새로운 위협기반의 보안 모델(Threat Centric Security)

네트워크 전 영역의 위협에 대한 보안전략

이성철이사
RM, GSSO APJ CISCO SYSTEMS Korea
December 2015

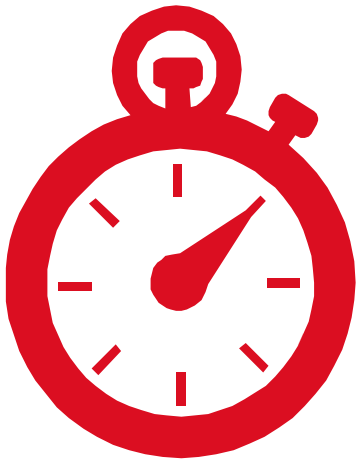
목차

악성코드의 진화

뉴스 헤드라인을 장식하는 보안 뉴스

공격 방식의 변화

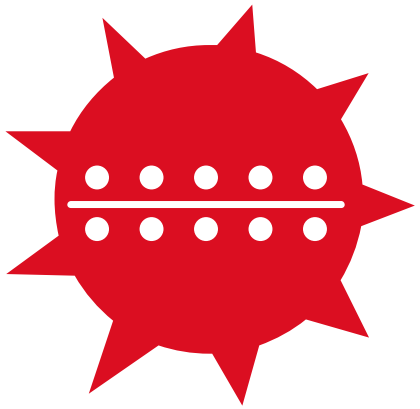
속도



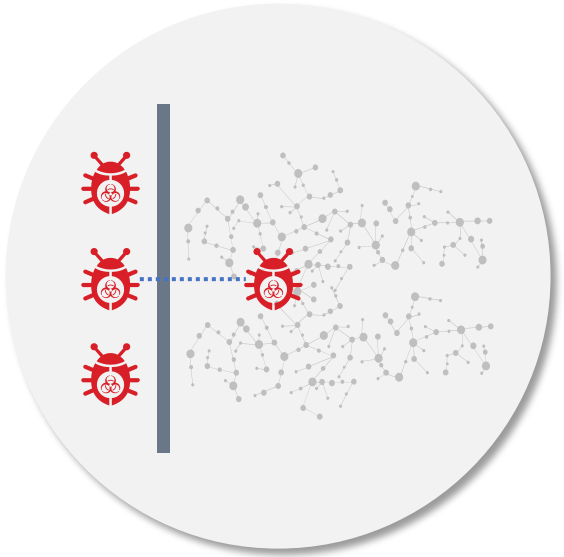
민첩

적응

파괴



지금 여러분의 환경에는 무슨 일이 ?

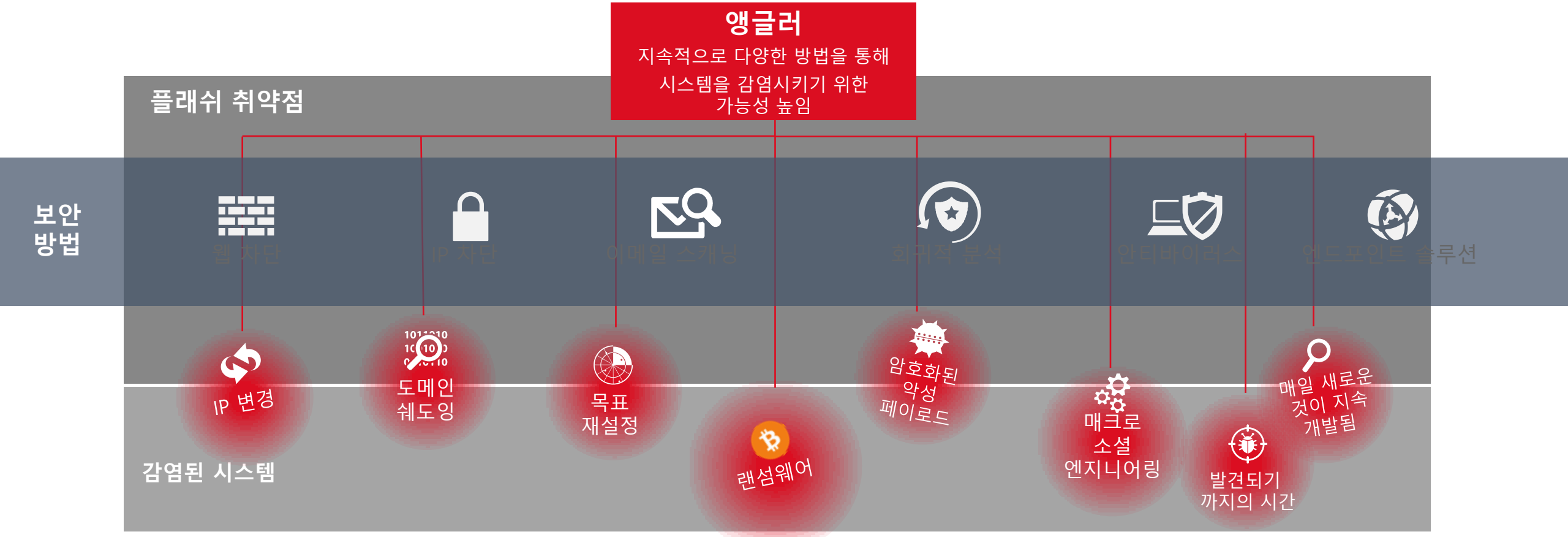


여러분의 환경에
침해사고가 발생될
수 있습니다.

이메일을 통해서
새로운 위협이
유입 될 수도 있습니다.

해커는 웹을 통한
명령어를 통해 제어를
할 수도 있게 됩니다.

앵글러 사례로 본 악성코드 진화



지속적인 업그레이드를 통해 앵글러의 침투 성공률은 40% 까지 증가

2014년의 다른 공격 키트에 비해 두 배이상 효과적

위협은 더욱 지능화 복잡화 되고 있습니다.

변화하는
비즈니스 모델

동적인
위협 환경

복잡성
및 단편화

다양한 보안 위협이 우리가 자주 방문하는 사이트안에 숨어 있습니다.

60%
몇 시간
만에유출되는
데이터의 비율

85%
수 주 동안
드러나지 않는
POS(point-of-sale)
침입의 비율

54%
수 개월 동안
드러나지 않은
데이터 유출
비율

51%
지난 해 보고한
손해가 천만 달러
이상인 기업의
증가 비율

시작 → 시간 → 주 → 월 → 연

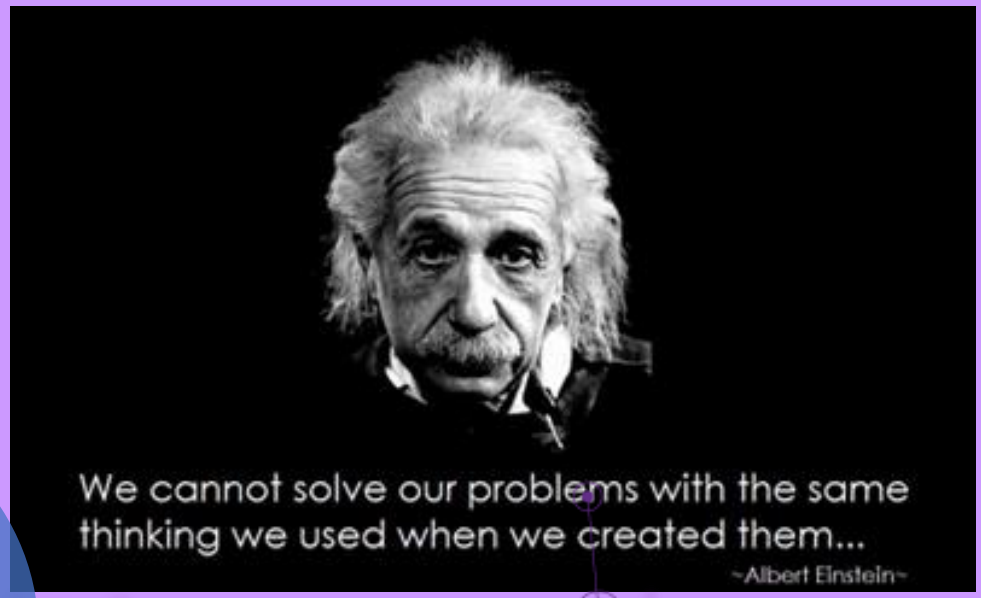
만약 여러분이 침해 사실을 알았다면,
여러분의 보안은 달라졌을까요 ?

위협중심의 차단 전략

왜 보안은 끝이 없을까요 ?

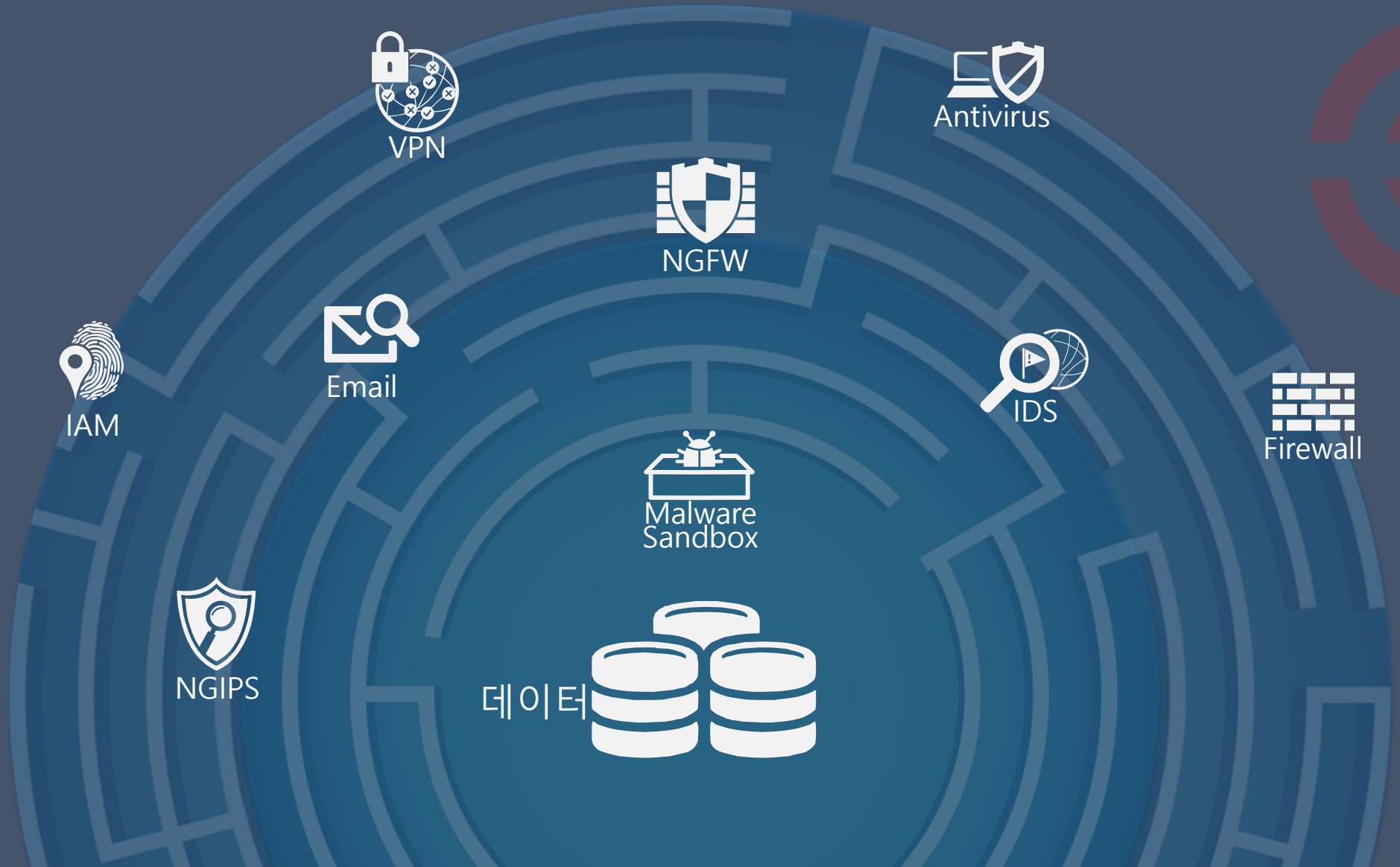
전체적인 가시성 확보 필요

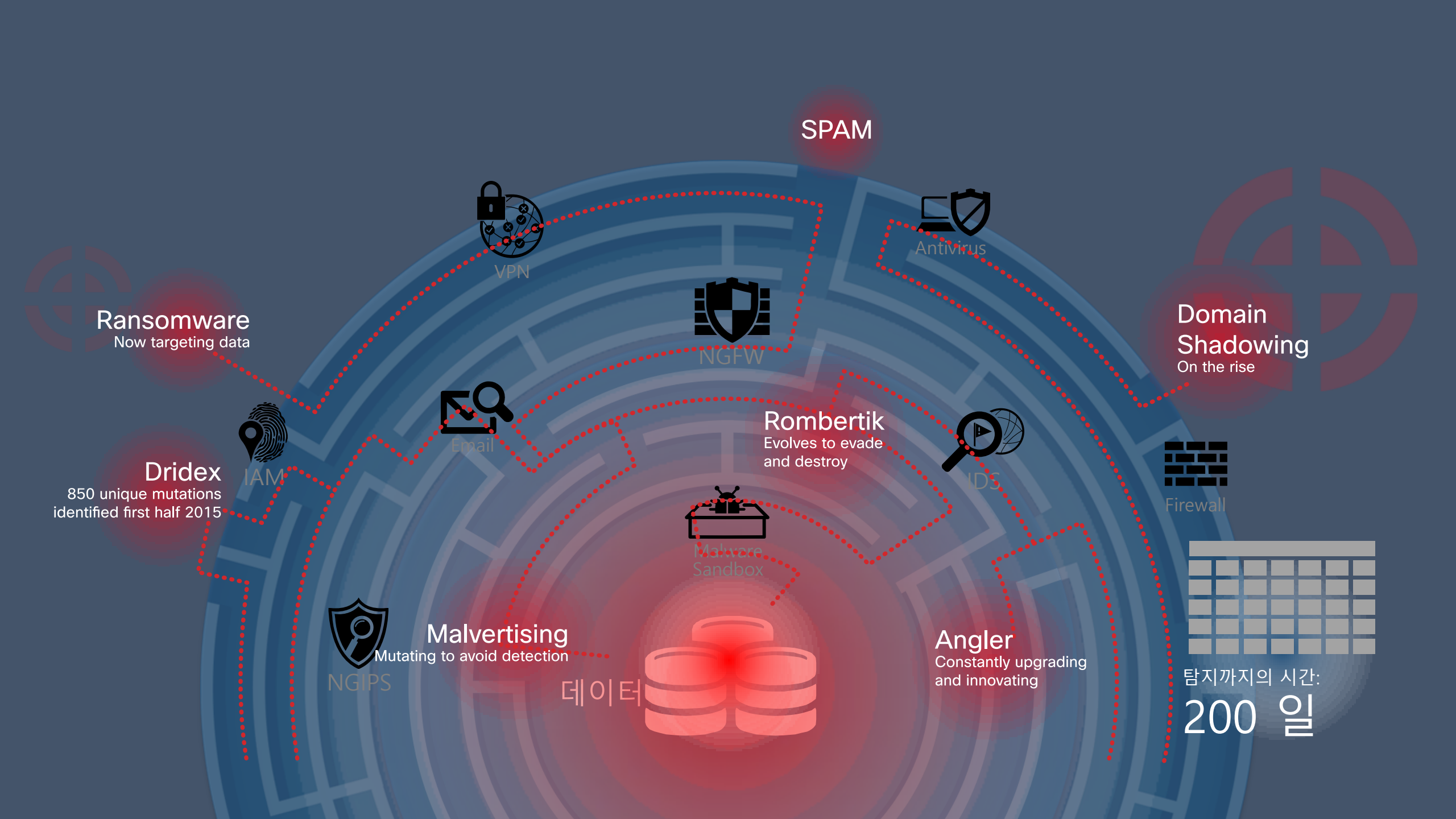
우리가 보는 것은 전체의
몇%나 될까요 ?



지금 여러분의 보안시스템은 ?

공격자들은 다양한 방법으로 공격을 수행



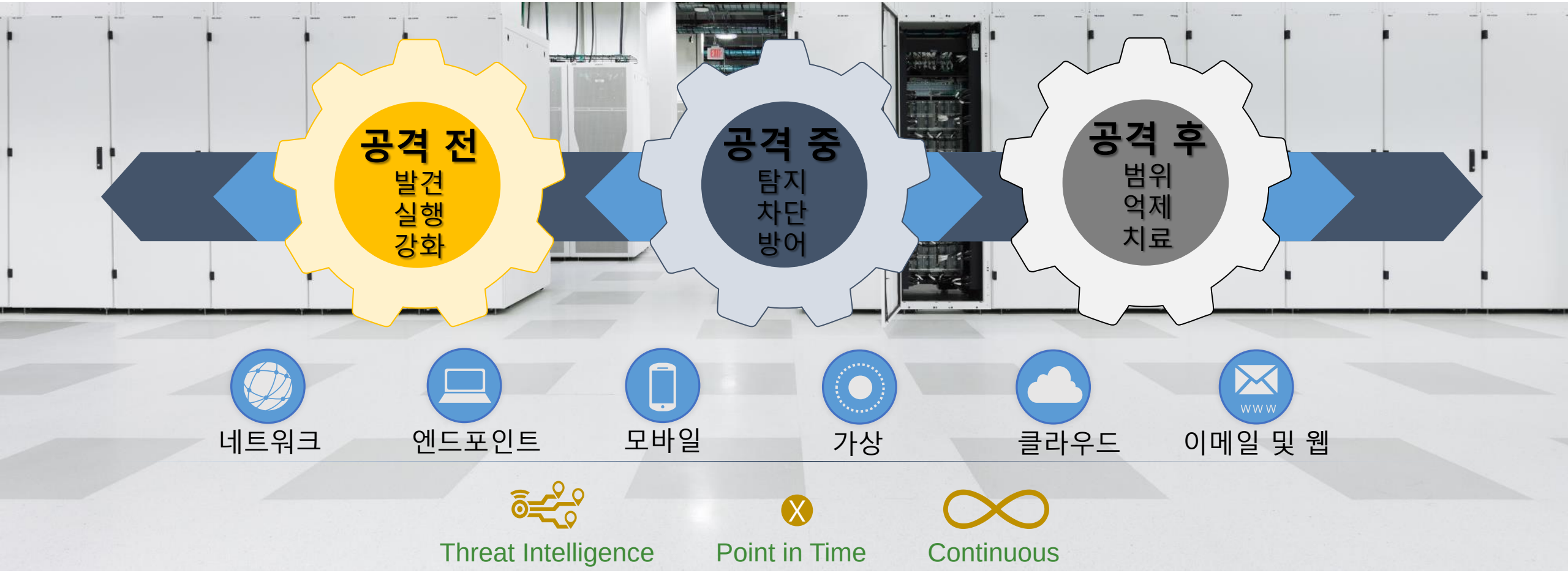

SPAM
VPN
Antivirus
Ransomware
Now targeting data
NGFW
Domain
Shadowing
On the rise
Email
Rombertik
Evolves to evade
and destroy
IAM
IDS
Dridex
850 unique mutations
identified first half 2015
Firewall
Malware
Sandbox
NGIPS
Malvertising
Mutating to avoid detection
데이터
Angler
Constantly upgrading
and innovating
탐지까지의 시간:
200 일

위협 중심의 차단 전략 필요

탐지하기 까지의 시간 :

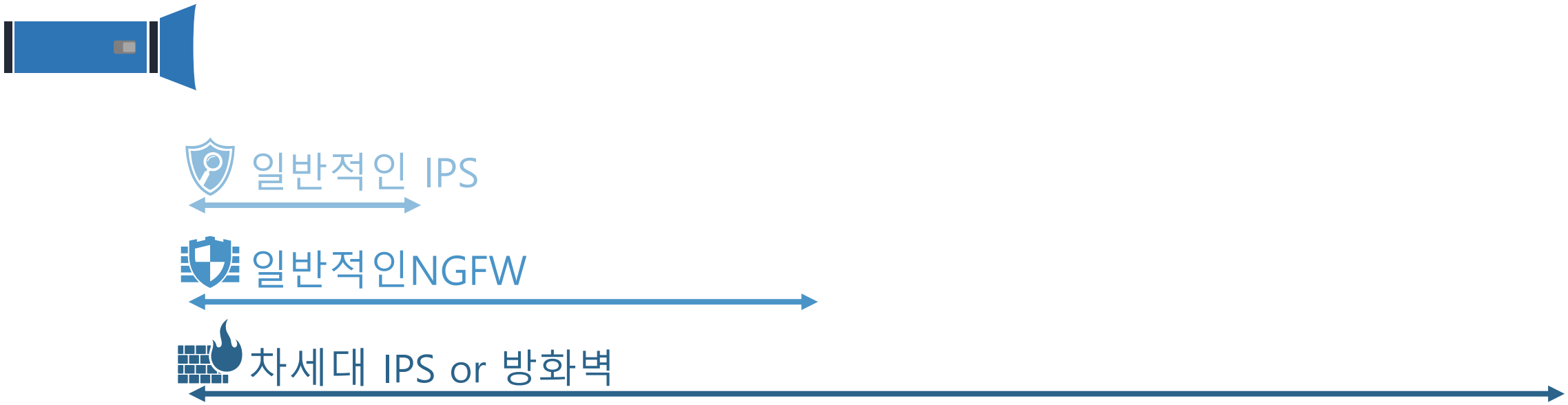
46 시간

새로운 보안 모델을 통한 전방위적인 차단 전략



여러분들의 위협을 얼마나 들여다 보고 있나요 ?

많이 이해 할수록 제대로 방어 할 수 있습니다



최신의 위협에 대한 빠른 대응

1001 1101 1110011 0110011 101000 0110 00
101000 0110 00 0111000 111010011 101 1100001 110
1100001110001110 1001 1101 1110011 0110011 101000 0110 00

1001 1101 1110011 0110011 101000 01
101000 0110 00 011100
1100001110001110 1001

Cisco Talos 위협 인텔리전스

이메일 | 엔드포인트 | 웹 | 네트워크 | IPS | 디바이스

3-5분간격의 자동업데이트

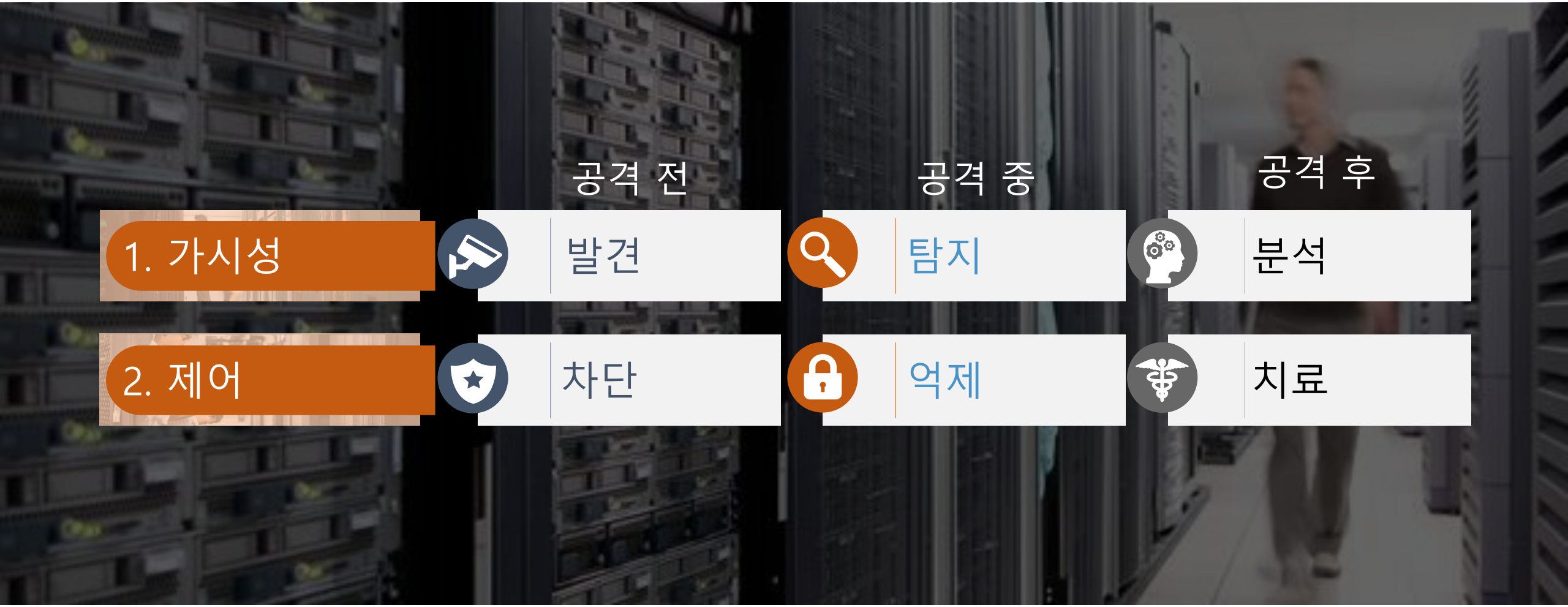
- 전 세계 160만 개의센서 매일 수신되는
- 100TB의 데이터
- 1억 5천만 개 이상 구축된 엔드포인트
- 600명의 엔지니어, 기술자, 연구원
- 35% 전 세계 이메일 트래픽 처리

- 130억 개의 웹 요청
- 24시간x7일x365일 운영
- 매일 4.3억 회의 웹 필터링 차단
- 40가지 이상의 언어
- 매일 수신하는 110만 개의 악성코드 샘플
- Cisco AMP 커뮤니티
- 비공개/공개 위협 정보 피드

- Talos Security Intelligence
- AMP Threat Grid Intelligence
- Cisco AMP Threat Grid Dynamic Analysis에서 매월 생성되는 1천만 개 파일
- Microsoft 및 업계보다 먼저 공개
- Snort & ClamAV 오픈소스 커뮤니티
- AEGIS™ Program

AMP
Advanced Malware Protection

보호의 2가지 기본 요인



	공격 전	공격 중	공격 후
1. 가시성	발견	탐지	분석
2. 제어	차단	억제	치료

악성코드의 스토리를 말하다

Tell the story

WHO

WHAT

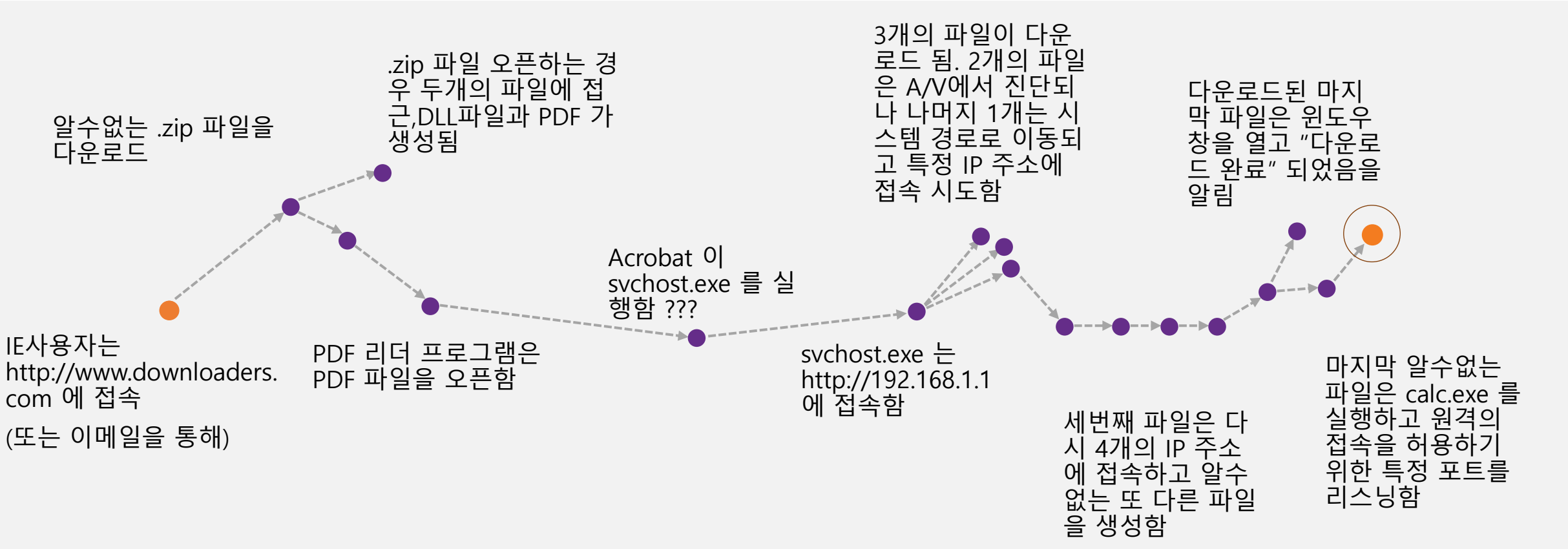
WHEN

WHERE

HOW

악성코드의 스토리를 말하다

스토리를 찾아 떠나다


알수없는 .zip 파일을 다운로드
.zip 파일 오픈하는 경우 두개의 파일에 접근,DLL파일과 PDF 가 생성됨
3개의 파일이 다운로드 됨. 2개의 파일은 A/V에서 진단되나 나머지 1개는 시스템 경로로 이동되고 특정 IP 주소에 접속 시도함
다운로드된 마지막 파일은 윈도우 창을 열고 "다운로드 완료" 되었음을 알림
Acrobat 이 svchost.exe 를 실행함 ???
IE사용자는 http://www.downloaders.com 에 접속
(또는 이메일을 통해)
PDF 리더 프로그램은 PDF 파일을 오픈함
svchost.exe 는 http://192.168.1.1 에 접속함
세번째 파일은 다시 4개의 IP 주소에 접속하고 알수없는 또 다른 파일을 생성함
마지막 알수없는 파일은 calc.exe 를 실행하고 원격의 접속을 허용하기 위한 특정 포트를 리스닝함

WHY VISIBILITY

이런 위협의 전체 스토리를 알 수 있으면 어떨까요?

Who

어떤 사용자가
처음 접근했나

What

어떤 애플리케이션
이 영향을 받았나

Where

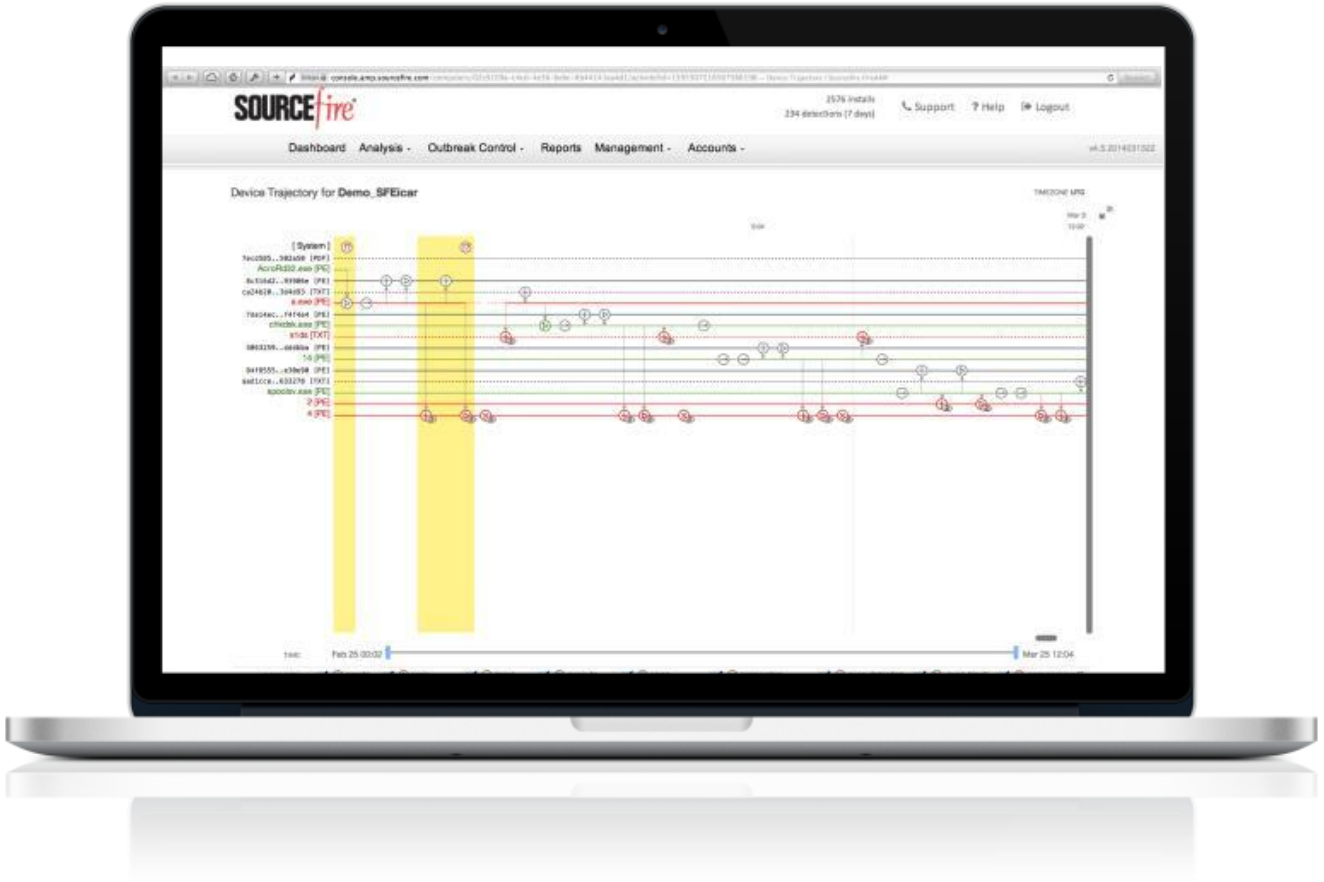
침해당한 영역 범위

When

위협에 노출된
시간과 타임라인

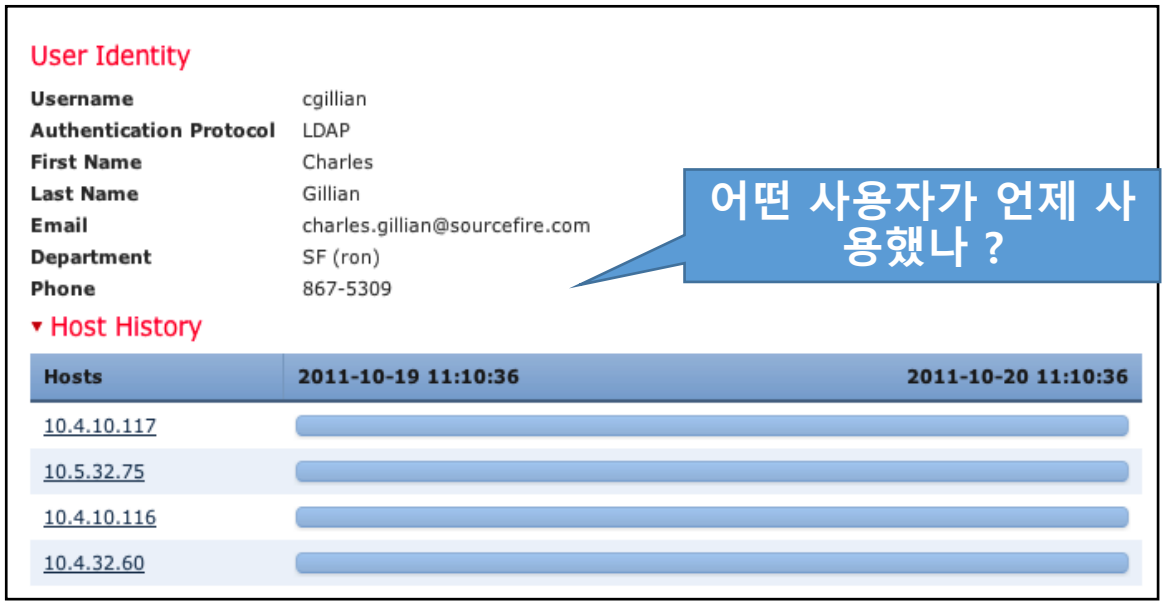
How

위협의 진행상황과
감염원인



트래픽 분석을 통한 실시간 자산 인식

가시성 확보
위협중심의 방어를 위한 기반

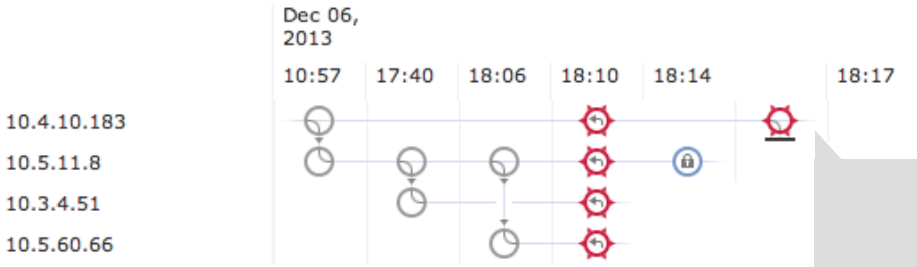


Network File Trajectory for 0517f034...588e1374

SAMPLE

File SHA-256	0517f034...588e1374	**First Seen**	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	**Last Seen**	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	**Event Count**	7
File Category	Executables	**Seen On**	4 hosts
Current Disposition	Malware	**Seen On Breakdown**	2 senders → 3 receivers
Threat Score	High		

Trajectory



Time 2013-12-06 18:17:27
Event Type File Sent
IP Address 10.4.10.183
Blocked Recipient 10.5.11.8
File Name WindowsMediaInstaller.exe
Disposition Malware
Action Malware Block
Application Protocol HTTP
Client Firefox

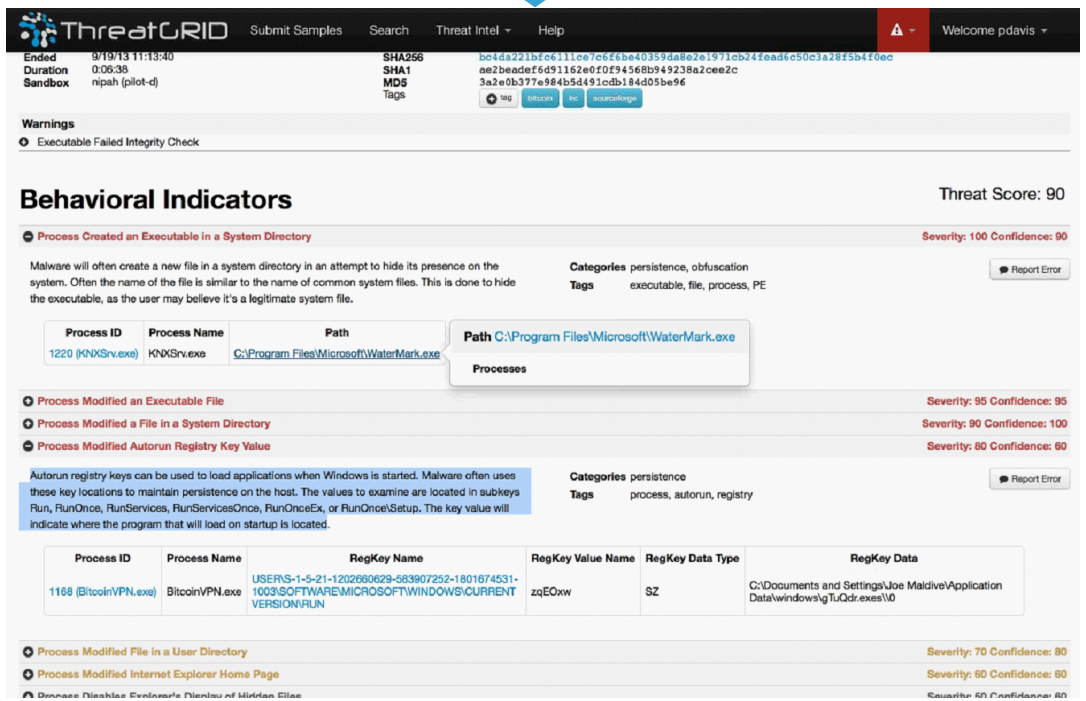
첫 공격후 8시간이 지난 시점에 악성코드는 초기 진입하였던 지점을 통해 재시도하려고하나 악성코드로 인지되어 차단됨

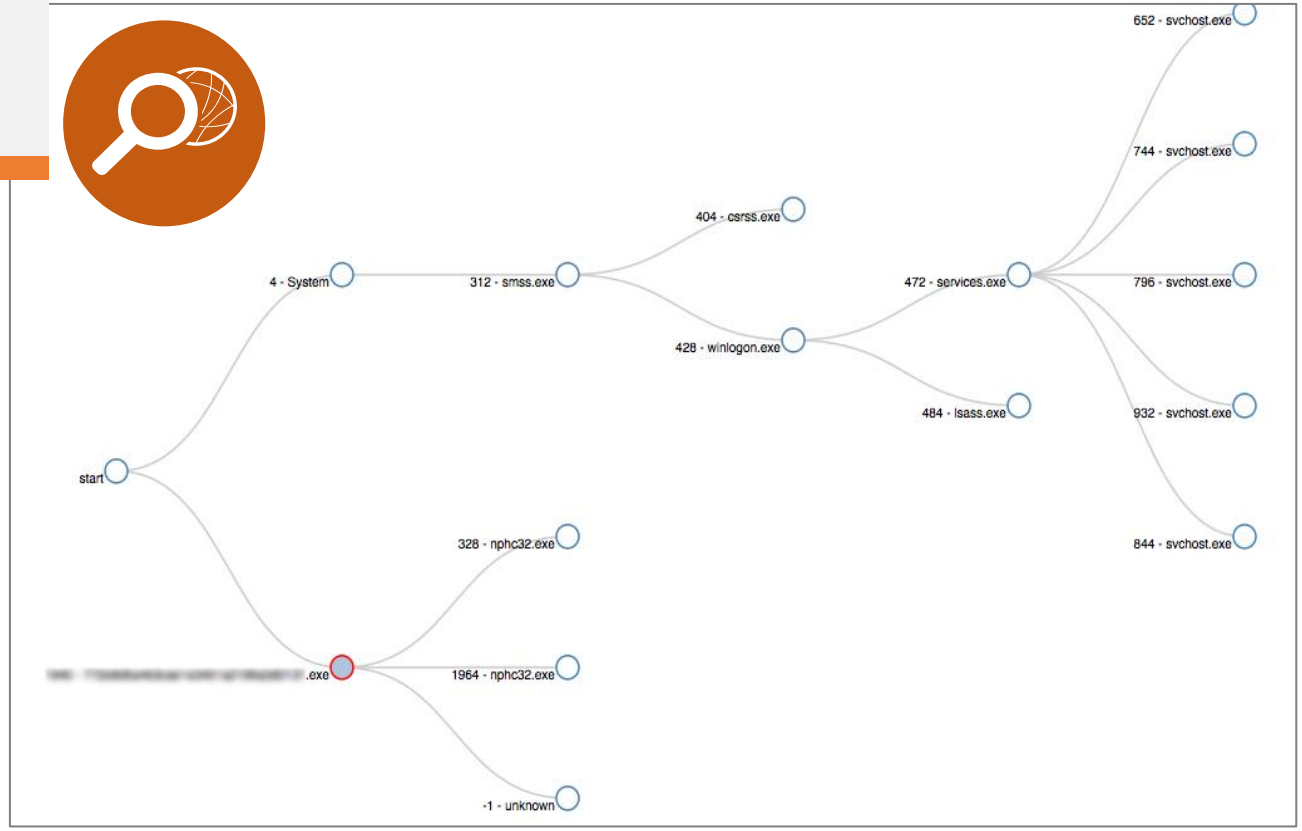
Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

너가 한 일을 모두 다 알고 있다.

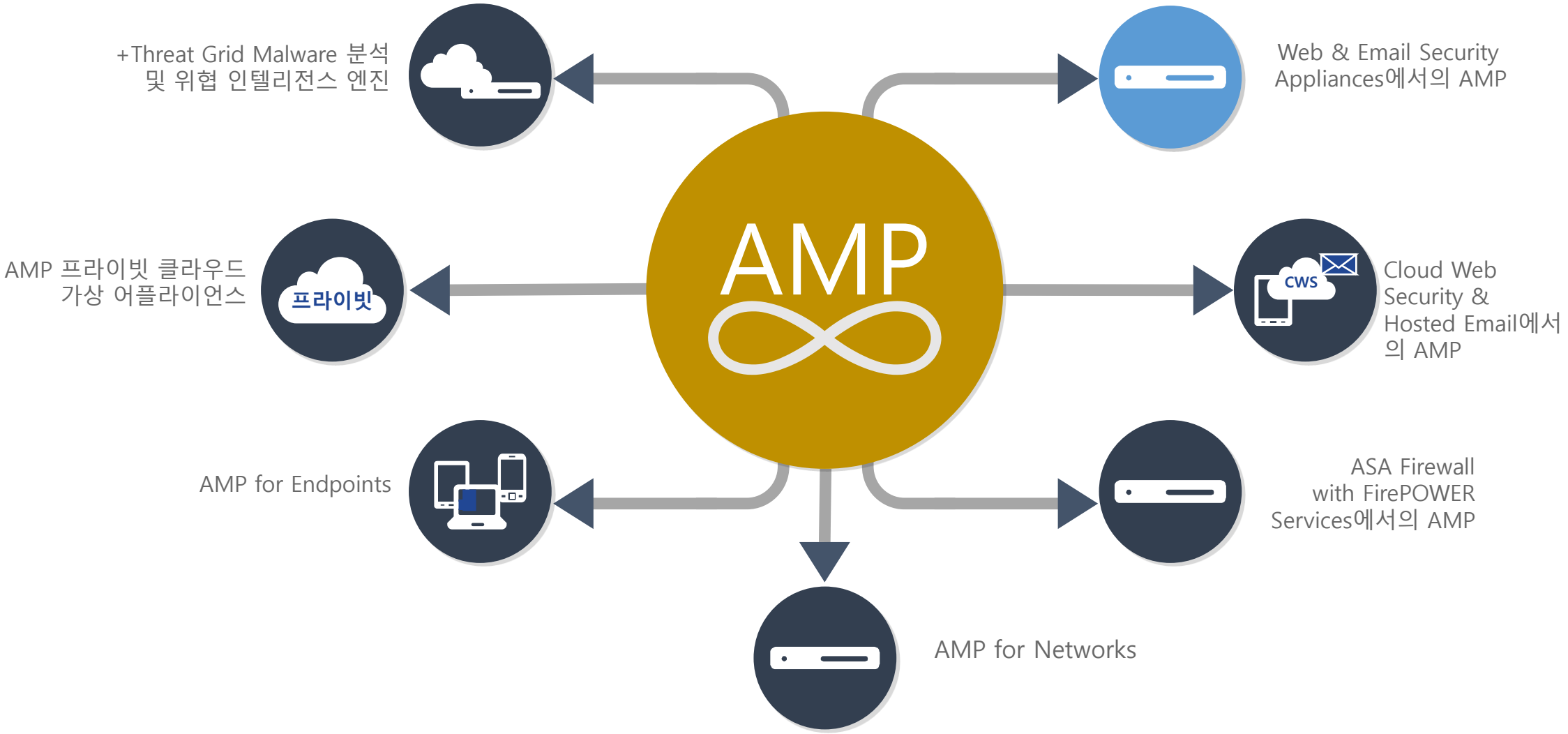
- 단순한 분석정보는 No
- 분석정보의 고도화
- 각 샘플과 수십억 개의 과거 악성코드간의 상관관계 분석





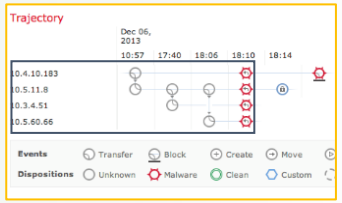
AMP Everywhere

네트워크 전체를 보호하는 Cisco AMP Everywhere 전략

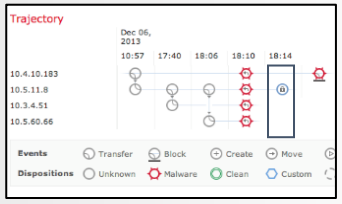


네트워크 전반의 보호

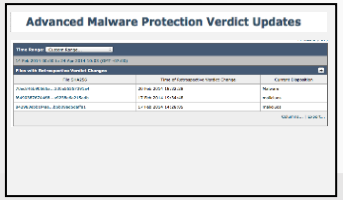
네트워크

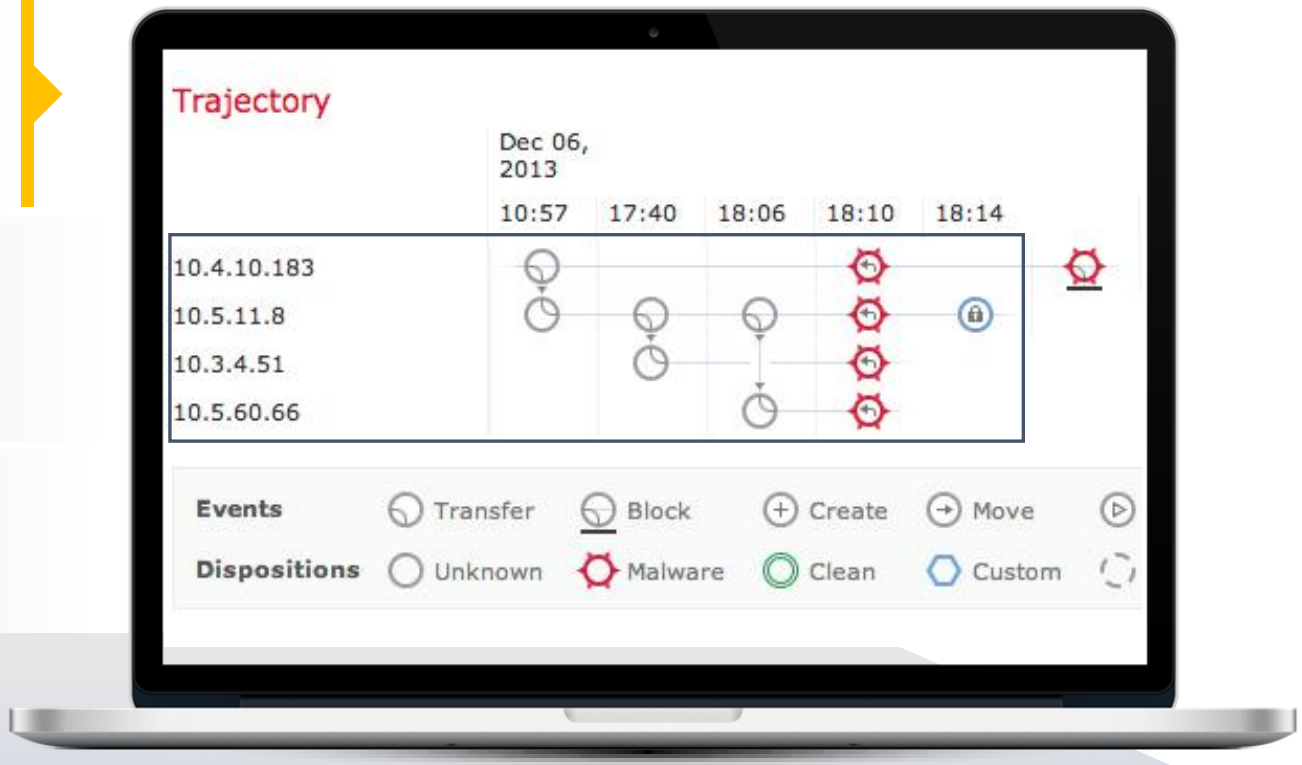


엔드포인트



컨텐츠

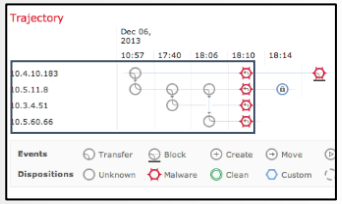




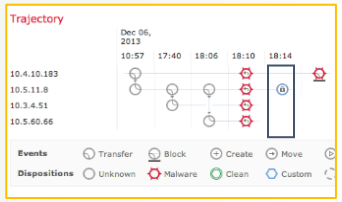
네트워크 플랫폼은 보안 침해 지표, 파일 분석 및 파일 경로 분석을 사용하여 운영 환경 전체에서 악성 파일이 이동한 방식을 정확히 나타냄

엔드포인트 전반의 보호

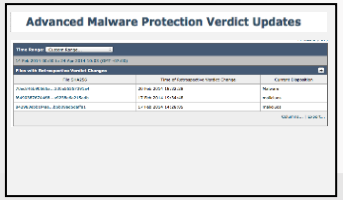
네트워크

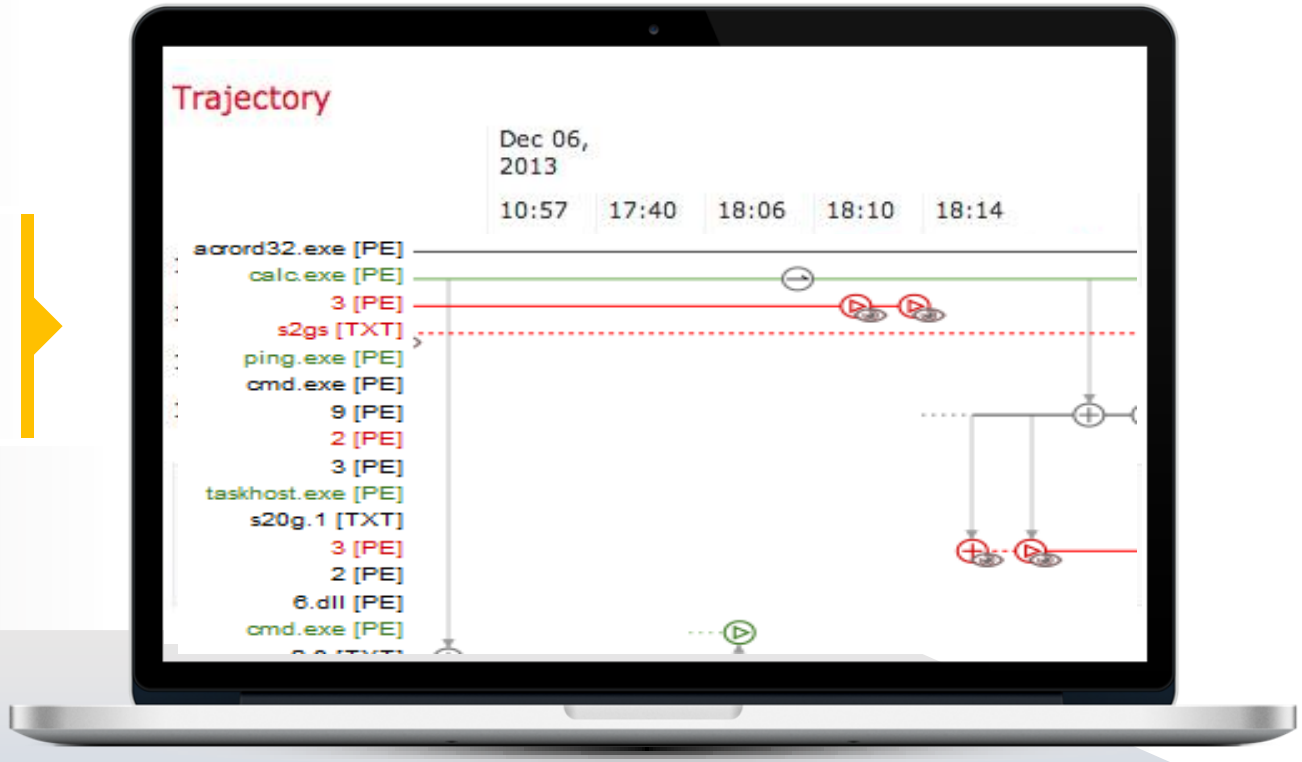


엔드포인트



컨텐츠

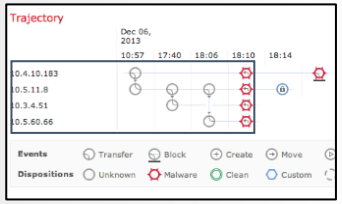




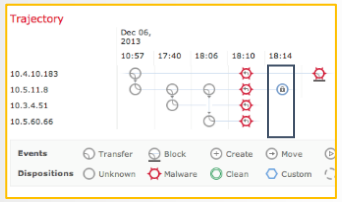
엔드포인트 플랫폼은 디바이스 경로 분석, 탄력적인 검색, Outbreak Control를 바탕으로 AMP for Endpoints 커넥터가 설치된 디바이스에서 최근에 탐지된 악성코드를 격리함

웹 및 이메일 전반의 보호

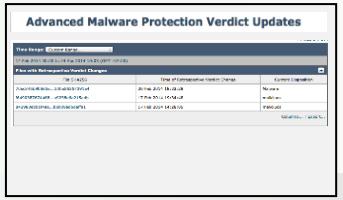
네트워크

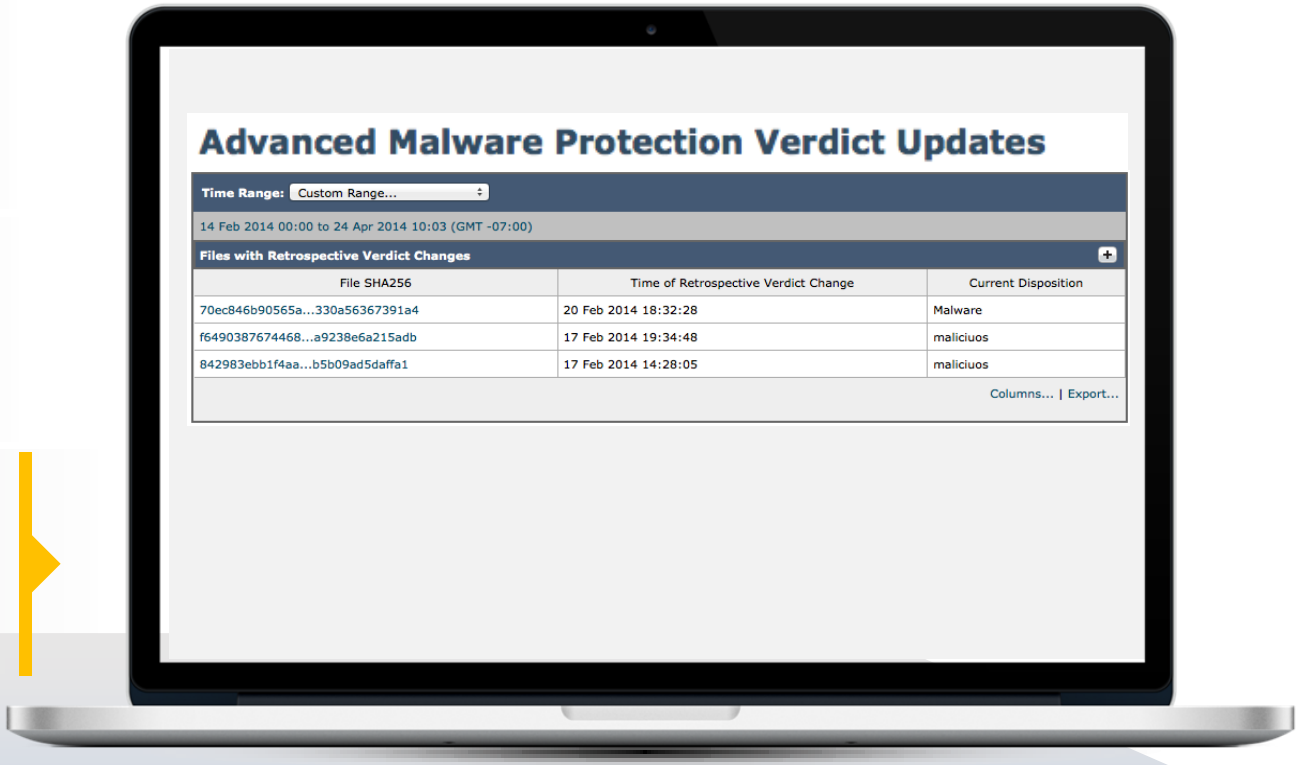


엔드포인트



컨텐츠





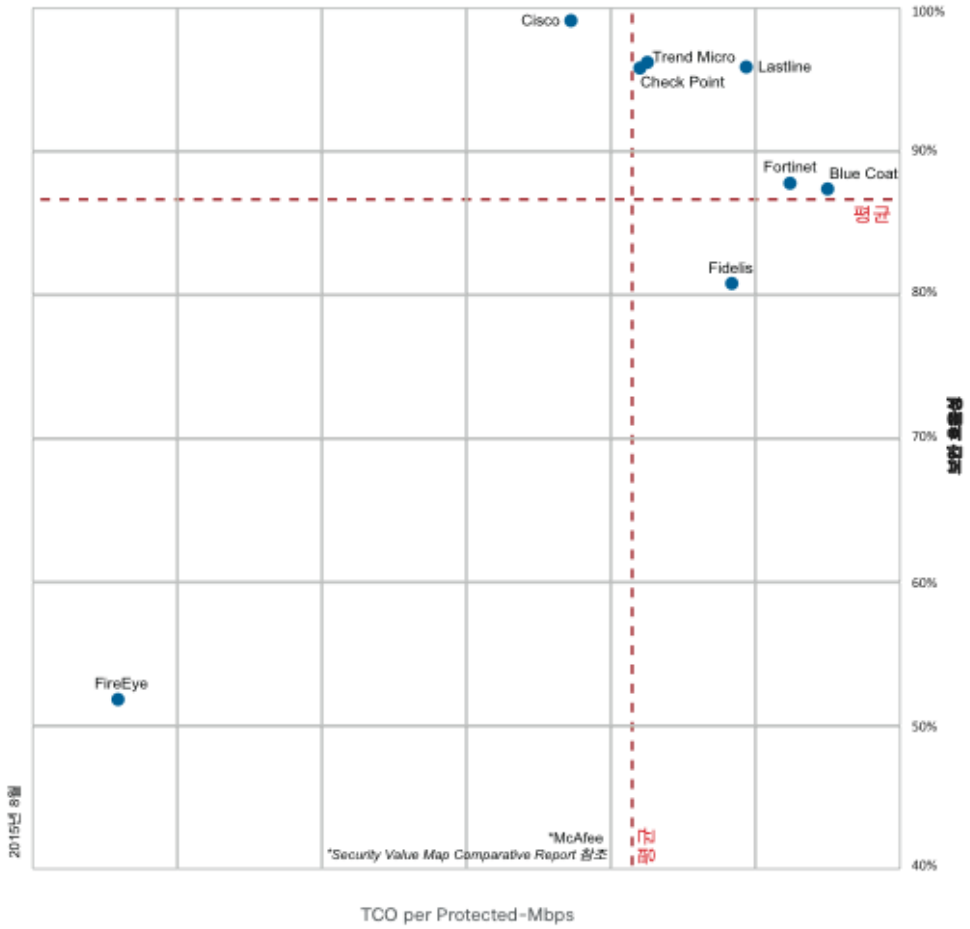
Cisco® AMP for Web and Email은 알려진 악성코드를 차단하고 알려지지 않은 파일이 악의적인 것으로 입증되면 회귀적 알림을 생성하여 웹 및 이메일 트래픽에서 악성코드 위협으로부터 보호함

다시 한번 NSS Test 정상에 오른 Cisco Advanced Malware Protection

NSS BDS(Breach Detection Systems) Security Value Map에서 최고의 보안 효율성 차지

Cisco AMP (Advanced Malware Protection)가 2년 연속 최고의 보안 효율성을 제공하는 선두주자로 자리매김 했습니다. 최신 NSS Labs BDS (Breach Detection Systems) 테스트에서 악성코드 및 익스플로잇을 99.2%, 우회 기술을 100% 차단했습니다.

NSS Labs Breach Detection Systems(BDS) Security Value Map™



현재의 위협 환경에서 위협을 탐지하고 해결하는 데 걸리는 시간이 기업의 수익을 크게 좌우할 수 있습니다. Cisco AMP만이 유일하게 특정 시점 탐지에 머무르지 않고 지속적인 분석 및 회귀적 보안을 통해 확장 네트워크의 전반에서 지속적으로 악성코드를 모니터링, 탐지, 차단, 억제, 치료합니다. Cisco AMP는 공격 전, 중, 후의 전 범위에서 최신 위협으로부터 보호하면서 위협 탐지 및 치료에 드는 시간을 모두 단축함으로써 기업의 시간과 비용 부담을 줄여줍니다. 또한, 지능형 위협은 광범위하게 영향을 미치므로 Cisco는 AMP Everywhere를 제공합니다. 네트워크, 데이터 센터, 엔드포인트, 모바일, 가상, 이메일, 웹 등 다른 어떤 솔루션보다 더 많은 공격 벡터에서 커버리지를 제공합니다.

2015 NSS Labs BDS 보고서에서 Cisco AMP가 어떻게 다음을 입증했는지 자세히 알아보십시오.

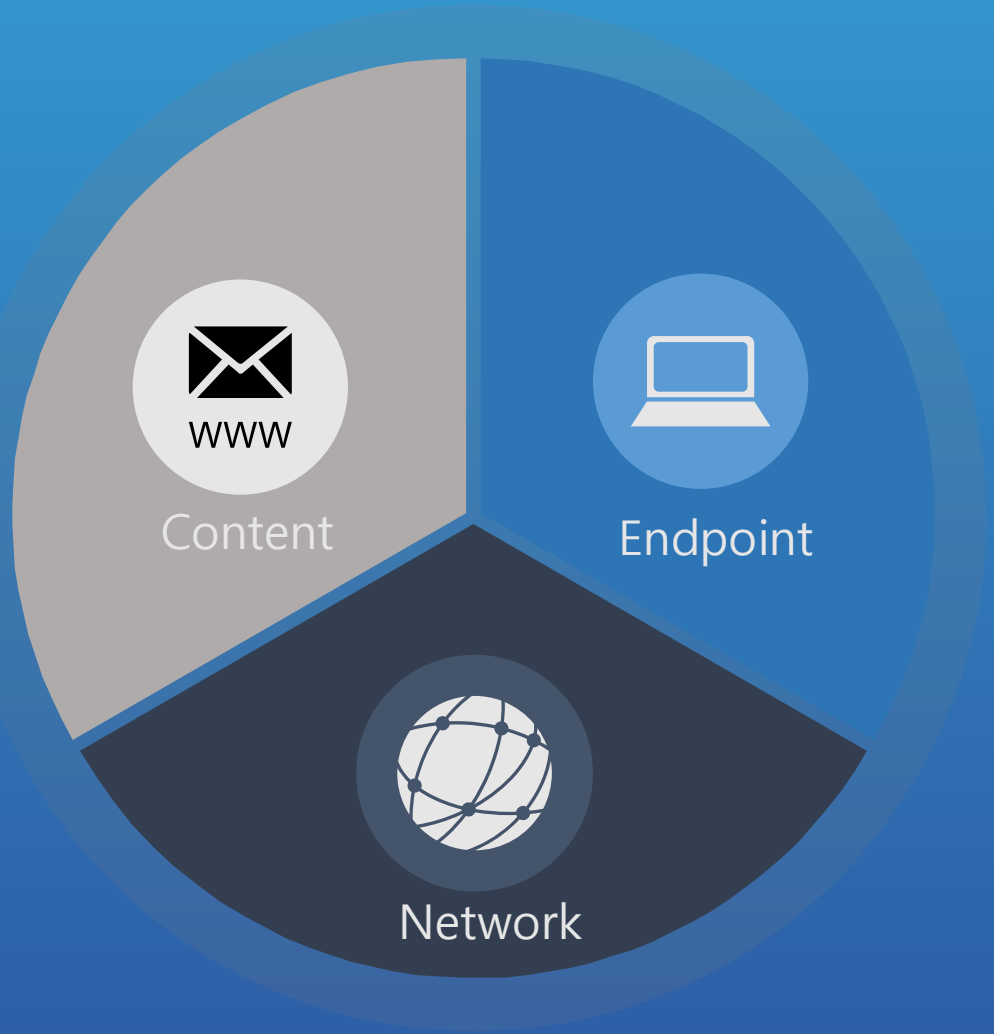
- 99.2% 보안 효율성 - 전체 테스트 대상 벤더 중 최고
- 벤더 중 유일하게 테스트 중에 모든 우회적 기술을 100% 차단
- 엔드포인트 또는 애플리케이션 레이턴시에 미치는 영향을 최소화하면서 뛰어난 성능 유지

최신 보고서에서 Cisco가 어떻게 다른 모든 테스트 대상 벤더보다도 많은 공격을 차단했는지 알아보십시오.

AMP Everywhere의 가치

악성코드에는 한계가 없습니다. 따라서 지능형 악성코드 차단 솔루션 역시 한계가 있어서는 안 됩니다. Cisco는 업계에서 가장 다양한 AMP (Advanced Malware Protection) 제품의 포트폴리오를 제공합니다. 엔드포인트, 네트워크 어플라이언스, 보안 콘텐츠 게이트웨이, 모바일 디바이스, 가상 환경 등 위협이 나타날 수 있는 확장된 네트워크의 모든 실행 지점에서 사용 가능한 제품으로 구성되어 있습니다. 또한, 고객은 NGIPS 및 NGFW 등 이미 구축된 Cisco 네트워크 인프라를 활용하여 구축을 능률화하고 비용 효율적으로 사용하도록 AMP를 적용함으로써 현재 그리고 미래의 투자 효과를 극대화할 수 있습니다.

Summary



1. 네트워크와 앤드포인트단까지 통합된 위협 중심의 보안 전략
2. 지능형 위협을 차단하기 위한 멀티 레이어 차단 전략
3. 단순히 한 지점이 아닌 전방위적인 관점에서 가시성 기반하 위협관리

TOMORROW starts here.