



Zero Trust Security

"You cannot protect what you cannot see and understand"

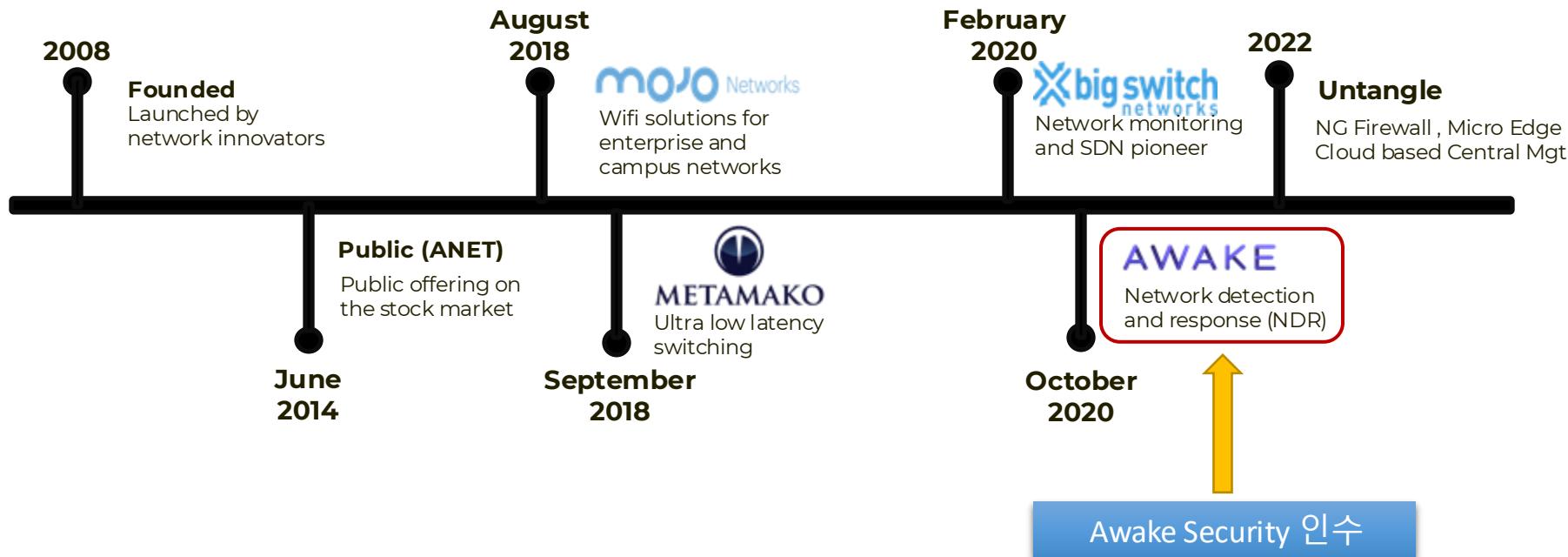
Arista NDR 솔루션 소개

Network Detection & Response

2025.Q3



Arista Networks 연혁



“Awake 플랫폼은 새로운 위협을 탐지하고 대응하는 능력이 탁월하고 비용 효율성 부분 1위에 Rank 된 솔루션으로 뛰어난 ROI로 기업에 큰 가치를 제공합니다”

더이상 침해사고를 방지해서는 안됩니다

- 지난 1년간 63% 기업이 침해사고를 경험
- USD 240M 평균 피해액
- 70% 외부로부터 침해사고를 확인



Network Detection & Response



네트워크 내부 다양한 종류의 Device / 어떻게 관리?

The Visibility Minefield



Core & Perimeter

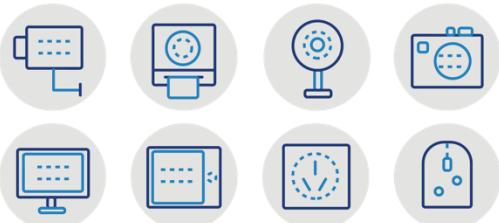
Shadow IT & IoT 단말

Supply chain
& Contractor

재택근무자

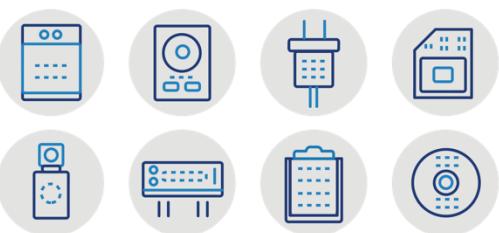
퍼블릭 클라우드 & SaaS

New normal



> 50%

관리 영역을 벗어난
“Unmanaged Device”



보안에 대한 인식의 전환 필요

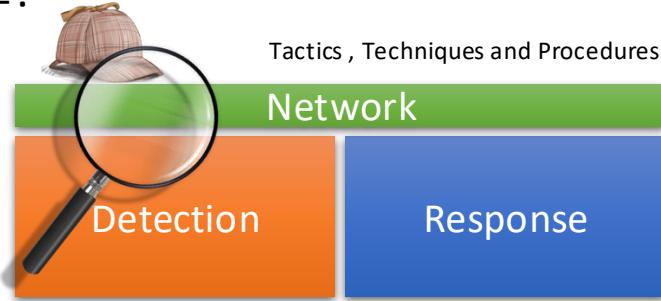
‘방화벽’만으로 ‘침해사고’를 막을 수 있을까요?

Indicators of Compromise

차단 (필터링)을 위한 보안



Tactics , Techniques and Procedures



경계 보안 솔루션 / Perimeter Security

차세대 방화벽 , IPS , UTM 웹방화벽 , Sandboxing(APT)

악성 IP / URL 정보는 쉽게 변경될 수 있음

수동적 보안

“위협은 발견하지 못했을 뿐 네트워크에 침투해 있다”



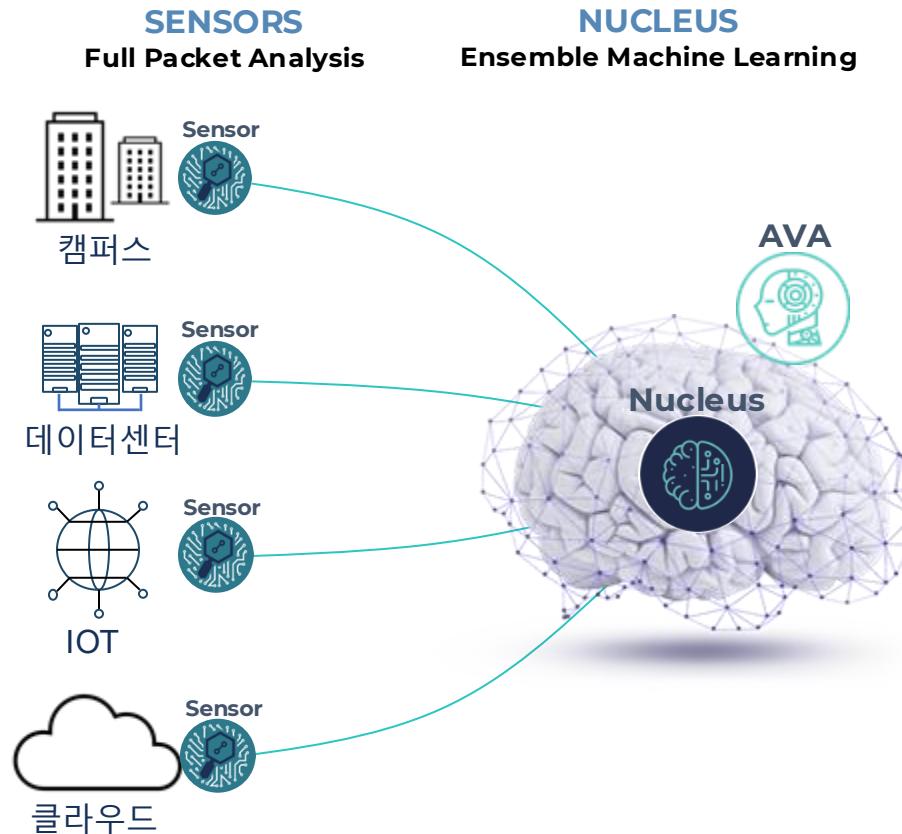
능동적 보안





ARISTA NDR 솔루션 상세 소개

Arista의 AI/ML 기반 NDR 솔루션 구성요소



Situational Awareness (EntityIQ™)

AI기반 Fingerprint 기법을 활용하여 네트워크의 장치, 사용자, 어플리케이션에 대한 Profiling을 제공하고 추적(Tracking) 관찰

위협 탐지 (Adversarial Modeling™)

전문가들이 구성한 위협 모델을 통해 오탐을 최소화하고 내/외부로부터의 위협을 감지

Autonomous Security (AVA™)

AI기반 Expert System AVA를 통해 위협 행위를 추적하고 침해 사고 판별 과정을 도움

Arista NDR 기대효과

보안분석

- 포렌식 패킷 로그 캡처
- 네트워크 프로토콜에서 상세한 활동 데이터 파싱 및 추출
- 네트워크 상에서 활동하는 앤티 티의 탐지, 추적, 특성화
- 악의적이거나 이상 행위의 탐지

Arista NDR



기대효과

AI 기반 보안 기능으로 네트워크의 자율 보안 (Self-Securing) 실현

IoT 및 unmanaged 장비 보안, 내부자 위협 및 공급망 위협, 랜섬웨어 대응 등 핵심 보안

End-point 경리, 경계 차단, 티켓 발급 등 3rd party 외의 통합을 통한, 사고 대응 및 복구 최적화

Arista Labs의 위협 헌팅 및 24/7 모니터링 전문성 제공 (On-Line 시)

기존 스위치 활용 시 간편한 구축 및 낮은 운영 비용 실현 (Arista Switch 사용 시)

Arista NDR Positioning

1. 방화벽 내부 ↔ 인터넷 연결 지점

- 조직 외부에서 시작된 모든 위협은 반드시 방화벽을 통과해야 하므로,
- 방화벽의 내부 트래픽을 모니터링하면 대부분의 원격 위협을 탐지 가능.
- 외부 서비스와 통신하는 내부 장비의 행동 특성 분석에도 매우 유리.

2. DMZ 및 VPN 연결 지점

- DMZ는 외부나 서비스와 연결되는 영역으로, 공격 등 위협탐지에 중요.
- 또한 DMZ에는 종종 VPN 서버가 배치되어 있으며, VPN을 통한 내부 접근은 피싱 등을 통해 탈취된 정상 사용자 계정으로 위장한 공격에 취약 할 수 있음.
- VPN의 입출입 트래픽 모니터링은 이와 같은 위협 경로 탐지에 필수.

3. 데이터센터 ↔ 캠퍼스 네트워크 연결 지점

- 데이터센터는 대부분의 기업에서 업무 핵심 애플리케이션과 데이터가 존재하는 핵심 자산입니다.
- 공격자는 종종 최종 사용자 장비를 먼저 감염시킨 후 **수평 이동(Lateral Movement)**을 통해 데이터센터 자산을 목표로 합니다.
- 사용자와 서버 간의 프로토콜 교환은 엔티티 특성 파악 및 탐지 정확도 향상에 큰 도움을 줍니다.

4. 캠퍼스 스위치 포트

- 최종 사용자 워크스테이션 감염이 초기 침해 단계인 경우가 많기 때문에, 사무실 네트워크 모니터링은 중요합니다.
- 캠퍼스 트래픽 분석을 통해 빠른 대응과 문제 장비 격리가 가능해집니다.
- Arista AVA Switch Sensor는 별도의 센서 없이 기존 스위치에서 보안 데이터 수집이 가능하여, 비용 및 복잡도는 낮추고 가시성을 극대화하는 독보적 기능을 제공합니다.

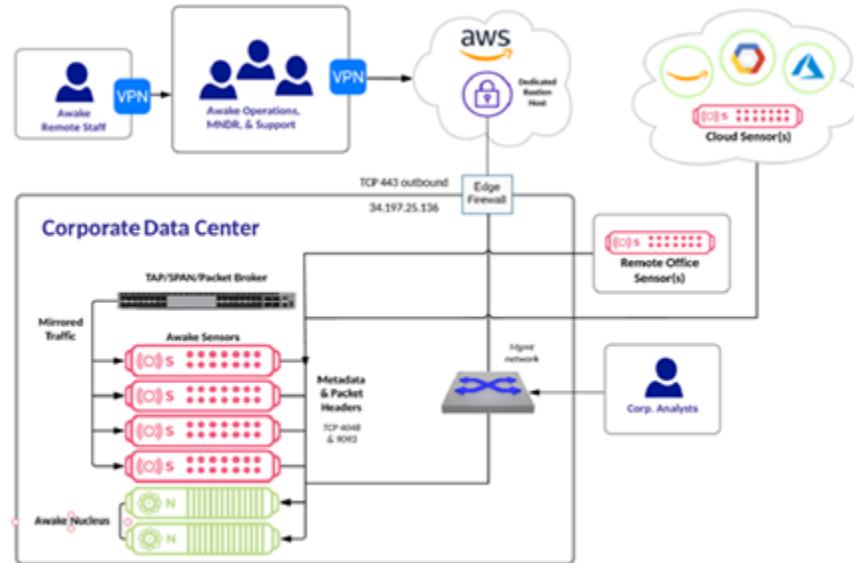
Arista NDR / Distribute 구성

- Sensor 와 Nucleus를 별도의 Appliance로 구성
- Sensor
 - Physical Sensor (100M / 1G / 5G / 10G)
– 2025년 4Q 40G 지원 예정
 - Virtual Sensor (500M / 1G / 5G)
 - Switch Sensor (Up to 149 / 150 ~ 499 / 500 over)
 - Cloud Instance Sensor (Amazon 1G / 5G , Google 1G)
- Nucleus
 - Physical Nucleus (10G / 20G)

구성 예시

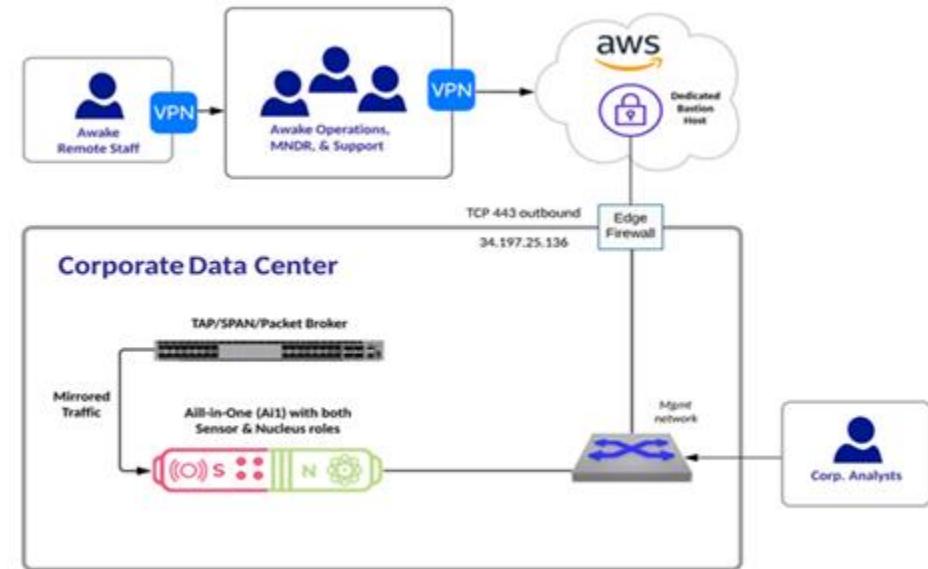
- ✓ 10G : Sensor 2대 , Nucleus 1대 구성
- ✓ 20G : Sensor 4대 , Nucleus 2대 구성
- ✓ 40G : Sensor 8대 , Nucleus 4대 구성

Sensor 구성은 최대 10대



Arista NDR / All-In-One 구성

- “Sensor”와 “Nucleus”를 하나의 플랫폼으로 통합 구성
- Arista NDR All-In-One Appliance 구성 시 평균 5 Gbps 최대 7Gbps (peak) 용량 처리



Arista NDR 솔루션 특징 - I (AI 분석 시스템)

Situation

** AVA : The Arista Virtual Assist

AI 시스템 (AVA)에 의한 '자율 위협 감지' 및 '판별'

- 비정상적 또는 의심스러운 이벤트에 대하여 연관된 Malicious Activity 를 조사
- 관리자가 Situation (Case)를 생성 후 관련 데이터(또는 Activity)를 해당 Case 에 추가
- Situation Open 후 Ava (AI엔진)가 스스로 관련 위협 정보를 수집하여 해당 Case 에 추가하고 , 위협 Event , activity 의 상관 관계를 Attack map 형태로 보여줌



“Situation”을 통한 위협 심층 분석 (Threat Hunting)

- Attack Map을 통해 각 단계별 Suspicious activity에 대한 Visibility 제공
- Ava (Arista Virtual Assistant)가 Autonomous Correlation 분석에 참여



“Situation”을 통한 위협 심층 분석 (Threat Hunting)

- Ava(AI 엔진)가 위협 헌팅에 참여하여 연관된 위협 정보를 조사 (Link Analysis)

Type	Name	Role	Source	First Attached
Activity	Exfiltration: Device sending unencrypted data to risky domain via HTTP post	Suspected Exfiltration		20:31:14 Aug 11, 2022
Activity	C2: Spoofed HTTP activity to Ava analyzed destination	Suspected C2		21:15:47 Aug 11, 2022
Domain	app.siseticogeti.com	Suspected Exploit Source		21:27:18 Aug 11, 2022
Domain	siseticogeti.com	Suspected Command & Control Source		21:50:32 Aug 11, 2022
Device	DESKTOP-TT1C69J	Suspected Victim		21:50:34 Aug 11, 2022
Ava Destination Analysis	Reputation for siseticogeti.com	Artifact Analysis		22:12:14 Aug 11, 2022
IP Usage Report	IP usage for siseticogeti.com	Artifact Analysis		22:12:56 Aug 11, 2022
Query	Domains first seen for DESKTOP-TT1C69J around time for siseticogeti.com.	Unknown		22:29:30 Aug 11, 2022
Query	All traffic to siseticogeti.com	Suspected C2		22:30:00 Aug 11, 2022

관리자에 의해 입력된 정보들

Ava (AI)에 의해 자동 입력된 정보



Arista NDR 솔루션 특징 - II (모델 기반 위협 탐지 및 분석)

ML기법이 연계된 Adversarial Model (공격 모델) 제공

** TTP : Tactic,Technique,Procedure(전략, 전술, 절차)

- 각종 사이버 공격 및 위협 행위에 대해 Arista Lab 전문가들이 AML 기반으로 생성한 TTP 라이브러리
- 각 Model 은 Machine Learning 결과와 연계되어 분석의 정확도를 높임 (Un-Supervised / Supervised ML)
- 기존 모델의 AML code 를 수정하여 고객사 환경에 맞는 custom 모델 생성 가능

Adversarial Models ⓘ								0 models selected							
<input type="checkbox"/>	Status	Package	Name	Expires On	Severity	Last Modified	User	Adversarial Model							
<input checked="" type="checkbox"/>	Active ⓘ	AWAKE	Lateral Movement: Transfer and Remote Code Execution Remote Execution, Lateral Movement	Never	9	07:32:20 Apr 01, 2025	Ava								
<input checked="" type="checkbox"/>	Active ⓘ	AWAKE	Lateral Movement: Uncommon Software Making Suspicious ...	Never	2	02:54:34 Mar 27, 2025	Ava								
<input checked="" type="checkbox"/>	Active ⓘ	AWAKE	Impact: Batched Dumping of Slack Data	Never	2	02:35:36 Mar 27, 2025	Ava								
<input checked="" type="checkbox"/>	Active ⓘ	AWAKE	Lateral Movement: SMB Client Negotiation Followed by Unc...	Never	2	09:05:34 Mar 26, 2025	Ava								
<input checked="" type="checkbox"/>	Active ⓘ	AWAKE	C2: Repeated TLS connections to uncommon domain	Never	0	10:54:56 Mar 21, 2025	Ava								
<input checked="" type="checkbox"/>	Active ⓘ	AWAKE	Credential Access: MSSQL Server Credential Brute Force	Never	3	06:22:03 May 29, 2024	Ava								
<input checked="" type="checkbox"/>	Active ⓘ	AWAKE	C2: Characteristic Indicative of Suspicious Use of Discord API	Never	6	10:51:24 Jan 29, 2025	Ava								
<input checked="" type="checkbox"/>	Active ⓘ	AWAKE	Initial Access: Supply Chain Popular Package Library Downl...	Never	1	17:50:44 Mar 06, 2025	Ava								

Arista NDR 솔루션 특징 - II (모델 기반 위협 탐지 및 분석)

MITRE ATT&CK 기반의 Adversarial Model

Coverage ⓘ MITRE ATT&CK							
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
54 Total Skills	67 Total Skills	43 Total Skills	29 Total Skills	79 Total Skills	84 Total Skills	140 Total Skills	85 Total Skills
Drive-by Compromise T1189	Command and Scripting Interpreter T1059	Account Manipulation T1098	Abuse Elevation Control Mechanism T1548	Abuse Elevation Control Mechanism T1548	Brute Force T1110	Account Discovery T1087	Exploitation of Remote Services T1210
11 Skills	21 Skills	0 Skills	2 Skills	2 Skills	19 Skills	30 Skills	9 Skills
Exploit Public-Facing Application T1190	Exploitation for Client Execution T1203	BITS Jobs T1197	Access Token Manipulation T1134	Access Token Manipulation T1134	Credentials from Password Stores T1555	Application Window Discovery T1010	Internal Spearphishing T1534
13 Skills	8 Skills	2 Skills	6 Skills	6 Skills	13 Skills	1 Skill	1 Skill
External Remote Services T1133	Inter-Process Communication T1559	Boot or Logon Autostart Execution T1547	Boot or Logon Autostart Execution T1547	BITS Jobs T1197	Exploitation for Credential Access T1212	Browser Bookmark Discovery T1217	Lateral Tool Transfer T1570
10 Skills	4 Skills	1 Skill	1 Skill	2 Skills	6 Skills	1 Skill	18 Skills
Hardware Additions T1200	Native API T1106	Boot or Logon Initialization Scripts T1037	Boot or Logon Initialization Scripts T1037	Deobfuscate/Decode Files or Information T1140	Forced Authentication T1187	Domain Trust Discovery T1482	Remote Service Session Hijacking T1563
1 Skill	1 Skill	1 Skill	1 Skill	1 Skill	4 Skills	7 Skills	Skill Range 0 1-3 4-7 8-11 12-17 18+

800 여개 모델

- Initial Access (54)
- Execution (67)
- Persistence (43)
- Privilege Escalation (29)
- Defense Evasion (79)
- Credential Access (84)
- Discovery (140)
- Lateral Movement (85)
- Collection (16)
- Command & Control (190)
- Exfiltration (92)
- Impact (14)

Arista NDR 솔루션 특징 - II (모델 기반 위협 탐지 및 분석)

Adversarial Model 상세 정보 예제

Adversarial Models / Lateral Movement: Transfer and Remote Code Execution

Lateral Movement: Transfer and Remote Code Execution AWAKE 5.0.6 → Unspecified Show Version History

Reference Identifier: models.lateralMovement.transferAndExecution

Description Expression Related Definitions Exceptions Skill Metadata

Description

Overview

Threat actors often move to additional devices on the network in order to establish an additional foothold. One way to do this is to transfer executable files or PowerShell scripts over SMB without a file path (indicating the file is located in C:\Windows\temp).

Technical Details

This model identifies Windows executables or PowerShell scripts being sent over SMB without a file path (indicating the file is located in C:\Windows\temp)

Investigation and Remediation

1. If possible, identify the user sending or receiving the file to determine if they have legitimate use for the file.
2. Identify both the source and target devices to determine the purpose of these devices (e.g. Software Deployment server).
3. Look for any new/unusual traffic shortly after the file was transferred.

References

- Mitre ATT&CK ID: T1021.002
- Mitre ATT&CK ID: T1021.006
- Mitre ATT&CK ID: T1210

Expression

Current

```
1 let models.lateralMovement.transferAndExecution =
2   model
3   /* Identify the query in AQL1 followed by activities matching the query in AQL2 within 10 seconds */
4   [
5     (
6       /* AQL1 query */
7       recipes.protocols.smb.files.executableTransferToSuspectDirectory &
8       !(device.name like r/^^(pentest:nirvRNA|nessus)/)
9     ),
10    (
```

- ✓ 위협 모델에 대한 구문 (Expression) 제공
- ✓ 각 모델은 Customizing 가능

해당 모델 요약 해석 (Lateral Movement: Transfer and Remote Code Execution)

“의심스러운 위치에 실행파일이 전송된 직후, 곧바로 그 파일을 실행하려는 SMB/WMI 명령이 발생하면 공격으로 의심”

Adversarial Model (AM) / 공격 모델 (800여개)

- 각 위협 모델(AM)별 match된 Device Count , Activity Count , Score 및 상세 정보 제공

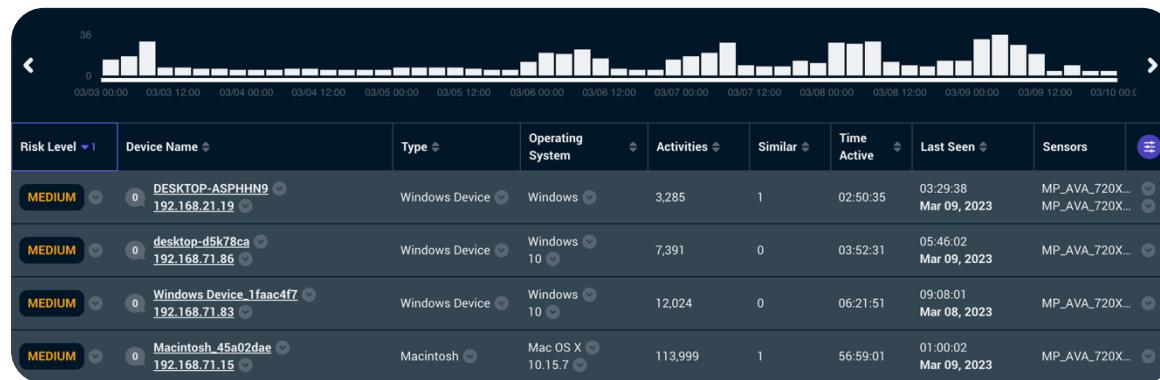
Model Matches ①										
All	Threats	Compliance	Score	Status	Name	Device Count	Activity Count	Last Matched Date	Last Matched Time	Actions
98	● Active	✓	C2: Spoofed HTTP Activity to Ava Analyzed Destination	7	71	Apr 01, 2025	08:00:00	View Matches		
89	● Active	✓	C2: Ava Analyzed Non-Browser HTTP to Newly Seen Server C2	10	120	Apr 01, 2025	06:00:00	View Matches		
66	● Active	✓	Exfiltration: SSL Upload From Non Browser To Suspicious Domain Exfiltration	1	103	Apr 01, 2025	12:00:00	View Matches		
65	● Active	✓	C2: Uncommon Executable Communicating with Suspect Destination C2	5	2,382	Apr 01, 2025	12:00:00	View Matches		
64	● Active	✓	C2: Ava Analyzed Non-Browser TLS to Newly Seen Server C2	10	131	Apr 01, 2025	09:00:00	View Matches		
46	● Active	✓	C2: Non-Browser TLS Communicating To Uncommon And Suspicious Domain C2	3	2,348	Apr 01, 2025	12:00:00	View Matches		
41	● Active	✓	Download: Executable Downloaded from Ava Analyzed Suspect Server Download	12	59	Apr 01, 2025	08:00:00	View Matches		
11	● Active	✓	Initial Access: Suspected click on phishing link Initial Access	1	6	Apr 01, 2025	07:00:00	View Matches		
10	● Active	✓	Discovery: Checking External IP Discovery	3	105	Apr 01, 2025	09:00:00	View Matches		
8	● Active	✓	Compliance: Possible Unencrypted Password Storage Discovery	3	48	Apr 01, 2025	07:00:00	View Matches		
6	● Active	✓	C2: DC Rat HTTP Indicators	1	1	Apr 01, 2025	02:00:00	View Matches		
4	● Active	✓	Download: Indicative of Download from Raw Github User Content Download	3	15	Apr 01, 2025	07:00:00	View Matches		

관련된 Activity
정보로 연계

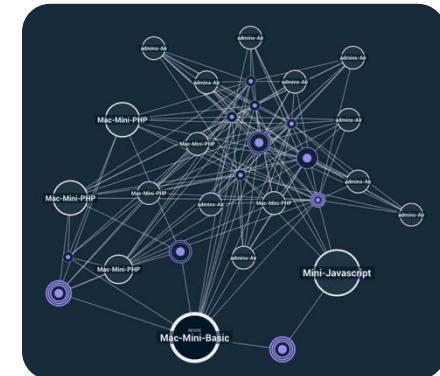
Arista NDR 솔루션 특징 – III (Device Profiling)

네트워크에 연결된 Managed , Unmanaged 장치를 모두 추적 !

- Machine Learning을 통해 Device 종류 , OS , User ID를 기준으로 Device Profile 제공
(** AD/LDAP등의 인사 DB 연동 없이 Packet data를 통해 정보 제공)
- 앤드포인트 보안이 적용되지 않은 네트워크 단말까지 모두 발견하여 추적
- 네트워크 단말 별 Risk Level 및 위협 행위 탐지
- 유사 장치 (Similar Device) 분석 기능 제공



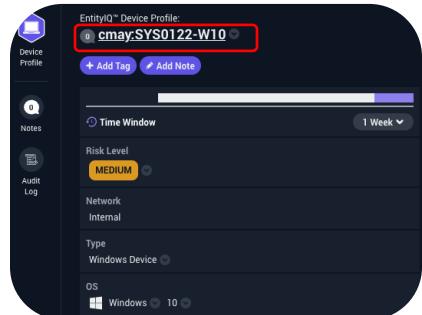
유사 장치 MAP



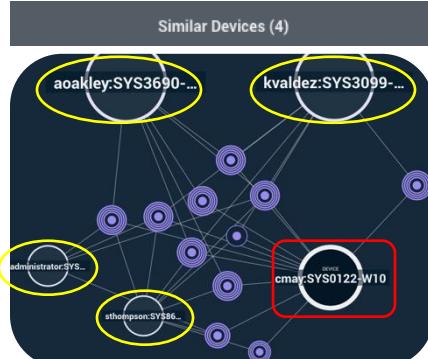
Arista NDR 솔루션 특징 – III (Device Profiling)

❖ Similar Device (유사 장치) 분석 기능

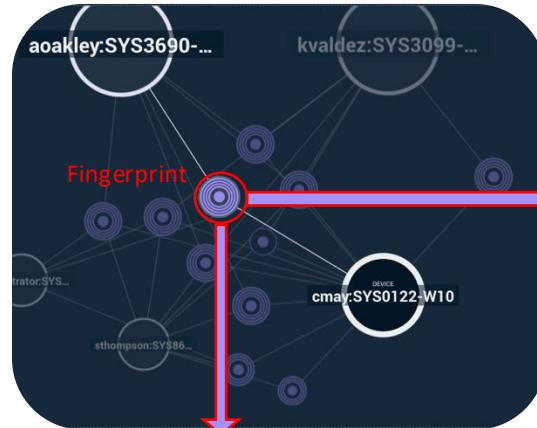
① 특정 Device 정보 확인 (cmay:SYS0122-W10)



② 총 4개의 유사 Device 확인



③ Fingerprint 선택



매칭 Count

④ Fingerprint 상세 정보 확인

DNS Request Stemmed	
10	"ml314.com"
1	"gvt1.com"
1	"krxd.net"
1	"mathtag.com"
1	"msauth.net"
1	"openx.net"
1	"quantserve.com"
1	"rubiconproject.com"

HTTP Request User Agent	
10	"Mozilla/5.0 (Windows NT 10.0; Win_
1	"Microsoft BITS/7.8"

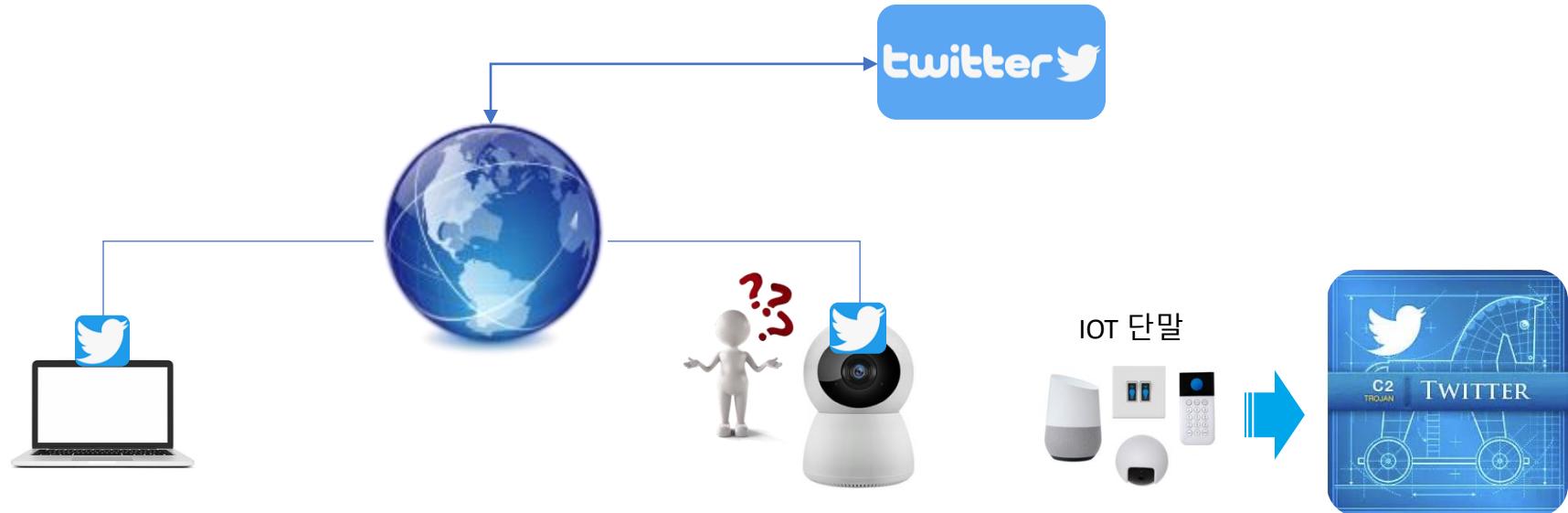
Destination Autonomous System D...	
1	"AS25751"
1	"COGECHO-PEER1"
1	"MEDIAMATH-INC"
1	"OMNITURE"

'네트워크 단말'에 대한 '식별'이 왜 중요할까?

- **Command & Control (C&C)**: 감염된 단말(PC, IoT)을 제어하는 서버

- SNS를 C&C로 활용하는 사례

- ✓ Twitter의 API나 DM 등을 이용해 명령을 전달
- ✓ 암호화된 명령을 게시하여 감염된 단말이 이를 읽고 실행



단말의 종류를 정확히 파악해야 **단말의 행동**이 “정상”인지 “비정상”인지 판단할 수 있음

Arista NDR 솔루션 특징 – IV (메타데이터 분석)

Protocol Metadata 및 Application ID 제공

❖ 26개 프로토콜에 대한 메타데이터 분석

- ✓ Transport
 - > IP
 - > TCP
 - > UDP
- ✓ Internet
 - > HTTP
 - > QUIC
 - > TLS
- ✓ Name Resolution
 - > DNS
 - > LLMNR
 - > MDNS
 - > NBNS
- ✓ Authentication
 - > Kerberos
 - > LDAP
- ✓ Remote Access
 - > DCERPC
 - > SMB
 - > TeamViewer
 - > SSH
 - > RDP
- ✓ Mail
 - > POP3
 - > SMTP
- ✓ Network & Device Mgmt
 - > DHCP
 - > NTLM
 - > ICMP
 - > WCCP2
 - > MSCLDAP
- ✓ ICS
 - > MODBUS
- ✓ Database
 - > TDS

❖ 3000종의 Application에 대한 Identification

NTP	BING	GOOGLE_ACCOUNTS
META_GEN	NETBIOS	HTTP_PROXY
INSTAGRAM	MAILSLOT	CHATGPT
SMB	DATA_SAVER	EVERNOTE
KAKAO	SYNOLOGY_BACKUP	BITDEFENDER_UPDATE
IPV6	SSDP	STUN
NAVER	UPNP	NEXON
SSH	FACEBOOK	MOZILLA
GOOGLE_API	GSTATIC	KAKAOCDN
OFFICE365	MS_EDGE	CONTENTFUL
CLOUDFLARE	SAMSUNG	GOOGLE_CALENDAR
GCP	OPENAI	XBOXLIVE

Arista NDR 솔루션 특징 – IV (메타데이터 분석)

Protocol Metadata 및 Application ID 제공 (Activity)

Activity	Start Time	Source	Destination	Protocols	Details
Details ▾	01:30:18 Mar 26, 2025	172.30.4.1 ▾	224.0.0.5 ▾	IPv4, OSPFIGP	IP-Protocol: OSPFIGP Source: 1 packet, 80 bytes Destination: 0 packets, 0 bytes
Details ▾	01:30:18 Mar 26, 2025	54.78.121.95 ▾	UnnamedDevice_f8238... 10.102.102.15 ▾	IPv4, ICMP	Ping Request: 1 packet, 40 bytes ← Reply: 1 packet, 40 bytes
Details ▾	01:30:18 Mar 26, 2025	54.171.34.28 ▾	Awake Security Platfor... 192.168.197.100 ▾	IPv4, ICMP	Ping Request: 1 packet, 40 bytes ← Reply: 1 packet, 40 bytes
Details ▾	01:30:18 Mar 26, 2025	ksh:DESKTOP-QCHMH8P ▾ 192.168.130.189 ▾: 63642 ▾	168.126.63.1 ▾:53 ▾	IPv4, UDP, DNS	Query: A katalk.kakao.com ▾ ← CNAME brewery-talk-external-azp9mem5.kgns1.com for 537s A 121.53.93.36 for 7s
Details ▾	01:30:18 Mar 26, 2025	UnnamedDevice_185fb... 172.30.0.3 ▾	Lights Out Management... 10.215.128.126 ▾	IPv4, ICMP	Time exceeded on path from 10.215.128.126 ▾ to 10.252.16.1 ▾
Details ▾	01:30:18 Mar 26, 2025	ksh:DESKTOP-QCHMH8P ▾ 192.168.130.189 ▾: 61095 ▾	katalk.kakao.com ▾ 121.53.93.36 ▾:443 ▾	IPv4, TCP, TLS	Application: KAKAO TALK Version: TLSv1.2, cipher suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, comp method: NULL_TLS_COMPRESSION Client requested server: katalk.kakao.com ▾, Session ID: 0x'a8ae389..." was not resumed Server Session ID: 0x'89f2514..." Server cert name: *.kakao.com, org: Kakao Corp., issued by: Thawte TLS RSA CA G1, valid: 2024-09-02T00:00:00Z - 2025-09-29T23:59:59Z

- ✓ 기본적으로 5-Tuples 세션 단위로 Activity 제공 (송/수신 패킷 수 및 데이터 Byte 정보 포함)
- ✓ Protocol 별 메타데이터 제공
- ✓ Application Identification Signature 제공 (3천여 개)

[Metadata Summary]

TLS
Lowest Version Supported TLSv1.0 ▾
Version Used TLSv1.2 ▾
Client Packet Count 3 ▾
Client Byte Count 804 ▾
Server Packet Count 8 ▾
Server Byte Count 7209 ▾
Server Name katalk.kakao.com ▾
Server Name (stemmed) kakao.com ▾
Client Hello Fingerprint 5d3ae2ac43a32741032b96fde7366733 ▾
JA3 Hash a3afc2c46ba4a7d7fbe1cfb7a3031c2f ▾
JA3S Hash 61be9ce3d068c08ff99a857f62352f9d ▾

Arista NDR 솔루션 특징 – IV (메타데이터 분석)

Activity Details (상세정보)

Artifacts / 2808d914-4b2e-4efc-833f-42b80686fe81

← 2808d914-4b2e-4efc-833f-42b80686fe81 Activity Profile + Add to Situation :

Start Time: Mar 25, 2025 15:49:41

Duration: 1us

IOC Matches: None

Source: UnnamedDevice_dde0a0f7 10.128.129.42 49186

Destination: 168.126.63.1 53

Protocols: IP, UDP, DNS

Sensor: MP_ID0

Extracted Data Activity Analysis Captured Data

Search Extracted Data

IP

Source IP	10.128.129.42
Destination IP	168.126.63.1
IP Protocol Number	17
Destination Autonomous System Number	4766
Destination Autonomous System Country Code	KR
Destination Autonomous System Description	KIXS-AS-KR Korea Telecom
Source Packets	0
Source Bytes	0
Destination Packets	1
Destination Bytes	97

DNS

DNS Transaction ID	64594
DNS Request Question Type (Deprecated)	A
DNS Request Question Type	A
DNS Request Question Name	time.google.com
DNS Request Name (Stemmed)	google.com
DNS Response Code	NoErr
DNS Response Question Type (Deprecated)	A
DNS Response Question Type	A
DNS Response Question Name	time.google.com

MAC

Mac Source	00:00:5e:00:01:1e
Mac Destination	0c:7b:c8:cc:ed:7e
Virtual LAN Identifier	0

예제) DNS 트래픽에 대한 metadata

상세한 메타데이터 정보 제공이 왜 중요할까?

- 정상과 비정상을 구분하는 핵심 근거는 결국 **Metadata**

- IP & Port 정보 만으로는 위협을 판단 근거로 부족



- 프로토콜 별로 상세 정보를 확인 하여야 비정상 행위를 판별 할 수 있음

(예: SMB 트래픽은 일반적으로 사용되지만, SMB 메타데이터 내에 TreeConnect, FileRead, FileWrite 등의 message 확인을 통해 Lateral movement 여부를 판단 할 수 있음)

메타데이터가 있어야 온밀한 위협, 내부자의 활동, C&C 통신을 정확하게 탐지

Full Packet 기반 분석 및 PCAP File Export

- ❖ Arista NDR 은 Full Packet 기반 분석을 제공하고 일정 기간 동안의 패킷을 보관 및 Export 가능

The screenshot shows the Arista NDR interface. At the top, there are tabs: Extracted Data, Activity Analysis, and Captured Data, with 'Captured Data' being the active tab. Below the tabs, a list of captured packets is displayed:

- 12 Bytes Starting 2025-04-01 05:00:08:091529000 (SSH-2.0-Go)
- 21 Bytes Starting 2025-04-01 05:00:08:122144000 (+0.030615000s) (SSH-2.0-OpenSSH_8.2)
- 1,168 Bytes Starting 2025-04-01 05:00:08:325604000 (+0.203460000s) (Source)

A context menu is open over the third packet, listing options: Add to Query, New Query, Copy to Clipboard, and Export to PCAP. The 'Export to PCAP' option is highlighted with a red box.

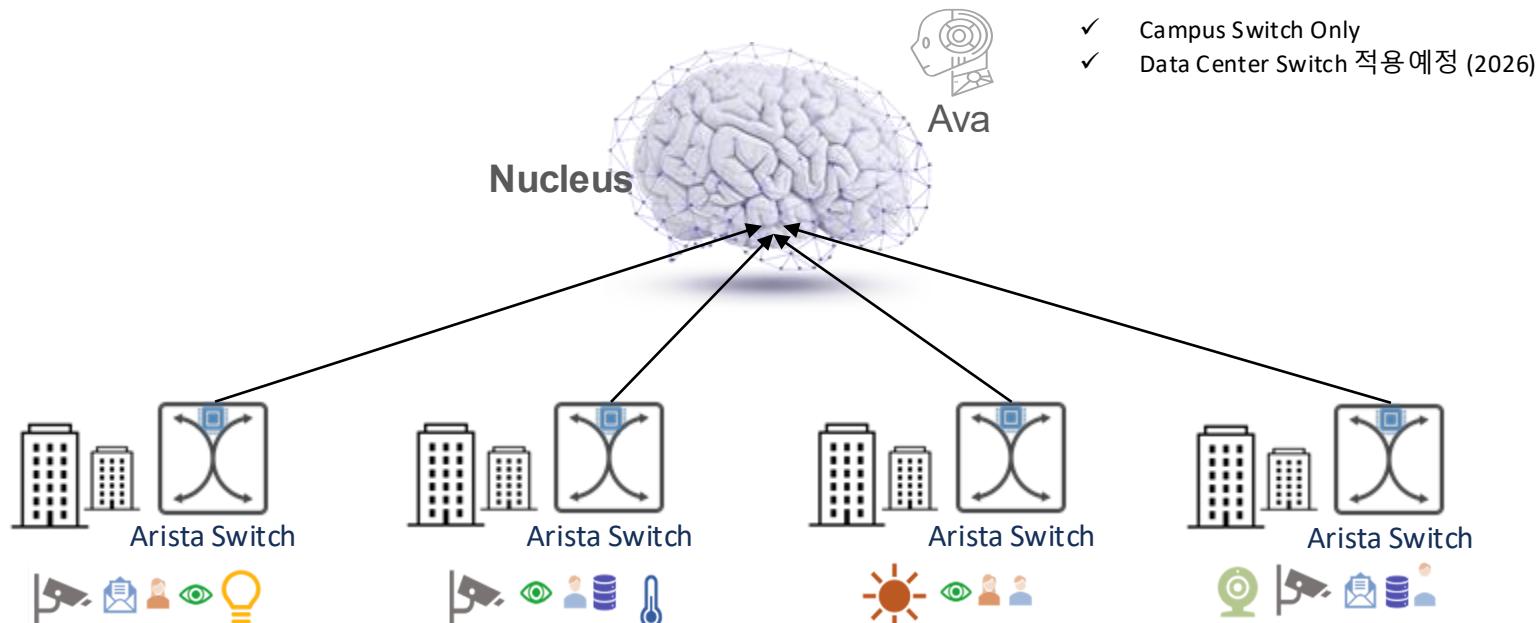
The detailed view of the third packet shows the raw hex and ASCII data:

```
00000000 ?d~@FuF0curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,ext-info-c,kex-strict-c-v0@openssh.com@rsa-sha2-256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-dss-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,rsa-sha2-256,rsa-sha2-512,ssh-rsa,ssh-dss,ssh-ed25519aes128-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,3des-cbc,aes128-cbciaes128-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,3des-cbc,aes128-cbcnhmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96nhmac-sha2-2
```



아리스타 스위치에서 직접 Application 메타데이터 분석

- 별도의 트래픽 수집기(Sensor) 없이 Arista 스위치에서 직접 Application Metadata 추출 후 Nucleus와 연동



Beyond NetFlow - 심도 깊은 트래픽 분석

스위치에서 각종 어플리케이션 별 Meta Data 제공

- Internet
 - ✓ HTTP, QUIC, TLS
- Name Resolution
 - ✓ DNS, MDNS, LLMNR
- Authentication
 - Kerberos, LDAP
- File
 - SMB
- Remote Access
 - DCERPC, SMB, Teamviewer
- Mail
 - SMTP, POP3
- Network & Device Mgmt
 - DHCP, NTLM, ICMP, WCCP2, MSCLDAP
- ICS
 - MODBUS

○ NetFlow vs ARISTA Switch Sensor Data 비교

NetFlow	BYTES	PKTS	IP_SRC_ADDR	IP_DST_ADDR	Protocol	Activity Records
	L4_SRC_PORT	L4_DST_PORT	TCP_FLAGS	VERSION		
smb.authentication.nt status		smb.share.open _statuz	smb.share.path	smb.authentication. ntlm.username	smb.authentication. n.ntlm.domain	
smb.authentication.ntl m.workstation		smb.authentication.k erberos.principal	smb.authentication.k erberos.tickethash	smb.authentication. kerberos.realm	smb.share.id	

More context ⇒ Better detection and response ⇒ Lower SecOps costs



Arista Switch
720X, 720D, 7010TX, 750XP

Arista NDR 솔루션 특징 – VI (DMF 솔루션 연동)

DANZ Forensics Exchange (DFX)

네트워크 가시성

Threat Detection & Response

DANZ Monitoring Fabric (DMF)

Visibility Fabric
(NPB)

Recorder Node
Service Node

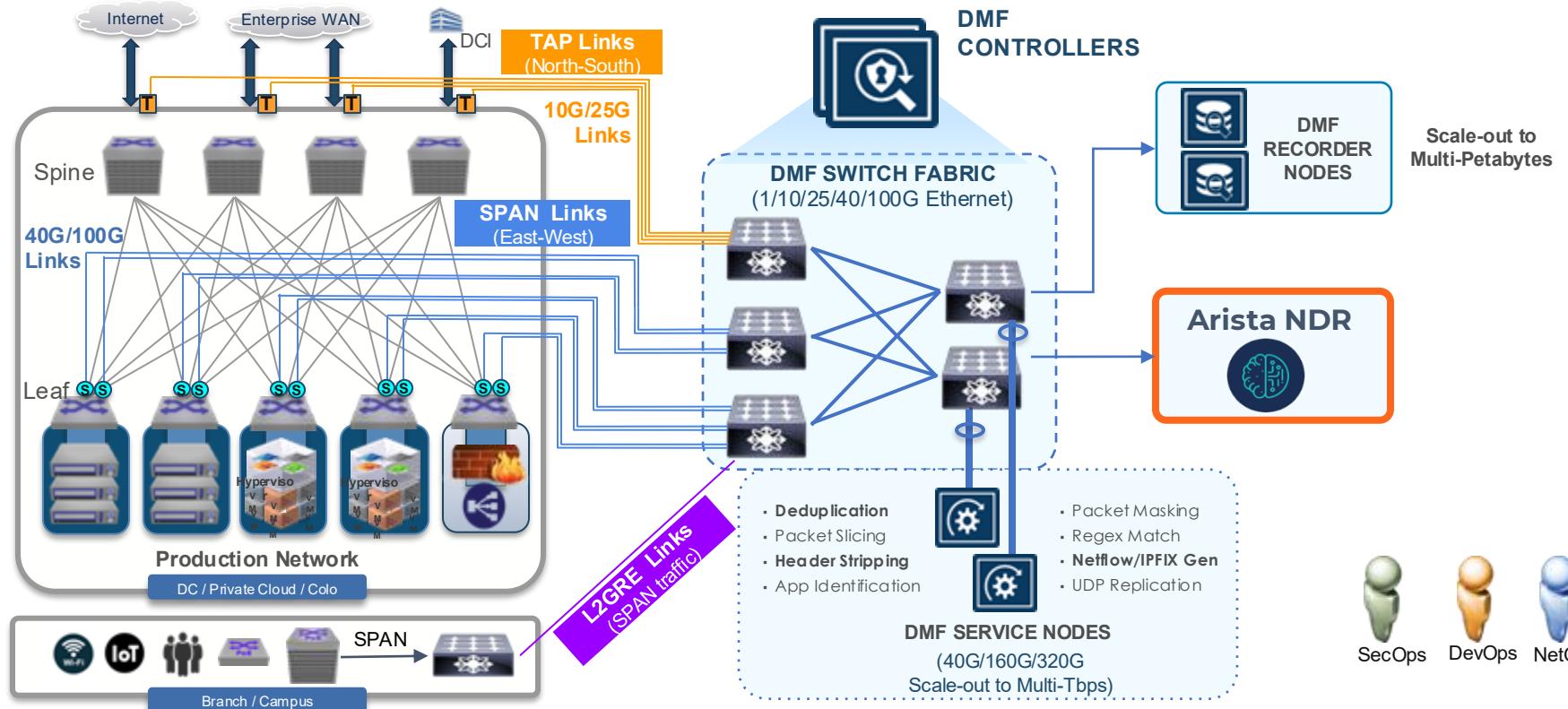


NDR

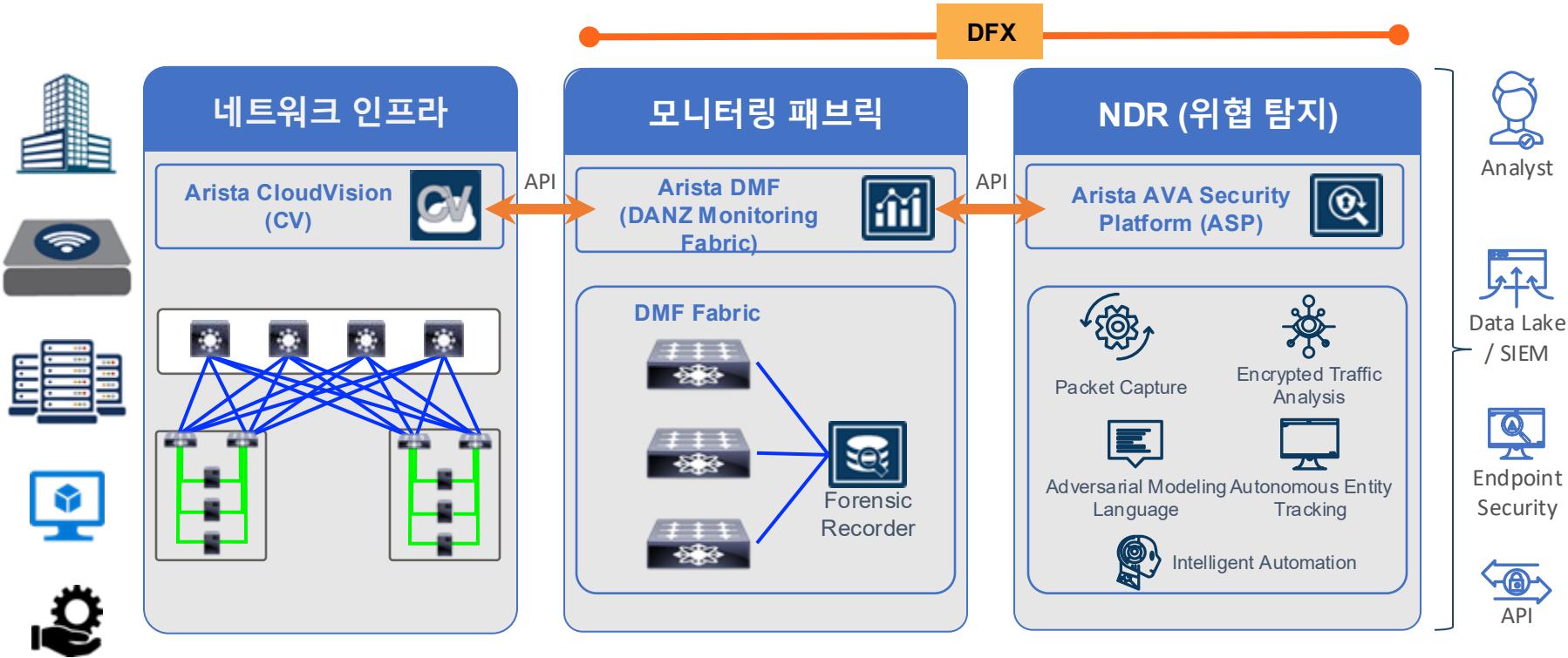
Sensors

Nucleus

Arista NDR 솔루션 특징 – VI (DMF 솔루션 연동)



Arista NDR 솔루션 특징 – VI (DMF 솔루션 연동)



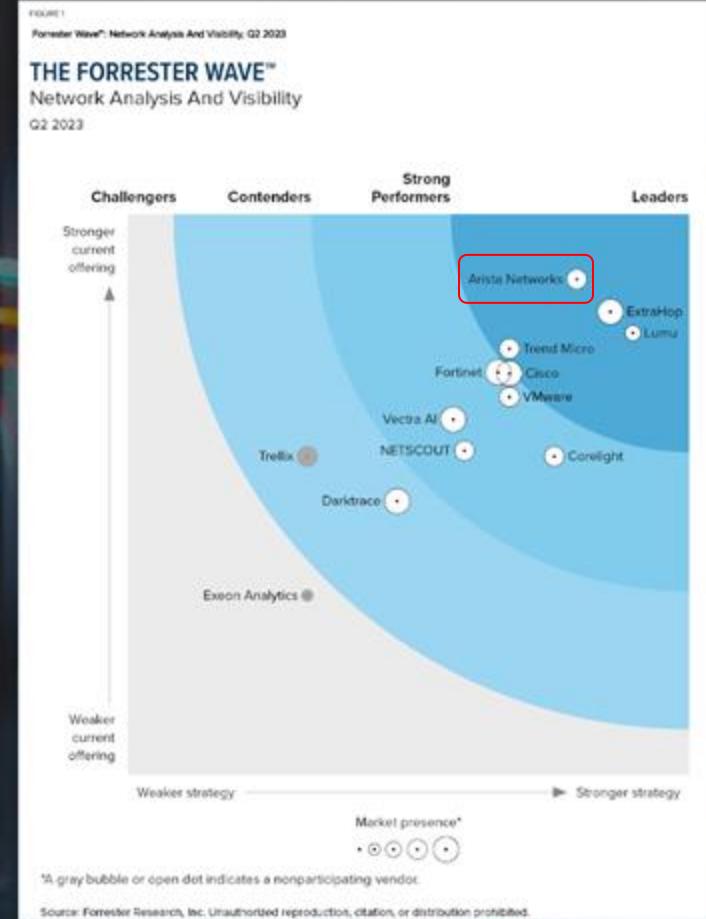
Arista Security Alliances

Category	Joint Value Proposition	Key Partners
Endpoint Security	<ul style="list-style-type: none">Speed up investigations and response with integrated xDRGain situational awareness across managed & unmanaged devices	Carbon Black.  Microsoft  Trellix   
Security Information and Event Management (SIEM)	<ul style="list-style-type: none">Optimize response workflows with high-fidelity detectionDeliver rich network context to other SIEM data sources	    
Ticketing, Orchestration & Automation	<ul style="list-style-type: none">Automate investigation, response and forensic tasksEstablish standardized workflows using context from the network	  
Perimeter Security	<ul style="list-style-type: none">Contain threats by blocking command and control/data exfiltration in real-timeProtect the entire enterprise by blocking access to attacker infrastructure	  
Cloud & SaaS	<ul style="list-style-type: none">Enable security monitoring of cloud workloadsGain insights into threats that spread laterally from traditional to cloud infrastructure	   

Fully documented and supported API/webhooks for additional integrations

Arista Named a Leader in The Forrester Wave™ : Network Analysis and Visibility, Q2 2023

[Get the Wave Report Now!](#)



Case Study

CASE STUDY 1 : 랜섬웨어 확산 방어

Industry : Manufacturing

Challenge

- 내부 중요 정보를 대상으로 랜섬웨어 공격 시도
- 파일 암호화로 인한 피해 발생 이후 단말에서 공격 탐지 확인

Ransomware attacks were only detected on the endpoint after the encryption event.

ARISTA NDR 도입 후

최초 감염 장치를 찾아냄과 동시에 정찰, 내부전파 등의
후속 행위를 탐지하여 랜섬웨어 확산을 조기 차단함

Identified patient 0 and early warning signs including reconnaissance and lateral movement to prevent spread across facilities

Ransomware Attack Forensic Summary Timeline



CASE STUDY 2 : Lateral Movement 탐지

- 공격자가 하나의 시스템을 장악한 후 내부 네트워크를 가로질러 다른 시스템으로 이동하려는 행동을 탐지

1. 행위 이상 탐지

- 평소에 접속하지 않던 장비 간의 SMB, RDP, WinRM, LDAP 등의 트래픽 발생 여부 분석
(사례: 일반적으로 연결되지 않던 서버간 RDP 세션이 갑자기 발생)

2. 세션 상관 관계 분석

- 동일 소스에서 순차적으로 여러 내부 IP에 접근 시도 포착 (동시다발적인 포트, 프로토콜 사용)
(사례: 같은 Source에서 다양한 Destination으로 SMB 통신 포착)

3. 인증 이벤트 이상 탐지

- 평소 사용하지 않던 시스템에 대해 Kerberos, NTLM 인증 시도 (특히 실패 포함)
(사례: 공격자가 도메인 사용자 권한으로 다른 시스템에 로그인 시도)

4. 비정상 스캔 탐지

- ARP, NetBIOS, ICMP, LDAP 쿼리 등으로 내부 정보 수집 패턴 탐지
(사례: 공격자가 내부 자산을 식별하기 위해 Broadcast 요청 시도)

5. 동시다발 접근 패턴 탐지

- 하나의 Host로 부터 매우 짧은 시간 내에 여러 자산에 접근하는 행위 탐지 (비정상적 패턴)
(사례: 하나의 감염된 PC에서 수십대의 서버로 동시에 SMB 연결 시도)



ARISTA

Zero Trust Security

Thank You!

www.arista.com

