Infoblox

제로 트러스트의 새로운 비전, DNS 보안과 DDI 통합

인포블록스 코리아

문현욱 상무, Solution Architect

Infoblox 소개

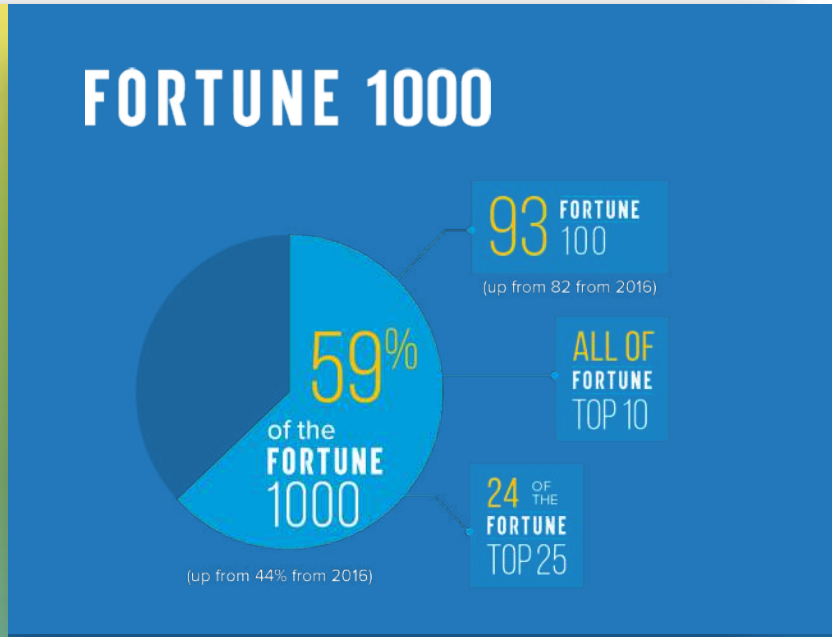
DDI 업계를 리드

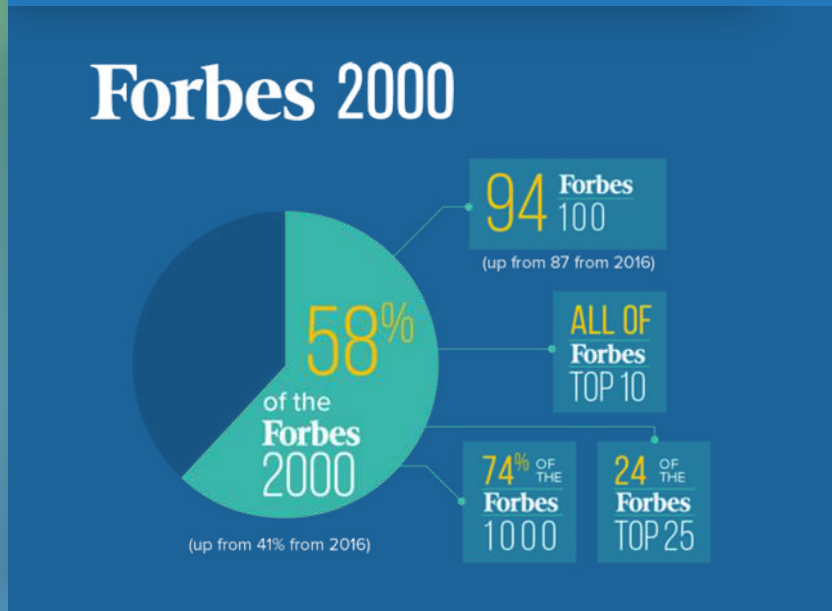
목표

고객이 계속 변화하고 확장하는 네트워크를 쉽고 안전하게 관리하도록 최고의 기술과 서비스를 제공합니다.

솔루션

Core Network Services, Cybersecurity, Secure Edge Services





Infoblox 사업 모델

주요 시장

DDI
DNS | DHCP | IPAM

비즈니스 핵심 네트워크 서비스

Security

새로운 보안 지형에서 비즈니스를 보호

Edge

확장이 유연한 시큐어 엣지 서비스

제품 포트폴리오

핵심 네트워크 서비스 (DDI)

- DNS 로드밸런싱 (DTC)
- 강력한 리포팅, 네트워크 가시성 확보 및 설정 관리 솔루션
- 네트워크 인텔리전트

보안 상태의 강화 및 최적화

- 전사적 보안 가시성 확보
- 최신 멀웨어와 데이터 유출 통제
- 강력한 위협 인텔리전스
- 에코시스템 강화, SOAR
- 인프라 보호 (ADP)

Cloud-native 기반의 인접 네트워크 및 보안 서비스

- SaaS 기반의 DDI, 근접 네트워크 및 보안 서비스 제공
- 신속하고 유연한 확장성 제공
- On-Premise 또는 SaaS
- 클라우드 관리의 단순성

최근 위협의 변화와 보안 운영의 현실

최근 네트워크의 변화

Work from Anywhere

SaaS Everywhere

IoT Everywhere

2025년까지, 엔터프라이즈 85%가 cloud-first 원칙을 취할 것입니다

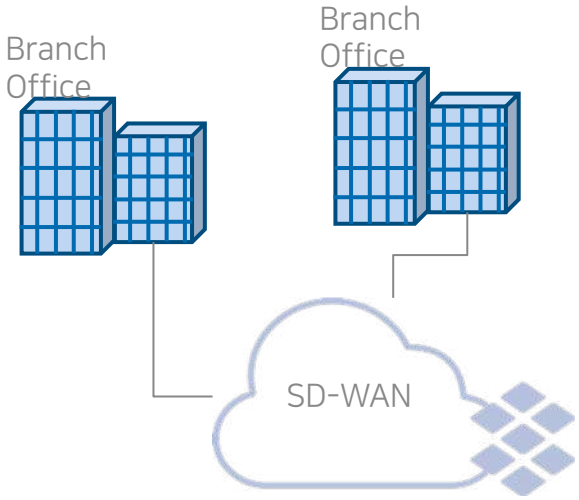
Source: Gartner

전통적 보안 모델은 변화하는 네트워크에 부적합

클라우드는 새로운 네트워크

Network 경계의 이동으로
고객은 어디에서나 클라우드로
직접 연결 시도

SD-WAN 기술로 네트워크의 전환 가속



인터넷에 직접 연결하는 원격 지사는
본사의 보안 수준을 갖추지 못함

IoT 기술로 디바이스의 폭발적인 증가

IoT와 같은 가벼운 장비에는
엔드포인트 보안을 배포하지 못하므로
침해 공격에 쉽게 악용됨

The Mantra, Zero Trust

Don’t treat packets as if they were people

Never trust, always verify

Assume breach

Verify explicitly

제로 트러스트의 기본 원리와 주요 기능

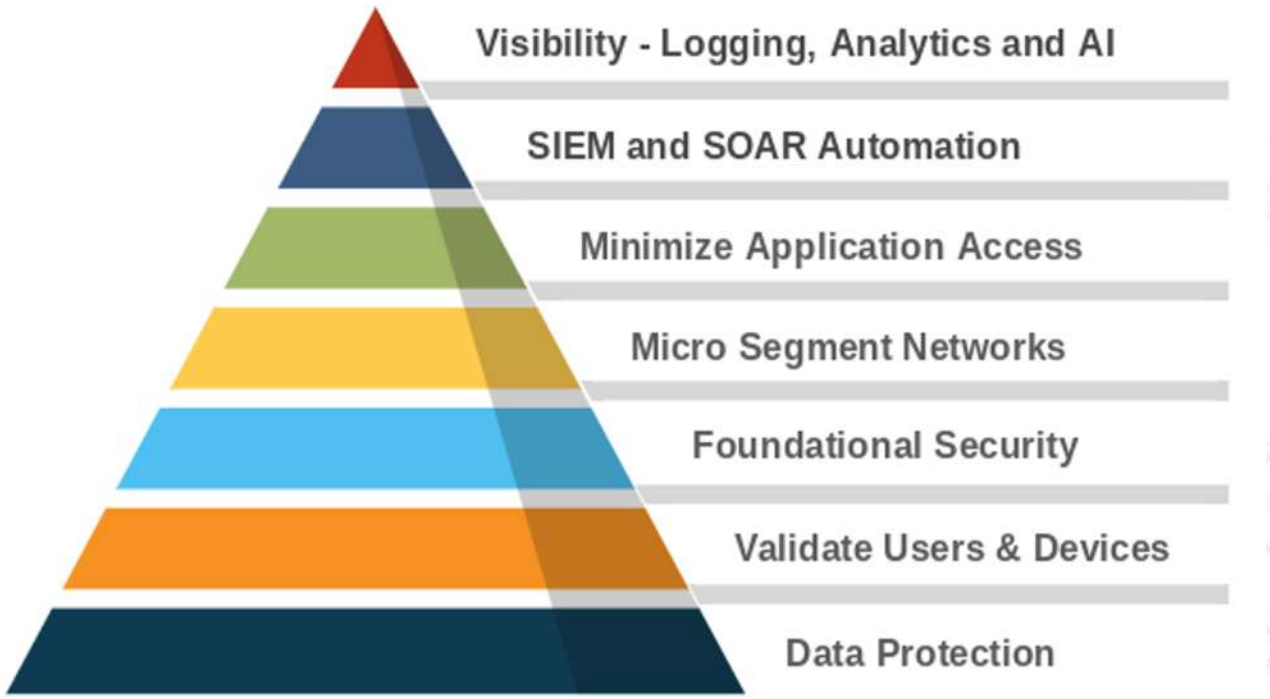
PROTECT DATA

UNDERSTAND DATA FLOW

MICRONETWORKS

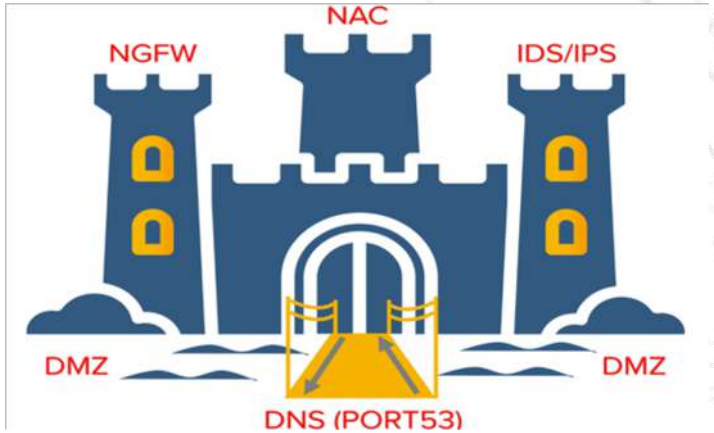
VISIBILITY & MONITORING

AUTOMATION



제로 트러스트 보안 컨트롤

- Micro-segmentation
- Foundational Security Using DNS
- Identity and Access Management (IAM)
- Two-Factor Authentication (2FA)
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation and Response (SOAR)
- Cloud Access Security Brokers (CASB) with Encryption, DLP and DRM
- Deception Technology
- Network Detection and Response (NDR)
- Endpoint Detection and Response (EDR)
- User and Entity Behavior Analytics (UEBA)
- Adaptive Access Control (AAC)



보안 위협의 진화

대응기술

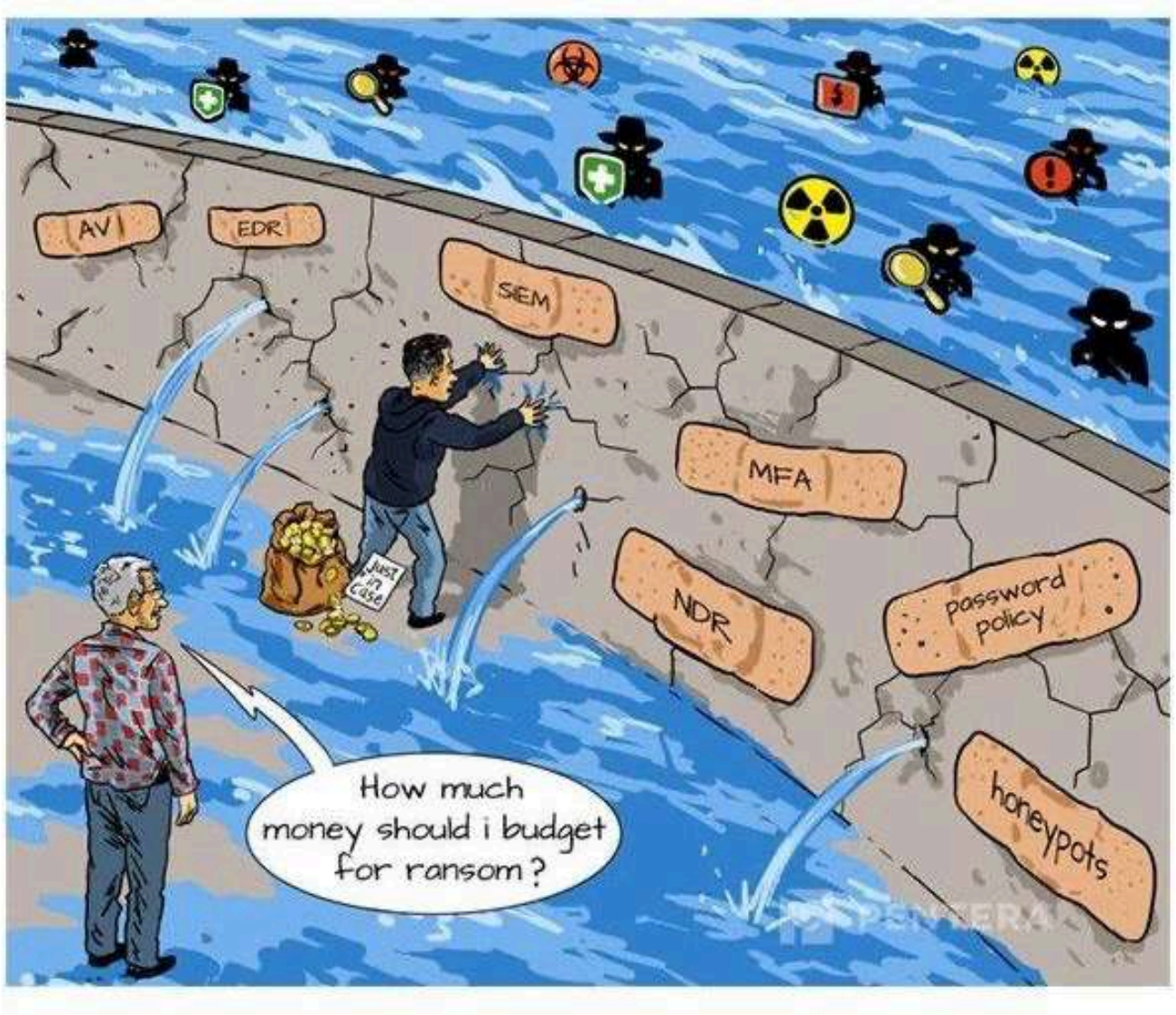
호스트 기반 (Anti-virus) 2000	네트워크 경계 보안 (IDS/IPS/FW) 2005	평판 기반 보안, NGFW & Sandboxing 2010	위협 인텔리전스 & 분석 Today

DNS Exploitation

증가하는 위협

 |

진화하는 위협의 대응에 비효율적인 보안 아키텍처



■2021년 하반기 주요 동향

21년 상반기 대비
악성코드 유포지 **23%** 증가

[자료=과기정통부 · KISA]

1 IoT 악성코드(Mozi) 관련 유포지 대량 탐지	2 Log4j 악성코드 유포 탐지
3 탐지된 경유지 관련 주요 업종 '제조', '건강/의학', '쇼핑'	4 다운로더 악성코드 유포 대량 탐지
5 가상통화 채굴 악성코드 유포 증가	6 정보유출 악성코드 유포 지속

Infoblox BloxOne Threat Defense

다양한 멀웨어 및 APT의 위협을
DNS 단계에서 빠르게 탐지 후 차단

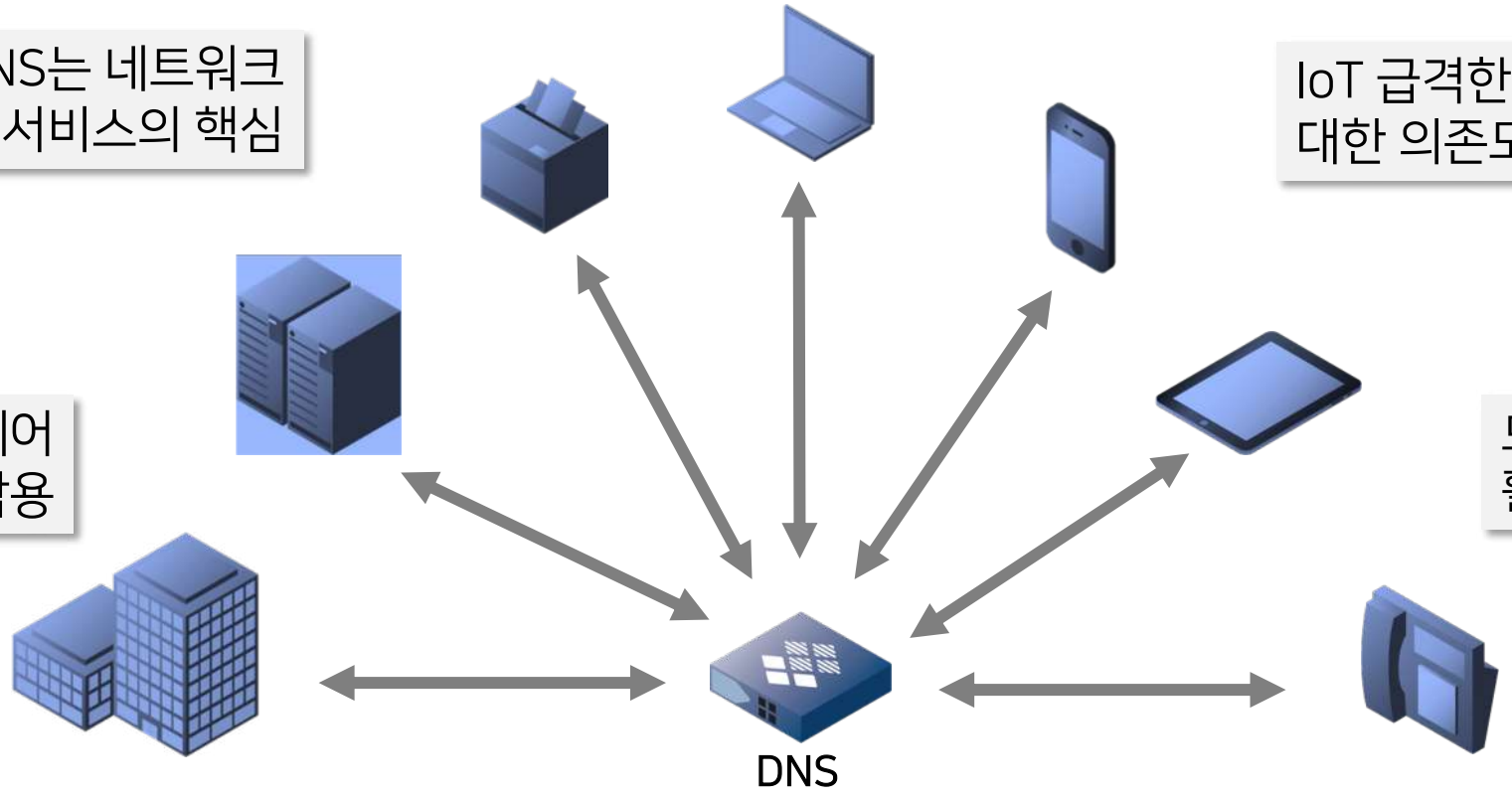
DNS는 제로 트러스트 보안을 위한 가시성 확보의 시작점

DNS는 네트워크 서비스의 핵심

IoT 급격한 증가로 DNS에 대한 의존도 향상

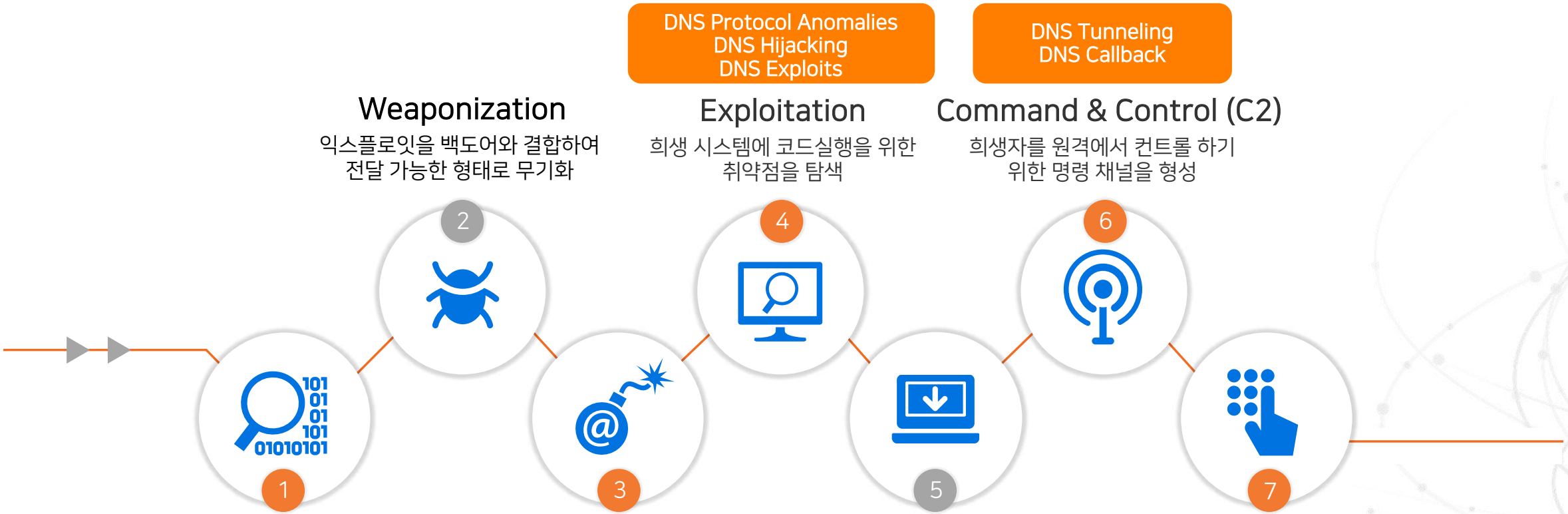
DNS는 멀웨어 활동에 악용

모든 기술에서 활용되는 DNS



"오늘날 거의 모든 온라인 커뮤니케이션 / 활동은 DNS 조회로 시작됩니다"

실제 92% 이상의 멀웨어 공격이 DNS 쿼리를 이용



 |

Gartner Research

Quick Answer: How Can Organizations Use DNS to Improve Their Security Posture?

Summary

DNS presents security and risk management leaders with some excellent opportunities to anticipate, prevent, detect and respond to prevailing threats. Organizations should implement DNS security to protect users, devices and other critical infrastructure.

Published: 08 June 2021

ID: G00723978

Analyst(s): Craig Lawson , John Watts

Table Of Contents

"DNS 의 보안으로, 목표 네트워크에 성공적으로 잠입하려는 멀웨어 공격의 92%를 줄일 수 있습니다."

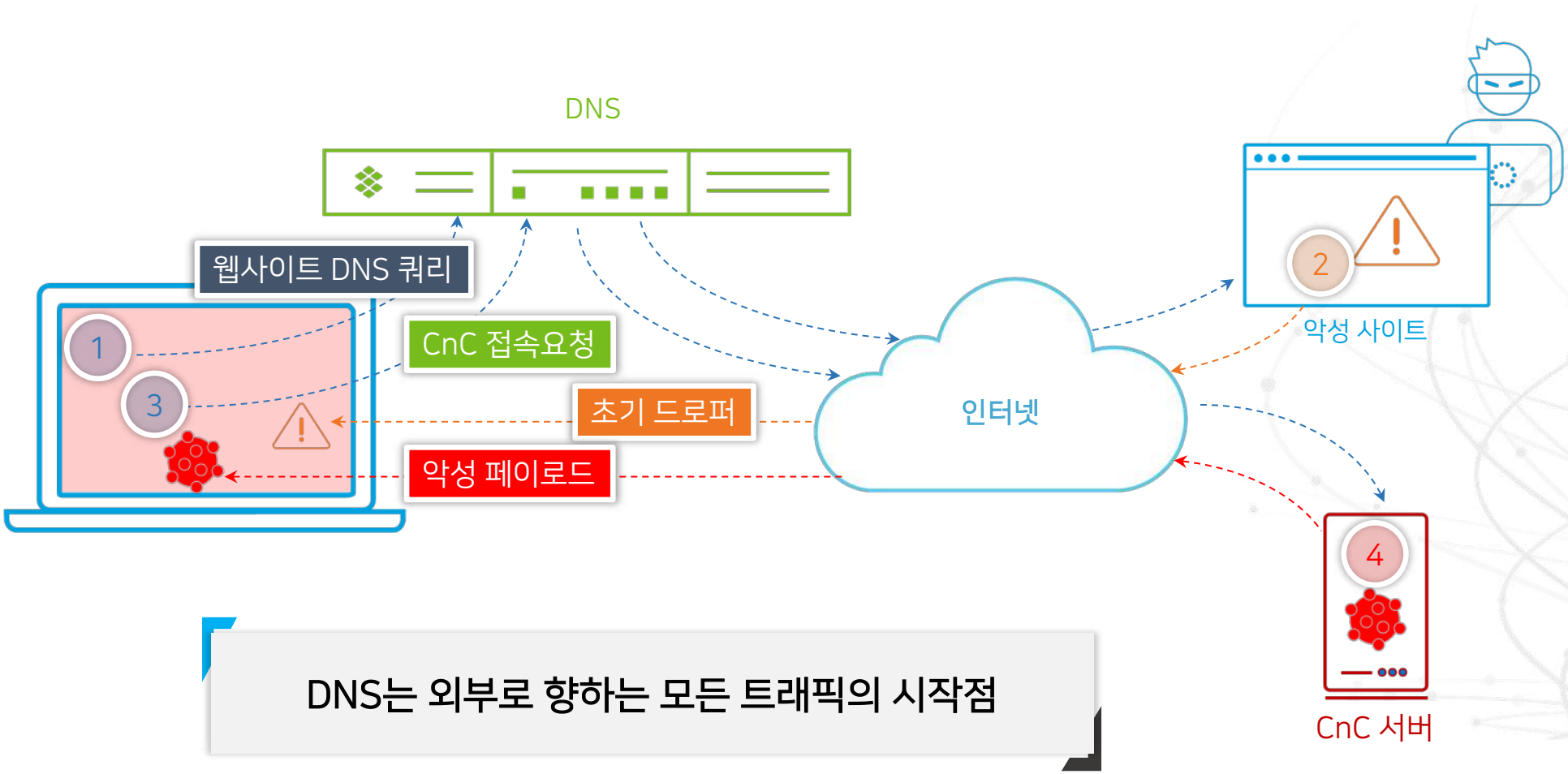
Anne Neuberger
Director, NSA Cybersecurity Directorate
(미국 국가안보국 사이버보안 국장)

 |

일반 DNS 서버를 통한 전형적인 멀웨어 / APT 침해 과정

- 멀웨어 공격의 95%가 DNS를 이용

1. 내부 사용자의 악성 사이트 접속
2. 웹사이트가 초기 드로퍼 전달
3. 설치된 드로퍼는 이후 CnC 연결
4. 악성 페이로드 다운로드

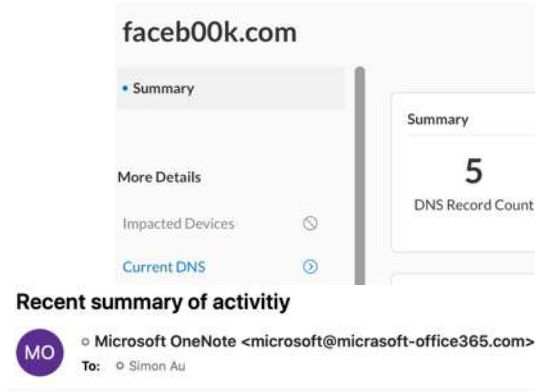


DNS는 외부로 향하는 모든 트래픽의 시작점

 |

악성 Domain, IP 주소의 위협 인텔리전스를 제공

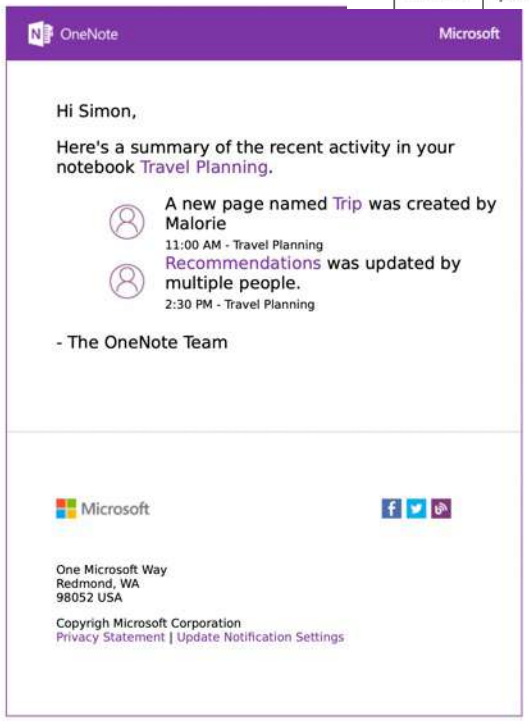
- 악성 피싱 이메일 링크
- Command&Control 트래픽
- 랜섬웨어 공격지
- 멀웨어 다운로드
- 침해된 IoT/OT 공격지
- 새롭게 등록된 도메인
- 유사 도메인 (Lookalike)

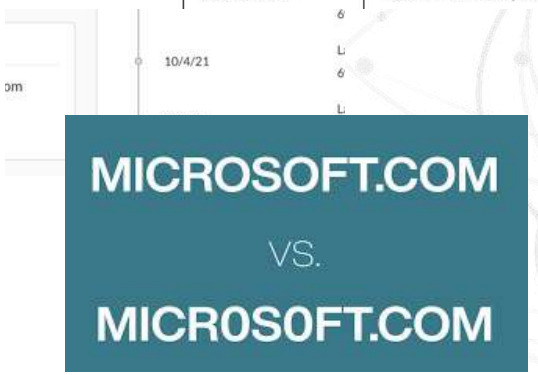


Infoblox will continue to monitor Log4j exploitation activity both internally and externally, as well as update this blog when new indicators are discovered.

Indicators Confirmed as Malicious

Type	IOC	Categorization	Notes
HOST	log[.]exposedbotnets[.]ru	malicious	Muhstik Botnet, C2
HOST	abrahackbugs[.]xyz	malicious	Elknot Botnet, C2
HOST	cuminside[.]club	malicious	Elknot Botnet, C2
HOST	m3[.]wtf	malicious	Elknot Botnet, C2
HOST	pwn[.]af	malicious	Elknot Botnet, C2

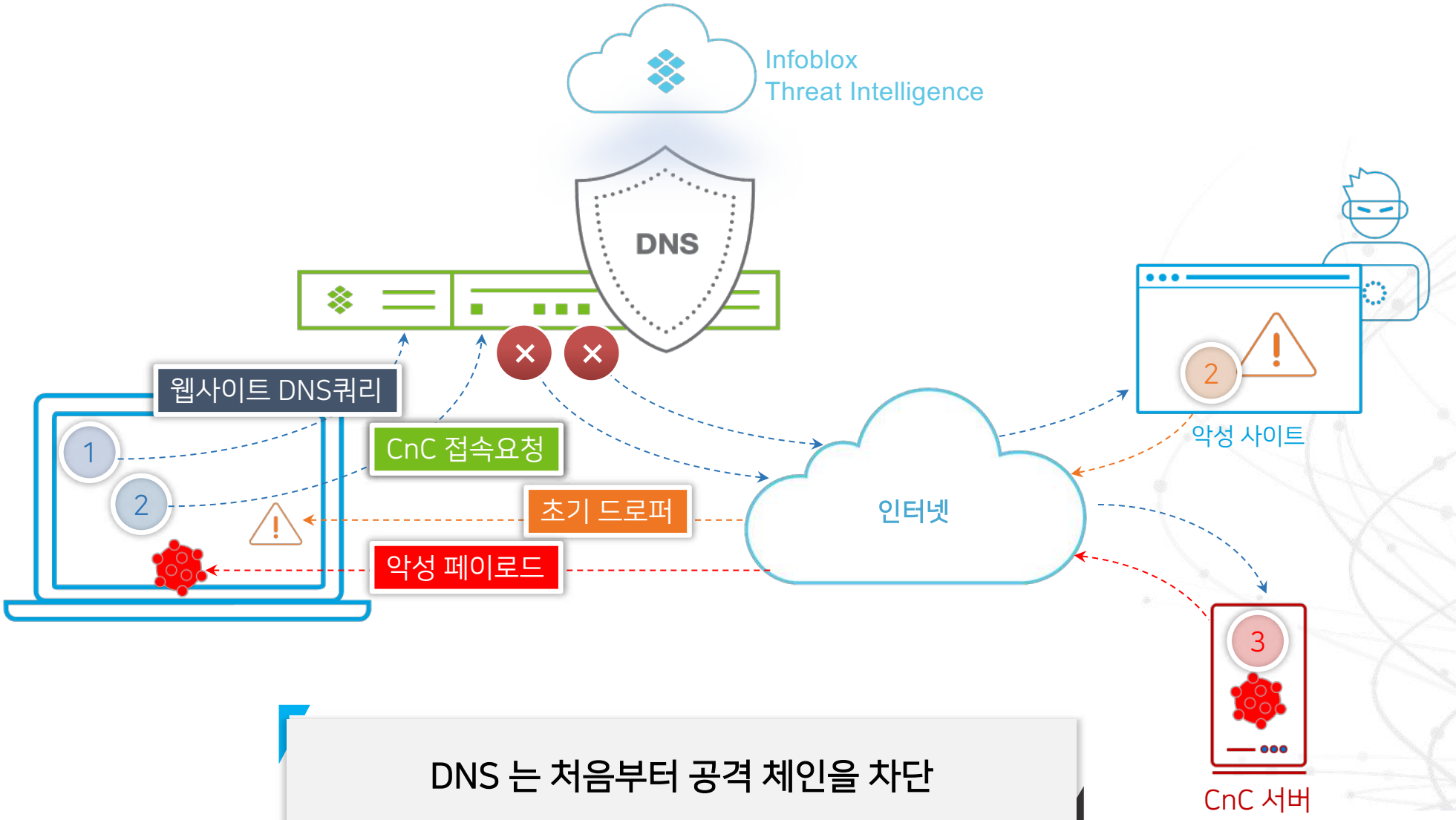




https://www.apple.com
https://www.apple.com

DNS 보안으로 멀웨어 공격 차단

1. DNS를 위해 준비된 위협 인텔리전트
2. DNS에서 악성 웹사이트 연결 차단
3. 이미 감염된 단말인 경우, DNS에 CnC로 연결을 요청할 때 차단



DNS 는 처음부터 공격 체인을 차단

 |

What we found?

실제 DNS 트래픽에서 Infoblox B1TD가 검출한 위협

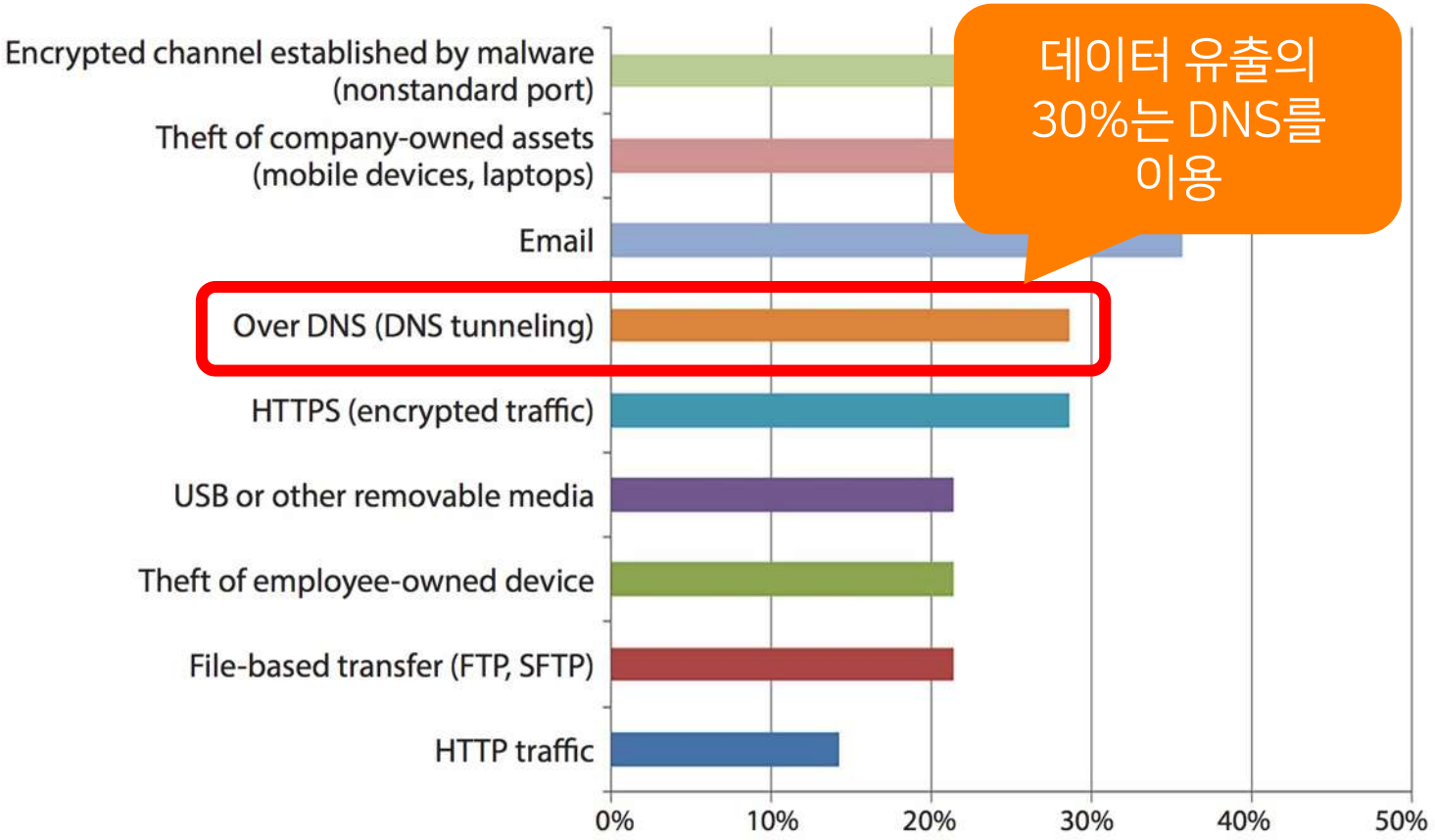
COUNT	THREAT CLASS	
89,650	MalwareC2	악의적인 해커가 봇넷의 봇 노드를 제어하는 서버로 네트워크의 명령을 전달하는 센터 역할을 함
81,019	Cryptocurrency	Cryptomining 멀웨어는 기업 리소스를 남용하여 비용을 증가시키고 조직을 위험에 더 많이 노출
60,299	MalwareC2DGA	DGA는 C&C 서버와의 통신 지점으로 사용할 수 있는 도메인을 대량으로 주기적으로 생성하는 알고리즘
26,861	MalwareDownload	멀웨어를 이용한 악의적인 활동을 위한 소프트웨어를 다운받는 행위
4,453	Data Exfiltration	DNS를 사용하여 차세대 방화벽, DLP, IDS 및 IPS를 쉽게 우회하여 조직에서 데이터를 무단으로 반출하는 공격 기법
3,967	Proxy	감염 단말이 프록시 서버로 파일, 연결, 웹 페이지 또는 다른 서버에서 사용할 수 있는 기타 리소스 등을 요청
2,595	Phishing	신뢰할 수 있는 것처럼 보이는 가짜 웹사이트나 이메일을 사용하여 사용자 이름, 암호 또는 개인 정보를 탈취

Infoblox BloxOne Threat Defense

DNS를 악용한 데이터 유출 시도 차단

내부 데이터 유출에 사용되는 경로

- 실제 침해를 받은 사례 조사 결과



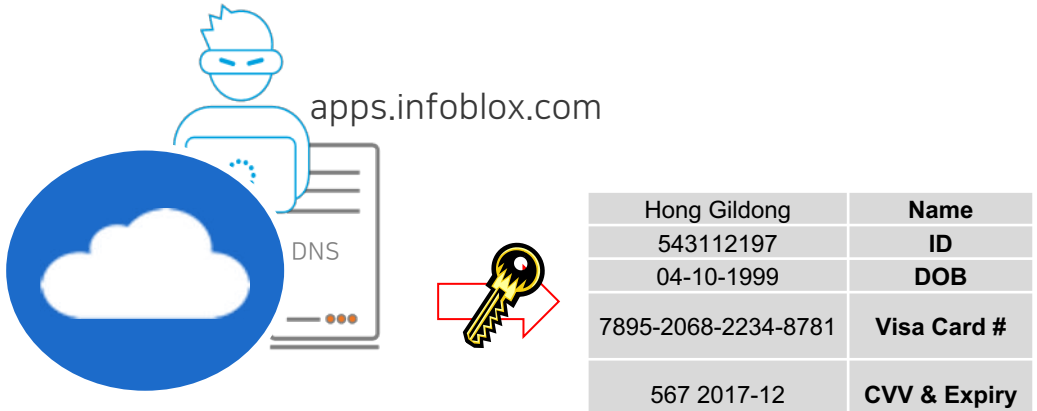
Malware / Group	Discovered	DNS Communication
Sunburst	2020	C2
Godlua	2020	C2
Quadagent / OilRig	2020	C2 / exfil / infil
Anchor_DNS / Trickbot	2019	C2 / exfil / infil
PsiXBot	2019	C2
Alina	2019	C2 / exfil
RogueRobin / DarkHydrus	2018	C2 / exfil / infil
	2018	C2 / exfil
	2017	C2 / exfil / infil
	2017	C2 / exfil / infil
	2017	C2 / infil
	2017	C2 / infil
	2017	C2
Trojan.Win32.Ismdoor.gen	2017	C2 / exfil
Wekby	2016	C2
Multigrain POS	2016	Exfil
ProjectSauron / Strider (NSA?)	2016	C2 / exfil
C3PRO-Raccoon	2015	C2
FrameworkPOS	2014	exfil
PlugX v2	2014	C2
CobaltStrike (pentesting tool)	2013	C2 / exfil / infil
FeederBot	2011	C2
Morto	2011	C2

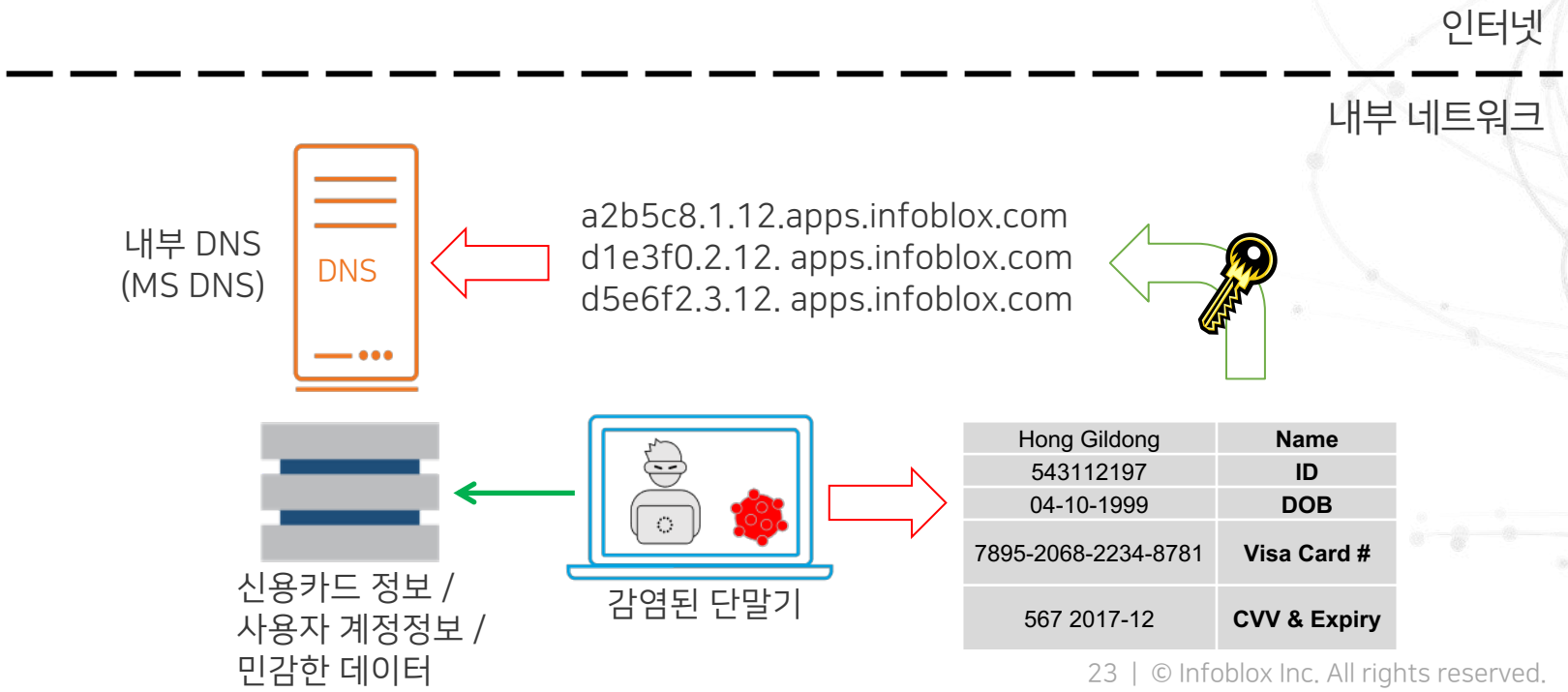
대부분 공격에서 DNS 통신을 악용

Source: SANS Data Protection Survey

Zero-Day DNS 공격 – DNS를 통한 데이터 유출

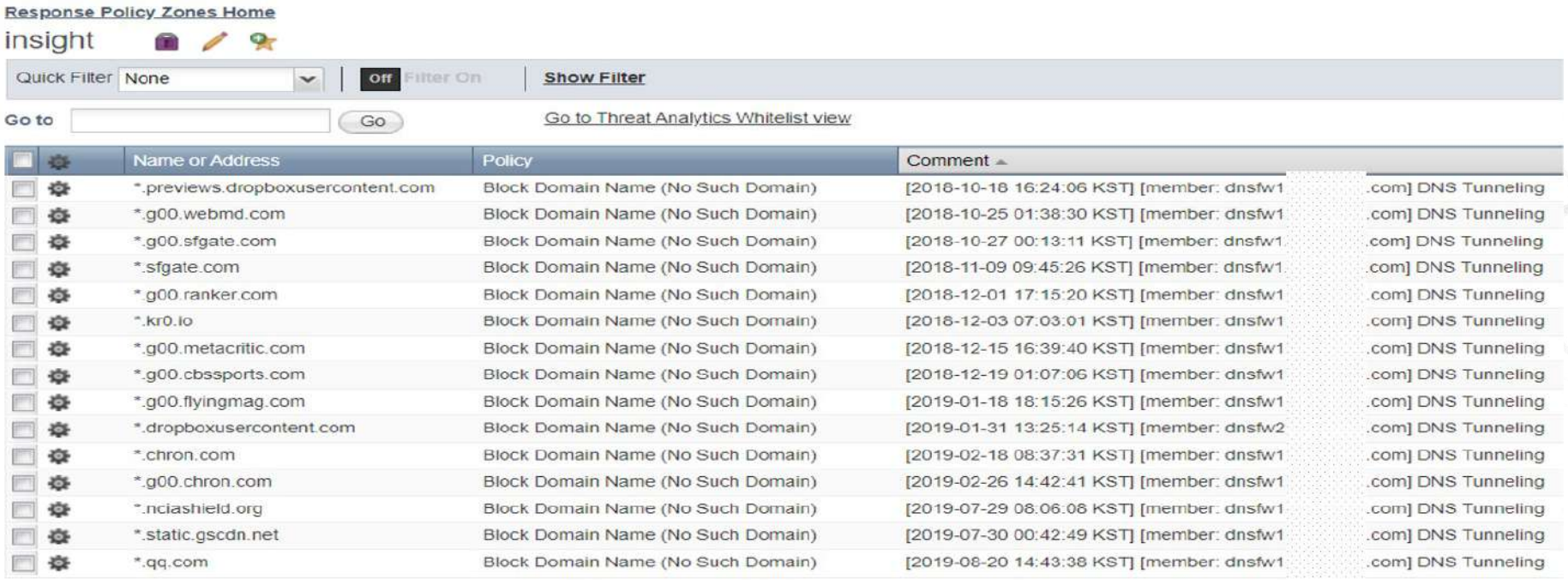
1. 감염 디바이스에서 민감한 데이터 조회
2. 멀웨어는 DNS 채널을 통해 데이터 전송
3. 레거시 보안 장비는 DNS 패킷 통과





사례 #1 - DNS를 통한 데이터 유출 시도 차단 (국내 대기업)

- Infoblox DNS 장비에서 DNS Tunneling 기법을 이용한 데이터 유출 시도를 탐지 후 자동 차단
- DNS Tunneling 은 형식적으로는 DNS 프로토콜 통신이므로 기존 방화벽 등은 정상 DNS 요청으로 인식하여 허용
- ML/AI 엔진에 의한 연속된 행위 분석으로 공격을 식별하고 차단 정책에 의해 세션을 차단



Response Policy Zones Home

insight

Quick Filter None | Off Filter On | Show Filter

Go to | Go | Go to Threat Analytics Whitelist view

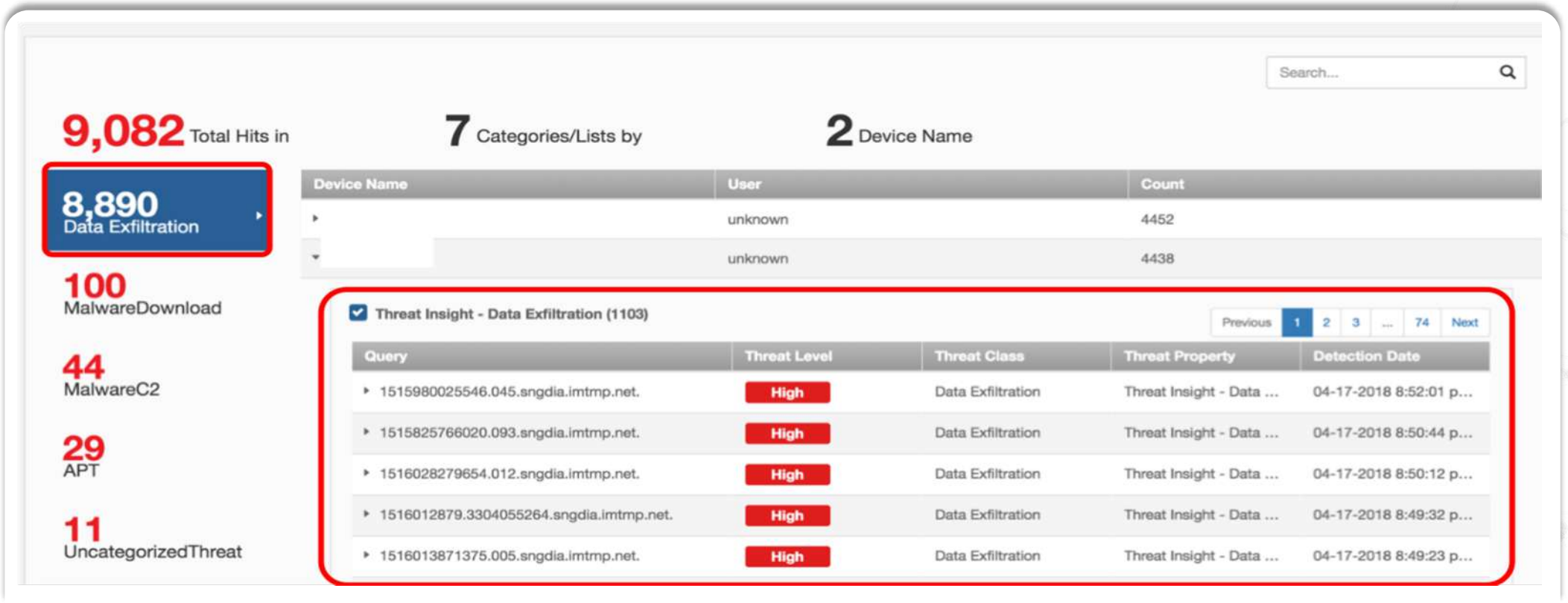
Name or Address	Policy	Comment
*.previews.dropboxusercontent.com	Block Domain Name (No Such Domain)	[2018-10-18 16:24:06 KST] [member: dnsfw1 .com] DNS Tunneling
*.g00.webmd.com	Block Domain Name (No Such Domain)	[2018-10-25 01:38:30 KST] [member: dnsfw1 .com] DNS Tunneling
*.g00.sfgate.com	Block Domain Name (No Such Domain)	[2018-10-27 00:13:11 KST] [member: dnsfw1 .com] DNS Tunneling
*.sfgate.com	Block Domain Name (No Such Domain)	[2018-11-09 09:45:26 KST] [member: dnsfw1 .com] DNS Tunneling
*.g00.ranker.com	Block Domain Name (No Such Domain)	[2018-12-01 17:15:20 KST] [member: dnsfw1 .com] DNS Tunneling
*.kr0.io	Block Domain Name (No Such Domain)	[2018-12-03 07:03:01 KST] [member: dnsfw1 .com] DNS Tunneling
*.g00.metacritic.com	Block Domain Name (No Such Domain)	[2018-12-15 16:39:40 KST] [member: dnsfw1 .com] DNS Tunneling
*.g00.cbssports.com	Block Domain Name (No Such Domain)	[2018-12-19 01:07:06 KST] [member: dnsfw1 .com] DNS Tunneling
*.g00.flyingmag.com	Block Domain Name (No Such Domain)	[2019-01-18 18:15:26 KST] [member: dnsfw1 .com] DNS Tunneling
*.dropboxusercontent.com	Block Domain Name (No Such Domain)	[2019-01-31 13:25:14 KST] [member: dnsfw2 .com] DNS Tunneling
*.chron.com	Block Domain Name (No Such Domain)	[2019-02-18 08:37:31 KST] [member: dnsfw1 .com] DNS Tunneling
*.g00.chron.com	Block Domain Name (No Such Domain)	[2019-02-26 14:42:41 KST] [member: dnsfw1 .com] DNS Tunneling
*.nciashield.org	Block Domain Name (No Such Domain)	[2019-07-29 08:06:08 KST] [member: dnsfw1 .com] DNS Tunneling
*.static.gscdn.net	Block Domain Name (No Such Domain)	[2019-07-30 00:42:49 KST] [member: dnsfw1 .com] DNS Tunneling
*.qq.com	Block Domain Name (No Such Domain)	[2019-08-20 14:43:38 KST] [member: dnsfw1 .com] DNS Tunneling

사례 #2 - DNS를 통한 데이터 유출 위험 대응 (국내 은행)

- 금융회사 대상으로 금융감독기관의 DNS를 통한 데이터 유출 취약점 점검
- 간단한 설치 구성으로 Infoblox 특허의 ML/AI 을 활용한 차단 효과 검증 후 도입
- DNS를 통한 데이터 유출 방어 뿐만 아니라 Zero-day 공격, 멀웨어, APT 공격 차단에도 높은 효과

사례 #3 - DNS를 통한 데이터 유출 시도 차단 (외국 정부기관)

- DNS Tunneling 기법을 이용한 데이터 유출 시도를 탐지 후 자동 차단 – 약 9,000 번의 악성 쿼리를 차단
- 연휴 기간 동안 정부 기관 대상으로 공격 시도, Infoblox 머신러닝 엔진의 행위 분석으로 식별 후 차단
- 기타 멀웨어 유포사이트, C2, APT 등 악성 URL의 쿼리 요청을 탐지, 차단한 이력 확인



 |

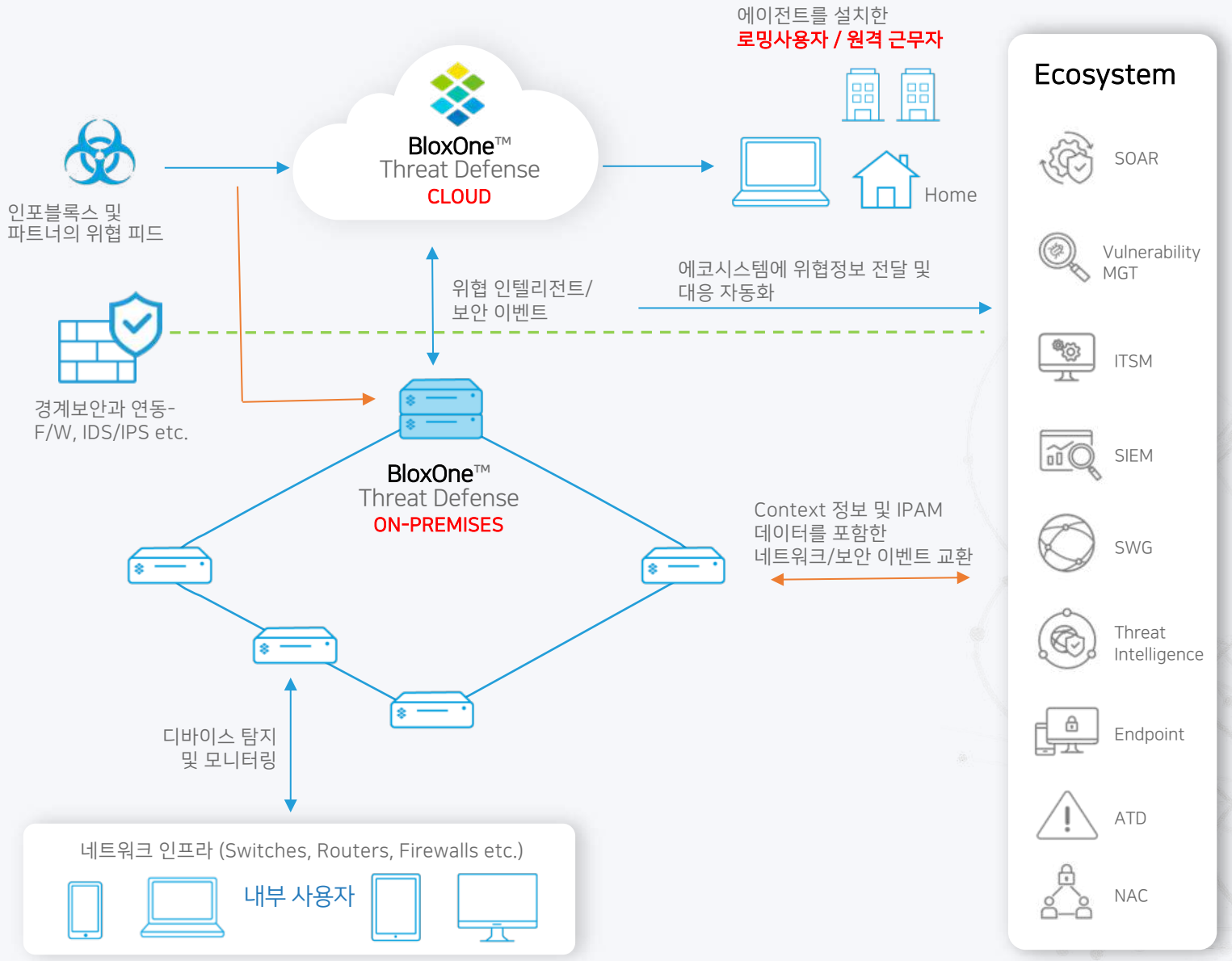
Infoblox BloxOne Threat Defense

- 위치에 관계없이 사용자, IoT 기기 모두를 보호
- 정교한 데이터 유출 행위를 탐지하는 Infoblox ML/AI 기술
- 수많은 지능형 공격 방어에 높은 ROI 효과
- 보안 스택과 강력한 연동으로 자동화 지원

BloxOne™ Threat Defense

DNS 단계에서 악성 트래픽 제거

- 최신 멀웨어, C&C 위협 도메인 식별 후 차단 (DNS쿼리 단계에서 미리 차단)
- 지능화된 데이터 유출 공격 차단 (Data exfil, DGAs)
- Infoblox Threat Intelligence를 기존 내부 에코시스템과 통합
- 내부 보안 솔루션과 연동 및 자동화로 SOC 효율 극대화
- 하이브리드 환경 지원 (클라우드, 온프레미스, 재택근무자 보안 통합)



 |

Threat Insight - 지능형 위협 탐지

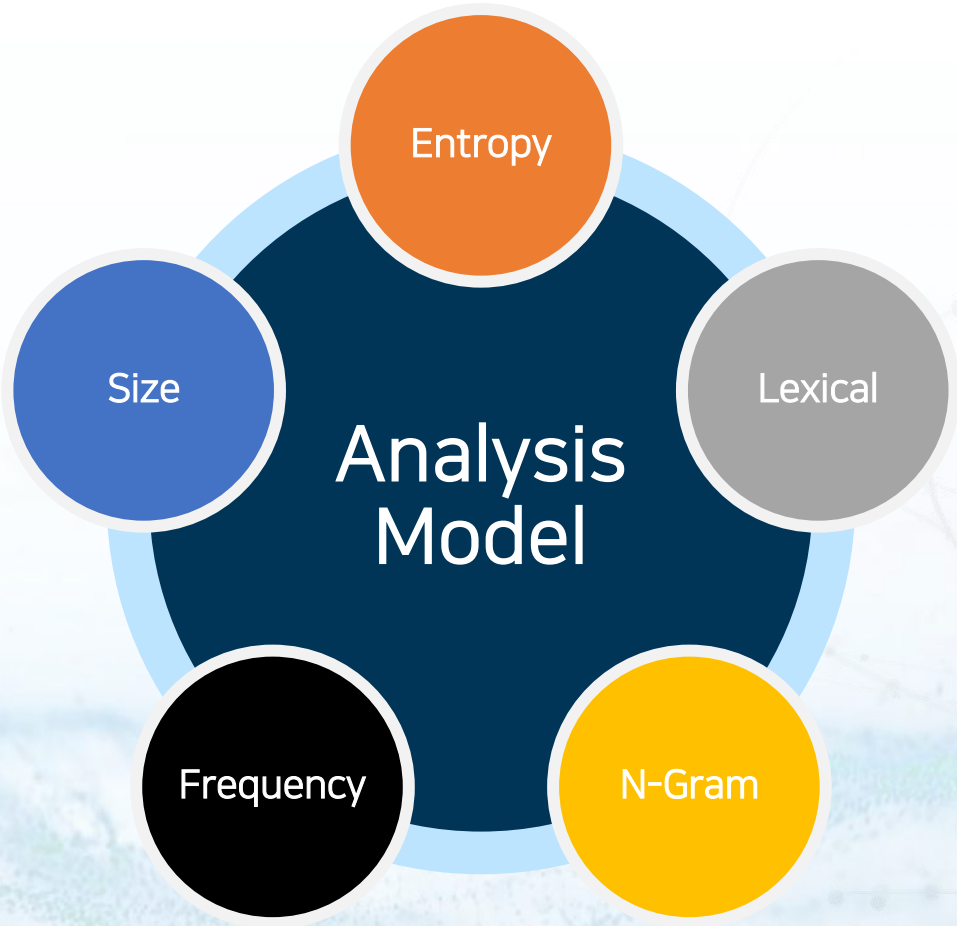
- DNS Tuned Threat Intelligence + Analytics + Infoblox Cyber Intelligence Unit

✓ 머신 러닝 (ML/AI) 기반의 행위 분석

- Data 유출/멀웨어 침투 (Exfiltration/Infiltration) 차단에 최적화
- Infoblox의 특허 기술로 5가지 분석 모델을 통한 최상의 DNS
- Signature 기반 보안솔루션은 검출하기 어려운 DGA, Fast Flux 등의 변칙적인 공격도 탐지
- Fileless Malware, Zero-day 등의 최신 위협에 대한 대응 기술

✓ 매우 정교한 IOCs

- 광범위한 IOC 네트워크를 활용하여 다양하고 강력한 보안 제공
- Infoblox 분석 팀의 리버스 엔지니어링으로 최상의 대응 방안 제공
- 오랜 노하우를 반영한 자체 알고리즘으로 False Positive 최소화
- 고객의 비즈니스를 연속성을 위해 가장 최신의 위협으로부터 보호
  ransomware, malware C&C, phishing, exploit kits, APTs



 |

인프라 보안 운영 구조 최적화

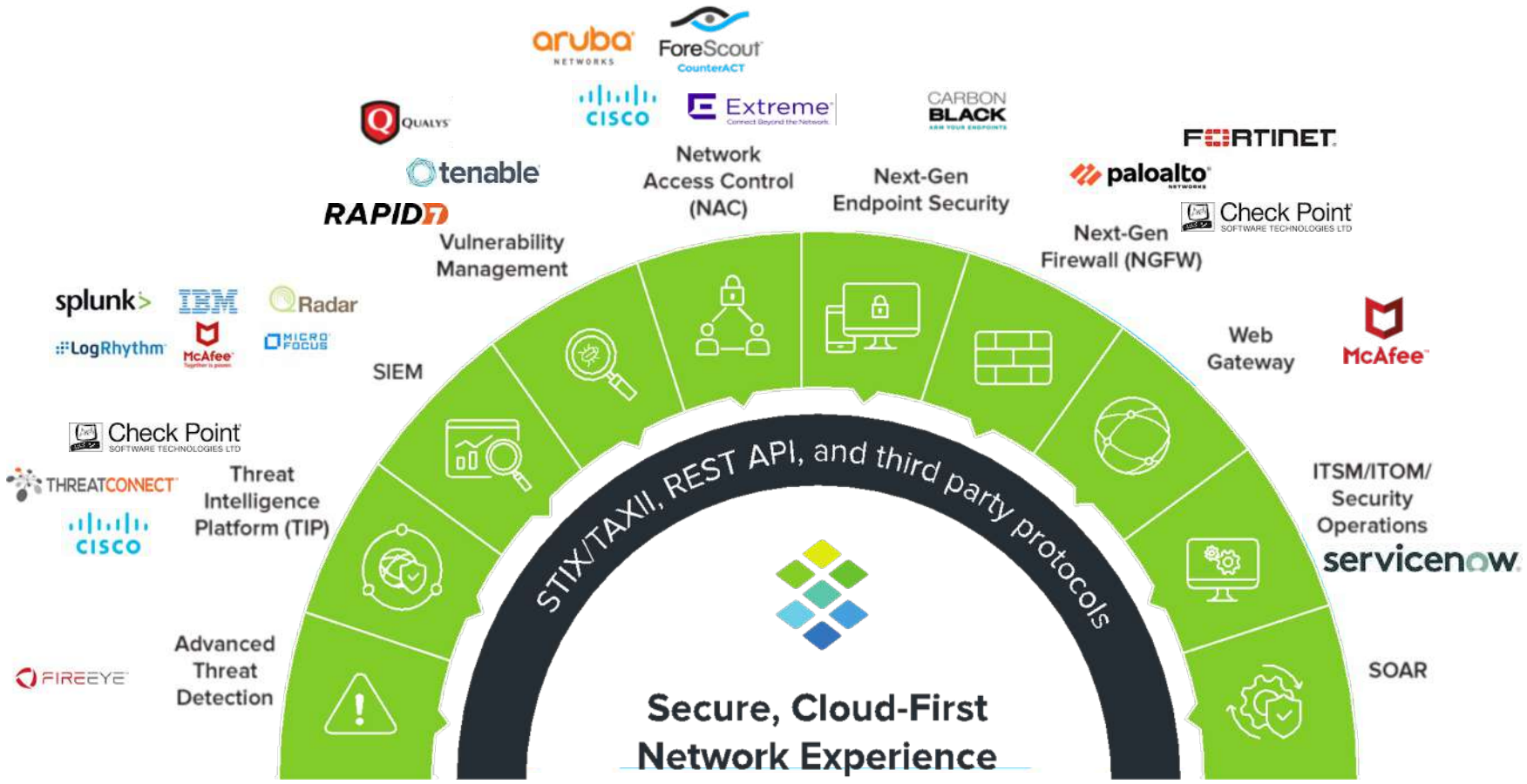
경계 보안의 가용 성능 확보

- 알려진 위협 차단으로 부하 감소
- NGFW, SWG, IDS/TPS 가 감당할 "Junk Traffic" 을 사전 제거
- 경계 보안이 탐지하지 못하는 위협 대응 – 데이터 유출, 피싱, APT

모든 디바이스의 보호

- **DHCP, IPAM, DNS 기반의 통제**
- 보안의 확장
  - 모든 엔터프라이즈 디바이스
  - 모든 IoT 디바이스
  - 원격 사용자/WFA

보안 운영 자동화 – Ecosystem



https://www.infoblox.com/products/cybersecurity-ecosystem/

수많은 경고 우선순위 처리 | 이벤트 조치 신속 대응 | 휴먼 에러 최소화

자동화 연동을 위한 정보 공유

DHCP

디바이스 핑거프린팅과 감사 추적

- 디바이스 정보, Mac, IP임대 정보

IPAM

응용프로그램과 비즈니스 관련 정보

- 확장 속성들의 메타데이터: 소유자, 위치, 연결된 스위치 및 무선 AP 등, Port 및 Vlan정보
- 정확한 위험 분석과 대응할 이벤트 선별을 위한 상황정보

DNS

- 보안 경계내에서의 해로운 활동들
- BYOD와 IoT 디바이스들이 DNS client 로 동작
- 디바이스 프로파일 및 사용자 활동들

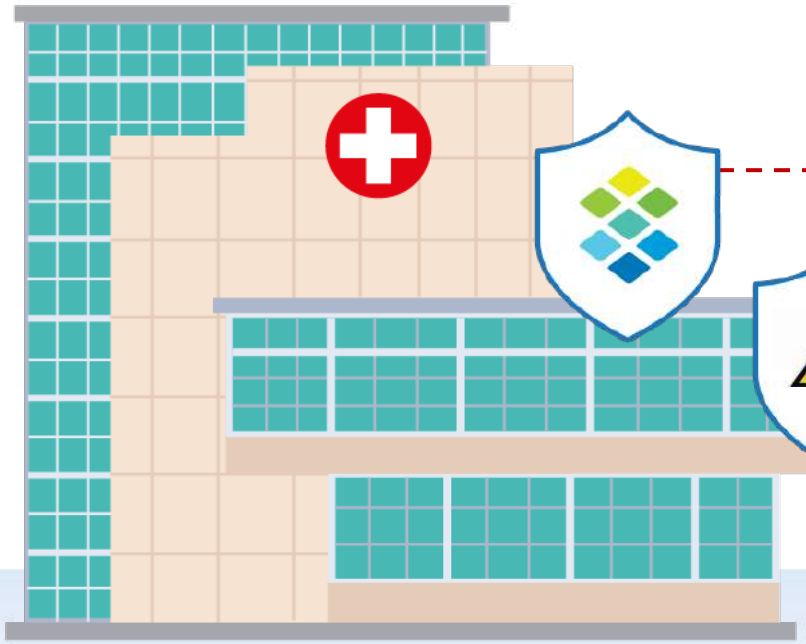
국내 고객 사례 : 국내 대기업 도입 효과

- 내부 BIND 서버의 CPU, 서비스 등 부하 감소
- 방화벽, ATP 등의 보안 솔루션에서 탐지율 감소 및 분석 용이
- Data Tunneling 공격으로 인한 Data 유출 차단
- 리포팅을 통한 악성 Client 식별 및 불필요한 도메인 쿼리 분별
- Malware, Ransomware 감염 감소
- CPU, Memory, 서비스, 리포팅 사용량 등을 1달 이상 데이터로 확인
- 악성 도메인을 조사하기 위한 Security Portal 제공
- 악성 도메인이 아니더라도, 원하는 도메인 차단 가능 (게임, 도박 등..)
- 도메인 뿐만 아니라, IP 기반으로도 차단 가능

Forrester Consulting 의 조사 결과
- Total Economic Impact™ (TEI)
- Return of Investment (ROI)

해외 고객 사례 - 대형 병원

1. 고객 정보 및 진료 정보 유출에 대해 매우 우려하는 병원 관계자



2. 모니터링 모드로 즉각적인 분석 진행

3. 24시간도 안돼서 Infoblox 솔루션은 데이터 유출 위협을 감지

4. SECOPS 팀에서 사용 중인 보조 도구를 분석해보니, 일부 문제를 감지했으나 너무 많은 알림으로 조치 어려움

5. SECOPS는 Infoblox가 즉각적으로 위협을 감지했다는 사실을 알게 되어 만족하여 바로 차단 모드로 전환

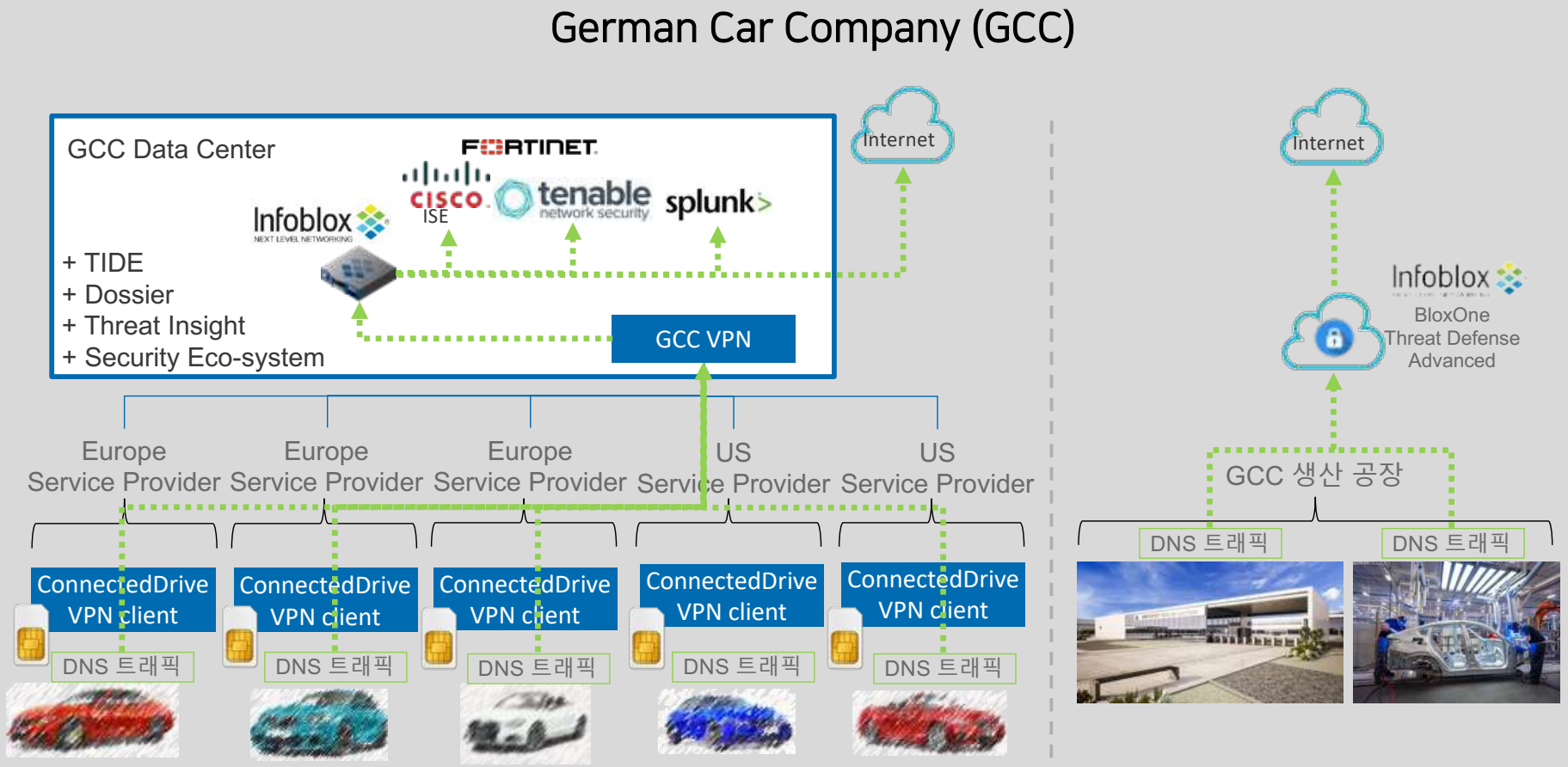
Value to customer:

- **배포 용이성:** 기존의 DDI 인프라에 즉시 적용하여 보안성 향상
- **데이터 보호:** 고객 정보의 유출 시도를 즉각적으로 탐지하고 차단
- **브랜드 보호:** 병원 평판이 무너질 수 있는 사건사고로부터 대비

해외 고객 사례 - 독일 자동차 기업

Value to customer:

- **보안 수준 향상:** TIDE의 위협 정보를 통합하여 전반적 보안 능력 향상
- **운영 효율성 향상:** Ecosystem 연동을 통한 자동화, Dossier로 이슈 분석 리드타임 축소
- **전사 보안 향상:** 보안 적용이 어렵고 매우 민감한 자동차, IoT에 특화된 보안 설계로 위협으로부터 안전한 서비스 제공



자동차에 SIM카드를 통한 Connected Drive 기능을 제공 (TeleService, 컨시어지 서비스, 인터넷, 실시간 트레픽 정보수신)

맺음말

- DNS는 모든 디바이스가 경유하는 새로운 경계
- Infoblox는 점점 정교해지는 사이버위협을 손쉽게 방어
- Infoblox의 클라우드 플랫폼으로 위치에 관계없이 디바이스를 보호
- Infoblox 는 고객의 제로 트러스트 보안 전략에 새로운 비전을 제공


감사합니다.