쇼미더 '네트워크' 시즌 2

네트워크를 이해하는 새로운 방법

19.09.30 / 지니언스

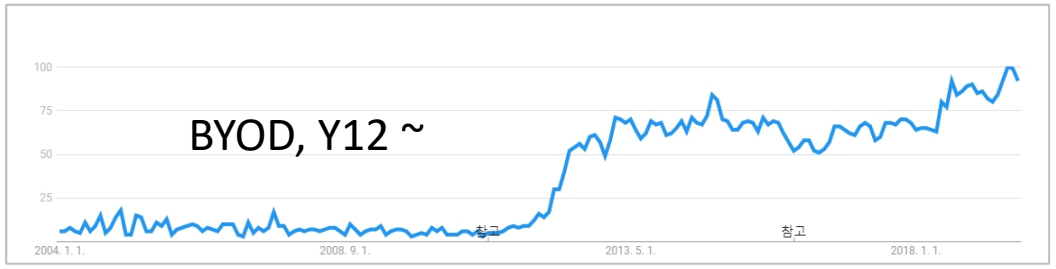
'501억' 개

(50,100,000,000)

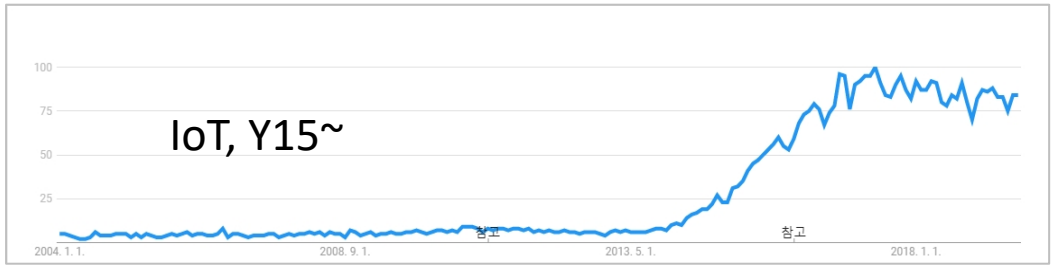
2020년 네트워크 상의 단말의 수 (by Cisco)

'BYOD' 와 'IoT'

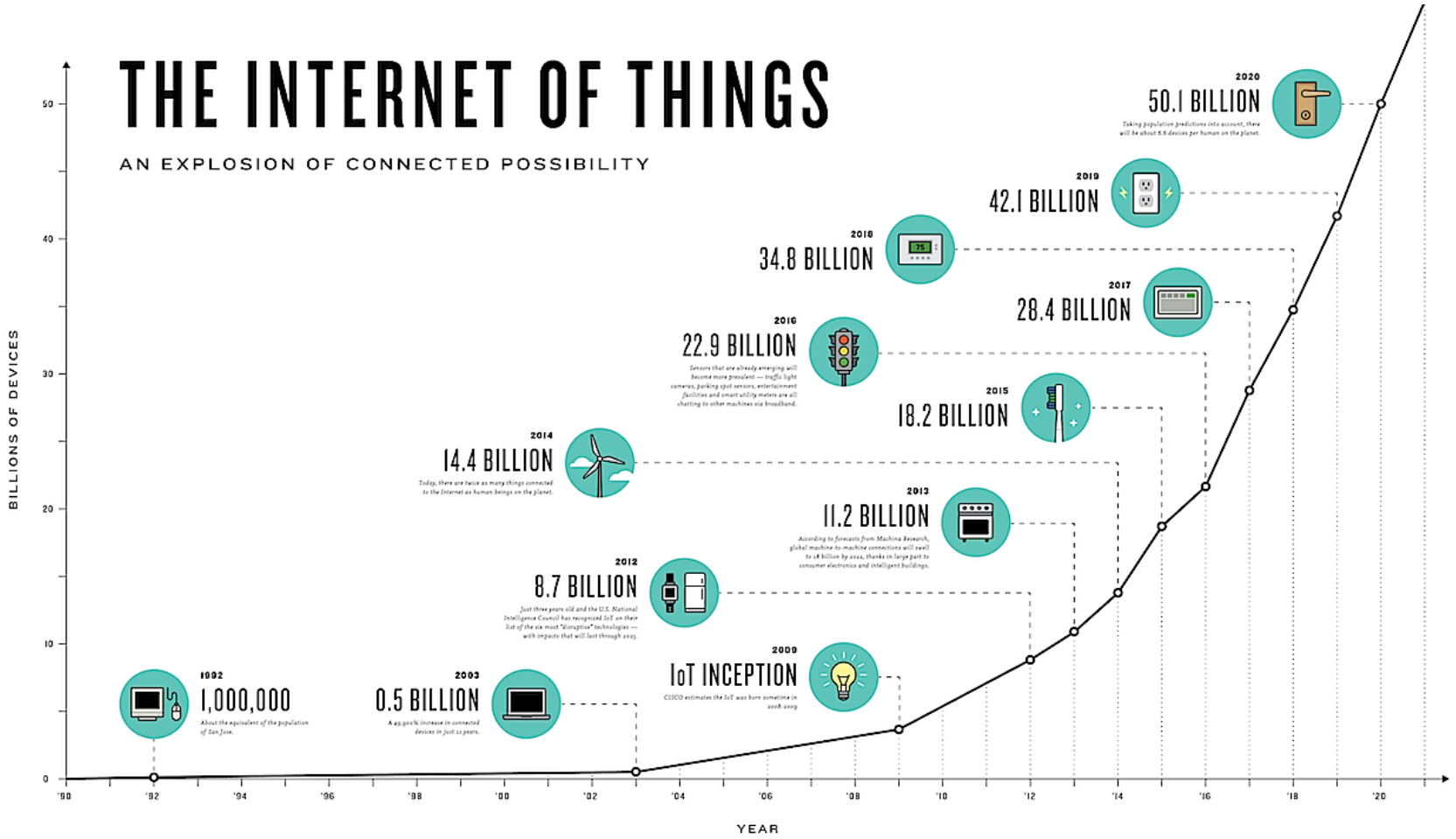
Bring Your Own Device



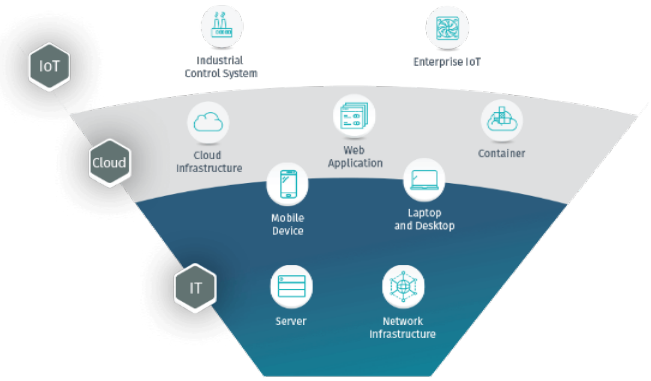
Internet of Things

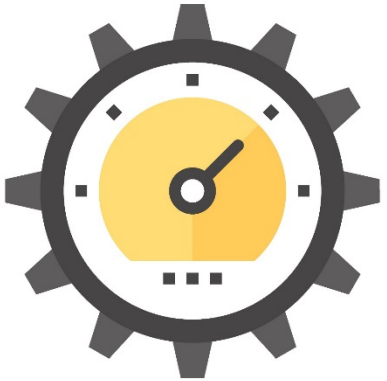


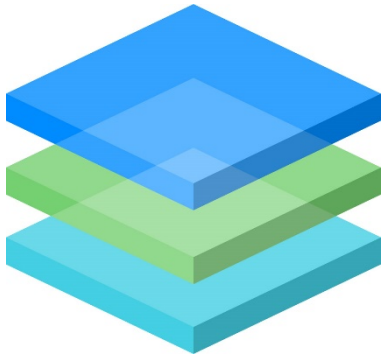
'IoT 단말' 폭발적 증가


THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY
BILLIONS OF DEVICES
YEAR
1992
1,000,000
About the equivalent of the population of San Jose.
2003
0.5 BILLION
A 49,900% increase in connected devices in just 11 years.
2009
IoT INCEPTION
CISCO estimates the IoT was born sometime in 2008-2009.
2012
8.7 BILLION
Just three years old and the U.S. National Intelligence Council has recognized IoT on their list of the six most "disruptive" technologies — with impacts that will last through 2025.
2013
11.2 BILLION
According to forecasts from Machina Research, global machine-to-machine connections will swell to 18 billion by 2024, thanks in large part to consumer electronics and intelligent buildings.
2014
14.4 BILLION
Today, there are twice as many things connected to the Internet as human beings on the planet.
2015
18.2 BILLION
2016
22.9 BILLION
Sensors that are already emerging will become more prevalent — traffic light cameras, parking spot sensors, entertainment facilities and smart utility meters are all chatting to other machines via broadband.
2017
28.4 BILLION
2018
34.8 BILLION
2019
42.1 BILLION
2020
50.1 BILLION
Taking population predictions into account, there will be about 6.6 devices per human on the planet.

'IoT 위협' 증가







Attack Surface

Resource Limitation

Open Platform

Is a Real?

The Jeep Hack (2015)

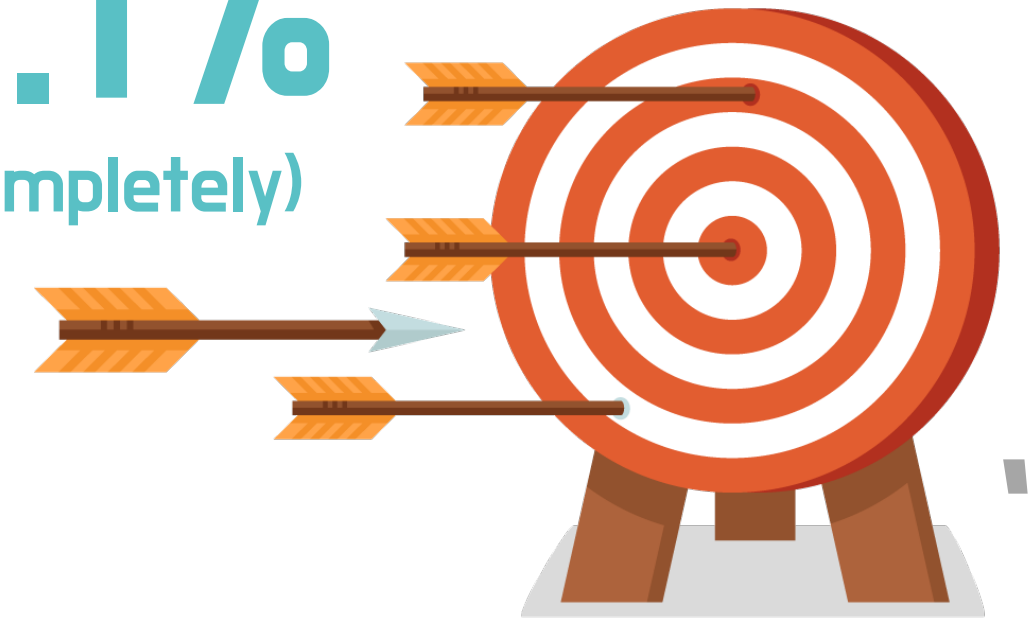
- ✓ 제조사 텔레메틱스 시스템 원격 취약점 발견
- ✓ 모바일 네트워크 연결 후 자동차 권한 획득
- ✓ 헤드유닛(라디오/네비게이션 등) 접근

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer (2018)

- ✓ 수족관 자동 온도조절장치를 해킹
- ✓ 카지노 서버에 침투
- ✓ 방문객 데이터를 절취

9.1%

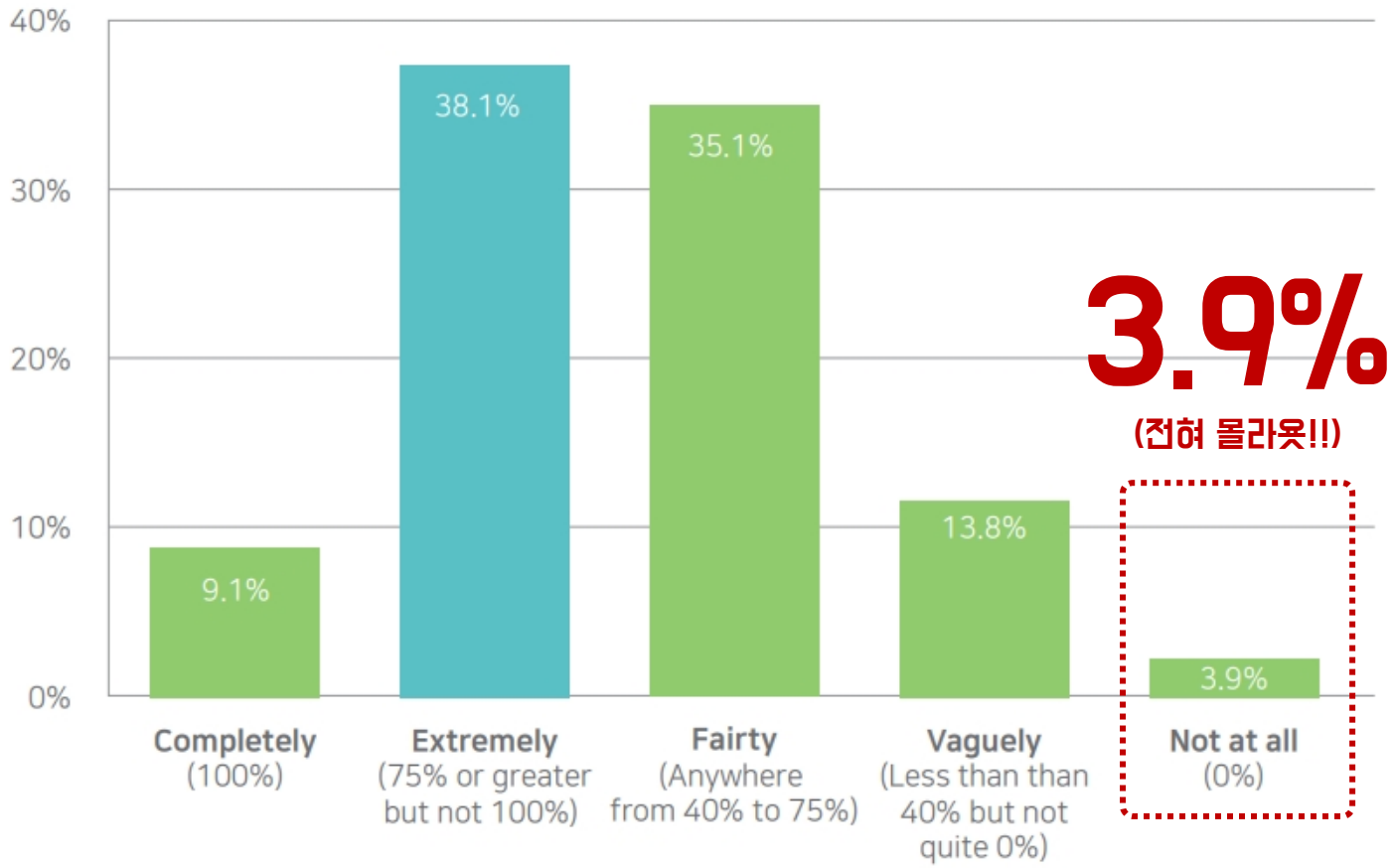
(Completely)



'Y12

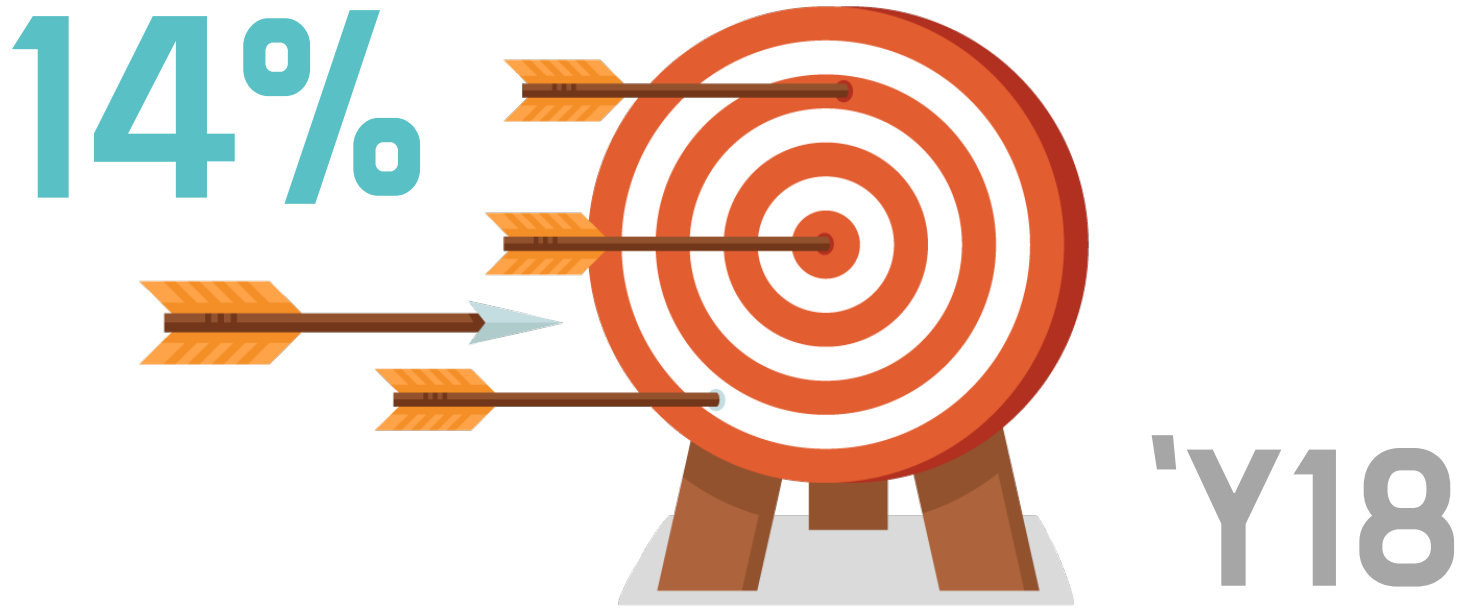
'State of Mobile Device Awareness'

자료: SANS Mobile/BYOD Security Survey 2012



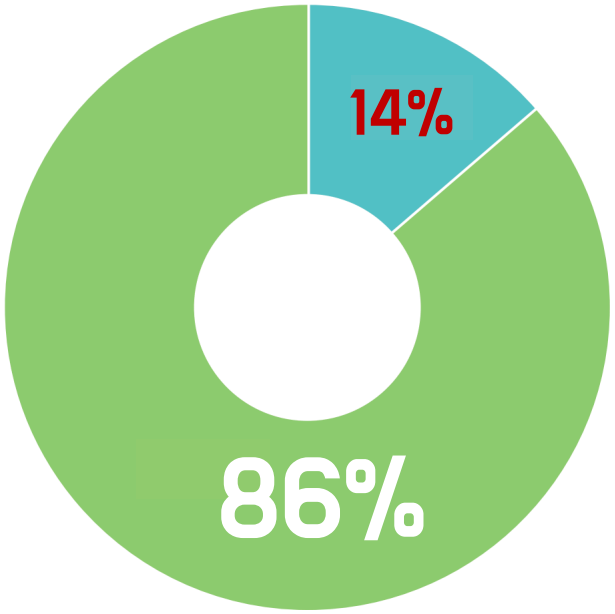
'State of Mobile Device Awareness'

자료: SANS Mobile/BYOD Security Survey 2012

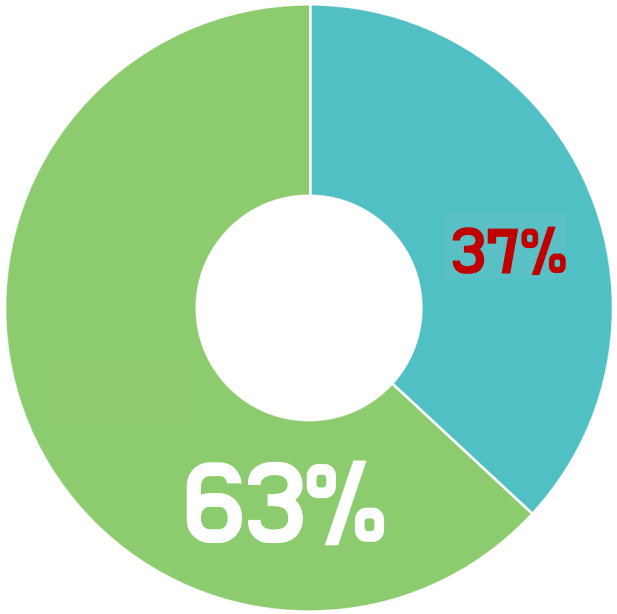


'Lack of IoT Security Awareness'

자료: Trendmicro Research Finds Major Lack of IoT Security Awareness, Nov. 2018



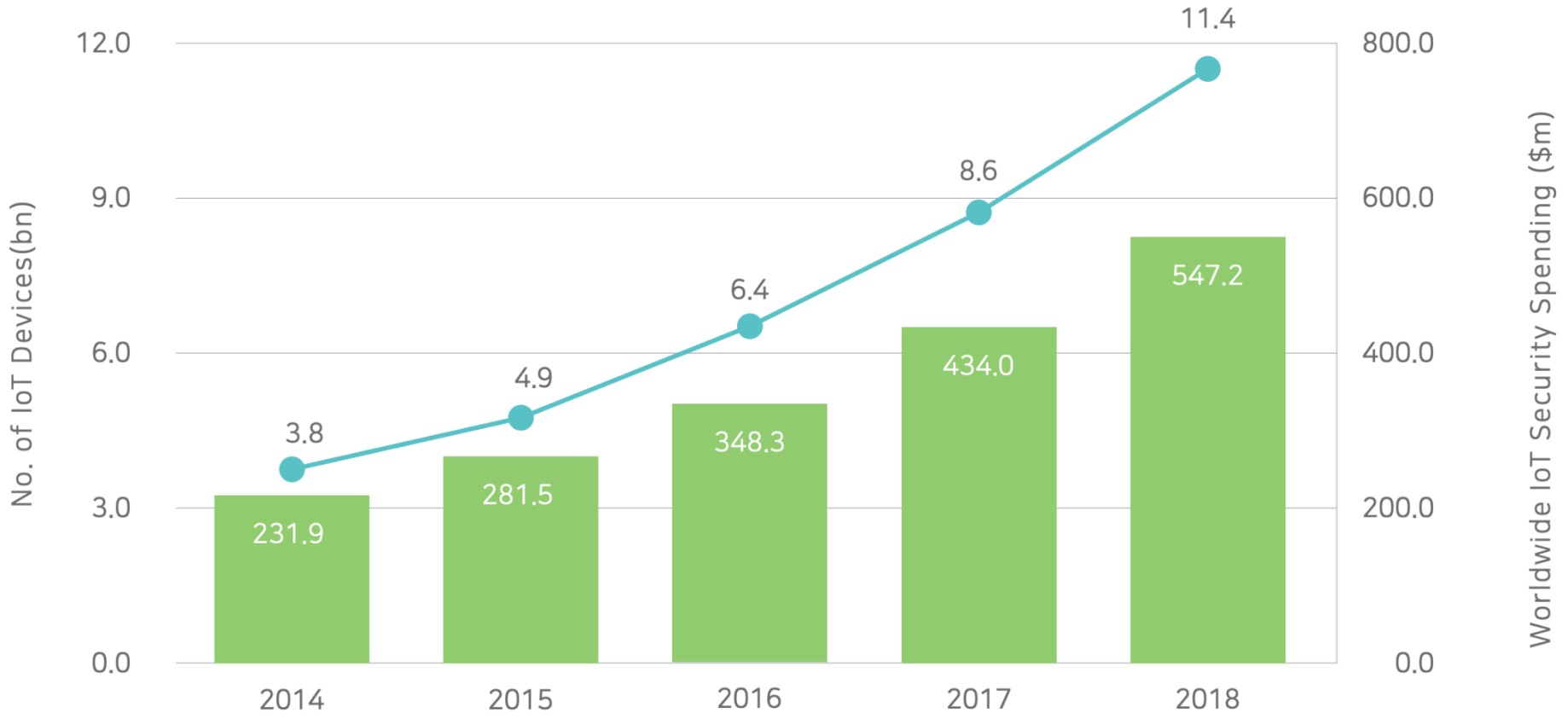
IoT 위협을 (완벽히) 인지
그렇지 않음



IoT 보안 요구사항을 인지
그렇지 않음

자료: Trendmicro Research Finds Major Lack of IoT Security Awareness, Nov. 2018

Spending vs Growth



자료: Gartner, TELECOM TV, Various

By 2020

25%

of Enterprise attacks will involve IoT

10%

of IT Security budgets allocate to IoT

50%

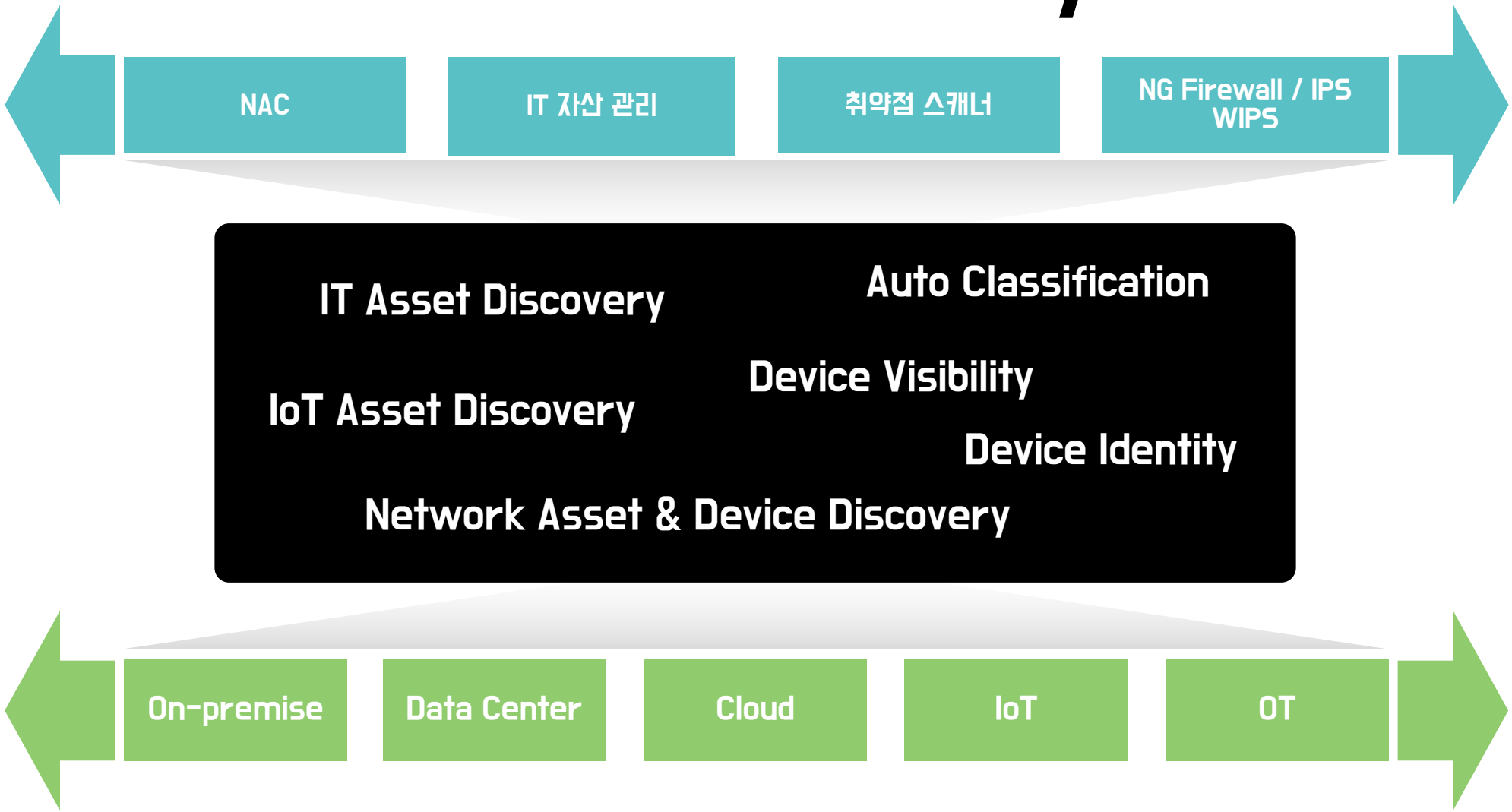
of IoT implementations will use Cloud security

자료: Gartner, TELECOM TV, Various

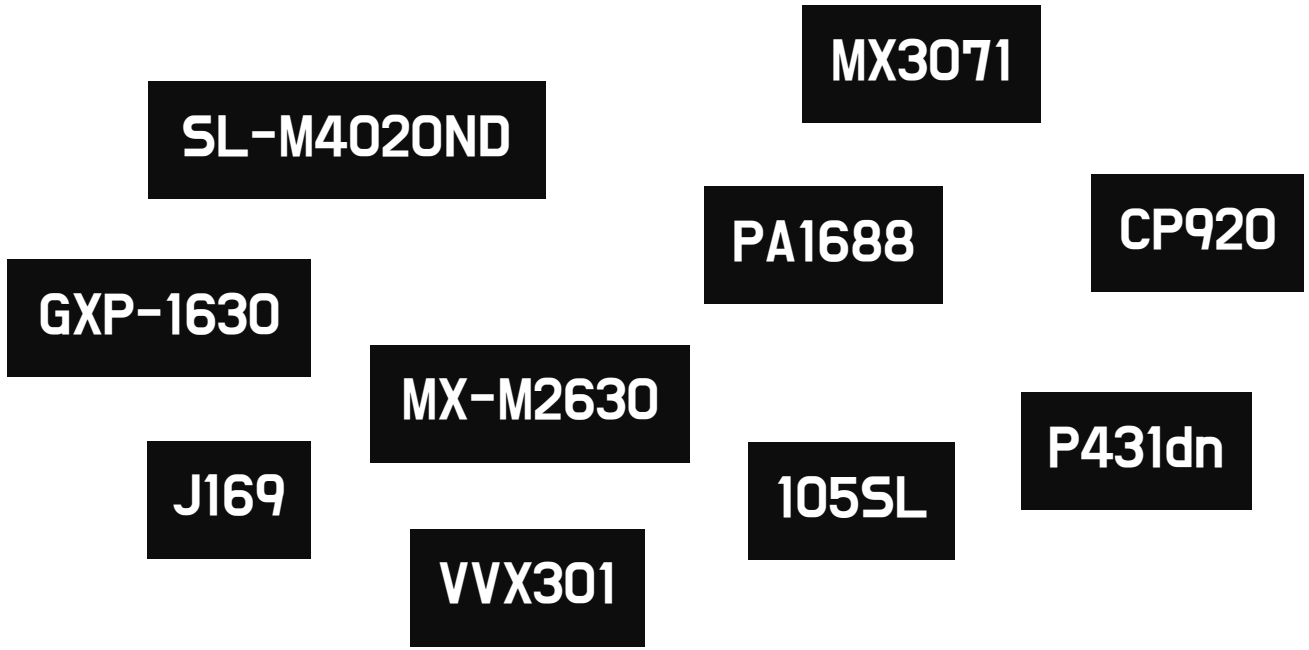
It's the Visibility, stupid

네트워크에 존재하는 '단말 가시성' 확보가 중요

가시성(Visibility)



가시성(Visibility) v1.0



'같은 종류'로 구분해 보세요.

가시성(Visibility) v1.0

'같은 종류'로 구분해 보세요. 다르죠?

Human Friendly

MX3071

P431dn

SL-M4020ND

105SL

MX-M2630

Printer

J169

PA1688

GXP-1630

VVX301

CP920

VOIP Phone

'Resolution' (해상력, 분해능)

192.168.50.24 I 40:8D:5C:1A:D0:E4 I

192.168.50.24 I 40:8D:5C:1A:D0:E4 I Desktop I

192.168.50.24 I 40:8D:5C:1A:D0:E4 I Desktop I Ubuntu Linux I

192.168.50.24 I 40:8D:5C:1A:D0:E4 I Desktop I Ubuntu Linux I Scott I

192.168.50.24 I 40:8D:5C:1A:D0:E4 I Desktop I Ubuntu Linux I Scott I Boston

The more, the better

Visibility Techniques

Active

To Node

- Scanning
- SNMP Request
- Agent Based Inspection
- Banner (FTP, Telnet…)
- HTTP user-agent
- Open Port
- UPnP
- ……

To Others(SVA*)

- Infrastructure Polling
- AP Controller Integration (Meraki, Cisco ACI…)
- Cloud Integration (AWS, AZURE)
- LDAP
- RESTful API
- Orchestrations(EDR…)

Passive

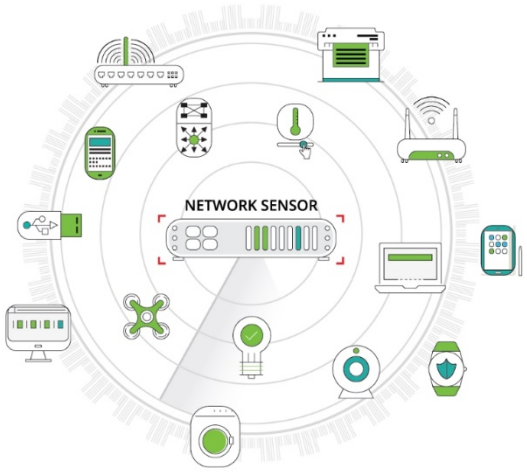
- SNMP Trap
- DHCP request
- HTTP user-agent
- ICS OT (Modbus..)
- Netflow
- RADIUS
- MAC OUI
- ……..

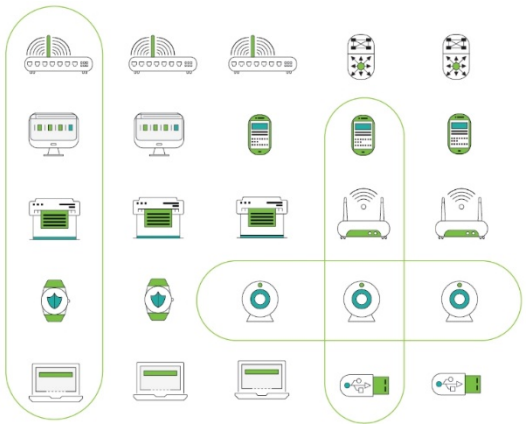
* SVA: Scan-less Vulnerability Assessment

SVA. Why?(Scan-less Vulnerability Assessment)

NAC(Network Access Control)

Illuminate Network → **Tidy Up Network** → **Control Network**



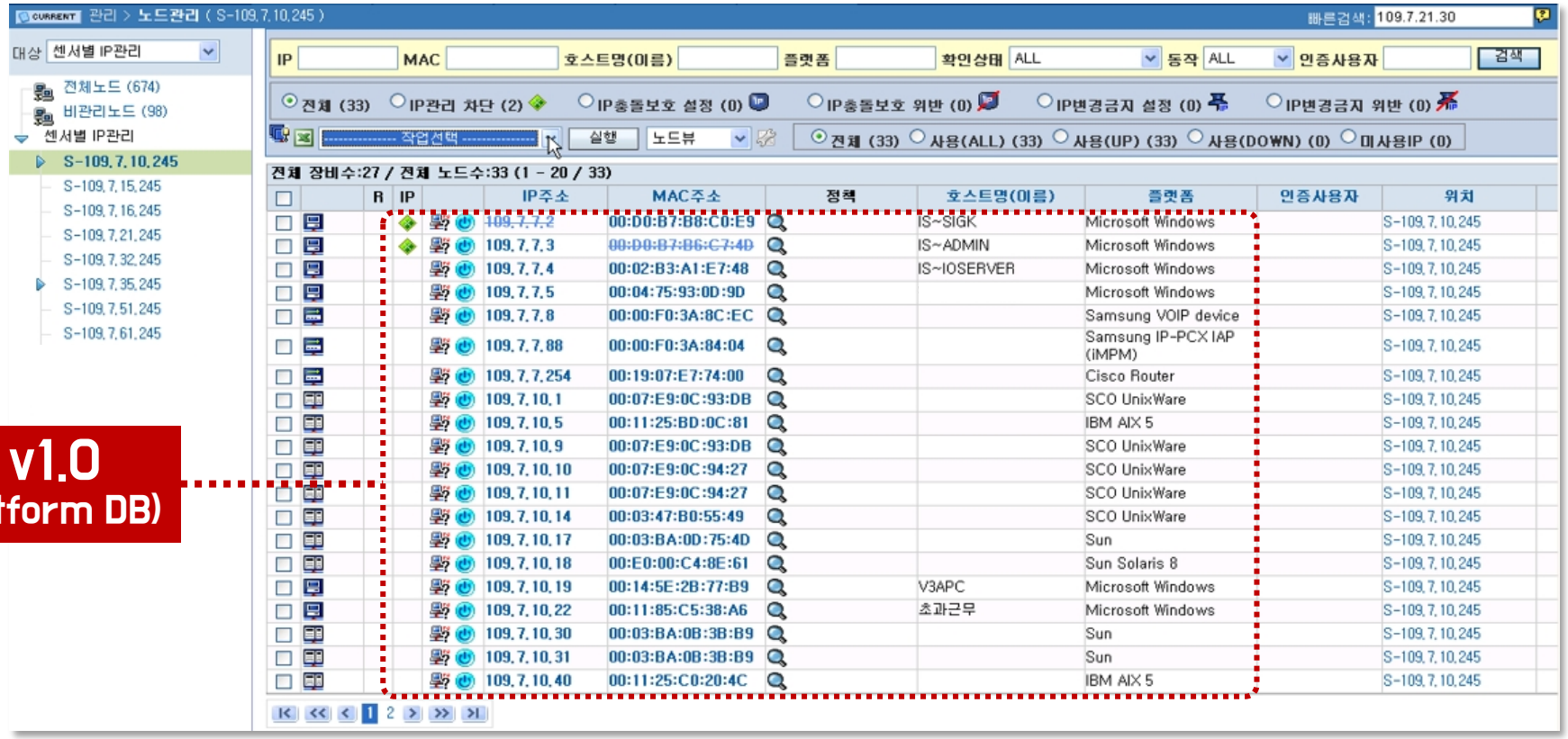


Detect / Identified Node

Classify / Group Node

Policy Enforced Node

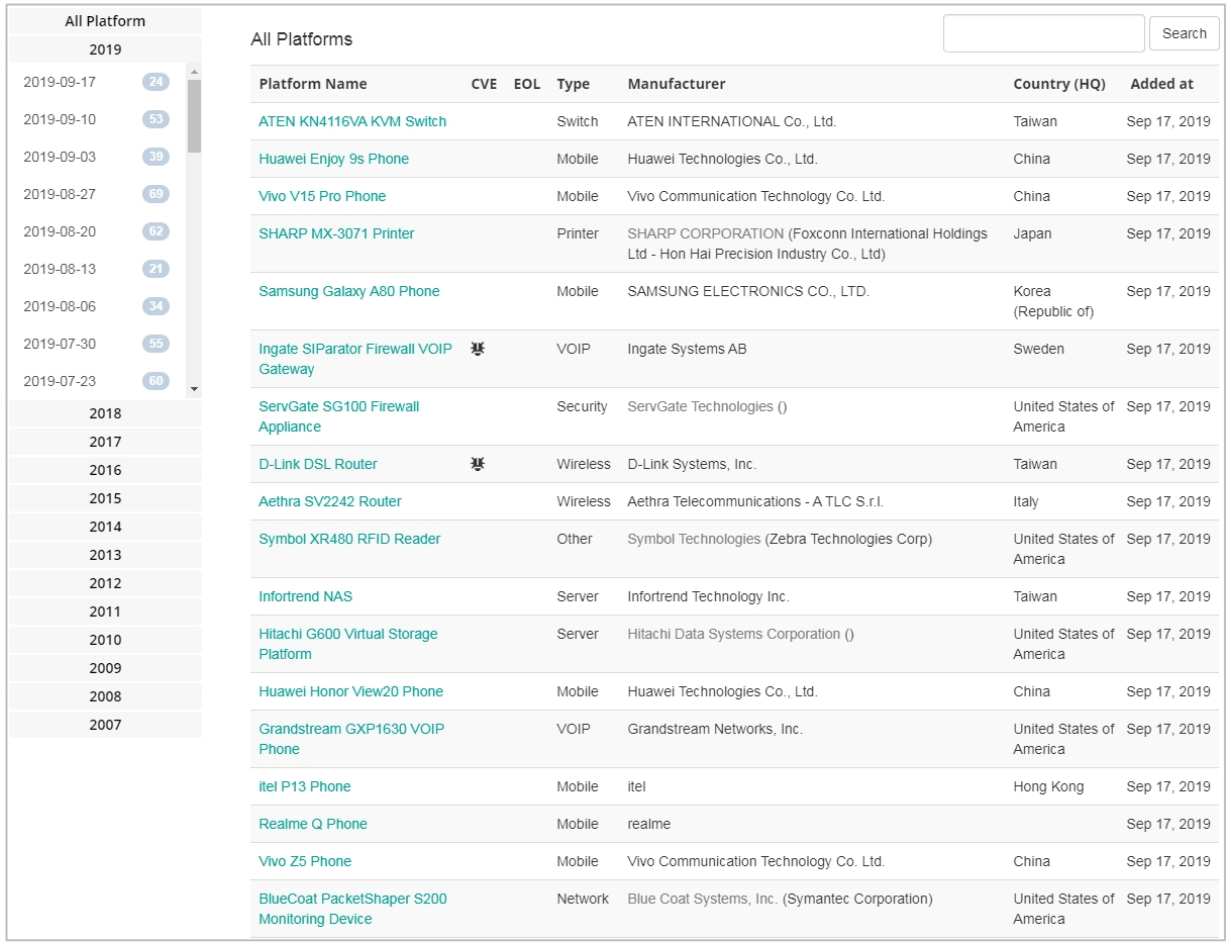
NAC(Network Access Control)



GPDB v1.0
(Genian Platform DB)

- IP 관리 어려움
- 단말 관리 어려움
- 관리 항목 증가

DPI(Device Platform Intelligence)



All Platform

2019

2019-09-17 24
2019-09-10 53
2019-09-03 39
2019-08-27 69
2019-08-20 62
2019-08-13 21
2019-08-06 34
2019-07-30 55
2019-07-23 60

2018
2017
2016
2015
2014
2013
2012
2011
2010
2009
2008
2007

All Platforms

Search

Platform Name	CVE	EOL	Type	Manufacturer	Country (HQ)	Added at
ATEN KN4116VA KVM Switch			Switch	ATEN INTERNATIONAL Co., Ltd.	Taiwan	Sep 17, 2019
Huawei Enjoy 9s Phone			Mobile	Huawei Technologies Co., Ltd.	China	Sep 17, 2019
Vivo V15 Pro Phone			Mobile	Vivo Communication Technology Co. Ltd.	China	Sep 17, 2019
SHARP MX-3071 Printer			Printer	SHARP CORPORATION (Foxconn International Holdings Ltd - Hon Hai Precision Industry Co., Ltd)	Japan	Sep 17, 2019
Samsung Galaxy A80 Phone			Mobile	SAMSUNG ELECTRONICS CO., LTD.	Korea (Republic of)	Sep 17, 2019
Ingate SIParator Firewall VOIP Gateway	☣		VOIP	Ingate Systems AB	Sweden	Sep 17, 2019
ServGate SG100 Firewall Appliance			Security	ServGate Technologies ()	United States of America	Sep 17, 2019
D-Link DSL Router	☣		Wireless	D-Link Systems, Inc.	Taiwan	Sep 17, 2019
Aethra SV2242 Router			Wireless	Aethra Telecommunications - A TLC S.r.l.	Italy	Sep 17, 2019
Symbol XR480 RFID Reader			Other	Symbol Technologies (Zebra Technologies Corp)	United States of America	Sep 17, 2019
Infortrend NAS			Server	Infortrend Technology Inc.	Taiwan	Sep 17, 2019
Hitachi G600 Virtual Storage Platform			Server	Hitachi Data Systems Corporation ()	United States of America	Sep 17, 2019
Huawei Honor View20 Phone			Mobile	Huawei Technologies Co., Ltd.	China	Sep 17, 2019
Grandstream GXP1630 VOIP Phone			VOIP	Grandstream Networks, Inc.	United States of America	Sep 17, 2019
itel P13 Phone			Mobile	itel	Hong Kong	Sep 17, 2019
Realme Q Phone			Mobile	realme		Sep 17, 2019
Vivo Z5 Phone			Mobile	Vivo Communication Technology Co. Ltd.	China	Sep 17, 2019
BlueCoat PacketShaper S200 Monitoring Device			Network	Blue Coat Systems, Inc. (Symantec Corporation)	United States of America	Sep 17, 2019

- GPDB v2.0
- Over 10 Years
- 30,000+ Rules
- L2 & L3 Fingerprint

DPI tells you…

IP Camera

Device
(식별정보)

- IP / MAC
- Platform Name
- Platform Type
- Platform OS
- Connection Type
- Image

Business
(확장정보)

- Manufacturer
- Platform URL
- End of Life
- End of Support
- Out of Business
- Acquisition

Vulnerability
(취약성정보)

- CVE for Platform / Manufacturer
- Severity
- Description
- News (plan)

DPI. It's Real

Platform's Common Vulnerabilities and Exposures (CVE)

CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2017-10796 07/02/2017	MEDIUM	LOW	On TP-Link NC250 devices with firmware through 1.2.1 build 170515, anyone can view video and audio without authentication via an rtsp://admin@yourip:554/h264_hd.sdp URL.

« < 1 > »

Manufacturer's Common Vulnerabilities and Exposures (CVE)

CVE-ID	Severity v3.0	Severity v2.0	Descript
CVE-2019-13268 08/27/2019	HIGH	MEDIUM	TP-Link Arch a guest netw packets, bet issue an ARI requests des factor, one m
CVE-2019-13267 08/27/2019	HIGH	MEDIUM	TP-Link Arch a guest netw network, the an IGMP Me transferred v
CVE-2019-13266 08/27/2019	HIGH	MEDIUM	TP-Link Arch a guest netw ID field. Follo that the route DHCP Requ
CVE-2019-15060 08/22/2019	HIGH	MEDIUM	The tracerou code executi
CVE-2019-12104 08/14/2019	HIGH	HIGH	The web-bas authenticatio

TP-Link NC250 WiFi Camera

Platform Information	https://www.tp-link.com/us/home-networking/cloud-camera/tl-nc250/#specifications
Search Engine	Search on Google
End of Sales	Yes more info
End of Support	Yes more info
Wired Connection	Yes
Wireless Connection	Yes
Fingerprinting Source	HTTP NIC VENDOR
Added at	May 28, 2019
Manufacturer Name	TP-Link Technologies Co., Ltd
Homepage	http://www.tp-link.com/us/
Headquarters	China
Business Status	Ongoing

Suggest Update

DPI Coverage

IT(OA)


Mobile

Desktop


Wireless


Laptop


Server


Switch

IoT


Gateway


IP Camera


Meter


Speaker

Sensor


Monitor

Industrial IoT


Controller


Panel


Building Adapter


Industrial Printer


PLC


HMI

DPI Fingerprint Source

Active

Layer 2

- MAC OUI / Vendor
- DHCP
- Hostname (netbios-ns)
- SMB
- uPNP
- HPSLP / BJNP / CUPS
- SIP
- CDP / LLDP

Layer 3

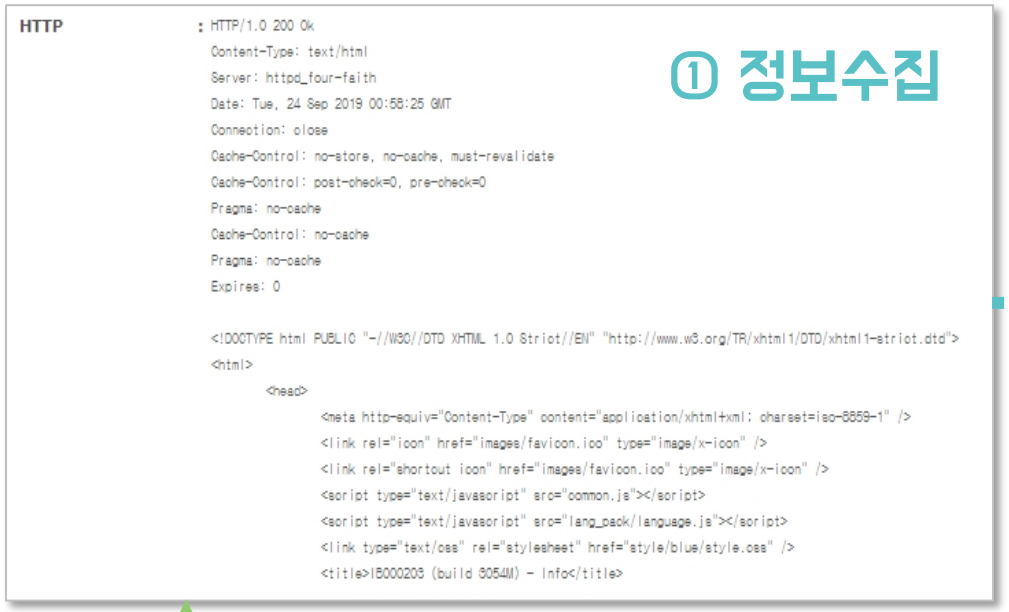
- Telnet
- FTP
- SNMP OID / Desc.
- Open Port
- HTTP(S) User-agent
- HTTP Page
- HTTP Certificate
- ModBus / BACnet

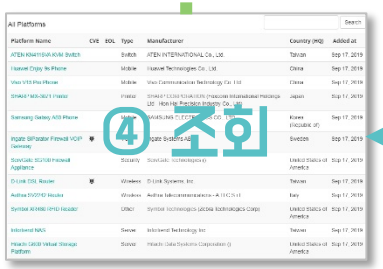
Passive

- FTP
- HTTP(S) User-agent
- SMTP
- DHCP
- MAC OUI / Vendor

지원예정

DPI Work Flow

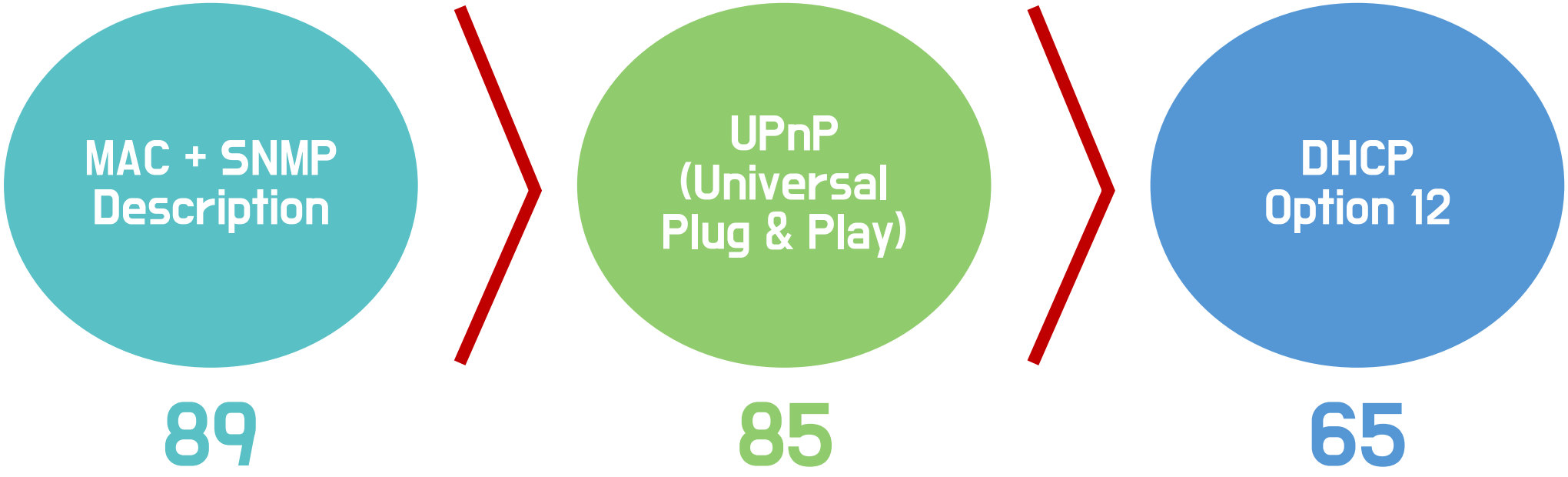




Matches	Node Type	Manufacturer	Platform Name	OS	Connection Type	Trust Score	Rules
134	@VOIP	MOIMSTONE	Moimstone VOIP Phone	Other	Indeterminable	64	VENDOR DHCP
874	@VOIP	MOIMSTONE	Moimstone VOIP Phone	Other	Indeterminable	50	VENDOR
104	@Server	The Linux Foundation	Linux	Generic Linux	Indeterminable	47	SNMPDescription
40	@VOIP	MOIMSTONE	Moimstone VOIP Phone	Other	Indeterminable	45	DHCP

③ 규칙생성

Trust Score



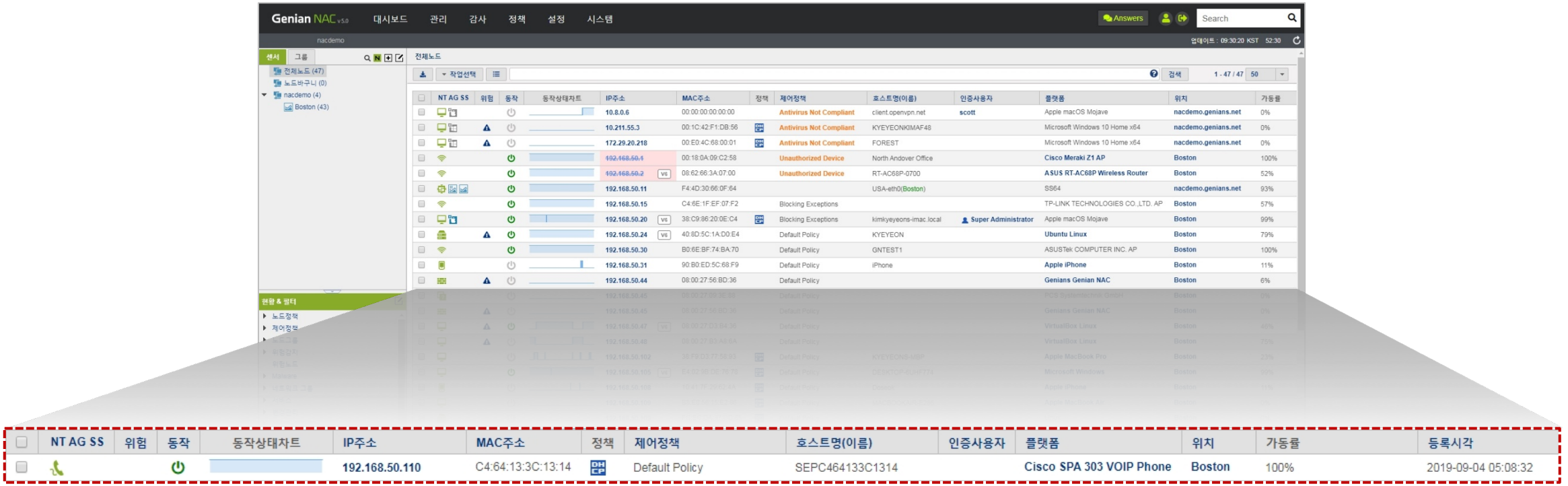
오랜 경험과 시행착오의 결과

Comparison. DPI는 이미 글로벌

Device Resolution Vs Coverage

자료: 비교의 수준은 Genians 자체 평가 결과임

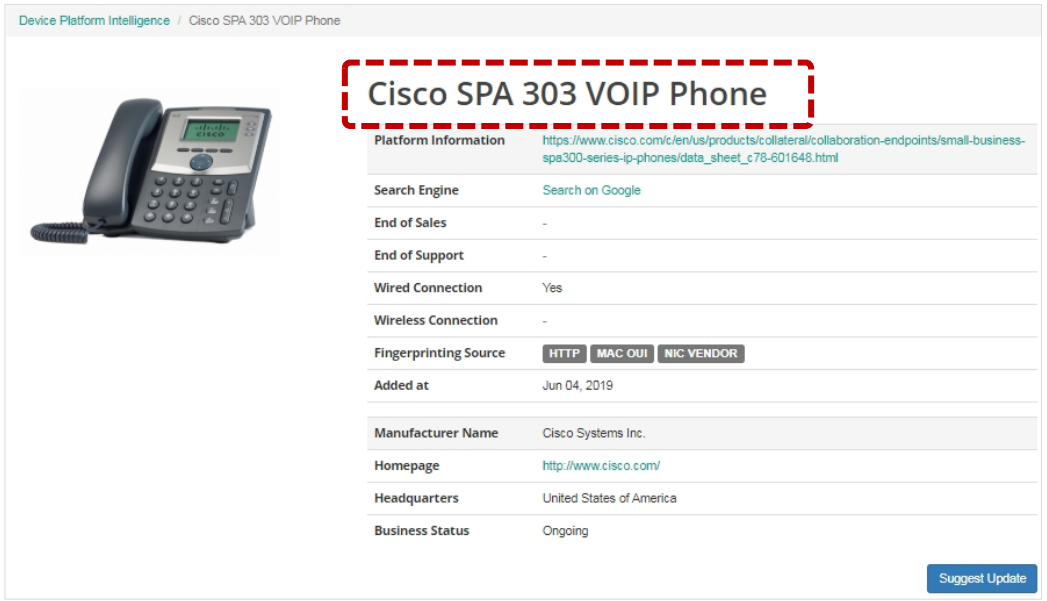
DPI in Genian NAC

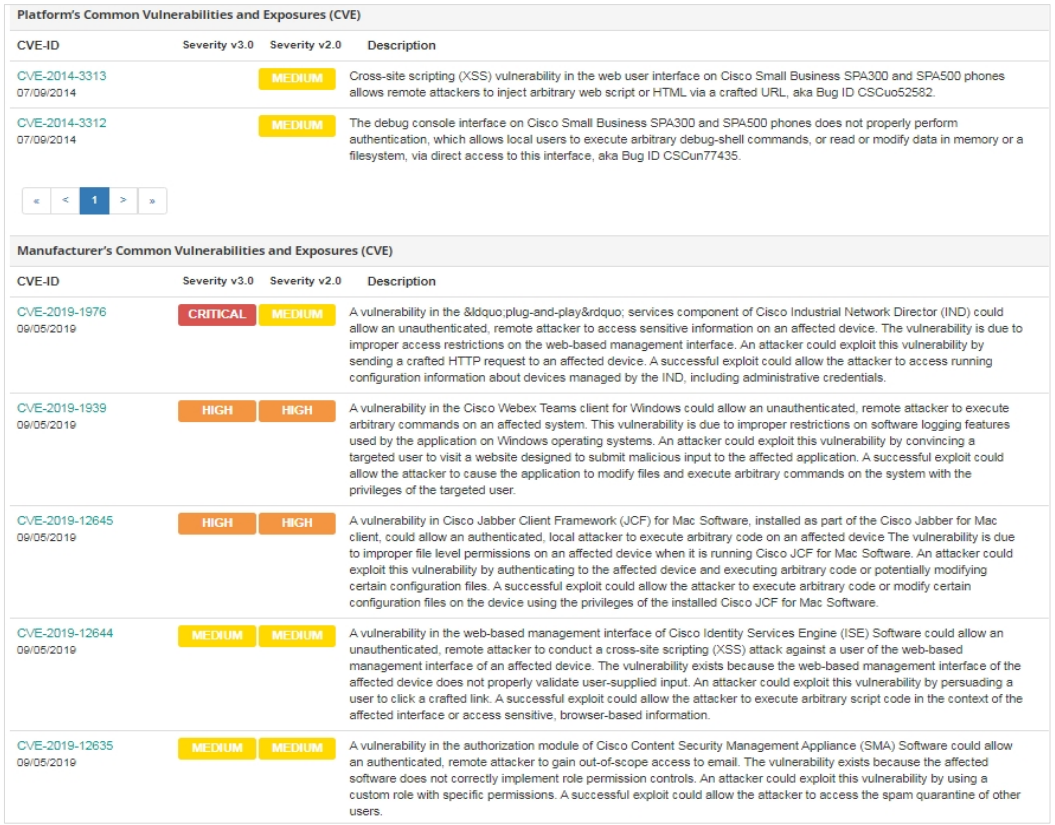


NT AG SS	위험	동작	동작상태차트	IP주소	MAC주소	정책	제어정책	호스트명(이름)	인증사용자	플랫폼	위치	가동률	등록시각
				192.168.50.110	C4:64:13:3C:13:14		Default Policy	SEPC464133C1314		Cisco SPA 303 VOIP Phone	Boston	100%	2019-09-04 05:08:32

Node Identity(식별정보)

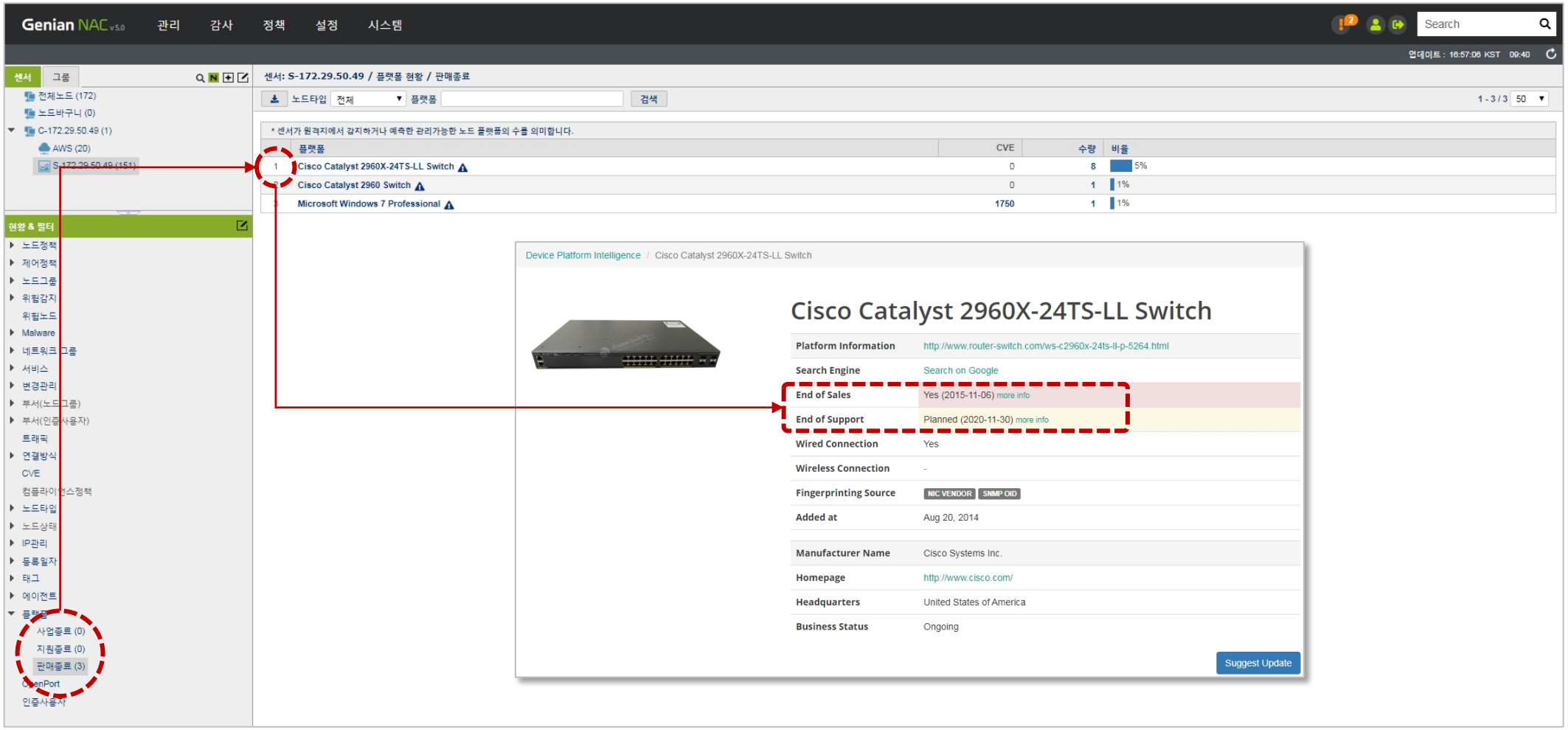
DPI in Genian NAC





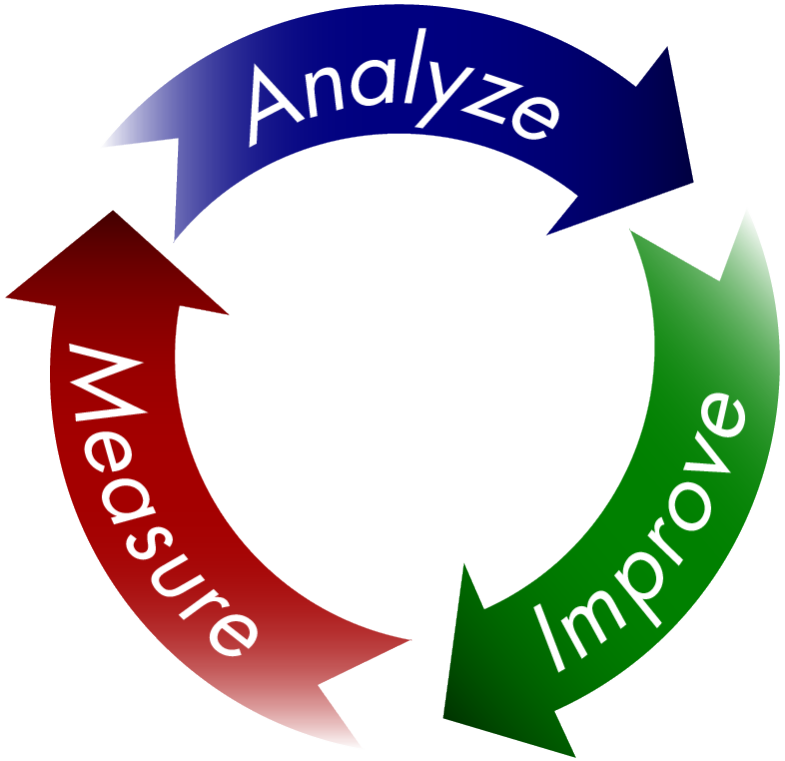
Node Business(확장) & Vulnerability(취약성)

DPI in Genian NAC



Value of DPI

- Granular Visibility
- Lifecycle Mgmt.
- Vulnerability Mgmt.
  (Scan-less Vulnerability Assessment)



Granular Visibility

Device Fingerprinting

- Device Platform

Device Vulnerability

- CVE for Platform / Manufacturer
- Security News (Coming Soon)

Device Information

- Platform Name
- Platform Type
- Platform OS
- Platform URL
- Connection Type
- Manufacturer

Business Information

- EOL(End of Life)
- EOS(End of Support)
- Acquisition
- Out of Business

Lifecycle Mgmt.

Windows 7 지원이 2020년 1월 14일자로 종료됩니다.

적용 대상: Windows 7

Windows 7 지원 수명 주기

Microsoft는 2009년 10월 22일에 Windows 7을 출시하면서 10년 간 제품 지원을 제공하겠다고 약속한 바 있습니다. 10년의 지원 기간이 종료되면 Microsoft는 최신 기술과 새로운 환경을 지원하는 데 투자를 집중할 수 있도록 Windows 7 지원을 중단할 생각입니다. Windows 7의 지원 종료일은 2020년 1월 14일입니다. 그 이후에는 PC 보호를 돕기 위한 기술 지원 및 Windows 업데이트를 통한 소프트웨어 업데이트가 더 이상 제공되지 않을 것입니다. 더 이상 제공되지 않는 서비스나 지원이 필요한 상황이 발생하지 않도록 2020년 1월 전까지는 Windows 10으로 전환하는 것이 좋습니다.

모두 표시

- 지원이 종료되면 어떻게 되나요?
- 어떻게 해야 하나요?
- 기존 PC를 Windows 10으로 업그레이드할 수 있나요?
- Windows 10을 무료로 업그레이드하려면 어떻게 하나요?
- Windows 7을 계속 사용하면 어떻게 되나요?
- 2020년 1월 14일 이후에도 여전히 Windows 7을 정품 인증할 수 있나요?

  지원 종료일 이후에도 여전히 Windows 7을 설치 및 정품 인증할 수는 있지만, 보안 업데이트를 받아볼 수 없기 때문에 보안 위협과 바이러스에 더 취약해집니다. 2020년 1월 14일 이후에는 Windows 7이 아닌 Windows 10을 사용하는 것이 좋습니다.
- Internet Explorer는 Windows 7에서 여전히 지원되나요?
- Windows 7 Enterprise를 실행하고 있는 경우에는 어떤가요?
- Windows 7 Embedded는 어떤가요?
- 기존 프로그램을 새 Windows 10 PC로 이동할 수 있나요?
- Windows 7 지원 종료는 내 Microsoft Office 앱에 영향을 줍니까?

자료: https://support.microsoft.com/ko-kr/help/4057281/windows-7-support-will-end-on-january-14-2020

Vulnerability Mgmt.

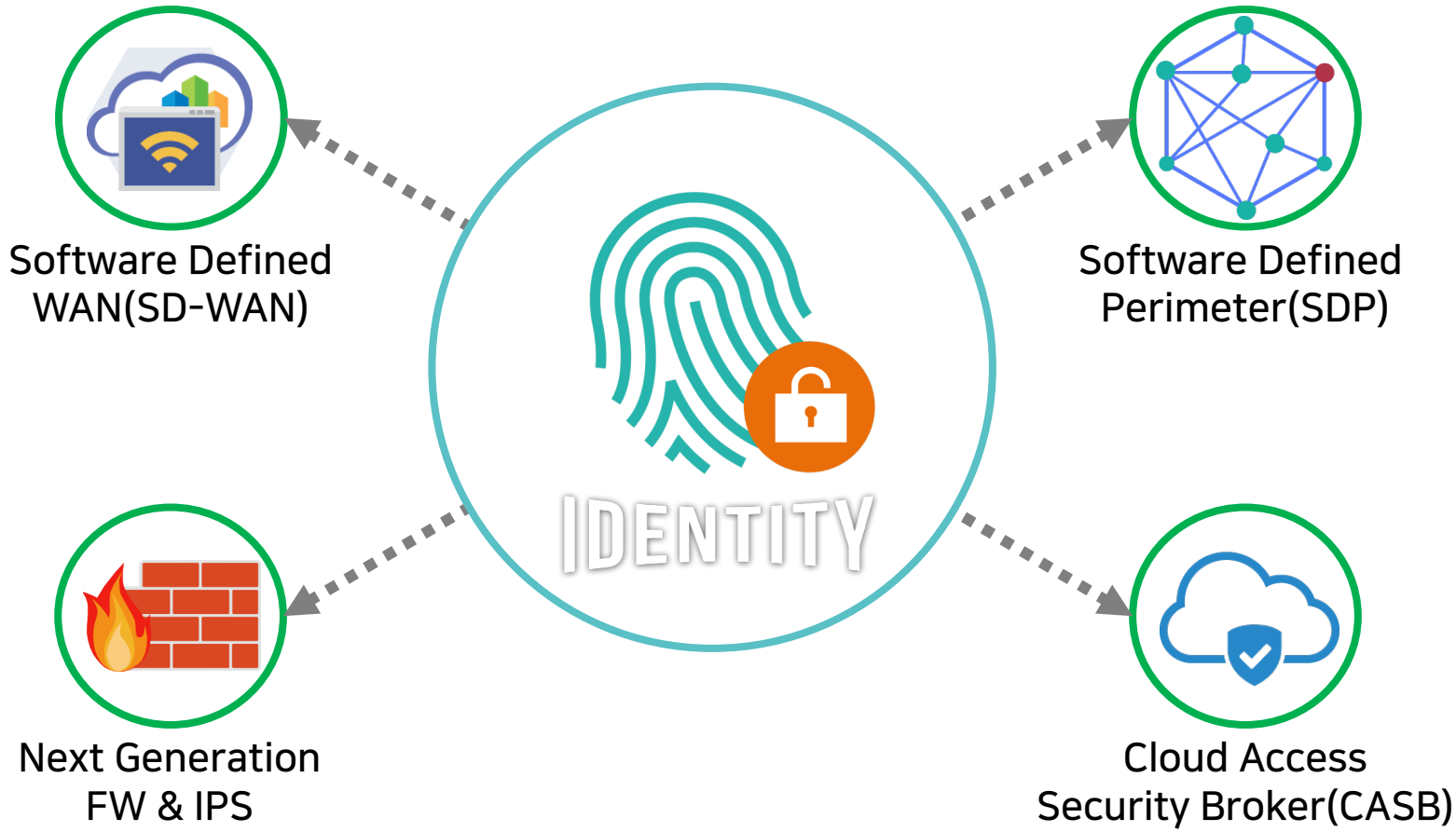
NC250

- ✓ 1분이면 안방까지 뚫린다 … 사물인터넷 파고든 해킹 (KBS)
- ✓ 안방 CCTV를 누군가 훔쳐본다…스마트 홈 파고드는 'IoT 해킹' (동아일보)
- ✓ IP 카메라 해킹해 남의 집 안방 훔쳐본 외국인 강사 벌금형 (연합뉴스)
- ✓ 홈 IoT 도어락 해킹해 10초만에 딸깍 (보안뉴스)
- ✓ '실종된 사생활'…IoT 해킹경고 (디지털타임스)
- ✓ "현관문 따고 집안 훔쳐보고"…'IoT 60%' 스마트홈 해킹 '숭숭' (KBS)

Platform's Common Vulnerabilities and Exposures (CVE)

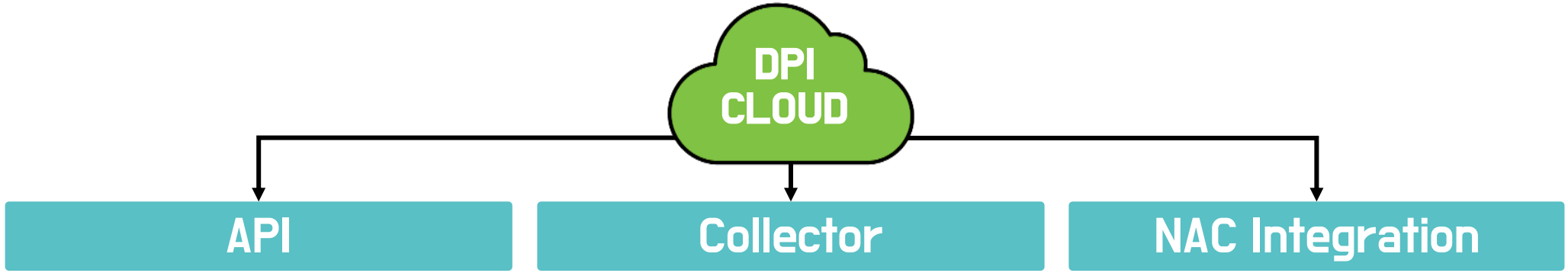
CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2017-10796 07/02/2017	MEDIUM	LOW	On TP-Link NC250 devices with firmware through 1.2.1 build 170515, anyone can view video and audio without authentication via an rtsp://admin@yourip:554/h264_hd.sdp URL.

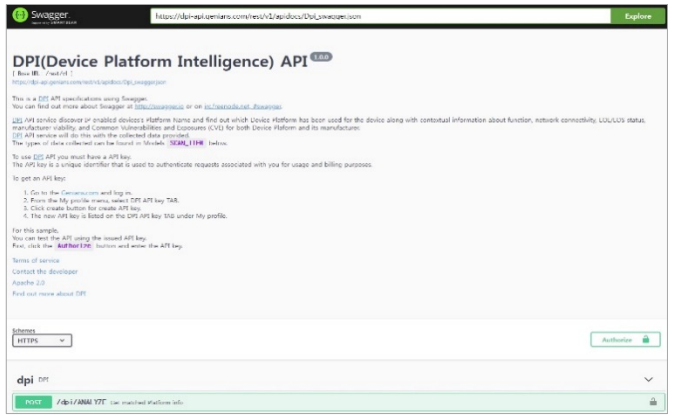
DPI 의 미래



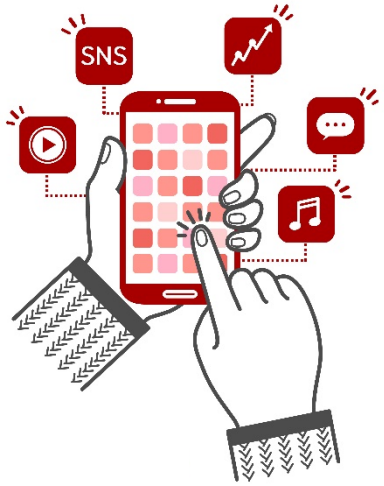
'Identity' based Security Policy

DPI Cooperation

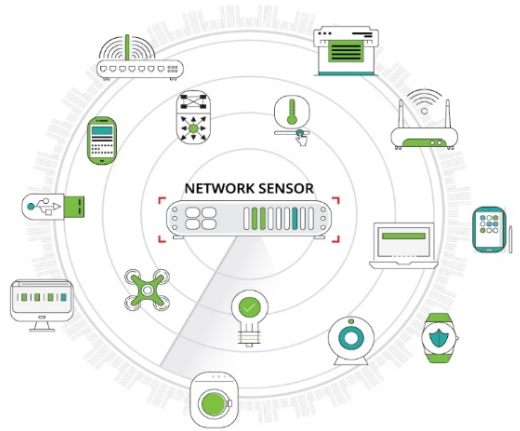




Query - Response



Standalone App.



Working with

감사합니다.