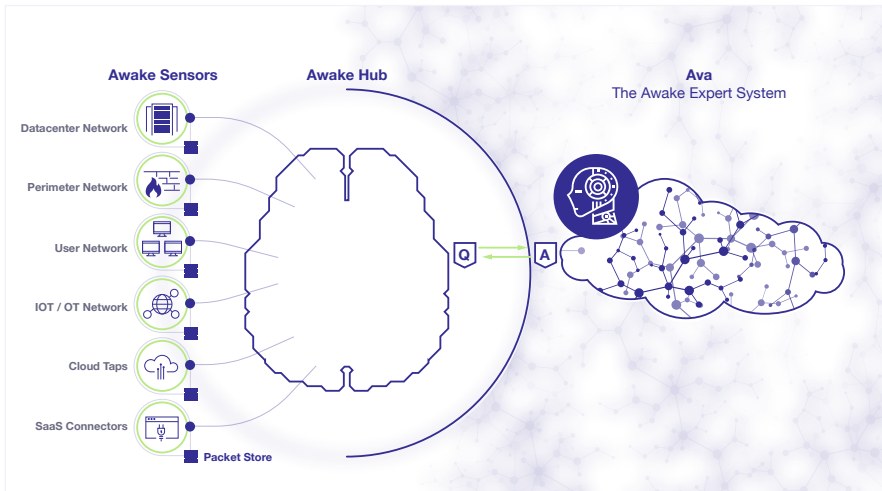


## DATASHEET

# Awake Security Platform

Modern attackers have changed their tactics to circumvent defenses that are increasingly effective at discovering and blocking malware. These threat actors engage in multi-stage blended attacks which utilize tools that every organization needs to run their business and operate their IT function. This living-off-the-land attack trend is occurring at the same time as organizations move to an automated and connected workplace where the very definition of the network is changing with unmanaged IoT, BYOD, cloud infrastructure and shadow IT. In this new reality, security teams are asked to distinguish between good and bad when everything looks like normal activity, and to do this while being blind to upwards of 40% of the infrastructure.

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, perimeter, core, Internet of things and operational technology networks as well as cloud workload networks and SaaS applications. Unlike other network traffic analysis solutions, Awake parses and processes layer 2 through layer 7 data, including performing encrypted traffic analysis. With this information, Awake autonomously profiles entities such as devices, users and applications, while also preserving these communications to provide historical forensic context.



Extracted activity data feeds into the **Awake Hub** which then identifies and visualizes incidents through automatic correlation across entities, time, protocols and attack stage. The platform also learns from past incidents as well as Awake's customized cyber security, governance, risk and compliance playbooks to provide the security analyst with both automated and manual response options. These can trigger workflows within integrated solutions or simply recommend response steps such as evidence collection.

Awake's **Ava** is the world's first privacy-aware security expert system. Ava brings both a global and an industry specific perspective to perform autonomous threat hunting and incident triage. Using a combination of artificial intelligence, open source intelligence and Awake's own human expertise, Ava minimizes the number of incidents the security team must act on. Through Ava, customers also have on-demand access to Awake experts for up-to-the-minute threat research, hunting and investigation support. Importantly, federated machine learning allows Awake customers to see these benefits while keeping their private data firmly within their infrastructure.

"Awake has helped us completely transform our alert-focused security program to one centered on risk—to and from the entities we are protecting and interacting with. "

– Fortune 500 Retail CISO

## Only Awake



Automatically detects TTPs to expose evasive threats including insider threats, credential misuse, lateral movement, and data exfiltration.



Automates triage and campaign analysis by reconstructing and visualizing incidents across entities, time, protocols and attack stages.



Delivers comprehensive context on network traffic as well as the source devices / users & destination domains, autonomous systems (ASNs) and IP addresses.



Uses federated machine learning and encrypted traffic analysis to deliver value without compromising privacy and violating regulations.



Uses AI-based behavioral analysis to detect and respond to threats that are organization-specific.



Requires no agents, manual configuration or lengthy training periods.

## Use Cases



### Detection

The platform uses AI to detect & prioritize mal-intent & behavioral threats from both insiders & outside attackers.



### Response

Ava forensically correlates incidents across entities, time, protocols and attack stages, delivering all the context necessary to respond rapidly to any threat.



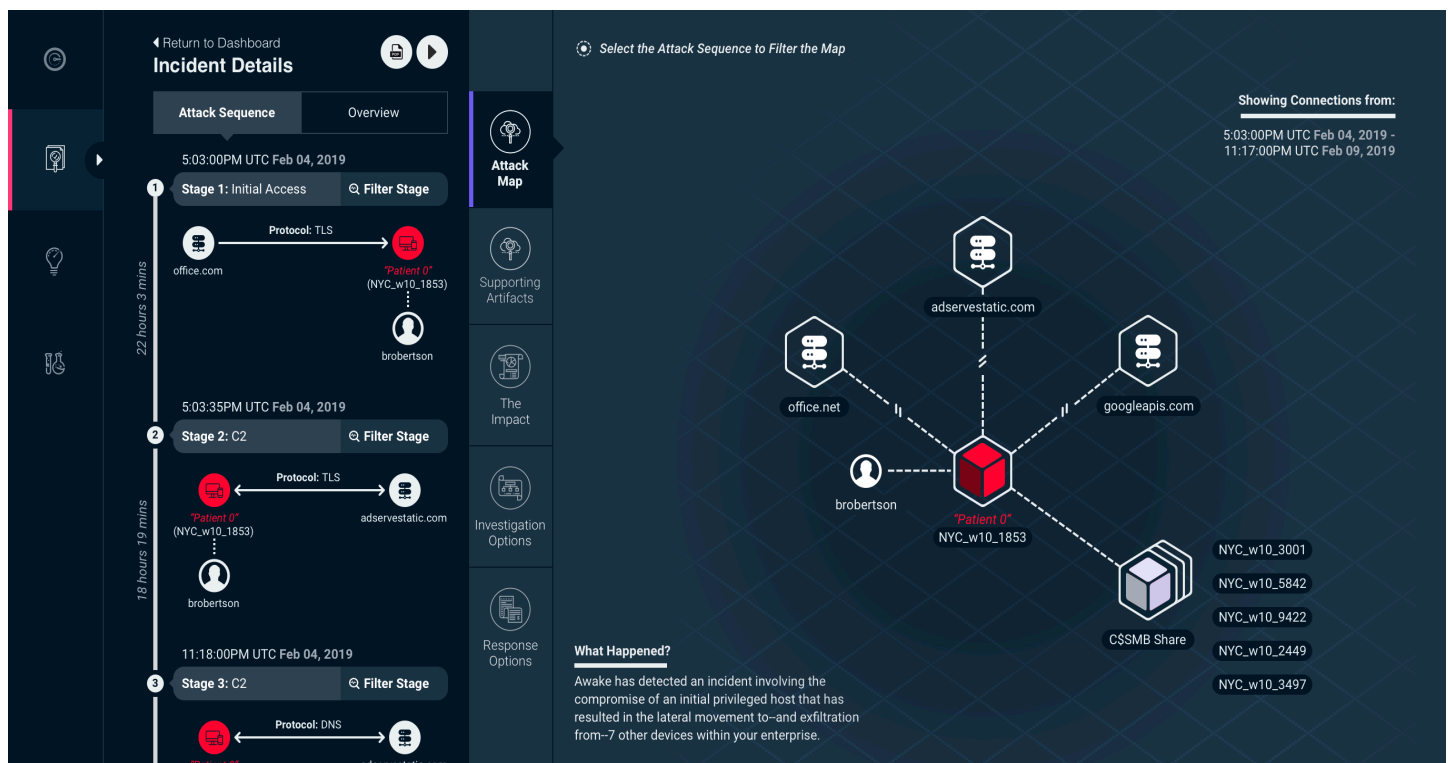
### Situational Awareness

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.



### Regulatory Compliance

By combining deep insights on your infrastructure with institutional knowledge, Awake enables compliance with regulations such as PCI, NIST, GLBA and NYS DFS.



## Integrations

The Awake Security Platform integrates with and amplifies existing solutions through integrations into industry-leading SIEM, business intelligence 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

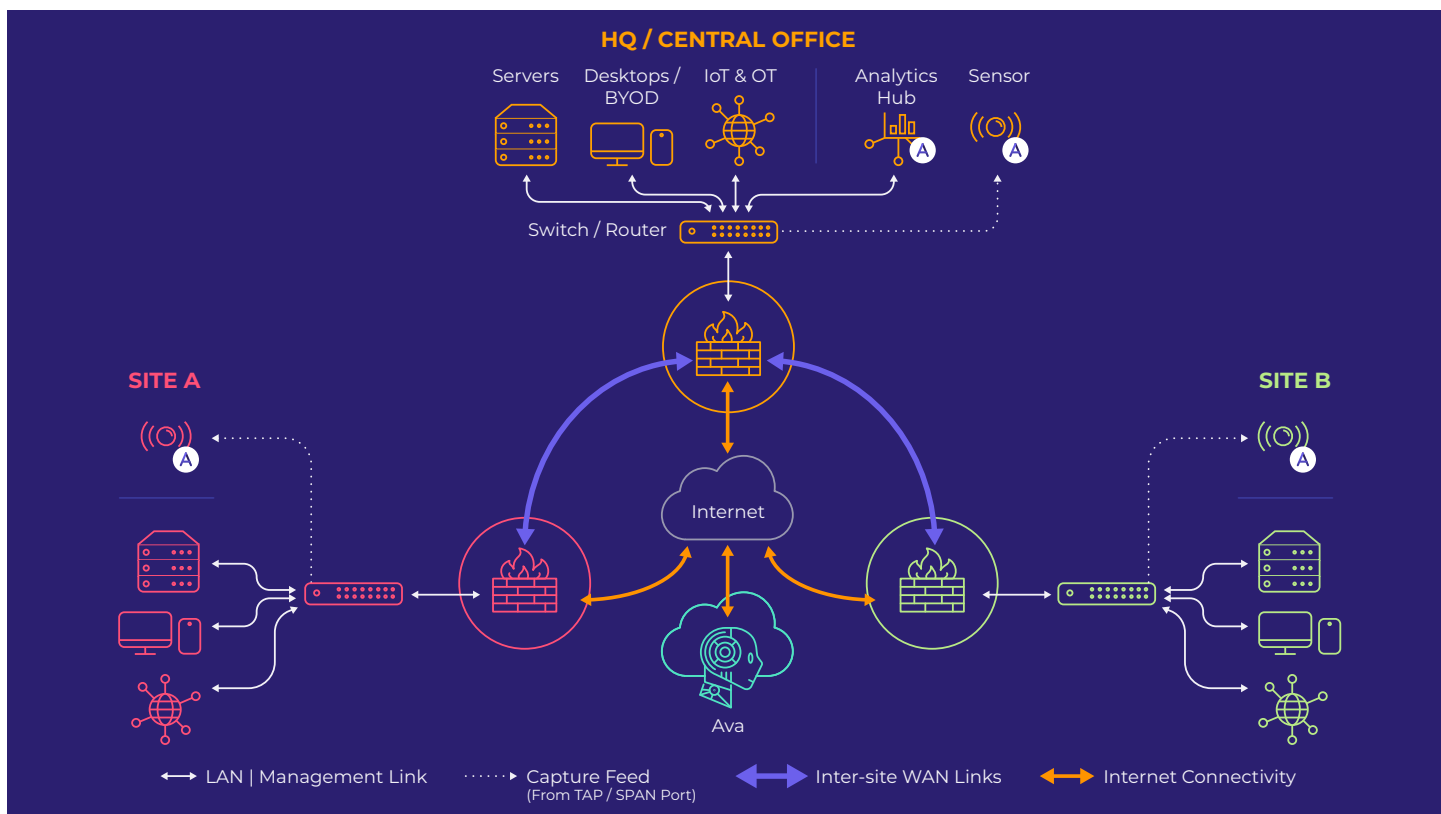
The Awake Security Platform can be deployed in two modes depending on customer requirements and network architecture:

### All-in-one

The Awake Sensor and Awake Analytics Hub 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 Analytics Hub are deployed separately. Sensors can be deployed in a variety of form factors including physical or virtual appliances. The Analytics Hub can also be deployed as a hardware cluster to support higher performance requirements.



## AWAKE SECURITY PLATFORM HARDWARE SPECIFICATIONS

Model #		ASP-S-NS	ASP-L-NS	ASP-L-AH	ASP-L-Ai1
Performance & Capacities	Function	Sensor Only	Sensor Only	Analytics Hub Only	All in One
	Network Performance	Up to 750 Mbps	Up to 5 Gbps	Up to 10 Gbps	Up to 5 Gbps
	Meta Data Storage	N/A	N/A	90 days	90 days
	Max # Devices	N/A	N/A	200,000	100,000
	Cluster Mode	N/A	N/A	2x 2U: 20 Gbps / 180 days / 400,000 max devices or 2x 2U: 10 Gbps / 90 days / 1 million devices	N/A
	Maximum Sensors	N/A	N/A	12	N/A
	Full Packet Storage	Extensible JBOD Storage Support			
Hardware Specifications	Rack Unit	1U	2U	2U	2U
	CPU Cores	12	64	64	64
	RAM	128 GB	512 GB	512 GB	512 GB
	Disk Storage	4x 6TB	12x 6TB	12x 6TB	12x 6TB
	SSD	1x 1 TB	2x 240GB	2x 240GB	2x 240GB
	Non-volatile Memory	-	-	1x 3.2 TB PCIe NVME	1x 3.2 TB PCIe NVME
	Network	2x 1Gig Onboard Ethernet 4x 10Gig Intel SFP+	2x 1Gig Onboard Ethernet 4x 10Gig Intel SFP+ Ports	4x 1Gig Onboard Ethernet 2x 10Gig Intel Ethernet	4x 1Gig Onboard Ethernet 4x 10Gig Intel SFP+ Ports
	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