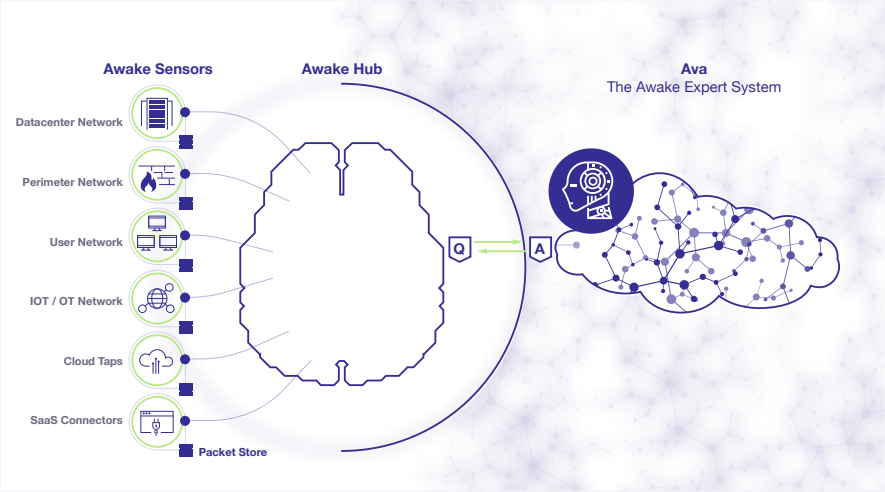
DATASHEET

Awake Security Platform

Modern attackers have changed their tactics to circumvent defenses that are increasingly effective at discovering and blocking malware. These threat actors now exploit tools that every organization needs to run their business and operate their IT function. This is happening 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 full packet capture data input from **Awake Sensors** that span the "new network"—including the data center, perimeter, core, Internet of things and operational technology networks and those connecting cloud and SaaS resources. 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 remediation 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 incident triage. Using a combination of cloud-scale federated machine learning, open source intelligence and 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.

> "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.
- Uses federated machine learning and encrypted traffic analysis to deliver privacy-aware analytics.
- Combines institutional knowledge with machine learning & AI to detect and respond to threats that are organization-specific.
- Requires no agents, manual configuration or lengthy training periods.

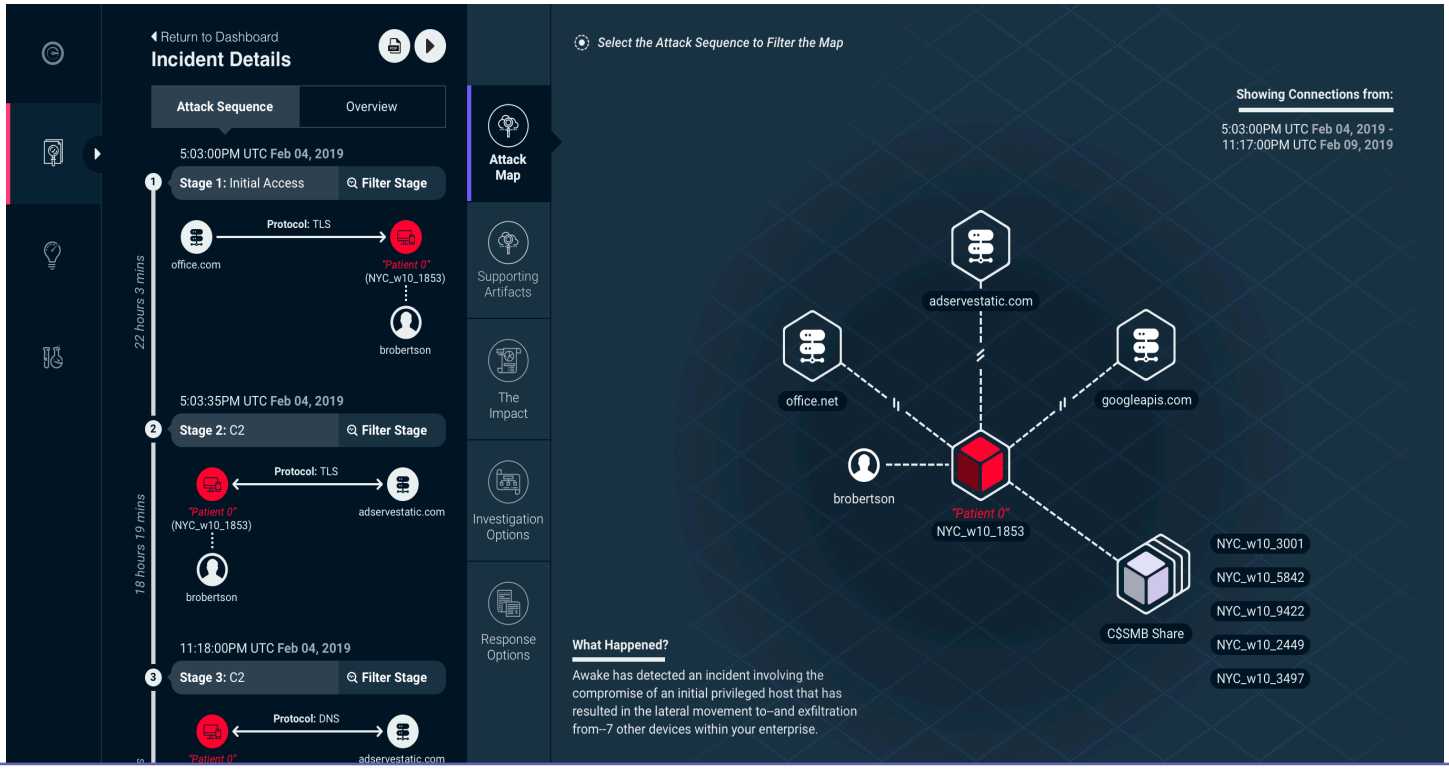
Use Cases

Discovery
Awake autonomously learns & tracks entities across IT & OT environments whether they are on-premise, cloud or SaaS and managed or unmanaged.

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

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

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



AWAKE SECURITY PLATFORM HARDWARE SPECIFICATIONS	
Form factor	2RU Appliance
Throughput	2.5 Gbps
Storage	33TB usable storage
Processor	Intel Broadwell-based Xeon 2x18 cores
RAM	512 GB
Interfaces	5x10G monitoring ports (1 Copper; 4 Copper or Fiber) 1x10G management port (Copper)

Integrations

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

AWAKE

For additional information about Awake please visit awakesecurity.com