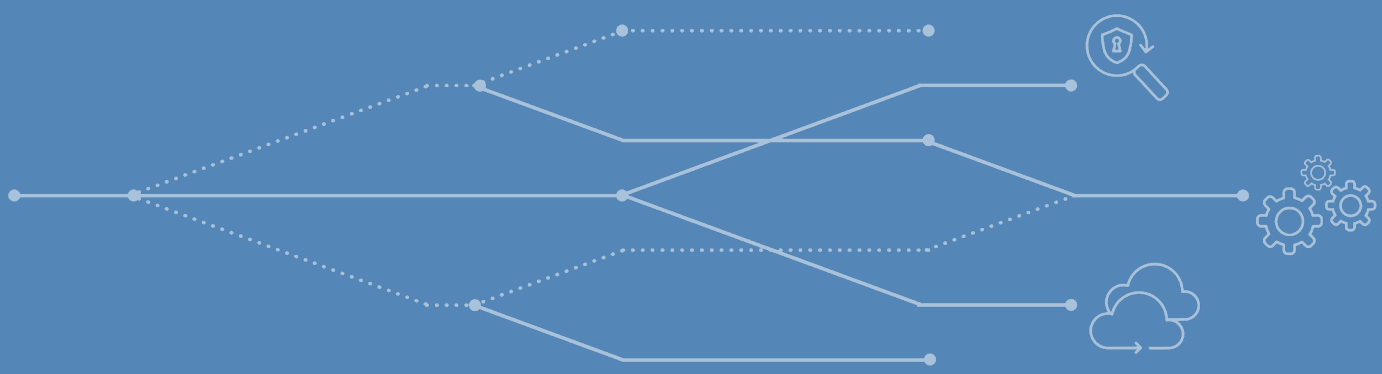

Attack Surface Assessment

Engage a team of proven professionals to help combat today's dynamic threat and improve the organization's breach response resilience.

The Attack Surface Assessment (ASA) 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 threat assessment focuses on identifying:

- Technical risks within the environment including devices, users or applications that may not be monitored today by the organization's security program
- Existing internal and external risk factors that increase the likelihood of a breach
- Early warning signs of an existing breach including the presence of potential threat actor activity
- Gaps in incident remediation practices

Scope

The ASA is offered in tiers based on the size of the organization. For larger organizations please reach out to awake-services@arista.com.

Item	Tier 1 (Organizations with up to 5,000 users)	Tier 2 (Organizations with up to 10,000 users)
Breach response program analysis	✔	✔
Endpoint visibility for end-user devices	Sampling of up to 500 devices	Sampling of up to 1000 devices
OSINT	✔	✔
Breach response	20-hour retainer included	40-hour retainer included

Benefits

- Obtain a deep understanding of risk across data center, campus, cloud and IoT.
- Prioritize security investments based on how an adversary is likely to target the organization.
- Spot process flaws and remediate them before they are exploited by attacks such as ransomware.
- Rapid access to industry-leading incident response expertise whenever you need it via a retainer.

Approach

The ASA identifies ongoing or past attacker activity in the environment. This threat assessment looks at the organization from an adversary's point of view using publicly available information, often called open-source intelligence (OSINT), to identify potential attack vectors. The Awake Labs experts also identify systemic weaknesses within the organization, focusing on the planning, detection, response, and remediation of attacks including ransomware, insider threats and other malicious activity.

The phases of an Attack Surface Assessment include:

Plan and Deploy	Data Collection	Recon and Hunt	Analysis	Reporting
• Establish an engagement plan • Determine the appropriate strategy and architecture for deploying endpoint, network, and open-source technology solutions	• Obtain key details about the architecture, technology and external footprint	• Discover devices, users, applications across the environment • Perform reconnaissance to identify the external attack surface using OSINT • Identify potential misconfigurations / default insecure settings that result in risk • Perform network and endpoint threat hunting	• Review and investigate controls and high-risk threats using threat intelligence, automation and human expertise	• Deliver a report of the findings and recommendations identified during the assessment

During the assessment, the Awake Labs team will provide regular status updates of the overall project and proactive notifications on critical issues.

Attack Surface Assessment Analysis

The overall scope of the engagement will focus on data collection and reconnaissance across the environment, reviewing specific controls such as program and technology analysis, network areas of analysis, endpoint areas of analysis, and OSINT areas of analysis which are defined below.

Program and Technology Analysis

- Review of incident response program documentation
- Review of incident response backup restoration plans and processes
- Review of detection and response operations
- Identification of protections associated with key IT assets including domain controllers, fileservers, key application systems, key databases, critical data systems that may include PHI or PII
- Endpoint security protections
- Network segmentation strategy and approach
- Offline systems for incident response

Network Analysis

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

Endpoint Analysis

- MITRE ATT&CK tactics and techniques
- Validation of network threats
- Security policy and control bypass
- Potential unapproved software
- A review of endpoint security solutions, coverage, and containment strategy

OSINT Analysis

- Exposure associated with publicly available corporate email addresses
- Exposure with employee user account and data associated with past breaches of third-party services and applications
- Available surface and exposures with identified public host assets
- Available surface and exposures with publicly available IP addresses
- Risk associated with employee social media public profiles
- External search of people associated with the organization
- Potential open shares and configurations

Attack Surface Retainer

- Remote Response - by phone or email, within 8 hours of an incident declaration
- Initial investigation assistance and direction including clarification of the potential scope of the investigation
- Forensic system and log analysis
- Containment and remediation planning and assistance
- Evidence collection and analysis
- Detailed technical report and executive presentation based on the findings and recommendations

Deliverables

The deliverables produced for this engagement include:

Daily and/or weekly status reports

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

Attack Surface Assessment Report

- Executive Summary: Key findings and an overview of the services provided
- Endpoint Deployment Summary: Summary of the number of endpoints deployed and the percentage of the environment reviewed
- 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 review findings, network and endpoint adversarial model and compromise findings, OSINT findings, and general observations about the attack surface
- Remediation Recommendations: Priority ranked recommendations and mitigation techniques for key identified weaknesses as well as preparations to defend against ransomware and other attacks

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