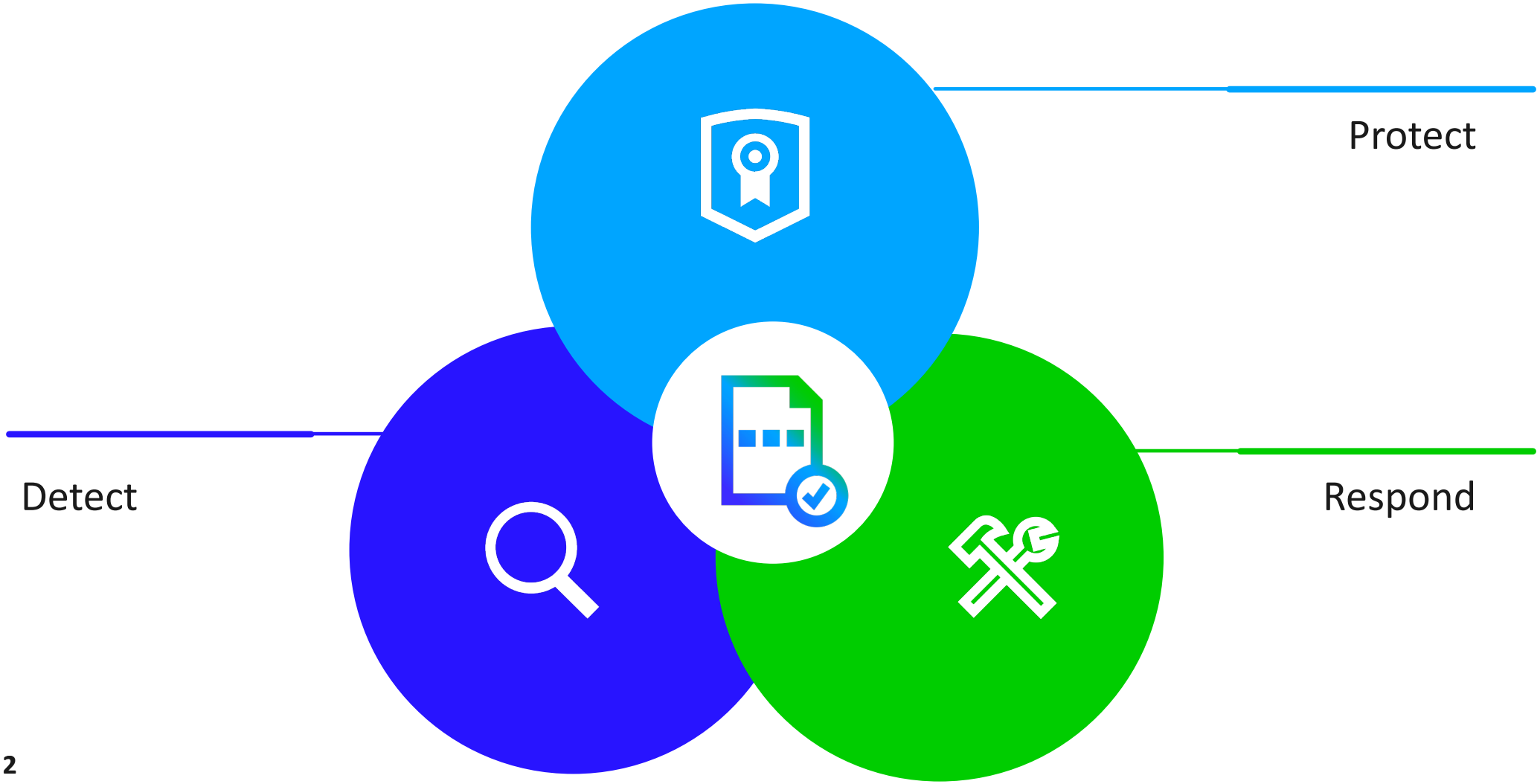
Trellix

엔드포인트 보안,
이상 징후 탐지의 시작

Trellix Korea

Sept 2022

한 눈에 보는 트렐릭스 엔드포인트 보안



트렐릭스가 엔드포인트 보안을 위해 하는 방법

Protect

- Malware Protection
- Malware Guard
- Exploit Guard
- Process Guard

Detect

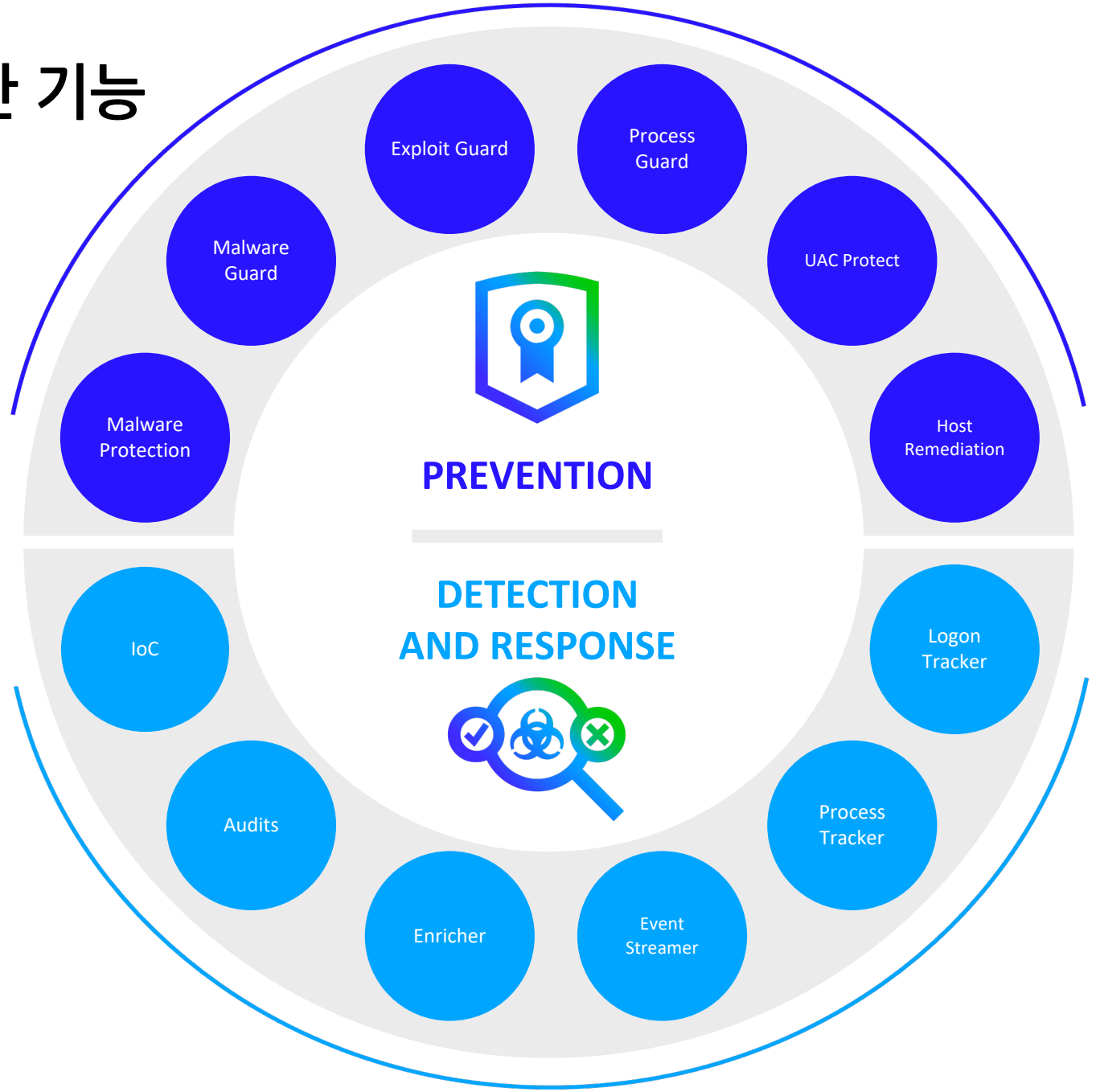
- Indicators of Compromise
- Enterprise Search
- Investigative Data Acquisition
- Process Tracker

Respond

- Auto Containment
- On or off-network response
- Respond at scale

Trellix

트렐릭스 엔드포인트 보안 기능



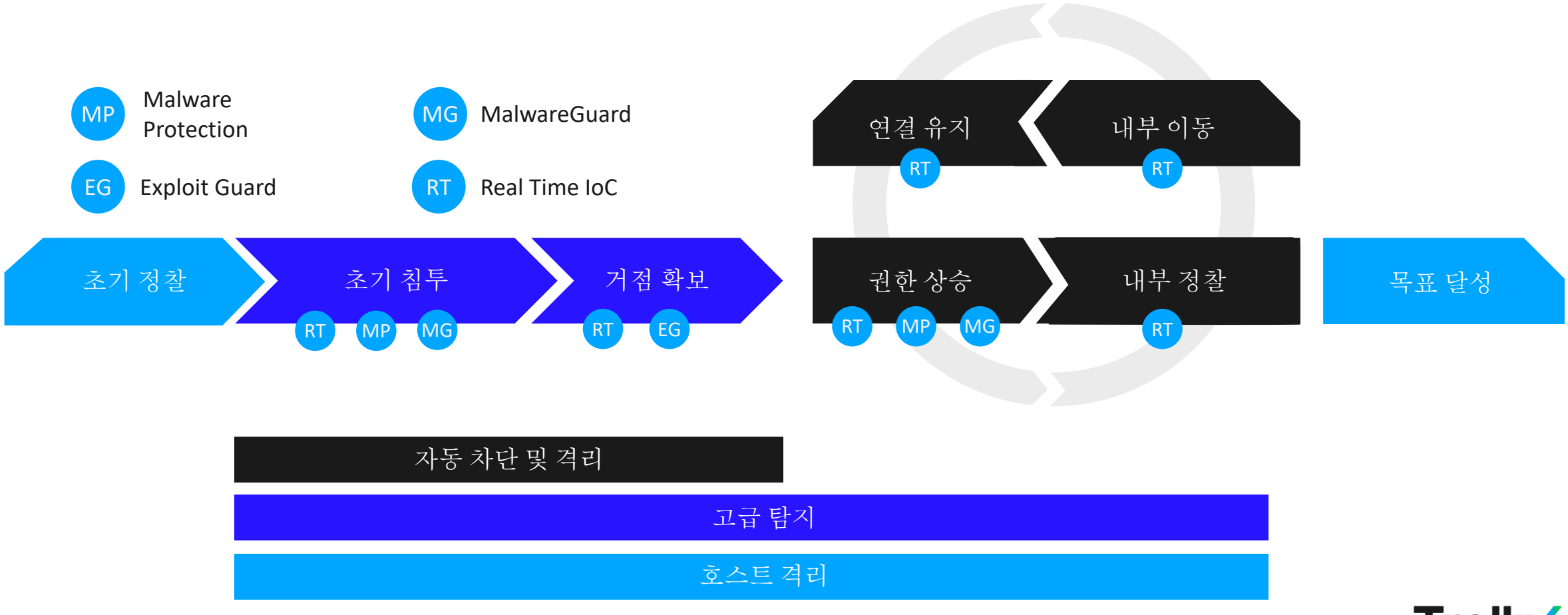
Trellix

엔드포인트 보안 모듈 (HX 5.2 & xAgent 34.X)

	보호 모듈	탐지 및 대응	운영 및 관리
정식 사용 가능	Process Guard (A)	Process Tracker (A) Event Streamer (A) Enricher (S) Host Remediation (A+S)	Agent Console (A) Host Management (S) API Documentation (S) Ask an Expert (S) Storytime (S)
기술 미리보기	UAC Protect (A) Device Guard (A)	AMSI (A) Logon Tracker (A) IOC Streamer (A)	Server Health (S)
출시 예정	Deny List (A)		Scan Summary (A)

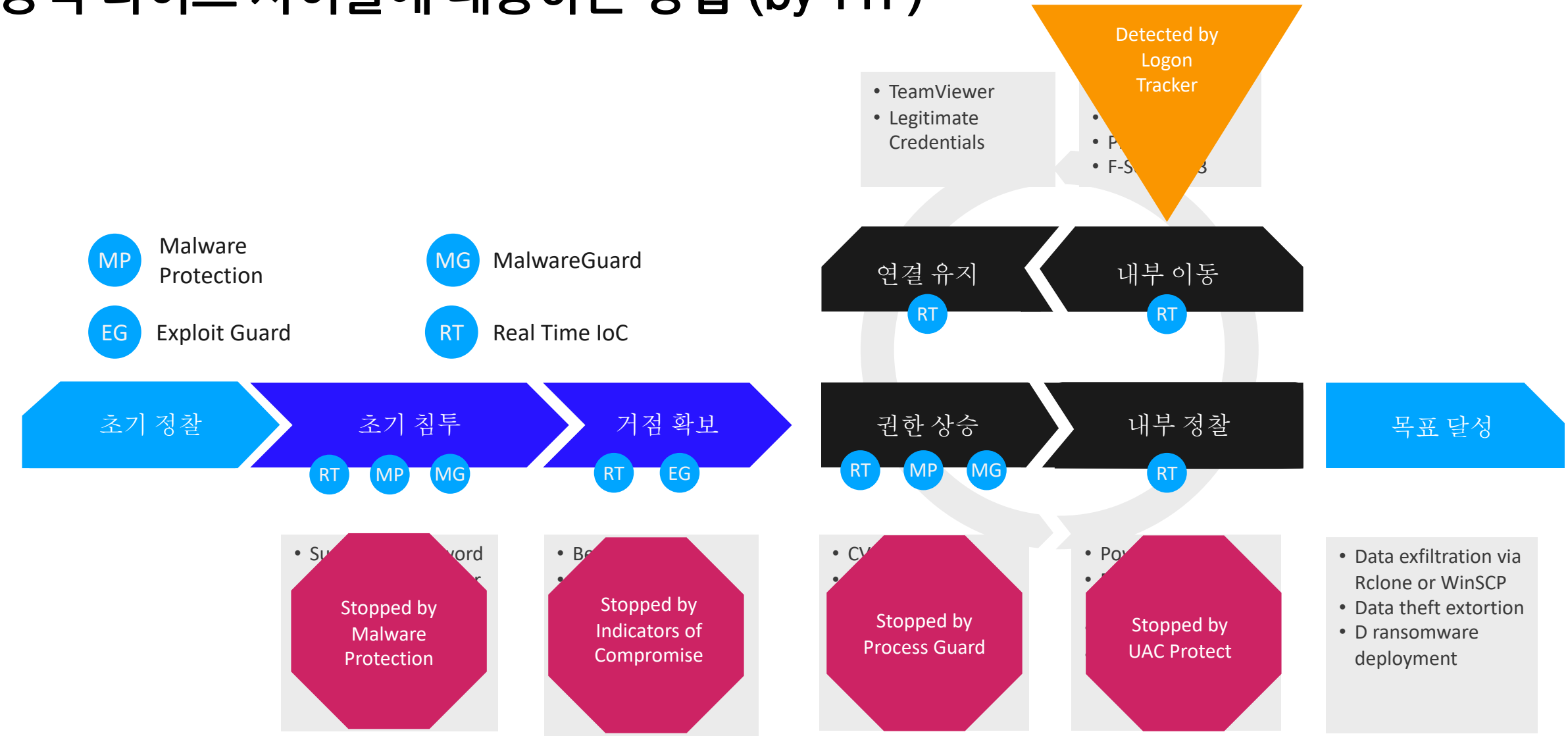
Trellix

공격 라이프 사이클에 대응하는 방법



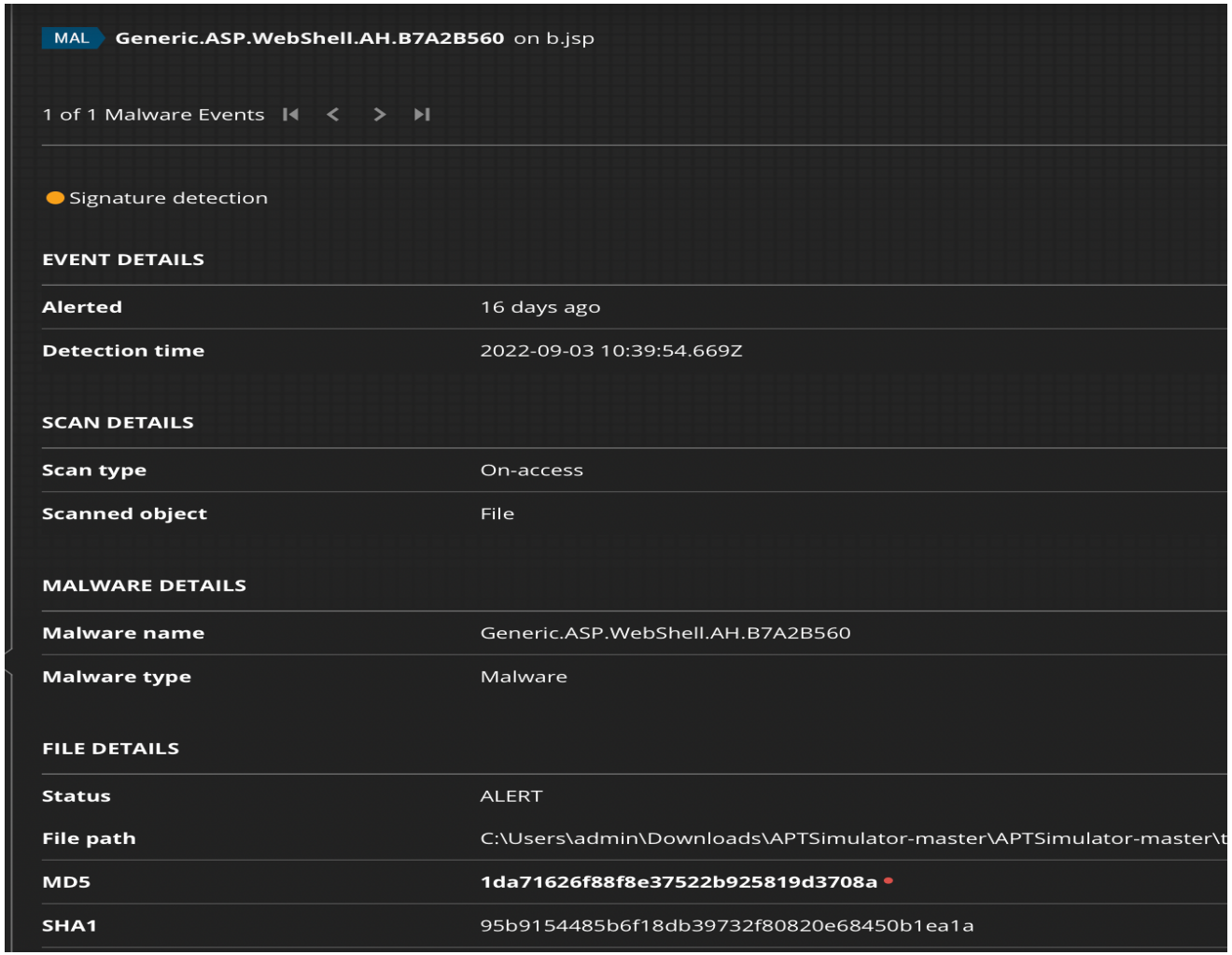
Trellix

공격 라이프 사이클에 대응하는 방법 (by TTP)



Trellix

Case1. 임직원 PC에서 서버까지 HX Agent 확장



[기존현황]

- HX Agent.가 임직원 개별 호스트에만 설치 된 상황
- 서버들은 부하를 염려하여 설치하지 않음

[탐지 및 대응]

- 개발자 PC에서 Webshell 탐지 이벤트 발생
- 탐지된 Webshell 의 경로를 통해 추론한 결과 서비스 중인 서버에서 내려 받은 것으로 확인

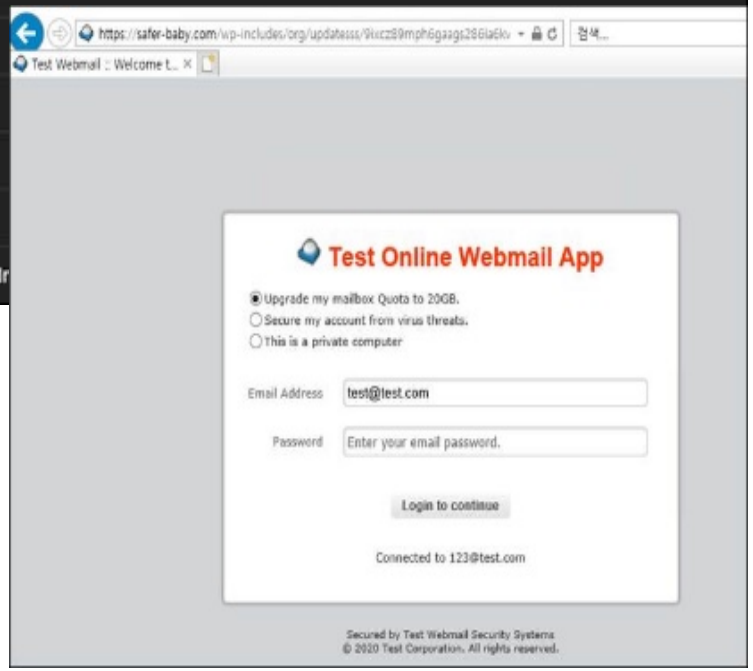
[개선사항]

- 서버가 침해당한 사실을 역으로 개발자 PC에서 확인됨
- 차후 사고 방지를 위해 서버에도 HX Agent 설치

Trellix

Case2. CM 연동을 통한 엔드포인트에서 피싱 차단

urlMonitorEvent/timestamp	2020-02-17 08:07:58Z
urlMonitorEvent/hostname	ricebasmati.ru
urlMonitorEvent/requestUrl	/image/cache/app/?email=yhseo@lottedacc.com
urlMonitorEvent/urlMethod	GET
urlMonitorEvent/userAgent	Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
urlMonitorEvent/httpHeader	GET /image/cache/app/?email=yhseo@lottedacc.com HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: ko-KR User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ricebasmati.ru Connection: Keep-Alive
urlMonitorEvent/remoteIpAddress	87.236.16.204
urlMonitorEvent/remotePort	80
urlMonitorEvent/localPort	53921
urlMonitorEvent/pid	14784
urlMonitorEvent/process	iexplore.exe
urlMonitorEvent/processPath	C:\Program Files (x86)\Ir



[기존현황]

- CM, EX, HX 가 함께 구성되어 있음.

[탐지 및 대응]

- EX 에서 URL 끝 부분에 이메일을 인자로 전달받는 형태의 피싱메일 탐지
- 이후 CM 을 통해 관련 패턴이 HX 로 전달
- 이후 HX에서 유사 URL 접근시 탐지

Trellix

HX 5.3 및 xAgent 35.X 의 새로운 기능

추가된 기능

- Scan Now for Windows
- Automatic Triage Exclusion
- Multiple File Acquisition

기능 개선

- Generic Alert False Positive Support
- Supported Audit Features for Microsoft Edge
- Browser Audit Improvement
- Custom Triage Package

원 콘솔, 통합된 에이전트

- 원 콘솔이란…

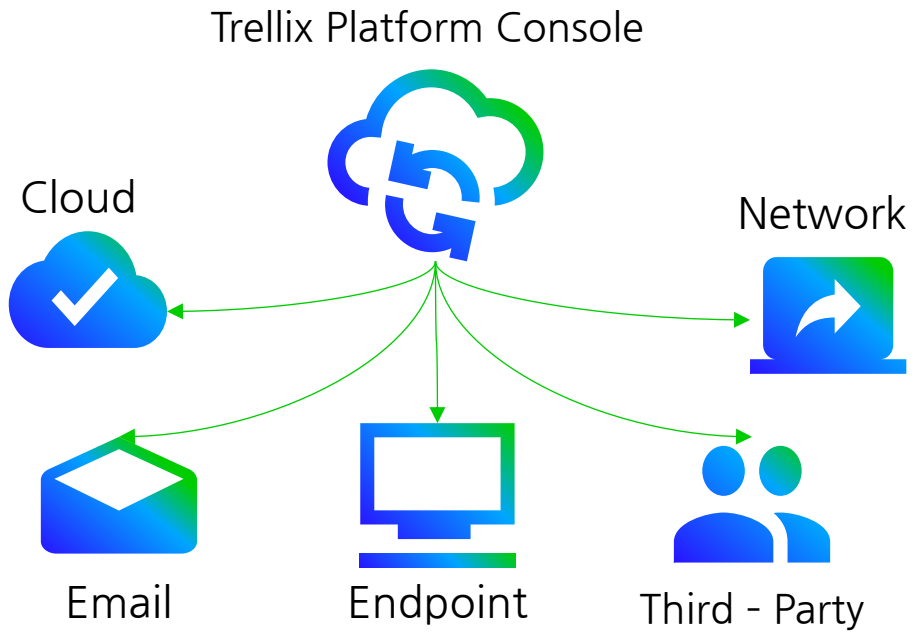
단일화 된 관리

단일화 된 대시보드

단일화 된 Alert 흐름

단일화 된 UI

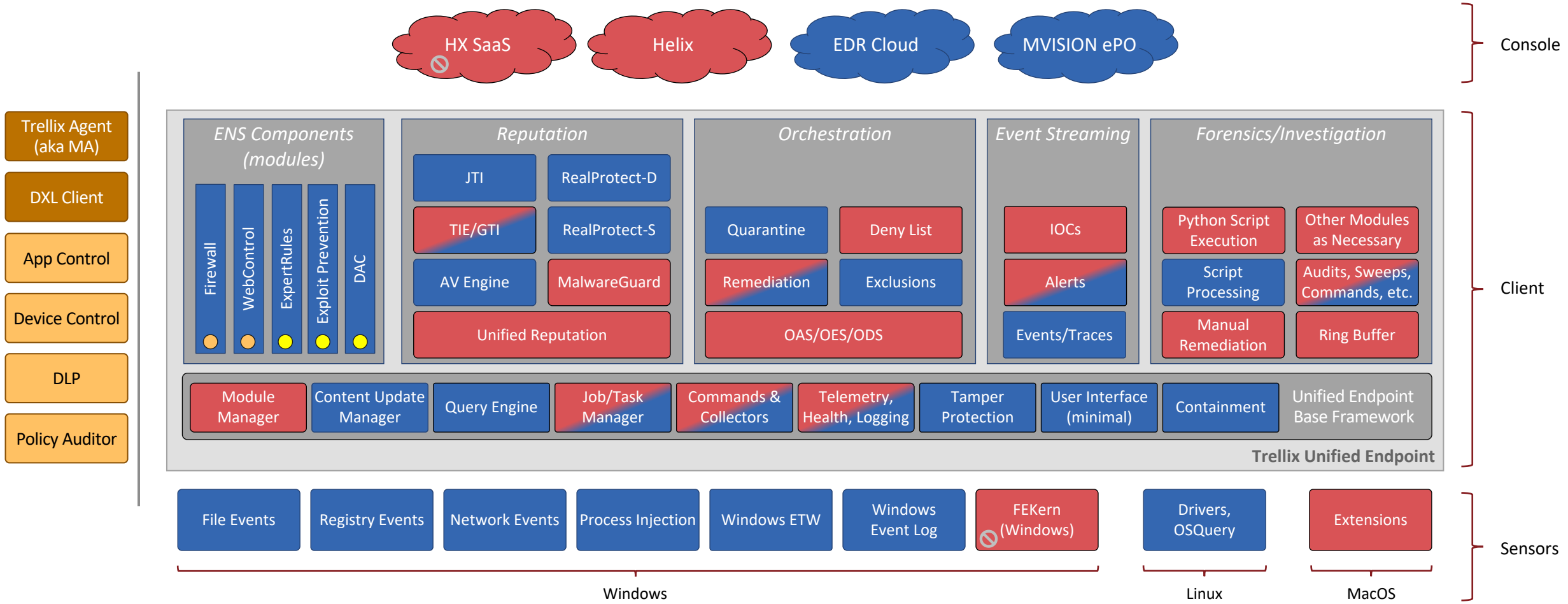
단일화 된 업무 흐름



모든 제어는 동일한 보안 경험을 통해 제공됩니다!

Trellix

통합된 엔드포인트 아키텍처



Trellix

감사합니다.