Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT APT 통합 대응 플렛폼

SandBlast FAMILY

WELCOME TO THE FUTURE OF
CYBER SECURITY

CHECK POINT
INFINITY

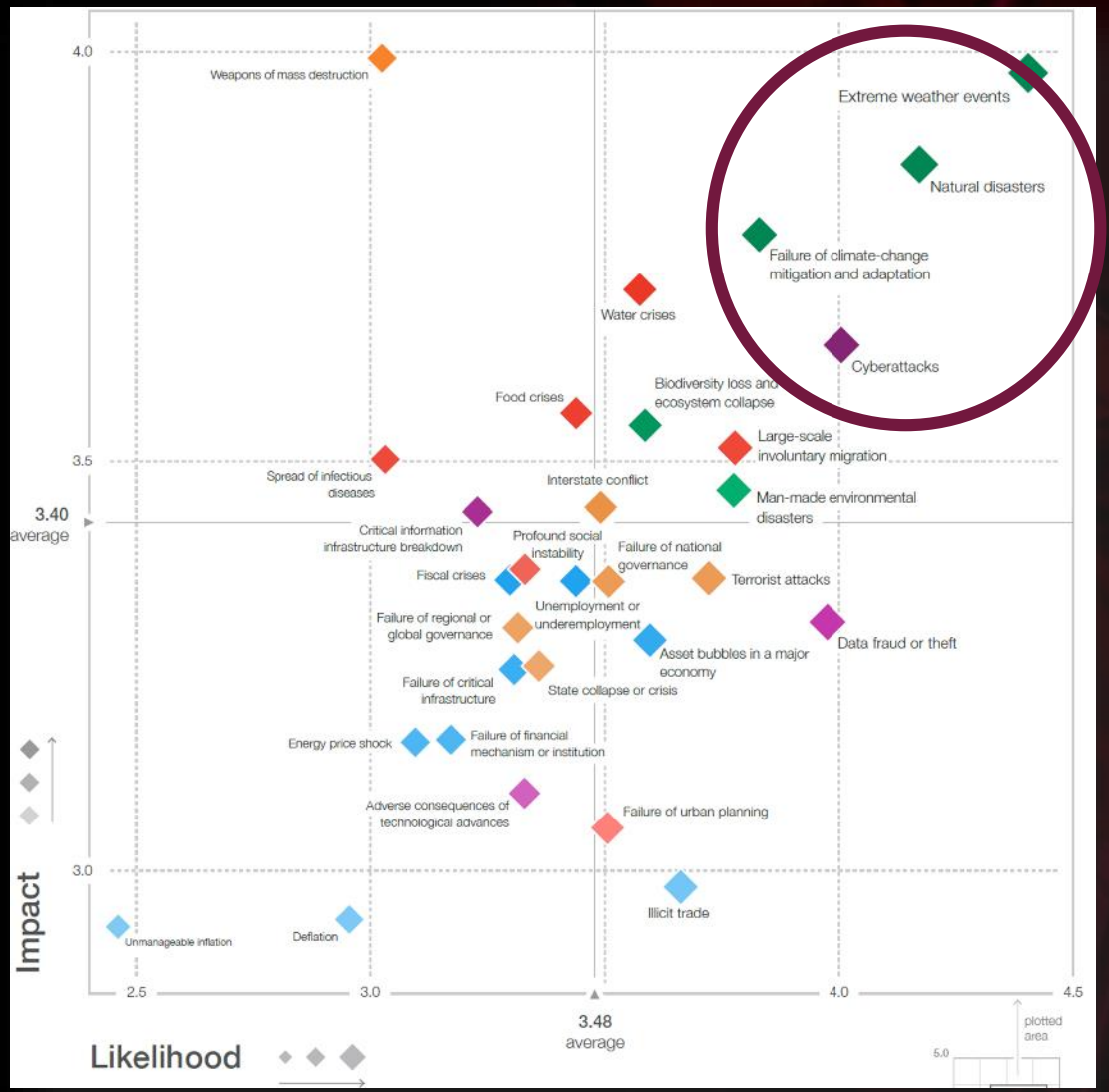
CLOUD • MOBILE • THREAT PREVENTION

CHECK POINT APT 통합 대응 플렛폼

SandBlast FAMILY

THE GLOBAL RISKS REPORT 2018

WORLD ECONOMIC FORUM



- CIA, NSA 툴 유출
  3월 7일, 4월 14일
- Uber 데이터 유출 11월 21일, 16 일
- WannaCry 5월 12일, 17일
- Equifax hack 5월 13일, 7월 17일 30일
- NotPetya attack 6월 17일, 28일

WE ARE AT AN INFLECTION POINT !

THREATS

Gen I

Virus

Gen II

Networks

Gen III

Applications

Gen IV

Payload

Gen V

Mega

1990

2000

2010

2017

2018 – GEN V OF ATTACKS

1 국가 및 사업전반의 대규모 공격

2 주정부 후원

3 막대한 금전적 손실

4 다중 공격

ADVANCED THREAT PREVENTION
5th GENERATION OF CYBER SECURITY

GEN V

NETWORK

- Known/Unknown 공격
- 악성 URL
- 차세대 센드박스
- 익스트렉션

AGENT

- 포렌식
- 안티렌섬웨어
- 차세대 센드박스
- 안티피싱
- 익스트렌션

CLOUD

- Known/Unknown 공격
- 악성 URL
- 차세대 센드박스
- 익스트렉션

MOBILE

- 블루투스 공격
- App 취약점
- OS 취약점
- 차세대 센드박스
- SMS 스미싱
- 중간자 공격

<API>

- 이기종 호환성 제공
  Known/Unknown 공격 방어

Check Point SandBlast APT 대응 관점
Zero-day, Unknown, APT 공격 파일 실시간 차단

탐지

네트워크, 이메일, 엔드포인트 로
유입되는 Zero-day, Unknown 파일 대한
실시간 탐지와 가시성 확보

분석

CPU 레벨 분석, OS레벨 동적분석,
다운로드 링크 분석 엔진 등 다계층
보안 엔진을 통해 악의적인 행위를 하는
파일 식별

실시간 차단

Zero-day, Unknown 악성코드 1차
유입되는 시점부터 실시간 차단 제공.

전통적인 APT 솔루션은 1차 분석이 끝난 후 2차 유입시 차단.

Check Point SandBlast 다계층 엔진
Zero-day, Unknown, APT 모든 유입경로 대응

에뮬레이션

- 이메일, 네트워크, 엔드포인트로 유입되는 요소들의 OS레벨 동적 분석, CPU레벨 분석을 통해 Zero-day, Unknown 악성 파일 탐지 제공

익스트렉션

- 이메일,네트워크로 유입되는 문서, 이미지 동적요소를 제거하는 PDF 변환 기술 을 통해 100% 멀웨어 제거
- 이메일, 네트워크 가용성 영향 없는 빠른 PDF 변환 제공

제로피싱

- URL, IP, Domain 등 평판 정보 이용 악의적인 피싱사이트의 접근, 사용자 ID, Password 유출 탐지 차단 제공

포렌식

- 엔드포인트에 유입된 악성파일의 네트워크 행위, 레지스트리, 파일 조작 등의 모든 악성 행위 정보를 제공

안티렌섬웨어

- 사용자 단말의 암호화 행위를 모니터링 하여, 이상행위 탐지시 암호화 대상 파일을 즉각 백업, 복원 기술을 통해 렌섬웨어 원천 봉쇄 제공

ThreatCloud

- 클라우드 기반의 보안 지식 데이터베이스
- Cyber Threat Alliance 회원으로써 가장 빠르게 확장되는 세계 최대의 보안 인텔리전스

SandBlast 에뮬레이션
Zero-day, Unknown, APT 공격 탐지

CPU레벨 탐지 기술을 적용한 차세대 센드박싱 기술을 이용 높은 탐지율, 센드박스 우회기술 원천 차단 제공

높은 탐지율

이메일 유입
Unknown 악성코드
100% 탐지

센드박스 우회기술 차단

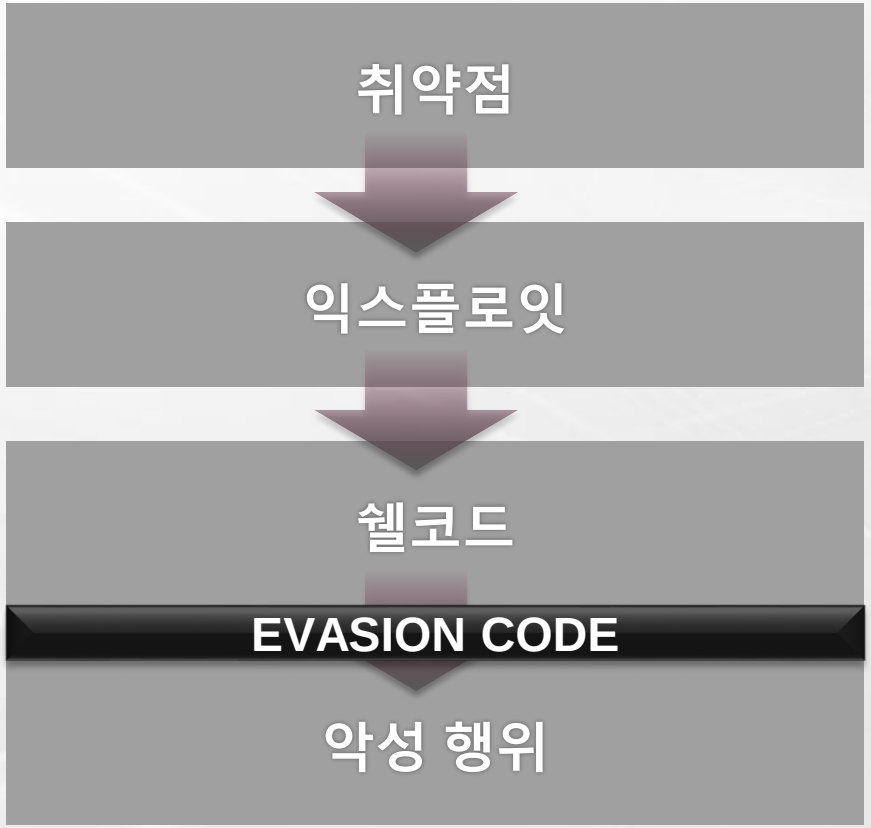
센드박스 인지
우회기술 100%
차단

빠른탐지 높은효율성

평균 3분이내
악성행위 탐지

*source: 2016 NSS Labs Breach Detection Systems Test Report

SandBlast 에뮬레이션
Zero-day, Unknown, APT 공격 탐지



CHECK POINT
SandBlast™
ZERO-DAY PROTECTION

CPU 탐지 엔진

악성 파일 다운로드전 사전 탐지

센드박스 우회 전 탐지

전통적인 센드박스 탐지 단계

SandBlast 에뮬레이션
다양한 구성 옵션 제공

미러링 + SandBlast TE Appliance

SandBlast TE Appliance

Switch

SandBlast TE Appliance 인라인

SandBlast TE Appliance

NGTX + SandBlast TE Appliance

SandBlast TE Appliance

Check Point NGTX

NGTX + 클라우드 센드박스

클라우드 센드박스

Check Point NGTX

SandBlast 익스트렉션
100% 악성파일 대응

PDF 변환 기술이용 이메일, 네트워크 지연없는 100% 안전한 파일 전달

선제대응

선제대응 기술을 통해 파일 안전성 제공

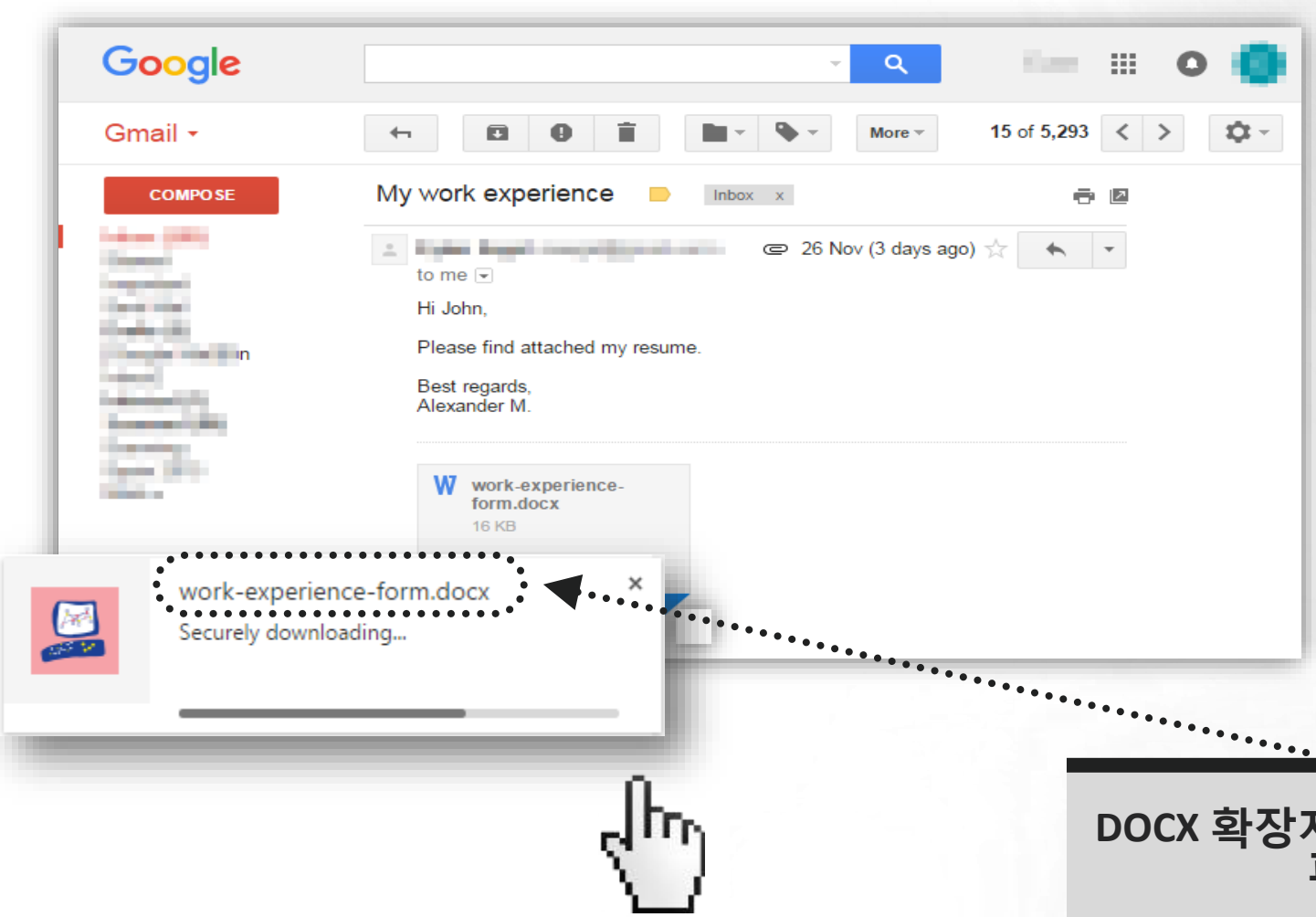
동적요소제거

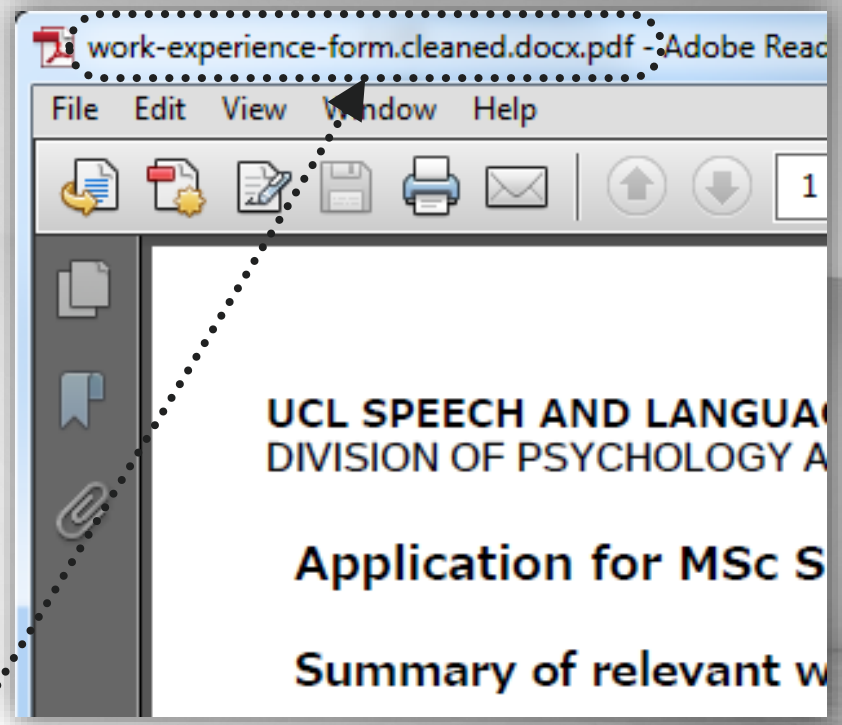
URL, IP, 메크로 등 동적 요소 제거 제공

인프라 가용성 확보

높은 보안성, 높은 인프라 가용성 동시 제공

SandBlast 익스트렉션
웹 브라우저로 유입되는 악성코드 대응





DOCX 확장자를 동적 요소를 제거한 PDF 파일로 즉시 변환

SandBlast 익스트렉션
이메일로 유입되는 악성코드 대응

Reply Reply All Forward

Tue 5/4/16 6:03 PM

Yonni Shelmerdine

SECURITY ALERT! Skipped Invoice

To Yonni Shelmerdine

Message invoice.cleaned.pdf

*Check Point SandBlast Threat Extraction has **cleaned** an attachment named **Invoice.doc** as it was determined to contain potentially malicious elements.*

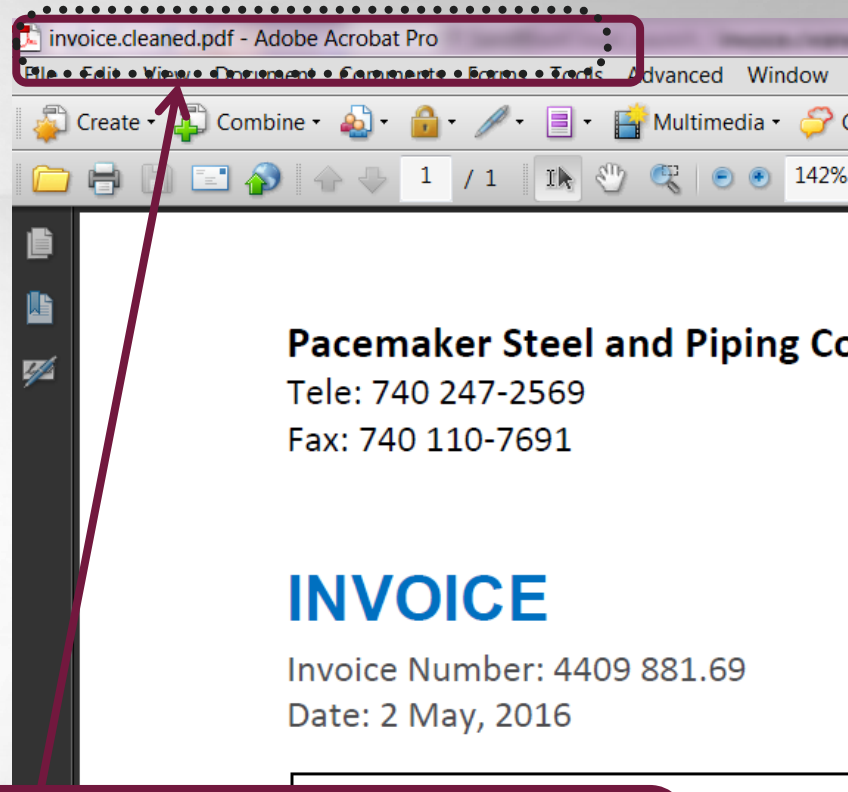
To access the original file, please click here

Hi Yonni,
Attached is invoice #4409 881.69 from May which was missing from the original summary.

I am out of the office tomorrow and Monday, so I'm emailing you now to request that you go over the invoice, submit the detail [Blocked Malicious URL] and complete they payment as soon as possible.

Julia Reyes / Credit Manager
Pacemaker Steel and Piping Co. Inc.
Tele: 740 247-2569
Fax: 740 110-7691

This Email was secured by Check Point SandBlast Connector for Office 365



동적 요소를 제거한 PDF 변환을 통해 안전성, 가용성 동시 제공

SandBlast 익스트렉션
이메일로 유입되는 악성코드 대응

Reply Reply All Forward

Tue 5/4/16 6:03 PM

Yonni Shelmerdine

SECURITY ALERT! Skipped Invoice

To Yonni Shelmerdine

Message invoice.cleaned.pdf

*Check Point SandBlast Threat Extraction has **cleaned** an attachment named **Invoice.doc** as it was determined to contain potentially malicious elements.*

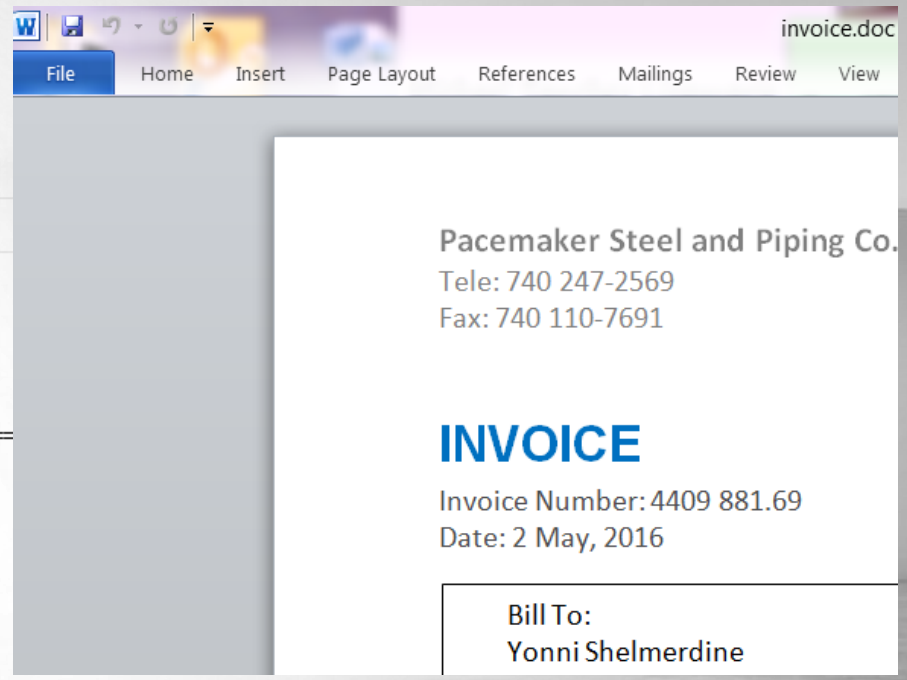
To access the original file, please click here

Hi Yonni,
Attached is invoice #4409 881.69 from May which was missing from the original summary.

I am out of the office tomorrow and Monday, so I'm emailing you now to request that you go over the invoice, submit the details here [Blocked Malicious URL] and complete they payment as soon as possible.

Julia Reyes / Credit Manager
Pacemaker Steel and Piping Co. Inc.
Tele: 740 247-2569
Fax: 740 110-7691

This Email was secured by Check Point SandBlast Connector for Office 365



악성요소 미 탐지시
원본파일 다운로드 링크를 통해 원본 다운

SandBlast 제로피싱
Unknown, Zero-day 피싱 웹사이트 접속 차단

피싱웹사이트 접속 차단

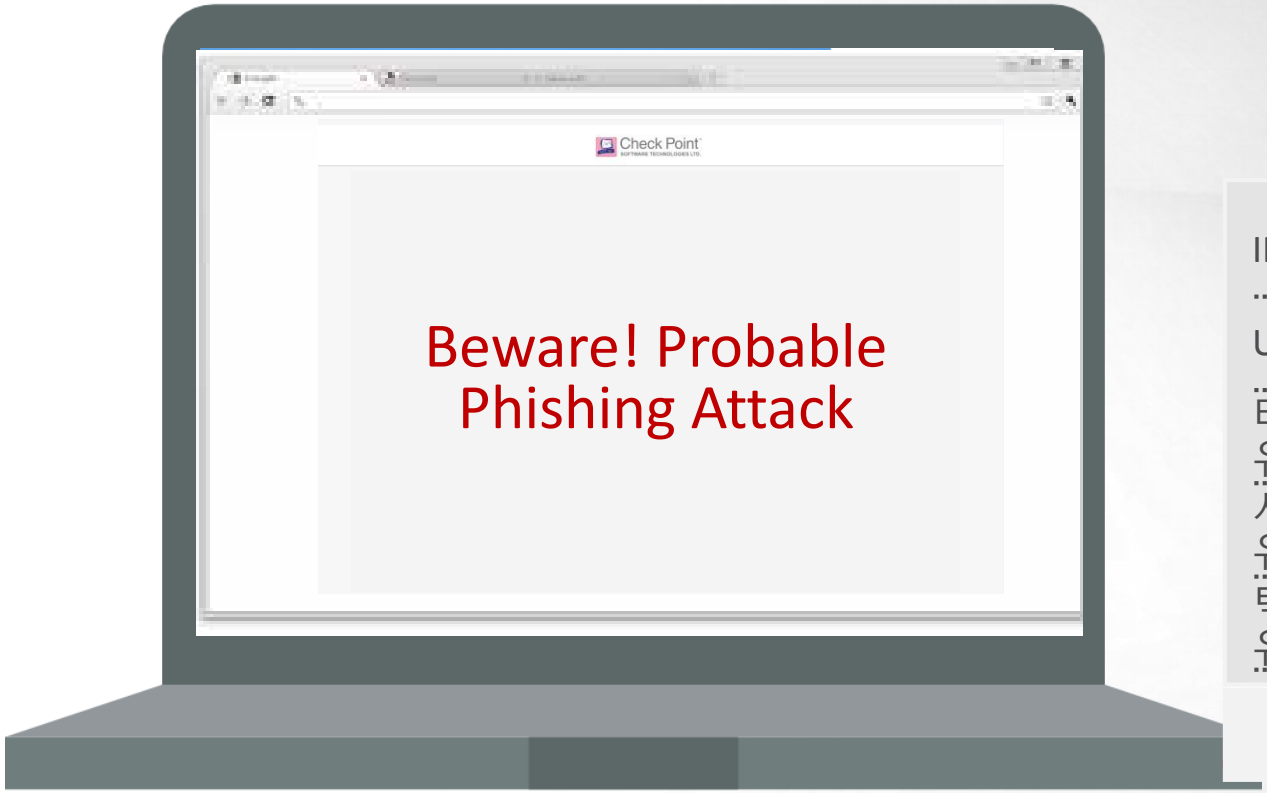
평판 정보를 바탕으로 Unknown 피싱 웹사이트 접속 탐지 차단 제공

계정정보 재 사용 차단

사내 계정 정보를 업무상 관계 없는 웹사이트 사용 탐지 차단 제공

소셜 엔지니어링 공격 효율적인 차단 제공

SandBlast 제로피싱
Unknown, Zero-day 피싱 웹사이트 접속 차단



THREATCLOUD™

IP 평판	✗	Domain 평판	✗
URL 유사성	✓	페이지 유사성	✗
타이틀 유사성	✗	이미지 전용 페이지	✓
시각정보 유사성	✗	멀티 도메인	✓
텍스트 유사성	✗	파비콘 유사성	✗

피싱 사이트 확률 : 95%

1 신규 웹사이트 접속 시도 탐지

2 휴리스틱, 평판기반 피싱 사이트 여부 분석

3 피싱 웹사이트 시 수 초내 차단

SandBlast 포렌식
효율적인 보안 인시던트 대응

모든 위협 가시성 확보

보안사고 발생시
효율적인 분석
정보제공

자동화된 대응

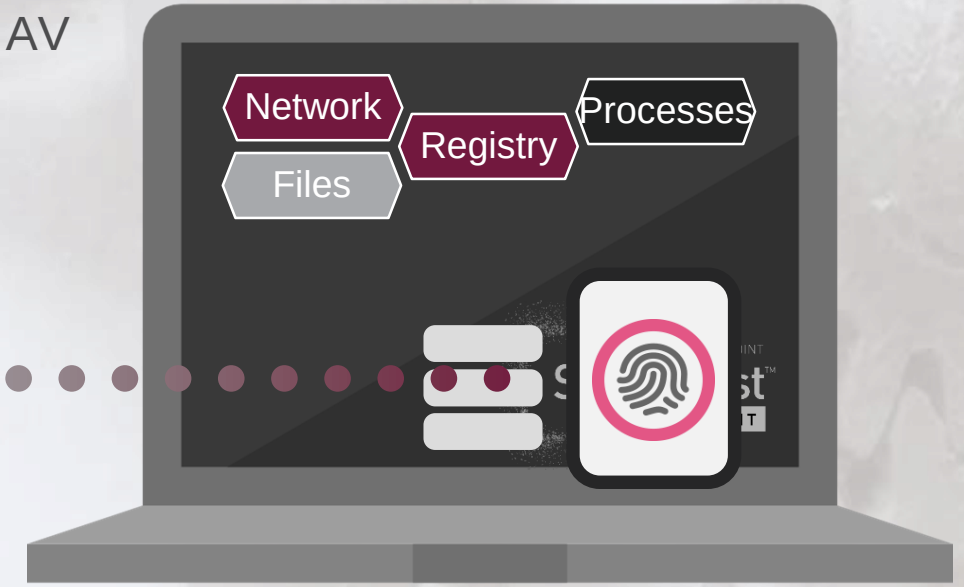
Known, Unknown
위협 제거

FORENSICS

SandBlast 포렌식
보안 인시던트 발생 시 대응 방안

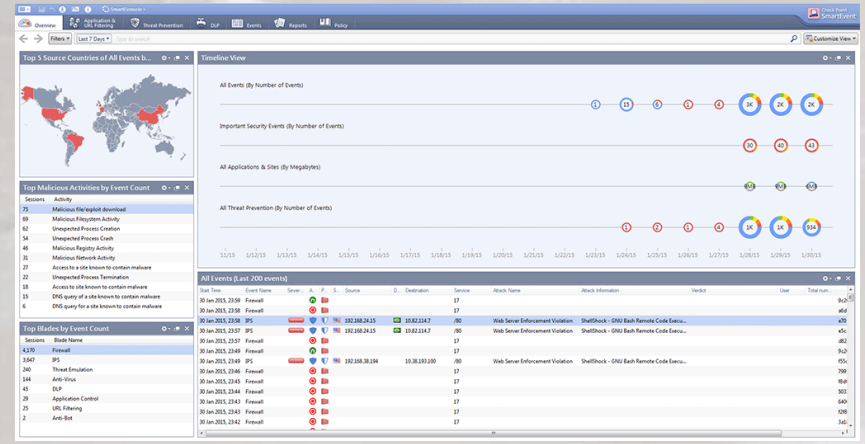
1 파일, 네트워크, 레지스트리, 시스템 정보 등 수집

2 네트워크 또는 3rd Party AV 이벤트 탐지시 자동화된 보고서 생성

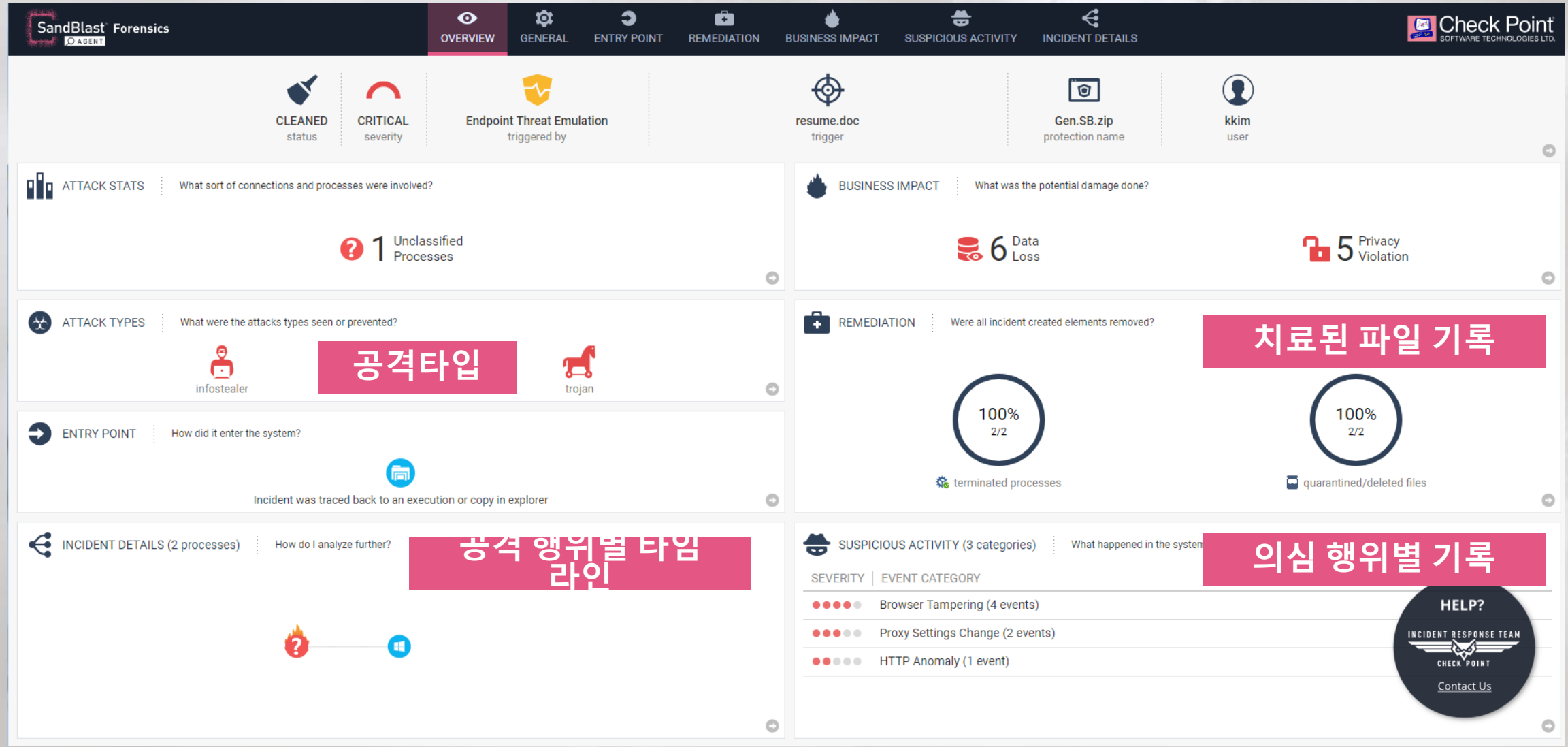


3 포렌식 알고리즘 이용 분석

4 통합 이벤트 관리 서버에 전달



SandBlast 포렌식
포렌식 리포트 이용 상세 분석 제공



SandBlast 안티렌섬웨어

사용자 단말에서 발생하는 랜섬웨어 원천 차단

렌섬웨어 전용 엔진

사용자 단말의 렌섬웨어 원천 차단

변종 렌섬웨어 대응

Zero-day, 변종 렌섬웨어 원천 차단

복원

암호화 행위 탐지시 즉시 대상 백업 → 복원

SandBlast 안티랜섬웨어

안티랜섬웨어 동작 순서

데이터 암호화 탐지

- 행위 분석
- 암호화 행위 분석
- 데이터 스냅샷

대응

- 랜섬웨어 탐지/차단
- 데이터 복원

CHECK POINT SandBlast™ AGENT with *Anti-Ransomware*

파일 백업 생성 → 행위전 랜섬웨어 차단 → 랜섬웨어 식별 및 차단 → 원본 파일 복원

THREATCLOUD
세계최대 규모의 보안 지식 베이스

CYBER THREAT ALLIANCE

ThreatCloud

- 클라우드 기반의 보안 지식 데이터 베이스
- 가장 빠르게 확장되는 세계 최대의 보안 인텔리전스
- Cyber Threat Alliance 회원으로, 보안 업계 리더인 회원 업체와의 인텔리전스 협업
- 전 세계 Check Point GW, TE 와 실시간 연동
- 50만 업데이트 / Day

+ 5.5M

악성 사이트

+ 11M

말웨어 시그니처

+ 250M

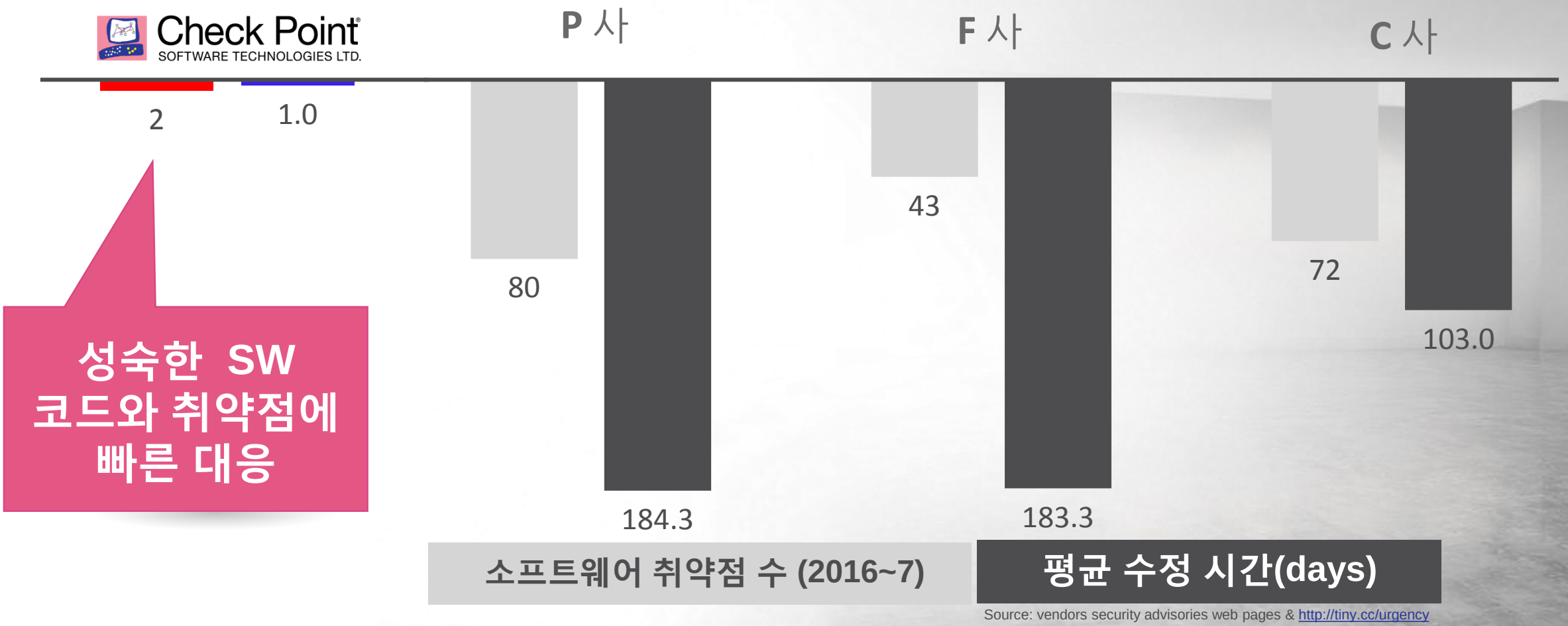
봇 어드레스

CHECK POINT APT 통합 대응 플렛폼

특장점

안전한 소프트웨어
취약점이 가장 적은 안전한 소프트웨어를 제공

Check Point는 가장 보안적으로 안전하고 성숙한 소프트웨어를 제공 하여 높은 수준의 보안성을 제공 하여, 외부 공격시 안전한 운영환경을 제공 합니다.



Source: vendors security advisories web pages & http://tiny.cc/urgency

하이브리드 APT 플렛폼
단일 플렛폼 이용 모든 APT 유입 경로 대응

Check Point SandBlast TE는 단일 플렛폼으로 Zero-day, Unknown, APT 공격 유입처인 네트워크, 이메일, 엔드포인트 모두 대응

이메일 APT

SSL 복호화

네트워크 APT

500 Users

1000 Users

2000 Users

가장빠른 동적 분석
경쟁사 대비 빠른 Zero-day, Unknown 악성코드 대응

- 악성 첨부파일 이메일 유입

Check Point SOFTWARE TECHNOLOGIES LTD.

- 악성여부 판단 4분
- 악성코드 차단 0분

F사

- 악성여부 판단 8분
- 악성코드 차단 0분

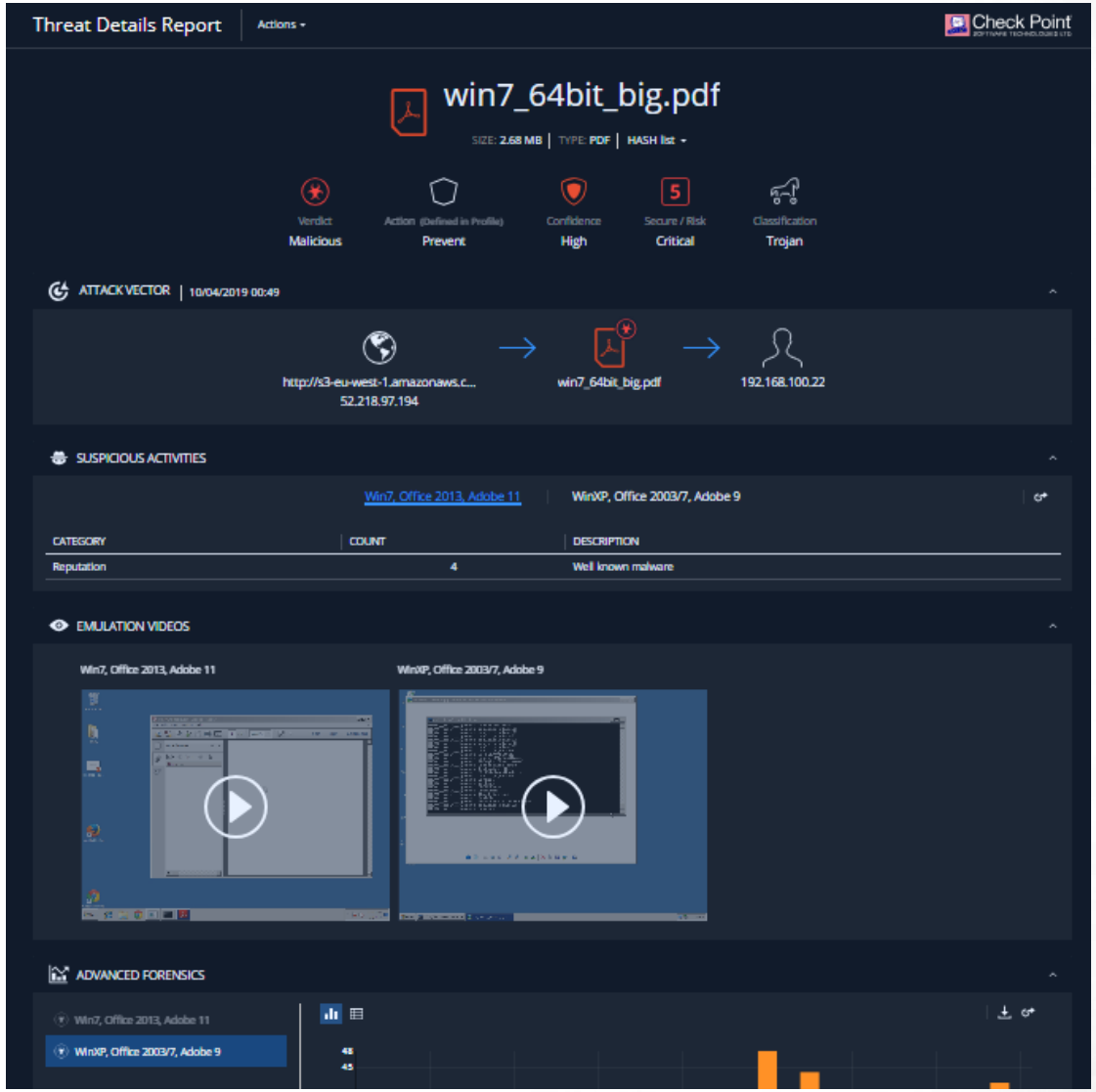
P사

- 악성여부 판단 8분
- 악성코드 차단 68분

F사

- 악성여부 판단 19분
- 악성코드 차단 79분

리포트
직관적이고 효율적인 TE 리포트



TE 리포트

- 위험도, 민감도, 악성 여부
- 레지스트리, 파일, 네트워크 행위 등 행위 정보
- OS별 행위 상세 정보, PCAP 정보
- **악성파일 실행 이후 현황 동영상 재생**
- ROOT, Embedded, Dropper 파일 정보
- 이메일 플로우 정보

통합 콘솔
네트워크, 이메일, 엔드포인트 콘솔 통합 운영

통합 모니터링

정책 통합

커스텀 데쉬보드

Check Point SandBlast™ ZERO-DAY PROTECTION

INCIDENT RESPONSE TEAM
보안 사고 발생시 신속한 분석, 해결책 제공

INCIDENT RESPONSE TEAM

CHECK POINT

7x24 Incident Response

- 멀웨어 침입
- 디도스 공격
- 무차별 공격
- 데이터 유출
- 포렌식

Incident Response Hours

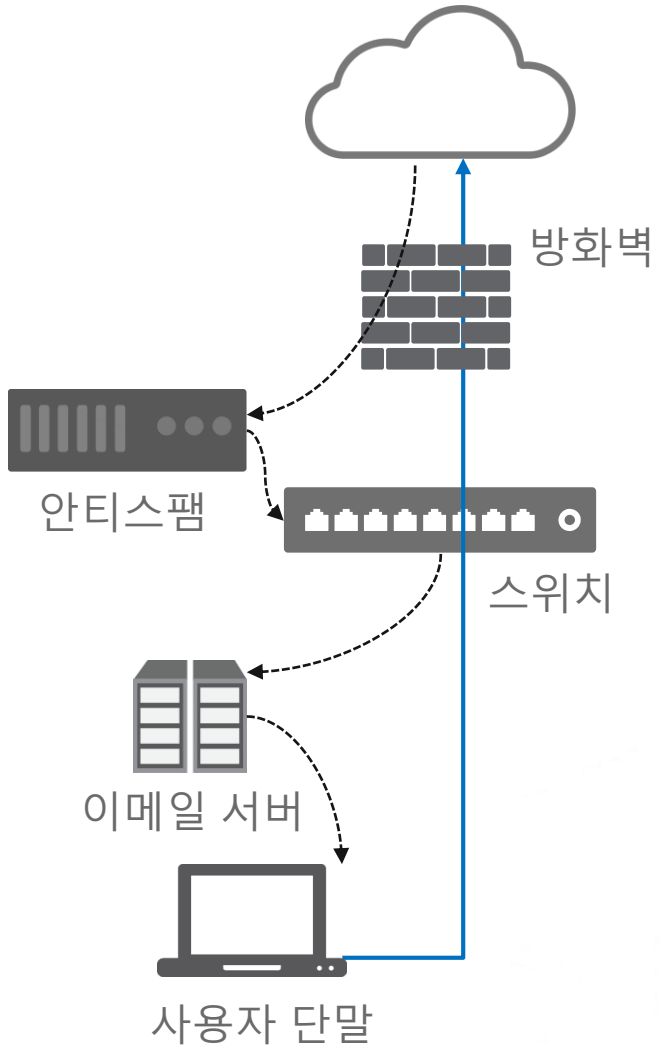
Check Point TE 구매시 무상 서비스

TE250X: 10 시간 | TE1000X: 20 시간 | TE2000X: 30 시간

CHECK POINT APT 통합 대응 플렛폼

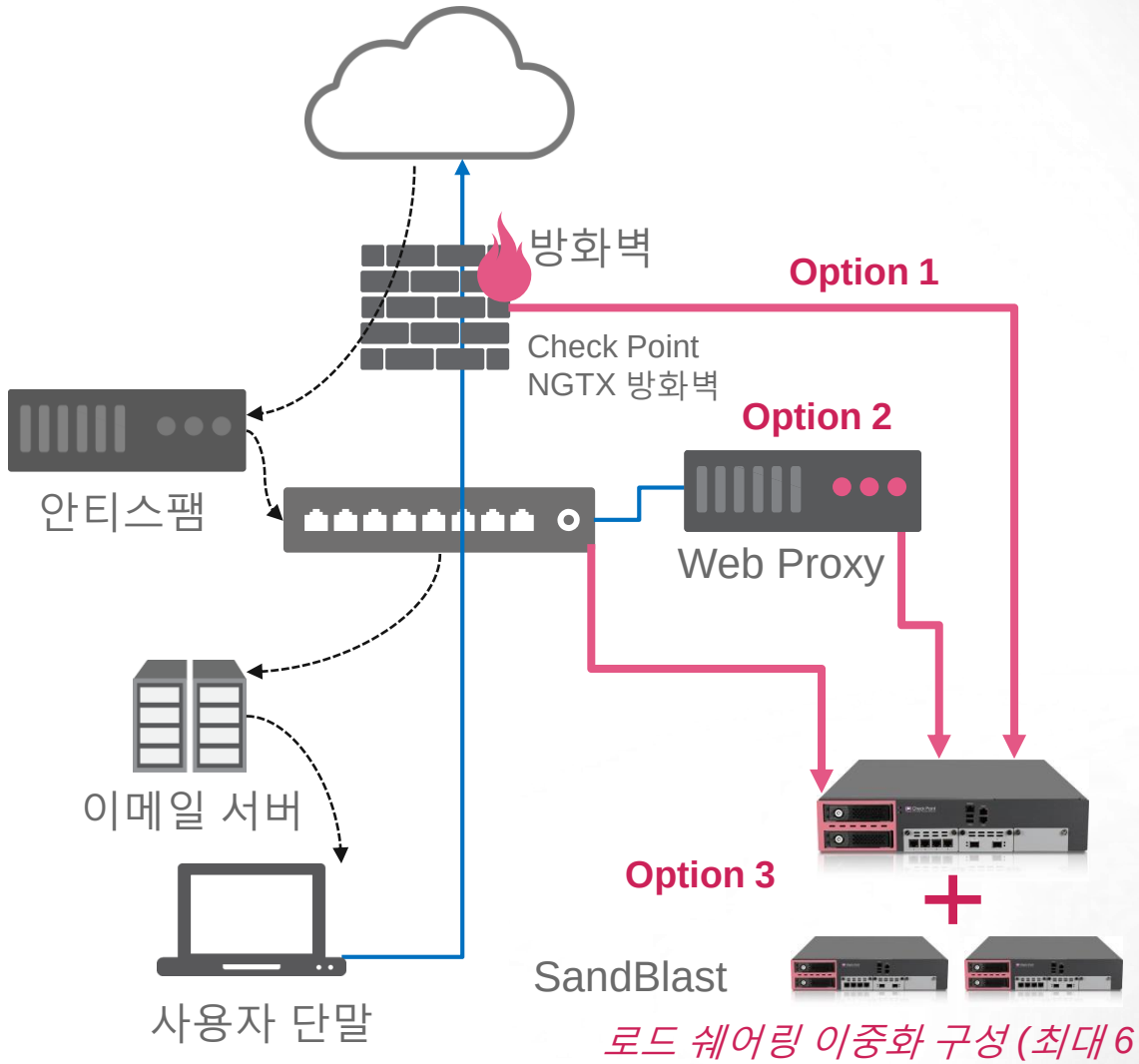
구성방안

SandBlast 구성 전
일반적인 Known 공격 대응



Zero-day, Unknown, APT 공격에
노출되어 대응방안 필요

SandBlast 네트워크
네트워크를 통한 APT 유입 대응



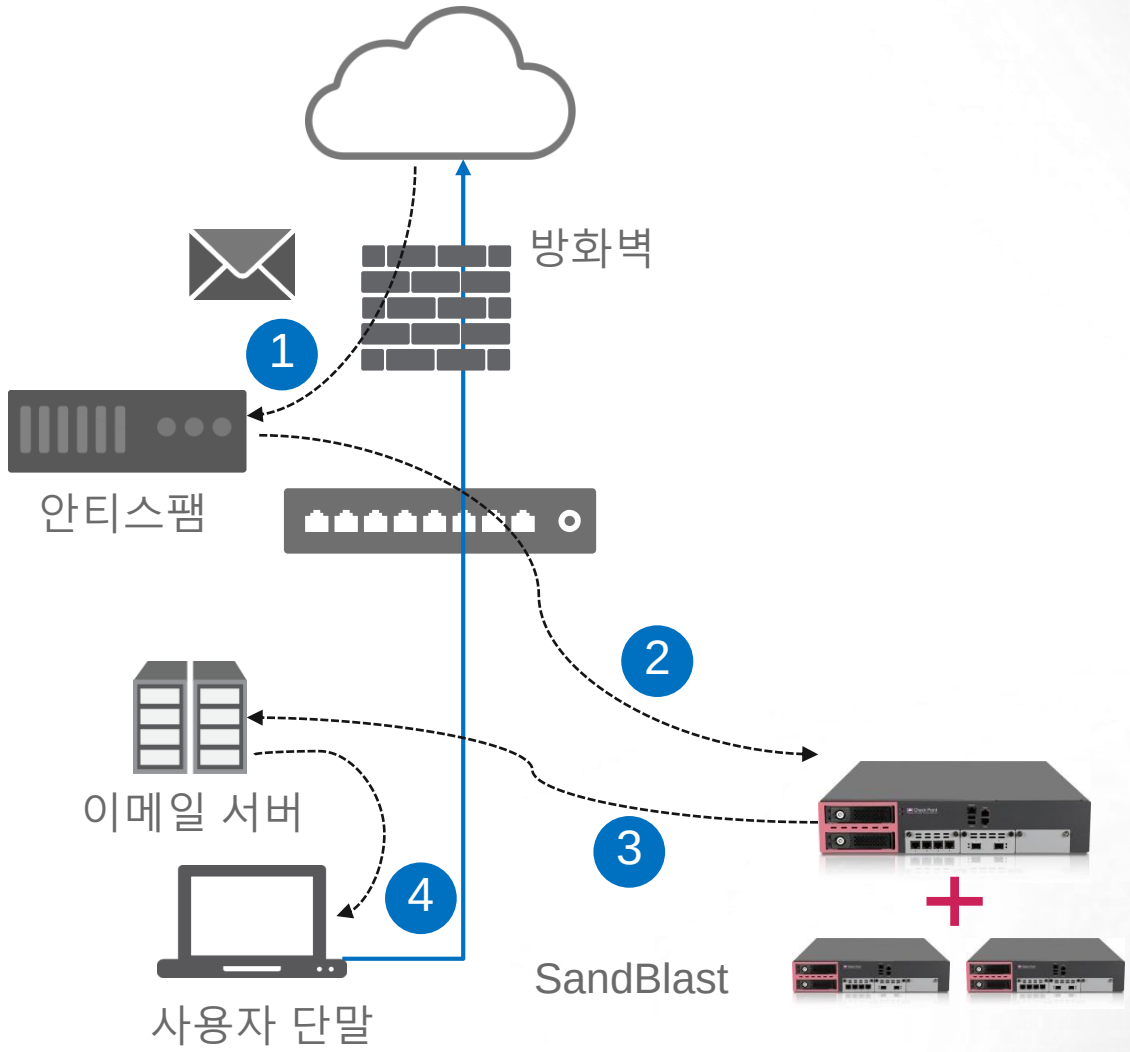
로드 쉐어링 이중화 구성 (최대 6 식 제공)

Option 1:
Check Point 방화벽과 연동

Option 2:
ICAP을 통한 3rd Party Web Proxy 연동

Option 3:
미러링 구성 (모니터링 제공)

SandBlast 이메일
이메일을 통한 APT 유입 대응

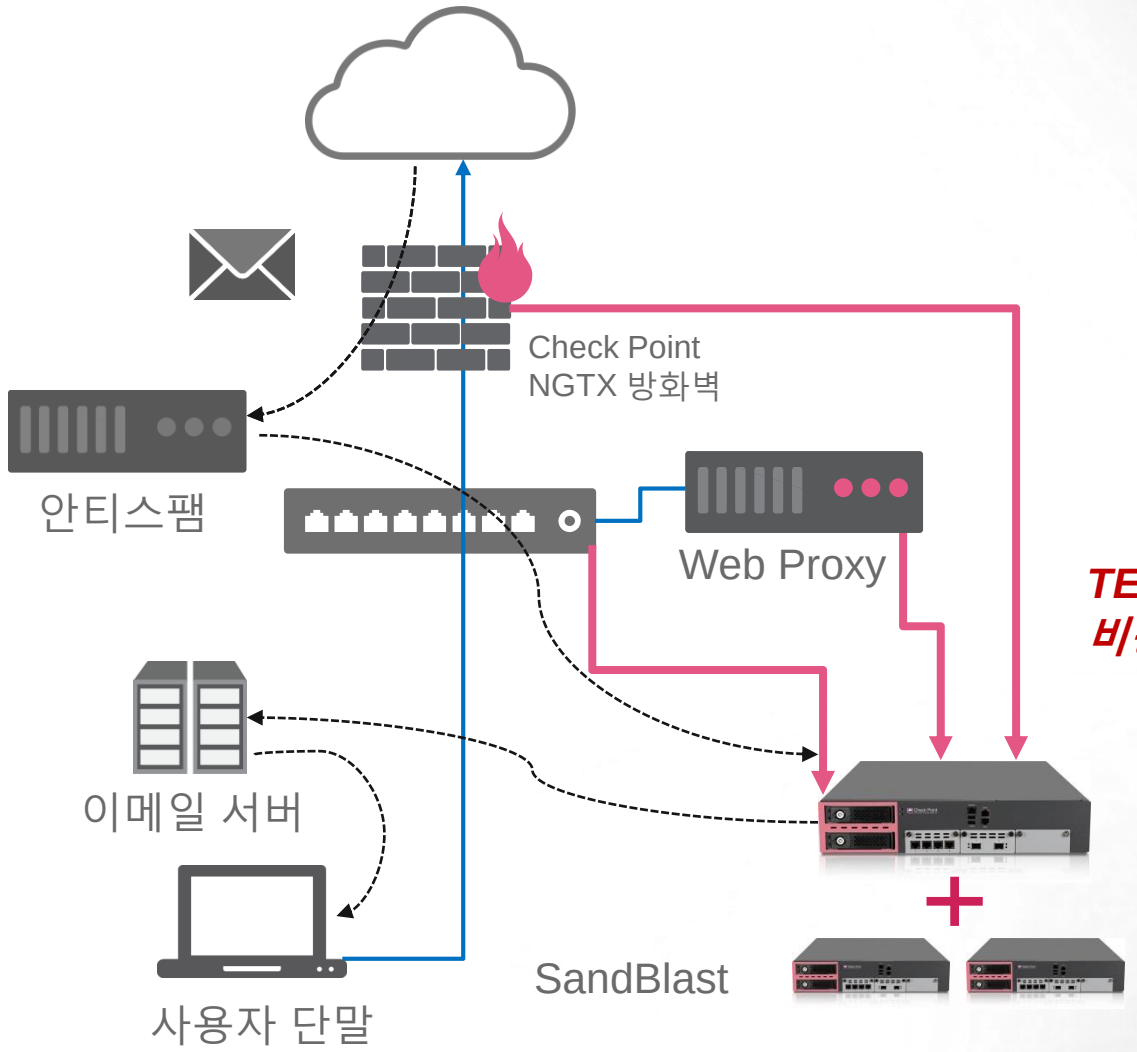


Option 1:
MTA 구성

Option 2:
BCC 모드 (모니터링)

Option 3:
미러링 구성 (모니터링)

SandBlast 하이브리드
네트워크 이메일을 통한 APT 유입 대응

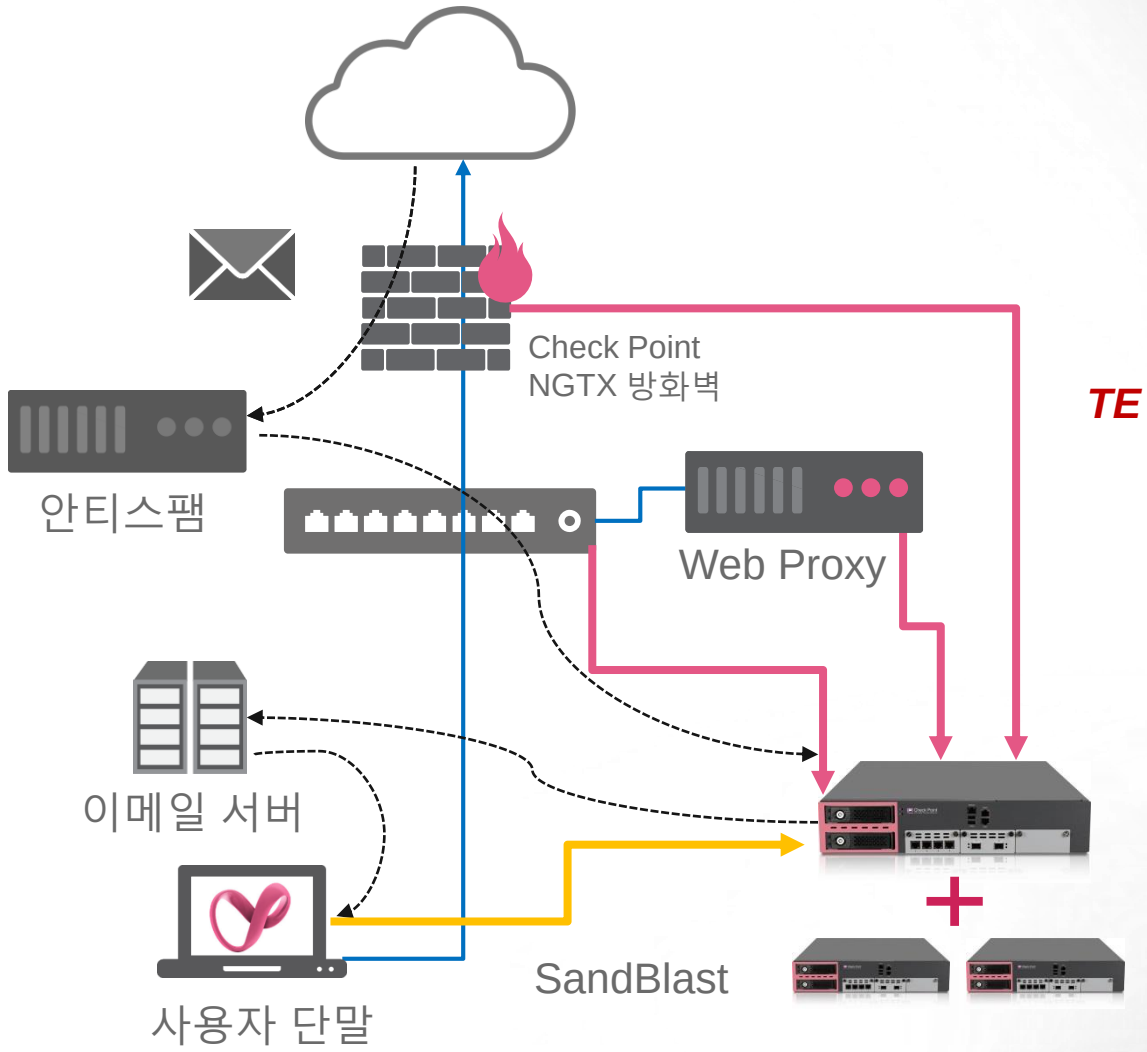


네트워크:
Check Point 방화벽 연동, ICAP 연동, 미러링

이메일:
MTA,BCC, 미러링

TE 1식으로 네트워크, 이메일로 유입되는 Zero-day, Unknown, APT 비용대비 효율적인 대응 제공

SandBlast 하이브리드 + 엔드포인트
네트워크 이메일 엔드포인트를 통한 APT 유입 대응



엔드포인트:
랜섬웨어 전용 엔진, 포렌식, 제로피싱

TE 1식으로 Zero-day, Unknown, APT 공격 유입경로 통합 대응

CHECK POINT APT 통합 대응 플렛폼

외부평가

SandBlast 수상 내역

WINNER

PCM Biz IT Excellence

PCM Biz IT EXCELLENCE 2017

WINNER

Best APT Protection

SC 2017 awards

WINNER

Endpoint Threat Prevention

COMPUTERWORLD AWARDS 2016

RECOMMENDED

Breach Prevention System

CHECK POINT NSS RECOMMENDED

WINNER

Security product of the year

NETWORK computing AWARDS 2016 WINNER

Check Point SandBlast ZERO-DAY PROTECTION

More than **9,000** customers

More than **1,500,000** enterprise endpoints and mobile devices

More than **40,000** gateways

> *"Check Point SandBlast Zero-Day Protection was on a level by itself. Check Point was one of the only companies that could do Threat Emulation and Threat Extraction—and they were the best"*
>
> Russell Walker
> Chief Technology Officer
> Mississippi Secretary of State

THE GREAT SEAL OF THE STATE OF MISSISSIPPI · IN GOD WE TRUST

Summary

1. Zero-day, Unknown, APT 모든 유입경로 실시간 차단
2. 단일 플렛폼 으로 이메일, 네트워크, 엔드포인트 서비스
3. 높은 탐지율, 빠른 성능, 손쉬운 구성
4. 통합 콘솔이용 TCO 절감 효과
5. Check Point 방화벽과 연동, 최상의 보안과 효율성

Thank you