BLUE COAT

Security Empowers Business

진화하는 타겟 공격에 대한 기업의 현실적인 대응 방안

BLUECOAT KOREA

2015/04

BLUE COAT

Security Empowers Business

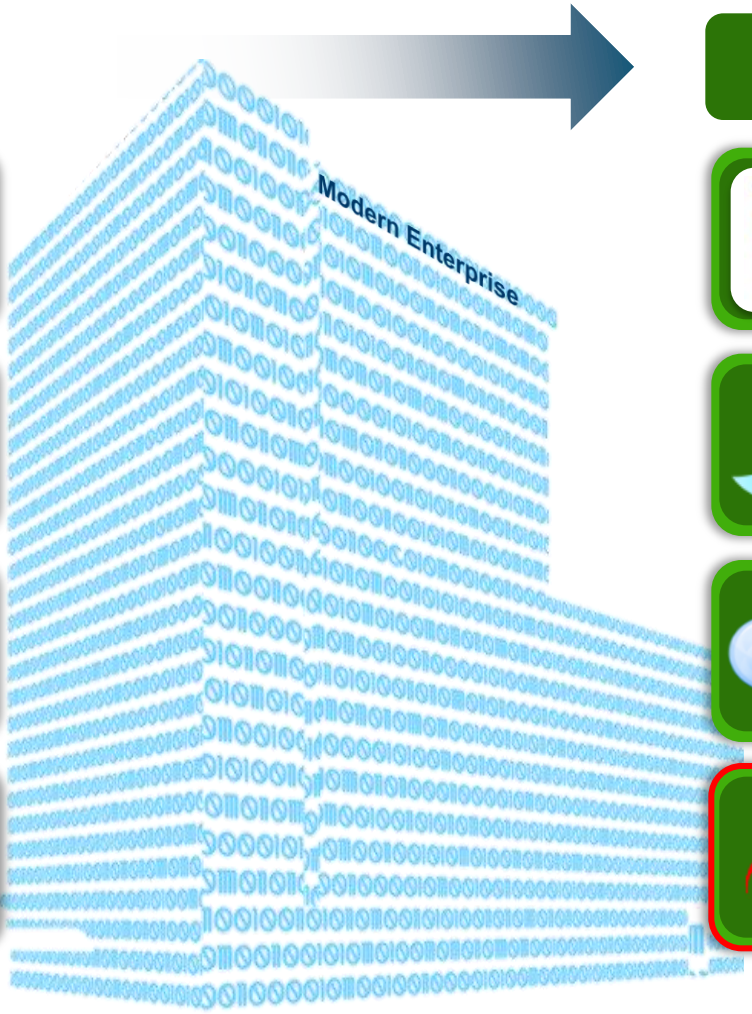
목차

- 보안위협의 진화
- 기업에서의 보안
- 지능화 공격 대응의 필요 사항

IT의 변화

YESTERDAY'S IT

- Few apps with predictable behavior
- Manageable data
- Infrastructure that's on-premise
- Traditional threat environment



TODAY'S IT

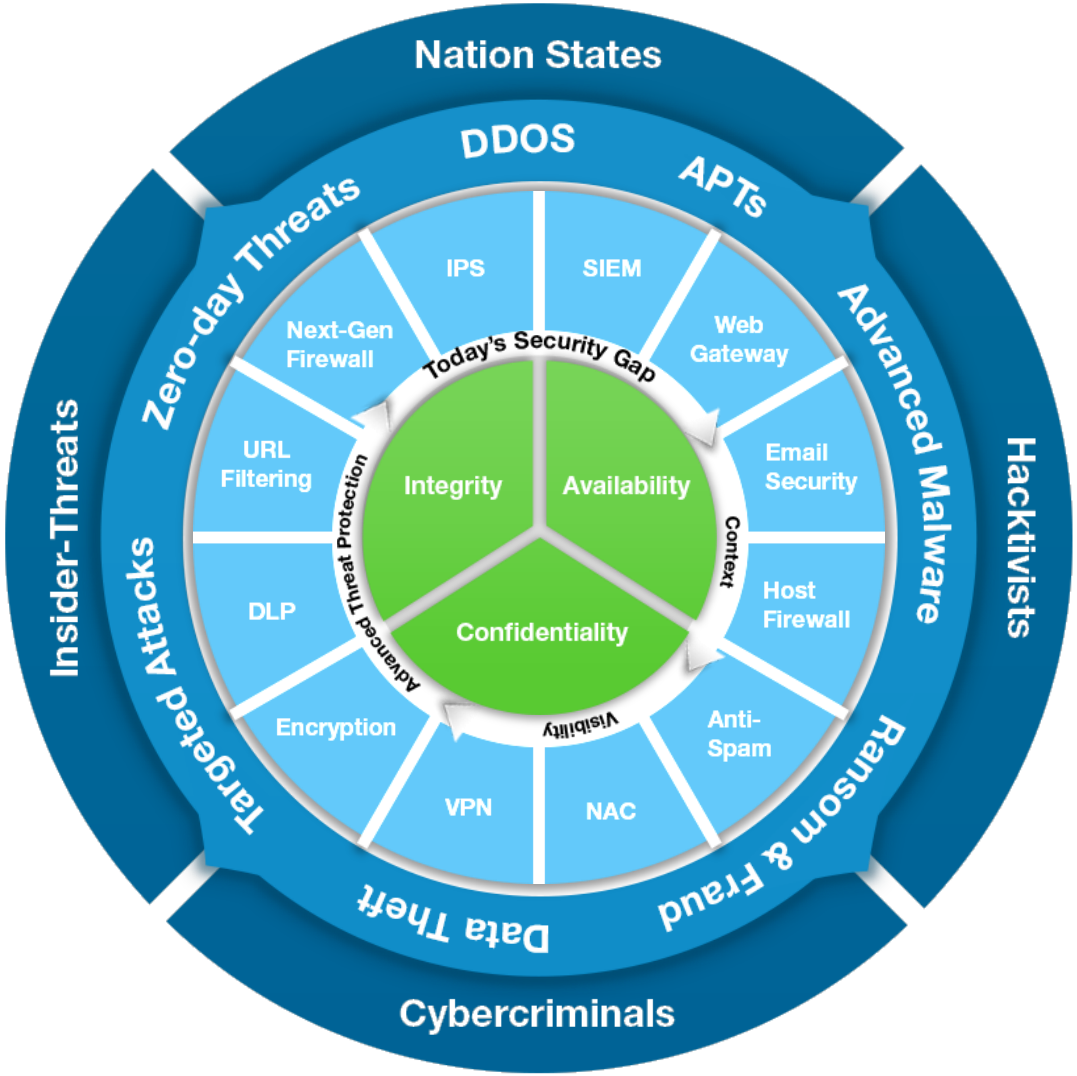
- Millions of unknown and risky Apps
- Big data explosion
- Cloud and hybrid infrastructure
- Advanced threat environment

최신 사이버 공격의 유형

다양한 목적을 갖는 TARGET 공격 수행

- 새로운 Advanced Threats 4년간 300% 증가
- 2초마다 3만개의 Malware가 발견됨
- ATP 공격으로 평균 60억 원의 피해 발생

블루코트 보안 연구소, 2014



2015년 주목해야 할 사이버 공격 TREND

- Encrypted traffic will increase and malware will increasingly hide behind encryption to evade detection
- Big media will say NO to malvertising.
- 2015 will be the year of PUS
- Unmarked bills or you'll never see your data again.
- Attackers will get social.
- Big Brother will absolutely be watching
- Heartbleed, Shellshock and Poodle, oh my. Expect more ‘common mode failure’ events,

일반 기업 보안 환경

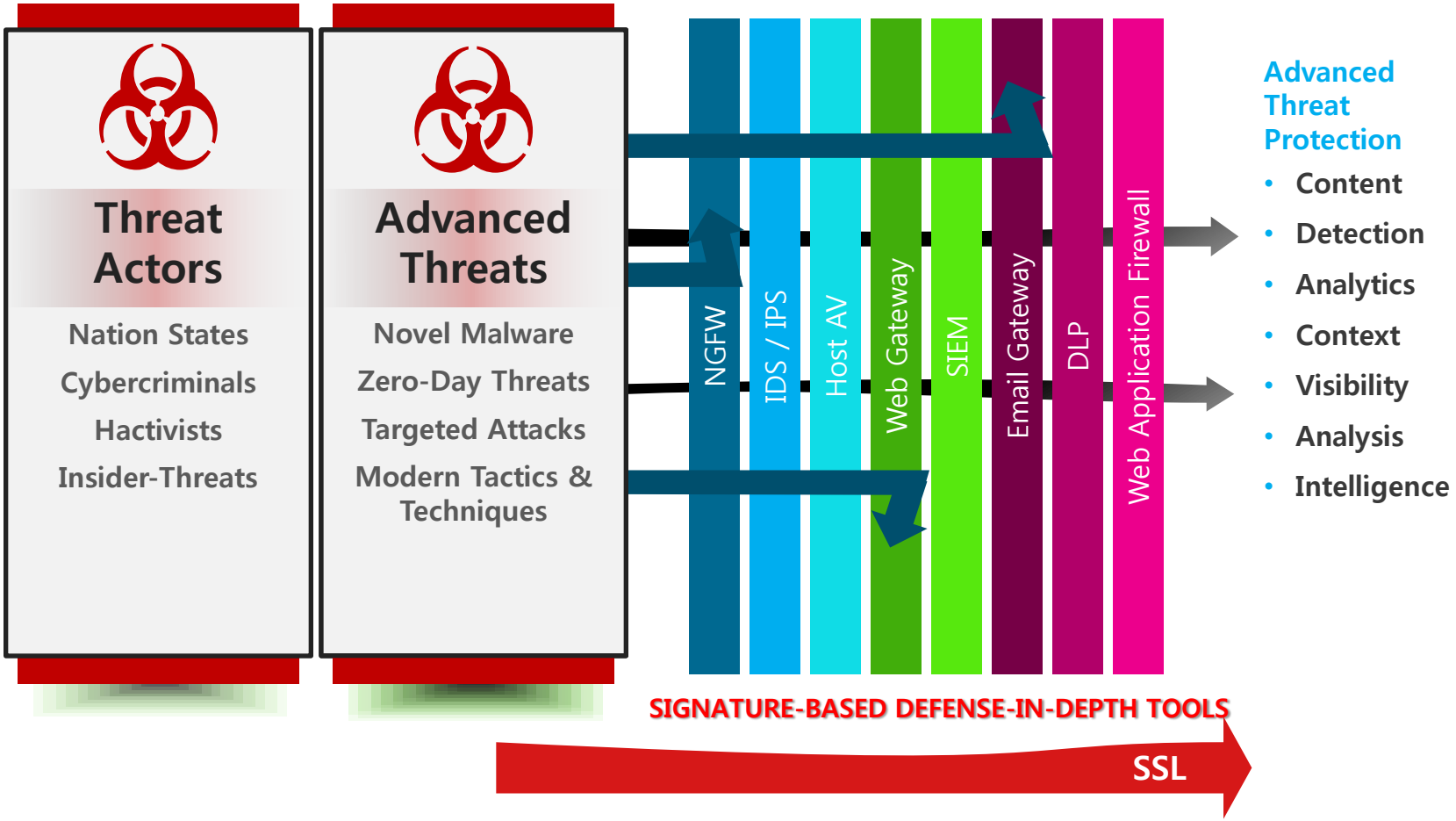
최신의 최고의 보안 시스템 구축 운영 및 지속적인 컨설팅/모니터링 수행

기업들의 보안 현실

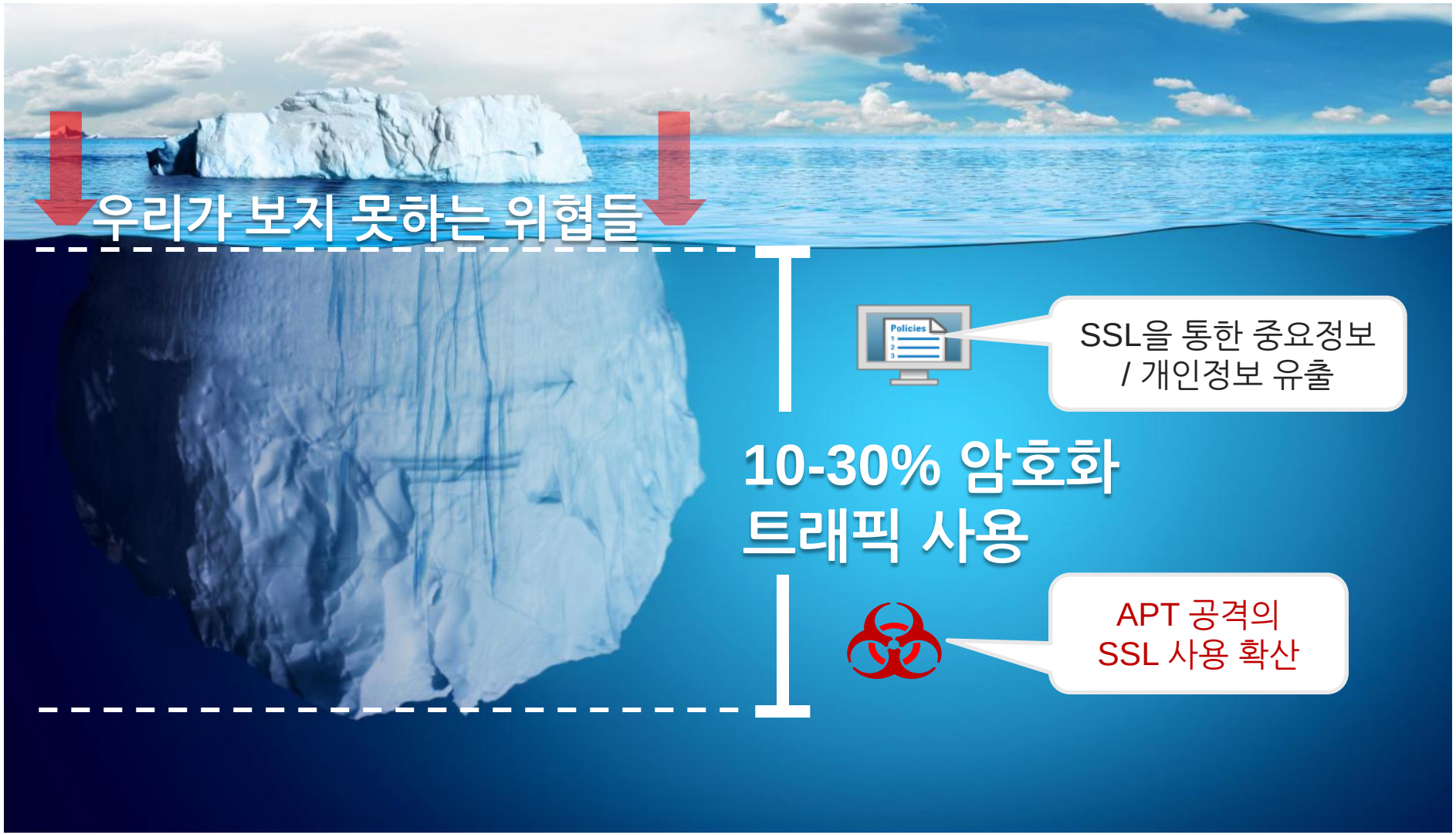
어떤 경고가 진짜 위험한지 알기 어려움

현 보안 운영의 어려움

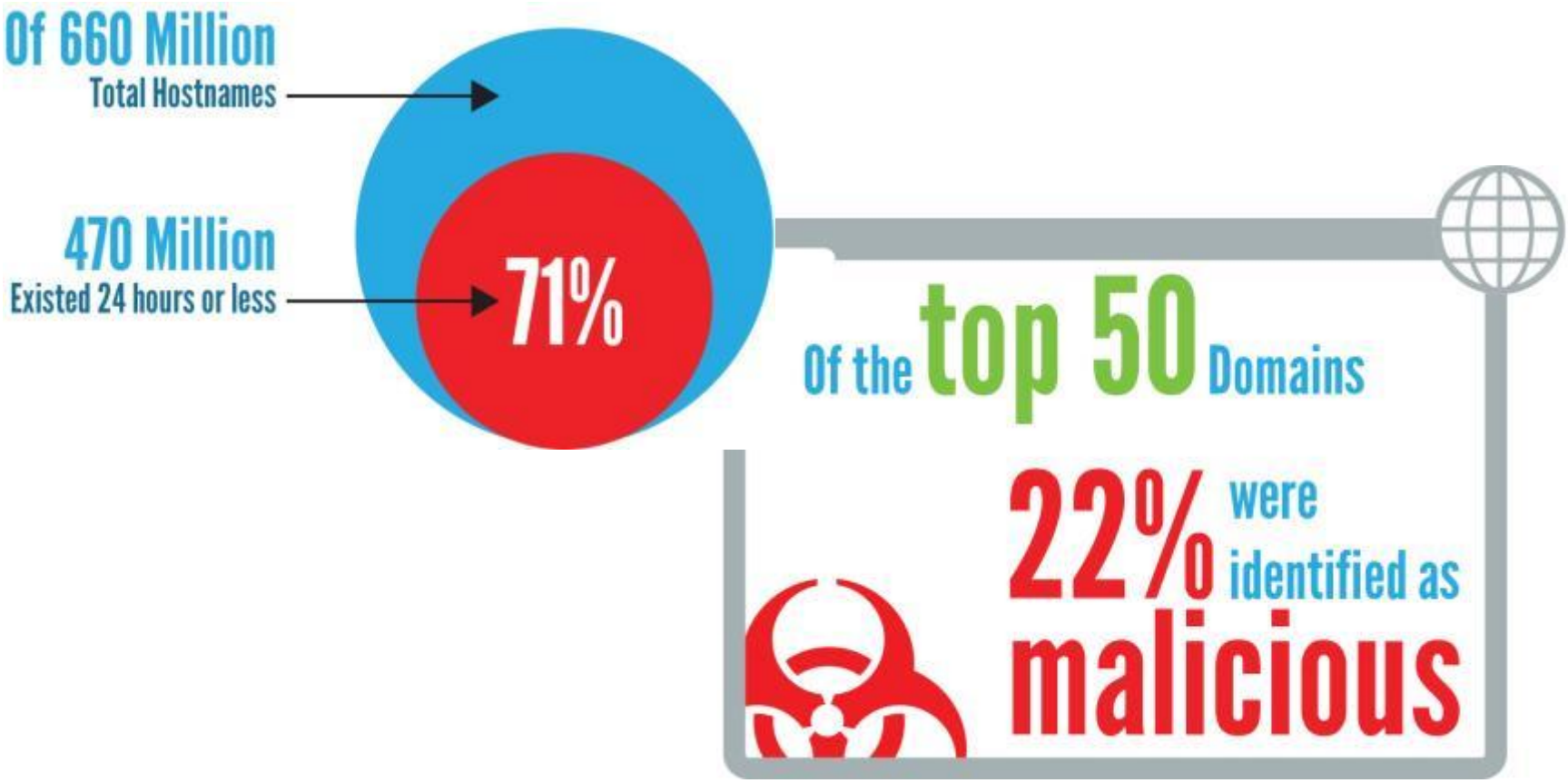
솔루션 도입만으로 APT를 막는 것은 어려움



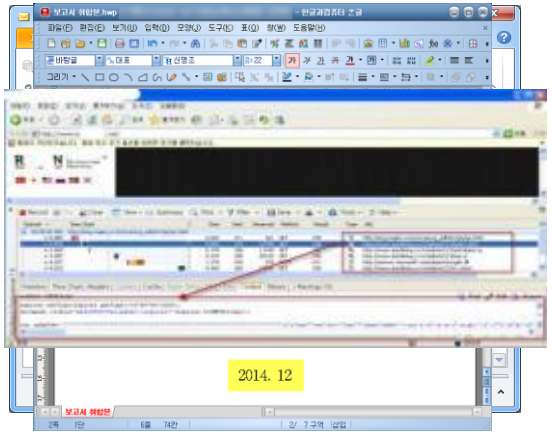
암호화 채널을 이용한 보안 위협 증가



공격은 순간, ROOT CAUSE를 찾기 어려움



기업의 보안 위협 사례



공격 준비
타겟 분석
공격 셋업
접속정보 분석
시스템 침투 경로 확보
공격 시작
타겟 접속
내부 권한 상승
내부 정보 유출
공격 완료
TIME

실제 공격자 정보유출 작업 기간

TIME
물리적 보안
악성코드 분석
방어 구축
공격 예측
모니터링 및 컨트롤
공격 인지
징후 리포팅
치료 및 삭제
피해상황 확인
임팩트 분석
시스템 전수조사
분석
공격 발견

최고의 보안 인프라에서도 보안 사고는 증가

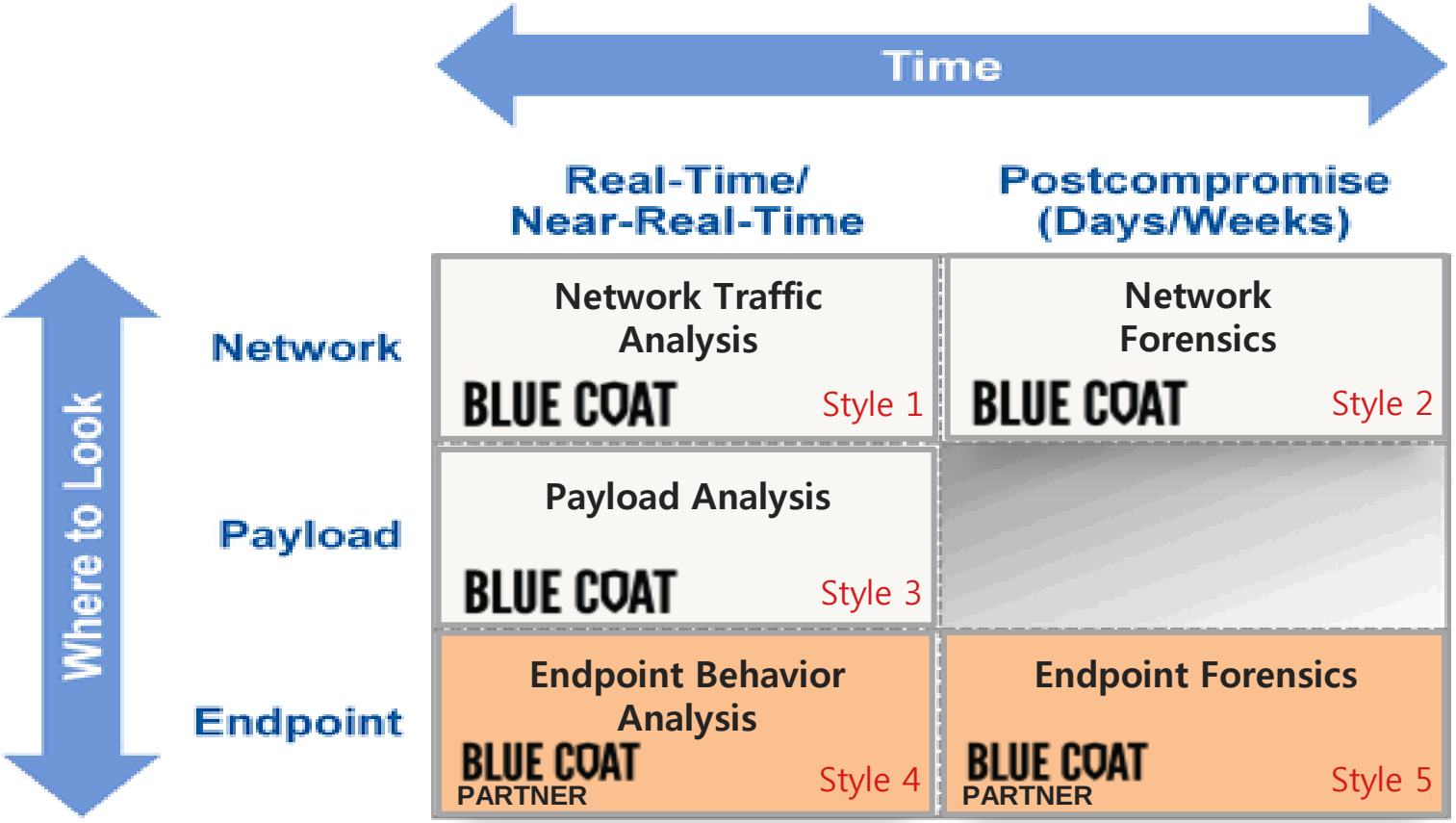
수많은 상황을 모두 통제할 수는 없음

지능화 공격 대응을 위한 필요 사항

- 새로운 위협에 대응할 수 있는 방법 필요
- 암호화 트래픽에 대한 가시성 제공 필요
- 모든 지점, 사용자들의 보안을 위한 유연한 구현 제공
- 기존 보안 시스템 연계를 통한 효과적인 공격 대응 고민 필요
- 확장성 및 성능 향상을 위한 구현 방법 필요

지능화 공격 대응을 위한 5가지 필요 유형

Gartner Five Styles of Advanced Threat Defense

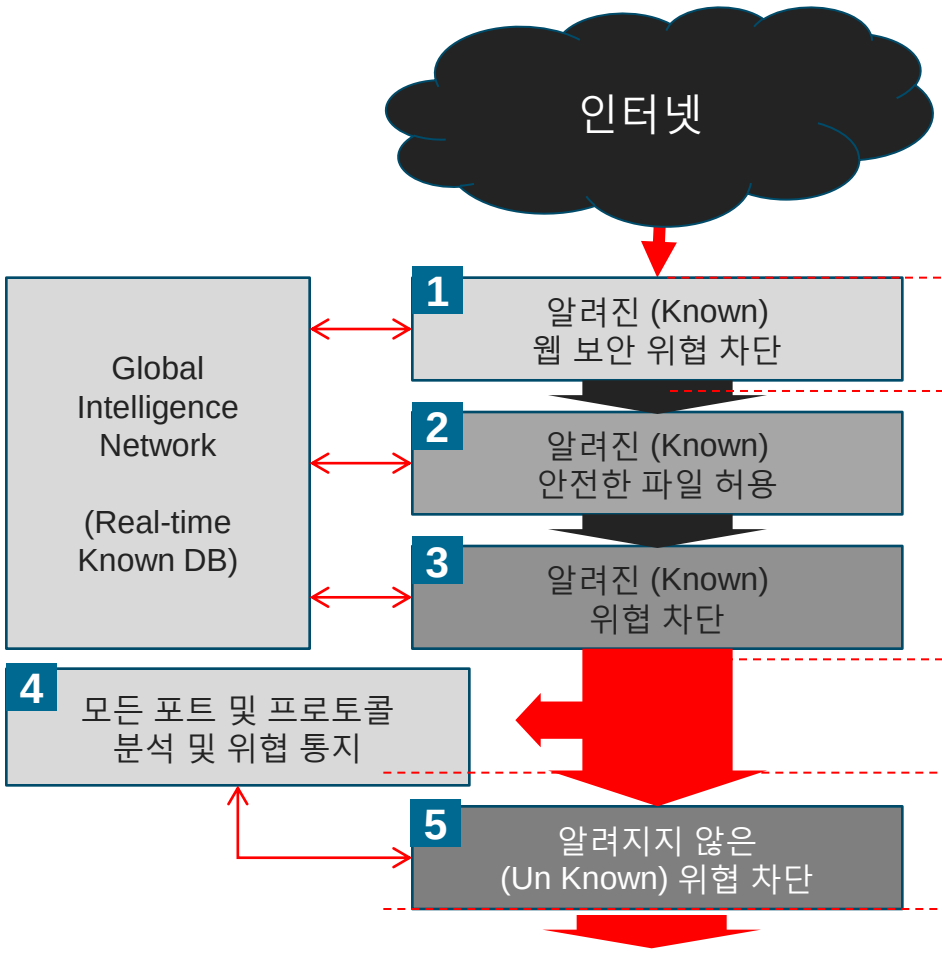


Source: Gartner (August 2013)

블루코트 라이프사이클 방어 모델

- 알려진 모든 위협에 대한 탐지 및 차단
- 알려지지 않은 공격에 대해서는 분석을 위한 에스컬레이션
- 검증을 통해 언제 발생이 되었고, 어떤 경로를 통해서 이루어 졌는지 상관관계 분석을 통해 근원 분석
  (어떤 경로를 통하여 악성코드 다운로드 되었는지 분석)
- 분석되고 검증되어진 정보는 다시 차단정책으로 업데이트

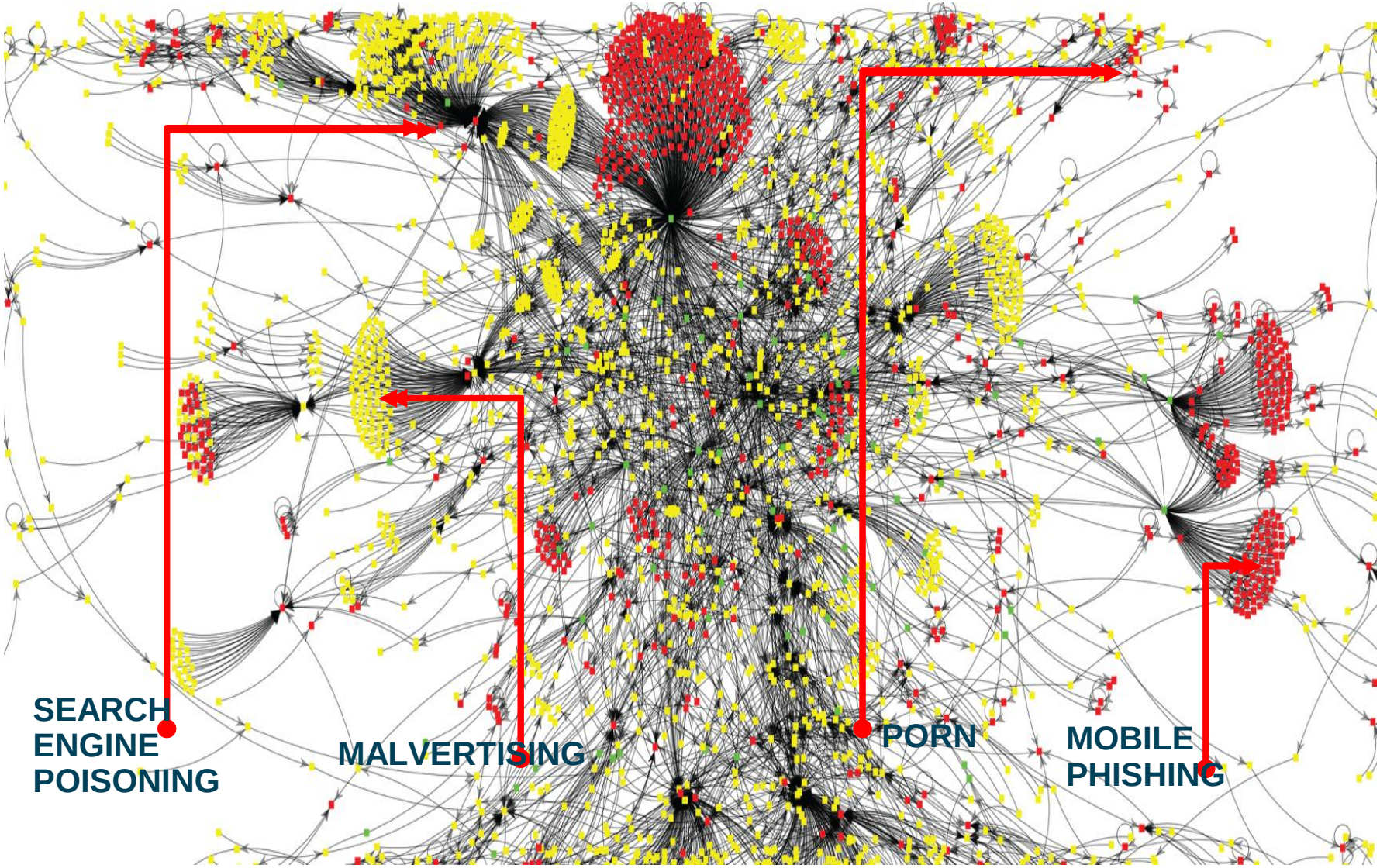
다 계층 구조의 보안 라이프 사이클 방어 체계



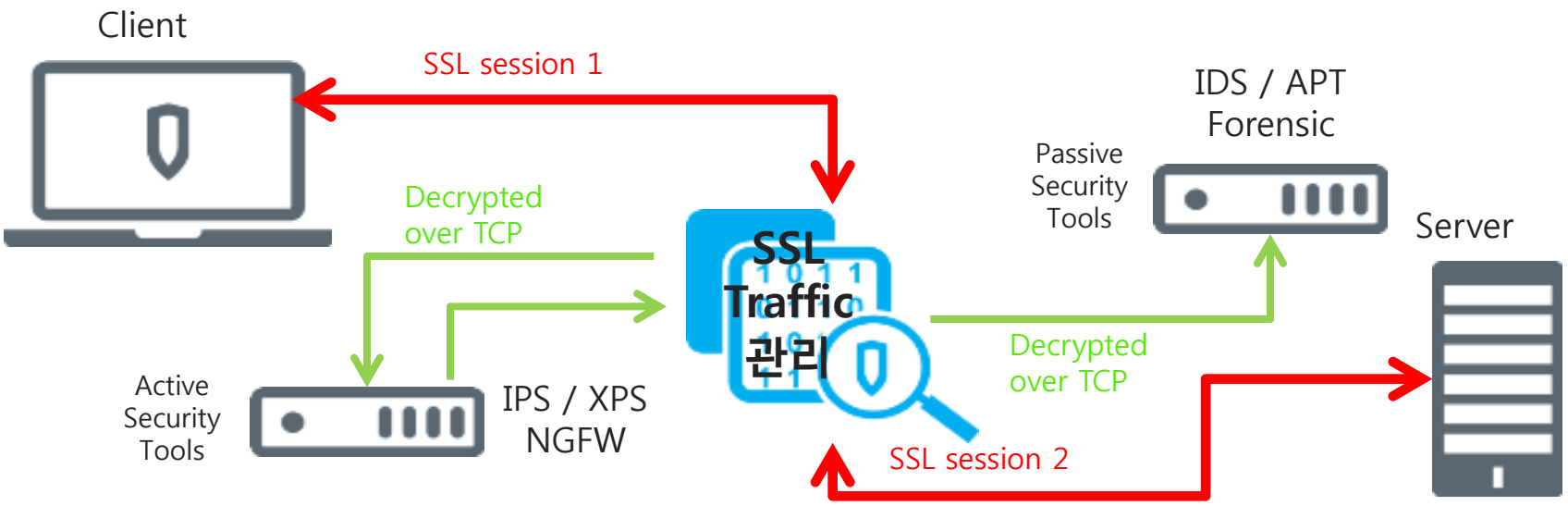
- 실시간 정보가 반영되는 DB를 통한 웹 접근 차단
- 사전 분류된 정보를 통한 안전한 파일만 허용
- 실시간 정보가 반영되는 악성 코드 정보를 통한 위협 차단
- 네트워크 빅데이터 보안 분석을 통한 모든 트래픽의 수집 및 분석
- 다중화 시뮬레이션을 통한 알려지지 않은 악성 코드 분석

보안 라이프사이클 방어 체계 구축

MALNET MANAGEMENT

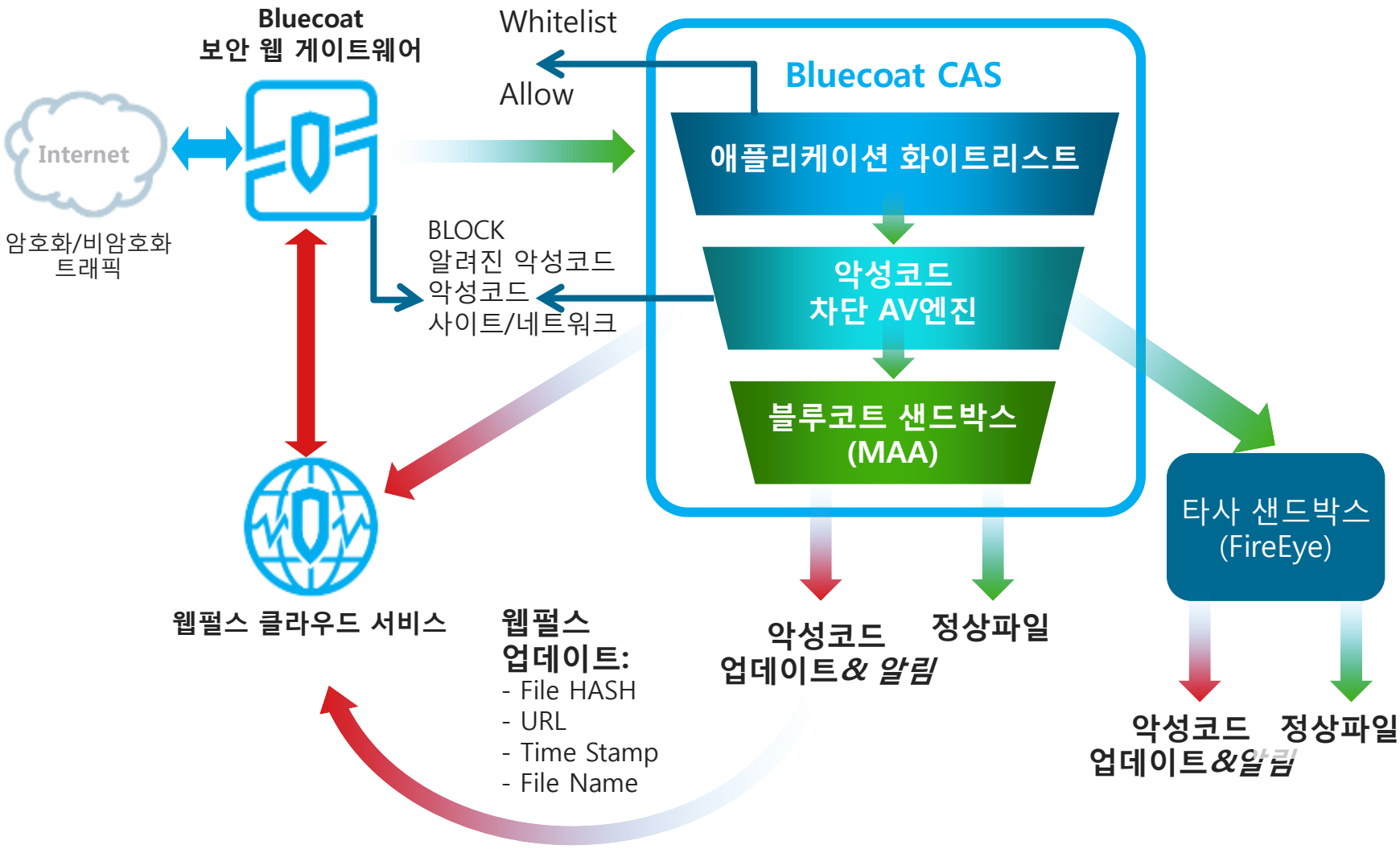


SSL 트래픽을 통한 위협의 관리



- 모든 포트에 대한 SSL 확인 수행
- Inline or passive 구성 지원
- 한번 복호화 된 트래픽에 대하여 다양한 보안 장비에서 분석하도록 연동 지원
- Inbound 또는 outbound SSL 트래픽에 대한 검사

알려진 공격에 대한 사전 차단



알려지지 않은 악성 URL, 파일 등에 대한 심층 분석

다양한 환경을 통한
악성행위 분석

SAMPLE FILES AND URLS

Customized 어플리케이션 설치를 통한 기업별 주요 사용 환경 구성

INTELLIVM PROFILE

Windows 7 | Microsoft Windows xp | Windows 8

PLUGIN

Java | | | | | |

Task Resources Include
Files Generated or Used by The Sample,
Plus Files Created by the Plugin Itself

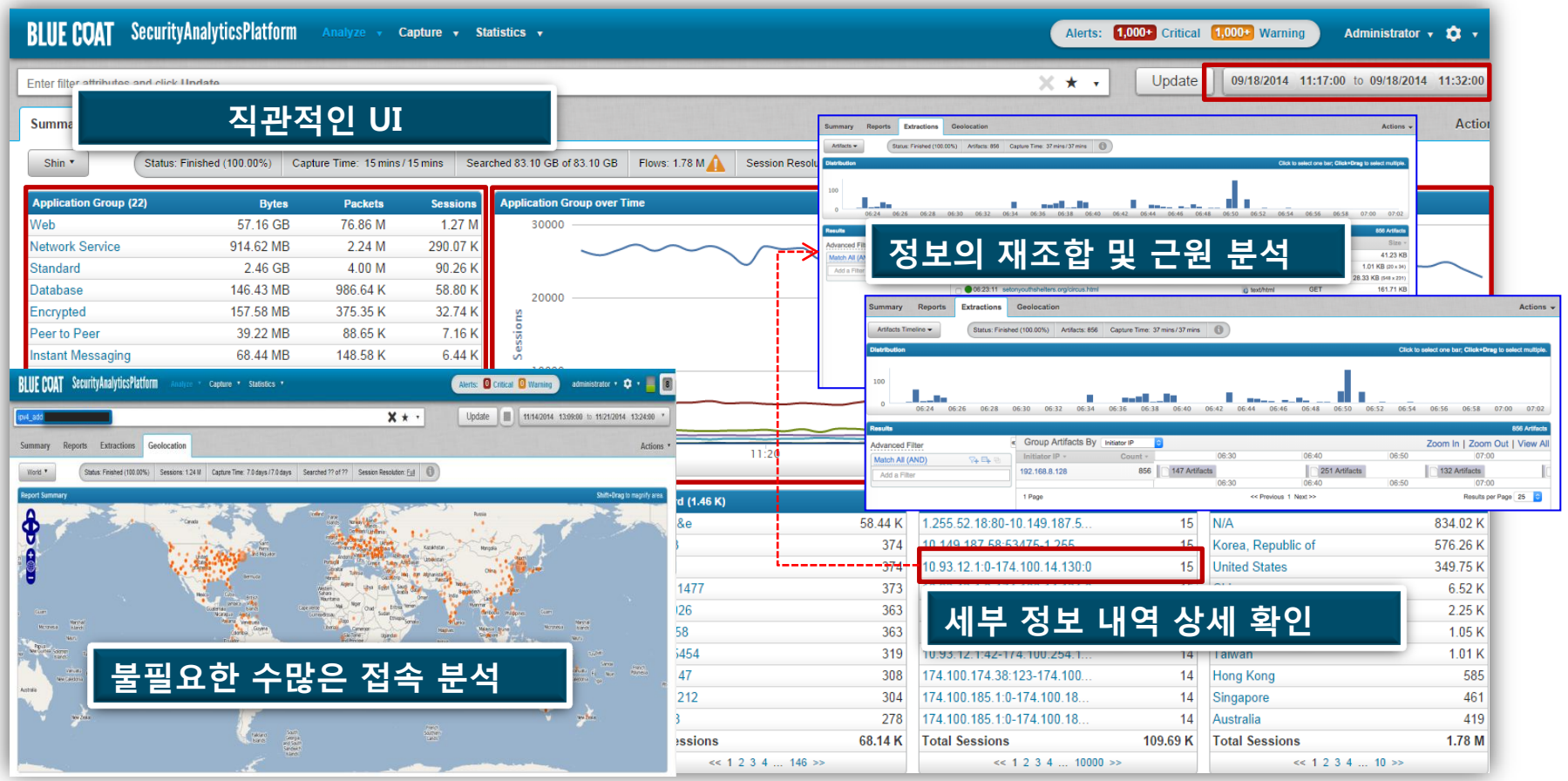
TASK RESOURCES

PCAPs	Dropped Files	Screen Shots	HTTP Archives
Memory Dumps	Pattern Hits	Event Lists	Risk Scores

Risk Score 10

심층 분석을 통한 신속한 위협 확인

- 직관적인 통합 UI를 통한 신속하고 편리한 분석
- Root Cause 분석, 상관 관계 분석, 다양한 위협 요소의 분석



지능화된 공격 대응 방안

PCAP/패킷 (Layer 2 ~ 7 분석)	다양한 분석 Tool 제공 - 세션재조합, IP추적, 타임라인분석,데이터뷰 등
Real Time Intelligence (실시간 모니터링)	실시간 모니터링 - 네트워크 위협, 정책기반, 인스턴스 복구, 파일 분석
Context-aware security (상관 관계 분석)	최상의 보안기술 통합 - full-payload event, 위험 전후의 모든 알람 등
Application Classification (어플리케이션 분류)	Application 분류 - 1,200개 이상의 Application, 컨텐츠 타입(속성 포함)등
Root Cause Explorer (근원 분석)	근원 분석 - 네트워크,객체, 웹, 세션 등 - 특정 의심 시점 재연(타임라인)

블루코트의 통합 지능형 위협 대응 솔루션

지능형 보안위협 대응을 위한 블루코트 ATP 솔루션

SSL 가시성 보장

SSL VA

보안 웹 게이트웨이 & Content 게이트웨이

ProxySG

CAS

샌드박스

MAA

빅데이터 보안 분석

Solera Appliances

Solera Storage Appliances

Solera Central Manager

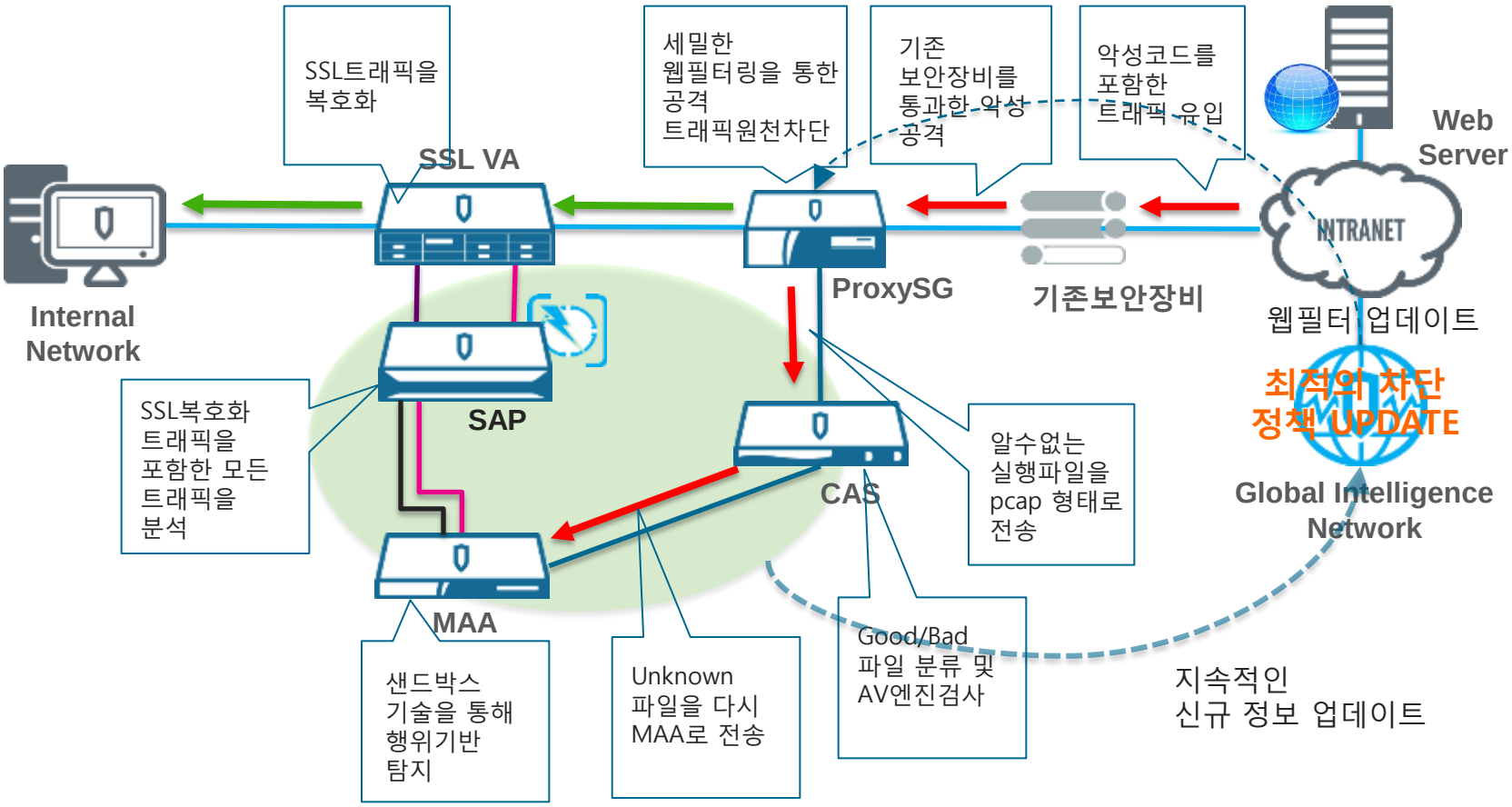
ThreatBLADES

WebThreat BLADE

MailThreat BLADE

FileThreat BLADE

지능화된 공격 대응 방안 – BLUECOAT SOLUTION



THREAT INTELLIGENCE 'NETWORK EFFECT

NEW THREAT INTELLIGENCE SHARED LOCALLY AND GLOBALLY

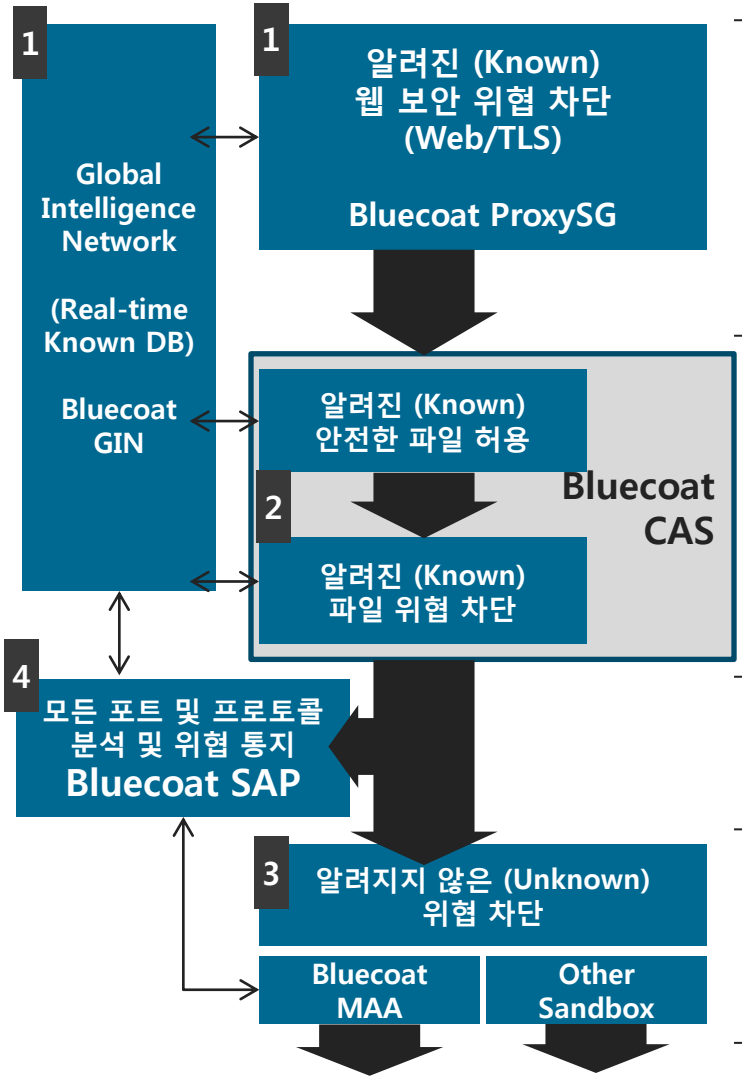
비용 효율적인 위협 분석

알려진 위협에 대하여
게이트웨이 단에서 차단

악성코드 스캔을 최소화하여
시스템 성능 향상

오탐지를 최소화한
강력한 위협 분석

고객 사례



구성 방안	기대 효과
▪ IP, Port, URL/URI, 컨텐츠, 파일 확장자/타입, 파일사이즈 조건에 따른 차단 ▪ 비 준프로토콜/애플리케이션에 대한 분석 및 차단	▪ 악성코드 네트워크 유입 단계에서 실시간 차단을 통한 유입 방지 ▪ Event 기록 관리 ▪ 사용자에게 차단 정보 통지
▪ 사전 분류된 정보를 통한 안전한 파일 허용	▪ Good/Bad 파일 사전 분류를 통한 내부 보안 시스템 리소스 가용성 극대화
▪ 실시간 정보가 반영되는 악성 코드 정보를 통한 위협 차단	▪ 파일에 포함된 악성코드 차단을 통한 보안위협 감소
▪ 모든 트래픽의 수집 및 실시간 위협 요소 분석	▪ 모든 Traffic을 수집/분석을 통한 실시간 보안 위협 대응
▪ 다중화 시뮬레이션을 통한 알려지지 않은 악성 코드 분석	▪ Dual Sandbox를 통하여 오탐의 최소화 ▪ 장비 증설의 요구의 최소화

BLUE COAT

Security Empowers Business

감사합니다

Blue Coat Korea
John.seo@bluecoat.com