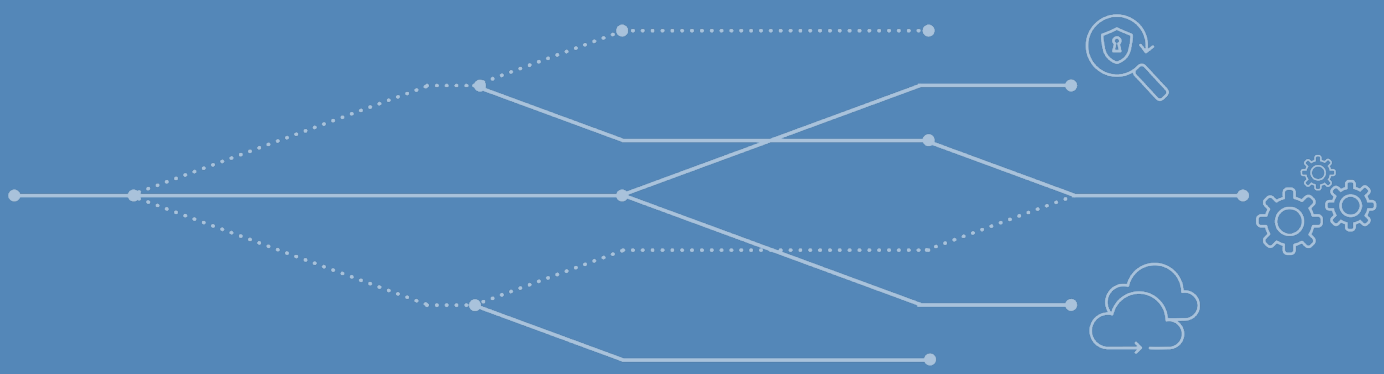

Network Compromise Assessment

Benefits

- Obtain a deep understanding of risk especially for assets that are not protected by endpoint security and log-based security solutions.
- Identify threats that are latent in the environment and spreading laterally using living-of-the-land and other non-malware techniques.
- Spot process flaws and remediate them before they are exploited by attacks such as ransomware.

Uncover threats targeting the organization's broad attack surface including IoT, shadow IT, contractors, supply chain and BYOD while improving incident response resilience.

The Network Compromise Assessment combines human expertise in digital forensics and incident response from Arista's Awake Labs team with threat intelligence and the company's industry-leading network detection and response technology. This assessment focuses on identifying environmental risks, security incidents, and threat actor activity while providing network visibility into aspects such as:

Anomalous encryption tunnels	Security policy bypasses
Anomalous resource sharing	Shadow IT
Data leakage and sensitive clear text information	Suspicious credential usage
Uncommon application activity	Suspicious content
Phishing vectors	Local and remote network challenges
Suspicious domains	Common ransomware tactics and techniques
Unmanaged devices such as IoT, contractor and supply chain	Common early warning indicators associated with ransomware attacks

Scope

That Network Compromise Assessment is offered in two tiers:

Item	Tier 1	Tier 2
Network visibility via the Awake Security Platform	Up to 5 Gbps throughput	Up to 10 Gbps throughput
Duration of monitoring	30 days	30 days
Number of appliances[1] included	1	Up to 3

If additional network traffic or locations need to be monitored, an incremental scope would apply requiring additional appliances provided for a 30-day duration.

[1] Software is licensed under Awake Security's EULA. Awake Labs retains title to the Hardware and grants Customer the limited, personal, non-transferable, non-assignable license, for the period during which the Services are performed, to use the Hardware solely in conjunction with the Services. Within 14 days of the expiration or termination of the Services, Customer will return the Hardware to Awake Labs, in good working condition, reasonable wear and tear excepted, in accordance with Awake Labs' RMA process or will pay the pro-rated purchase price for such Hardware on receipt of an invoice.

Approach

The Network Compromise Assessment is a phased approach that helps provide situational awareness, detection, and the context required to respond. The phases of the project include:

Deployment	Detection and Hunting	Analysis	Reporting
The technology installation requred for the assessment	Discovery of devices, users, applications and threats within the environment	Review and investigation of the high-risk threats using threat intelligence, automation and human expertise	A report of the findings and recommendations identified during the assessment

In addition, Awake Labs professionals will provide regular updates during the assessment of the overall status and proactive updates on critical issues.

Network Detection and Response (NDR) Technology

Awake Labs' network-based review uses the Awake Security Platform which includes hardware and software[1] provided by Awake Labs to review network traffic across both managed and unmanaged devices, thus delivering exceptional visibility beyond the reach of endpoint security platforms. Awake Sensors are deployed at internet egress points and other key network locations. All traffic analysis is contained within the deployed platform, where Awake Labs responders can connect and assess risk remotely.

These Awake Sensors span the "new network"—including the data center, perimeter, core, IoT and operational technology networks as well as cloud workload networks and SaaS applications. Awake parses and processes layer 2 through layer 7 data, including performing encrypted traffic analysis. Awake uses this information to autonomously profile entities such as devices, users and applications, while also preserving these communications for historical forensics.

As part of a network compromise assessment, Awake Labs will provide installation guidelines and consulting support for network deployment activities.

Requirements

To ensure the success of the Network Compromise Assessment, Awake Labs works with the customer to meet the following key requirements:

- Awake Sensors must be deployed at key locations to allow for adequate analysis of managed and unmanaged devices
- All Awake devices within the desired environment must be accessible via remote network connectivity for Awake Labs analysis
- The Customer must provide the appropriate pre-engagement details including documentation, company IP address space, and relevant domains for the assessment
- The Customer must identify a point of contact for the engagement
- The Customer must provide all relevant information for the system and network that are within the scope of the engagement
- The Customer is responsible for network availability at all times during the engagement. The lack of network availability and readiness may hamper Awake Labs' ability to perform certain functions
- If a breach is discovered, and a compromise has been identified, the Customer may need to perform incident response, which may involve additional response work that is outside the scope of this assessment if a retainer does not exist

Work Schedule

The engagement will commence on a mutually agreed date. For each engagement, a kickoff call will be held to confirm and review project logistics and goals.

Work schedules will be based on resource availability and the contract signature date. In some cases, work may be performed with multiple resources or in parallel with other efforts to expedite delivery if appropriate.

Deliverables

The deliverables produced for this engagement include:

Daily and/or weekly status reports

- Summary of activities completed
- Network connectivity and modeling status
- Issues requiring attention and plans for the next reporting period

Network Compromise Assessment Report

- Executive Summary: Key findings and an overview of the services provided
- Network Deployment Summary: Summary of the number of sensors deployed, duration of traffic monitored, and number of models that were triggered
- Relevant Findings: Plan and documentation, network findings and general observations
- Remediation Recommendations: Priority ranked recommendations for the identified weaknesses

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor

Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard

#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062