PROTECTION BEYOND THE OS

ReaQta 제품소개서

REAQTA

BellI&S
Bell Information&Solutions

목 차

1. 회사소개

- 일반현황 및 연혁
- 2014년에 설립된 Next generation Cyber Attack Protection 보안솔루션의 회사로 RSA에서 신기술로 인정한 보안솔루션 전문기업으로 최신의 엔드포인트 APT솔루션을 선도하는 기업입니다.

회사개요

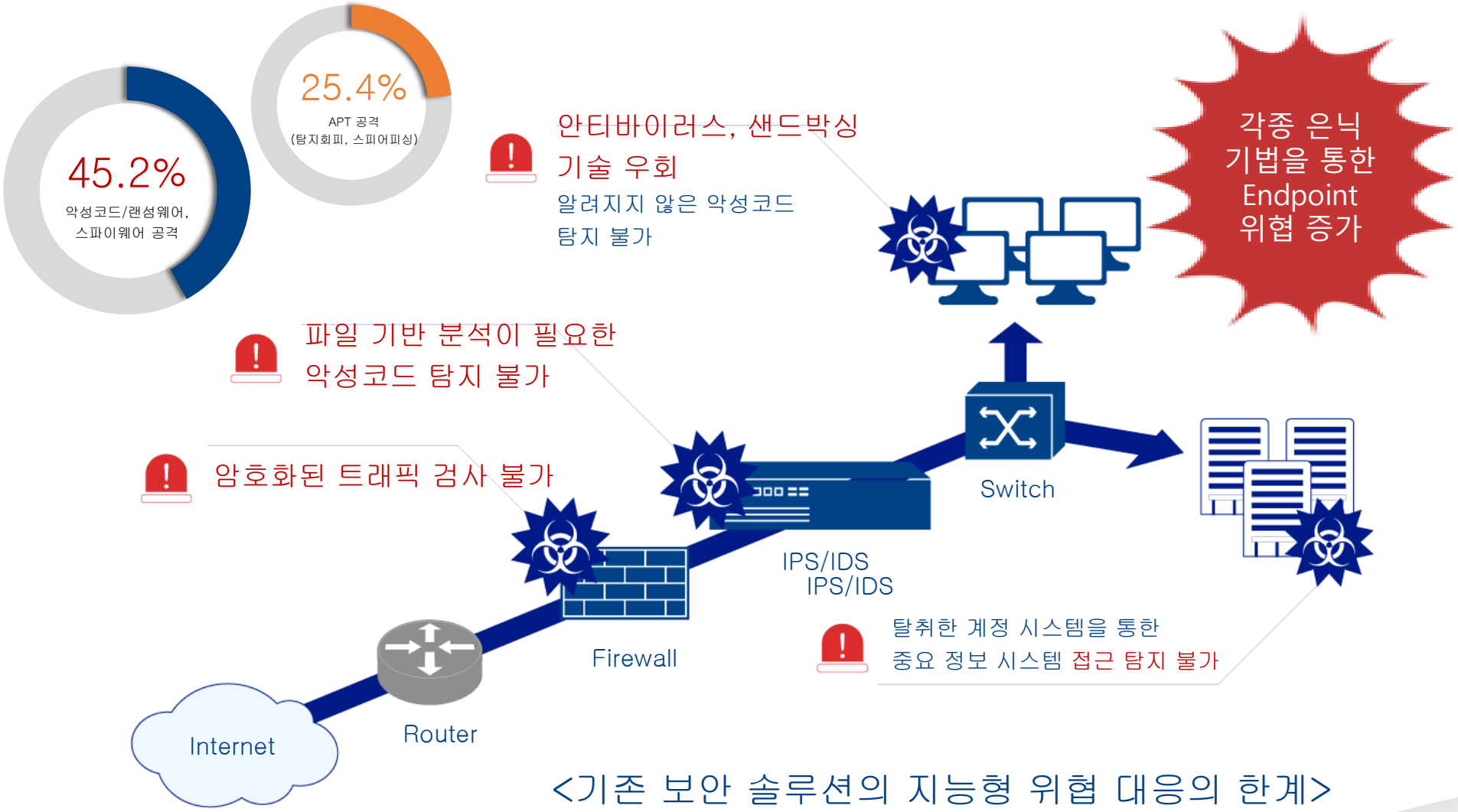
회 사 명	**리쿼타 주식회사 (ReaQta Co., Ltd.)**
설 립 년 도	2014년 01월
대 표 이 사	**Alberto Pelliccione**
주요 솔루션	**1. ReaQta Core** ▪ ReaQta-core ▪ ReaQta-aggregator ▪ ReaQta-brain **2. ReaQta Core with two Option** ▪ ReaQta-core ▪ ReaQta-aggregator ▪ ReaQta-brain ➢ two option ▪ ReaQta-Investigator ▪ ReaQta-Live Threat Analysis

1. 제품 요약

- 제품명 : REAQTA Core
- 제품개요 : 차세대 **EPP** APT솔루션
  - 신종 APT공격, **랜섬웨어 및 멀웨어공격**, 제로데이 취약점공격 등에 대한 효과적인 방어개념의 엔터프라이즈 프로텍트 보안솔루션 (EPP : Enterprise Protect Platform)
  - CPU기반의 행위탐지 보안솔루션
  - 익스플로잇(탈취)차단, 멜웨어(랜섬웨어)방어, 데이타보호, 인공지능 AI분석 등의 다단계층의 차단시스템 기능
- 제품 특장점
  - 익스플로잇(탈취)시도를 방어하기 위해 모든 어플리케이션 및 서버의 실행내용을 실시간 검사
  - 탈취 시도가 발견되면 공격중인 익스플로잇은 즉시 차단되고 대시보드에 보고
  - 어플리케이션의 정상적인 OS외부에 위치하면서 프로세스의 상호작용을 감사, 탐지 및 차단
  - 흐름의 변경하려는 모든 형대의 멀웨어 활동 방어 및 개인정보 탈취나 보호되어야 할 리소스 접근제어
  - 민감한 데이터에 접근을 요하는 어플리케이션들을 제한 할 수 있음
  - 멀웨어 및 렌섬웨어 공격에 보호가 필요한 중요데이터 및 클라이언트에 대한 보안정책 설정
  - **인공지능 AI엔진을 통한 행위기반 모델링 및 전체 인프라구조를 모델링**하고 변종을 탐지하고 시스템운영자에게 Alert 기능 통보
- 기대효과
  - **멀웨어 및 렌섬웨어 등의 지능형공격(APT)에 대한 사내중요 데이터 보호, 신속한 침해대응 및 확산방지**

1. 제품 소개 지능형 위협의 증가

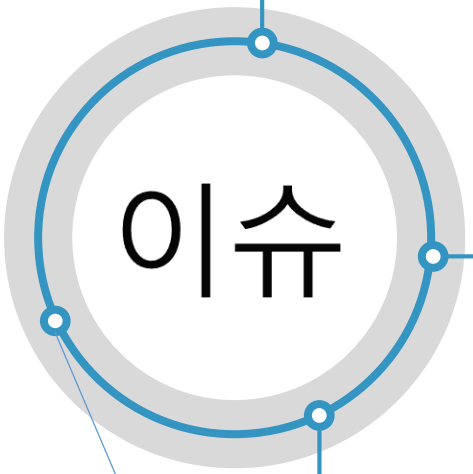
멀웨어 및 렌섬웨어 등의 지능협 위협 (Advanced Persistent Threat) 및 고도화된 공격



<기존 보안 솔루션의 지능형 위협 대응의 한계>

1. 제품 소개 기존 솔루션들의 문제점

기존 보안 솔루션은 신종 APT 공격, 랜섬웨어, 제로데이 취약점 공격 등에 한계를 보임



대다수의 안티바이러스 솔루션은 시그니처 기반으로 운영

✓ 새로운 공격 패턴에 대한 효과적인 대응 방안 필요

가상환경에서의 멀웨어를 분석하는 샌드박스 기술 유행

✓ 해커들은 신종 멀웨어를 개발하여 샌드박스의 기능을 무력화함

점점 무기력해지는 네트워크 감시 (Network Monitor)

✓ 암호화 구조에 대한 검사 및 의심 데이터 구분 불가

보안 전문가들을 위한 정규 데이터의 안정성 최대한 보장 필요

✓ 공격 감지는 사이버 공격 후 평균 8개월 후에나 가능

CPU기반의 지능형 행위 탐지 EPP 보안 솔루션

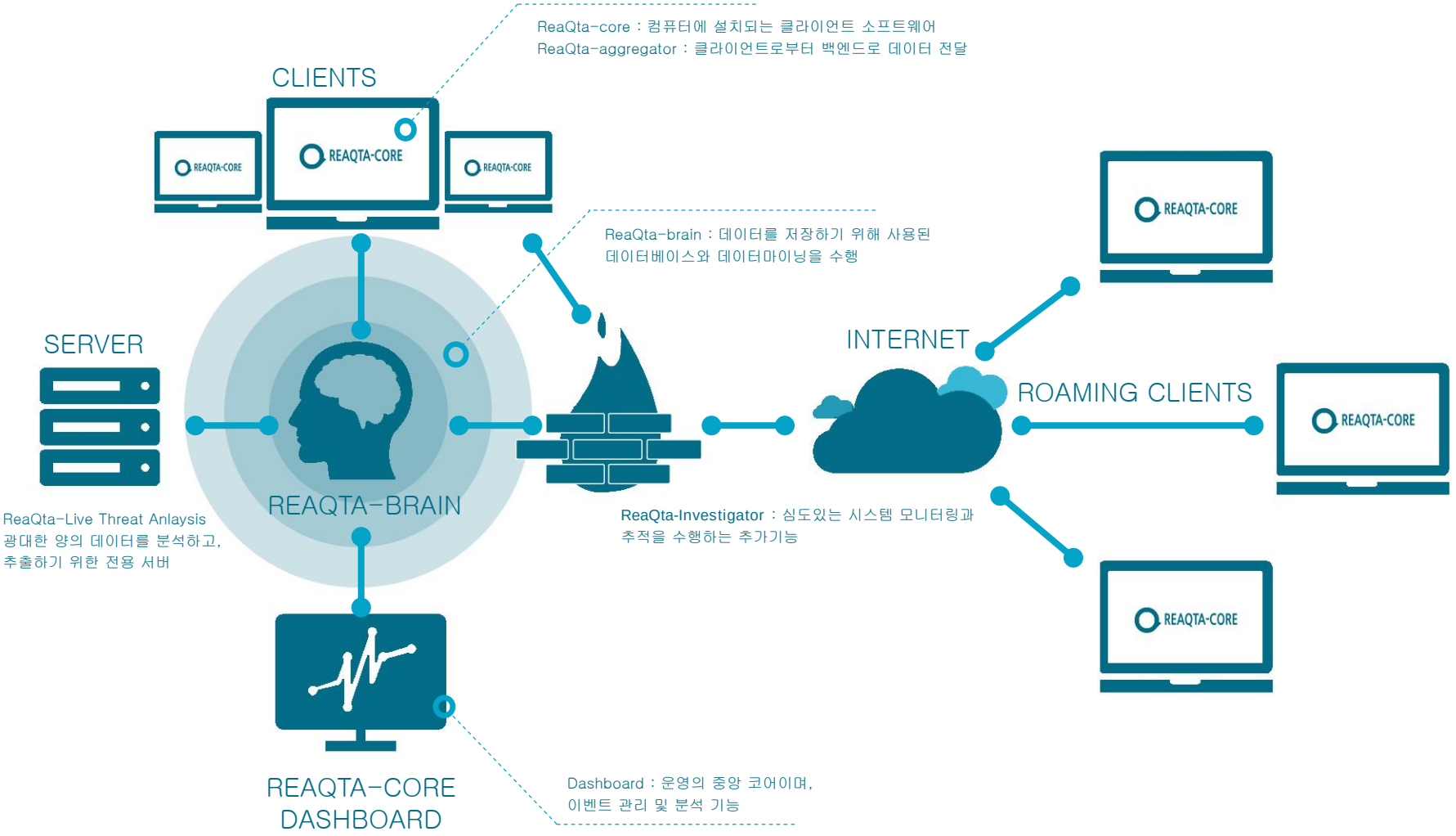
차세대 위협 대응을 위한 최적의 솔루션

- ✓ 멀웨어 및 렌섬웨어로부터 클라이언트 완벽 보안
- ✓ 행위 탐지 기반 EPP 보호 솔루션
- ✓ OS 외부에서 동작 (Beyond OS)

➢ **REAQTA는 OS로부터 하드웨어에 접근하기 위한 유일한 접근 통로**

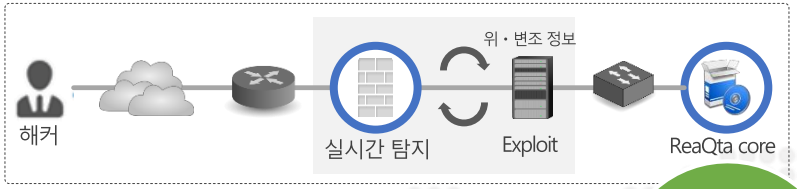
2. 제품 구성

CPU기반의 지능형 행위 탐지 EPP 보안 솔루션



3. 제품 주요 기능

익스플로잇(Exploits) 실시간 탐지 기능



✓ ReaQta는 현재의 모든 알려진 익스플로잇 기술들 (스택 오버플로우, ROP 체인, heap spray)을 탐지할 수 있는 실시간 컨트롤 플로우 엔진 채택

Layer 1
Exploit

멀웨어 및 렌섬웨어 탐지 기능

✓ 모든 어플리케이션은 작동되는 모든 기간 동안 검사되고, 악의적인 활동의 징후가 보이면 즉시 차단하고, 모든 프로세스 상호작용을 무력화함

Layer 2
MALWARE

REAQTA-CORE
A.I.

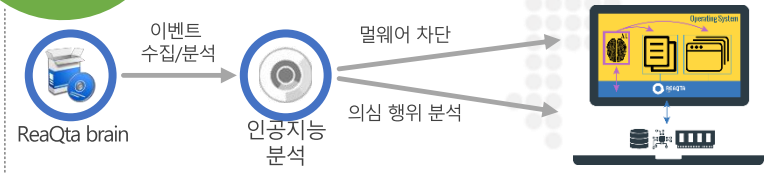
✓ 모든 자원에 대한 접근을 감시하고, 사용된 암호화에도 관계 없이, 모든 형태의 접근에 대한 포괄적인 제어 가능

Layer 3
EXFILTRATION

데이터 유출(Data Exfiltration) 차단 기능

✓ ReaQta 인공지능 엔진은 클라이언트로부터 보내어진 데이터를 학습하여 끊임없이 진화하는 환경에 엔진을 최적화함

Layer 4
인공지능 A.I

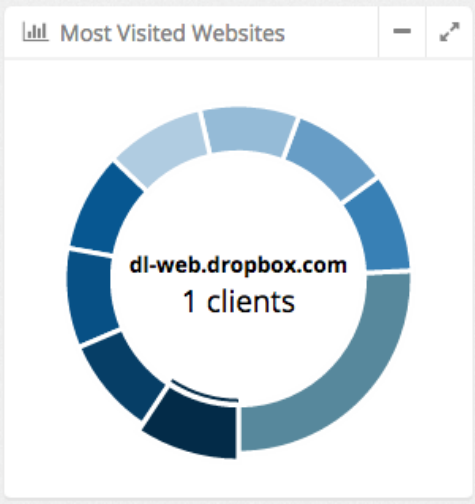


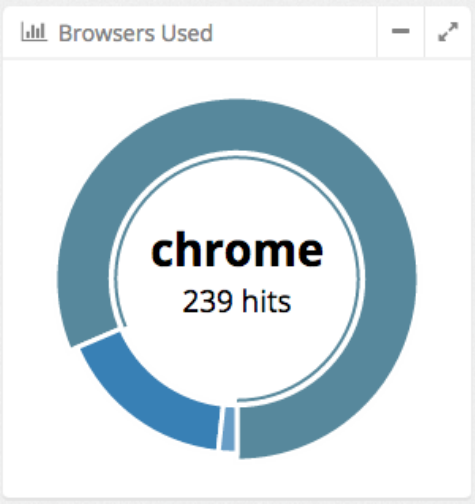
지능형 행위 탐지 기능 (인공지능 A.I)

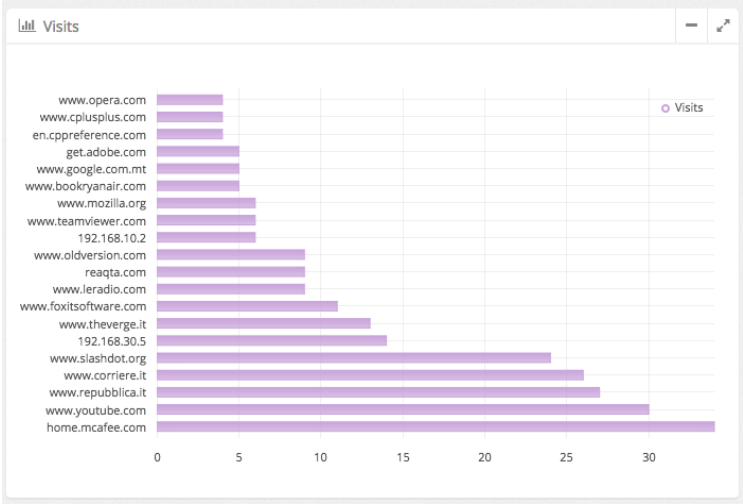
4. 제품 특장점 – 클라이언트 자료 수집

➢ 클라이언트 자료 수집 (Client Profiling)

- ReaQta-core는 User/PC(로)부터 권한을 부여 받은 강력한 차단 시스템.
- 디바이스의 사용에 관한 정확한 정보를 획득할 수 있으며, 이를 통한 정확한 사건 재구성과 추적 용이.







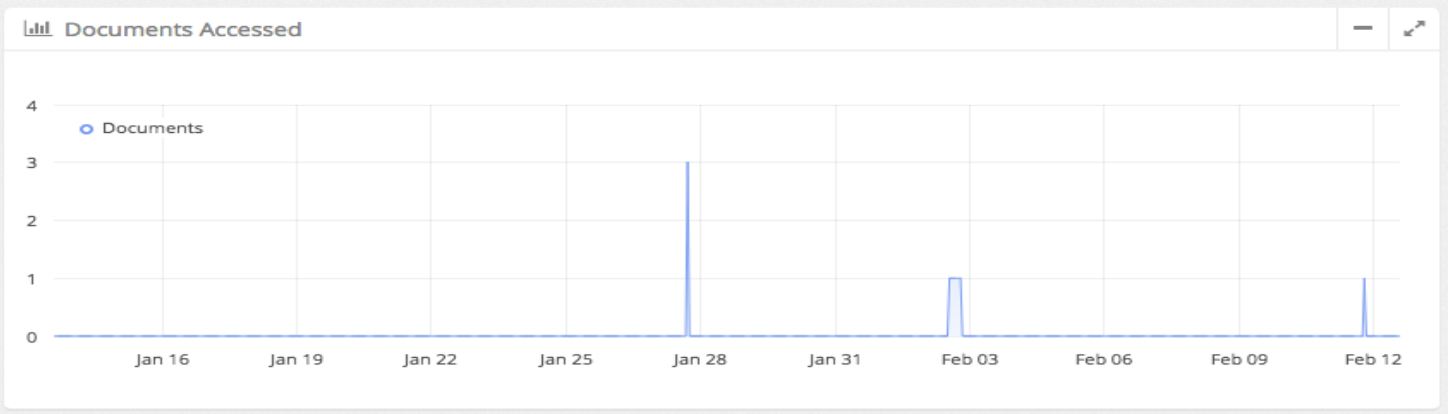
Visited URLs

Date	Device	User	Browser	URL
2015/02/11 14:46:28 +0100	WIN-9FMAJPAEU1C	User	firefox	https://www.mozilla.org/en-US/firefox/35.0.1/firstrun/
2015/02/11 14:43:37 +0100	WIN-O4ME0VJNJU7	W8TestRQT	chrome	http://home.mcafee.com/root/campaign.aspx?cid=83831
2015/02/11 14:43:16 +0100	WIN-9FMAJPAEU1C	User	firefox	https://www.mozilla.org/en-US/firefox/35.0.1/firstrun/
2015/02/11 14:40:05 +0100	WIN-9FMAJPAEU1C	User	firefox	https://www.mozilla.org/en-US/firefox/35.0.1/firstrun/

4. 제품 특장점 – 문서 접근

➢ 문서 접근 제어 (Documents Access)

- ReaQta-core는 사용자에 의해 접근된 문서를 모니터링하고, 민감한 리소스에 대한 추적 기능 제공
- 악의적인 공격이 가능한 소스에 대한 정보 제공



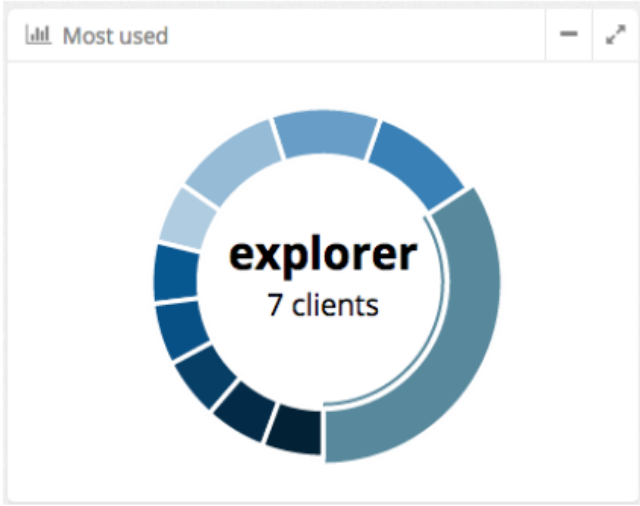
Documents

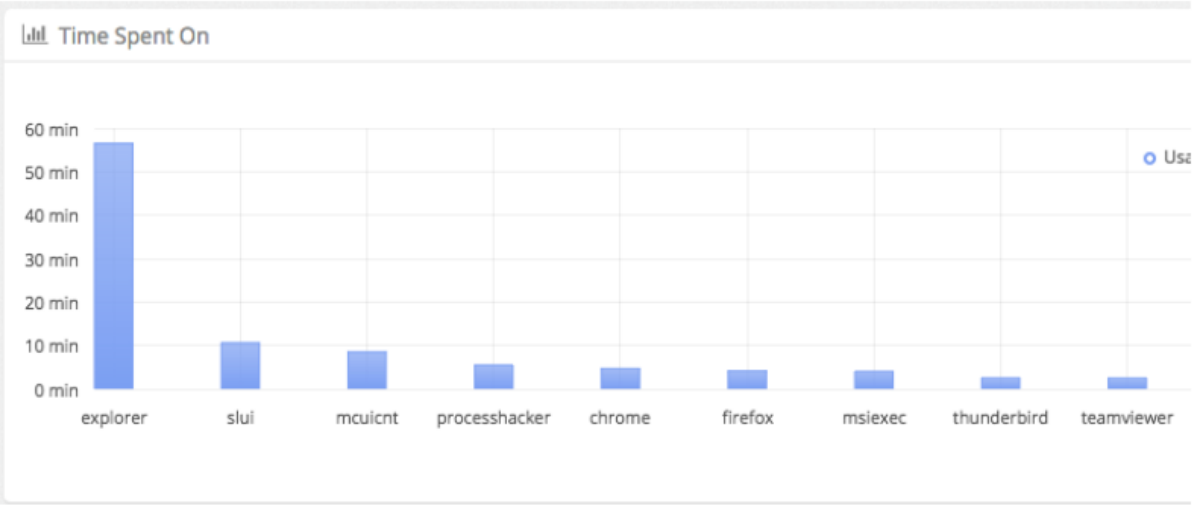
Date	Device	User	Application	Document
2015/02/11 20:47:15 +0100	WIN-4BQR6BRS7KP	Test	wmplayer	\Users\Test\AppData\Local\Microsoft\cd[2].xml
2015/02/02 14:49:55 +0100	MASAMUNE	Giuseppe	explorer	\Users\Giuseppe\Desktop\正体字繁体字.pdf
2015/02/02 14:37:52 +0100	MASAMUNE	Giuseppe	acrord32	\Users\Giuseppe\Desktop\正体字繁体字.pdf

4. 제품 특장점 – 어플리케이션 컨트롤

➢ 어플리케이션 컨트롤 (Application Control)

- 클라이언트에 의해 사용된 어플리케이션은 모니터링 되고, 후에 사용 분석을 위해 저장
- 각각 사용된 시간은 사용자의 활동에 대한 자료수집을 위하여 계산





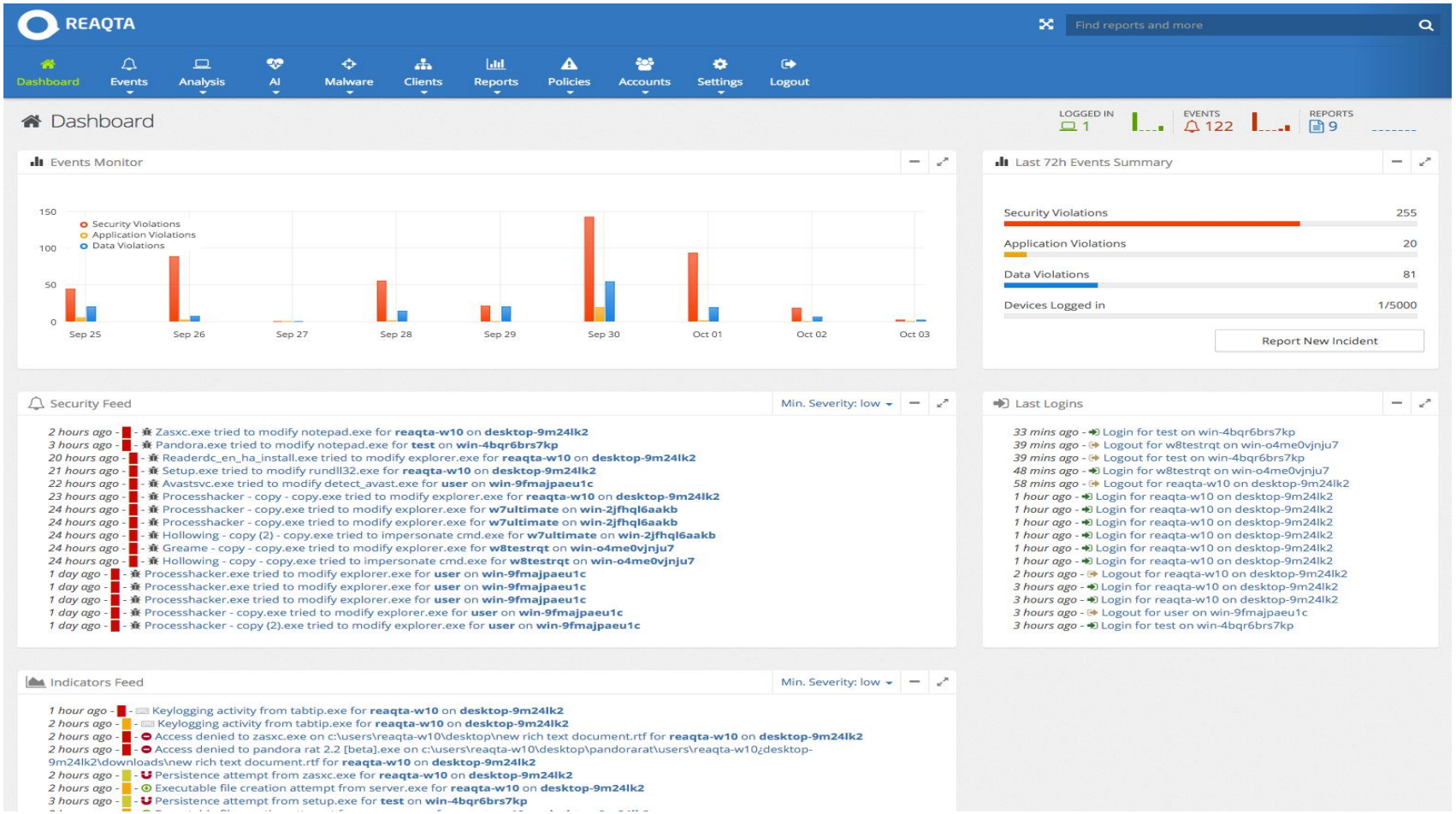
Used Apps

Date	Device	User	Application
2015/02/11 19:39:28 +0100	WIN-2JFHQL6AAKB	W7Ultimate	msiexec
2015/02/11 19:38:00 +0100	WIN-4BQR6BRS7KP	Test	explorer
2015/02/11 19:36:24 +0100	WIN-2JFHQL6AAKB	W7Ultimate	msiexec

4. 제품 특장점 – 대쉬보드

➢ 강력한 대쉬보드 기능

- 모든 필드가 실시간으로 완벽히 탐색 가능하고, 분석자에게 명확한 뷰(VIEW) 제공
- 단순한 데이터가 아닌 의미 있는 데이터로 구성될 수 있도록 모든 수행된 활동 파악



4. 제품 특장점 – 그룹 및 정책

➢ 그룹 관리

- 정책의 효율적인 배포를 위하여 대시보드에서 그룹 설정 가능(LDAP, AD 연동 가능)

Clients List

This page shows a list of every client that has been registered with the platform at least once. Clicking *disable* on a client will inactivate its license, the protection system will be disabled and a license slot will be made available to be used by the next client that connects to the system.

Show Group: Management Manage

Registration Date	Device	User	OS	Core Version	Group	License
2015/02/11 19:34:34 +0100	WIN-4BQR6BRS7KP	Test	Windows 7 Professional	2015020200	Management	remove
2015/02/06 09:27:36 +0100	GIUSEPPE-REAQTA	Giuseppe	Windows 8.1 Pro	2015020200	Management	remove
2015/02/10 16:43:51 +0100	GIUSEPPE-REAQTA	Giuseppe	Windows 8.1 Pro	2015020200	Management	remove
2015/02/02 14:24:12 +0100	WIN-8BN18JUU0TB	Giuseppe	Windows Server 2008 R2 Datacenter	2014101501	Management	remove
2015/02/11 14:22:09 +0100	WIN-9FMAJPAEU1C	User	Windows 8.1 Enterprise N	2015020200	Management	remove
2015/02/04 14:00:27 +0100	GIUSEPPE-REAQTA	Giuseppe	Microsoft Windows 8.1 Pro	2014101501	Management	remove
2015/02/04 14:00:59 +0100	WIN-2JFHQL6AAKB	W7Ultimate	Microsoft Windows 7 Ultimate	2014101501	Management	remove
2015/02/02 14:11:43 +0100	WIN-O4ME0VJNJU7	W8TestRQT	Windows 8	2014101501	Management	remove

Search

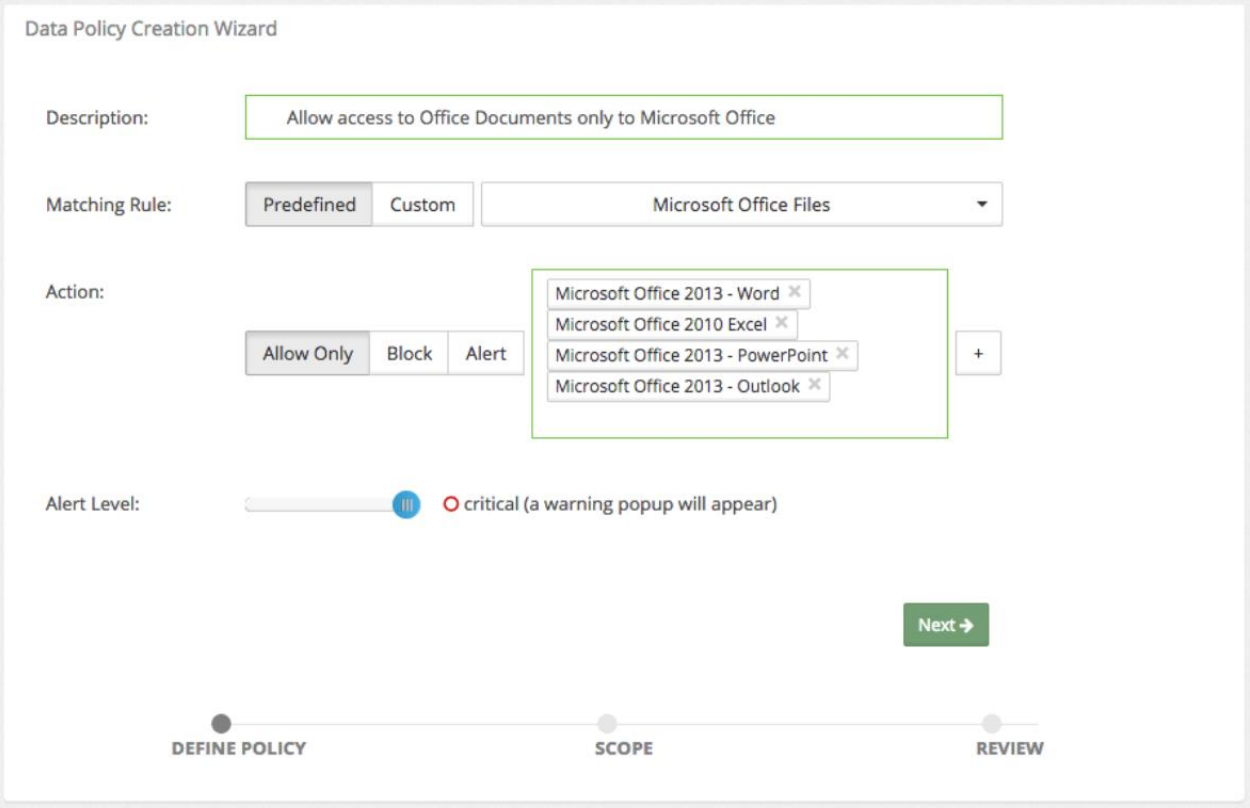
1 - 8 displayed , 8 in total

4. 제품 특장점 – 그룹 및 정책

➢ 정책 관리

• 쉽고 빠르게 민감한 데이터를 보호하기 위하여 3가지의 정책 제공

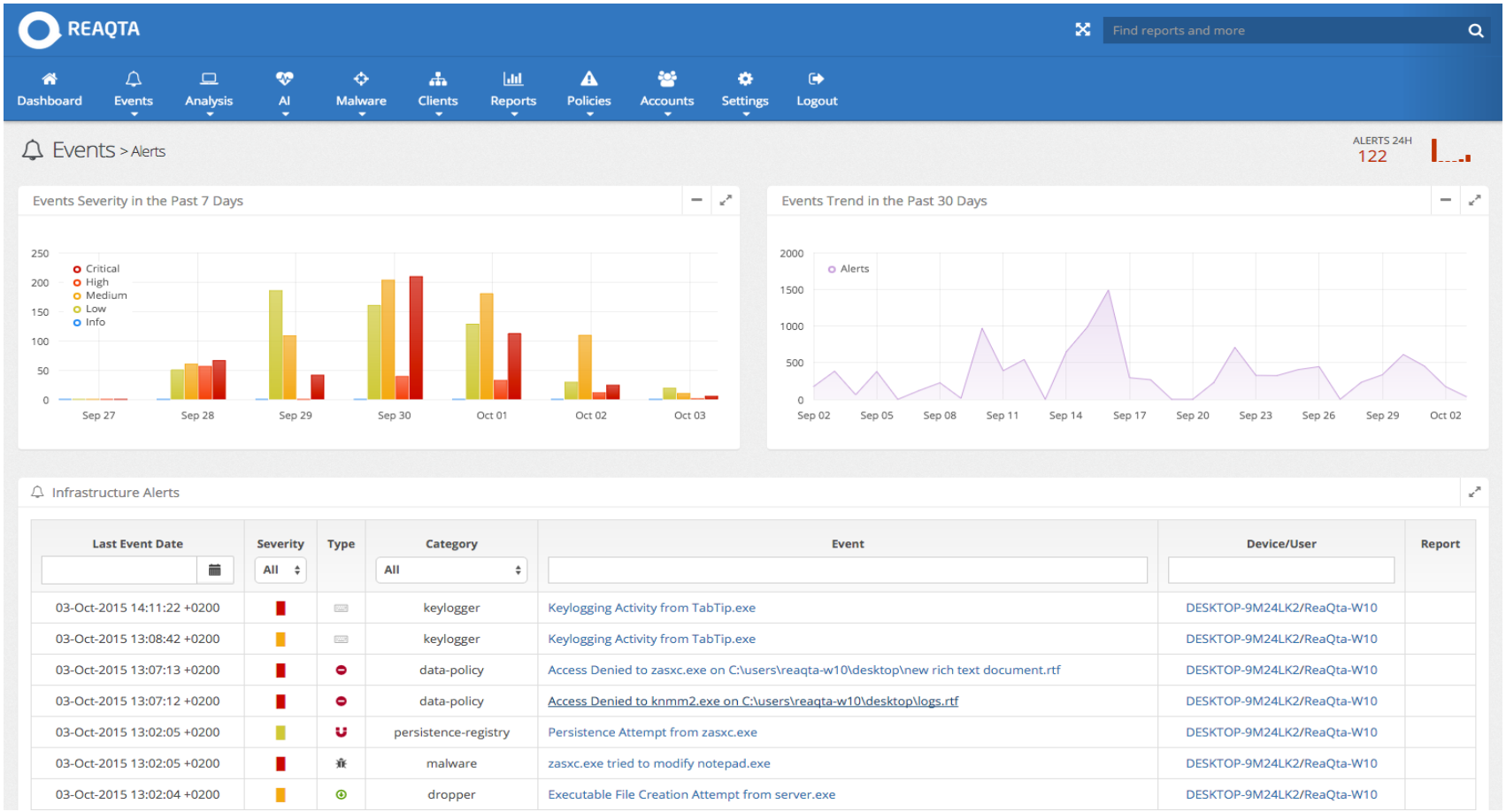
1. 어플리케이션 정책 : 특정 어플리케이션을 차단하거나 관심 있는 어플리케이션의 알람 적용
2. 데이터 정책 : 민감한 데이터를 보호하거나 민감한 데이터를 요구하는 어플리케이션에 대한 접근 제어 및 모니터링
3. Feature 정책 : 키로거(Keylogger), 스크린샷 시도, 드라이버 설치 등 시스템 컨트롤



4. 제품 특장점 – 이벤트 추적

➢ 이벤트 추적 및 경고

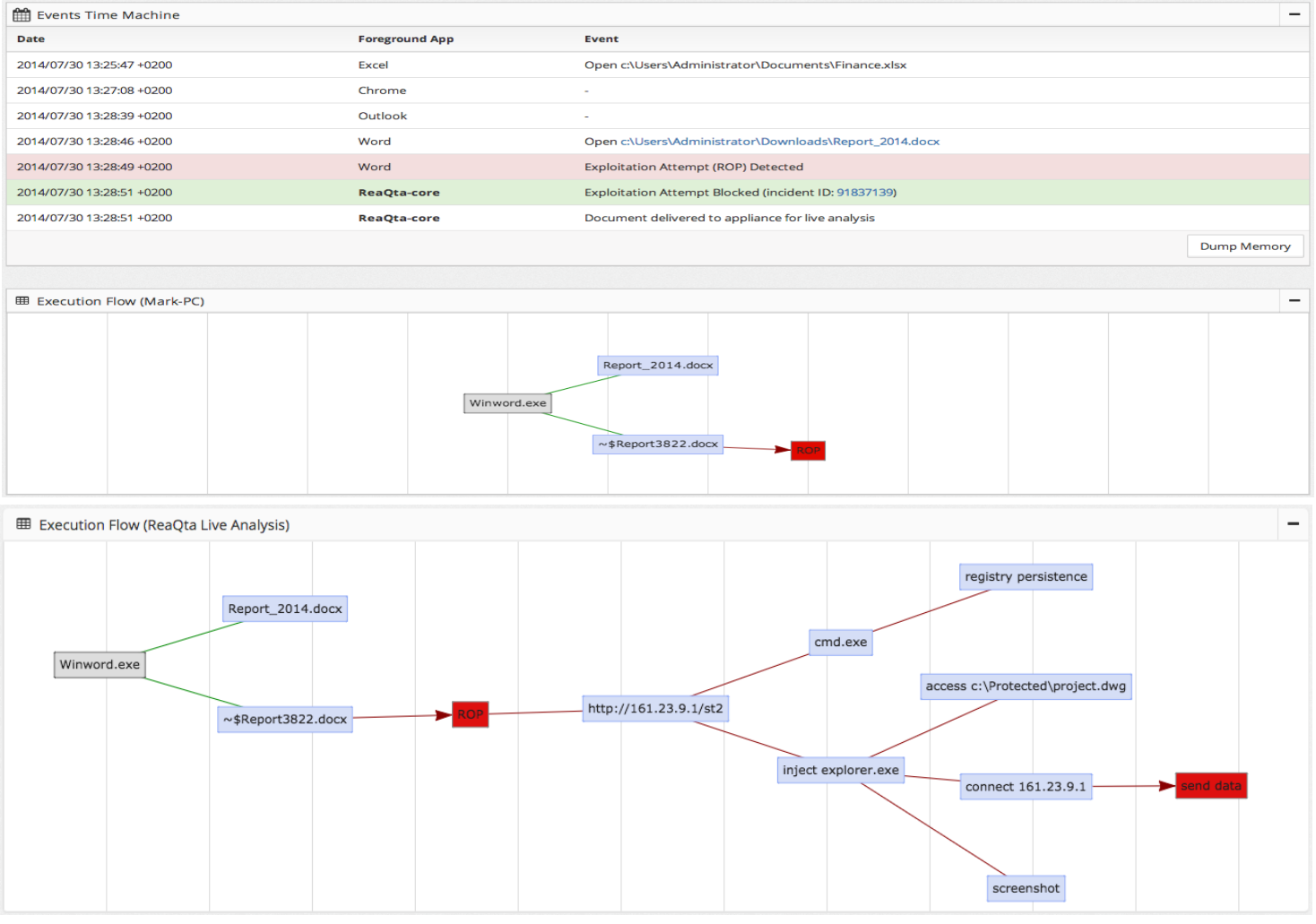
- 모든 어플리케이션의 전체 실행 구조 파악이 가능하므로, 어떠한 이벤트든 시작부터 추적 가능
- 멀웨어 및 렌섬웨어 파일 또는 익스플로잇(exploit)의 검사와 빠른 격리 제공
- 위협을 중지하기 위하여 어떠한 간섭도 필요 없으며, 인공지능이 자체적으로 위협 처리



4. 제품 특장점 – 라이브 위협 분석

➢ 라이브 위협 분석 (Live Threat Analysis)

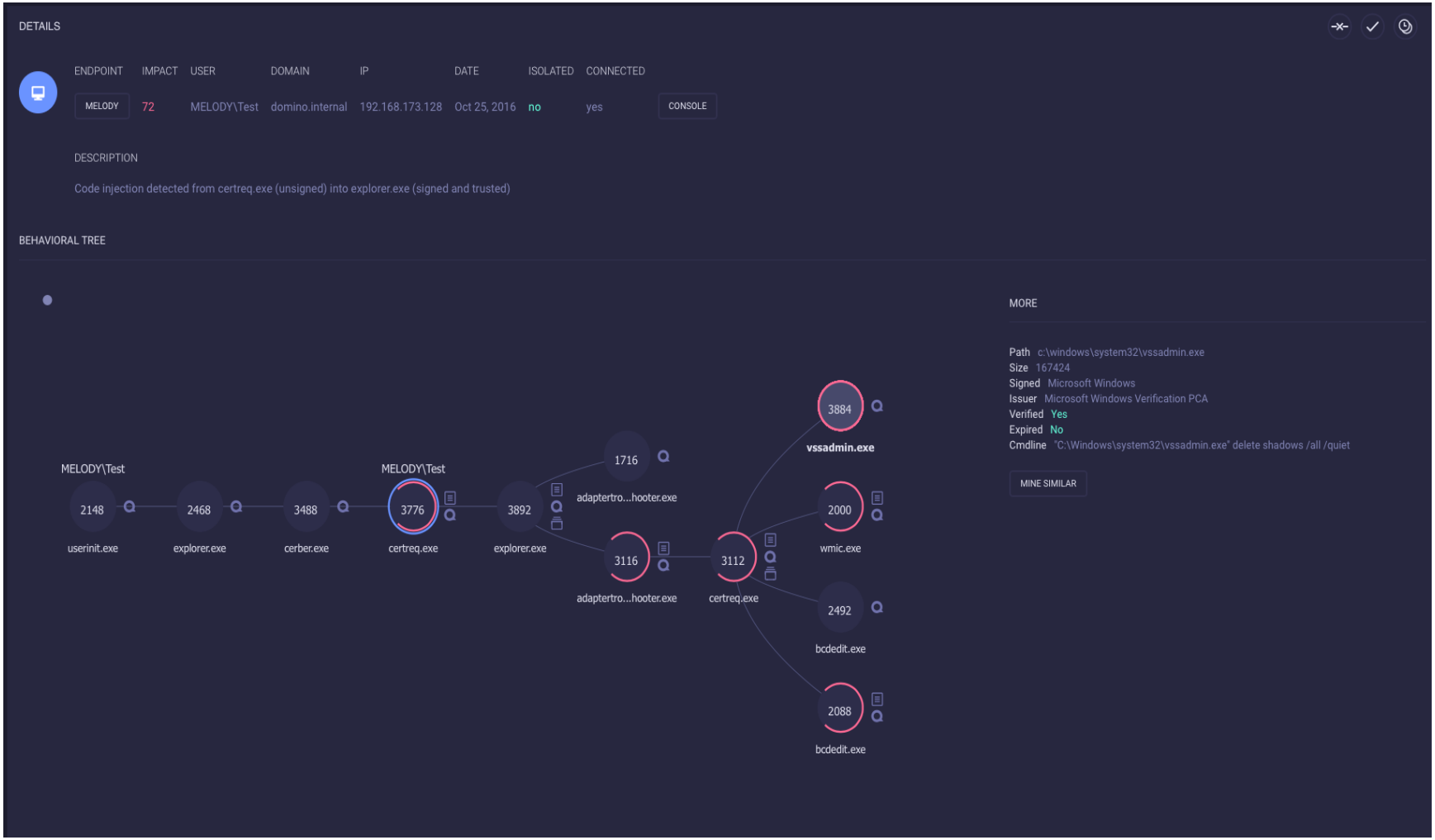
- 타겟 공격 동안의 방첩 활동 또는 조사를 위하여 시나리오를 수집하는 지능화 기능
- 사이버 위협에 대한 공격의 특성을 이해하고 공격자가 관심 있어 하는 데이터 파악



4. 제품 특장점 – 위협분석

➢ 위협 분석 (reconstrution)

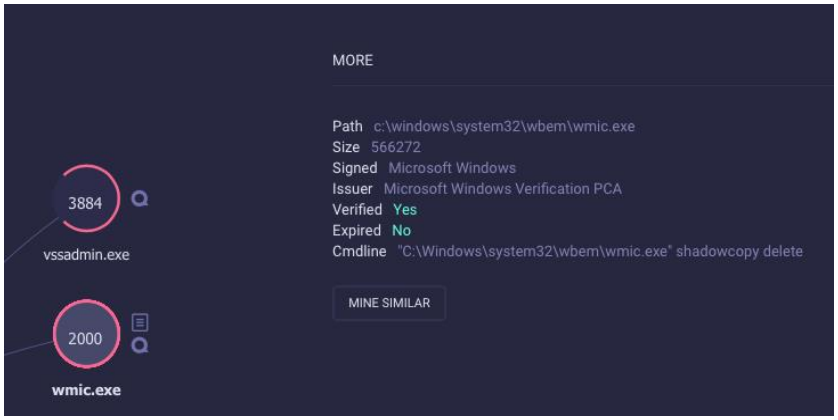
- 대시 보드에서 멀웨어/랜섬웨어등의 공격 흐름을 보여줍니다.

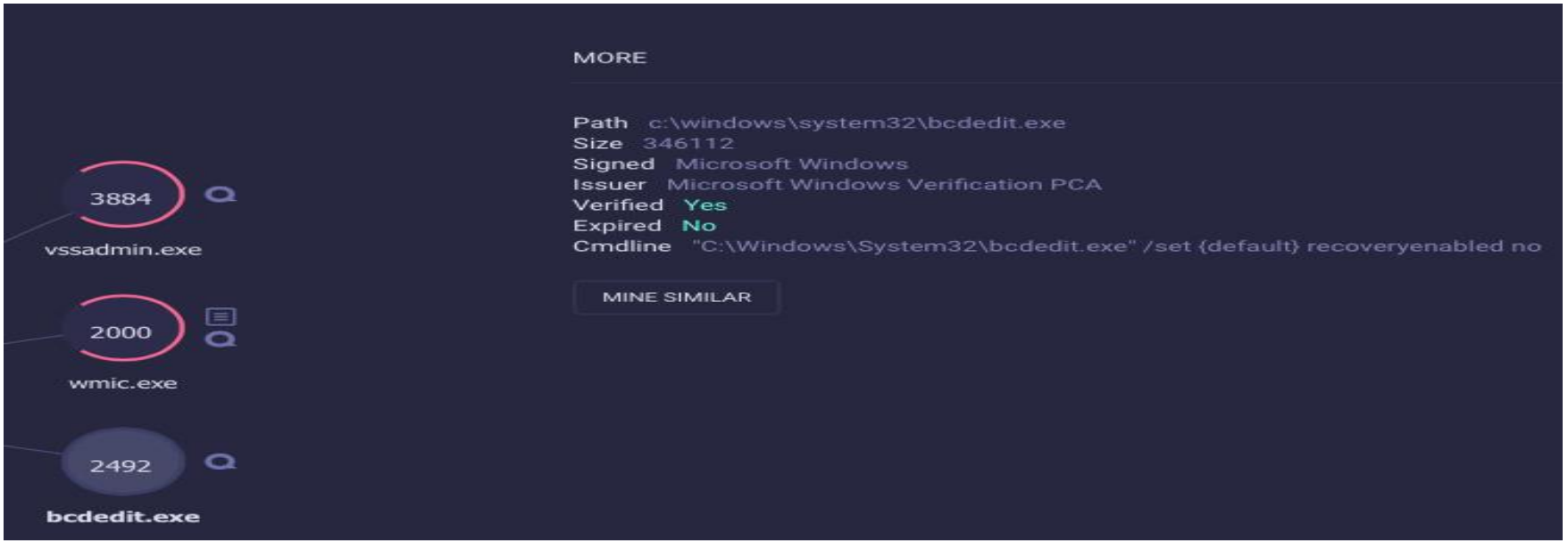


4. 제품 특장점 – 위협분석(계속)

➢ 위협 분석 (reconstrution)

• 대시 보드에서 멀웨어/랜섬웨어등의 공격 흐름을 보여줍니다.





4. 제품 특장점 – 위협분석(계속)

➢ 위협 분석 (reconstrution)

• 대상 Client에 실시간 쿼리를 수행하고 악성 프로세스를 종료 할 수 있습니다.

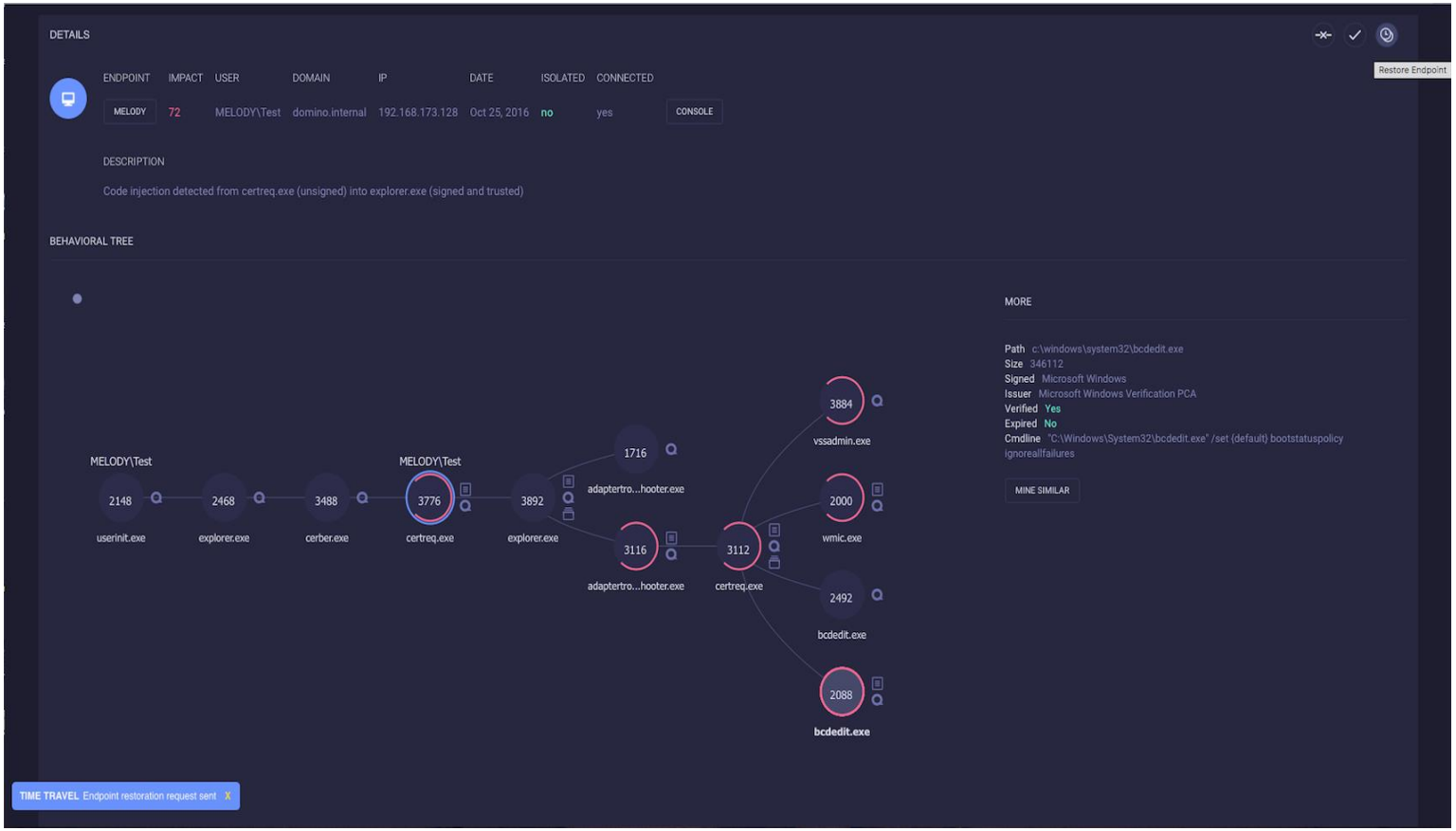
show procs

PID	PPID	PROCESS	PATH	USER	KILL
0	0	[System Process]			×
4	0	System		NT AUTHORITY\SYSTEM	×
276	4	smss.exe	C:\Windows\System32\smss.exe	NT AUTHORITY\SYSTEM	×
364	352	csrss.exe	C:\Windows\System32\csrss.exe	NT AUTHORITY\SYSTEM	×
416	352	wininit.exe	C:\Windows\Syst...m32\wininit.exe	NT AUTHORITY\SYSTEM	×
428	408	csrss.exe	C:\Windows\System32\csrss.exe	NT AUTHORITY\SYSTEM	×
480	408	winlogon.exe	C:\Windows\Syst...32\winlogon.exe	NT AUTHORITY\SYSTEM	×
508	416	services.exe	C:\Windows\Syst...32\services.exe	NT AUTHORITY\SYSTEM	×
532	416	lsass.exe	C:\Windows\System32\lsass.exe	NT AUTHORITY\SYSTEM	×
540	416	lsm.exe	C:\Windows\System32\lsm.exe	NT AUTHORITY\SYSTEM	×
640	508	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\SYSTEM	×
708	508	vmacthlp.exe	C:\Program File...ls\vmacthlp.exe	NT AUTHORITY\SYSTEM	×
752	508	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\NETWORK SERVICE	×
816	508	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\LOCAL SERVICE	×
876	508	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\SYSTEM	×
932	508	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\SYSTEM	×
500	508	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\LOCAL SERVICE	×
1104	508	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\NETWORK SERVICE	×
1200	508	spoolsv.exe	C:\Windows\Syst...m32\spoolsv.exe	NT AUTHORITY\SYSTEM	×
1232	508	svchost.exe	C:\Windows\Syst...m32\svchost.exe	NT AUTHORITY\LOCAL SERVICE	×
1352	508	keeper.exe	C:\Program File...aQta\keeper.exe	NT AUTHORITY\SYSTEM	×
1564	508	VGAuthService.exe	C:\Program File...AuthService.exe	NT AUTHORITY\SYSTEM	×

4. 제품 특장점 – Restore

➢ Restore

- 랜섬웨어등에 감염되기 전에 상태로 다시 되돌릴 수 있습니다.
- Hash값등의 키값을 보유하여 감염전 상태로 실시간 Roll-Back.(재부팅/로그오프 X)



- 랜섬웨어 복원 동영상
https://www.youtube.com/watch?v=Of1m1MOUwbY

5. ReaQta AI 엔진

➢ ReaQta-Core 2개의 AI 엔진 적용

1. The 1st AI : SVM(Support_vector_machine) and Dynamic Time Warping algorithms
   - *The 1st AI resides in every device and works independently without any connection to the backend server or internet.* ***It detects and block in realtime cross memory operation such as process impersonation, injection etc****.*
2. The 2nd AI : SVM and Apriori algorithms
   - *The 2nd AI resides at ReaQta-brain and it attempts to predicts whether an event (received from the device) could be malware or goodware*

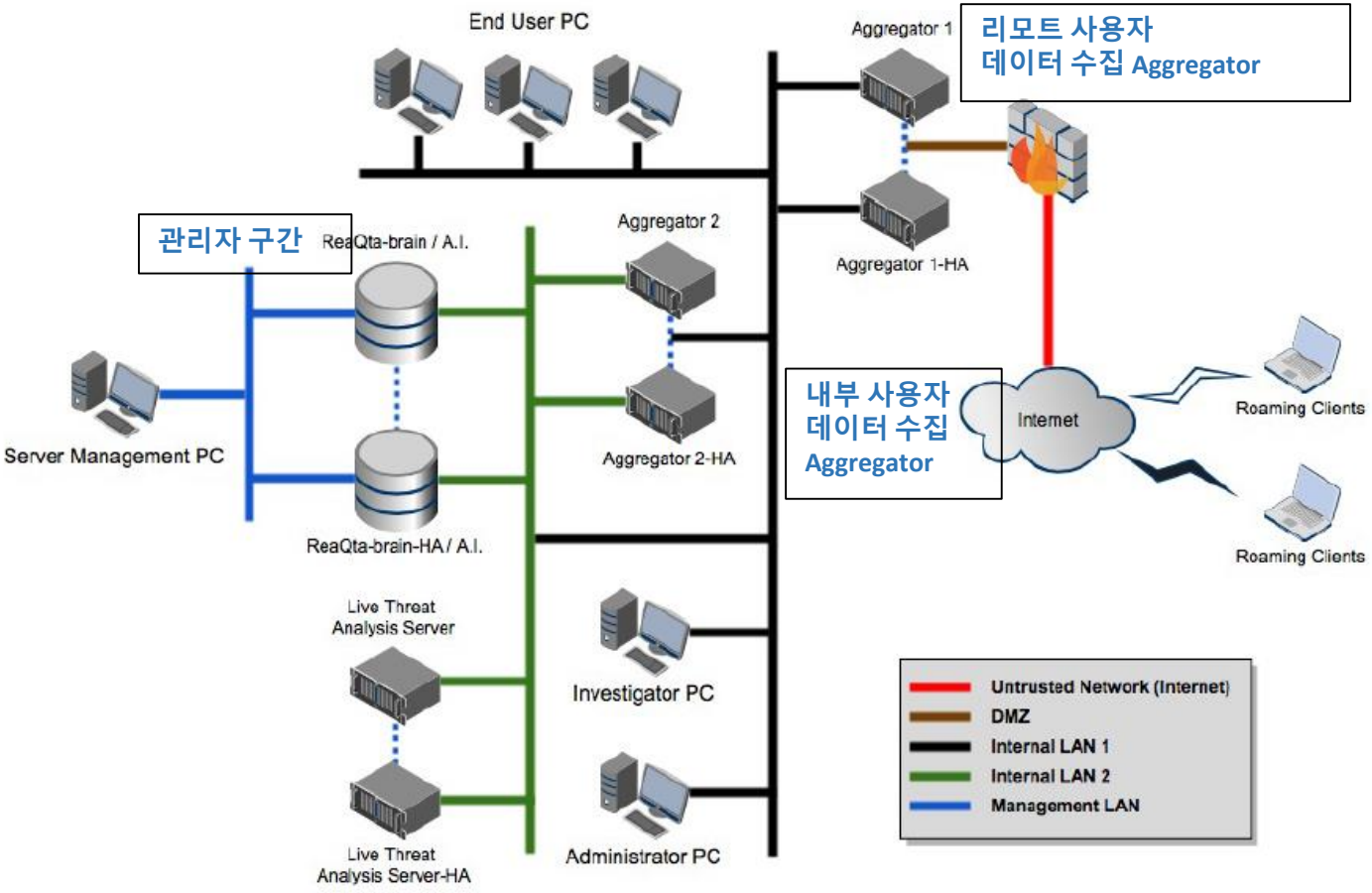
➢ AI엔진 학습

1. ReaQta labs 에서 수백만 개의 멜웨어 와 own honey pots구축으로 신규 멜웨어를 지도학습 및 비지도 학습을 합니다.
2. The 1st AI and 2nd AI은 고객사에서 별도의 학습 없이 최신의 버전으로 작동하며, 매 분기마다 버그수정, 신규기능을 포함하여 학습된 최신의 AI엔진을 배포 합니다.
3. ReaQta AI엔진은 최신의 학습없이 멜웨어의 악의적인 행위기반의 학습 및 분석을 통해서 unknown malwares에 대한 탐지능력을 가지고 있습니다.

6. 시스템 구성도

설치 구성도

- 이중화로 구성된 설치 방안으로 완벽한 기능 제공
- 시스템 성능에 최소의 영향을 주도록 pure assembly x64에서 동작 (64비트 운영체제에서 사용 가능)



7. 지원 환경

➢ 클라이언트 하드웨어 사양

ReaQta-core는 NanoOS가 올바르게 동작할 수 있는 Intel 또는 AMD CPU 위에 설치됩니다.

➢ 클라이언트 소프트웨어 사양

ReaQta-core와 ReaQta-Investigator를 위한 지원되는 클라이언트의 OS는 다음과 같습니다.

- Windows 7
- Windows 7 SP0
- Windows 7 SP1
- Windows Server 2008 R2
- Windows 8
- Windows 8.1
- Windows Server 2012 R2
- Windows 10

➢ ReaQta-core는 가상머신의 VM 옵션에서 VT-x접근이 활성화되어 있다면 가상 머신 내에서 운영중인 운영체제에도 설치됨.

➢ Vmware workstation/Virture Box 가능, Hiper-V Host PC 불가능(Hiper-V 가상PC 가능).

8. 경쟁사 비교

	Reaqta-Core	Countertack Sentinel	Palo Alto Traps	Mcafee Deep Security	**cybereason**
Detection from outside operating system	✔	-	-	✔	-
Lightweight Agent	✔	?	?	?	✔
0-Day Exploitation Detection	✔	✔	?	✔	?
0-Day Exploitation Prevention	✔	-	?	✔	?
Exploit remediation	✔	-	?	?	?
APT Detection	✔	✔	✔	?	✔
APT Blocking	✔	-	✔	✔	✔
Malware remediation	✔	-	?	?	?
Future proof protection using Artificial Intelligence	✔	-	-	-	?
Organizational correlation of threats	✔	✔	-	-	✔
Data protection policies	✔	-	-	-	-
Application Whitelisting/Blacklisting	✔	-	-	-	-
Effective protection regardless of machine state	✔	-	?	?	-
Local deployment without connecting to cloud	✔	?	✔	✔	✔
Offline Protection	✔	-	✔	✔	-
Signature-less detection	✔	?			?

감사합니다

Q & A

솔루션사업부/컨설팅팀 **김기준, 이세현**
Email : shlee@bellins.net
서울특별시 서대문구 충정로 13 삼창빌딩 3층
Tel. 02-6925-1130 Fax. 02-2664-1575