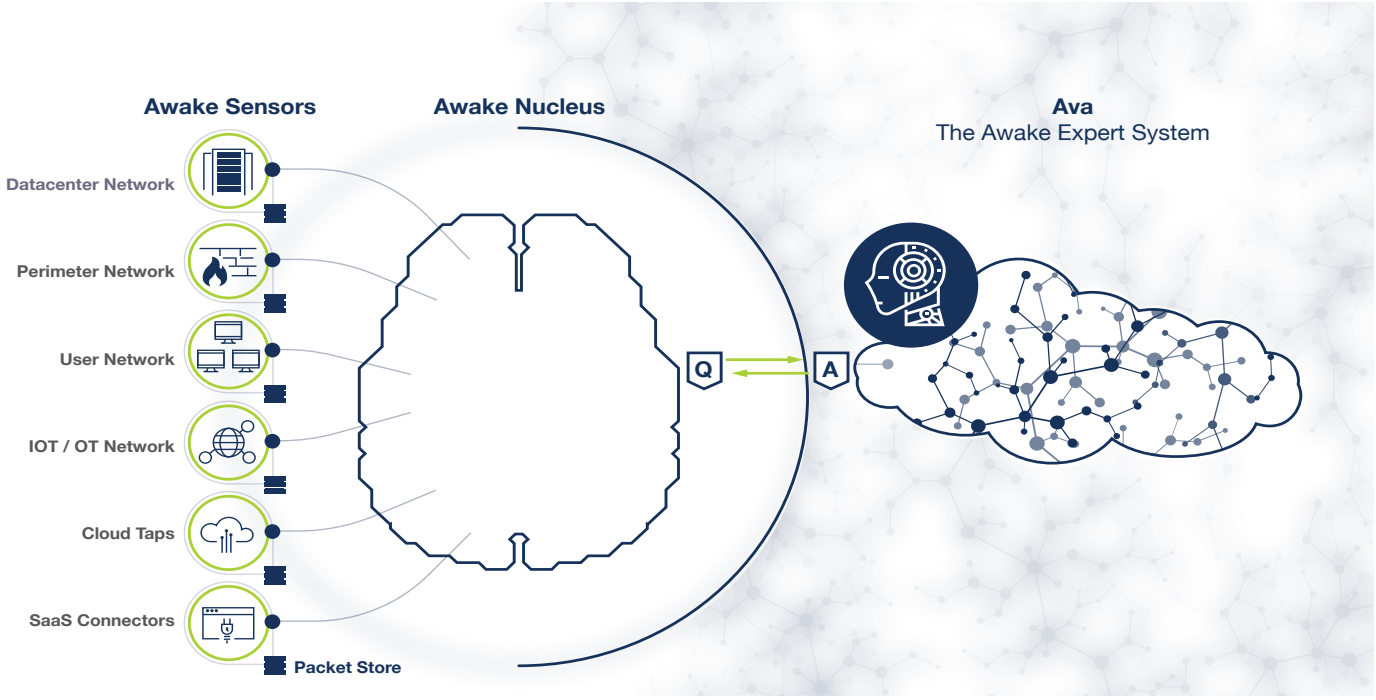
> "The Awake Security Platform has exceeded our expectations and empowered us to secure our connected workplace more effectively and autonomously than ever."
> – Rich Noguera, Fmr. CISO, Gap Inc.

As attackers have evolved beyond malware, supply chain threats, insider attacks and living off the land tactics challenge the ability for organizations to defend themselves effectively. At the same time a new network has emerged with unmanaged Internet of things, cloud infrastructure, contractor and third-party devices and shadow IT. Security teams recognize the need for threat hunting to deal with this evolving landscape, but struggle with the time and skills necessary to distinguish between good and bad when everything looks like normal activity.

The Awake Security Platform is built on a foundation of deep network analysis from **Awake Sensors** that span the "new network"—including the data center, campus, IoT as well as cloud workload networks and SaaS applications. Unlike other network detection and response solutions, Awake parses over three thousand protocols and processes layer 2 through layer 7 data. The platform analyzes encrypted traffic 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. **Awake's EntityIQ**™ technology uses this information to autonomously profile entities such as devices, users and applications, while also preserving these communications for historical forensics.

Only Awake

- Delivers EntityIQ™ to autonomously discover & profile every device, user & application whether managed or unmanaged by the organization.
- Delivers visibility into encrypted traffic using AI to classify the application communicating, nature of traffic etc.
- Enables Adversarial Modeling™ that exposes attacks including insider threats, credential misuse, lateral movement & data exfiltration.
- Reduces false positives & negatives by avoiding basic unsupervised learning on IP address data.
- Includes Ava™ to automate triage & investigations and provides a decision support system to the analyst.
- Requires no agents, manual configuration or lengthy training periods.



Extracted activity data feeds into the **Awake Nucleus** which uses a combination of detection models to uncover malicious intent. An ensemble of machine learning approaches avoid reliance on simplistic and noisy anomaly detection or unsupervised learning. Awake'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 suspicious activity and then gather corroborating evidence to support conviction. The modeling language delivers rich data analysis capabilities as well as a vocabulary to express attacker TTPs, so that even a relatively junior analyst can now hunt. The Nucleus provides a single sign-on and role-based user experience as well as a full API for extensibility, notifications and integrations with other IT and security solutions for automated response and remediation.

Ava, Awake's autonomous security analyst, is the world's first AI-based security expert 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 Awake customers to gain these capabilities while keeping their private data firmly within their infrastructure.

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

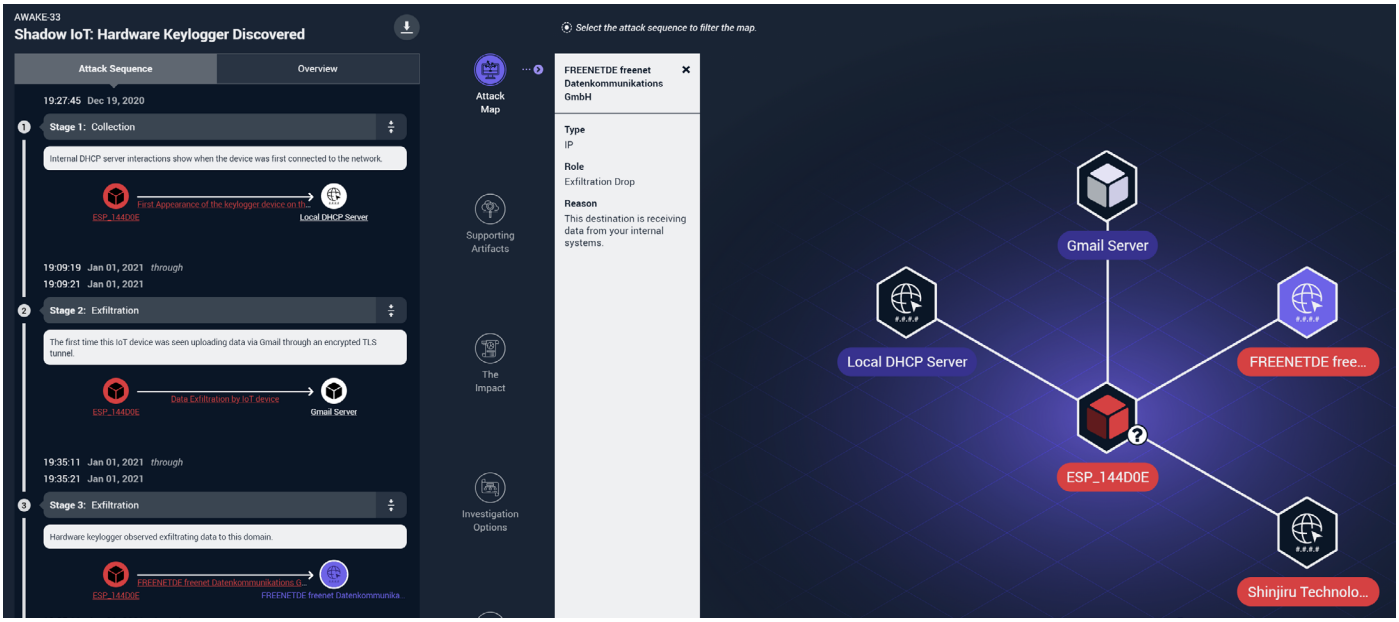
Ava forensically correlates incidents across entities, time, protocols and attack stages, surfacing Situations with all the decision support data necessary to respond rapidly to any threat.

Situational Awareness

Awake learns & tracks entities across IT, OT or IoT environments whether they are 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 in a matter of minutes autonomously expose the entire kill-chain.



Integrations

The Awake Security 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 a 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 similar device(s) for campaign analysis. Similarly, endpoint integrations allow for one click quarantining of compromised devices or retrieval of endpoint forensic data.

Deployment Modes

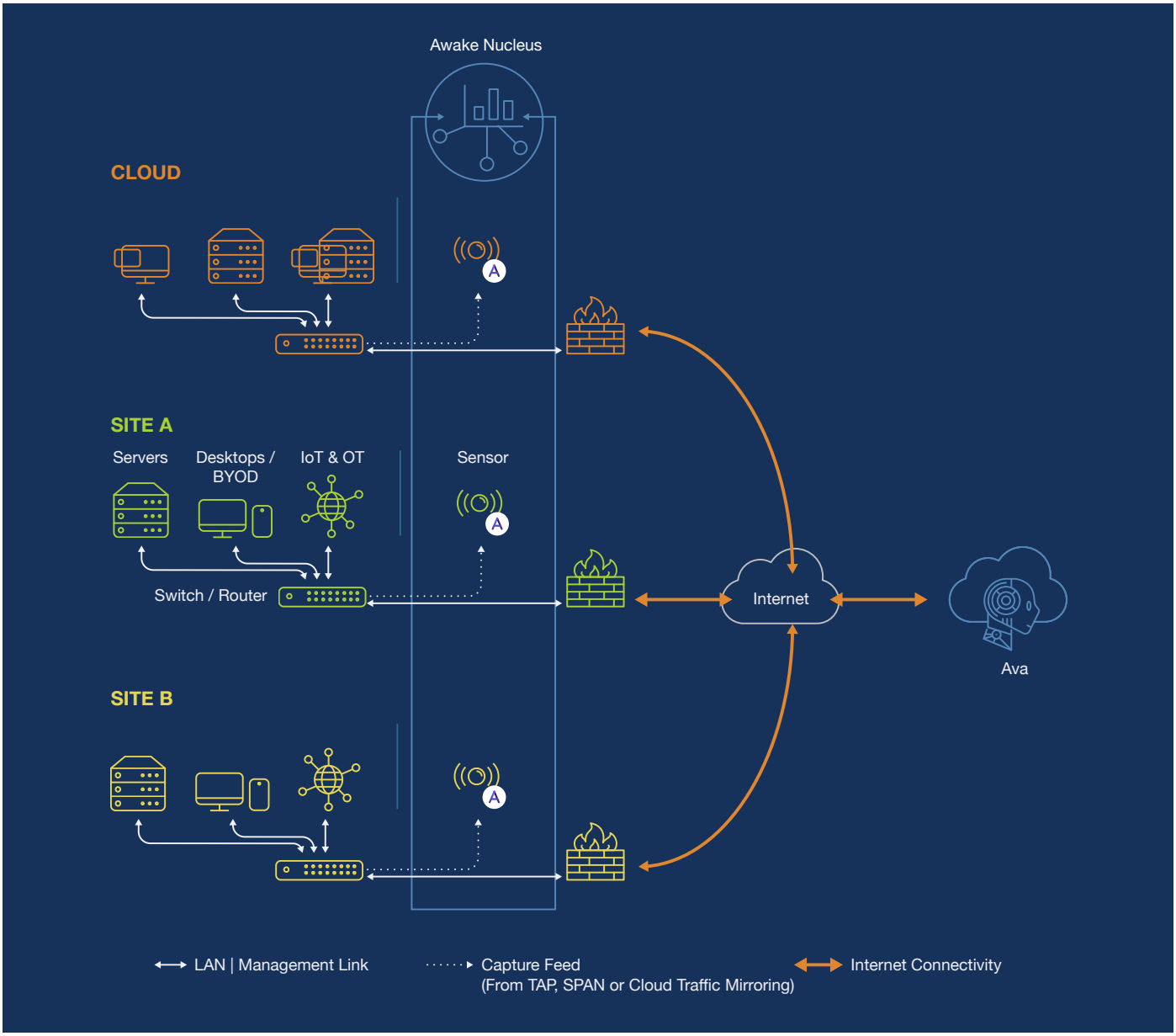
The Awake Security Platform can be deployed in two modes depending on customer requirements and network architecture:

All-in-one

The Awake Sensor and Awake Nucleus in this case are deployed on a single appliance. This deployment is ideal for customers who deploy a single instance of Awake or do not require a centralized view of their deployment.

Split

When deployed in this mode, the Sensor and Nucleus are deployed separately. Sensors can be deployed in a variety of form factors including physical or virtual appliances. The Nucleus can also be deployed as a hardware cluster to support higher performance requirements as well as in Amazon Web Services to support distributed deployment of sensors.



Awake Security Platform Hardware Specifications

Model #	ASP-S-NS	ASP-L-NS	ASP-L-AN	ASP-L-Ai1
PERFORMANCE & CAPACITIES				
Function	Sensor Only	Sensor Only	Nucleus Only	All in One
Network Performance	Up to 1 Gbps	Up to 5 Gbps	Up to 10 Gbps[1]	Up to 5 Gbps
Meta Data Storage	N/A	N/A	90 days	90 days
HARDWARE SPECIFICATIONS				
Rack Unit	1U	2U	2U	2U
CPU Cores	32	64	96	96
RAM	512 GB	512 GB	1 TB	1 TB
Disk Storage	1 TB	12x 6 TB	10x 8 TB	10x 8 TB
SSD	1x 1 TB	2x 480 GB	2x 480 GB	2x 480 GB
Non-volatile Memory	-	-	2x 3.2 TB PCIe NVME	2x 3.2 TB PCIe NVME
Network	2x 1/10 Gbps Onboard Ethernet 4x 10 Gbps Intel SFP+ 1x Out of Band Management Interface	2x 1 Gbps Onboard Ether-net 4x 10 Gbps Intel SFP+ Ports 1x Out of Band Management Interface	4x 1 Gbps Onboard Ether-net 2x 10 Gbps Intel Ethernet 1x Out of Band Management Interface	4x 1 Gbps Onboard Ether-net 4x 10 Gbps Intel SFP+ Ports 1x Out of Band Management Interface
Power Supply	2x 750W - Redundant and Hot Swappable	2X 1400W- Redundant and Hot Swappable	2X 1400W- Redundant and Hot Swappable	2X 1400W- Redundant and Hot Swappable

Model # (Virtual Sensors)	ASP-S-VS	ASP-L-VS
PERFORMANCE & CAPACITIES		
Function	Sensor Only	Sensor Only
Network Performance	Up to 500 Mbps	Up to 1 Gbps
SYSTEM REQUIREMENTS		
Supported Hypervisors	VMware ESXi 5.5+	VMware ESXi 5.5+
Supported vCPUs	8	12
Minimum Memory	128 GB	128 GB
Minimum Disk Drive	20 GB	20 GB
Network Connectivity	2x 1 Gbps Ethernet (including 1 Management Inter-face)	2x 1 Gbps Ethernet (including 1 Management Inter-face)

Model #	ASP-S-AWS-VS	ASP-S-GCP-VS
PERFORMANCE & CAPACITIES		
Cloud	Amazon Web Services	Google Cloud Platform
Function	Sensor Only	Sensor Only
Network Performance	Up to 1 Gbps	Up to 1 Gbps
SYSTEM REQUIREMENTS		
Minimum Instance Size Supported	r5.4xlarge - 16 vCPU	n1-highmem-16 - 16 vCPU
Minimum Disk Drive	160 GB	160 GB
Minimum Memory	128 GB	104 GB

[1] **Cluster mode supported for higher throughputs**

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 & B, 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