THE SECOND ECONOMY | The Market Dynamics of Cybersecurity

Find and Convict Threats Faster with Dynamic Endpoint & Active Response

Darren Kim – Intel Security - North Asia Senior Sales Engineer

intel Security

Agenda

THE SECOND ECONOMY

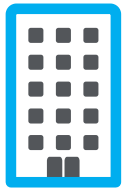
- Dynamic Endpoint Overview?
- Adaptive Threat Protection
- Active Response: Easier and Faster
  - Are we under attack?
  - What has happened?
  - How do we stop it?
- Conclusion

THE SECOND ECONOMY

Dynamic Endpoint Overview

Everyday Enterprises Face the Battle Against Cyber Threats

진화된 공격은
기업이나 조직을
괴롭히는 것을 지속



기업은 너무 많은
데이터를 가지고
복잡하며
인텔리젼스가 불충분

위협에 대한 가시성
부족으로 심층적인
조사 및 확신있는
치료를 방지의 어려움

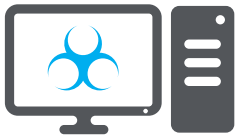
Silos 및 수작업
프로세스로 인해
가동 시간이
길어지며 방어가
어려워짐

Security's Perfect Storm

THE SECOND ECONOMY

사이버 범죄의 산업화

매년마다
55%[1] 위협이
증가



70-90%[1]
의 악성 코드는 단일
조직에서만 고유

28%[1]
의 공격이 타겟형

단편적인 보안 시장

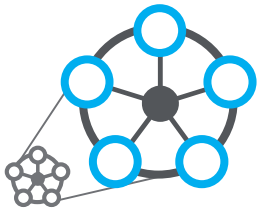
50 offerings[2]
까지 환경을 평가하고 확보

[1] Verizon DBIR 2015 / Intel Security Golden Hour Survey 2015
[2] Intel Security

intel Security

The State of Threat Intelligence Today

THE SECOND ECONOMY



77%

의 북미 및 유럽 기업 보안 정책 결정자의 우선 순위가 향상된 위협 인텔리전스 기능을 보고 [1]

관리중인

50+

조각난 인텔리젼스 피드는 너무복잡[2]

88.1%

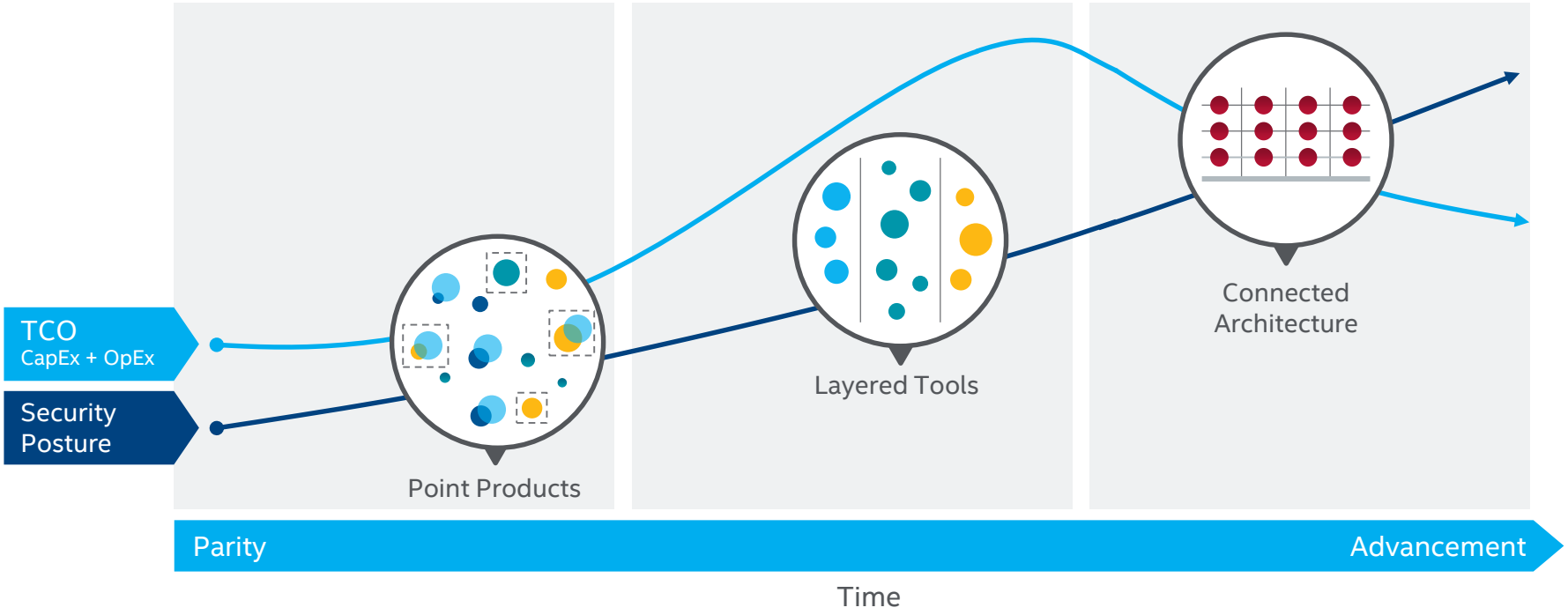
거의 모든 소스로부터 위협 정보를 수집 할 수있는 능력이 없음[3]

[1] Forrester
[2] Intel Security
[3] SANS Institute, "Who's Using Cyberthreat Intelligence and How?"

intel Security

Building Security by Silo

Delivering Operationally-Effective Security




VCR
PLASMA TV
DVD
YAMAHA
RECEIVER
LASER DISK
SATELLITE
TOSHIBA
SELECT
MENU
INFO
GUIDE
LIST
FAV
ACTION
BANNER
MUTE
STOP/SOURCE
PAUSE
REW
FF
PLAY/PIP
REC
INPUT
VOL
CH
EXIT
TV
VCR
DVD

보안 위협은 어떻게 최소화 시킬까요?

오늘날의 보안 문제를 해결하기 위해서는 통합된 시스템이 필요합니다.

THE SECOND ECONOMY

EXPANDING ATTACK SURFACE

GOLDEN HOUR OF RESPONSE

talent SHORTAGE

Protect

처음부터 위협가능성을 최소화

Detect

제로데이 감염을 더 빨리 발견 하고 유출을 최소화

Correct

교정할 수 있는 인력, 시간 및 비용을 절감

Adapt

보호 기능을 실시간으로 자동 학습 하고 업데이트

엔드 포인트 보안의 진화

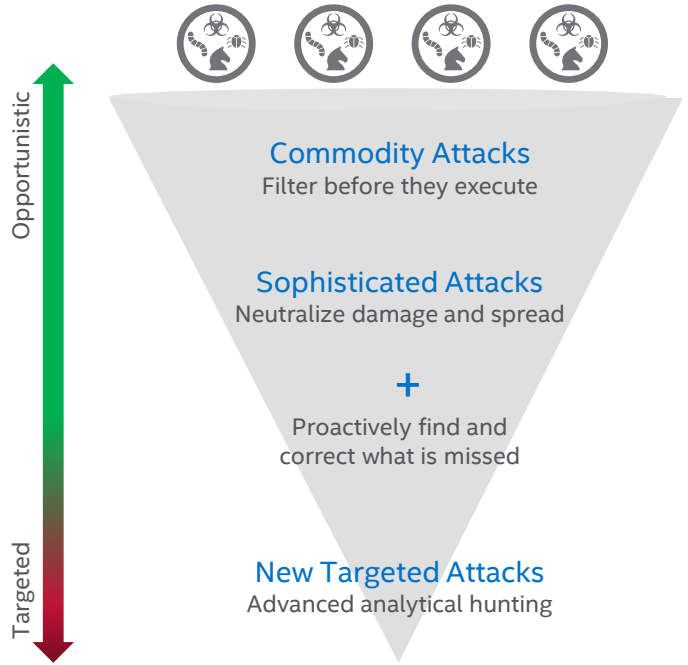
더 이상의 위협방지 기능은 없습니다.

THE SECOND ECONOMY

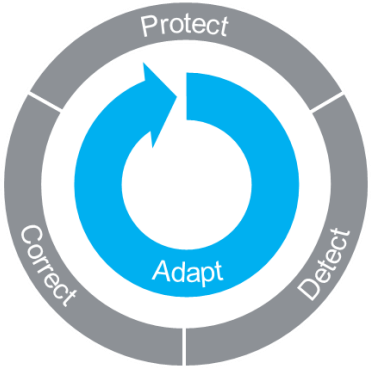
다이나믹 엔드포인트 위협 방어

Integrates protect, detect, correct, and adapt in a single solution

THE SECOND ECONOMY



Dynamic Endpoint Platform



Threat Intelligence	Block Known Bad	Allow Known Good
Behavior Detection	Exploit Detection	Contain Spread
Proactive Monitoring	Search and Hunt	Remediate and Adapt

다이나믹 엔드 포인트 확장

통합된 엔드 포인트 위협 방어 및 대응

THE SECOND ECONOMY

Dynamic Endpoint Platform

Threat Prevention | Firewall | Web Control

NEW **Adaptive Protection**

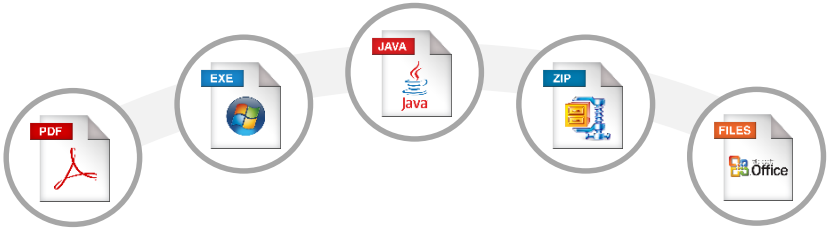
NEW **Active Response**

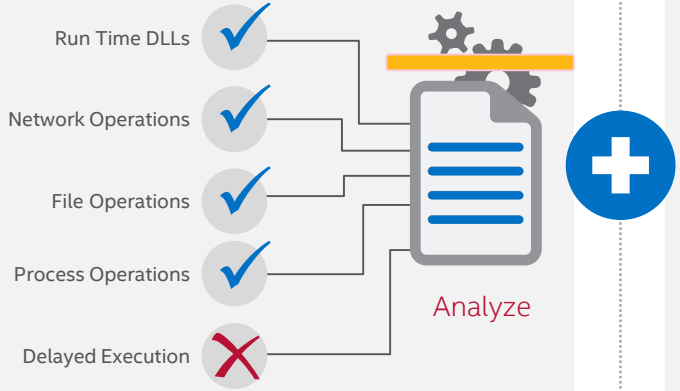
최적화 된 성능으로 광범위한 위협 보호

행동 머쉰러닝 및 응용 프로그램 봉쇄

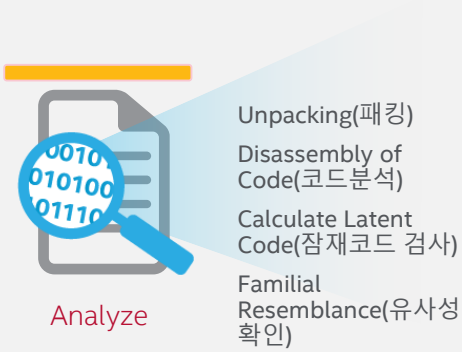
사전에 찾지 못한 것을 찾아 조사하고 교정

Dynamic and Static Code Analysis On ATD(Sandbox)





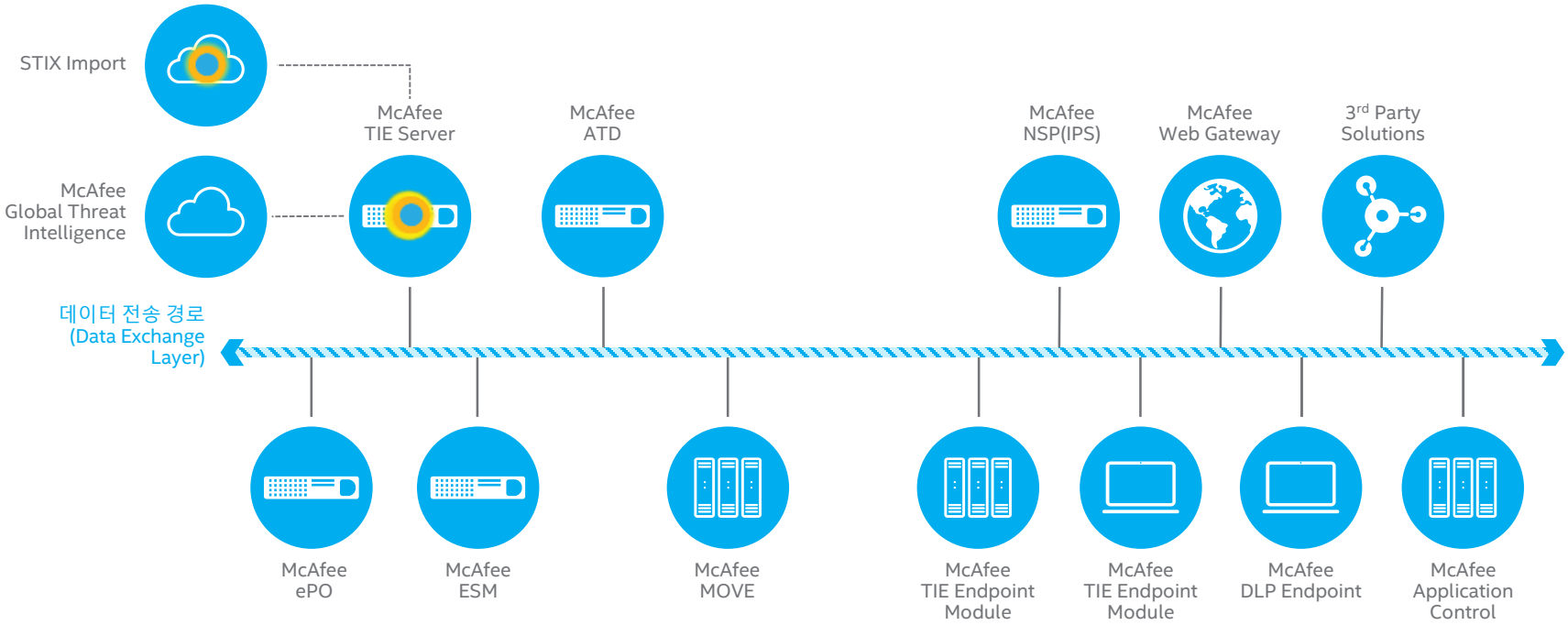
동적분석/Dynamic Analysis



정적분석/Static Code Analysis

Operationalizing Threat Intelligence

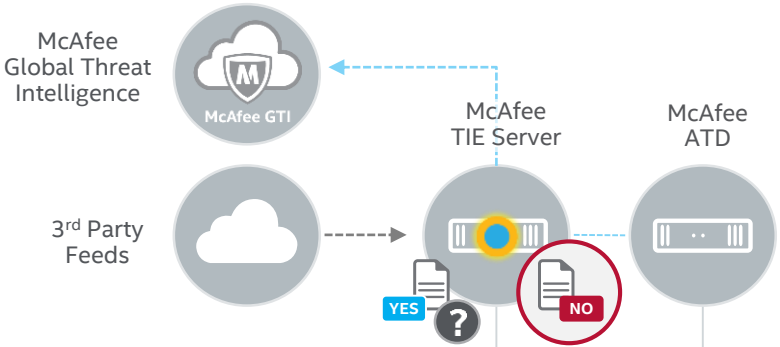
THE SECOND ECONOMY



intel Security

McAfee Dynamic Endpoint Threat Defense

적용과 면역—밀리초 단위를 상대를 봉쇄

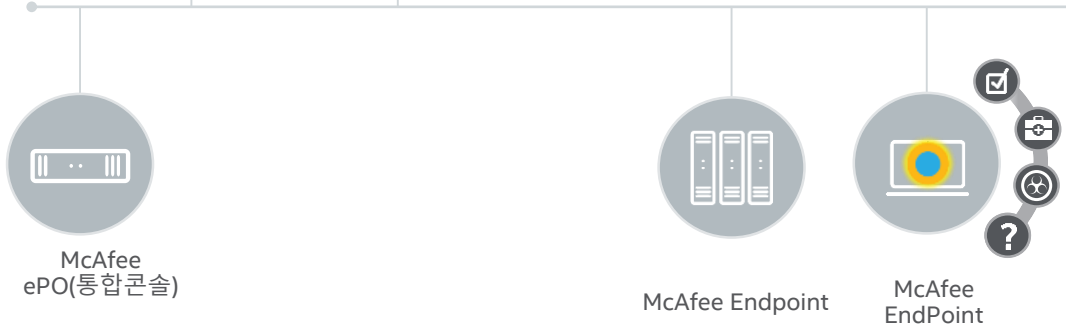


적응형 보안으로 악성코드 방지 보호 기능을 향상

- Gary 파일에 대한 더 나은 분석
- 클라우드로 부터 자신의 환경에서 평판을 업데이트
- 부서/시스템 유형에 걸쳐 위험 관리

실용적인 정보 – Actionable intelligence

- 공격의 시작될때 처음 발견 플래그에 대한 조기 인식
- 누군가 시스템을 침해 했을 경우 파일 평판이 변경

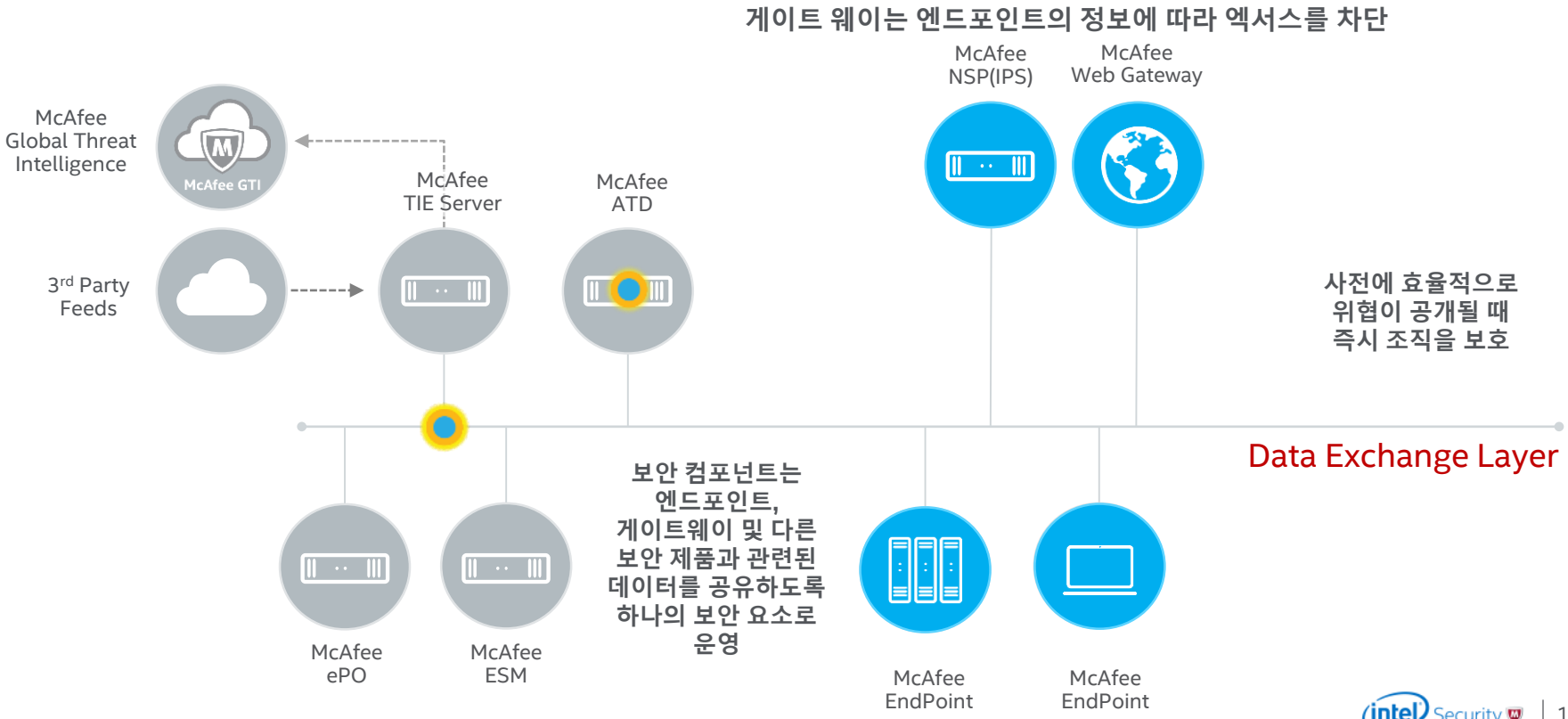


데이터전송경로

(Data Exchange Layer)

McAfee Dynamic Endpoint Threat Defense

Instant protection across the enterprise



지능형 엔드 포인트 보호

THE SECOND ECONOMY

Endpoint Protection

McAfee® Endpoint Security 10

Web Protection

McAfee Web Gateway (via McAfee Client Proxy Agent)

Threat Intelligence

McAfee Threat Intelligence Exchange

Advanced Malware Detection

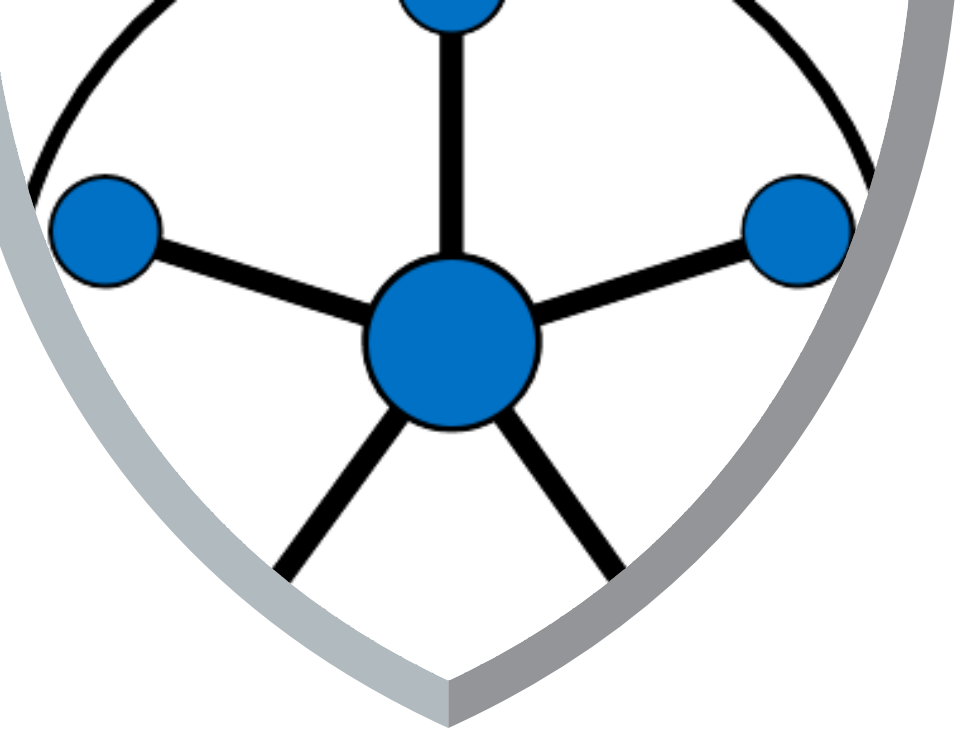
McAfee Advanced Threat Defense

Endpoint Detection and Response (EDR)

McAfee Active Response

Management Platform

McAfee® ePolicy Orchestrator® (McAfee ePO™)



THE SECOND ECONOMY

Adaptive Threat Protection

Dynamic Application Containment (DAC)

THE SECOND ECONOMY

- 시스템에 악의적인 변경을 가하기위한 그레이웨어의 기능 감소
- “Patient zero”저장 하고 확산을 방지
- 무거운 샌드 박스 / VM 또는 앱 가상화를 사용하거나 필요로하지 않기 때문에 최종 사용자의 영향을 최소화
- Online 또는 offline 에서 작업
- 비즈니스 연속성을 손상시키지 않으면서 보호

Containment(봉쇄) = 엔드포인트 탐지 분석을 실행하는 동안 Gray ware가 엔드포인트를 변경하는 기능을 제한하거나 제거합니다.

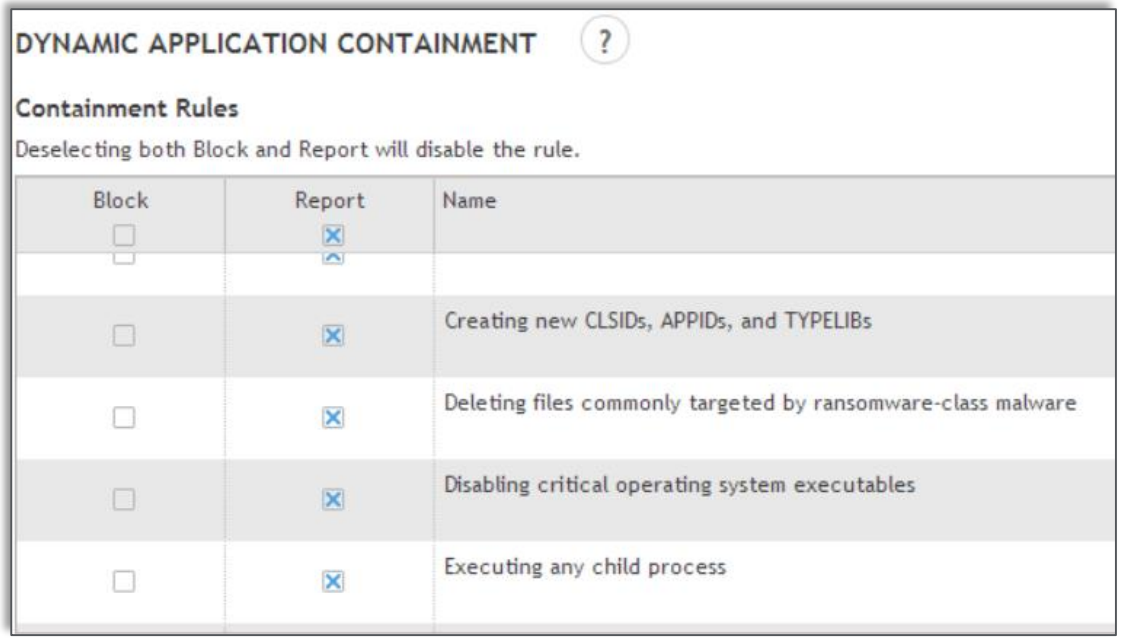
“The Grey”: Containment Rules

가장 널리 퍼진 악의적인 제로 데이 행위에 대한 50+ 차단 규칙

THE SECOND ECONOMY

Specific Ransomware

- 일반적으로 타겟팅 된 파일 읽기
- 사용자 데이터 폴더 수정하기
- 일반적으로 타겟팅 된 파일 삭제하기
- 중요한 Windows 파일 수정



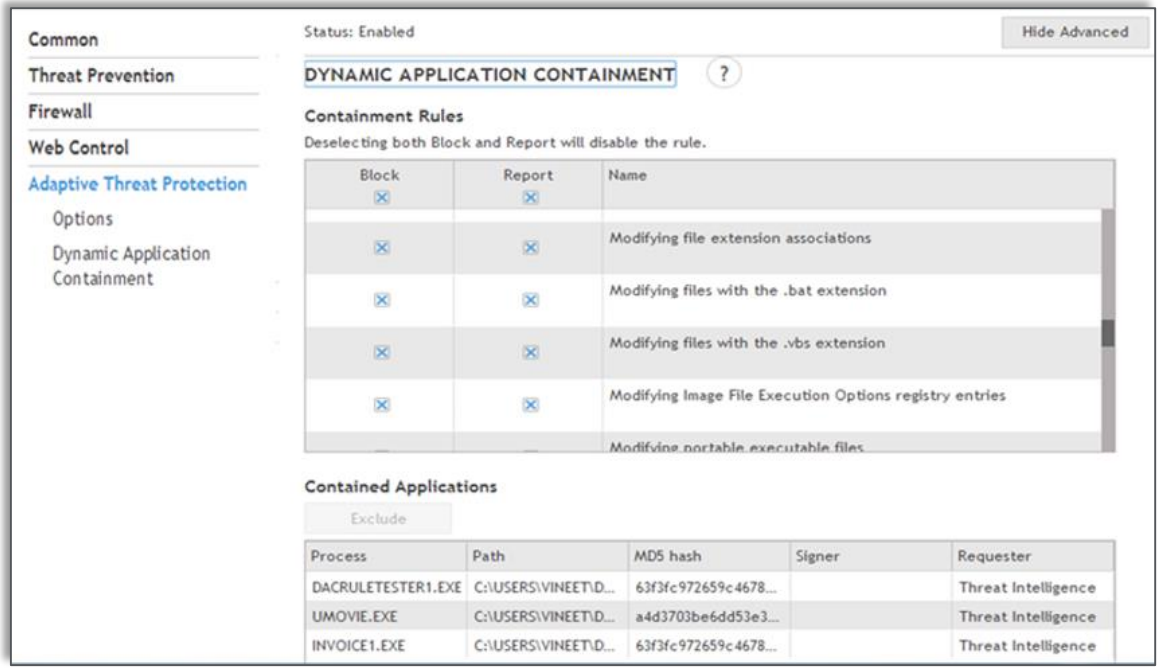
“The Grey”: Containment Rules

THE SECOND ECONOMY

Containment watches only the suspicious grey application

What is contained

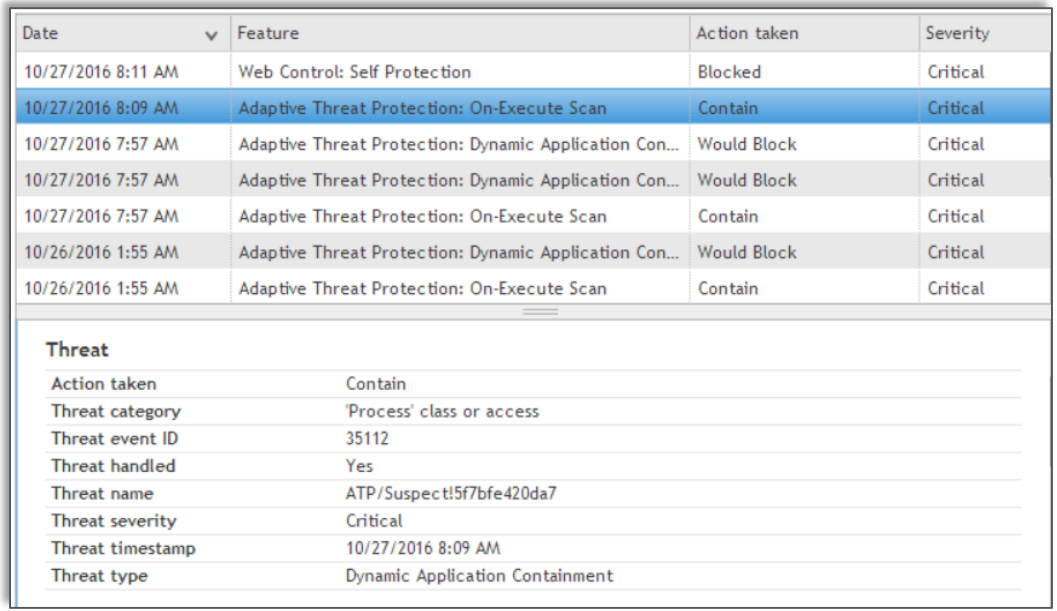
- Process
- Path
- MD5 hash



“The Grey”: Threat Intelligence

추가 조사를 위해 응용 프로그램 동작에 대한 인텔리전스 제공

THE SECOND ECONOMY



Date	Feature	Action taken	Severity
10/27/2016 8:11 AM	Web Control: Self Protection	Blocked	Critical
10/27/2016 8:09 AM	Adaptive Threat Protection: On-Execute Scan	Contain	Critical
10/27/2016 7:57 AM	Adaptive Threat Protection: Dynamic Application Con...	Would Block	Critical
10/27/2016 7:57 AM	Adaptive Threat Protection: Dynamic Application Con...	Would Block	Critical
10/27/2016 7:57 AM	Adaptive Threat Protection: On-Execute Scan	Contain	Critical
10/26/2016 1:55 AM	Adaptive Threat Protection: Dynamic Application Con...	Would Block	Critical
10/26/2016 1:55 AM	Adaptive Threat Protection: On-Execute Scan	Contain	Critical

Threat

Action taken	Contain
Threat category	'Process' class or access
Threat event ID	35112
Threat handled	Yes
Threat name	ATP/Suspect!5f7bfe420da7
Threat severity	Critical
Threat timestamp	10/27/2016 8:09 AM
Threat type	Dynamic Application Containment

Actionable, real-time logs

- 공격 소스 및 목적지에 대한 자세한 내용.
- 인텔리젼스를 이해하기 쉬운 언어로 설명

What Types of Threat Forensics are Available?

Machine

- Host Name
- Ipv6 Address
- Ipv4 Address
- Mac
- Location

Target

- Ipv4 Address
- Ipv6 Address
- Port
- URL
- Share Name
- Mac
- Protocol
- User Name
- Process Name
- Hash
- Signed
- Signer
- Description
- Parent Process Signed
- Parent Process Signer
- Name
- Path
- File Size
- Modify Time
- Access Time
- Create Time
- Device Display Name
- Serial Number
- Device VID
- Device PID

Source

- Ipv4 Address
- Ipv6 Address
- Port
- URL
- Share Name
- Mac
- User Name
- Process Name
- Parent Process Name
- Parent Process Hash
- Parent Process Signed
- Parent Process Signer
- File Path
- File Size
- Hash
- Signed
- Signer
- Modify Time
- Access Time
- Create Time
- Device Serial Number
- Device VID
- Source Description

Additional

- Cleanable
- Task Name
- API Name
- First Attempted Action
- Second Attempted Action
- First Action Status
- Second Action Status
- Event ID Description
- Natural Language Description
- Duration Before Detection
- Attack Vector Type
- Direction
- ICMP Type
- Firewall Event Type
- Throttled Event Count

Detection Feature

- Name
- Version
- Content Version
- Content Creation Date
- Rule ID
- Rule Name
- Reg Info
- GTI Query
- Name

Threat Data

- Event ID
- Severity
- Name
- Type
- Action Taken
- Handled
- Detected On Create
- Impact
- Event ID

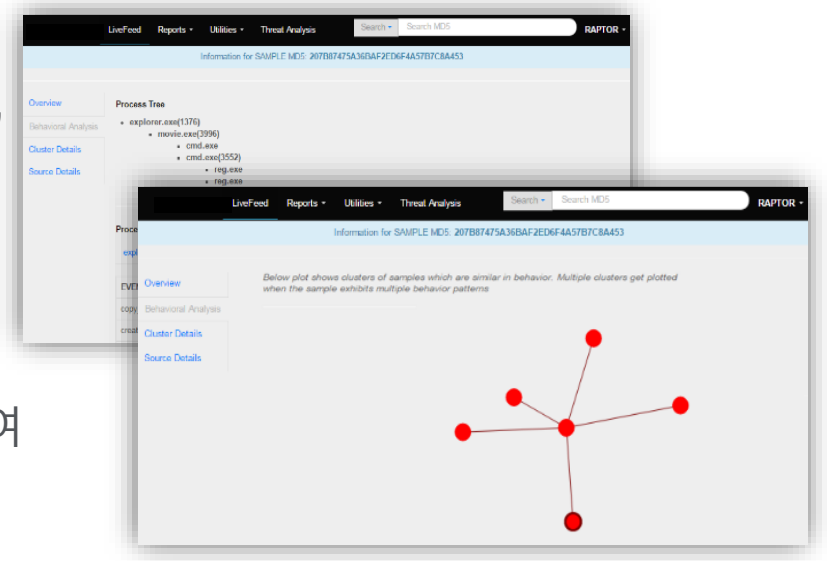
Detect, understand, and track the attack

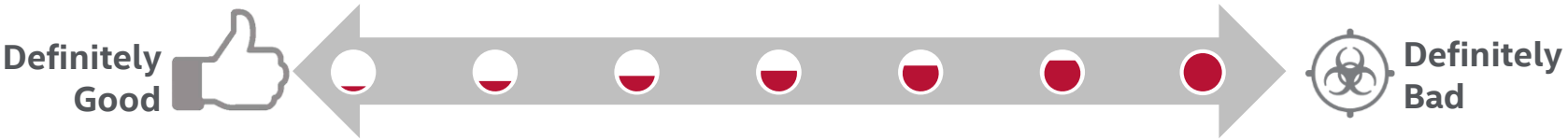
Real Protect

THE SECOND ECONOMY

Signatures 없는 악성파일을 탐지

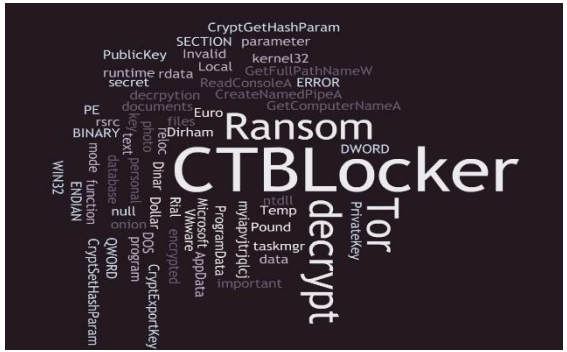
- 동작을 캡처하기 위해 실시간으로 추적 실행 (파일, 레지스트리, 네트워크 통신)
- Dynamic 과 static data 를 모두 캡쳐
- Machine learning 분석
- 분류할 Data analytics in cloud 를 사용
- 엔드 포인트에서 로컬 시스템 학습 모델을 사용하여 온라인 및 오프라인으로 작업





Real Protect: 더 많은 것을 방지

THE SECOND ECONOMY



우리가 생각할 수 있는 것은...

Ransomware: CTB-Locker
(pre-execution)

분류는 엔드 포인트에서 오프라인 머신러닝 모델에 대해 수행

"실제로" 무엇을하는지

Ransomware: CTB-Locker
(post-execution)

파일 시스템, 레지스트리 및 네트워크 변경 작업으로 파일 암호화 시작

- **Generates** a unique computer identifier
- **Surviving** reboot by moving itself into Appdata folder
- **Deactivate**: Shadow copies, Startup repair, Windows error recovery
- **Stops**: Windows Security Center, Defender, Update Service, Error reporting and BITS
- **Inject:** into explorer.exe, svchost.exe
- **Retrieve:** Externel IP-address
- **Starts encryption process**

“The Grey”: 간단한 룰

THE SECOND ECONOMY

Rule Assignment

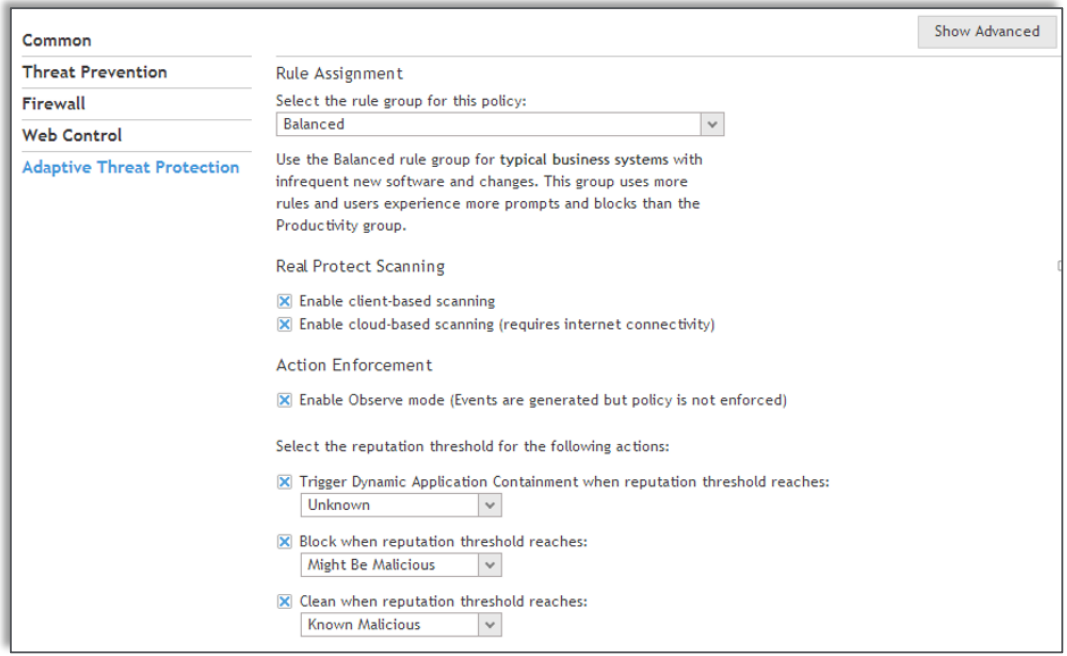
- Balanced
- Productivity
- Security

Behavior Scanning

- Static, pre-execution
- Dynamic, post-execution

Action Enforcement

- Block
- Clean

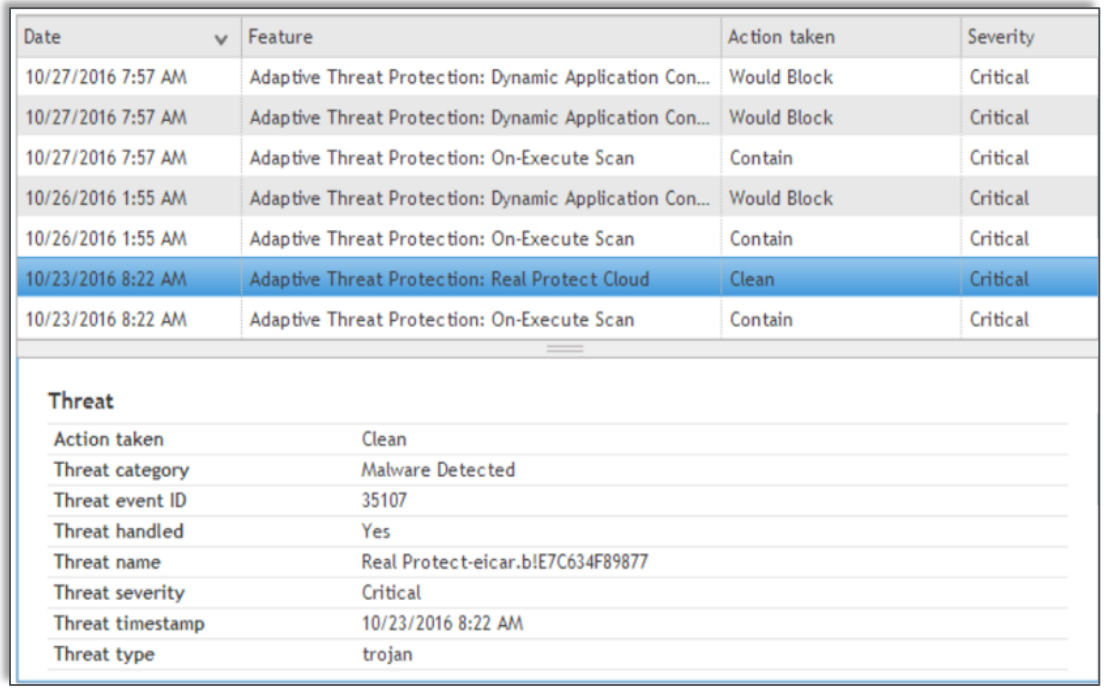


“The Grey”: 행위 인텔리젼스

실행 가능한 실시간 위협 로그

THE SECOND ECONOMY

- 공격 소스 및 목적지에 대한 자세한 내용
- 이해하기 쉬운 언어로 설명 된 실행 가능한 인텔리젼스를 제공



Date	Feature	Action taken	Severity
10/27/2016 7:57 AM	Adaptive Threat Protection: Dynamic Application Con...	Would Block	Critical
10/27/2016 7:57 AM	Adaptive Threat Protection: Dynamic Application Con...	Would Block	Critical
10/27/2016 7:57 AM	Adaptive Threat Protection: On-Execute Scan	Contain	Critical
10/26/2016 1:55 AM	Adaptive Threat Protection: Dynamic Application Con...	Would Block	Critical
10/26/2016 1:55 AM	Adaptive Threat Protection: On-Execute Scan	Contain	Critical
10/23/2016 8:22 AM	Adaptive Threat Protection: Real Protect Cloud	Clean	Critical
10/23/2016 8:22 AM	Adaptive Threat Protection: On-Execute Scan	Contain	Critical

Threat

Action taken	Clean
Threat category	Malware Detected
Threat event ID	35107
Threat handled	Yes
Threat name	Real Protect-eicar.b!E7C634F89877
Threat severity	Critical
Threat timestamp	10/23/2016 8:22 AM
Threat type	trojan

Adaptive Protection In Action

행위 보호로 모든 엔드 포인트를 자동으로 즉시 보호합니다.

THE SECOND ECONOMY

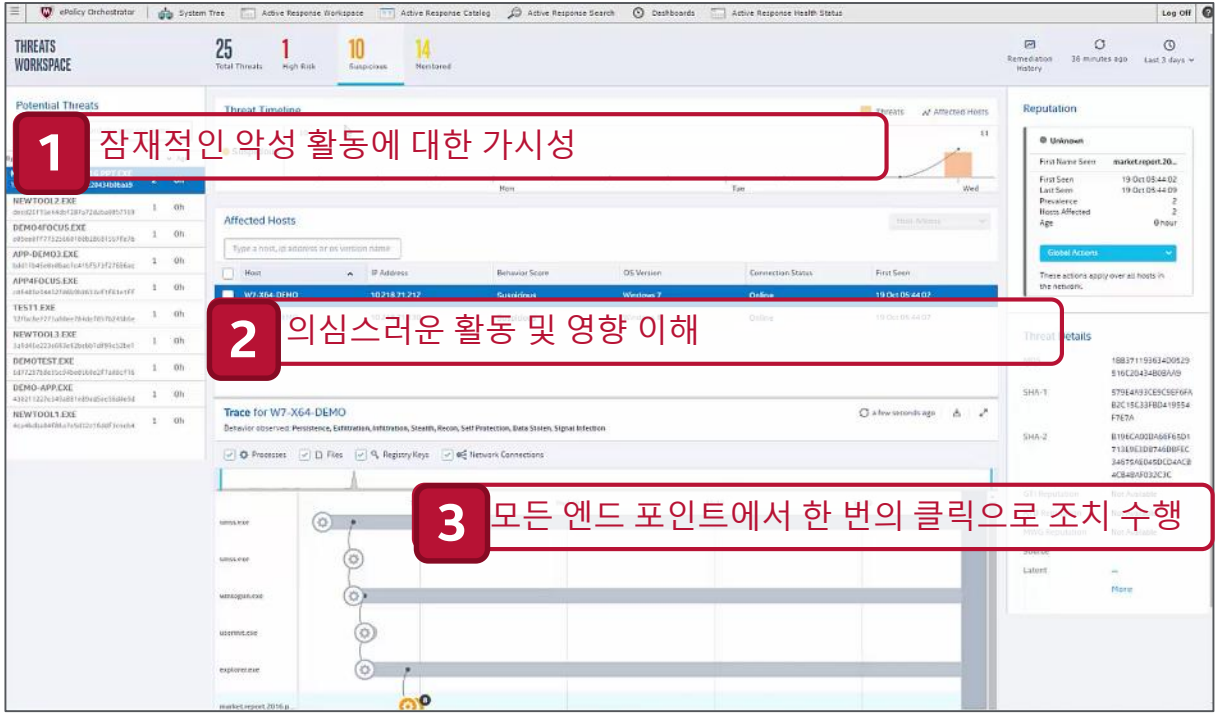
THE SECOND ECONOMY

Active Response: Easier and Faster

Introducing McAfee® Active Response 2.0

수일 또는 수주가 아닌 몇 초 내에 찾기, 조사 및 응답

THE SECOND ECONOMY



- McAfee® ePO™
- 단일 화면
- 워크플로우
- “unknowns” 확인
- 자세한 조사
- 원클릭 액션

Requires McAfee Active Response Cloud Services

위협 인텔리젼스로 시작

위협이 과거의 보호 수단이라고 생각하면 많은 것을 배울수 있다.

THE SECOND ECONOMY

- 알 수없는 앱이거나 신뢰할 수있는 앱의 비정상적인 동작
- 알려진 행위나 익스플로잇 필터와 일치하지 않음
- 정적 분석을 피하기 위해 행위를 은닉
- 머쉰러닝 알고리즘에서 벗어남
- 샌드박스 분석을 우회
- 엔드포인트를 벗어나는 동작이 있을 수 있음

보호 지식(The protection knowledge informs)은
우리가 무엇을 적극적으로 지켜야하는지 알려....

Demo: Advanced Exfiltration Attempt

공격을 더 빨리 찾아 내고 멈추는 법

THE SECOND ECONOMY

Nate
CISO

민감한 데이터가 공격
대상이 될 수 있다는 의심!!!!

Hector
Security Analyst

위협을 발견, 조사 및
해결하는 임무가 부여됨

SCENARIO

정교한 표적공격
엔드포인트 통한
기업의 파일을 타겟
유출시도

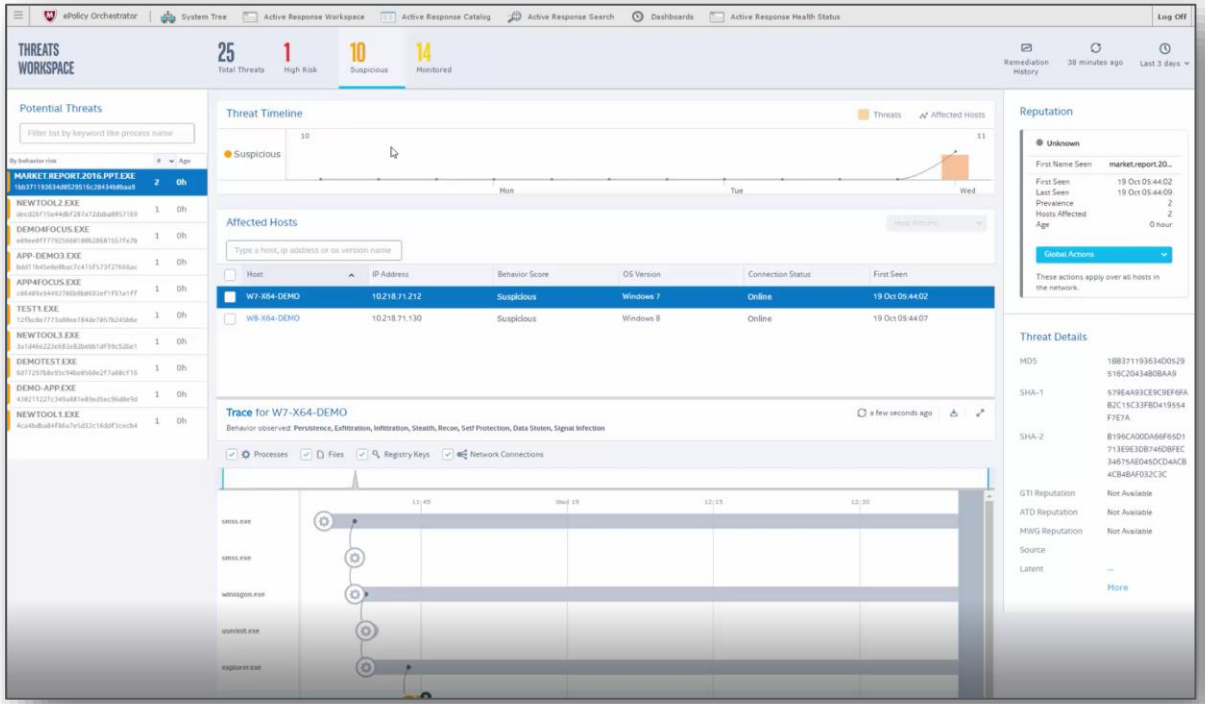
1. Are We Under Attack?

THE SECOND ECONOMY

- 지난 24 시간 동안의 위험 및 고위험군은 무엇입니까?
- 엔드 포인트에서 위험이 높은 항목이 있습니까?
- 침해사고지표(Indicator of Compromise)를 찾을 수 있습니까?

1.Demo: 위협 찾기

THE SECOND ECONOMY



- Filter by behavior risk
- View, filter, or search
- Sort by prevalence / age
- Select to investigate

2. What Has Happened?

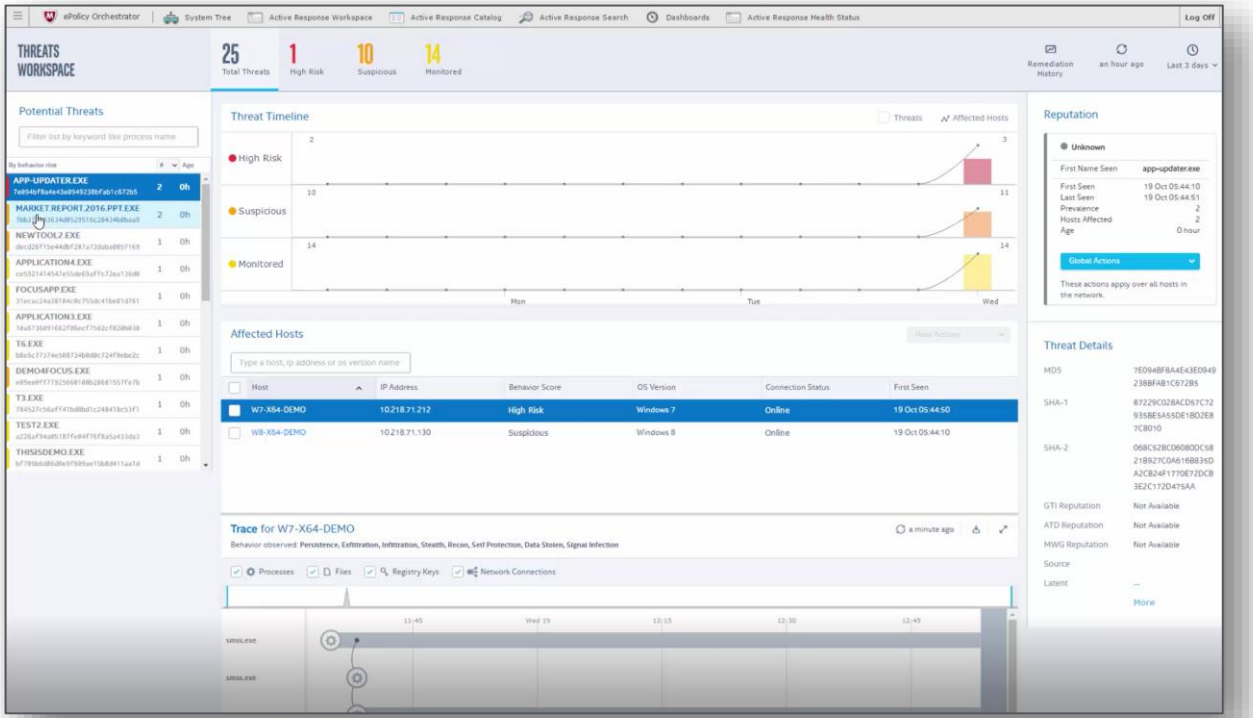
THE SECOND ECONOMY

- 우리는 이미 어떤 위협 정보를 가지고 있습니까?
- 어떤 엔드 포인트를 처음 보았고 최악의 행위을 보였습니까?
- 엔드 포인트에서 어떤 위험한 행동을 실행합니까?
- 우리가 다른 곳에서 본 것을 검색 할 수 있습니까?

2.Demo: 위협 조사

THE SECOND ECONOMY

- Threat intelligence
- Endpoint analytics cloud service
  - Unknown processes
  - Process relationships
  - Commonly abused apps
  - File, registry, & IP events
  - Login/logout events
- Live search across all endpoints in seconds



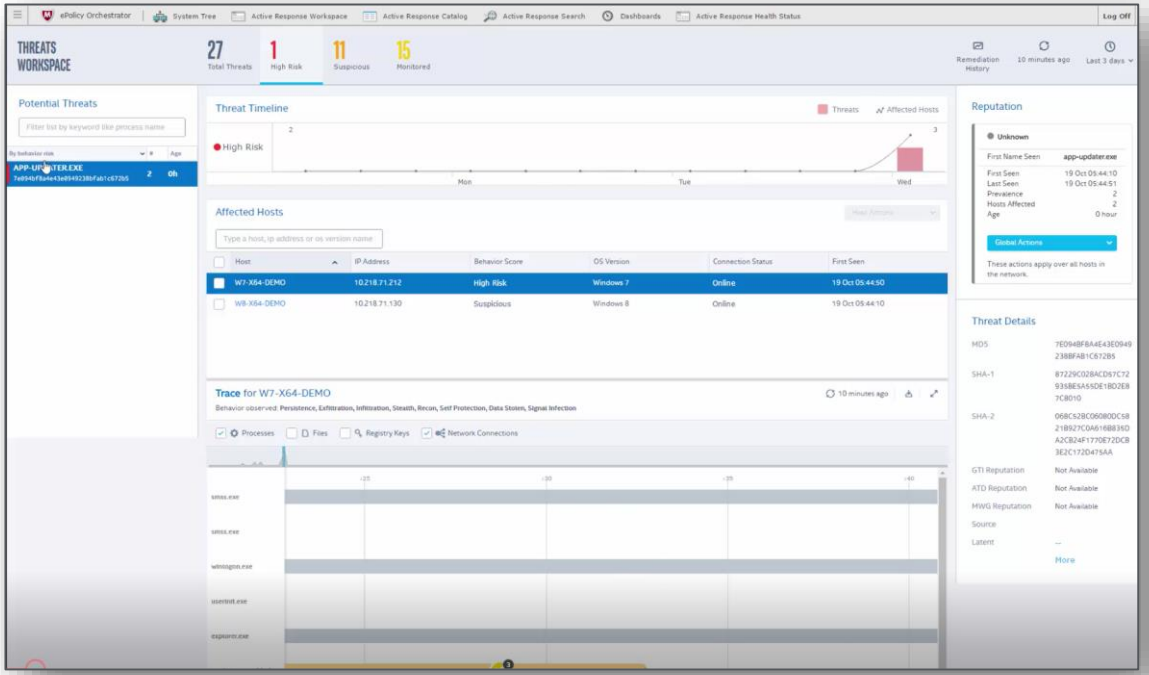
3. How Can We Stop an Attack?

THE SECOND ECONOMY

- 어떤 옵션을 사용하여 공격을 중단하고 정리해야합니까?
- 공격을 종료하는 데 시간이 얼마나 걸리나요?
- 보호를 업데이트하기 위해 우리가해야 할 일은 무엇입니까?

3.Demo: 액션 실행

THE SECOND ECONOMY



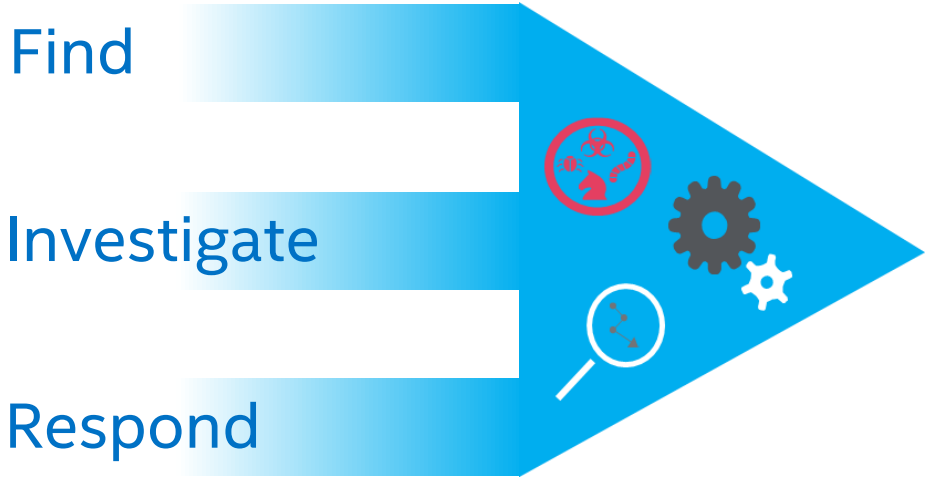
Action at Three Levels

1. Investigating Action
   - Delete files, kill processes
2. Endpoint Action
   - Kill & cleanup
3. Global Action
   - Kill & cleanup everywhere
   - Adapt protection everywhere

신속한 대응으로 위험 감소

알려지지 않은 것을 발견하고 모든 곳에서 신속하게 해결할 수있는 컨텍스트를 제공

THE SECOND ECONOMY



Reducing Risk Faster with Integrated Threat Defense

McAfee® Active Response
1 Screen, 3 Clicks
Correct and Adapt Protection

Vendor A: 5 Screen Changes, 13 Clicks
Vendor B: 4 Screen Changes, 9 Clicks
Vendor C: 3 Screen Changes, 5 Clicks

THE SECOND ECONOMY

Summary

차세대 엔드포인트 위협방어와 대응

THE SECOND ECONOMY

McAfee
엔드포인트 APT

+

McAfee
엔드포인트 EDR

APT 공격을 지연시키고 차단

APT 공격을 사전에 찾고 교정

APT 공격에 대한 엔드포인트 보안을 확장하는 New Add-on Suite!!!

✓ *McAfee Dynamic Endpoint Threat Defense and Response* adds on

✓ Adaptive Protection,

✓ Threat Intelligence Exchange,

✓ Advanced Threat Defense(SandBox)

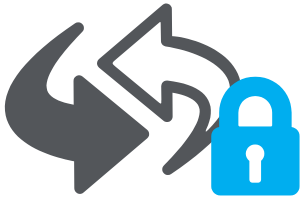
✓ Active Response(EDR)

Conclusion: McAfee Active Response

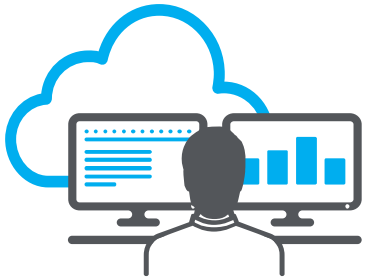
THE SECOND ECONOMY

1. 잠재적 위협을 사전에 파악
2. 심층적인 위협 조사
3. "한 번의 클릭"으로 위협을 중지하고 보호

Resolve more threats ...



... faster ...



... with fewer resources.