



쇼미더 '네트워크' 시즌 2

네트워크를 이해하는 새로운 방법

19.09.30 / 지니언스

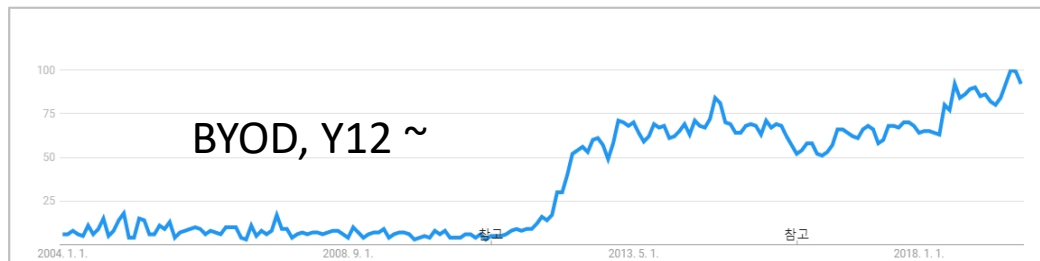
'501억' 개
(50,100,000,000)



2020년 네트워크 상의 단말의 수 (by Cisco)

'BYOD' 와 'IoT'

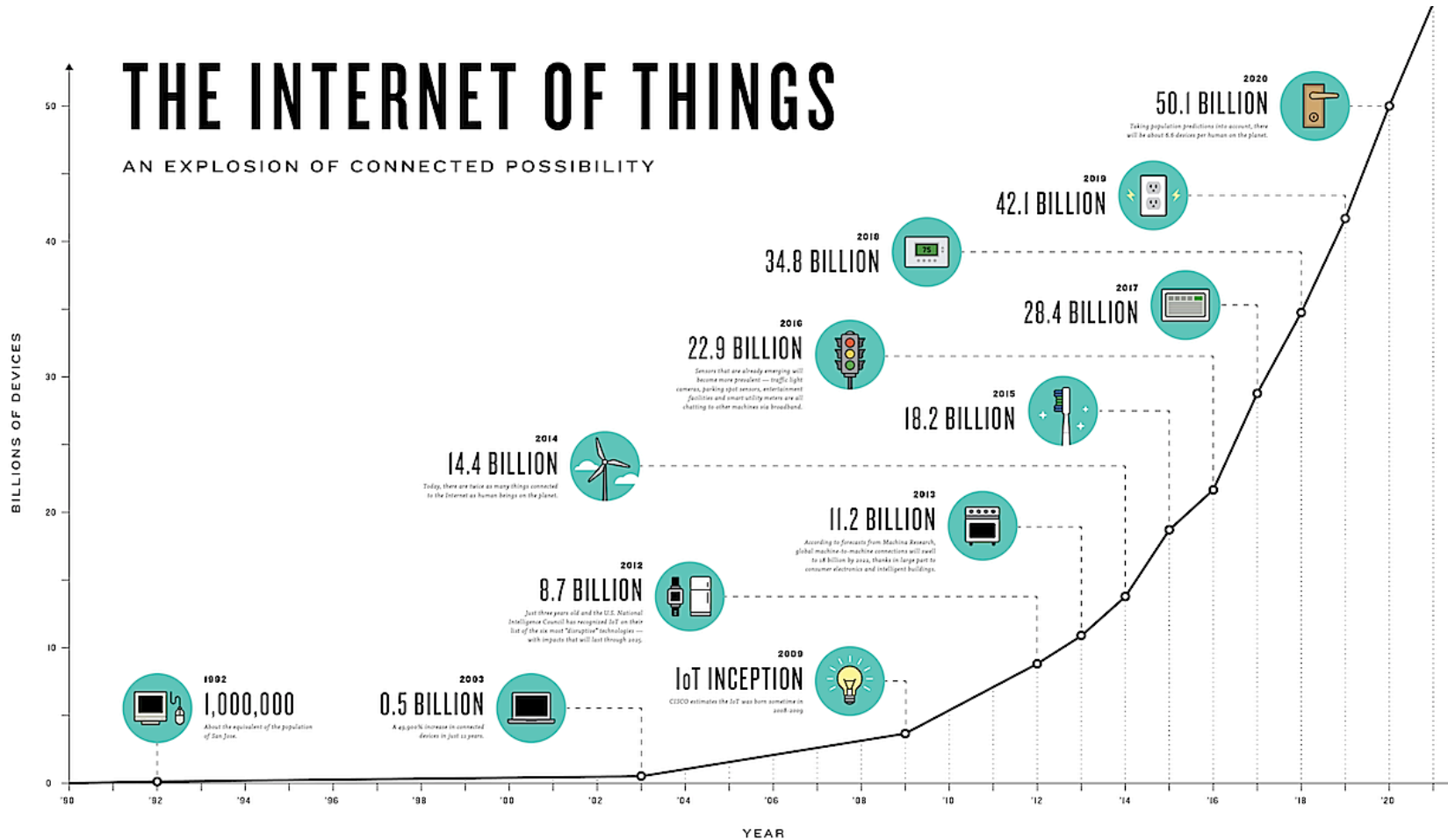
Bring Your Own Device



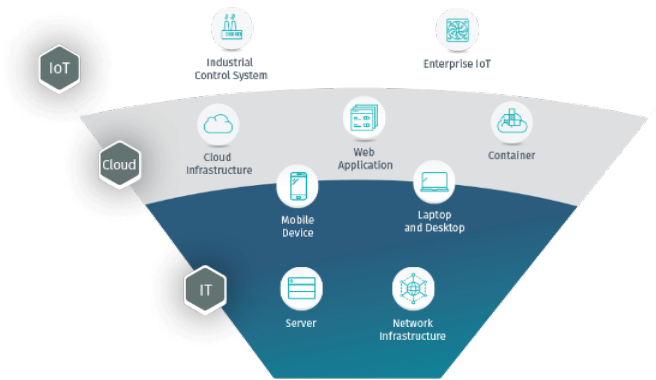
Internet of Things



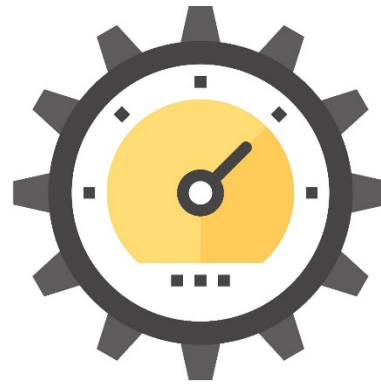
'IoT 단말' 폭발적 증가



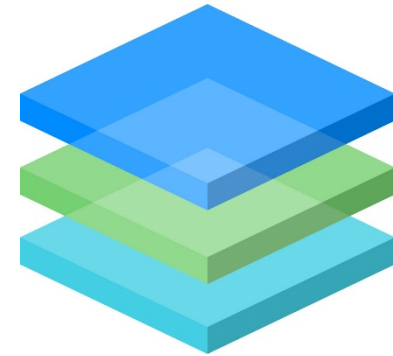
'IoT 위협' 증가



**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

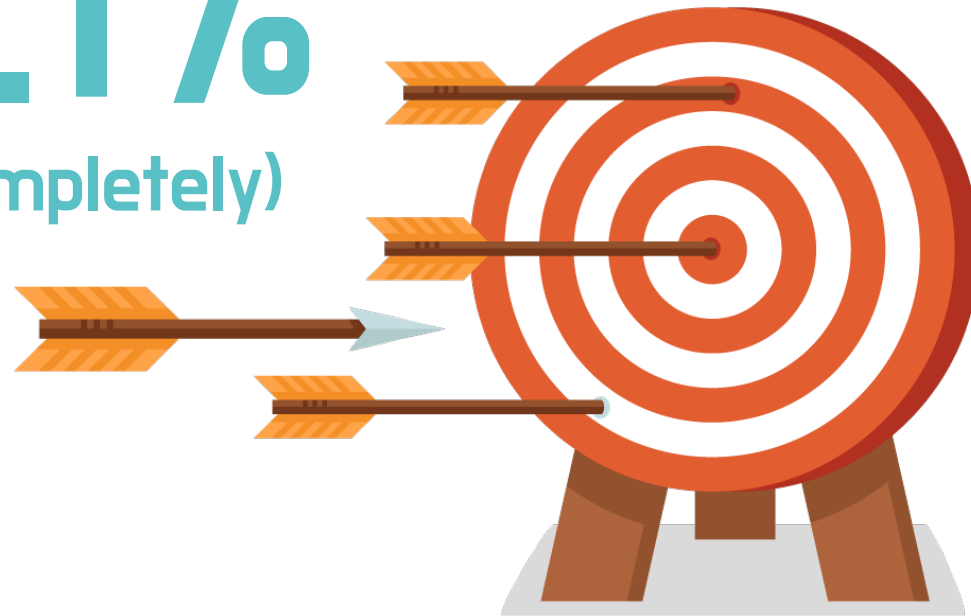


Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer (2018)

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

9.1%

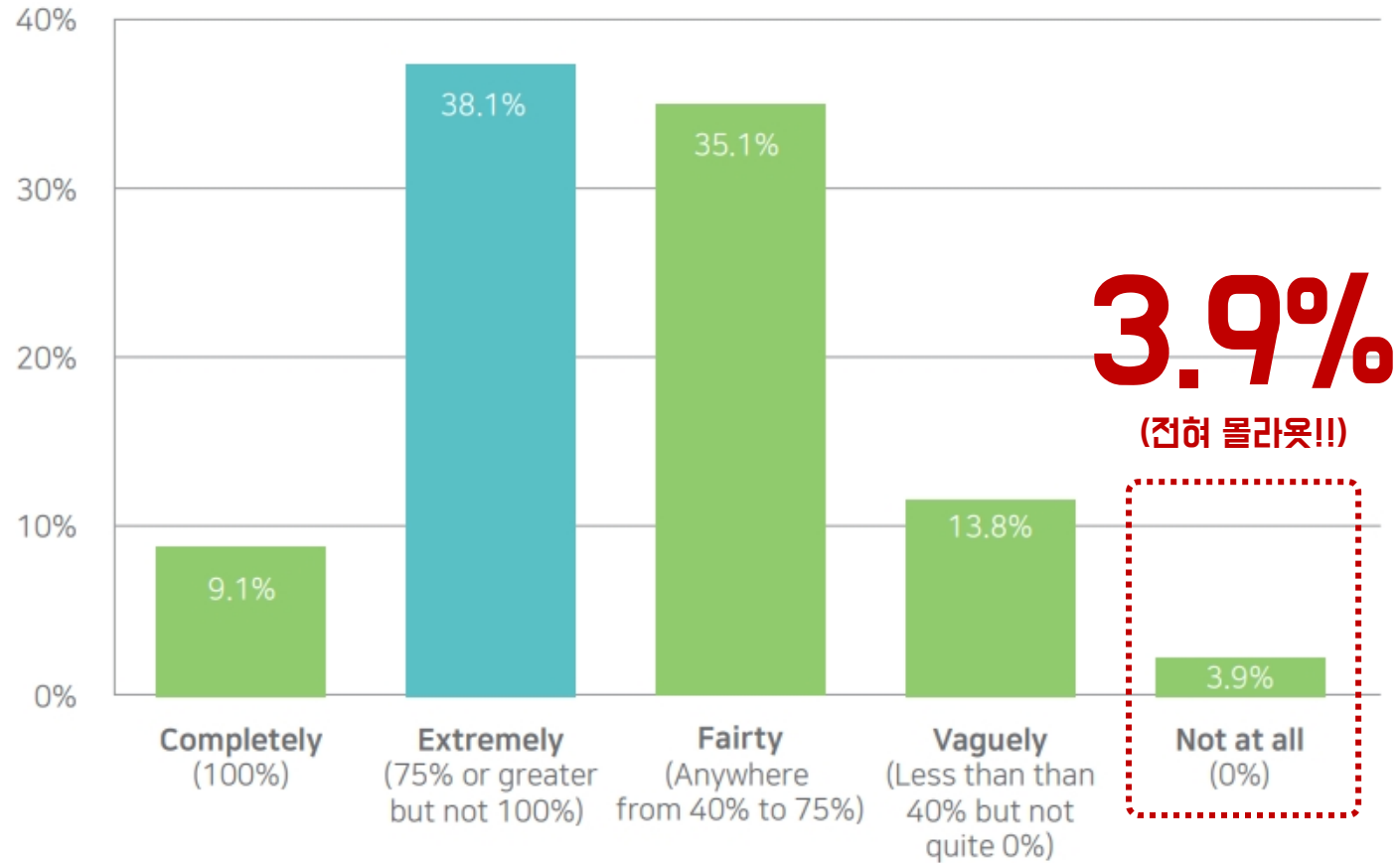
(Completely)



'Y12

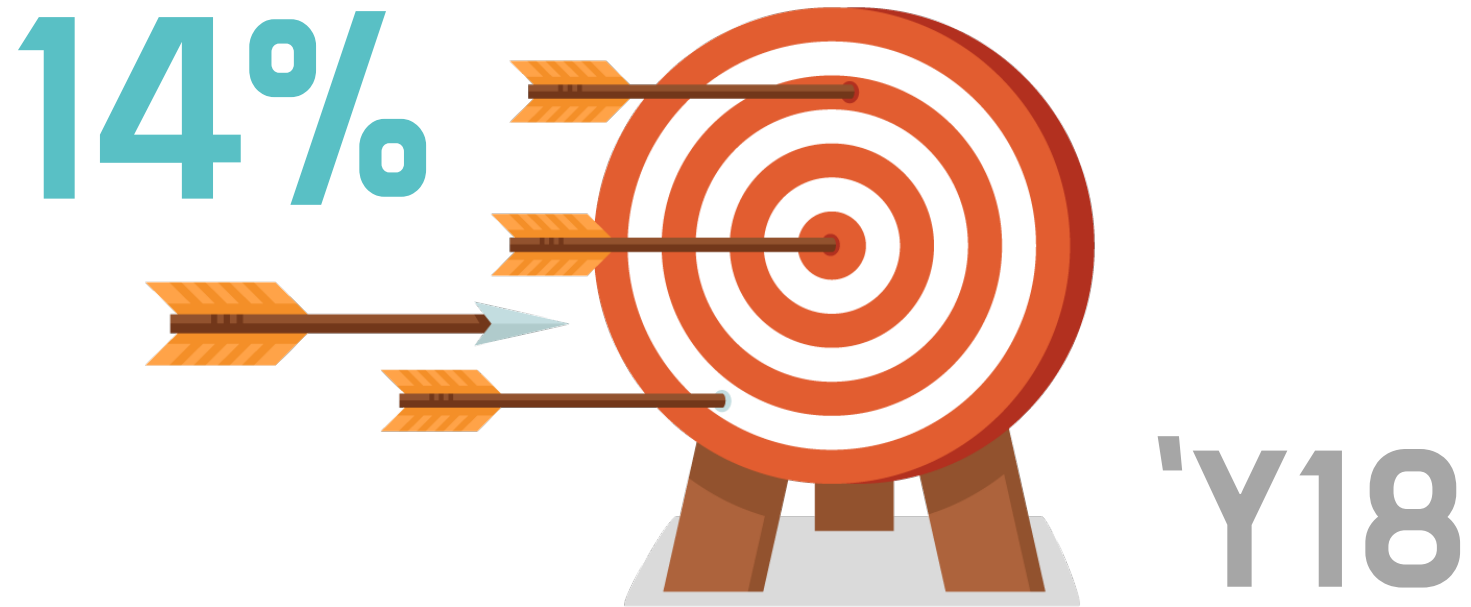
'State of Mobile Device Awareness'

자료: SANS Mobile/BYOD Security Survey 2012



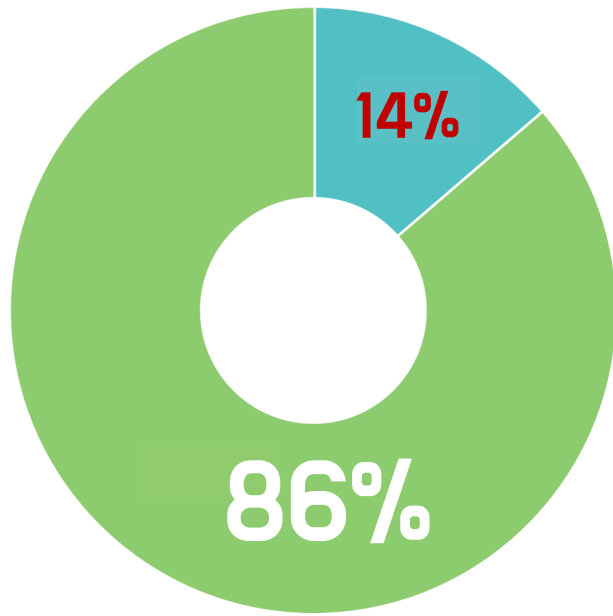
'State of Mobile Device Awareness'

자료: SANS Mobile/BYOD Security Survey 2012

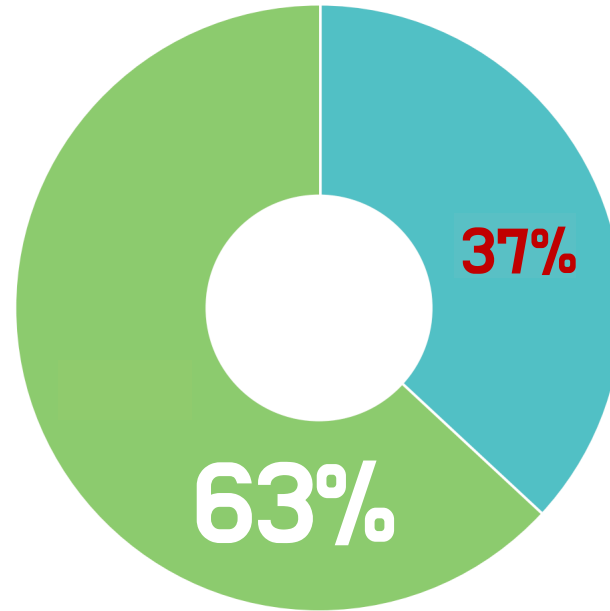


'Lack of IoT Security Awareness'

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



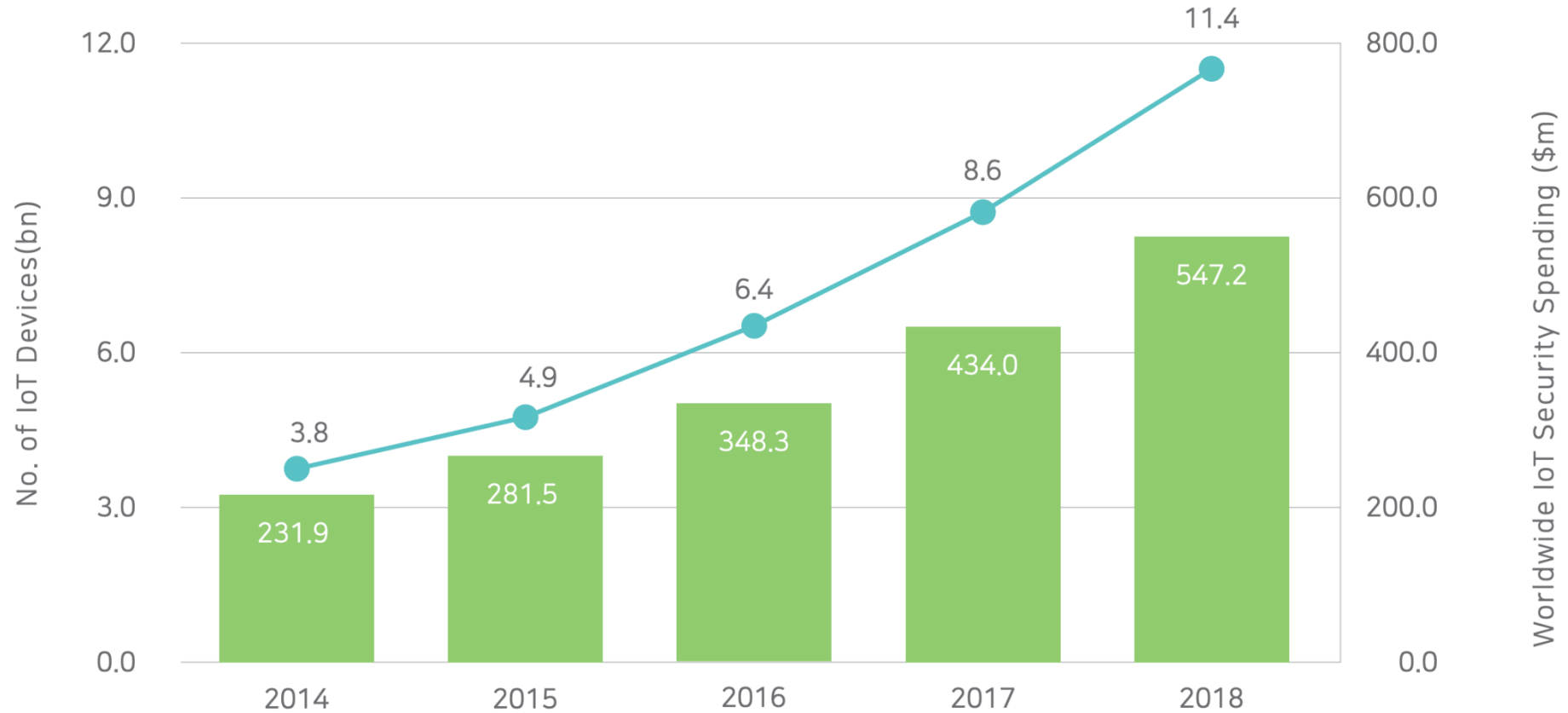
■ IoT 위협을 (완벽히) 인지
■ 그렇지 않음



■ 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

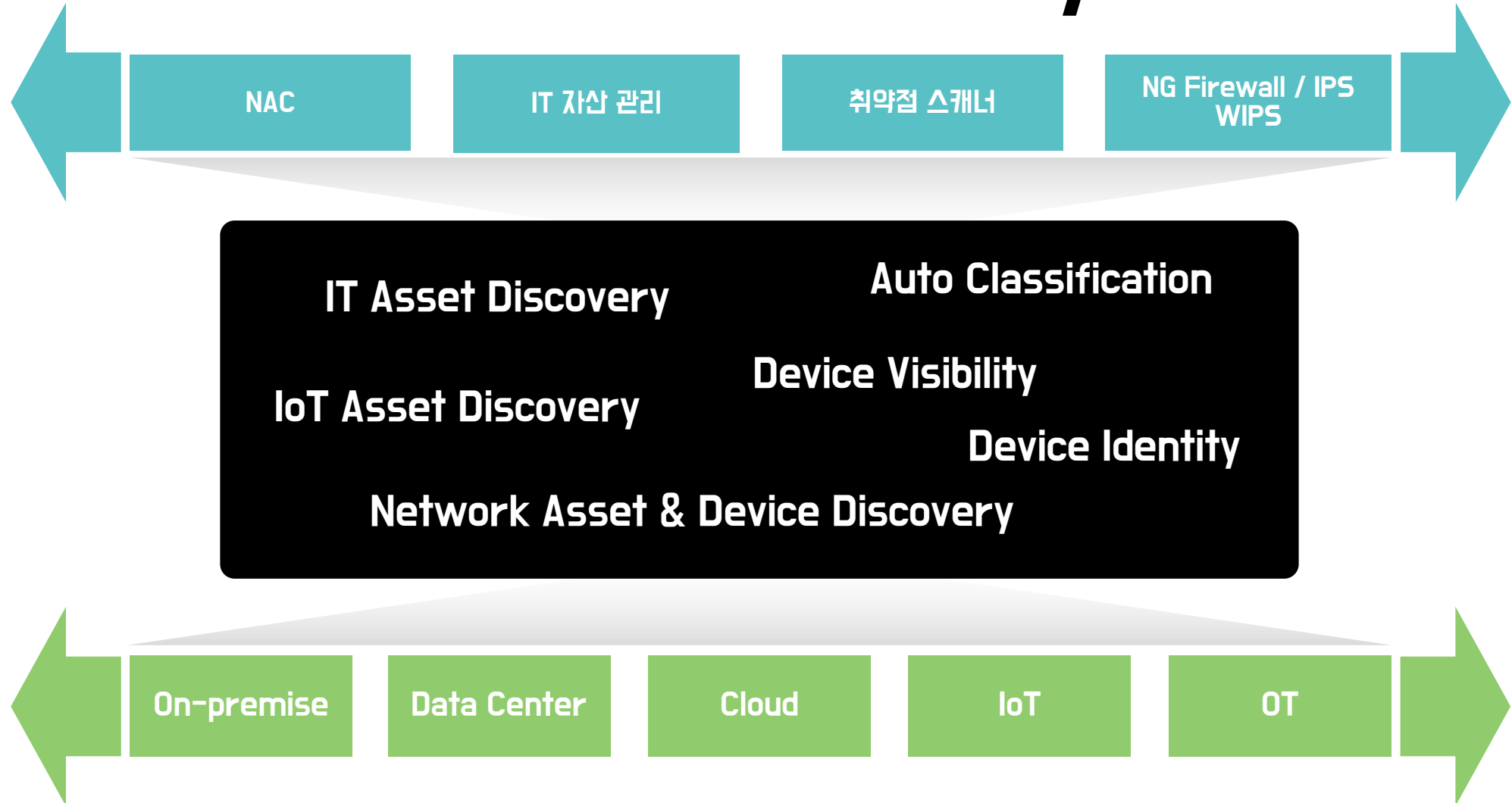
자료: Gartner, TELECOM TV, Various

It's the **Visibility.** stupid

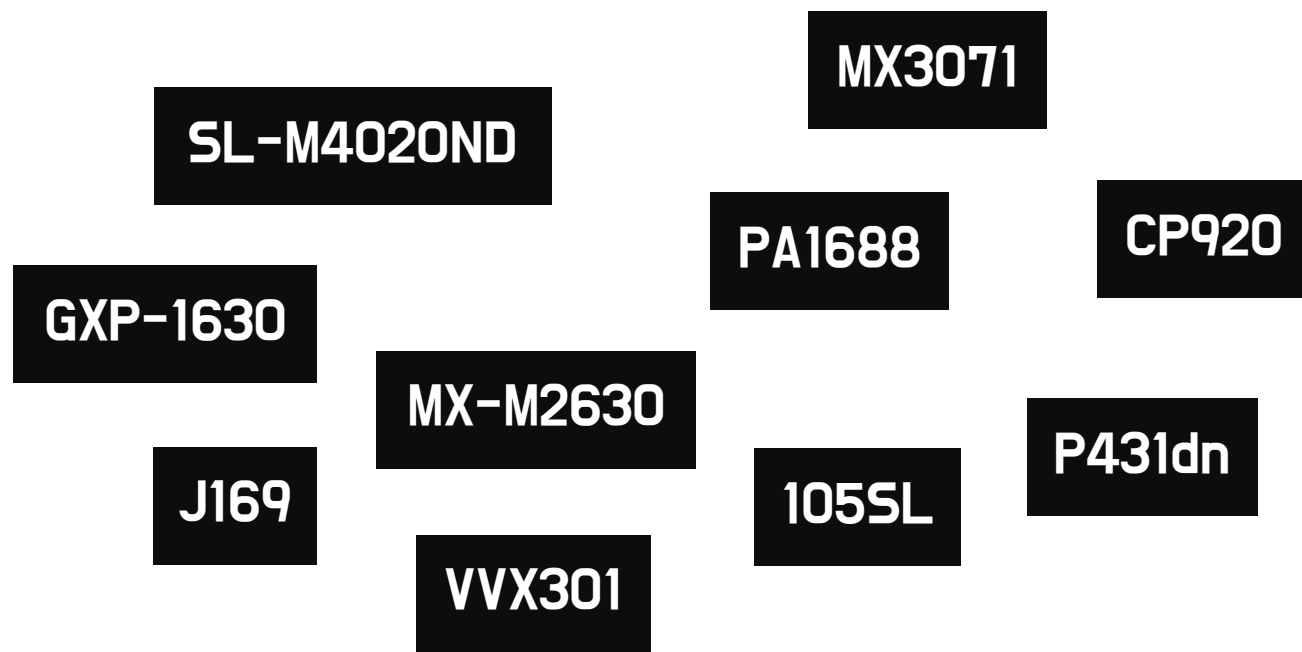


네트워크에 존재하는 '단말 가시성' 확보가 중요

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



1055L



MX-M2630

Printer



J169



PA1688



GXP-1630



VVX301



CP920

VOIP Phone

'Resolution' (해상력, 분해능)

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

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

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

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

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

IP	MAC	Category	OS	User	Location
----	-----	----------	----	------	----------

⋮

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

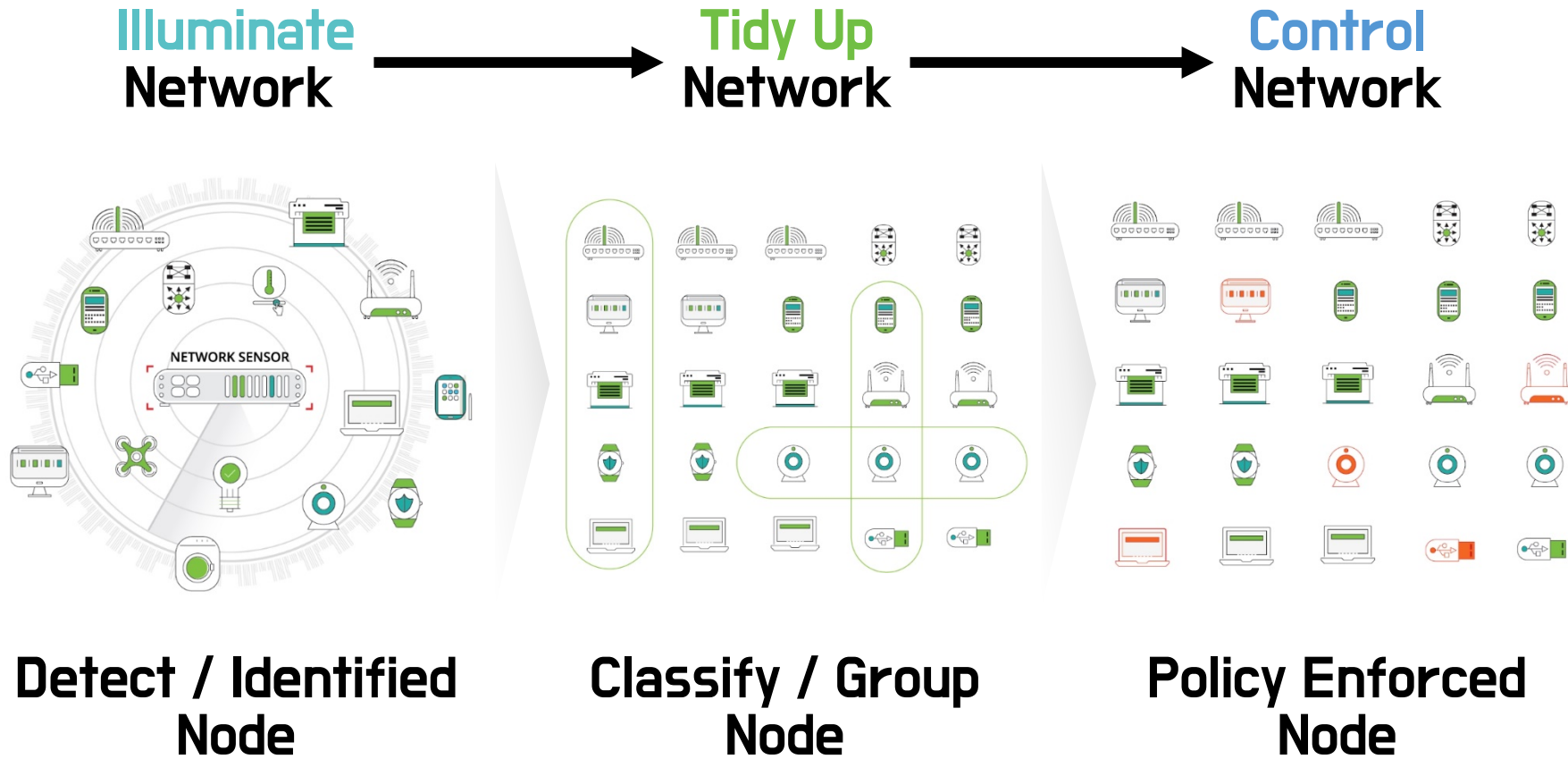
- SNMP Trap
- DHCP request
- HTTP user-agent
- ICS OT (Modbus..)
- Netflow
- RADIUS
- MAC OUI
-

* SVA: Scan-less Vulnerability Assessment

SVA, Why? (Scan-less Vulnerability Assessment)



NAC(Network Access Control)



NAC(Network Access Control)

CURRENT 관리 > 노드관리 (S-109.7.10.245) 빠른검색: 109.7.21.30

대상: 센서별 IP관리

전체노드 (674)
비관리노드 (98)
센서별 IP관리
▶ S-109.7.10.245
S-109.7.15.245
S-109.7.16.245
S-109.7.21.245
S-109.7.32.245
▶ S-109.7.35.245
S-109.7.51.245
S-109.7.61.245

전체 (33) IP관리 차단 (2) IP충돌보호 설정 (0) IP충돌보호 위반 (0) IP변경금지 설정 (0) IP변경금지 위반 (0)

작업선택 실행 노드뷰

전체 장비수:27 / 전체 노드수:33 (1 - 20 / 33)

	R	IP	IP주소	MAC주소	정책	호스트명(이름)	플랫폼	인증사용자	위치
☐			109.7.7.2	00:D0:B7:B8:C0:E9		IS-SIGK	Microsoft Windows		S-109.7.10.245
☐			109.7.7.3	00:D0:B7:B8:C7:4D		IS-ADMIN	Microsoft Windows		S-109.7.10.245
☐			109.7.7.4	00:02:B3:A1:E7:48		IS-IOSERVER	Microsoft Windows		S-109.7.10.245
☐			109.7.7.5	00:04:75:93:0D:9D			Microsoft Windows		S-109.7.10.245
☐			109.7.7.8	00:00:F0:3A:8C:EC			Samsung VOIP device		S-109.7.10.245
☐			109.7.7.88	00:00:F0:3A:84:04			Samsung IP-PCX IAP (IMPM)		S-109.7.10.245
☐			109.7.7.254	00:19:07:E7:74:00			Cisco Router		S-109.7.10.245
☐			109.7.10.1	00:07:E9:0C:93:DB			SCO UnixWare		S-109.7.10.245
☐			109.7.10.5	00:11:25:BD:0C:81			IBM AIX 5		S-109.7.10.245
☐			109.7.10.9	00:07:E9:0C:93:DB			SCO UnixWare		S-109.7.10.245
☐			109.7.10.10	00:07:E9:0C:94:27			SCO UnixWare		S-109.7.10.245
☐			109.7.10.11	00:07:E9:0C:94:27			SCO UnixWare		S-109.7.10.245
☐			109.7.10.14	00:03:47:B0:55:49			SCO UnixWare		S-109.7.10.245
☐			109.7.10.17	00:03:BA:0D:75:4D			Sun		S-109.7.10.245
☐			109.7.10.18	00:E0:00:C4:8E:61			Sun Solaris 8		S-109.7.10.245
☐			109.7.10.19	00:14:5E:2B:77:B9		V3APC	Microsoft Windows		S-109.7.10.245
☐			109.7.10.22	00:11:85:C5:38:A6		초과근무	Microsoft Windows		S-109.7.10.245
☐			109.7.10.30	00:03:BA:0B:3B:B9			Sun		S-109.7.10.245
☐			109.7.10.31	00:03:BA:0B:3B:B9			Sun		S-109.7.10.245
☐			109.7.10.40	00:11:25:C0:20:4C			IBM AIX 5		S-109.7.10.245

GPDB v1.0
(Genian Platform DB)

- IP 관리 어려움
- 단말 관리 어려움
- 관리 항목 증가

DPI(Device Platform Intelligence)

All Platform		All Platforms								Search
2019		Platform Name	CVE	EOL	Type	Manufacturer	Country (HQ)	Added at		
2019-09-17	24	ATEN KN4116VA KVM Switch			Switch	ATEN INTERNATIONAL Co., Ltd.	Taiwan	Sep 17, 2019		
2019-09-10	53	Huawei Enjoy 9s Phone			Mobile	Huawei Technologies Co., Ltd.	China	Sep 17, 2019		
2019-09-03	39	Vivo V15 Pro Phone			Mobile	Vivo Communication Technology Co. Ltd.	China	Sep 17, 2019		
2019-08-27	69	SHARP MX-3071 Printer			Printer	SHARP CORPORATION (Foxconn International Holdings Ltd - Hon Hai Precision Industry Co., Ltd)	Japan	Sep 17, 2019		
2019-08-20	62	Samsung Galaxy A80 Phone			Mobile	SAMSUNG ELECTRONICS CO., LTD.	Korea (Republic of)	Sep 17, 2019		
2019-08-13	21	Ingate SIParator Firewall VOIP Gateway	🚩		VOIP	Ingate Systems AB	Sweden	Sep 17, 2019		
2019-08-06	34	ServGate SG100 Firewall Appliance			Security	ServGate Technologies ()	United States of America	Sep 17, 2019		
2019-07-30	55	D-Link DSL Router	🚩		Wireless	D-Link Systems, Inc.	Taiwan	Sep 17, 2019		
2019-07-23	60	Aethra SV2242 Router			Wireless	Aethra Telecommunications - A TLC S.r.l.	Italy	Sep 17, 2019		
2018		Symbol XR480 RFID Reader			Other	Symbol Technologies (Zebra Technologies Corp)	United States of America	Sep 17, 2019		
2017		Infortrend NAS			Server	Infortrend Technology Inc.	Taiwan	Sep 17, 2019		
2016		Hitachi G600 Virtual Storage Platform			Server	Hitachi Data Systems Corporation ()	United States of America	Sep 17, 2019		
2015		Huawei Honor View20 Phone			Mobile	Huawei Technologies Co., Ltd.	China	Sep 17, 2019		
2014		Grandstream GXP1630 VOIP Phone			VOIP	Grandstream Networks, Inc.	United States of America	Sep 17, 2019		
2013		itel P13 Phone			Mobile	itel	Hong Kong	Sep 17, 2019		
2012		Realme Q Phone			Mobile	realme		Sep 17, 2019		
2011		Vivo Z5 Phone			Mobile	Vivo Communication Technology Co. Ltd.	China	Sep 17, 2019		
2010		BlueCoat PacketShaper S200 Monitoring Device			Network	Blue Coat Systems, Inc. (Symantec Corporation)	United States of America	Sep 17, 2019		
2009										
2008										
2007										

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

DPI tells you...



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	Description
CVE-2019-13268 08/27/2019	HIGH	MEDIUM	TP-Link Arch a guest network packets, between issue an ARP requests des factor, one m
CVE-2019-13267 08/27/2019	HIGH	MEDIUM	TP-Link Arch a guest network, the an IGMP Me transferred v
CVE-2019-13266 08/27/2019	HIGH	MEDIUM	TP-Link Arch a guest network 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 authentication



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

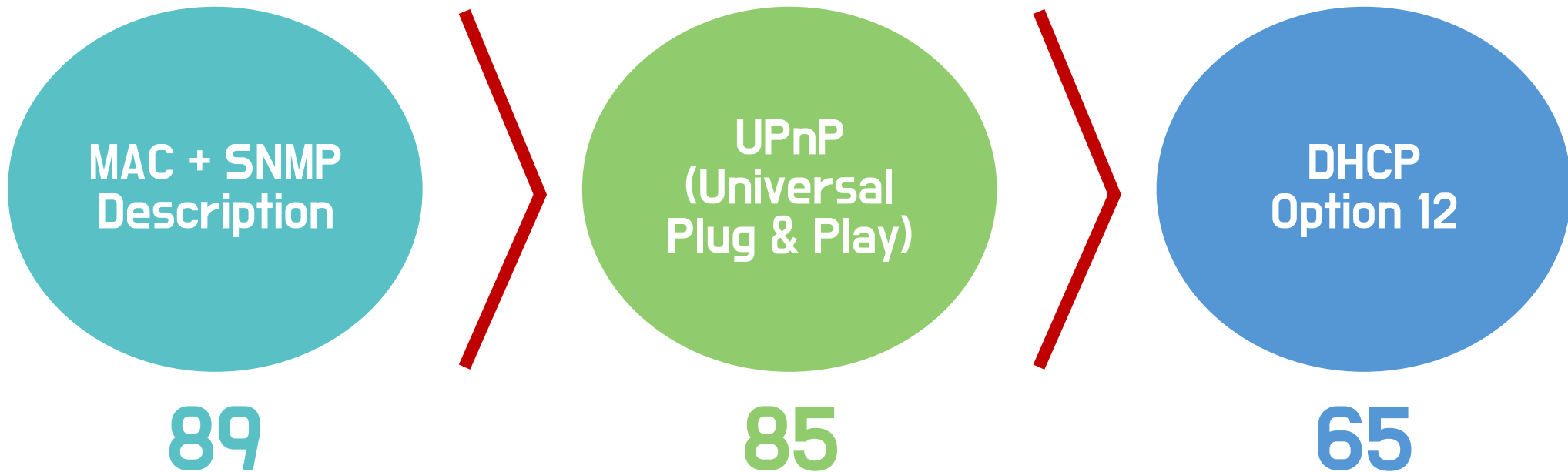
- Telnet
- FTP
- SNMP OID / Desc.
- Open Port
- HTTP(S) User-agent
- HTTP Page
- HTTP Certificate
- ModBus / BACnet

Passive

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

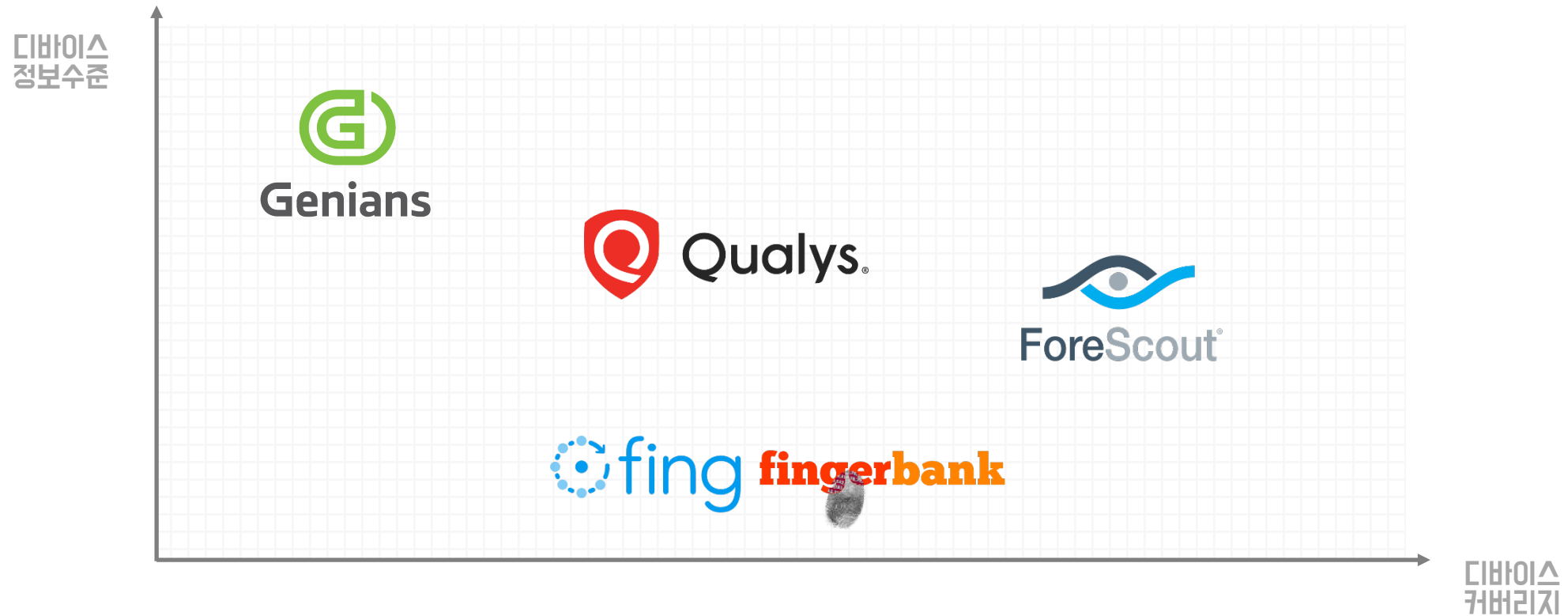
지원예정

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

Genian NAC v5.0 대시보드 관리 감사 정책 설정 시스템

Answers

Search

현재노드 (47)

노드하구니 (0)

nacdemo (4)

Boston (43)

전체노드

작업선택

검색 1 - 47 / 47 50

NT AG SS	위험	동작	동작상태차트	IP주소	MAC주소	정책	제어정책	호스트명(이름)	인증사용자	플랫폼	위치	가동률
10.8.0.6				10.8.0.6	00:00:00:00:00:00		Antivirus Not Compliant	client.openvpn.net	scott	Apple macOS Mojave	nacdemo.genians.net	0%
10.211.55.3				10.211.55.3	00:1C:42:F1:DB:56		Antivirus Not Compliant	KYEEONKIMAF48		Microsoft Windows 10 Home x64	nacdemo.genians.net	0%
172.20.20.218				172.20.20.218	00:E0:4C:68:00:01		Antivirus Not Compliant	FOREST		Microsoft Windows 10 Home x64	nacdemo.genians.net	0%
192.168.50.4				192.168.50.4	00:18:DA:09:C2:58		Unauthorized Device	North Andover Office		Cisco Meraki Z1 AP	Boston	100%
192.168.50.2				192.168.50.2	08:62:66:3A:07:00		Unauthorized Device	RT-AC68P-0700		ASUS RT-AC68P Wireless Router	Boston	52%
192.168.50.11				192.168.50.11	F4:4D:30:66:0F:64			USA-eth0(Boston)		SS64	nacdemo.genians.net	93%
192.168.50.15				192.168.50.15	C4:6E:1F:EF:07:F2		Blocking Exceptions			TP-LINK TECHNOLOGIES CO.,LTD. AP	Boston	57%
192.168.50.20				192.168.50.20	38:C9:86:20:0E:C4		Blocking Exceptions	kimyeyeons-imac.local	Super Administrator	Apple macOS Mojave	Boston	99%
192.168.50.24				192.168.50.24	40:8D:5C:1A:D0:E4		Default Policy	KYEEON		Ubuntu Linux	Boston	79%
192.168.50.30				192.168.50.30	B0:6E:BF:74:BA:70		Default Policy	GNTST1		ASUSTek COMPUTER INC. AP	Boston	100%
192.168.50.31				192.168.50.31	90:80:ED:5C:68:F9		Default Policy	iPhone		Apple iPhone	Boston	11%
192.168.50.44				192.168.50.44	08:00:27:56:BD:36		Default Policy			Genians Genian NAC	Boston	6%
192.168.50.45				192.168.50.45	08:00:27:56:BD:36		Default Policy			PCB Systematics GmbH	Boston	0%
192.168.50.45				192.168.50.45	08:00:27:56:BD:36		Default Policy			Genians Genian NAC	Boston	0%
192.168.50.47				192.168.50.47	08:00:27:02:94:76		Default Policy			VirtualBox Linux	Boston	40%
192.168.50.48				192.168.50.48	08:00:27:03:A8:64		Default Policy			VirtualBox Linux	Boston	75%
192.168.50.102				192.168.50.102	35:F9:D3:72:96:93		Default Policy	KYEEON5-MBP		Apple MacBook Pro	Boston	23%
192.168.50.105				192.168.50.105	F4:52:06:0E:76:72		Default Policy	GENIACOP-4040FT14		Microsoft Windows	Boston	50%
192.168.50.108				192.168.50.108	10:41:7F:28:02:4A		Default Policy	Genian		Apple iPhone	Boston	11%
192.168.50.104				192.168.50.104	08:00:27:56:BD:36		Default Policy	MAC-00:0C:03:00:00:00		Apple MacBook Air	Boston	0%

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

Device Platform Intelligence / Cisco SPA 303 VOIP Phone



Cisco SPA 303 VOIP Phone

Platform Information	https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/small-business-spa300-series-ip-phones/data_sheet_c78-601648.html
Search Engine	Search on Google
End of Sales	-
End of Support	-
Wired Connection	Yes
Wireless Connection	-
Fingerprinting Source	HTTP MAC OUI NIC VENDOR
Added at	Jun 04, 2019
Manufacturer Name	Cisco Systems Inc.
Homepage	http://www.cisco.com/
Headquarters	United States of America
Business Status	Ongoing

Suggest Update

Platform's Common Vulnerabilities and Exposures (CVE)			
CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2014-3313 07/09/2014		MEDIUM	Cross-site scripting (XSS) vulnerability in the web user interface on Cisco Small Business SPA300 and SPA500 phones allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCuo52582.
CVE-2014-3312 07/09/2014		MEDIUM	The debug console interface on Cisco Small Business SPA300 and SPA500 phones does not properly perform authentication, which allows local users to execute arbitrary debug-shell commands, or read or modify data in memory or a filesystem, via direct access to this interface, aka Bug ID CSCun77435.
« < 1 > »			
Manufacturer's Common Vulnerabilities and Exposures (CVE)			
CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2019-1976 09/05/2019	CRITICAL	MEDIUM	A vulnerability in the "plug-and-play" services component of Cisco Industrial Network Director (IND) could allow an unauthenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to improper access restrictions on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to access running configuration information about devices managed by the IND, including administrative credentials.
CVE-2019-1939 09/05/2019	HIGH	HIGH	A vulnerability in the Cisco Webex Teams client for Windows could allow an unauthenticated, remote attacker to execute arbitrary commands on an affected system. This vulnerability is due to improper restrictions on software logging features used by the application on Windows operating systems. An attacker could exploit this vulnerability by convincing a targeted user to visit a website designed to submit malicious input to the affected application. A successful exploit could allow the attacker to cause the application to modify files and execute arbitrary commands on the system with the privileges of the targeted user.
CVE-2019-12645 09/05/2019	HIGH	HIGH	A vulnerability in Cisco Jabber Client Framework (JCF) for Mac Software, installed as part of the Cisco Jabber for Mac client, could allow an authenticated, local attacker to execute arbitrary code on an affected device. The vulnerability is due to improper file level permissions on an affected device when it is running Cisco JCF for Mac Software. An attacker could exploit this vulnerability by authenticating to the affected device and executing arbitrary code or potentially modifying certain configuration files. A successful exploit could allow the attacker to execute arbitrary code or modify certain configuration files on the device using the privileges of the installed Cisco JCF for Mac Software.
CVE-2019-12644 09/05/2019	MEDIUM	MEDIUM	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability exists because the web-based management interface of the affected device does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.
CVE-2019-12635 09/05/2019	MEDIUM	MEDIUM	A vulnerability in the authorization module of Cisco Content Security Management Appliance (SMA) Software could allow an authenticated, remote attacker to gain out-of-scope access to email. The vulnerability exists because the affected software does not correctly implement role permission controls. An attacker could exploit this vulnerability by using a custom role with specific permissions. A successful exploit could allow the attacker to access the spam quarantine of other users.

Node Business(확장) & Vulnerability(취약성)

DPI in Genian NAC

Genian NAC v5.0 관리 감사 정책 설정 시스템

업데이트 : 16:57:06 KST 00:40

센서: S-172.29.50.49 / 플랫폼 현황 / 판매종료

노드타입 전체 플랫폼 검색

* 센서가 원격지에서 감지하거나 예측한 관리가능한 노드 플랫폼의 수를 의미합니다.

플랫폼	CVE	수량	비율
Cisco Catalyst 2960X-24TS-LL Switch	0	8	5%
Cisco Catalyst 2960 Switch	0	1	1%
Microsoft Windows 7 Professional	1750	1	1%

Device Platform Intelligence / Cisco Catalyst 2960X-24TS-LL Switch

Cisco Catalyst 2960X-24TS-LL Switch

Platform Information <http://www.router-switch.com/ws-c2960x-24ts-ll-p-5264.html>

Search Engine [Search on Google](#)

End of Sales Yes (2015-11-06) [more info](#)

End of Support Planned (2020-11-30) [more info](#)

Wired Connection Yes

Wireless Connection -

Fingerprinting Source NIC VENDOR SNMP OID

Added at Aug 20, 2014

Manufacturer Name Cisco Systems Inc.

Homepage <http://www.cisco.com/>

Headquarters United States of America

Business Status Ongoing

[Suggest Update](#)

Value of DPI



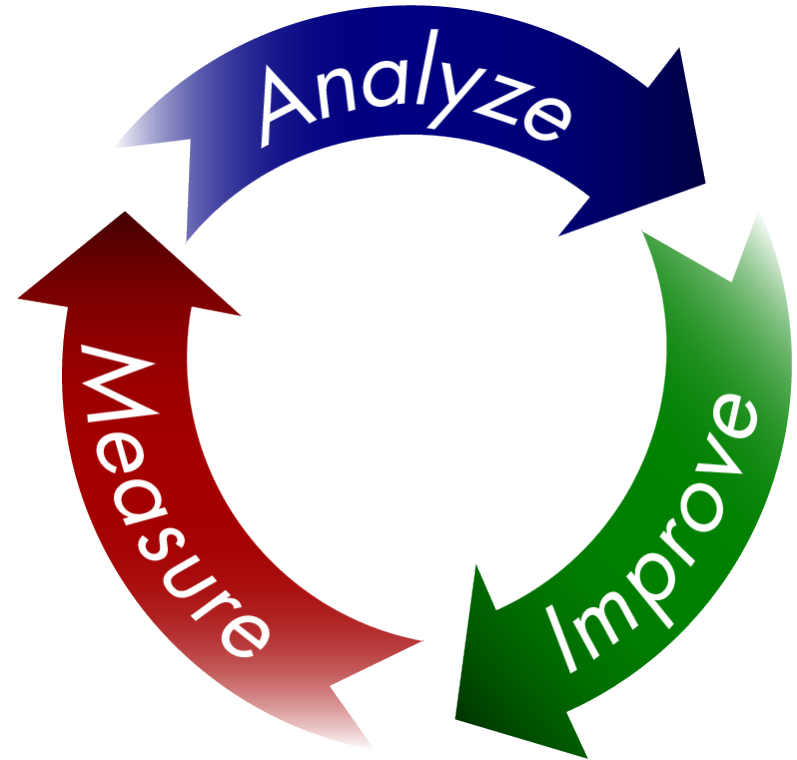
Granular Visibility



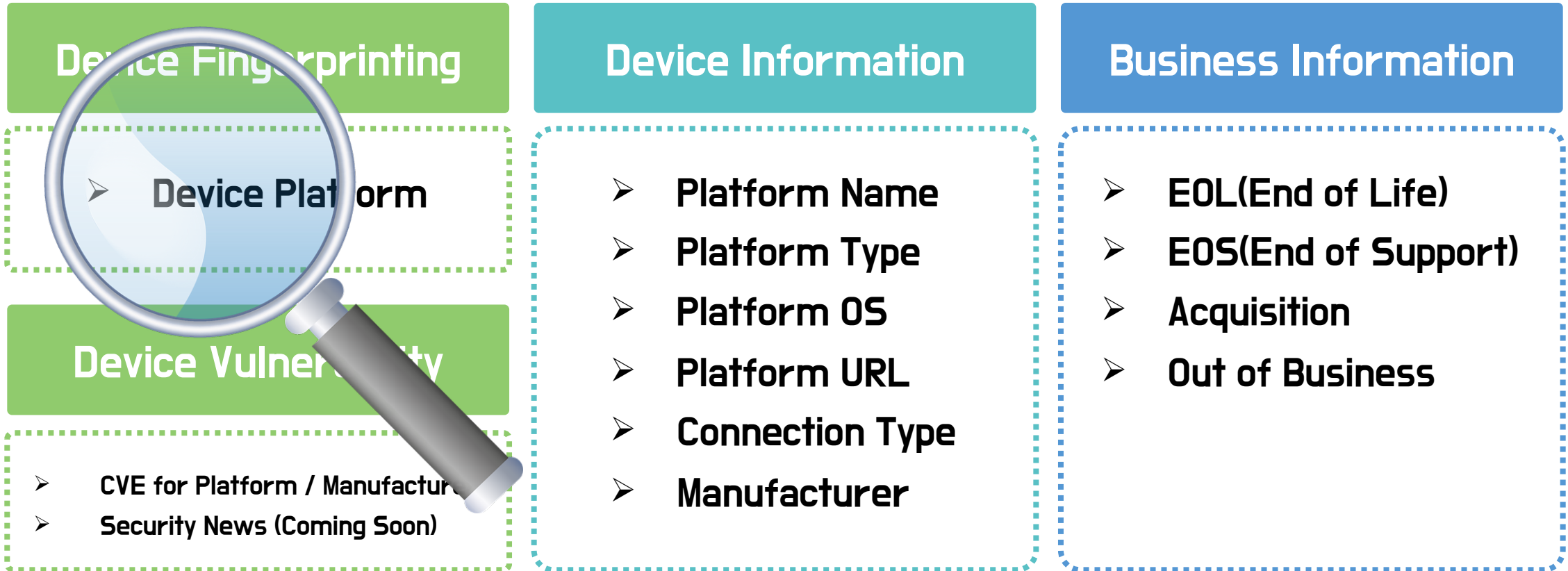
Lifecycle Mgmt.



Vulnerability Mgmt.
(Scan-less Vulnerability Assessment)



Granular Visibility



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.



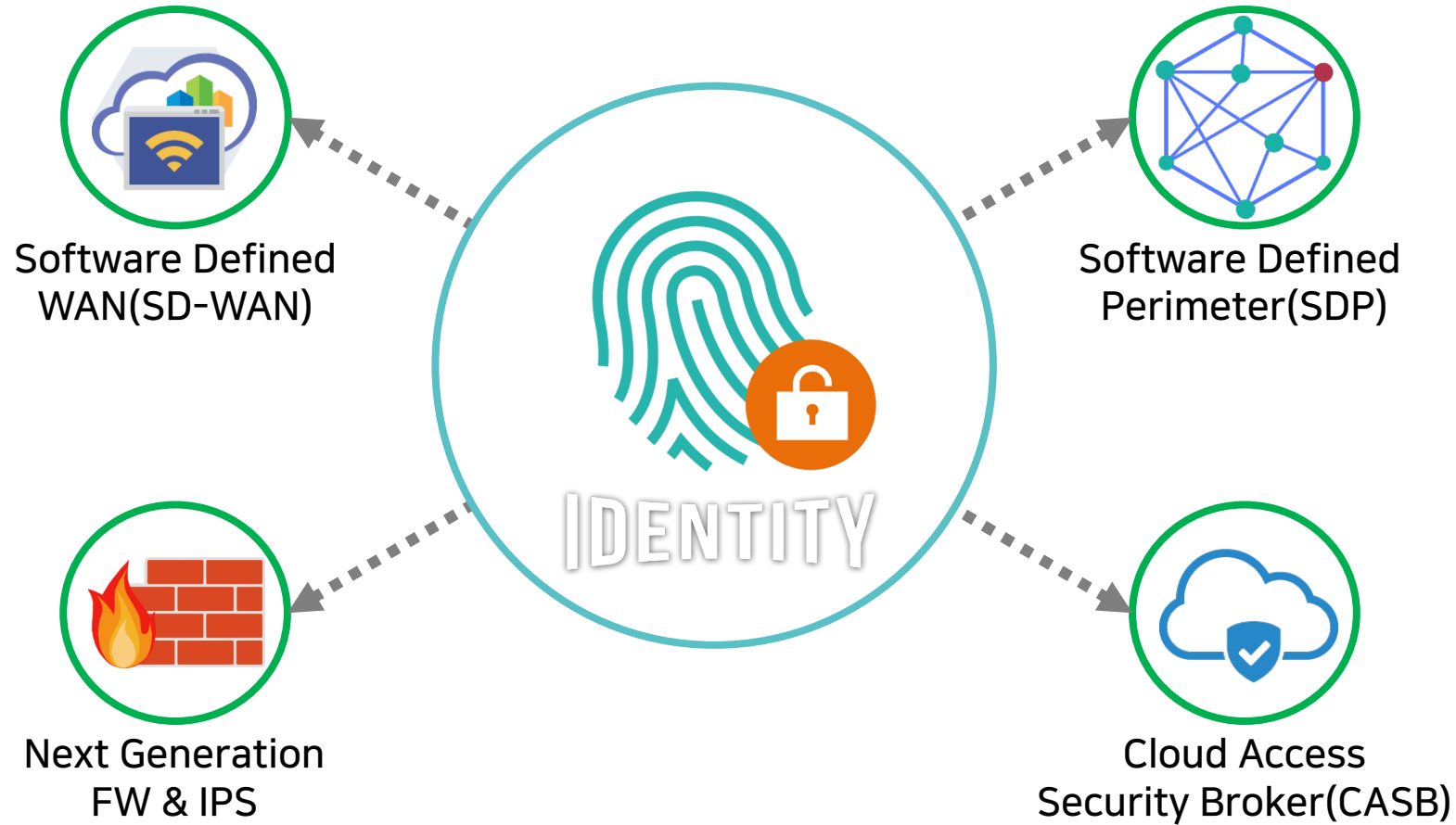
NC250

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

Platform's Common Vulnerabilities and Exposures (CVE)

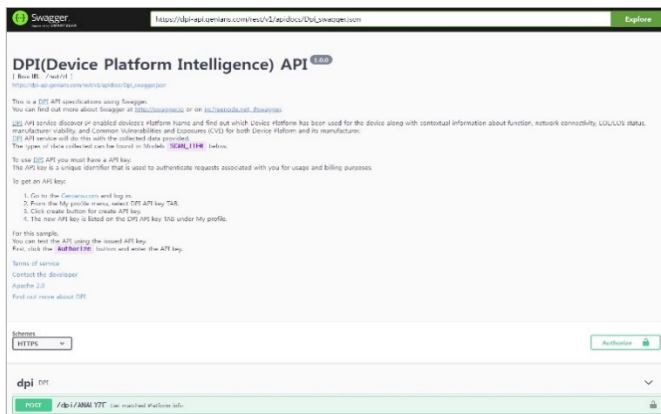
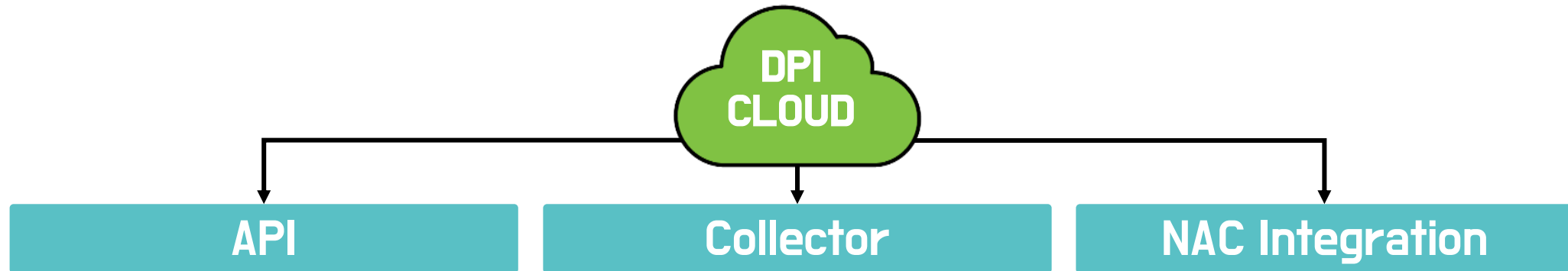
CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2017-10796 07/02/2017	MEDIUM	LOW	On TP-Link NC250 devices with firmware through 1.2.1 build 170515 anyone can view video and audio without authentication via an rtsp://admin@yourip:554/h264_hd.sdp URL.

DPI 의 미래

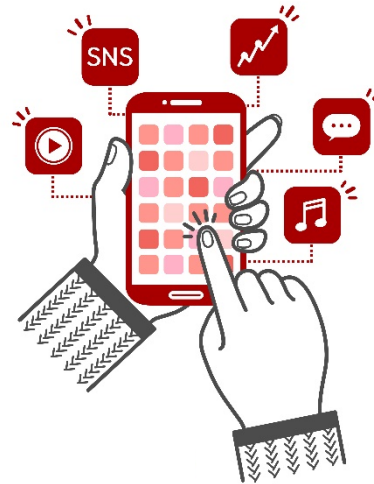


'Identity' based Security Policy

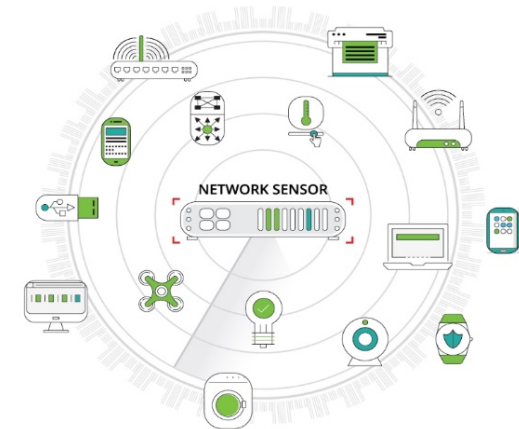
DPI Cooperation



Query - Response



Standalone App.



Working with



감사합니다.