NES 2016 차세대 기업 보안 세미나

BLUE COAT | Network + Security + Cloud

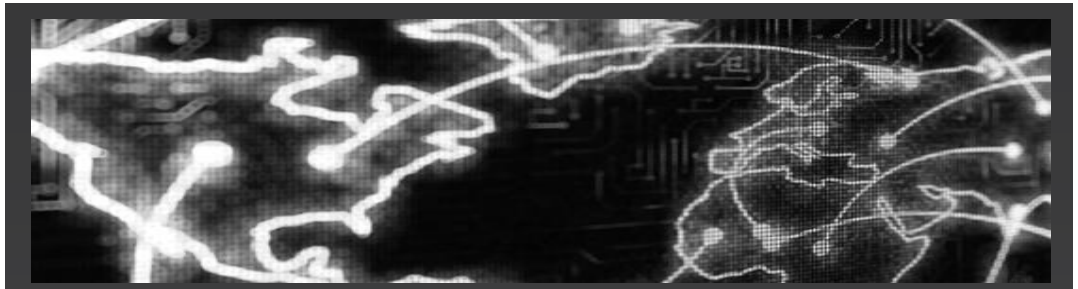
클라우드 보안 및 지능형 보안 위협에 대한 기업의 효과적인 대응 전략

서종렬 상무/블루코트 코리아

Agenda

- 보안위협의 진화
- 클라우드 환경에서의 보안
- 지능형 보안 위협 및 클라우드 환경에서의 기업의 대응 전략

블루코트 소개



Established Global Presence

- Business in 32 countries
- **2,000+** channel partners worldwide
- **44%** market share in Secure Web Gateway
- 132 patents & 63 patents pending
- Best of breed ecosystem
- Global hybrid cloud Infrastructure (over 40 Cloud Center)
- Global Intelligence Network of 75 million users
- **86%** of FORTUNE Global 500 Companies
- **Over 30%** of FORTUNE Global 10K Companies

Forbes

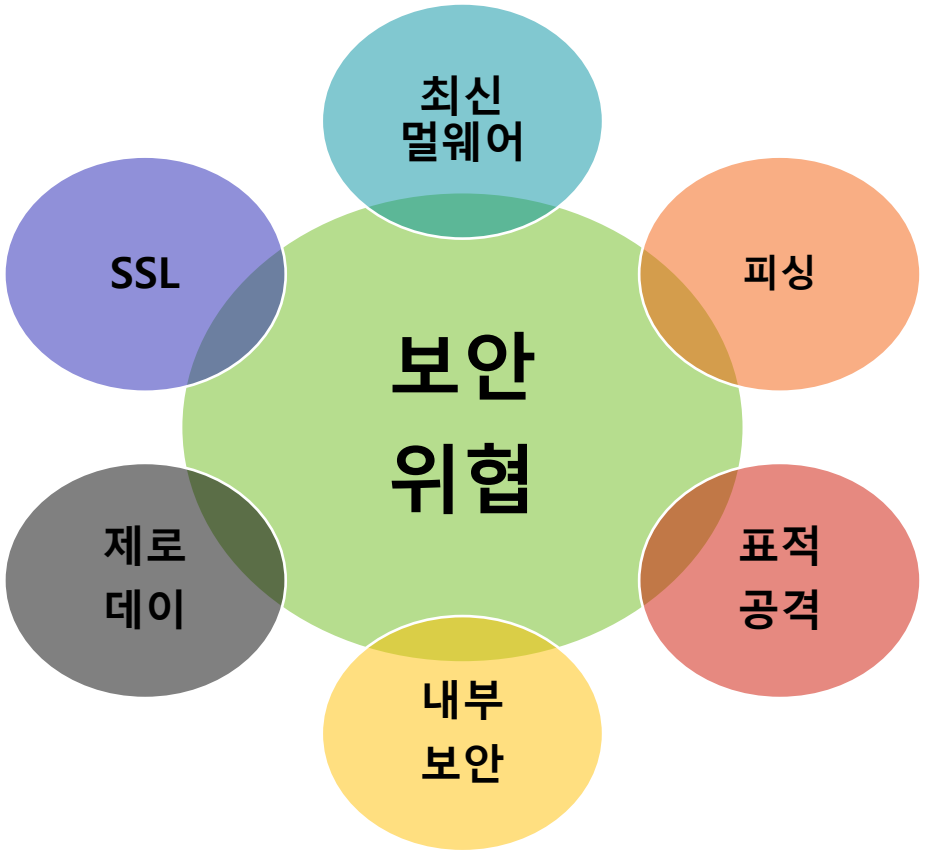
The World's Most Valuable Brands – 2015 Ranking

	#1	APPLE	BLUE COAT
Microsoft	#2	MICROSOFT	BLUE COAT
Google	#3	GOOGLE	
Coca-Cola	#4	COCA-COLA	BLUE COAT
IBM	#5	IBM	BLUE COAT
	#6	McDONALDS	BLUE COAT
SAMSUNG	#7	SAMSUNG	BLUE COAT
TOYOTA	#8	TOYOTA	BLUE COAT
	#9	GENERAL ELECTRIC	BLUE COAT
facebook	#10	FACEBOOK	

BLUE COAT

급증하는 보안 사고

기업을 괴롭히는 보안 위협



기존 시그니처로 탐지 불가한 첨부파일이 내부 사용자에게 전달

URL / 메일 필터를 교묘히 회피하여 내부 침투

어느새 새고 있는 정보, 표적의 환경을 통과 잠복하는 악성 코드

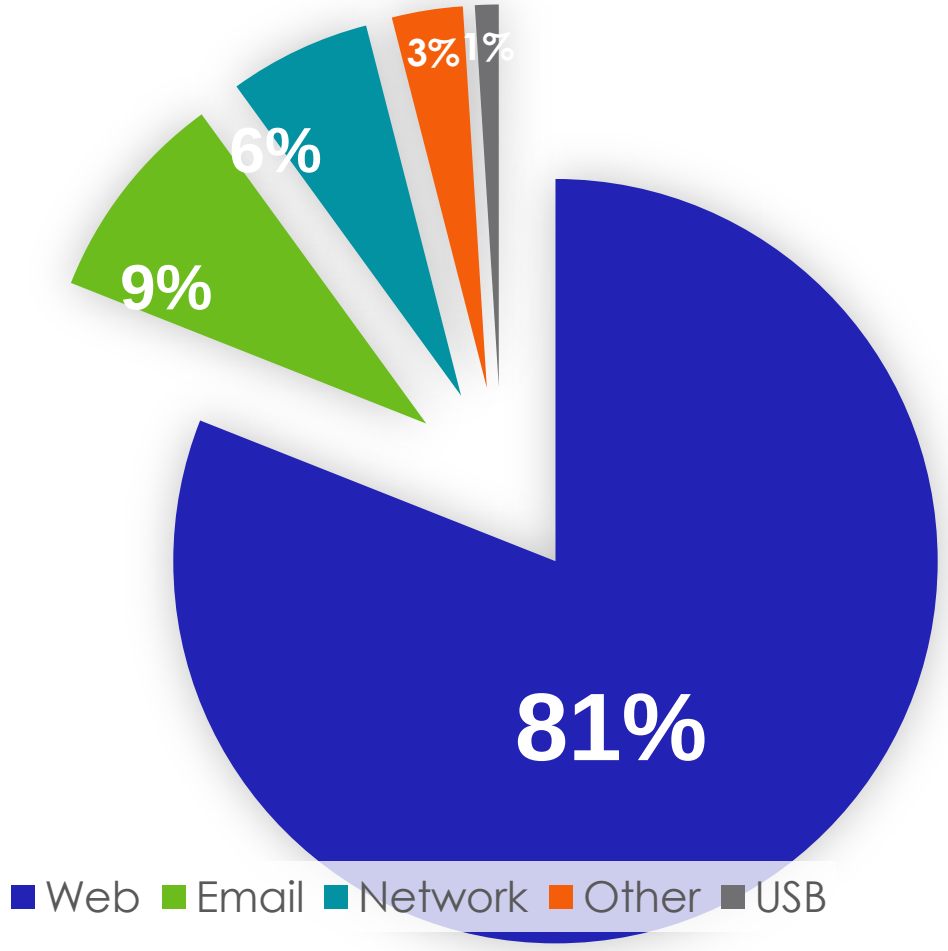
실시간 내부 보안 정보 관리 및 피해 상황 파악이 어려움

날마다 증가하는 의심 서버 통신의 실시간 대응 어려움

외부 통신의 절반 가까운 SSL을 보안 장비가 보지 못하는 현실

BLUE COAT

보안 위협의 유입 경로



The web delivers over 80% of all malware attacks

** Source: Verizon 2014 Data Breach Investigations Report*

23% of recipients now open phishing messages and 11% Click on attachments

** Source: Verizon 2015 Data Breach Investigations Report*

70-90% of malware are unique to an organization

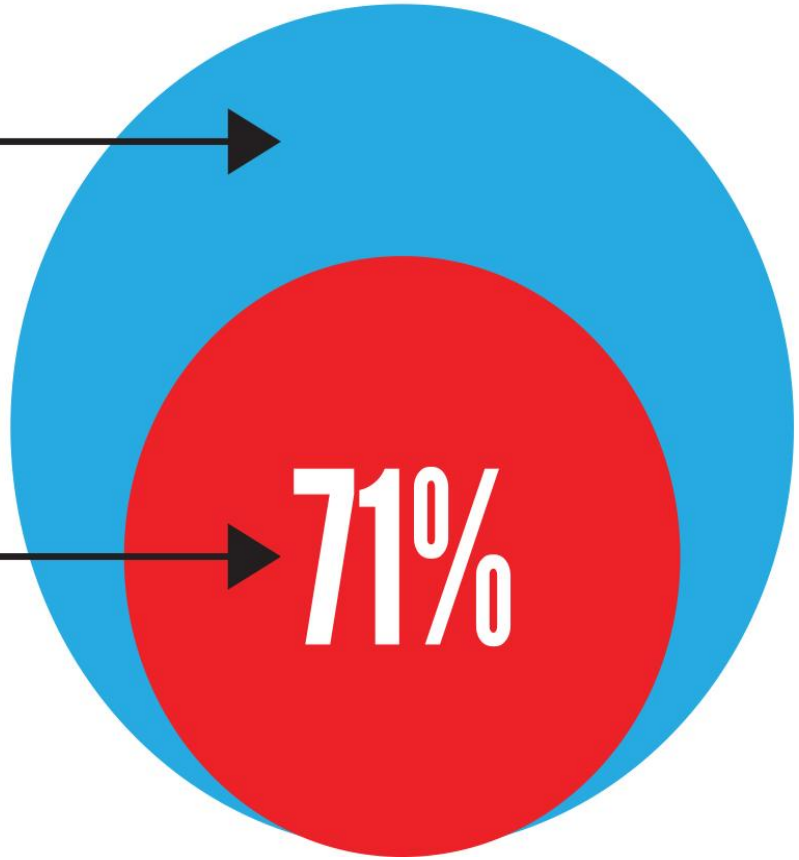
** Source: Verizon 2015 Data Breach Investigations Report*

BLUE COAT

One-day Wonders

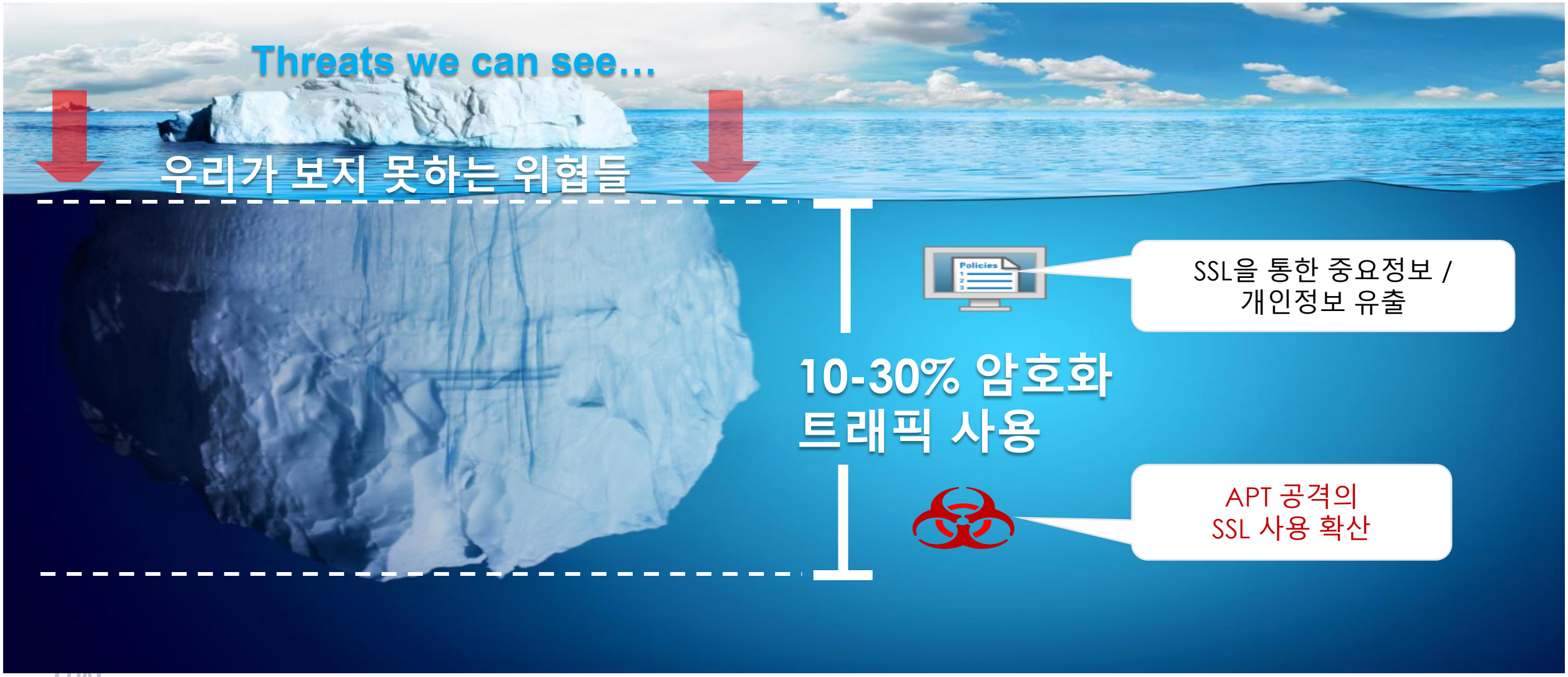
Of 660 Million
Total Hostnames

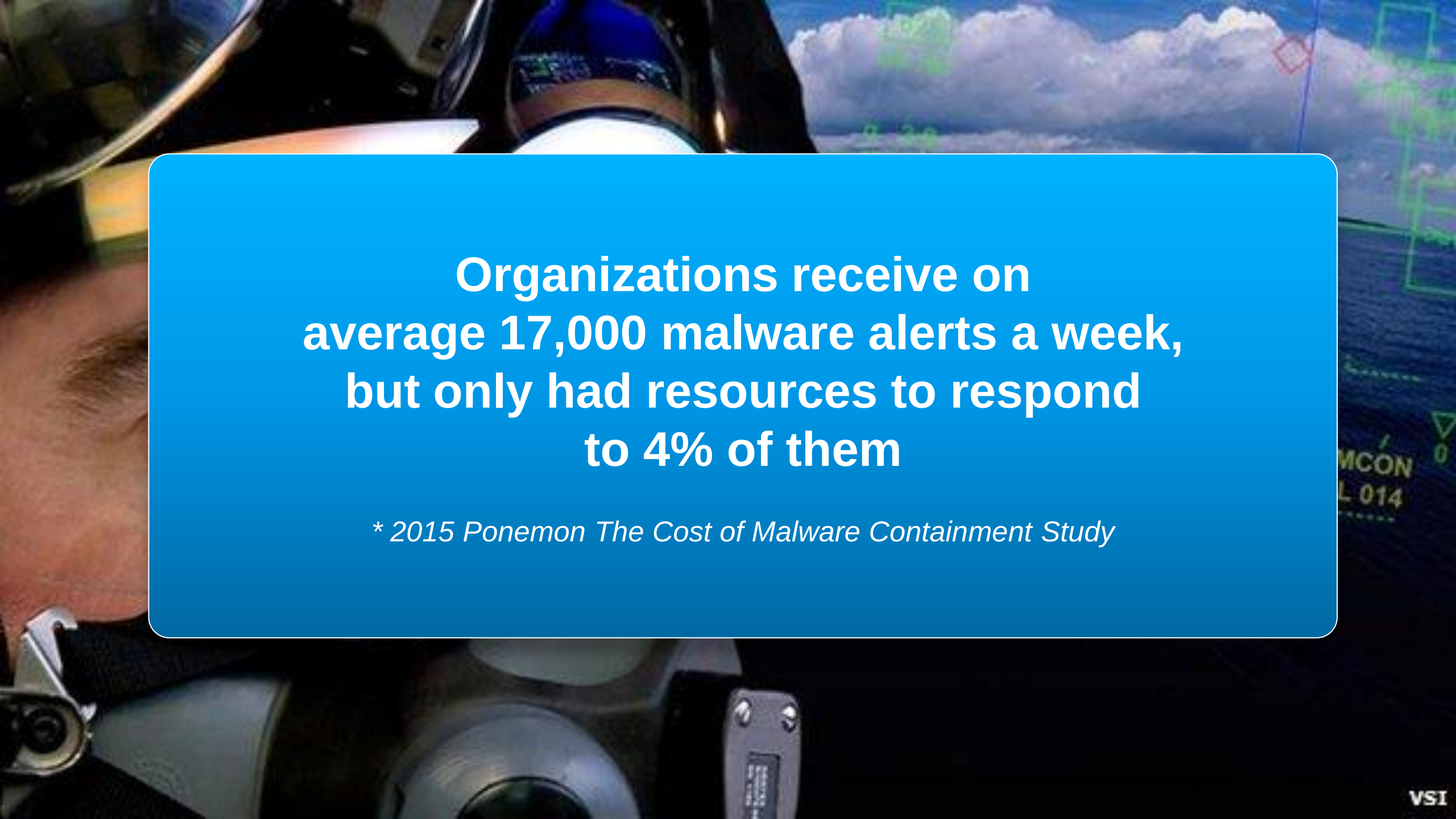
470 Million
Existed 24 hours or less



Of the top 50 Domains
22% were identified as malicious

암호화 채널을 이용한 보안 위협 증가





Organizations receive on average 17,000 malware alerts a week, but only had resources to respond to 4% of them

** 2015 Ponemon The Cost of Malware Containment Study*

Shadow IT

- 업무 관련 : Office365, Salesforce, Oracle 등
- 정보 관련 : Box, dropbox 등
- 고객 정보, 급여 정보, 개인 정보의 클라우드 유출
- 개인 정보 보호법 개정에 따른 대응이 필요

Source: [1]Elastica Q2 2015 Shadow Data Report

실제로는...
774 apps[1]

예측은...
40-50apps

72%
비공인된 클라우드
응용프로그램 사용s[1]

Source: [1]CIO Insight

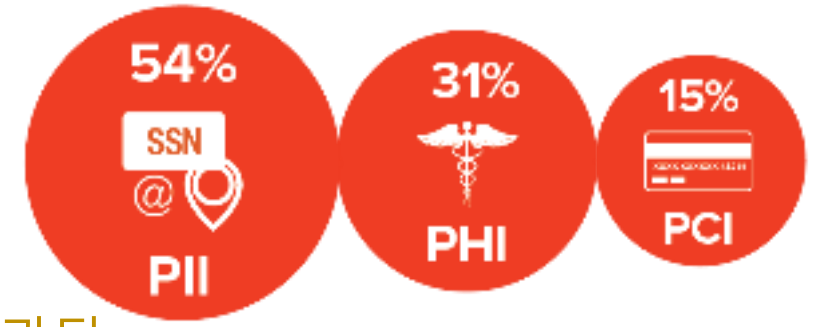
Shadow Data

사용자가 가지고 있는 파일중 25% 클라우드에서 보관됨

그 중에

12.5%

규제 준수 관련 정보를 포함한다



블루코트 보안 라이프사이클 방어 체계

효과적인 분석

- 모든 유형(SSL 포함)의 트래픽 분석
- 네트워크,객체, 웹, 세션 등을 분석,언제 발생이 되었고, 어떤 경로를 통해서 이루어 졌는지 상관관계 분석을 통해 근원 분석 (어떤 경로를 통하여 악성코드가 다운로드 되었는지 분석)
- 특정 의심 시점 재연(타임라인)
- 분석되고 검증되어진 정보는 차단정책으로 업데이트

강력한 차단

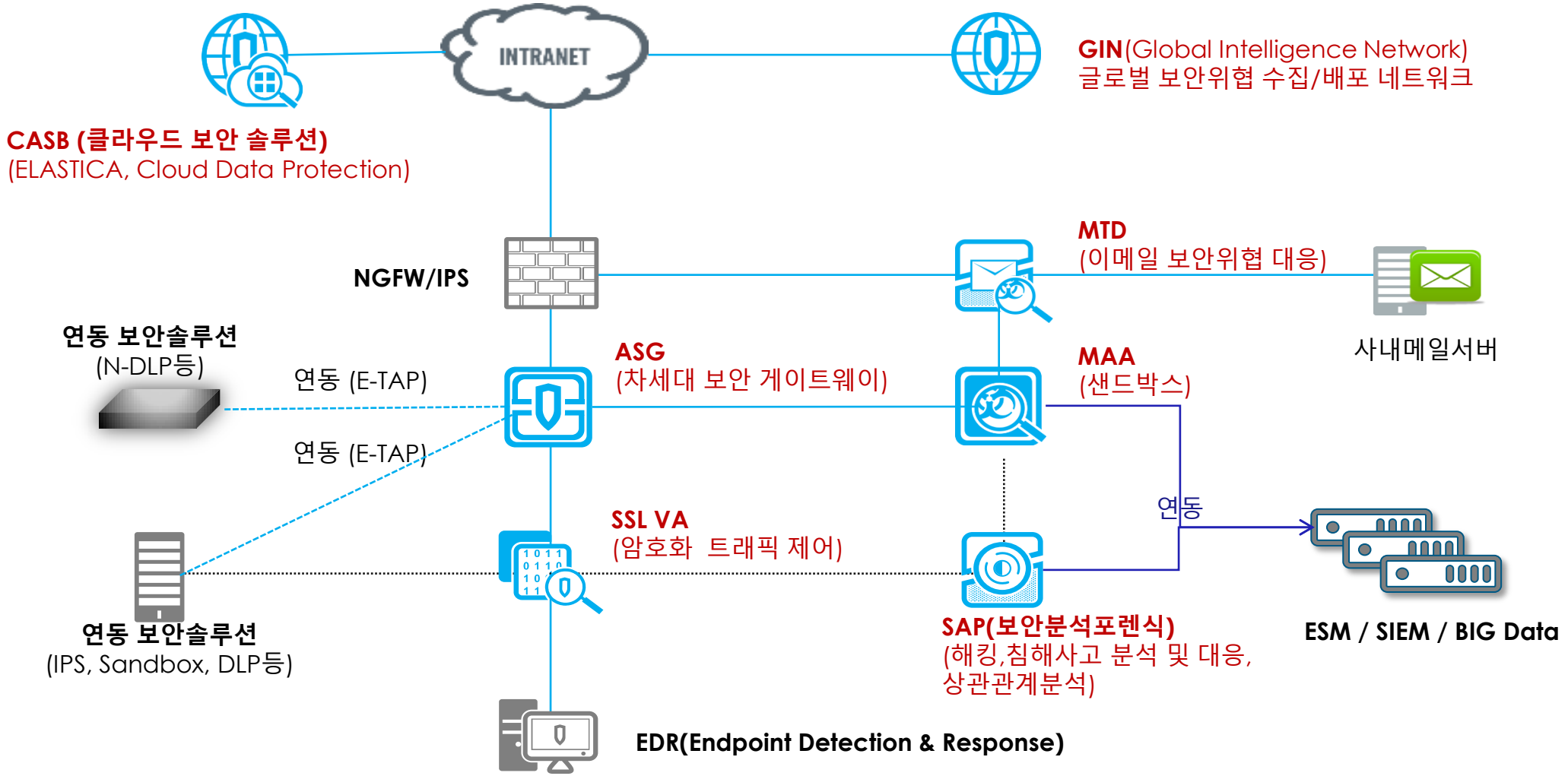
- 알려진 모든 위협에 대한 탐지 및 차단
- 알려지지 않은 공격에 대해서는 분석을 위한 에스컬레이션
- 분석되고 검증되어진 정보는 다시 차단정책으로 업데이트

보안 라이프사이클 방어 솔루션

클라우드	클라우드 접근/데이터 보안 (Elastica/Cloud Data Protection)	▪ PUBLIC CLOUD 접근 및 사용에 대한 가시성, 보안, 위협 차단 ▪ CLOUD 데이터의 안전한 보호 및 Compliance대응을 위한 Tokenization
분석	SSL 트래픽 처리/분석 - SSLVA (복호화 기술을 통한 분석)	▪ 호스트 카테고리에 따라 원하는 SSL 만 해독 ▪ 네트워크, 포트 변경 불필요, 모든 포트의 암/복호화 ▪ 250M~10G까지 SSL 성능 지원, 기존의 보안 제품을 연동
	패킷 기반의 전체 트래픽 분석 - SAP (근원 분석, 영향 분석, 증거 수집)	▪ 네트워크 감시 카메라, 편리한 사용 환경, 유연한 연계 ▪ 보안 위협에 대한 증거 확보, 경향 분석, 사건에 대한 재조합, 징후 경고 등
차단	알려지지 않은 악성코드 분석 - MAA (행위기반 분석)	▪ 정적 분석, 동적 분석, 행동 기반 분석 ▪ 유연한 커스터마이징 ▪ 강력한 API 를 활용한 다양한 보안 시스템과 연계 운영
	강력한 웹 보안 – ASG (분석정보를 바탕으로한 차단)	▪ 위협의 침입 경로 인 웹 및 이메일에 대한 실시간 대응을 위한 웹 접근 및 컨텐츠 차단/통제/관리 ▪ 제로 데이, 위험 수준이 높은 사이트 콘텐츠 선제적 대응 ▪ Good / Bad 파일 분류 ▪ 10억개 이상의 Good/bad 파일 DB 보유. 매일 백만개의 파일 업데이트 지원 등

BLUE COAT

보안 라이프사이클 방어 솔루션



클라우드 보안 솔루션

SOC 1.0

Traditional On-Premise SOC

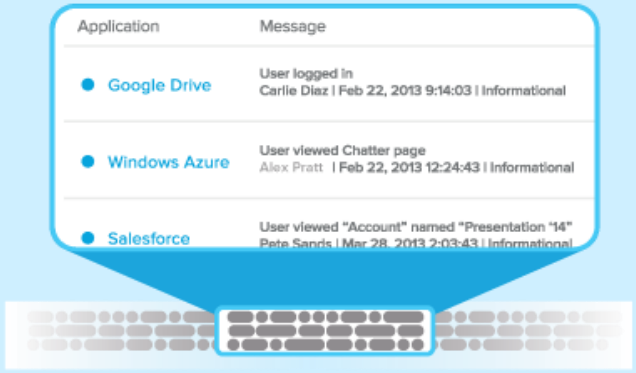
- Risk Assessment
- IDS/IPS
- DLP
- Firewall
- SIEM
- FORENSIC

PRE-CLOUD ERA

BLUE COAT

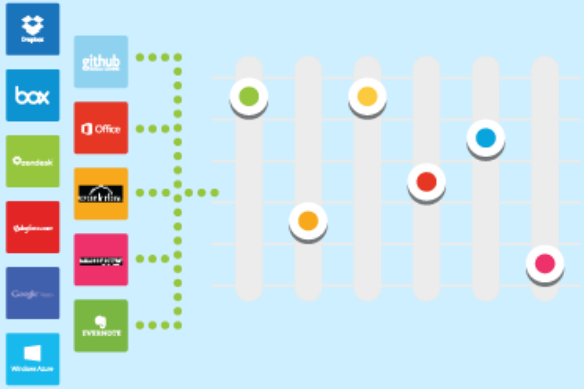
클라우드 보안

시각화



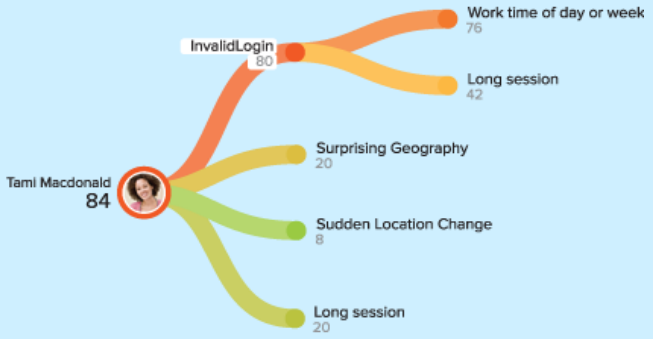
실시간으로 클라우드
응용 프로그램
사용 현황 시각화

효과적인 제어



클라우드에서
쉐도우 데이터에 대한
제어

지능적인 분석

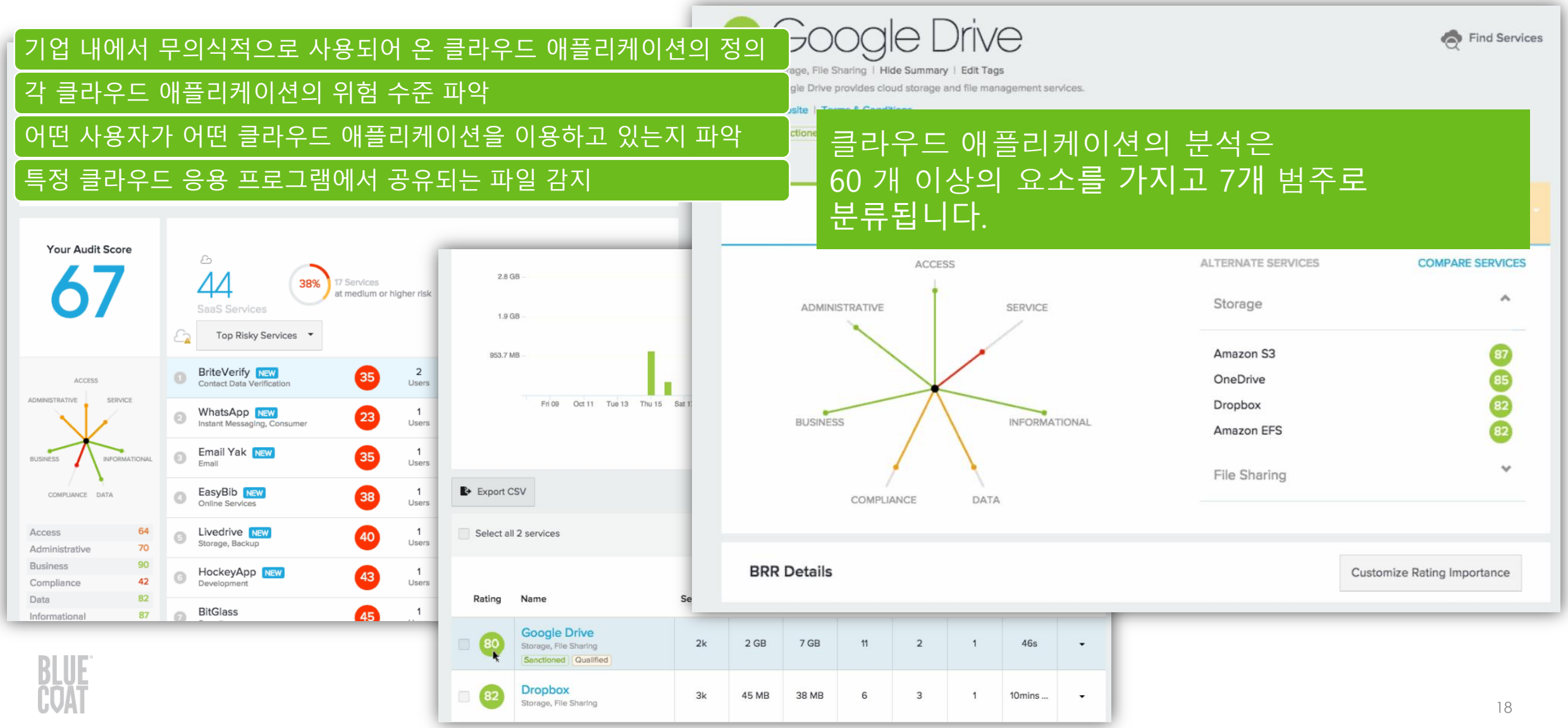


실시간으로 변화하는
사용자의 행동 패턴에서
위험 요소 분석

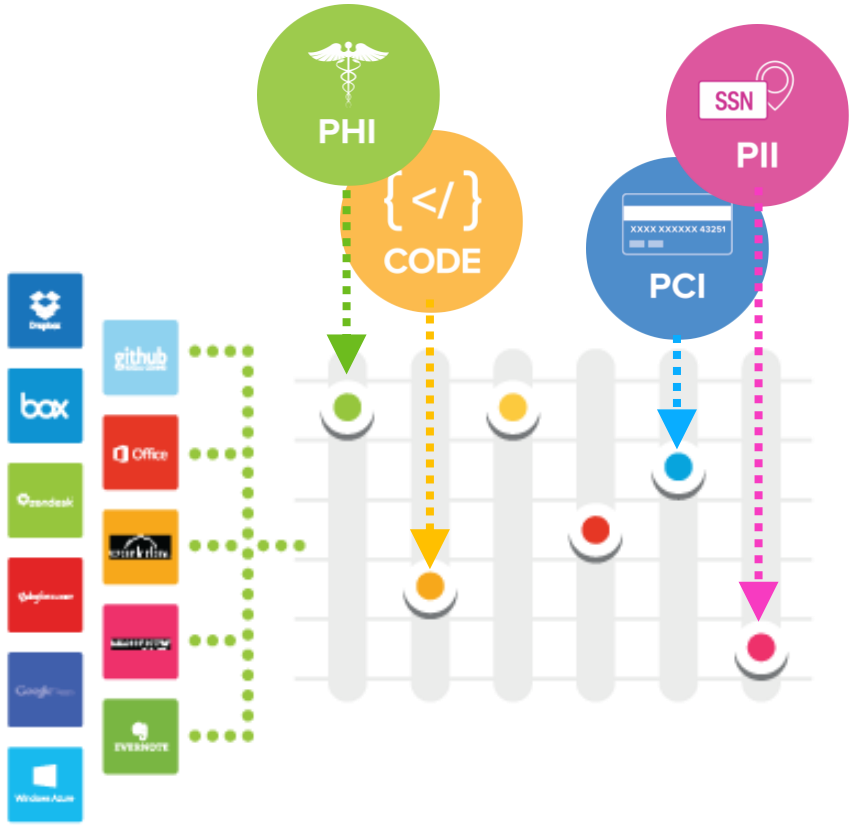
시각화 – 클라우드 어플리케이션의 위험을 분석

- 기업 내에서 무의식적으로 사용되어 온 클라우드 애플리케이션의 정의
- 각 클라우드 애플리케이션의 위험 수준 파악
- 어떤 사용자가 어떤 클라우드 애플리케이션을 이용하고 있는지 파악
- 특정 클라우드 응용 프로그램에서 공유되는 파일 감지

클라우드 애플리케이션의 분석은
60 개 이상의 요소를 가지고 7개 범주로
분류됩니다.



효과적인 제어 시행 - 위험 제어/통제



클라우드보다 먼저쉐도우 데이터를 컨트롤

- 데이터 유출 방지 정책 시행
- 액세스 제어를위한 정책 시행
- 파일 공유 및 전송을 제한하기위한 정책 시행
- 사용자 별 위험 값에 기초한 정책 시행

→전체적인 동작에 따라 적절한 정책을 제정 가능

→기밀 준수 관련 콘텐츠 관리

→콘텐츠의 유형에 따라 정책의 시행

→업계 기준에 따라 위험의 판단
(PII, PCI, PCI, FERPA, GLBA, ...)

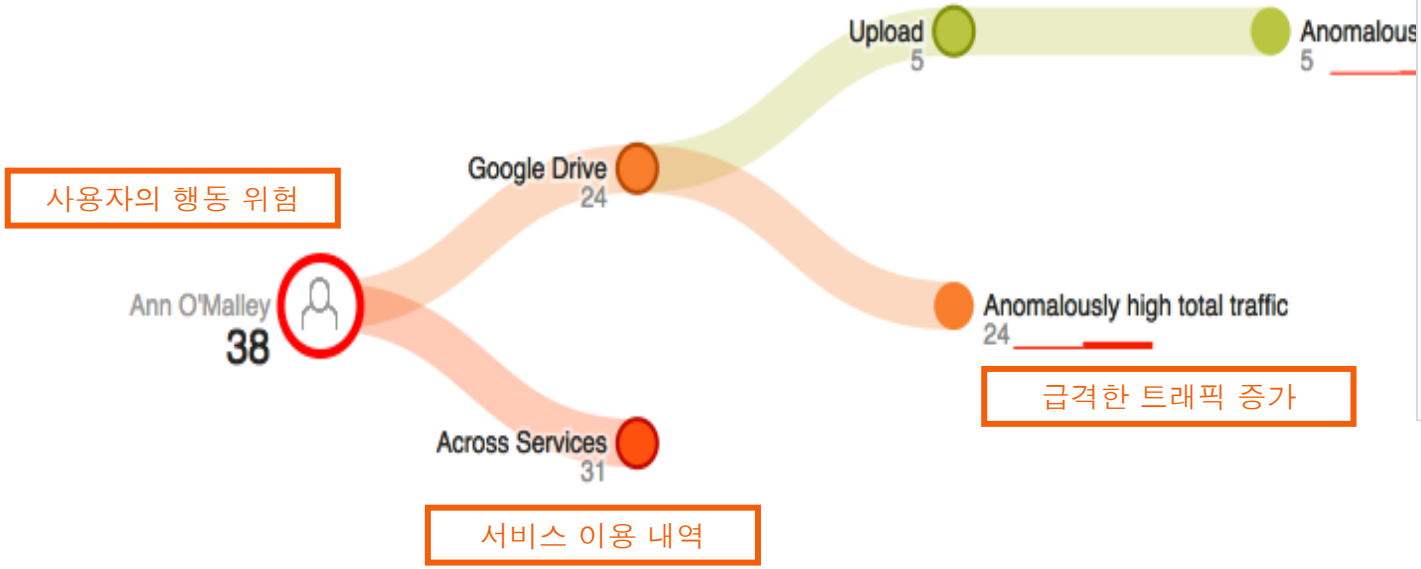
→프로필 커스터마이즈 대응

→위험도가 높은 파일에 대한 적절한 정책 자동 적용

BLUE COAT

지능적인 분석

- 임계 값을 기반으로 수상한 사용자의 동작을 감지
- 행동에 따른 수상한 사용자의 동작을 감지
- 이벤트 발생 순서에 따라 수상한 사용자의 동작을 감지



사용자의 행동 위험

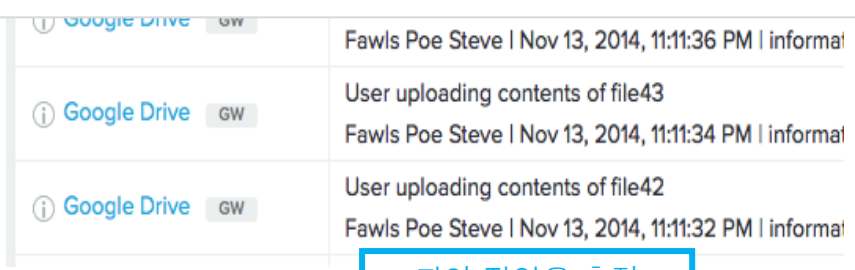
급격한 트래픽 증가

서비스 이용 내역

로그인 실패

평일 이외의 액세스

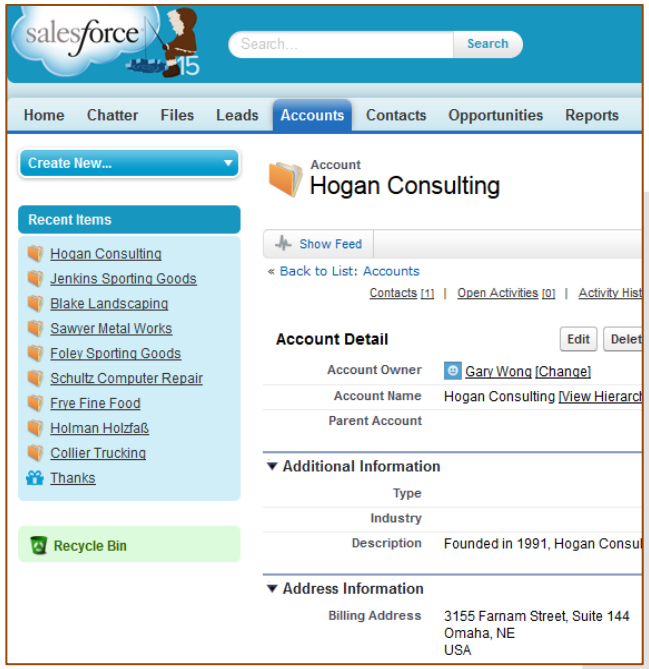
장시간 로그인

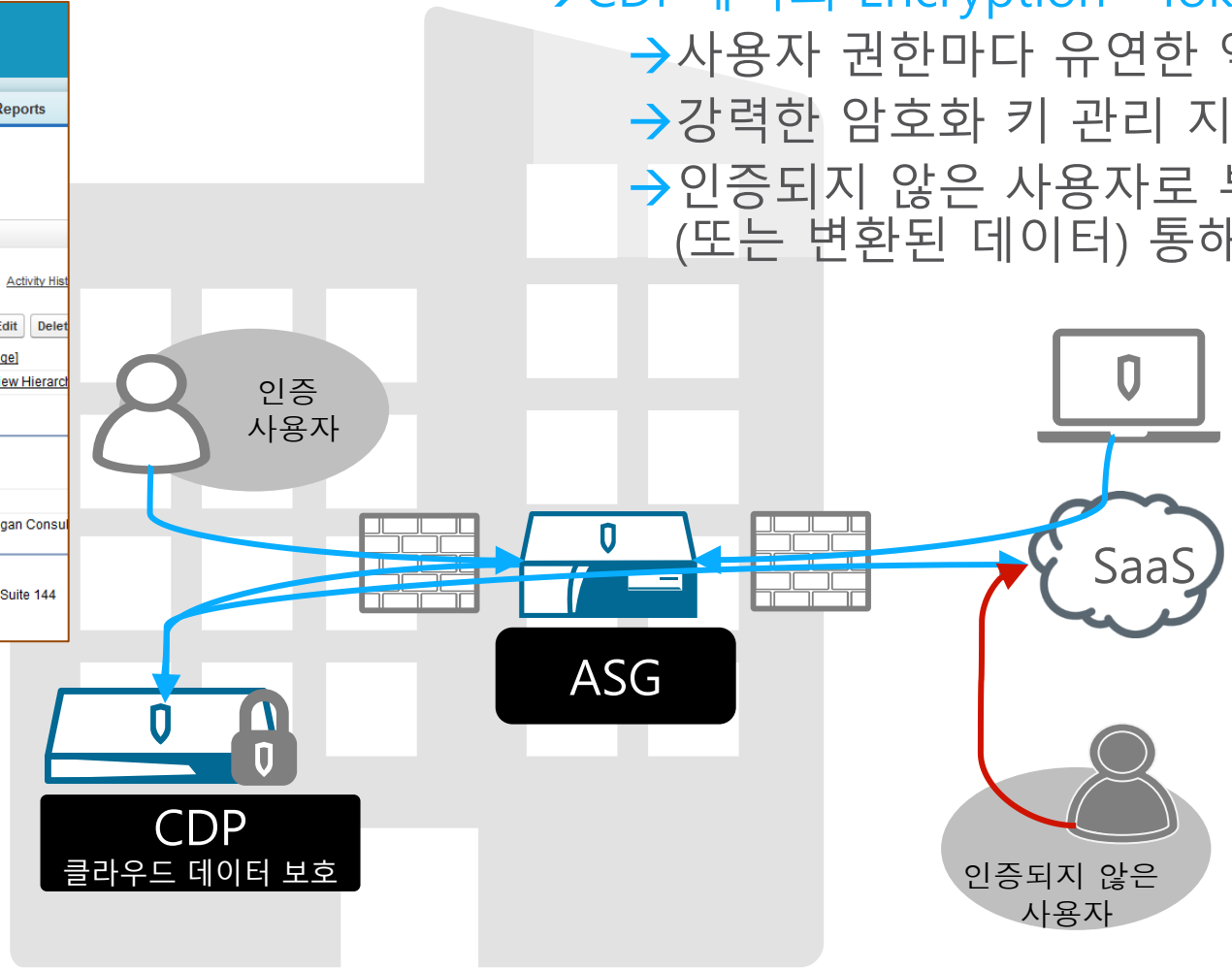


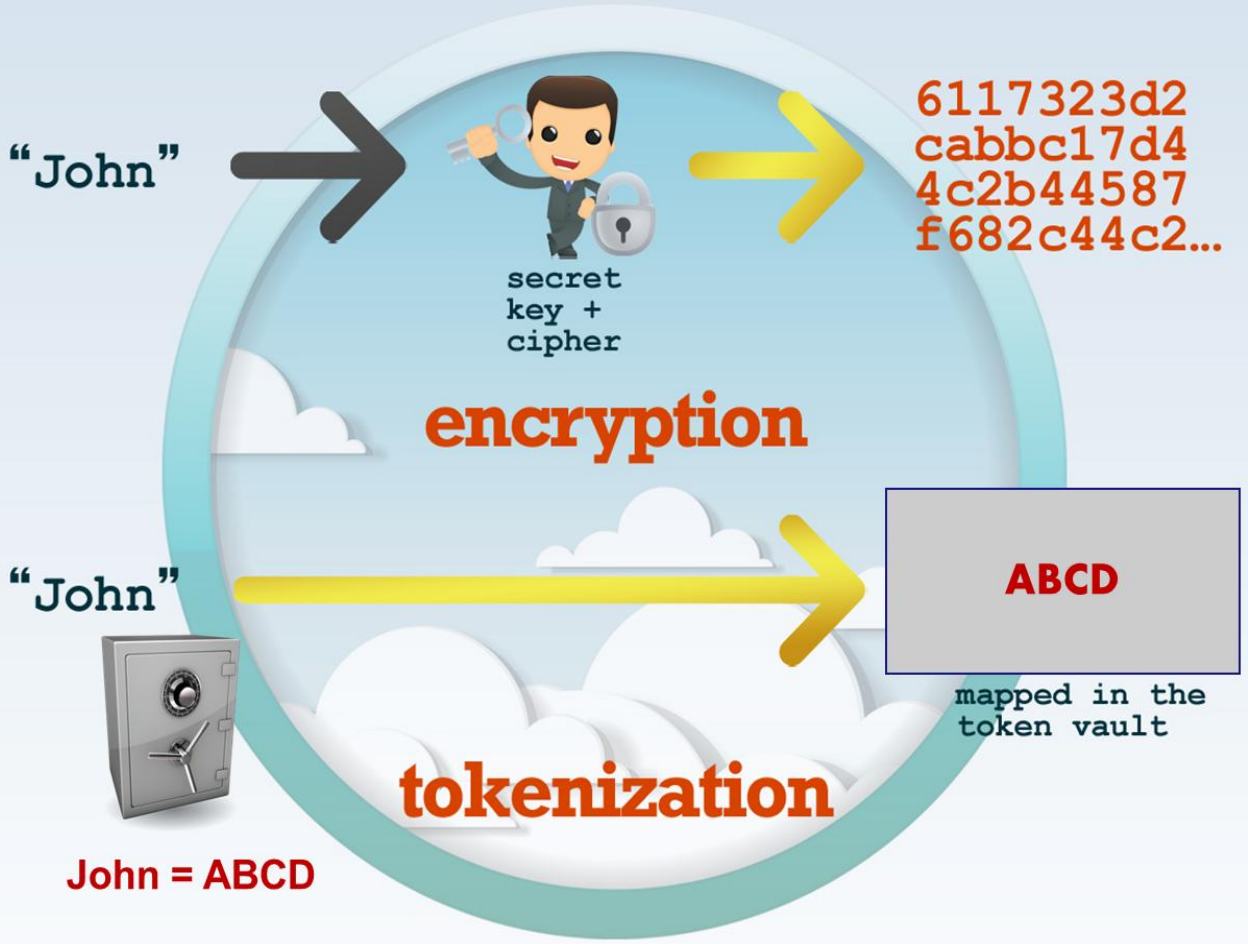
파일 작업을 추적

클라우드 환경에서 데이터 보호

→CDP에서의 Encryption · Tokenization 정책 시행
→사용자 권한마다 유연한 액세스 정책 시행
→강력한 암호화 키 관리 지원
→인증되지 않은 사용자로 부터 암호화된 데이터를 (또는 변환된 데이터) 통해 데이터 보호







Encryption

- Protection via "transformation"
- Mathematical link

Tokenization

- Protection via "replacement"
- No mathematical link

블루코트 클라우드 보안 솔루션

클라우드 시각화 및 인텔리전스

- → 비 인가 클라우드 액세스의 발견
- → 응용 프로그램, 데이터, 사용자 분석
- → 클라우드 리스크의 파악
- → 네트워크 트래픽의 기록과 증거의 확보

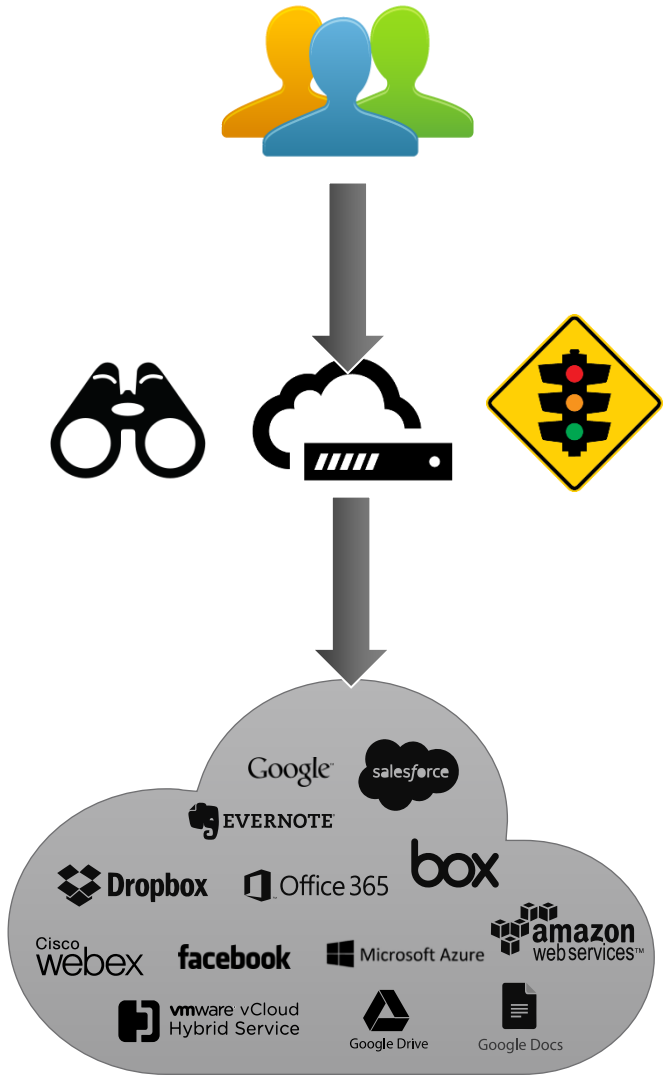
클라우드 액세스보안

- → 클라우드의 이용에 대한 제한 · 통제하는 정책의 시행
- → 악성 코드 방어
- → 유출 위험을 방지하기 위해 데이터의 검사
- → 정책 시행을위한 해독

데이터 보호 및 제어

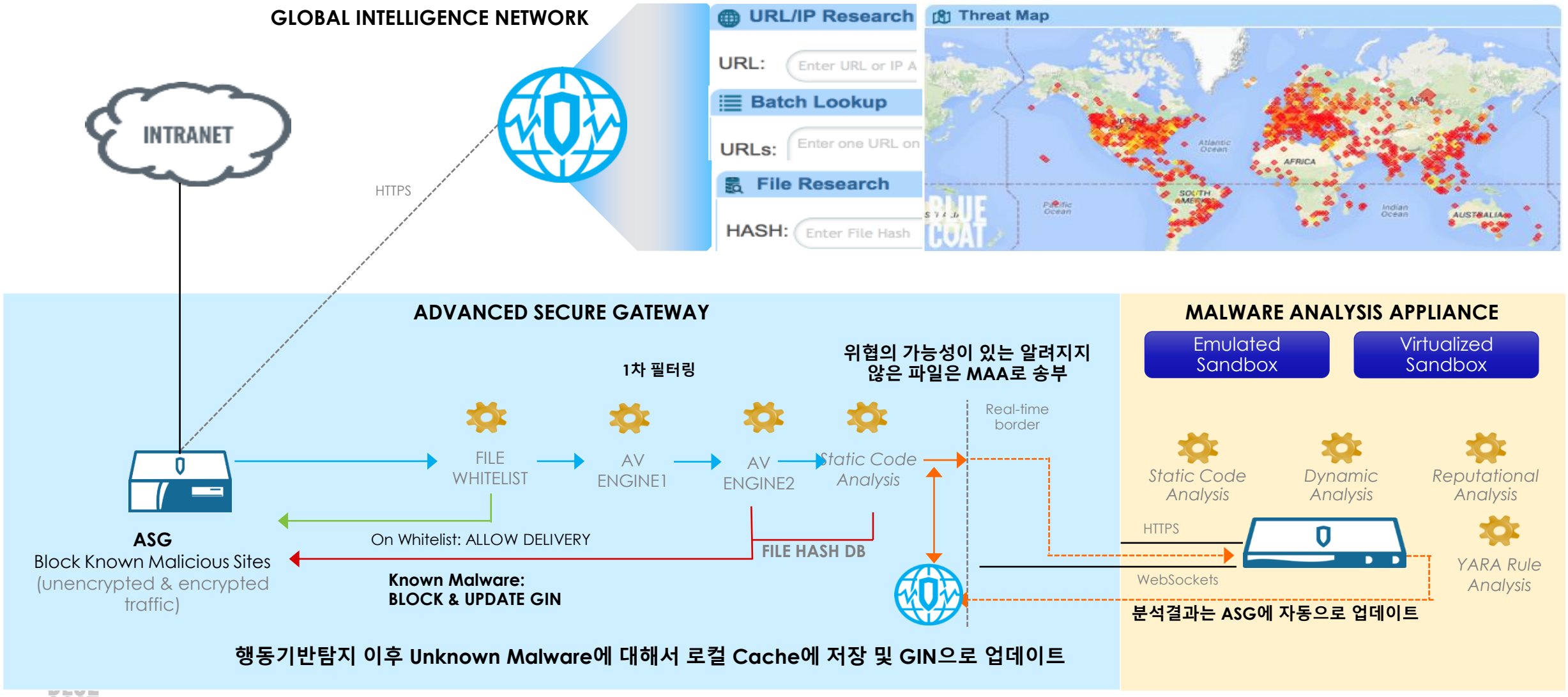
- → 토큰화, 암호화
- → 클라우드 기능은 유지
- → 클라우드 데이터 저장 위치에 의존하지 않고 규정 준수 가능한 데이터 보호 체계

클라우드를 포함한 차세대 웹 보안 게이트웨이 제공

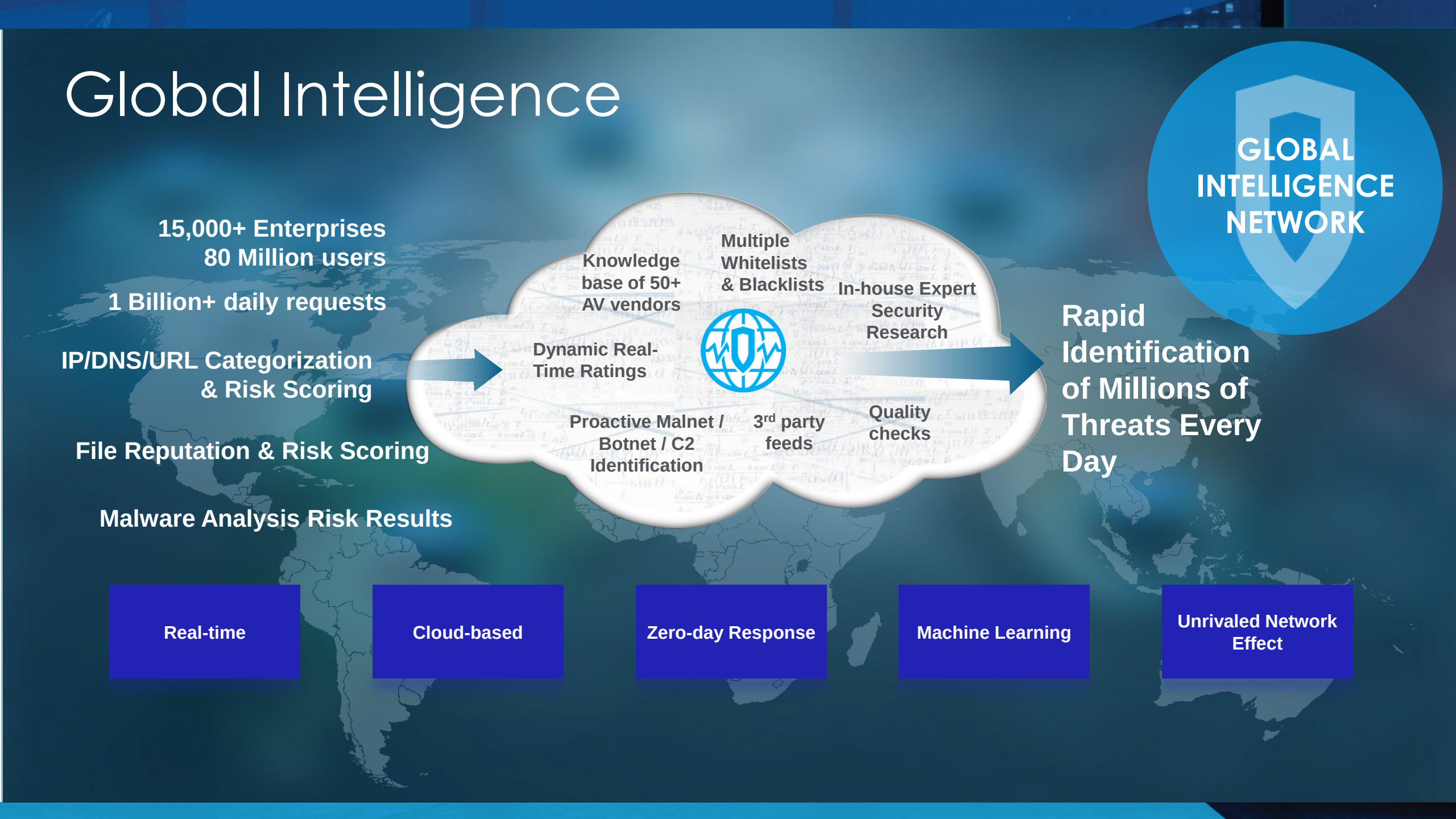


BLUE COAT

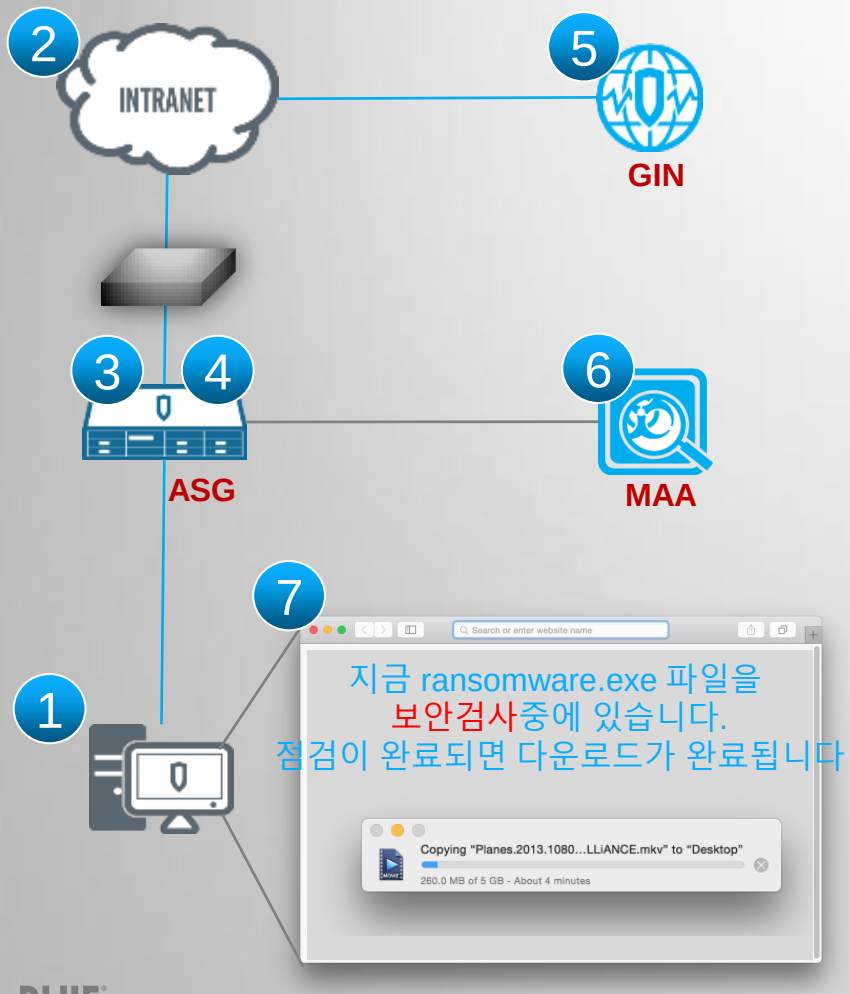
블루코트 지능형 보안 위협 차단 솔루션



Global Intelligence



랜섬웨어와 블루코트 보안 솔루션



1.인터넷 사용이 정책적으로 허용된 접속

2. 허용된 다운로드 발생

3. GIN으로 알려진 좋은 파일 혹은 알려진 나쁜 파일에 대한 1차 탐지

4. Dual AV 엔진 탐지

5. 블루코트 클라우드를 통한 시그네이처 DB의 주기적인 업데이트

6. 탐지되지 않은 파일은 MAA로 전송하여 행동기반탐지

7-1. 행동기반탐지 시 사용자의 웹페이지에는 보안검사중이라는 안내메시지 전송

7-2. 행동기반탐지에 의해 확인된 Unknown Malware는 Hash에 의해서 사전 차단

GIN (Global Intelligence Network) : 글로벌 보안위협 수집/배포 네트워크
ASG (Advanced Secure Gateway) : 차세대 웹게이트웨이
MAA (Malware Analysis Appliance) : 행동기반 탐지 솔루션

BLUE COAT

블루코트 지능형 보안 위협 분석 솔루션

다양한 보안 위협(Breached)을 방어하기 위해서는, 어떤 방법으로 무슨일이 일어났는지를 확인할 수 있는 효과적인 방법이 필요합니다.

실시간 기반으로 트레픽 및 컨텐츠를 통제하는 지금의 보안 시스템은, 유입되는 멜웨어나 유출되는 내부자료를 감사증적(Audit Trail) 하는 방법을 제공하지 않습니다

BLUE COAT

모든 트래픽에 대한 전체 보안 가시성 제공

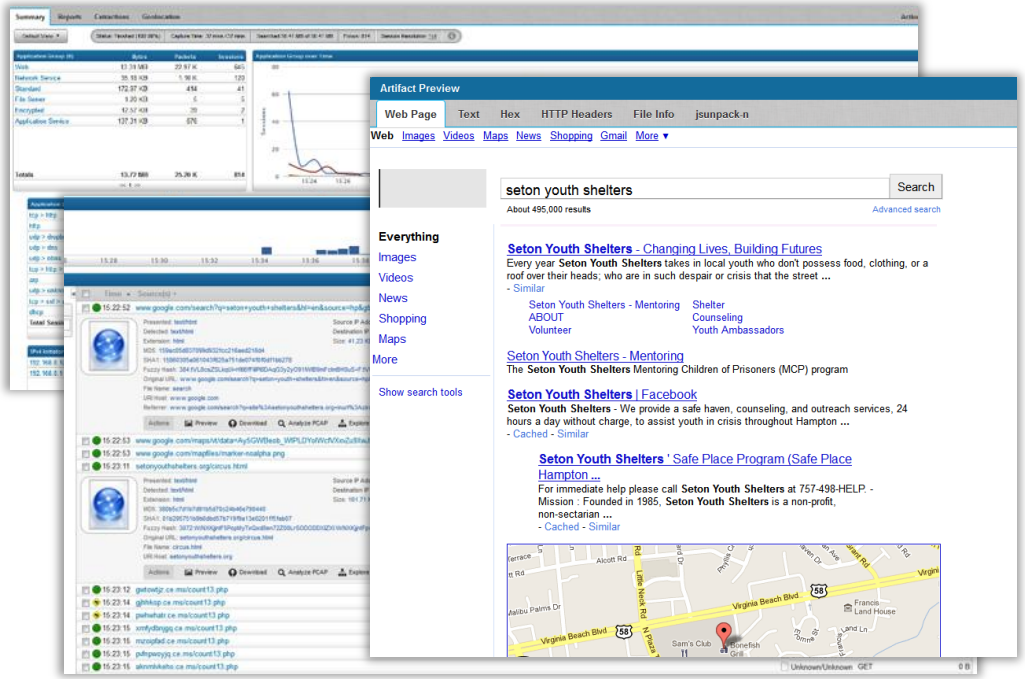
Full Security Visibility of All Network Traffic

- 고성능의 패킷 로스 없는 완벽한 트래픽 수집 (24/7 – all ports/all traffic)
- 2400여 개 이상의 어플리케이션 분류 제공 (Layers 2-7 indexing)
- 이벤트 재연 제공 (full packet, flow, session & file reconstruction)
- 다양한 보안 장비와의 연계를 통한 이벤트 검증
  (SIEM, IPS, Sandbox, FW, NGFW 등)
- 다양한 형태의 솔루션 제공으로 유연한 확장성 제공
  (appliance/software/virtual appliance)
- Anomaly Detection (Rule 설정 및 별도의 Rule 설정 없이
  Machine Learning 기술을 활용하여 수행)

BLUE COAT

주요 특징 – 세션 재조합

- 어플리케이션 레이어에 대한 세션 단위 재조합
- 웹 페이지 재연
- 이메일, VoIP, 메신저 등 재연
- 세션 기반의 데이터에 대한 다양한 필터링 제공
  - Search by MD5 or SHA1 hash
  - Filename, size, file type, etc.



Example Artifacts	**Archive files** (zip, rar, rpm), **Images** (bmp, gif, jpg, png), **Multimedia** (avi, flash, mov, mpg, wav, wmv), **Office files** (doc, docx, ppt, pptx, wpd, xls, xlsx), **PDF**, **DLL**, **EXE**, **HTML**, **Java**, **FTP**, email…more

"I view an email as an email and a Word doc as a Word doc.
***Not just a bunch of packets.** Nice!"*

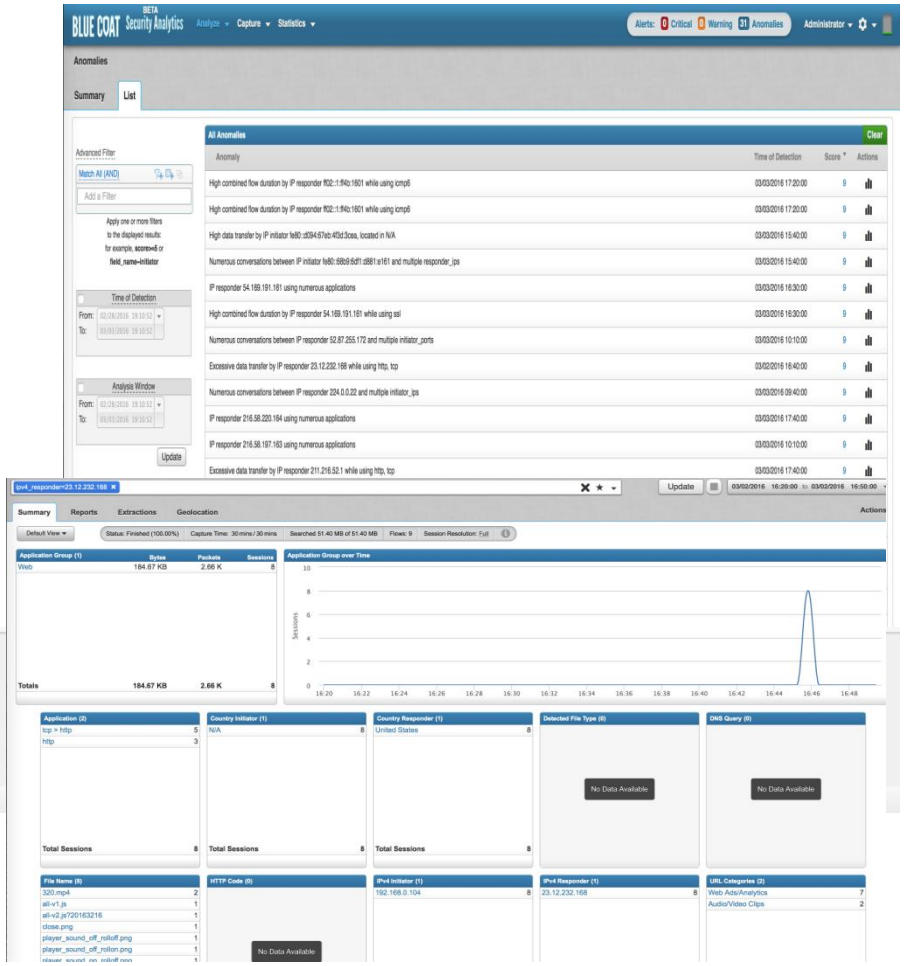
BLUE COAT

Anomaly detection

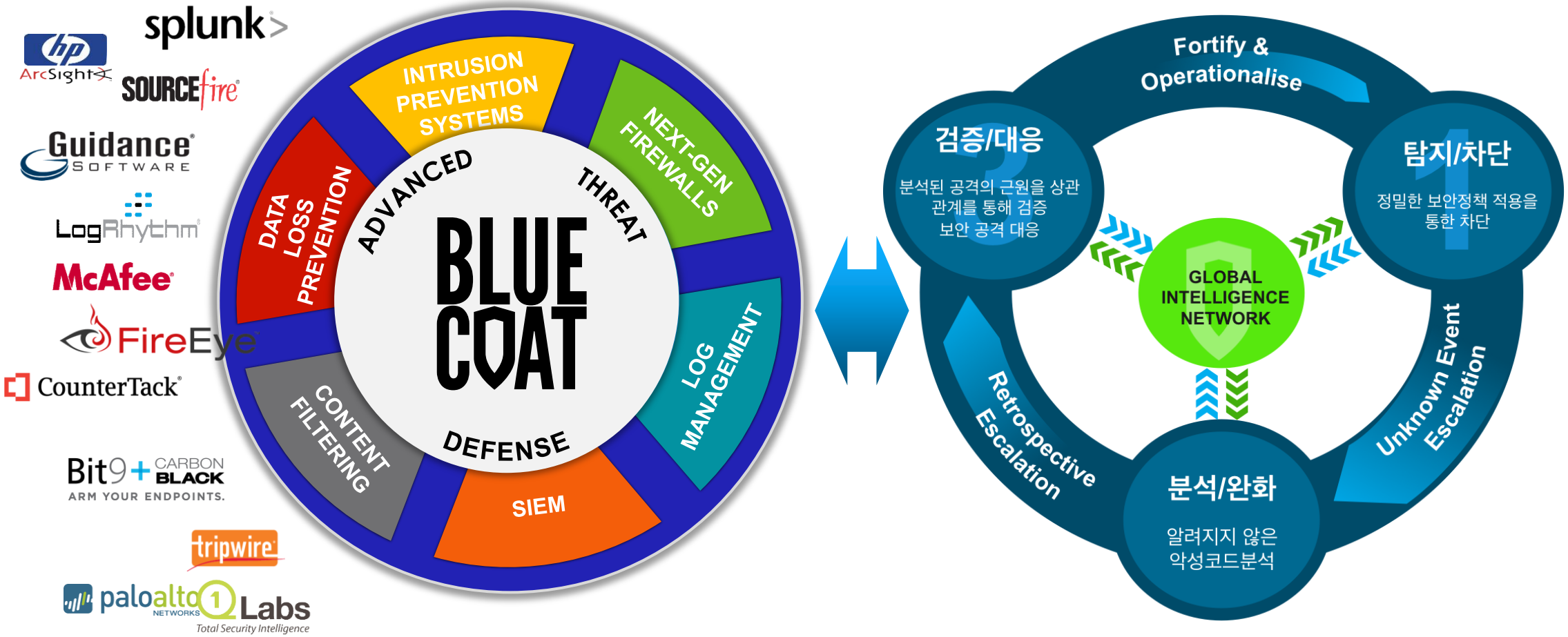
using machine learning technology

- 자동으로 경고를 발생
  - 하나의 dst IP에서 다양한 종류의 프로토콜이나 어플리케이션이 사용
  - 하나의 dst IP와 짧은 시간동안 많은 양의 통신이 발생되는 경우
  - 대용량의 데이터가 업로드 되는 경우
    (일정시간 동안 데이터 업로드 행위가 없었는데, 갑자기 drop box 등에 파일을 업로드 하는 행위가 발생되면서 이벤트 발생)
  - ssh, telnet 접속이 평상시 없었던 src IP를 통해 발생될 경우 이벤트 발생

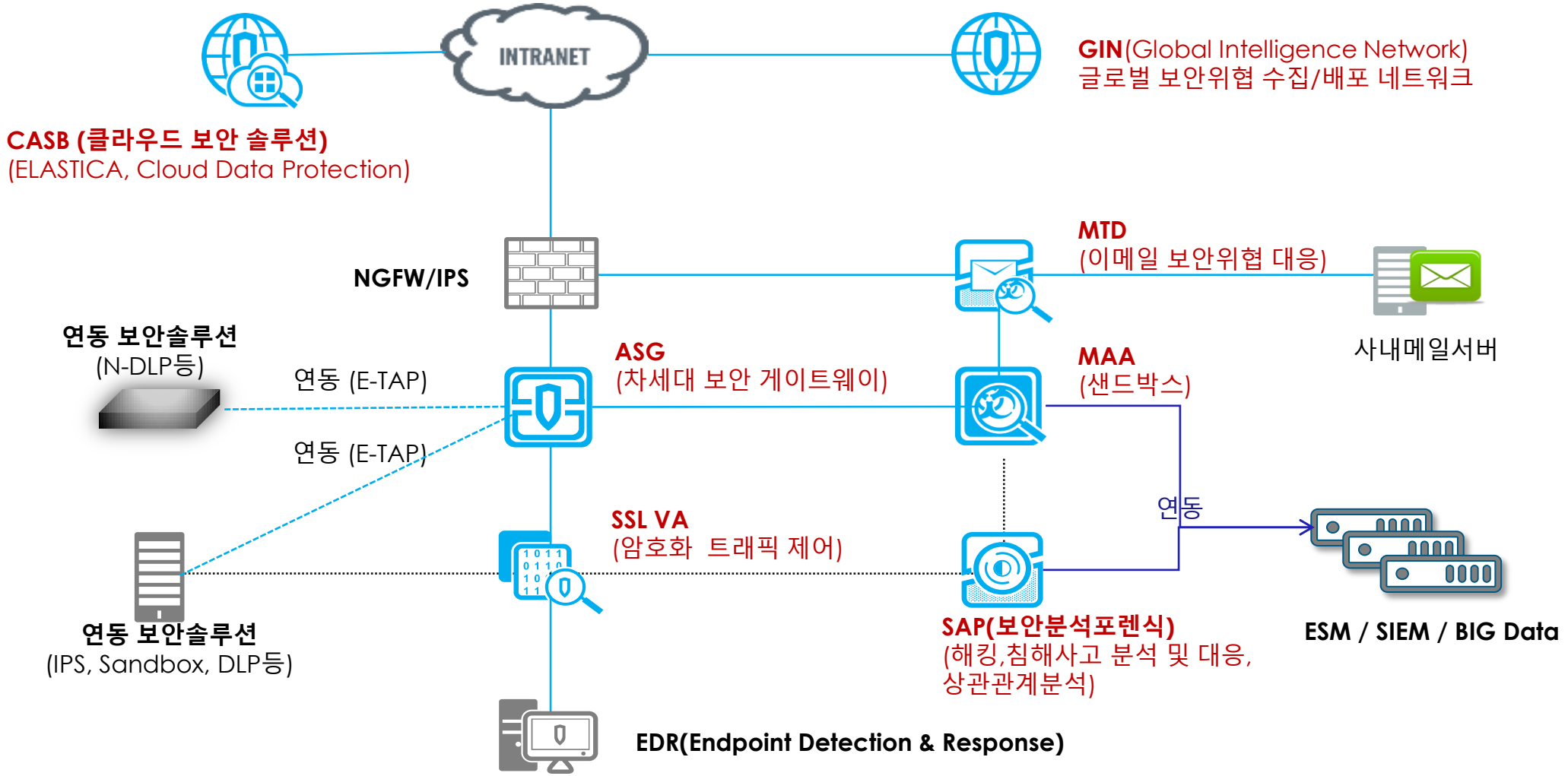
- 기본적으로 위와 같은 이벤트는 별도의 Rule 설정 없이,
  장비가 일정시간 동안 학습한 정보를 기반으로 축적된 데이터 분석을 통해 평상시와 다른 이상 패턴이 발생되면 자동으로 경고를 발생



협업을 통한 가시성 확보



블루코트 보안 솔루션 (Network + Security + Cloud)



Q&A


BLUE COAT
Network + Security + Cloud
감사합니다.