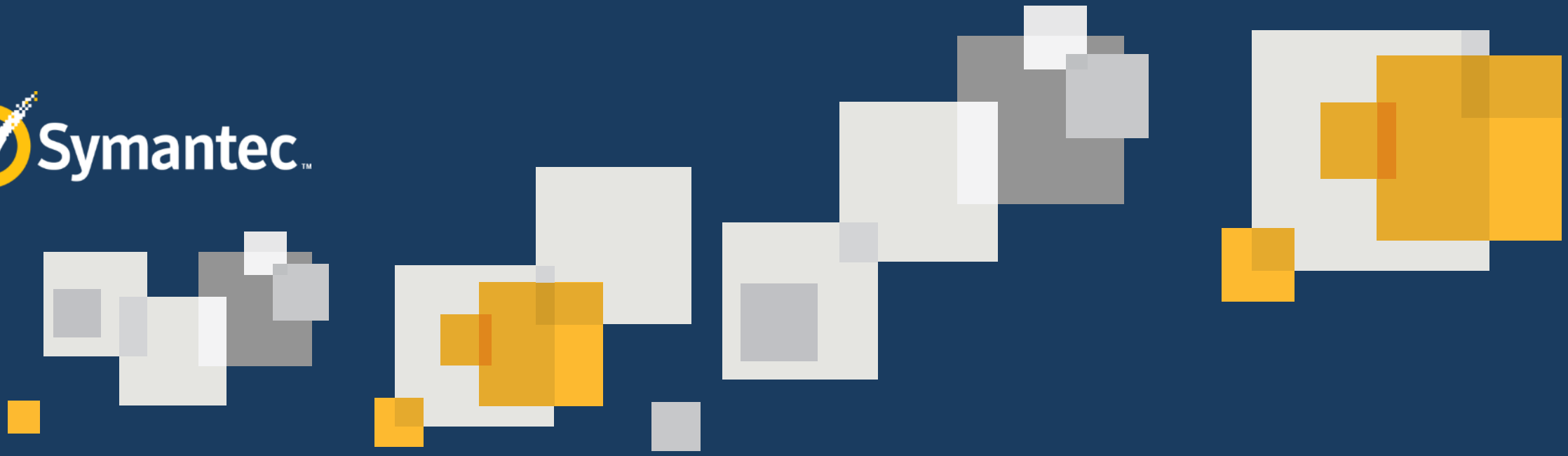


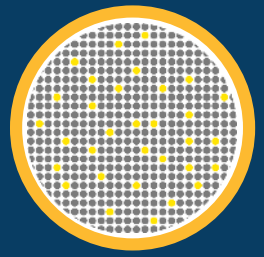
NEW 시만텍의 통합 사이버 보안 전략

서종렬 상무/시만텍 코리아

Agenda

1	보안 동향
2	시만텍 보안 전략
3	보안 전략 구현을 위한 핵심 솔루션

New Symantec | 요약



1억7천5백만
엔드포인트 보호

$46억불
연간 매출

2,123
특허

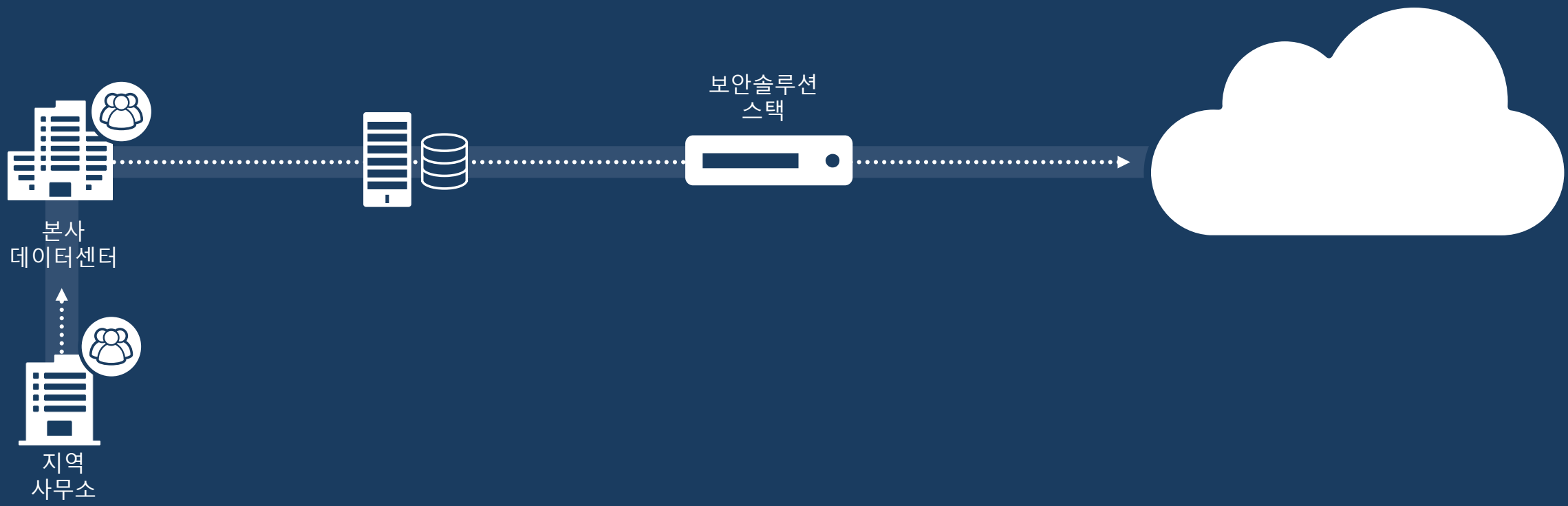
385,000
전세계 고객

3,000+
연구개발인력

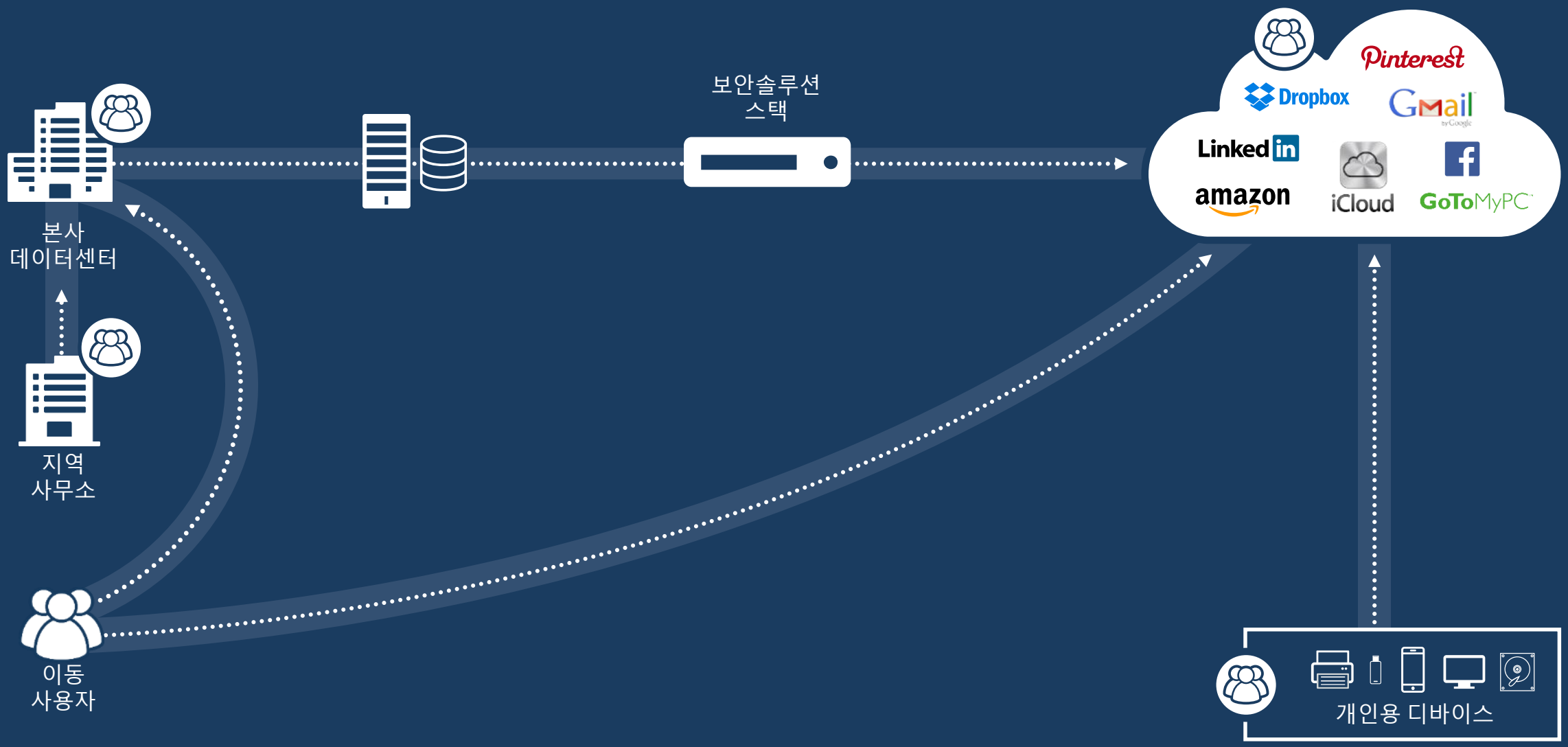
6 SOCs
보안 관제 센터


Office 365
servicenow
box
Dropbox
salesforce
workday
successfactors
An SAP Company
› 사용자 정의의 곤란
› 데이터 공격의 진화
› 네트워크 경계선의 확장
› 단계별 공격

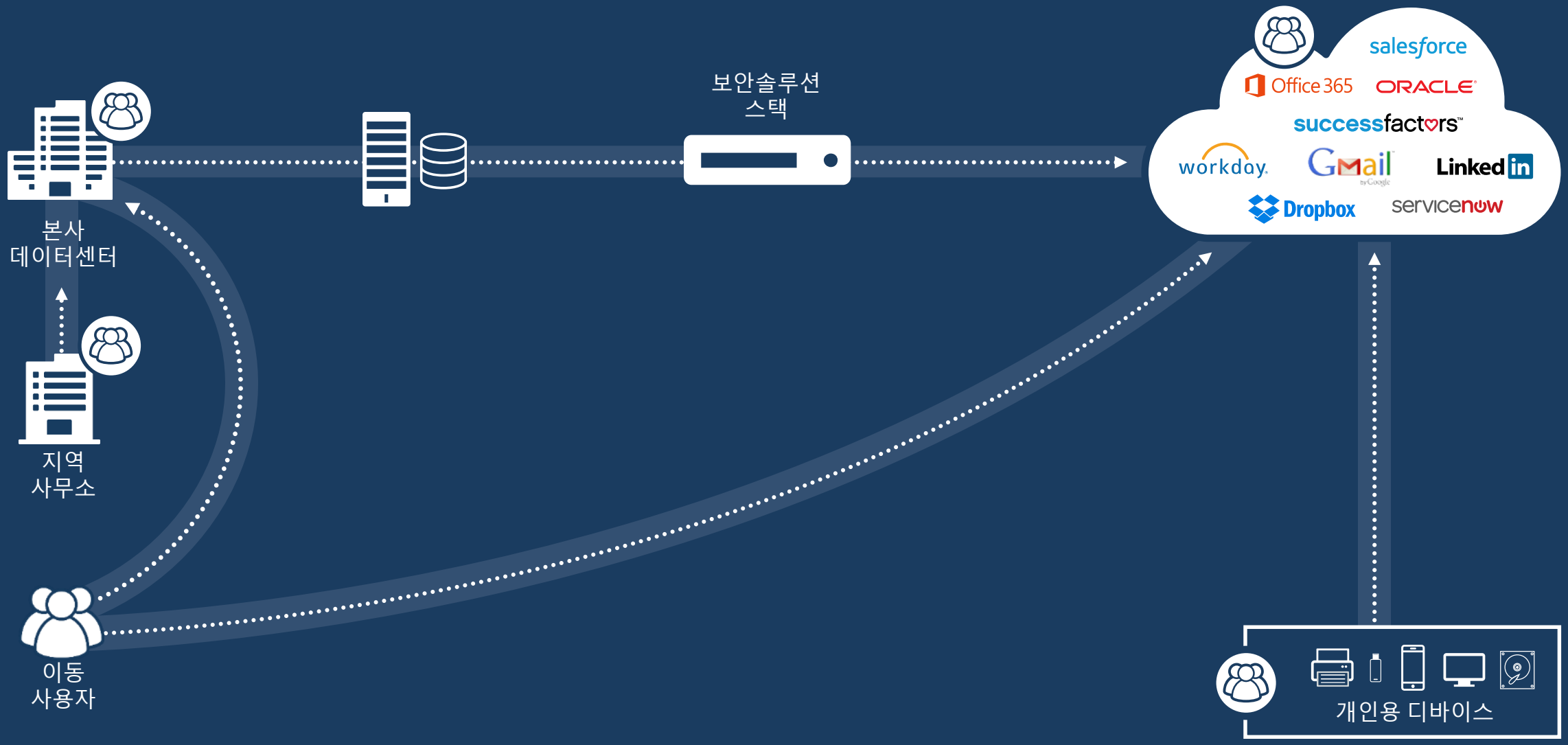
사용자 정의 곤란



사용자 정의 곤란

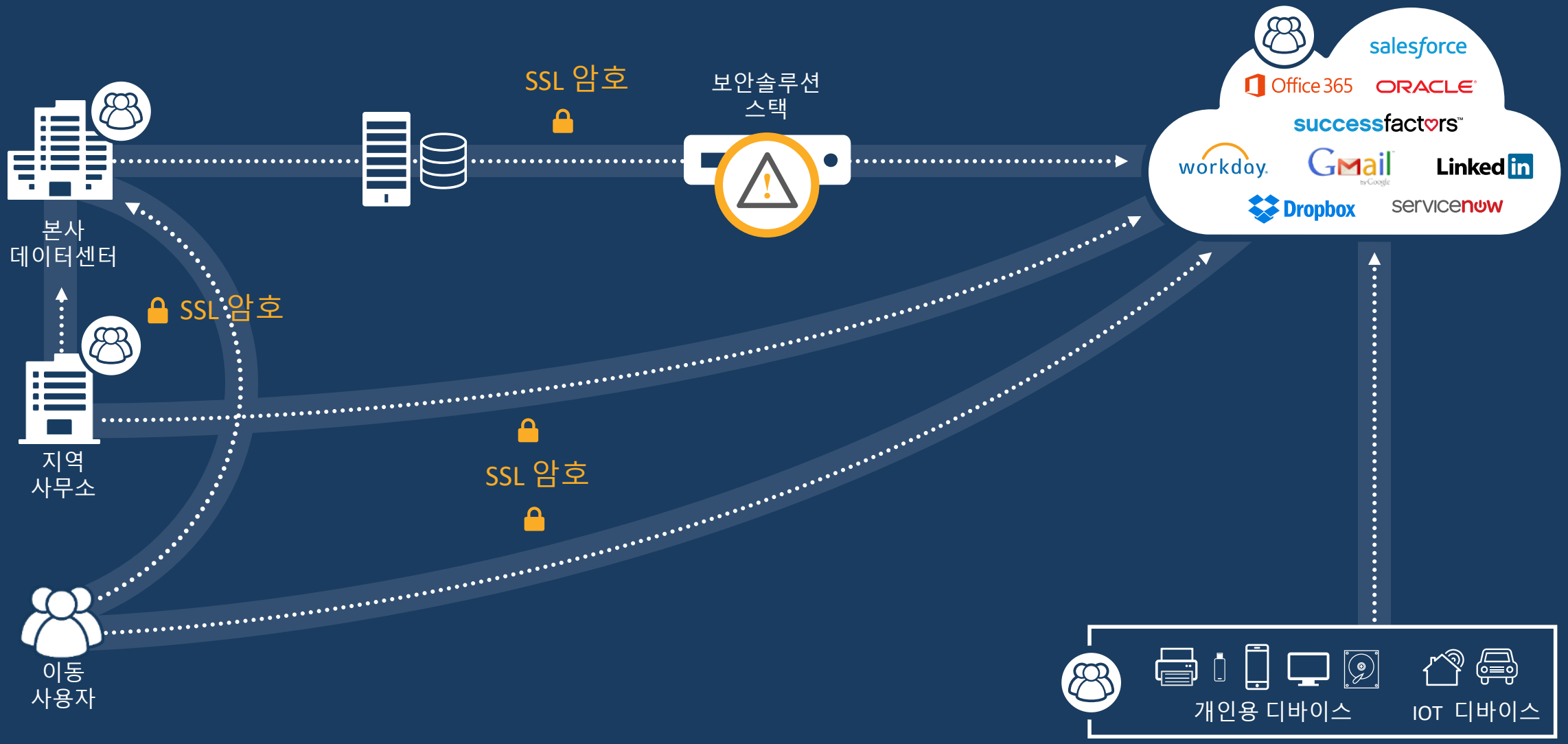

보안솔루션
스택
Pinterest
Dropbox
Gmail
LinkedIn
amazon
iCloud
GoToMyPC
본사
데이터센터
지역
사무소
이동
사용자
개인용 디바이스

데이터 공격의 진화

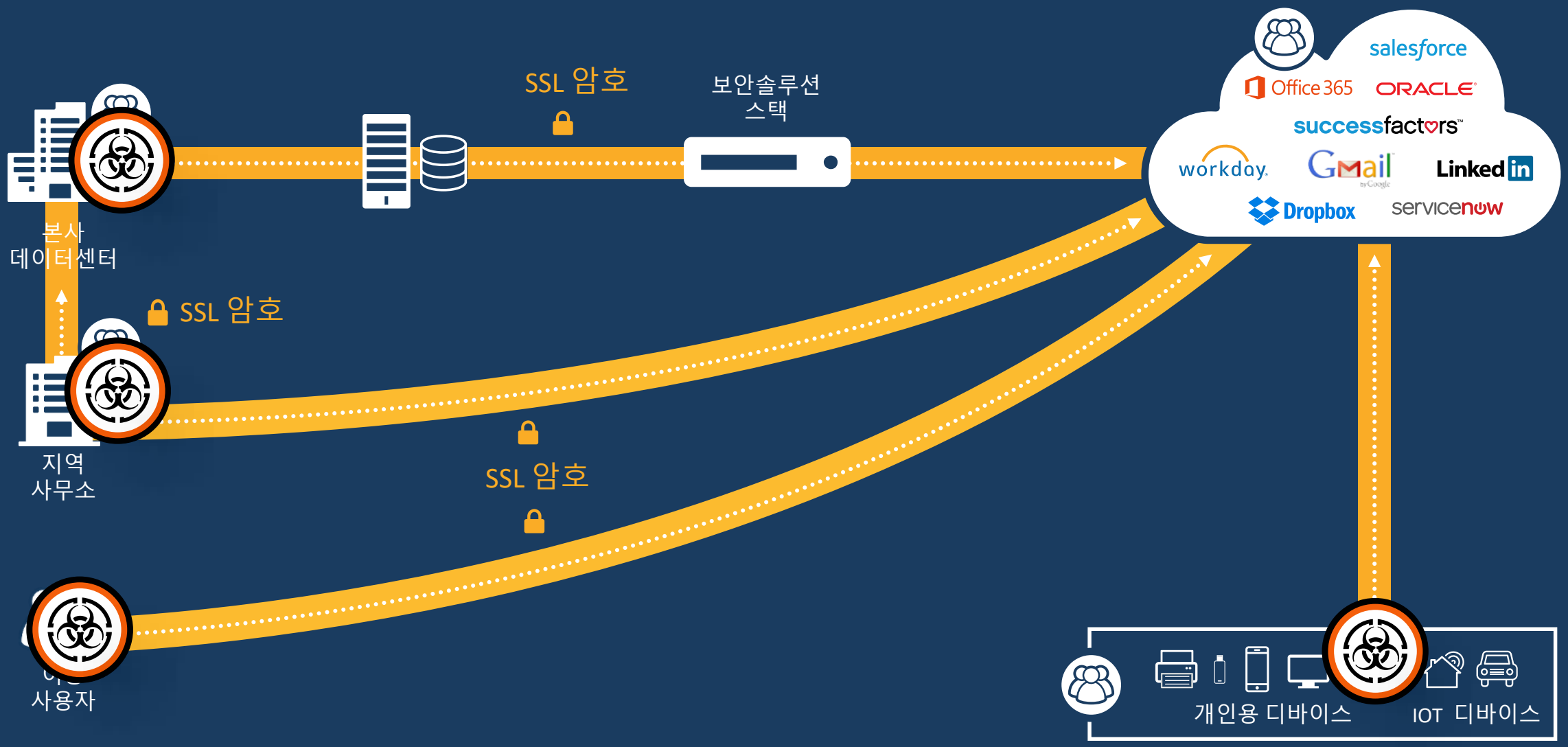

보안솔루션
스택
salesforce
Office 365
ORACLE
successfactors
workday
Gmail
LinkedIn
Dropbox
servicenow
본사
데이터센터
지역
사무소
이동
사용자
개인용 디바이스

네트워크 경계선의 확장

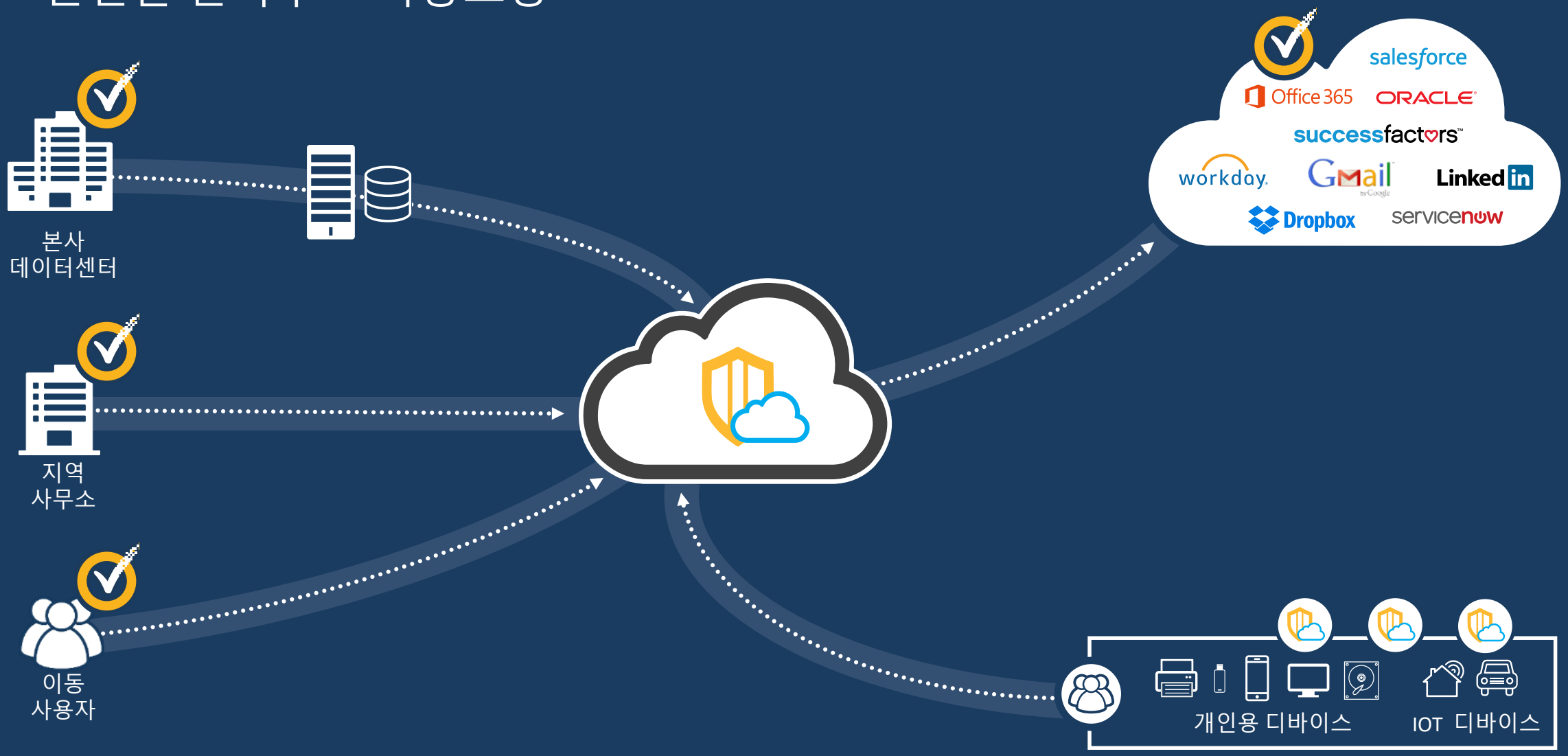
직접 연결로 인해 보호해야 할 네트워크가 확장됨

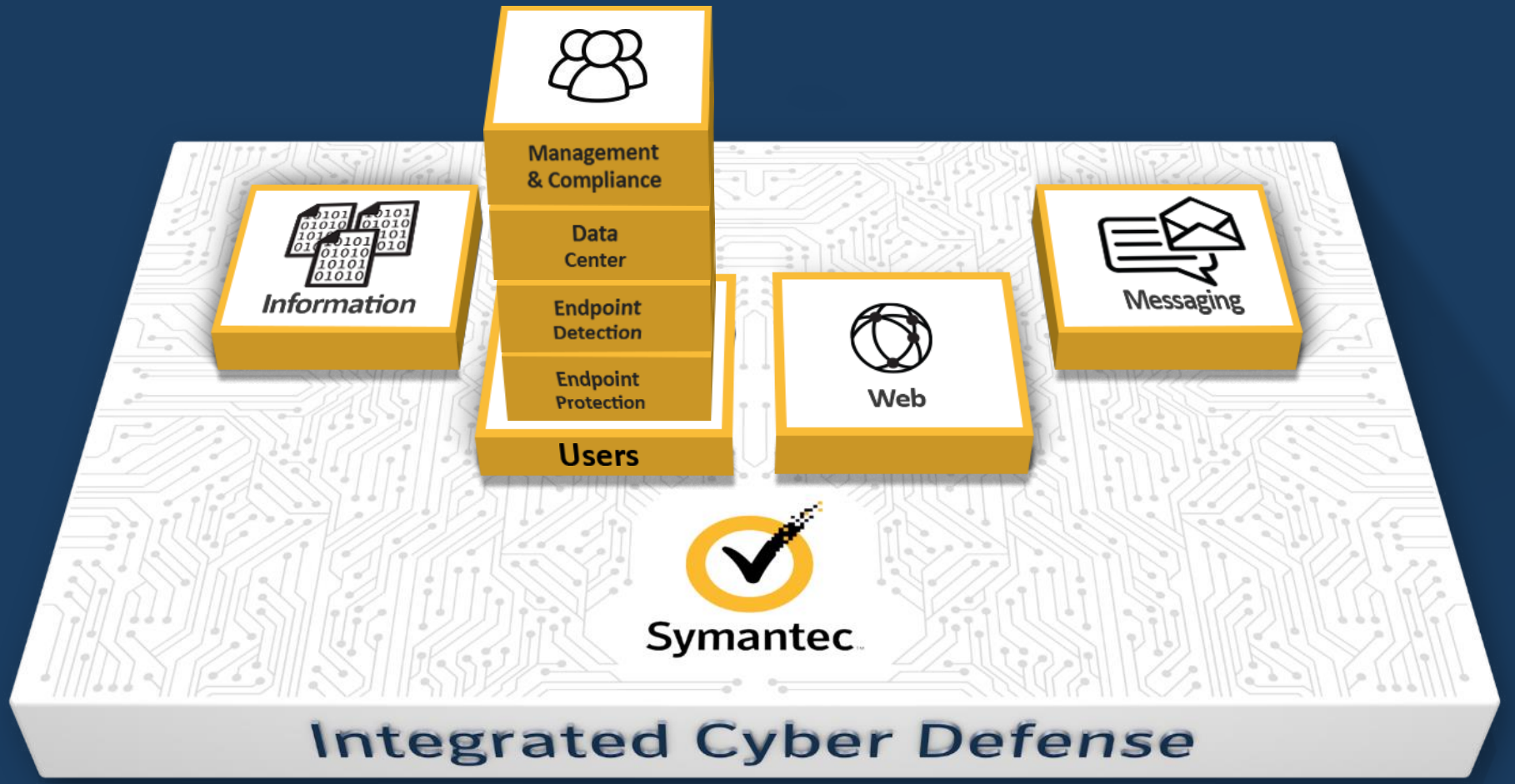


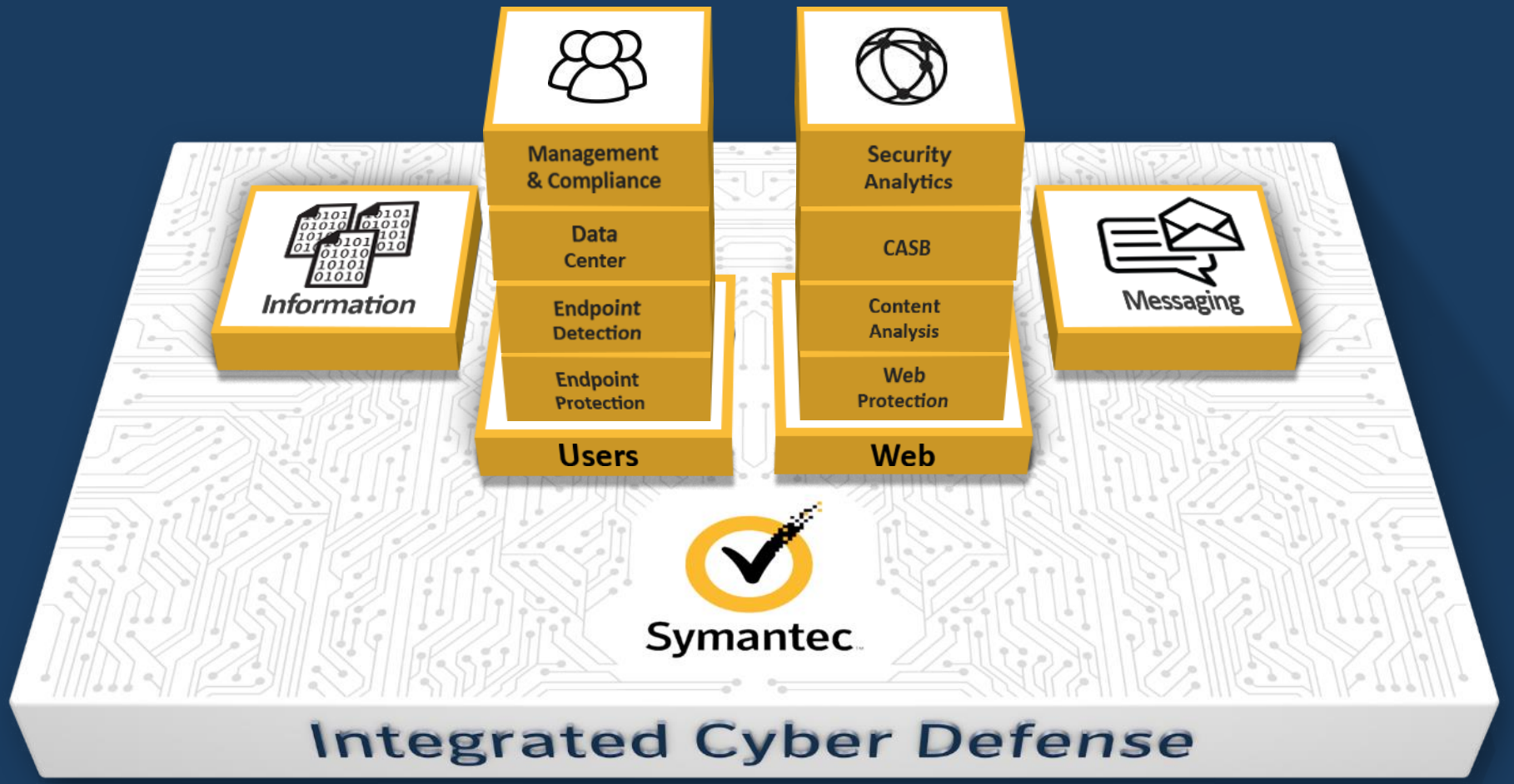
단계별 공격

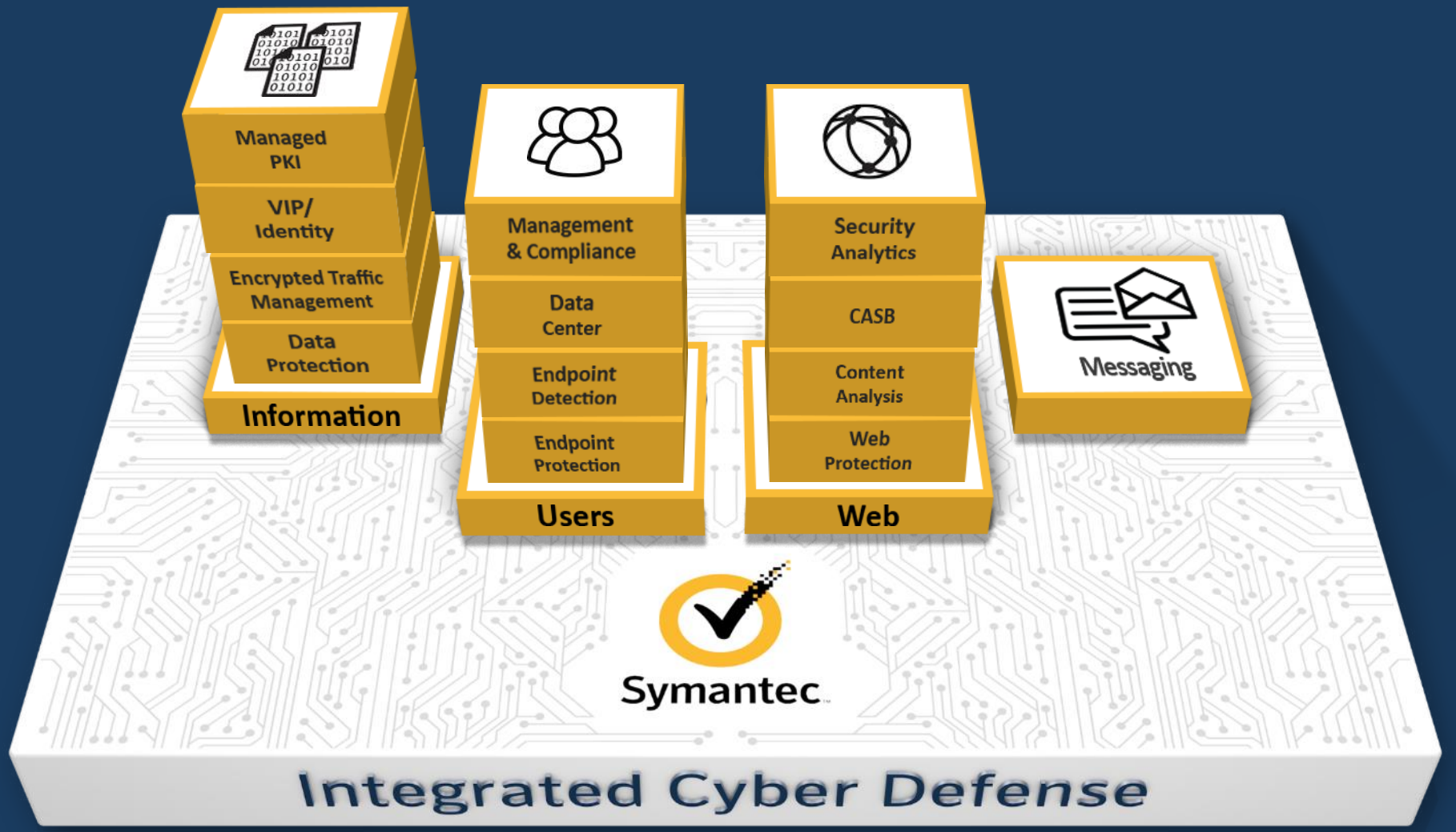

SSL 암호
보안솔루션
스택
salesforce
Office 365
ORACLE
successfactors
workday.
Gmail
LinkedIn
Dropbox
servicenow
본사
데이터센터
SSL 암호
지역
사무소
SSL 암호
사용자
개인용 디바이스
IOT 디바이스

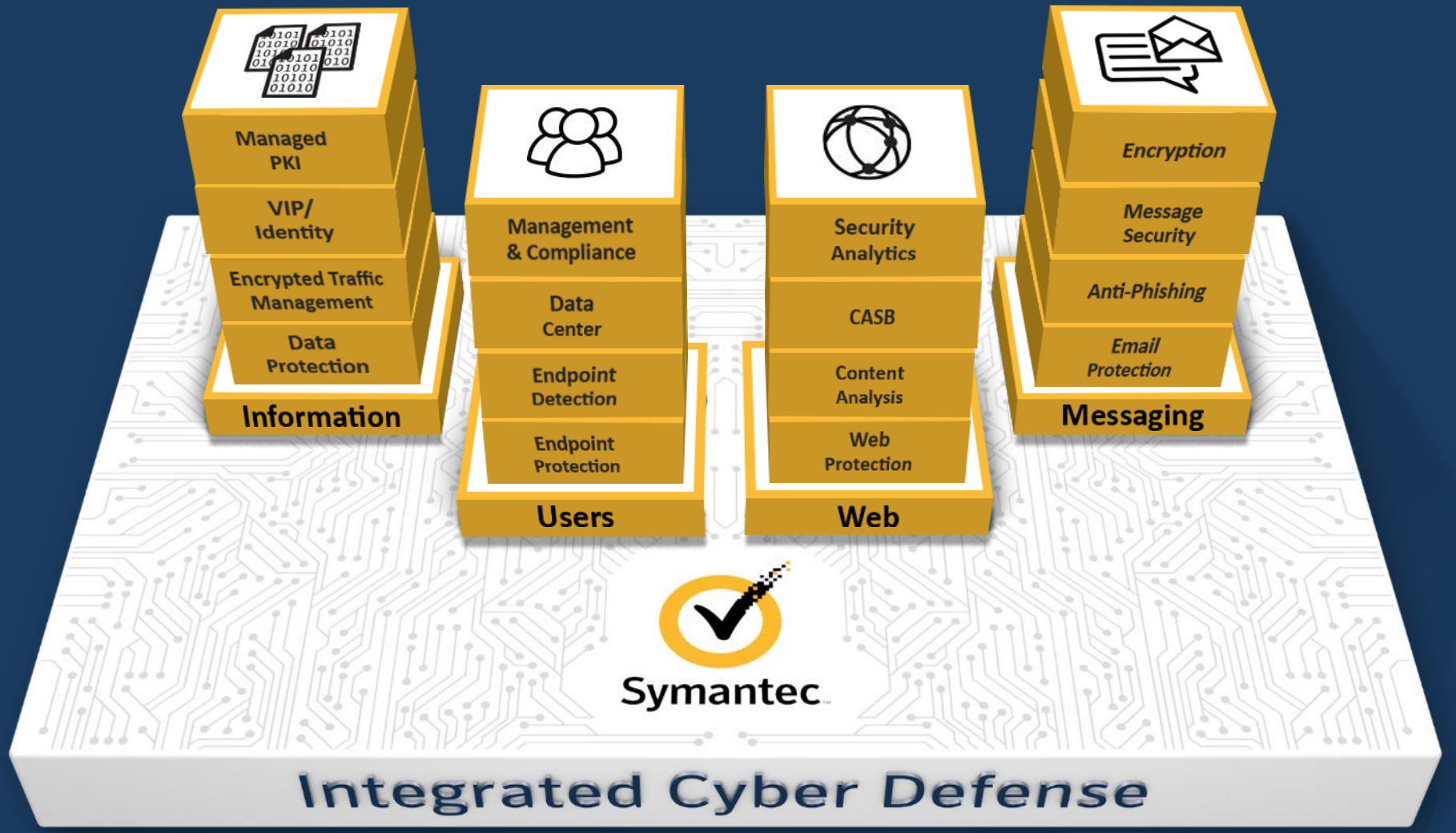
클라우드 제너레이션에 대한 혁신 필요:
안전한 클라우드 사용보장

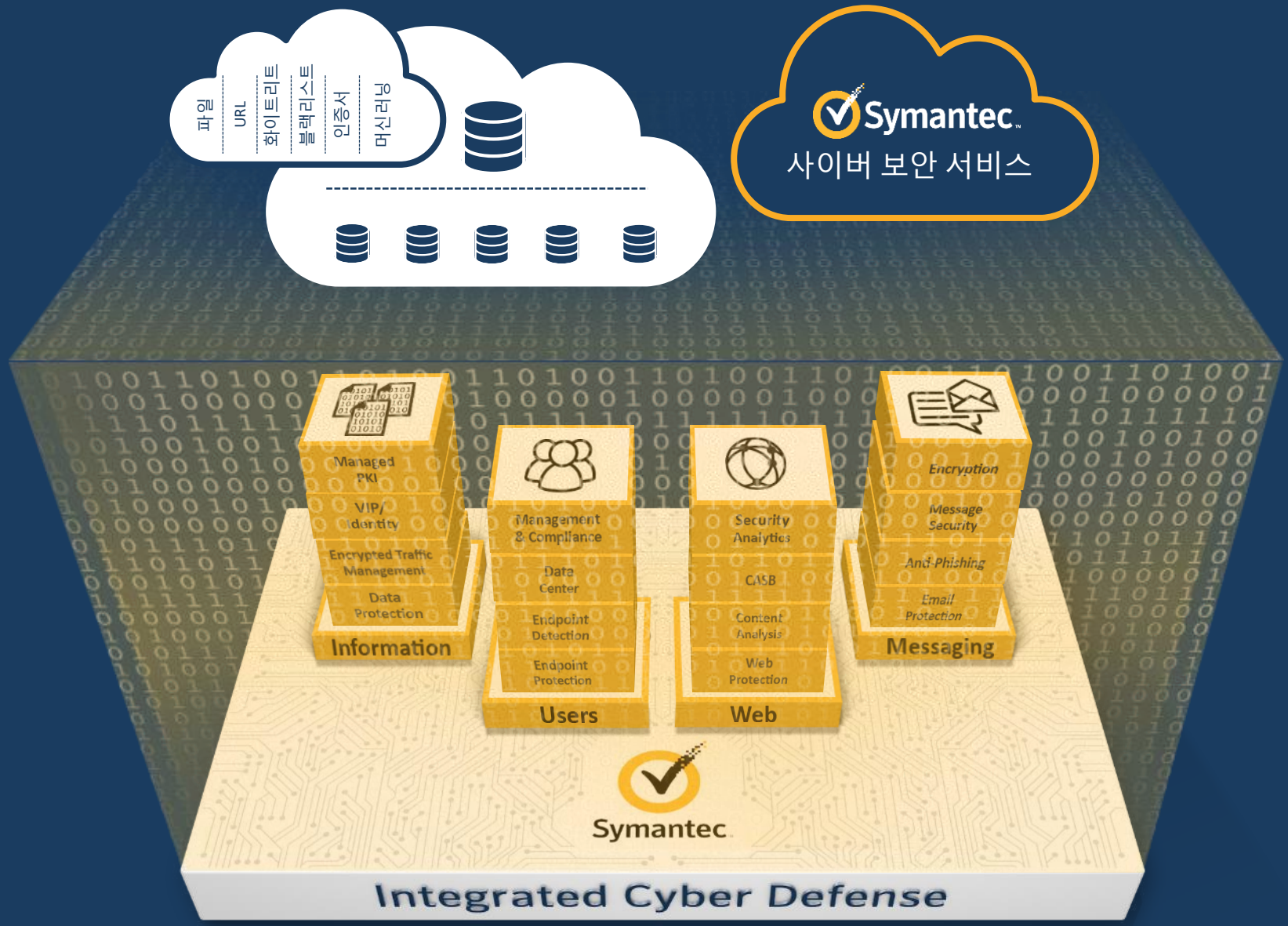


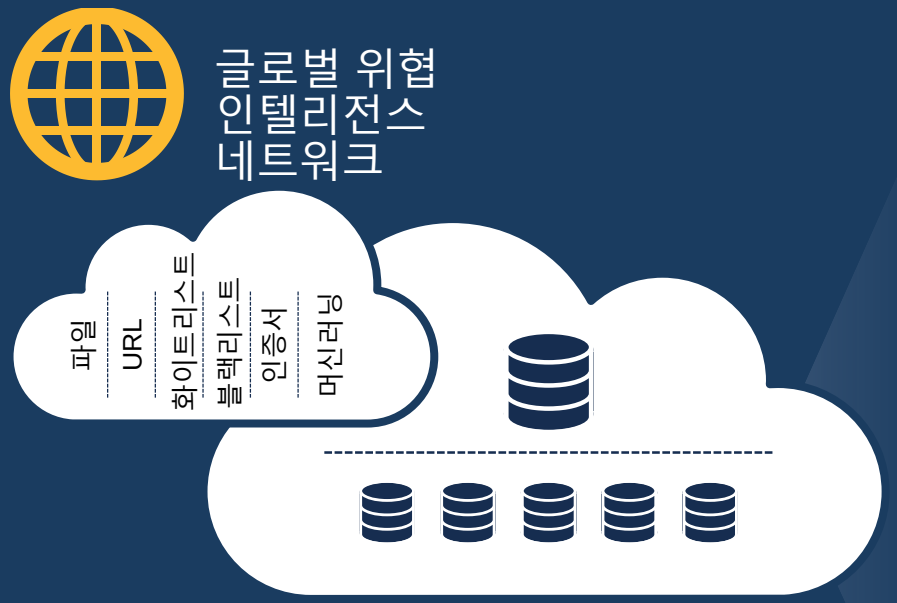

Management
& Compliance
Data
Center
Endpoint
Detection
Endpoint
Protection
Users
Information
Web
Messaging
Symantec
Integrated Cyber Defense


Management & Compliance
Data Center
Endpoint Detection
Endpoint Protection
Users
Security Analytics
CASB
Content Analysis
Web Protection
Web
Information
Messaging
Symantec
Integrated Cyber Defense


Managed PKI
VIP/ Identity
Encrypted Traffic Management
Data Protection
Information
Management & Compliance
Data Center
Endpoint Detection
Endpoint Protection
Users
Security Analytics
CASB
Content Analysis
Web Protection
Web
Messaging
Symantec
Integrated Cyber Defense


Managed PKI
VIP/ Identity
Encrypted Traffic Management
Data Protection
Information
Management & Compliance
Data Center
Endpoint Detection
Endpoint Protection
Users
Security Analytics
CASB
Content Analysis
Web Protection
Web
Encryption
Message Security
Anti-Phishing
Email Protection
Messaging
Symantec
Integrated Cyber Defense


파일
URL
화이트리트
블랙리스트
인증서
머신러닝
Symantec
사이버 보안 서비스
Managed PKI
VIP/ Identity
Encrypted Traffic Management
Data Protection
Information
Management & Compliance
Data Center
Endpoint Detection
Endpoint Protection
Users
Security Analytics
CASB
Content Analysis
Web Protection
Web
Encryption
Message Security
Anti-Phishing
Email Protection
Messaging
Symantec
Integrated Cyber Defense



- **4억3천만** 신규 악성코드 발견
- **1조** 악성이메일 차단
- **10억** 사회공학 스캠 차단
- **1만 5천+** 클라우드 애플리케이션 발견 및 보호
- **1억8천2백만** 웹 공격 차단

글로벌 인텔리전스의 데이터 기반

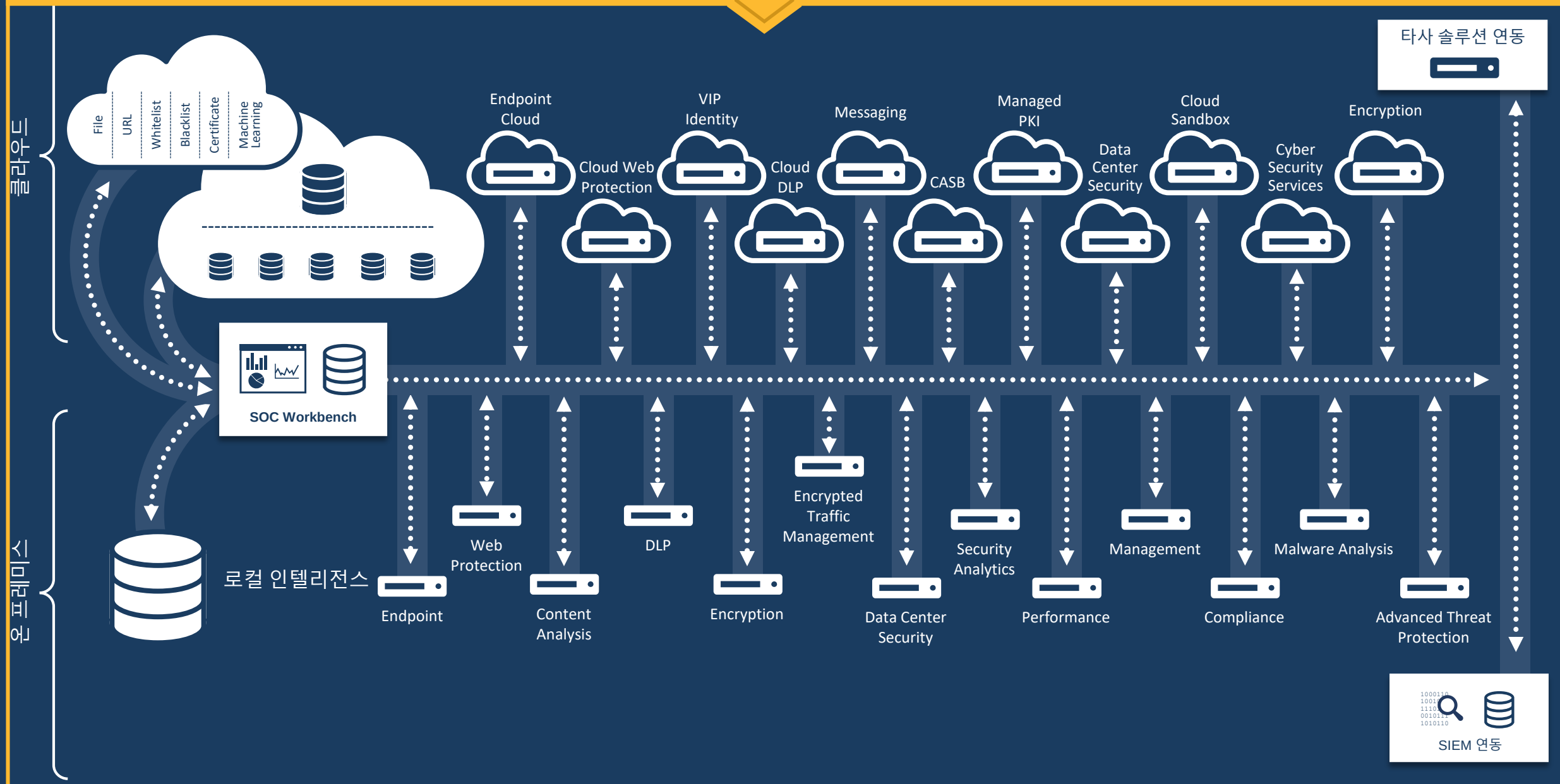
1 조
매일 신규 웹 요청 수

2 조
매일 이메일 스캐닝

1억7천5백만
개인/기업 사용자
엔드포인트 보호

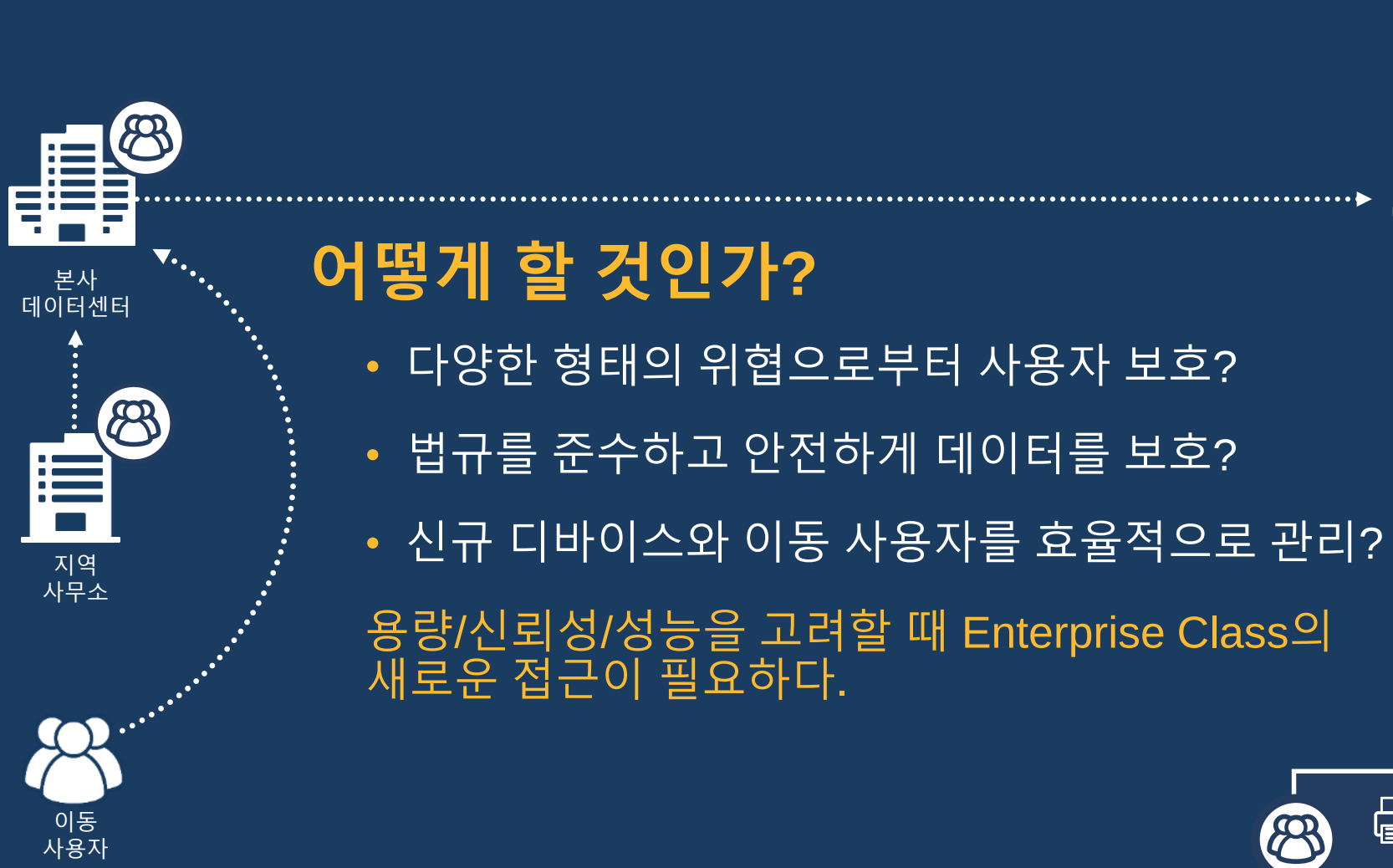
9 개의 글로벌 위협
대응센터 및
3,000 명의 연구 개발
엔지니어

Integrated Cyber Defense 플랫폼



웹/클라우드 보안:
웹/클라우드 사용 통제, 위협 대응 및 데이터 보호

새로운 변화에 따른 신표준



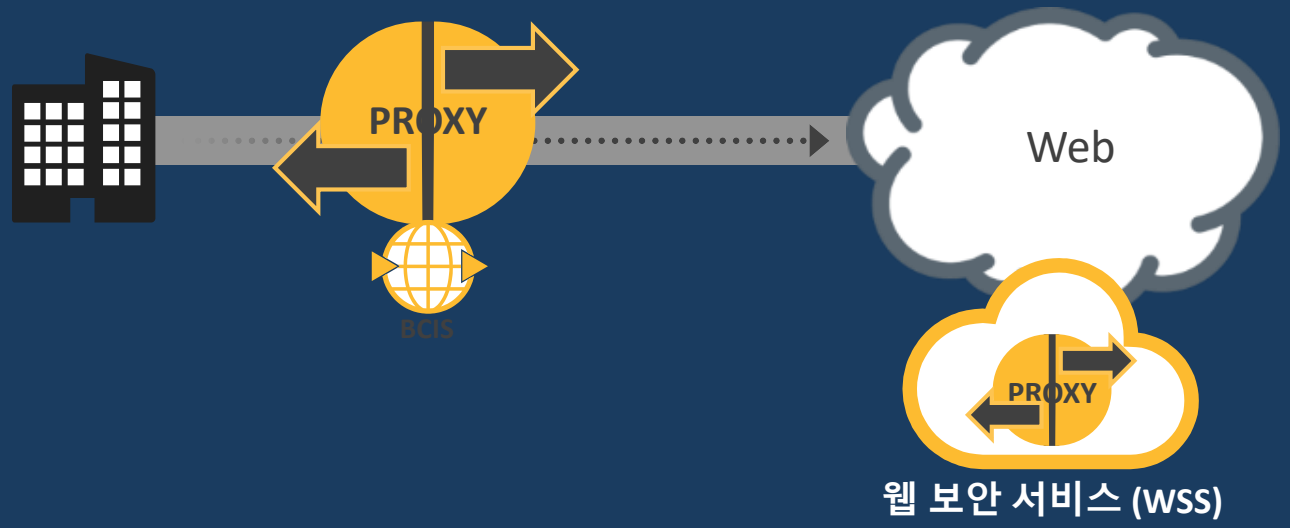
어떻게 할 것인가?

- 다양한 형태의 위협으로부터 사용자 보호?
- 법규를 준수하고 안전하게 데이터를 보호?
- 신규 디바이스와 이동 사용자를 효율적으로 관리?

용량/신뢰성/성능을 고려할 때 Enterprise Class의 새로운 접근이 필요하다.

프락시 기반 보안 웹게이트웨이 (SWG)

보안 및 컴플라이언스를 위한 중요한 네트워크 통제 영역



- 어플라이언스 (ProxySG)
- 가상 어플라이언스 (vSWG)
- 웹 보안 서비스 (WSS)

+ 시만텍 인텔리전스 서비스 (BCIS)
  또는 시만텍 웹 필터 (BCWF)

웹 접근 거버넌스 &
위협 보호

파일 추출 &
연동 서비스(ATP, DLP)

강력하고, 개방형 정책 플랫폼
- 클라우드, 온 프렘, 가상, AWS

보안 웹 게이트웨이
지능형 보안 웹 게이트웨이

모든 엔드포인트 프락시
- 트래픽 차단 및 복호화
- 모든 디바이스 형식 에뮬레이션
- 분석을 위한 컨텐츠 추출
- 인증 시스템 연동

위협 차단 및 컨텐츠 연동
- 지능형 컨텐츠 분석을 위한 샌드박스 프리필터
- DLP, 샌드박스, 애널리틱스를 위한 컨텐츠 전송
- 새로운 디바이스 연동을 위한 개방형 연동 아키텍쳐

웹통제 및 클라우드 거버넌스
- 섀도우 IT 위험 식별 및 통제
- 웹기반 위협 차단
- 접근제어 정책 구현 및 웹/클라우드 사용량 감사

사용자 경험 및 성능 향상
- 비디오 가속 및 스플릿 터널링
- 콘텐츠 비대칭 캐싱
- 프로토콜 지원 최적화

웹 및 클라우드 접근 통제
거버넌스 및 정책 구현

- 12,000+ 클라우드 앱 지원
- 60 개의 위험 속성 및 비즈니스 준비도
- 섀도우 IT 통제 정책 적용

클라우드 보안 (CASB)

- OWASP 상위 10 애플리케이션 보호
- 다이나믹 인텔리전스를 활용한 캐쉬 최적화

웹 방화벽/ 리버스프록시

웹 위협 보호

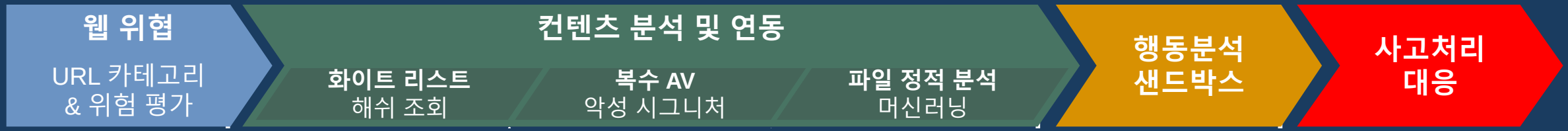
- 모든 위협의 90%이상 차단하는 12개의 보안 카테고리
- Malnet정보를 통한 제로데이 익스플로잇 차단
- URL 위협 – 과탐없이 보안성 증대

유연한 정책 지원

- 72 카테고리
- 55 개 언어 지원
- 다이나믹, 실시간 점수화

지능형 보안 게이트웨의 지능형 위협의 대응

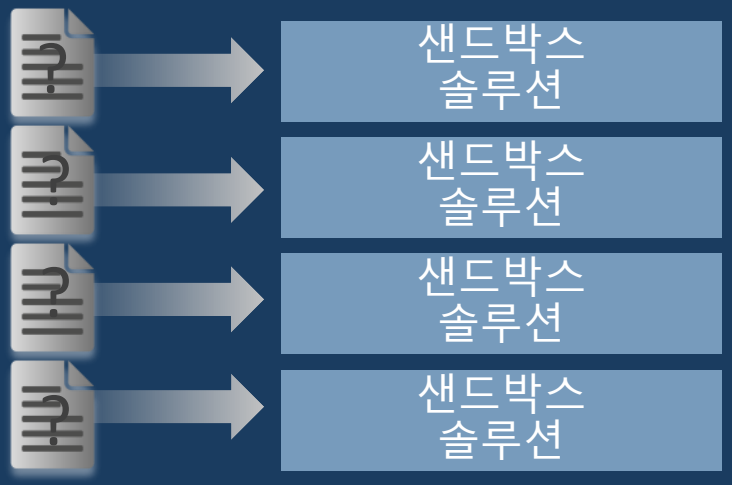
샌드박스 효율성 증대 및 경고 감소로 보안성 증대

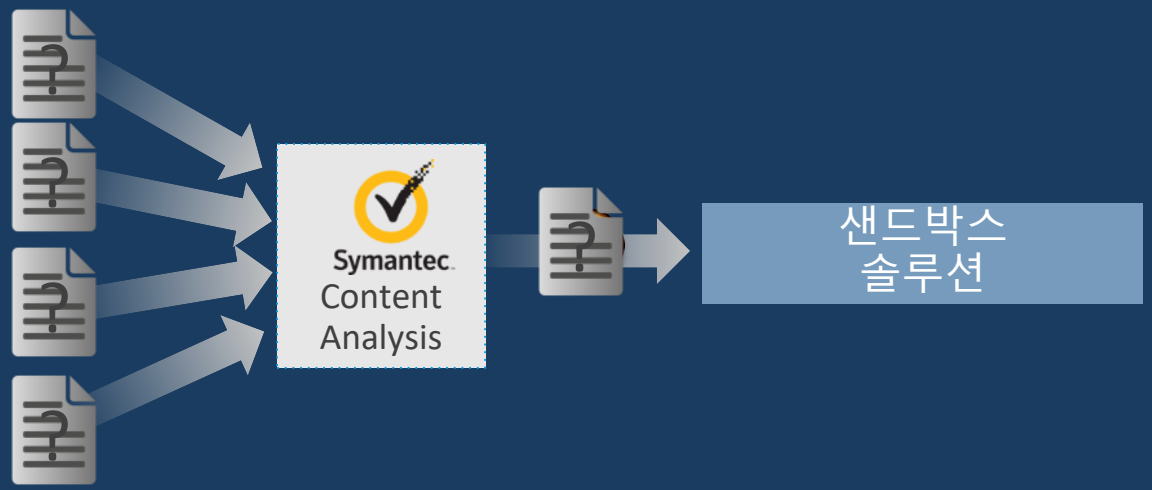


*실제 고객사례

샌드박스 운영 효율 증가 및 대응 비용 감소

지능형 보안 게이트웨이 활용(Advanced Secure Gateway)





“50% 비용절감” 샌드박스 비용

- 샌드박스 용량의 75% 감소효과
- 샘플 처리 급격한 감소
- 샌드박스 풀(pool) 아키텍쳐 운영
- 투자비용 감소

90% 절약 침해사고 비용

- 90%+ 경고 감소
- 분석 인력의 생산성 증대

클라우드 앱이 주는 혜택 vs. 보안문제로 사용 불가?

클라우드
새로운 도전과제

클라우드의 저장된
26%문서는
다양하게 공유됨

클라우드 앱의 확산

다양한 엔드포인트

섀도우 데이터 문제

계정 탈취

[1] 1H 2016 Shadow Data Report

전통적인 방어체계로는 부족함

SOC 1.0

SOC 1.0접근법으로는
보안 모델 우회

클라우드 시대

전통적인 데이터센터 SOC

- 위험 진단
- 침입탐지/차단
- 정보유출방지
- 방화벽
- 침해사고 대응
- 사고조사

클라우드 이전 시대

새로운 클라우드 보안 방어 체계 (CASB)

SOC 2.0

SOC 1.0

elastica CloudSOC™

AUDIT Shadow IT

DETECT intrusions in cloud

PROTEC against intrusions

INVESTI incidents & respor

전통적인 데이터센터 SOC

위험 진단

침입탐지/차단

정보유출방지

방화벽

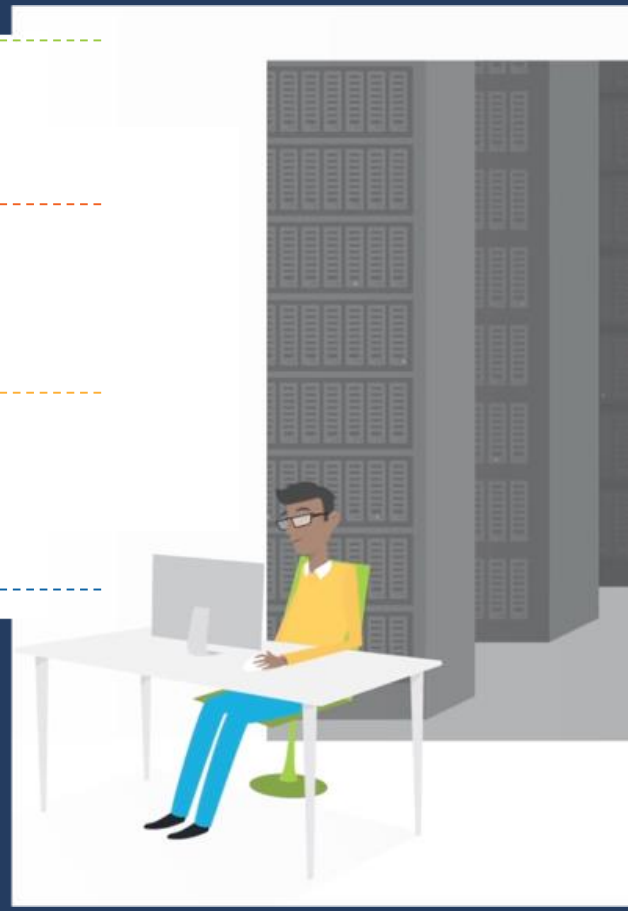
침해사고 대응

사고대응

SOC 1.0접근법으로는
보안 모델 우회

클라우드 시대

클라우드 이전 시대



새로운 클라우드 보안 방어 체계 (CASB)

클라우드 위협의 포괄적인대응

SOC 2.0

elastica CloudSOC™

AUDIT
Shadow IT

DETECT
intrusions in cloud apps account

PROTECT
against intrusions in cloud apps accounts

INVESTIGATE
incidents & respond

BEFORE

DURING

AFTER

클라우드 시대

SOC 1.0

전통적인 데이타센터 SOC

- 위험 진단
- 침입탐지/차단
- 정보유출방지
- 방화벽
- 침해사고 대응
- 사고조사

클라우드 이전 시대

포괄적인 클라우드 보안

클라우드API

클라우드 프락시

외부 경계선

이벤트

프락시

엔터프라이즈
경계선

CloudSOC™

StreamIQ™

ContentIQ™

ThreatScore™

- 위험 진단
- 침입탐지/차단
- 악성코드 탐지
- 프락시/방화벽
- 정보유출방지
- 침해사고 대응
- 사고조사

완벽한 엔드포인트 보호

Powered by SEP 14

신종 악성코드 vs. 일반적인 방어

위협

4억3천만
악성 코드

36% 증가
1 년간

5,585
신규 취약점

125% 증가
제로 데이

지능형 악성코드
우회기능 탑제

정적분석
엔드포인트 보안

**Source: Symantec 2016 Internet Security Threat Report: go.symantec.com/istr*

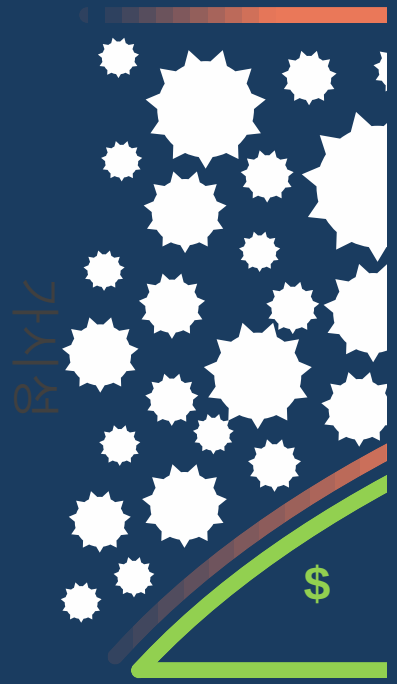
신종 악성코드 vs. 일반적인 방어

방어

- 기존 엔드포인트 대응 기술을 우회는 고양이와 쥐 싸움
- 모든것을 탐지할 수 있는 단일 기술은 존재할 수 없음
- 많은 위협이 유입됨
- 침입 이후 탐지 및 대응 기술에 대한 투자가 지속되고 있음

1% 문제: 미탐지 악성코드

일반 악성코드

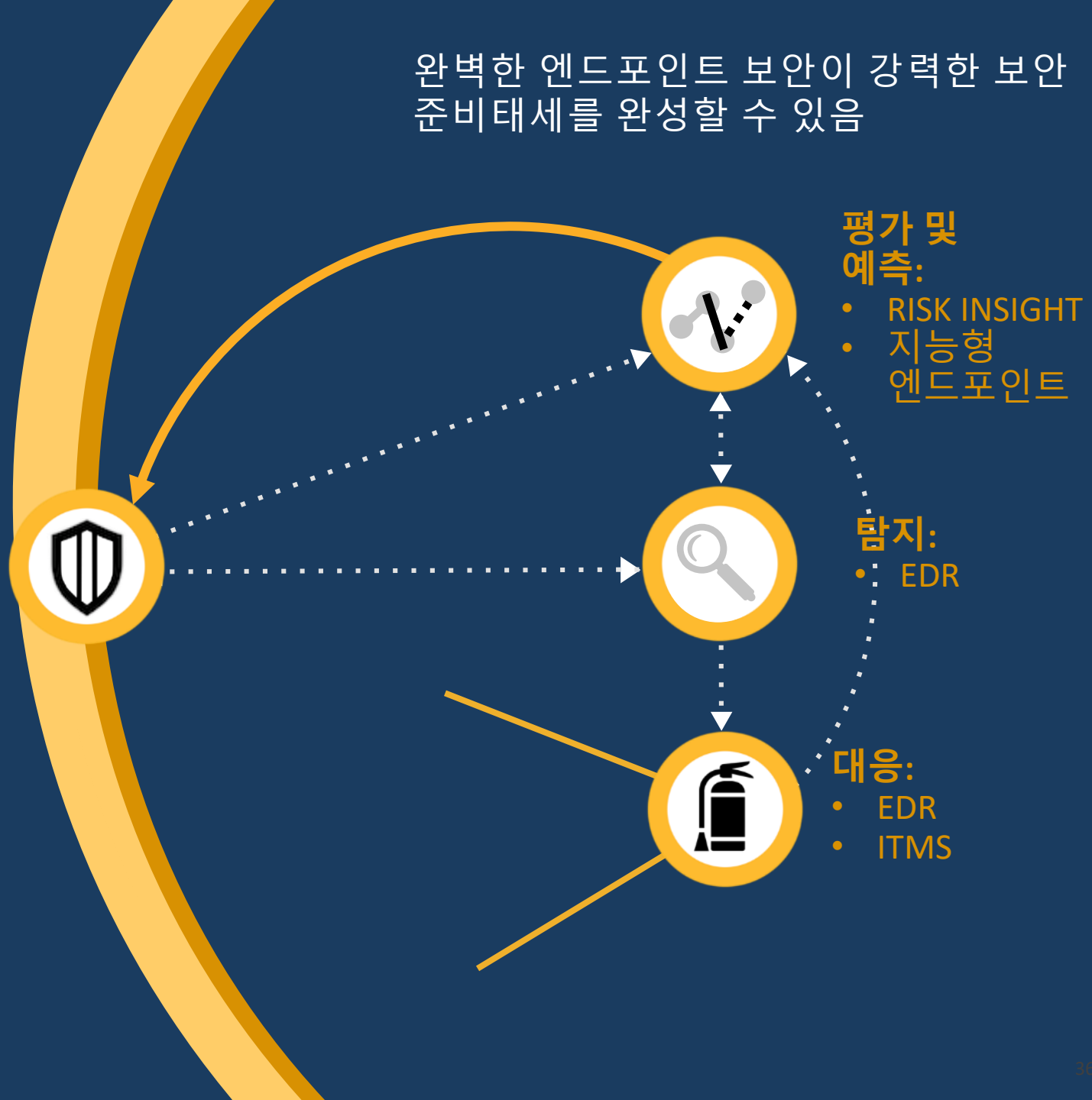


차단

포괄적인 엔드포인트 대응 전략

완벽한 엔드포인트 보안

완벽한 엔드포인트 보안이 강력한 보안 준비태세를 완성할 수 있음



차단:
- 엔드포인트 보호

평가 및 예측:
- RISK INSIGHT
- 지능형 엔드포인트

탐지:
- EDR

대응:
- EDR
- ITMS

최근 사이버 위협은 빈도 및 성숙도가 증가추세임

시만텍 엔드포인트 포트폴리오: 차단

- 공격체인 전반을 대응할수 있는 다계층 보호 기술
- 단일 에이전트
- 머신러닝을 탑제한 인공지능 기술
- 익스플로잇 차단
- EDR 기술 탑제
- 네트워크 보안 솔루션과 연동 가능
- 애플리케이션 제어
- 탐지 수준 조절

시만텍 엔드포인트 포트폴리오: 탐지

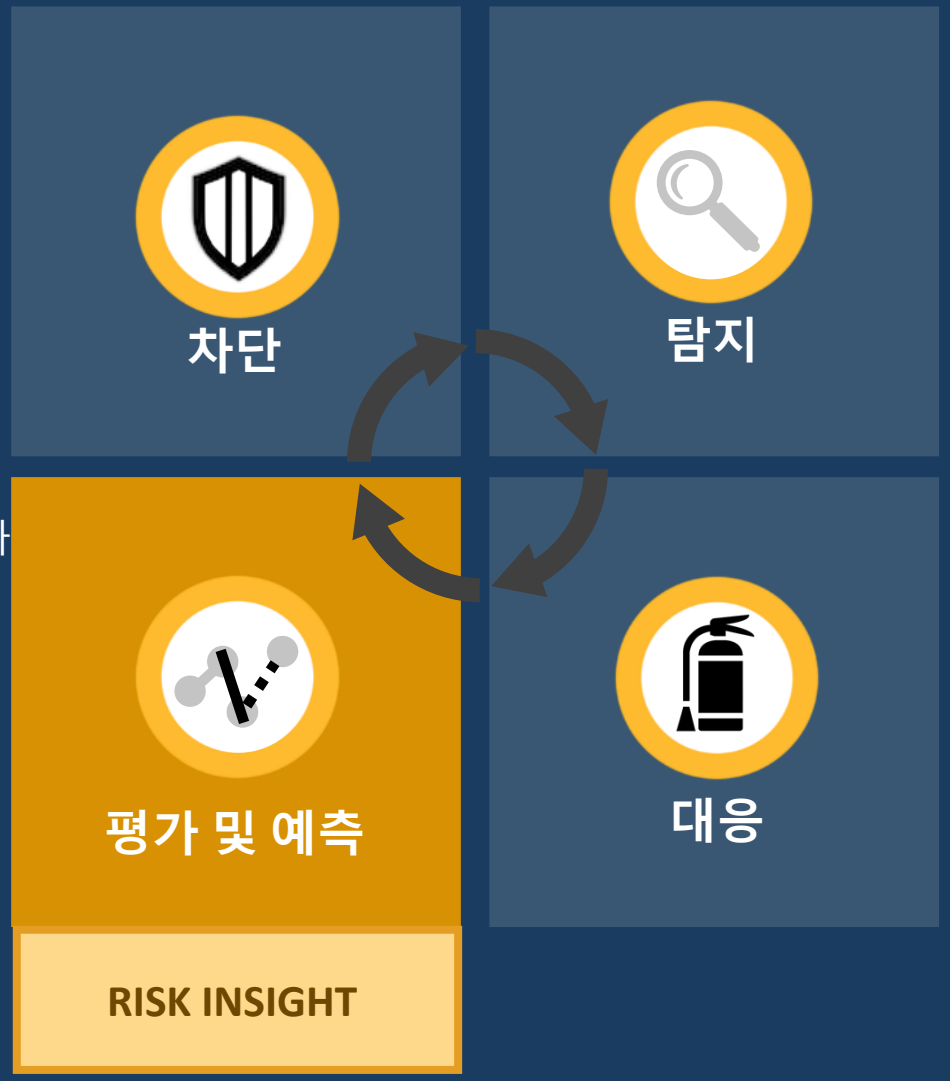
- 의심스러운 파일 식별 및 조사
- 중요순위에 따른 대응
- 모든 엔드포인트에서 IoC 검색
- 표적공격 식별
- 별도의 ATP agent필요없음 (SEP활용)

시만텍 엔드포인트 포트폴리오: 대응

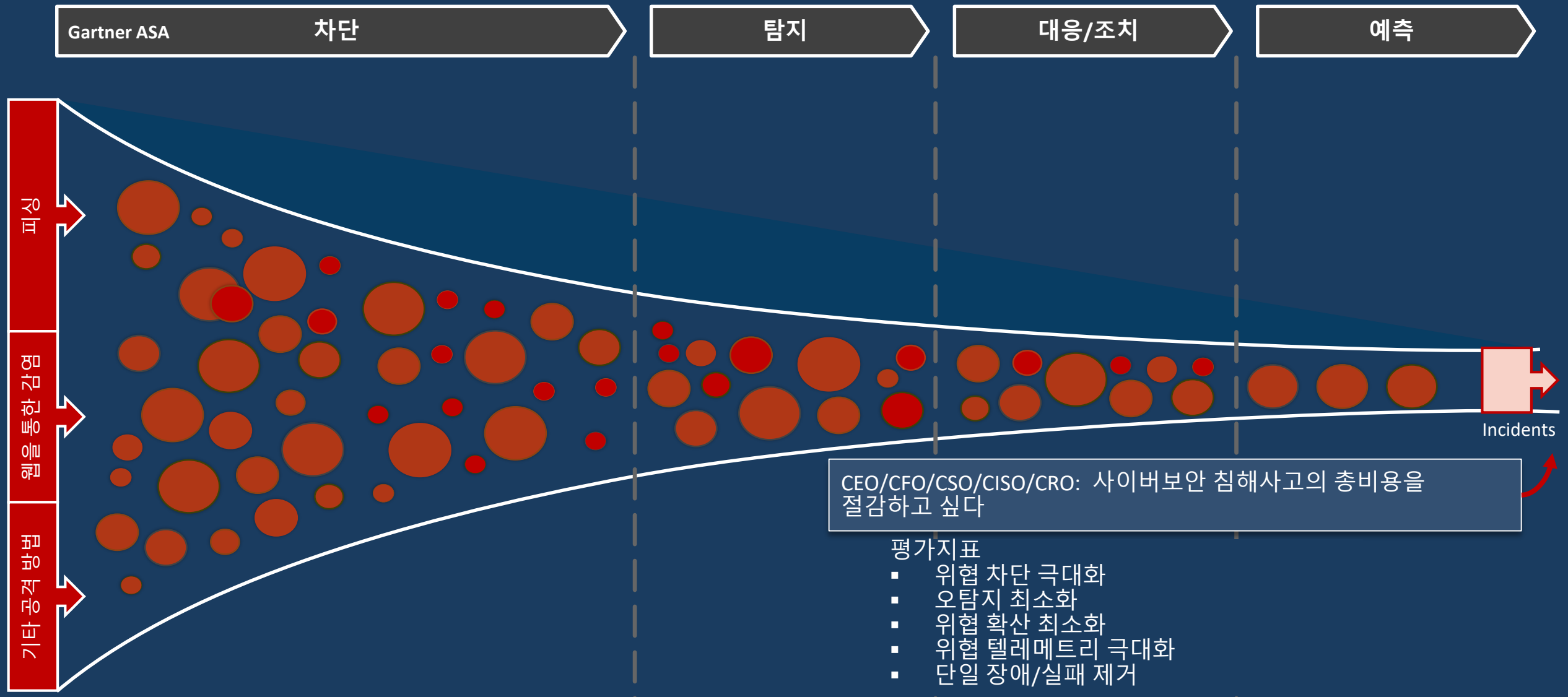
- 원클릭으로 수분내의 모든 공격 아티팩트 치료
- EDR을 위한 별도의 에이전트 필요 없음
- 추가 조사를 위한 감염 엔드포인트 격리
- 블랙리스트/화이트리스트 및 URL
- 타 SIEM장비와 연동
- 운영체제/애플리케이션 패치 및 업데이트

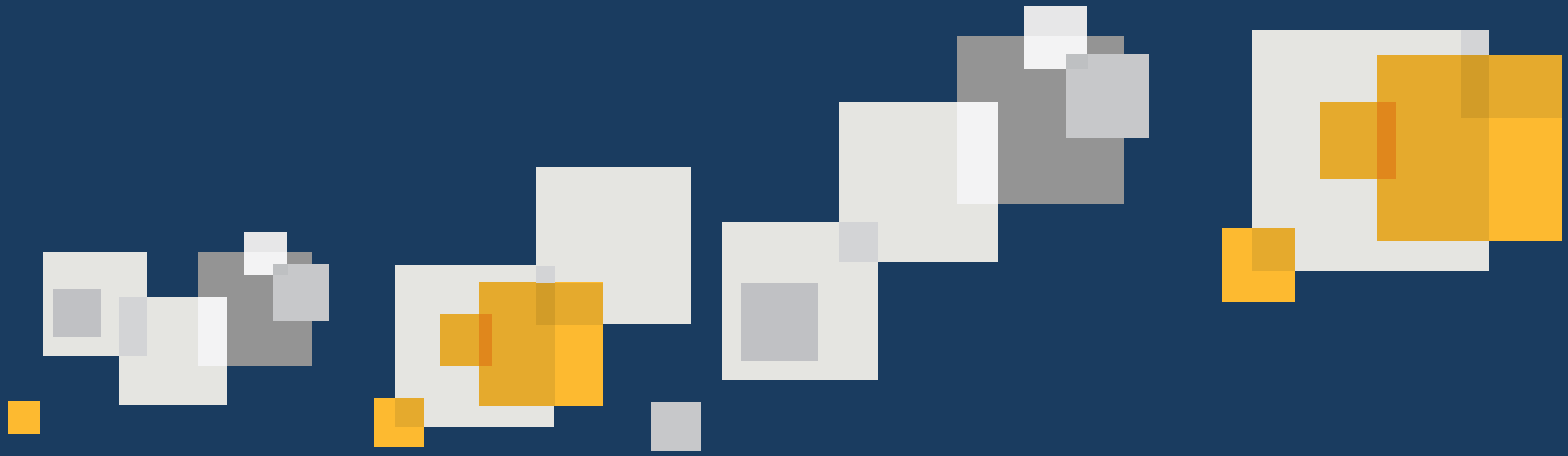
시만텍 엔드포인트 포트폴리오: 평가 및 예측

- 임원 의사결정용 다차원 위험 지표 대쉬보드(엔터프라이즈/일반사용자/산업별)
- 상위 취약한 엔드포인트 및 사용자 식별
- 탐지율 추이 기록
- 이사회와 운영팀 소통

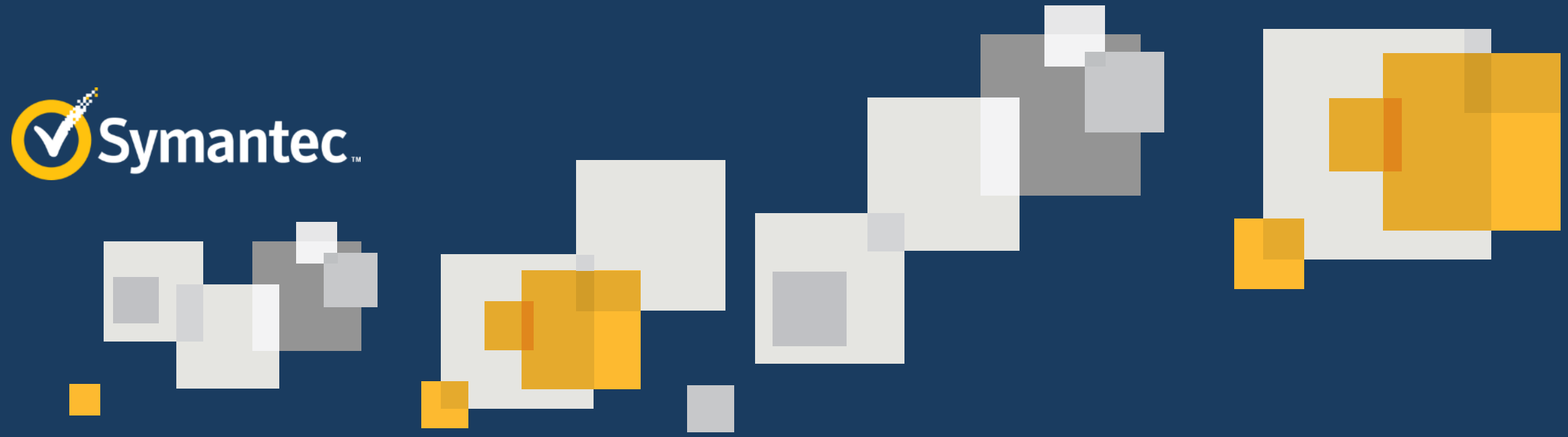


완벽한 엔드포인트 보안
조직 위험 최소화





Q&A



Thank you!

서종렬 상무

John_seo@Symantec.com
02) 3468-2020