AWAKE

Advanced Detection and Response for the Hybrid Cloud

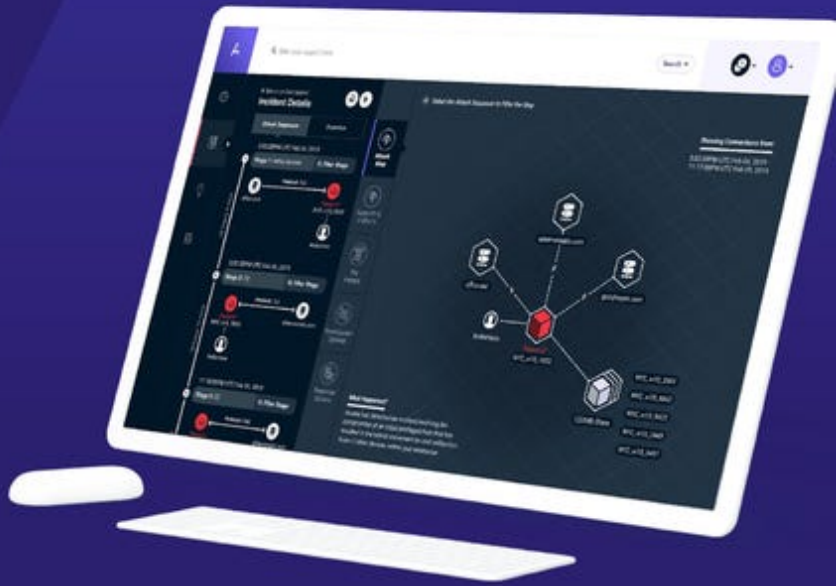
RSA Conference
Finalist: Most Innovative Security Company 2018

BUSINESS INSIDER
30 Hottest Security Startups

ETR+
#1 security solution in the Global 1000

OPPORTUNITY

To be **the market leader** in cyber detection and response for the hybrid cloud



Executive Summary

TEAM

65 employees

History of delivering category-leading products

Persistent & unreasonable in our goals

DIFFERENTIATORS

Immediate time-to-value

High efficacy detection & response

Platform-as-a-service approach

Patented Ava, EntityIQ & Adversarial Modeling

KEY CUSTOMERS

Strong customer traction

Greenfield & displacement opportunity (Cisco, RSA, Darktrace, etc.)

Land and expand dynamics

CURRENT INVESTMENT

Series A: Greylock

Series B: Bain & Greylock

FUND RAISE: $30 M

Awake Market Opportunity

MARKET GROWTH	2019	2024
Information Security (8.3% CAGR)	$121B	$182B
Network Detection & Response (14.1% CAGR)	$1.9B	$3.8B

LEADERS BY CATEGORY		MARKET CAP
Network Prevention	paloalto	$20B
Email Prevention	proofpoint.	$6B
Endpoint Detection & Response	CROWDSTRIKE	$13B
27 Pure-play Security Companies on Public Markets		$6B (AVG)

AWAKE

NETWORK DETECTION & RESPONSE

Source: https://momentumcyber.com/docs/Quarterly/Cybersecurity_Market_Review_1H_2019.pdf
https://momentumcyber.com/cybersecurity-snapshot-august-2019/
Gartner Forecasts

Leadership Team

Deep Expertise Across Security, Networking & Data Science

RAHUL KASHYAP
CEO

KEITH AMIDON
Chief Architect

RUDOLPH ARAUJO
VP, Marketing

RANDY CHEEK
VP, Sales

DEBABRATA DASH
Chief Data Scientist

GARY GOLOMB
Chief Scientist

RAJDEEP WADHWA
VP, Product

JEFFREY WANG
VP, Engineering

ASHEEM CHANDNA
Founding BoD Palo Alto Networks
Greylock Partners

SARAH GUO
Fmr. Board Member Demisto
Greylock Partners

KEVIN MANDIA
Founder, Mandiant
CEO, FireEye

ENRIQUE SALEM
Fmr. CEO Symantec
Bain Capital Ventures

ArcSight · big switch networks · Bromium · cisco · CYLANCE · DARKTRACE · E8 SECURITY · FOUNDSTONE

FireEye · hp · IntruVert NETWORKS · McAfee · NETWITNESS · symantec. · SS8 · vmware

Key Customers & Pipeline

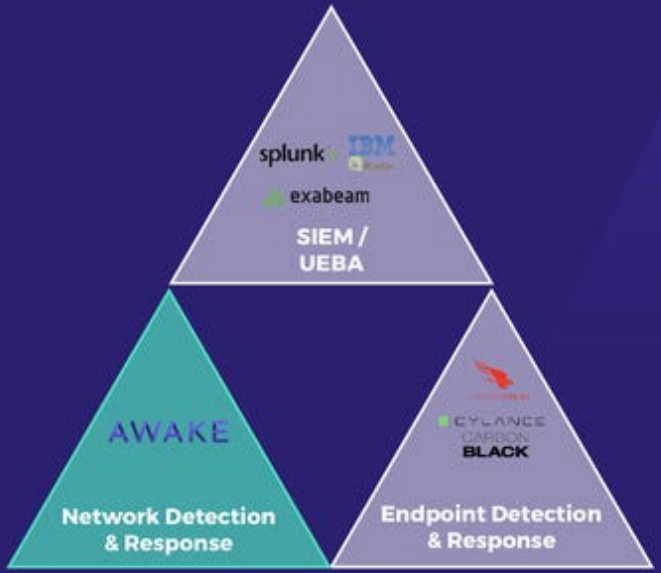
REDACTED

REDACTED

The Analyst Perspective

Security Operations Center Visibility Triad

Source: Gartner



> **IoT devices, mobile phones and OT technology**, may not have agents available or even the ability to produce security logs. In those cases, **network traffic becomes one of the only options** to provide visibility into what happens on those systems"
>
> Gartner

> Compliance mandates for network security are **elevating NVDR more toward the 'must have' category**, which is the easiest sales proposition in security. [...] Enterprise security teams justify **NVDR purchases for multi-cloud transformations as a modernization effort for replacing aged IDS/IPS** deployments, while satisfying clauses in compliance mandates.
>
> 451 Research

The Challenge

How Do You Secure the New Network?

> 50%

Devices are
"Unmanaged"

~ 50%

Breaches See
No Malware

> 3M

Unfilled
Security Jobs

Alerts → Answers

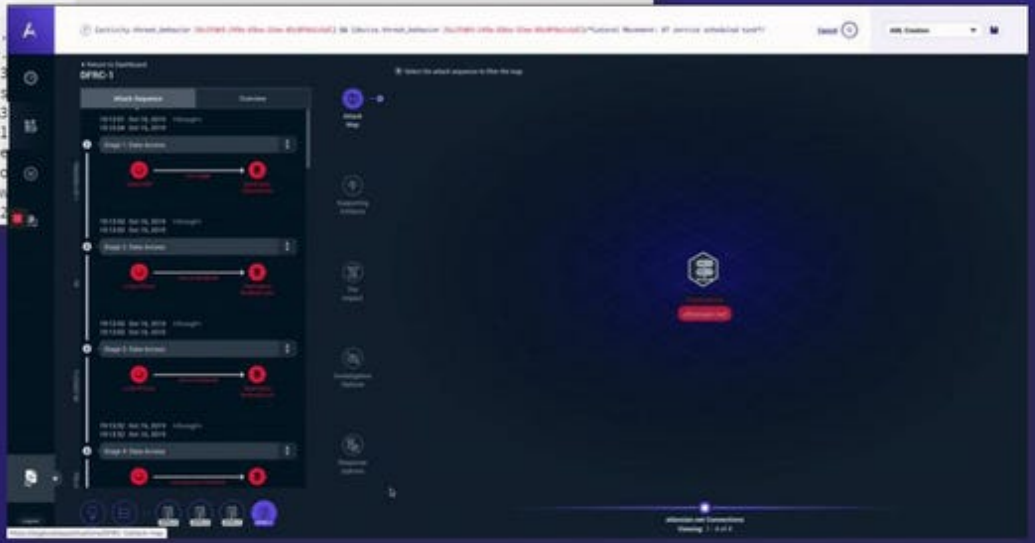
Reducing Time, Cost & Risk of Security Operations

From Alerts …

10/13/19 1:23:32.313 PM | Financial Crime Threat Intel | Intel Match: FIN4 Command and Control / Credential Theft

{"timestamp":"2019-10-13T13:23:32.313424+0000",
0.137.100.123","src_port":49167,"dest_ip":"209.
llowed","gid":1,"signature_id":2021113,"rev":1
t","category":"Financial Crime Threat Intel",
=&ct=15&init=0&s=f070&n=87146%3B87146%3B94047%
ttp_user_agent":"Mozilla\/5.0 (Macintosh; Intel
3029.96 Safari\/537.36","http_content_type":"te
00\/draymond-green-wishes-cleveland-cavaliers-
tatus":200,"length":0},"app_proto":"http","flow
lient":3207,"start":"2019-10-13T13:23:32.214322

…To Answers



The Awake Security Platform

Securing the New Network

SEE
THE NEW NETWORK

Monitor the
hybrid-cloud & IoT

KNOW
CURRENT THREATS

Identify insider &
external mal-intent

PROTECT
WITH HIGH ROI

Consolidate & automate
with an expert system

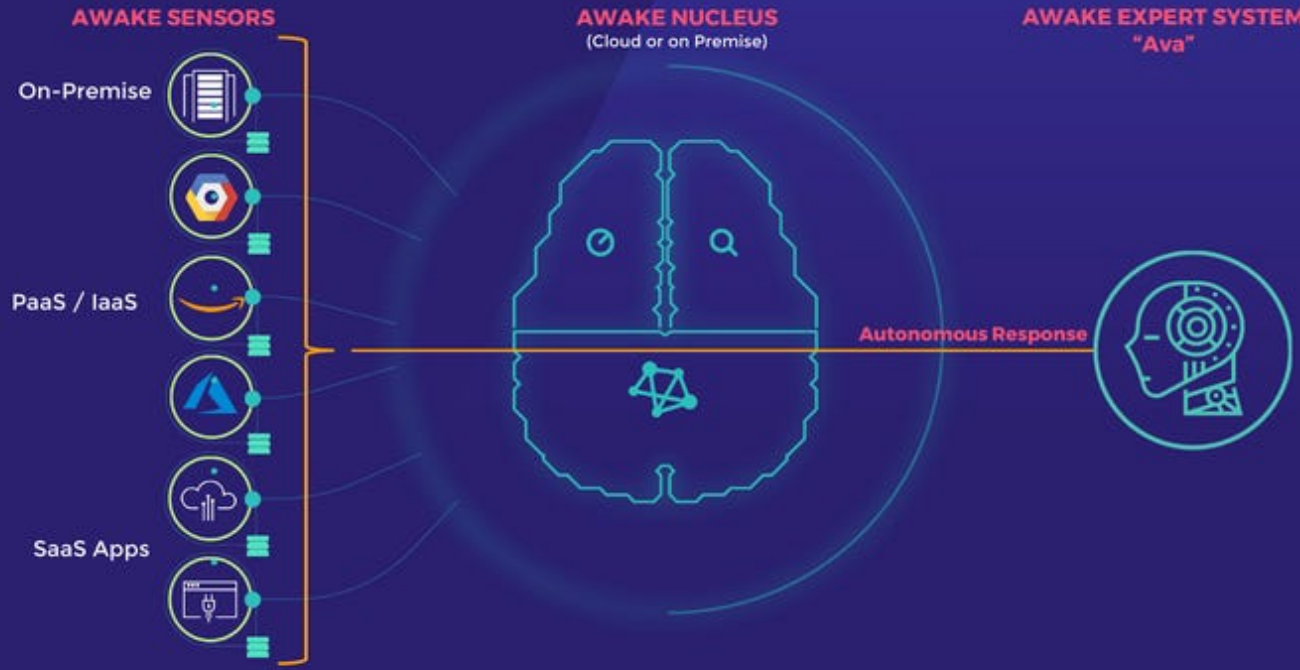
The Future of Detection & Response:
Intent Detection

Why We Win?

Key Differentiators

- Designed to support the **new network**
- **Consolidates** various network tools
- Autonomous **entity tracking** with network ground truth
- **Adversarial modeling** for high-efficacy intent detection
- **Autonomous triage** with Ava

Detection and Response for the Hybrid Cloud



RSA Netwitness Displacement

Case Study

INDUSTRY

Media & Entertainment (Fortune 100)

SIZE

X000+ employees

AWAKE DEPLOYMENT

XXX Awake Sensors and Nucleus // 60 Gbps

KEY USE CASES

Insider threat detection
Digital forensics and incident response
Threat hunting

WHY AWAKE VS. RSA?

Lower operational costs especially for storage
Broader set of use cases
Workflow integrations

$XXX (7 Figures)

Land, Renew & Expand

Case Study

INDUSTRY
Retail (Fortune 200)

SIZE
XXX,000+ employees

AWAKE DEPLOYMENT
XXX Awake Sensors and Nucleus

KEY USE CASES
Identifying threats across 3000+ store locations
Auditing existing controls/policies

WHY RENEW?
Satisfied Customer
Expanded threat hunting use cases
Single pane of glass

$XXX (High 6 Figures)

Incident Response to Product Sale

Case Study

INDUSTRY
Oil & Gas (Fortune 500)

SIZE
X,X00+ employees

AWAKE DEPLOYMENT
XXX Awake Sensors and Nucleus // 5 locations

KEY USE CASES
Digital forensics and incident response
Unmanaged devices/Supply chain monitoring
Threat hunting

WHY AWAKE VS. SIEM?
Immediate time to value
Broader set of use cases
Workflow integrations

$XXX (High 6 Figures)

Darktrace Displacement

Case Study

INDUSTRY
High Tech

SIZE
XXX+ employees

AWAKE DEPLOYMENT
XXX Awake Sensors and Nucleus // 10 locations across the globe

KEY USE CASES
Living off the land & insider threats
Global visibility

WHY AWAKE VS. DARKTRACE?
Broader IT and security integration
Advanced threat hunting capabilities
Managed Network Detection & Response

$XXX (High 6 Figures)

Cisco Stealthwatch Displacement

Case Study

INDUSTRY
Finance

SIZE
XXX+ employees

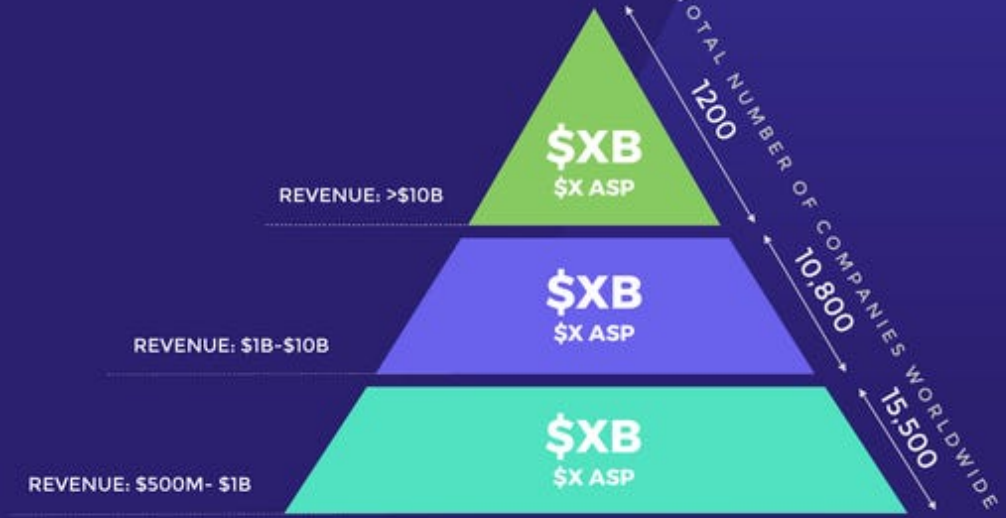
AWAKE DEPLOYMENT
XXX Awake Sensors and Nucleus // 2 locations

KEY USE CASES
GDPR / PCI compliance
Unknown attack surface monitoring

WHY AWAKE VS. CISCO?
Shadow IT visibility
Support for forensic investigations and threat hunting
Integrations with the security program

$XXX (6 Figures)

Path to the First $100M



$8.9B across **27,500** enterprises

Source: Forbes Global 2000 - https://www.forbes.com/global2000/
NAICS US Business Firmographics - https://naics.com/business-lists/counts-by-company-size/
World Bank Statistics - https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true&view=chart

REDACTED DETAILED FINANCIAL METRICS, FORECASTS ETC.

Summary

TEAM

65 employees

History of delivering category-leading products

Persistent & unreasonable in our goals

DIFFERENTIATORS

Immediate time-to-value

High efficacy detection & response

Platform-as-a-service approach

Patented Ava, EntityIQ & Adversarial Modeling

KEY CUSTOMERS

Strong customer traction

Greenfield & displacement opportunity (Cisco, RSA, Darktrace)

Land and expand dynamics

CURRENT INVESTMENT

Series A: Greylock

Series B: Bain & Greylock

FUND RAISE: $30 M

AWAKE

See More. Know More. Protect More.

THANK YOU!

AWAKESECURITY.COM | 833.292.5348

The Malicious Insider

HACKING THE VOIP PHONE SYSTEM

Industry

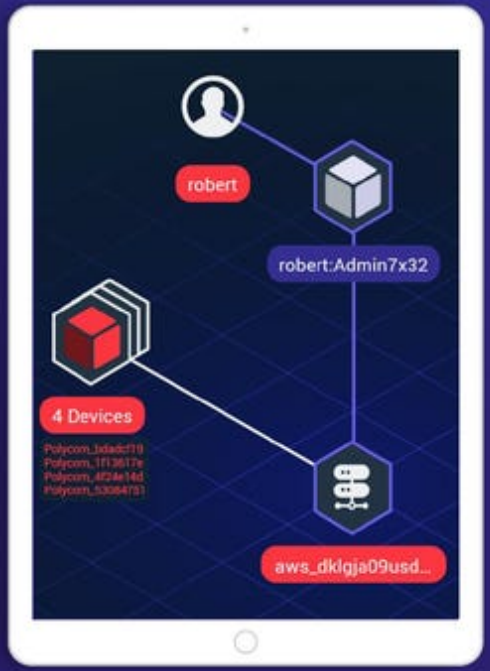
Consumer Finance

Challenge

IT contractor virtually tapped into phones, recorded calls and exfiltrated the data

Results

Awake identified the cluster of VoIP phones, spotted the outliers & the encrypted exfiltration and identified the attacker accessing the recordings



22

The Nation State Threat

HACKING A MUNICIPAL WATER AUTHORITY

Industry

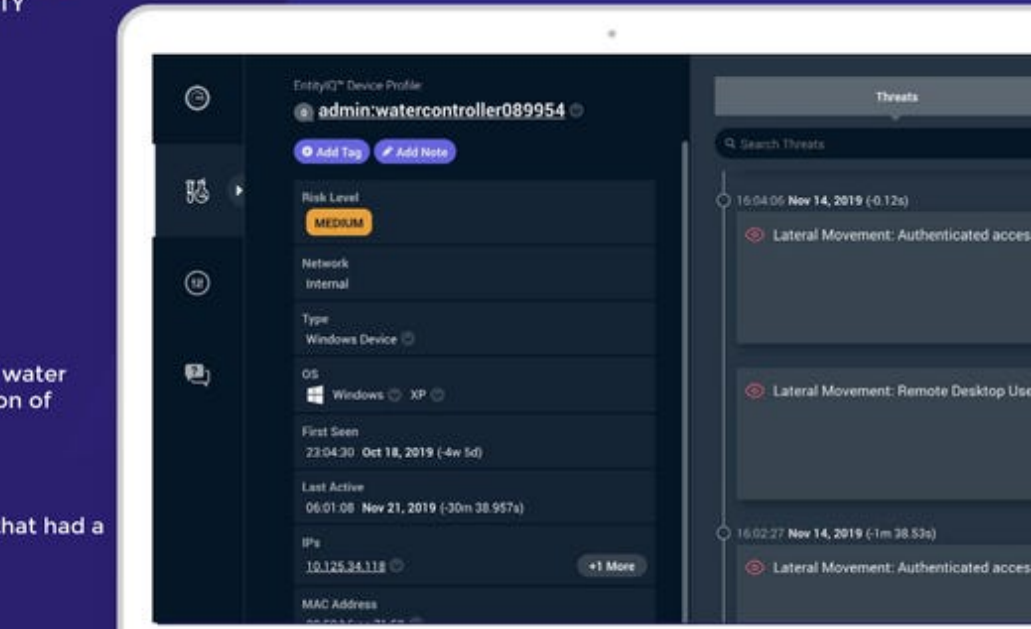
State & Local Government

Challenge

Critical infrastructure controlling the local water district was running an unsupported version of Microsoft Windows

Results

Awake identified a Windows 2003 server that had a Russian remote access tool installed



The Targeted Attack

HACKING THE CLOUD FROM ON-PREMISE ASSETS

Industry

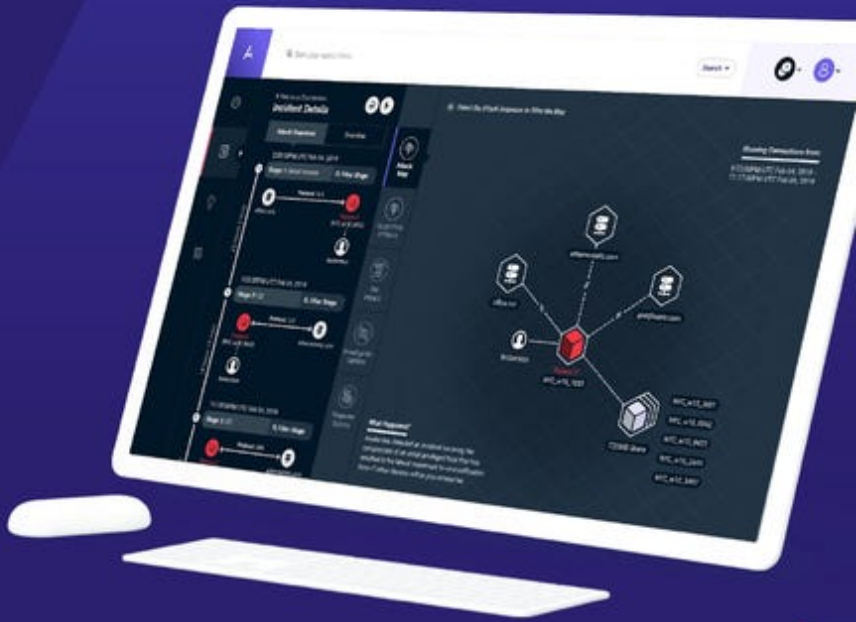
Financial Services

Challenge

An AWS administrator's credentials were stolen and used to access the organization's cloud infrastructure

Results

Awake detected a malicious Chrome extension being used to steal browser information including login data



24