REPORT REPRINT

Awake Security opens the eyes of security operations personnel

ERIC OGREN

11 MAY 2018

Security threats that are not instantly blocked eventually turn into incidents that first must be detected, and then human security specialists need to intervene. Awake's platform takes a unique approach by using network traffic analytics to automate hunting down threats as part of incident response activity.

When an incident report requires investigation, security operations center (SOC) teams sort through what can be terabytes of log data per day to assemble a workable chronology of network, device and account activity. Hunting threats and resolving incidents by connecting fragments of log data is a time-consuming process that is complicated by gaps in the data as not all useful information finds its way into security logs.

SOC are teams increasingly turning to network traffic analytics (NTA) to augment – not replace – log data analysis. Network traffic has the advantage of showing exactly who and what is active on the network over any time interval. Awake Security uses its ability to build endpoint profiles from network packets and headers to quickly present investigators with the information required to close security issues.

THE 451 TAKE

Awake approaches NTA as enhancing security operations, doing all of the background work necessary in composing network activity and device configurations to support SOC teams and incident responders. Three important facets of the company stand out. First, it captures and inspects network packets in addition to header information, allowing more thorough analysis and refined reporting of active threats. Second, Awake transparently amasses configuration information of all managed and unmanaged devices participating in network communications, without the need to deploy and administer software agents or rely on log data to be generated. Third, the company's out-of-the-box analysis based on attacker tactics and techniques detects threats that SOC teams have been missing.

Attacks are hard to find once they defeat detection and prevention products because they blend in so well with authorized business traffic, and because log files do not always contain sufficient information to guide incident response processes. Awake's approach to NTA is designed to detect and respond to such attacks and thus augment procedures steeped in log data analysis with insights from actual network traffic.

CONTEXT

Network traffic analytics is gaining traction for its ability to detect threats operating in the network after eluding prevention products. Most NTA products are tuned to detect threats based on a priori knowledge of attack behaviors or machine learning to expose anomalies in traffic patterns – resulting in alerts requiring investigation by a human for triage, deeper understanding and remediation. It requires a level of expertise that not all enterprises possess in their SOC.

The founders of Awake Security have firsthand experience regarding the frustrations of SOC teams struggling to piece together information necessary to contain an attack. There had to be a better way of hunting down IP addresses of affected machines, identifying network traffic detailing the mechanics of a spreading threat, locating endpoint insights to detect compromised processes, and tracking the completion of remediation actions across diverse sets of security products.

The vision of automating threat hunting and SOC efforts via NTA compelled Greylock Partners and Bain Capital Ventures to lead a $30m investment round in July 2017. In addition to a well-funded launch, Awake also has experienced security guidance in board members Asheem Chandna (Check Point) and Enrique Salem (Symantec).

The company's executive team includes Michael Callahan (HP), Gary Golomb (Cylance, NetWitness), Keith Amidon (IntruVert Networks, Nicira), Debabrata Dash (ArcSight, CipherCloud), Brad Kingsbury (Norton, McAfee) and Rudolph Araujo (FireEye, Foundstone). Awake was founded in October 2014 and is based in Sunnyvale, California.

PRODUCTS

The critical layers of Awake's architecture augment the log data and workflow management features of a traditional security operations center with network traffic analytics and device intelligence. The company applies NTA to not only detect threats, but also help SOCs efficiently resolve existing alerts and answer questions arising from incident response investigations.

Key capabilities of the Awake platform include:

- Network packet capture and analysis. Products that can explore unencrypted packets can unveil security signals that are otherwise unavailable to security operations personnel. Awake captures the information useful to security investigators while ignoring the superfluous data.
- It can identify devices on the network from source and destination addresses, and then characterize the devices so SOC teams know what is on the network at any time. This is achieved without the SOC burdens of deploying and managing endpoint agents and is especially useful with the presence of unmanaged devices on today's networks. We believe this real-time view of networked assets may be the company's most powerful feature.
- A library of threat analytics based on attacker tactics and techniques allows Awake to quickly detect attacks and present incident responders with threat details. The technology is customer-extensible, allowing Awake installations to evolve as new threats are introduced and as the business infrastructure transforms.
- It can enhance security information and event management (SIEM) investments with integrations that allow analysts to get detailed device and user profiles based on an IP address or email address for any alert captured by the SIEM.

Awake employs NTA to enable humans to understand the complex relationships between the devices in the environment. Machine learning can't do it all, log data analysis can't do it all, SOC teams can't do it all, and the prevalence of advanced threats means there will always be demand from medium-sized and large enterprises.

COMPETITION

Awake Security bridges incident response and threat detection in a single product, bringing network traffic analytics to SOCs in a manner that complements investments in SIEM products. Privately held NTA vendors are enhancing their ability to automate and orchestrate investigations and remedial actions based on NTA-derived alerts. We classify Awake alongside detection providers Corvil, Darktrace, ExtraHop, SecBI and Vectra Networks. We also see network data being pre-processed for security operations by network specialists Corelight and Gigamon. Strategic networking firms Cisco, FireEye and Fortinet have security operations support based on NTA capabilities.

Three vendors are worth calling out for aligning device hygiene and network activity with security investigations:

- Panaseer provides security operations personnel with visibility of devices, security profiles and incidents. Security and IT teams can work from a common view when investigating security incidents.
- ForeScout automatically characterizes device configurations upon connection to the network. While it is a network admission control provider and is not in the security detection and response space, its ability to automatically classify devices without agents is functionally similar to Awake.
- Palo Alto Networks is building an application framework to unite security applications around network traffic and security logs. Its cloud-based service offers programming interfaces to network security data for custom analytics and security applications.

SWOT ANALYSIS

STRENGTHS

Mapping and fingerprinting devices and users as they appear on the network offers security, networking and IT teams detection of advanced threats while automating response with up-to-date profiles of networked assets – without the need for agents.

WEAKNESSES

Incident response tends to be a SIEM function for real-time tracking and query support. Major SIEM specialists such as IBM, McAfee, Micro Focus and Splunk will be in every security investigation conversation.

OPPORTUNITIES

Awake has built the back-end infrastructure as well as the machine-learning algorithms to consume and analyze data sources beyond just network data that would give enterprises greater day-to-day value.

THREATS

Strategic infrastructure NTA firms can use analytic capabilities to map out devices and applications within enterprises networks, challenging Awake to penetrate major accounts.