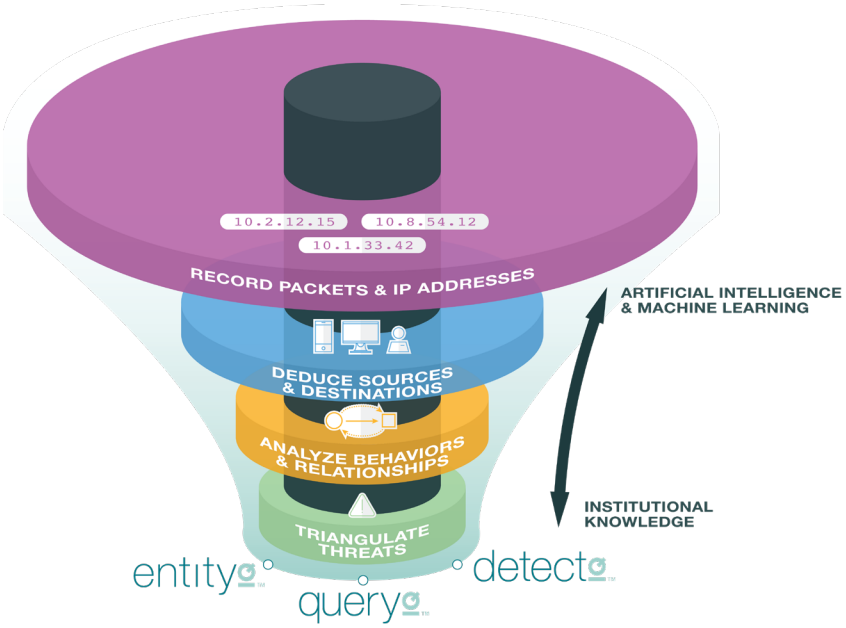
DATASHEET

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 uniquely combines machine intelligence and institutional knowledge to transform security operations by enabling teams to identify and protect the organization's highest-risk assets. The platform's patented **EntityIQ™** technology instantly analyzes billions of communications in real-time to discover every business asset—device, user and application—in the organization as well as the destinations and domains on the other end of the communications. By attributing and tracking behaviors for each of these entities over time, the Awake Security Platform can detect behavioral threats, mal-intent as well as known indicators of compromise. In addition, the security team can enrich the autonomously generated context with institutional knowledge about the entity.



The approach of combining a deep understanding of the source and destination entities with traffic analytics avoids the high false positives and negatives seen with other machine learning solutions that simply detect anomalies from a baseline for an individual IP address. The platform's **DetectIQ™** detection engine instead also compares each device to the other entities in the environment, grouping ones that are similar and then identifying behaviors that stand out from peer devices. In addition, Awake also provides **QueryIQ™**, a behavioral query language that enables security teams to discover attacker tactics, techniques and procedures (TTPs) such as ephemeral command and control infrastructure. With just network data, **QueryIQ™** can precisely find notable patterns and behaviors via a simple but powerful interface for simultaneously interrogating graph and structured data sources as well as the raw underlying packets. Unlike existing systems like SIEM, **QueryIQ™** provides interactive response even for very large datasets.

> "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 with **DetectIQ™**.
- Automates triage and campaign analysis with credit-rating-like risk scoring that enables conclusive response.
- Delivers comprehensive **EntityIQ™** context on network traffic as well as the source devices / users & destination domains.
- Provides **QueryIQ™** that allows teams to rapidly and precisely hunt for threats while customizing detection sensitivity.
- Combines institutional knowledge with machine learning & AI to detect and respond to threats that are organization-specific.
- Requires no agents, manual configuration or training period.

Use Cases

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

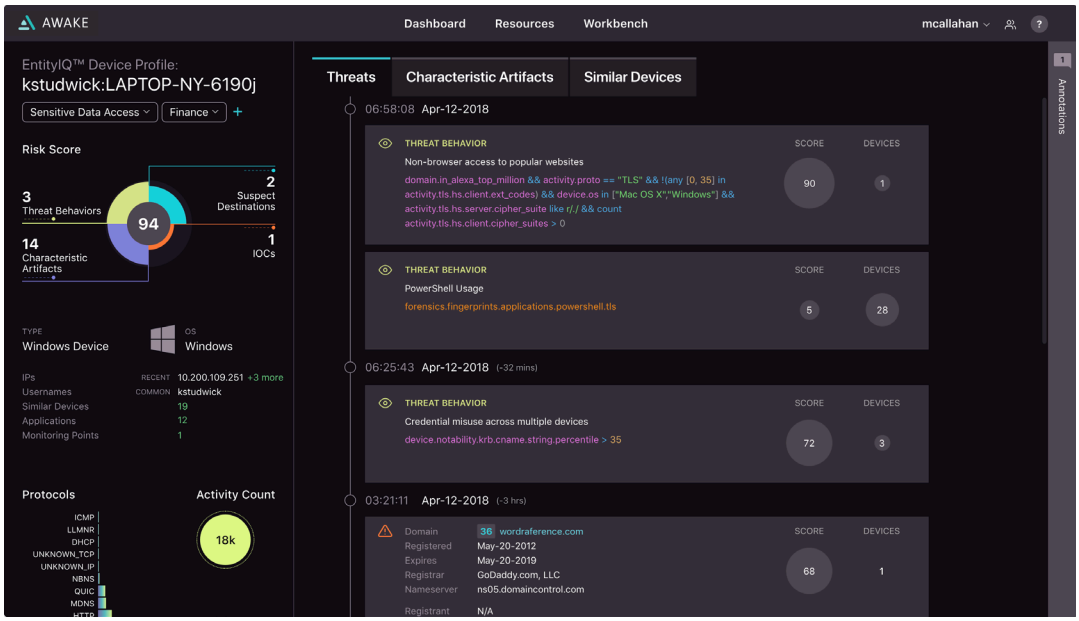
Detection
The platform uses AI to detect & prioritize mal-intent & behavioral threats from both insiders & outside attackers.

Response
Awake's virtual assistant automatically delivers all the context necessary to respond in minutes to any alert.

Compliance
Through deep knowledge of your infrastructure, Awake enables compliance with regulations such as PCI, NIST, GLBA and NYS DFS.

Key Benefits

- Track devices, people and other entities without logs or endpoint agents even as they move on the network and IP addresses change.
- Instantly access ML-powered **EntityIQ™** profiles that document associated devices or users, business function, email addresses, domains visited, files accessed, relationships, and more.
- Resolve alerts or hunt for new threats with **QueryIQ™** in minutes rather than hours, by ending the "coffee break" query experience that is typical of existing solutions.
- Enable junior analysts to effectively triage and analyze sophisticated campaigns with out-of-the-box integrations that augment existing investments such as SIEM, Endpoint Security and Orchestration platforms.
- Derive value immediately without the need for complex integrations, training periods or tuning.



AWAKE SECURITY PLATFORM HARDWARE SPECIFICATIONS	
Form factor	2RU Appliance
Throughput	2.5 Gbps
Storage	33TB usable storage (with supported drive data encryption)
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 an **Awake EntityIQ™** 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.

AWAKE

For additional information about Awake please visit **awakesecurity.com**