Information security company

EYEON Security

SentinelOne 소개서

주소 : 서울특별시 서초구 서초대로 255 2층 (고덕빌딩) | 사업자등록번호 : 215-87-70318 | 통신판매업신고번호 : 제 2019-서울서초-2940호
영업 문의 : 02-2105-4400 | 기술문의 : 02-2105-4455

Contents

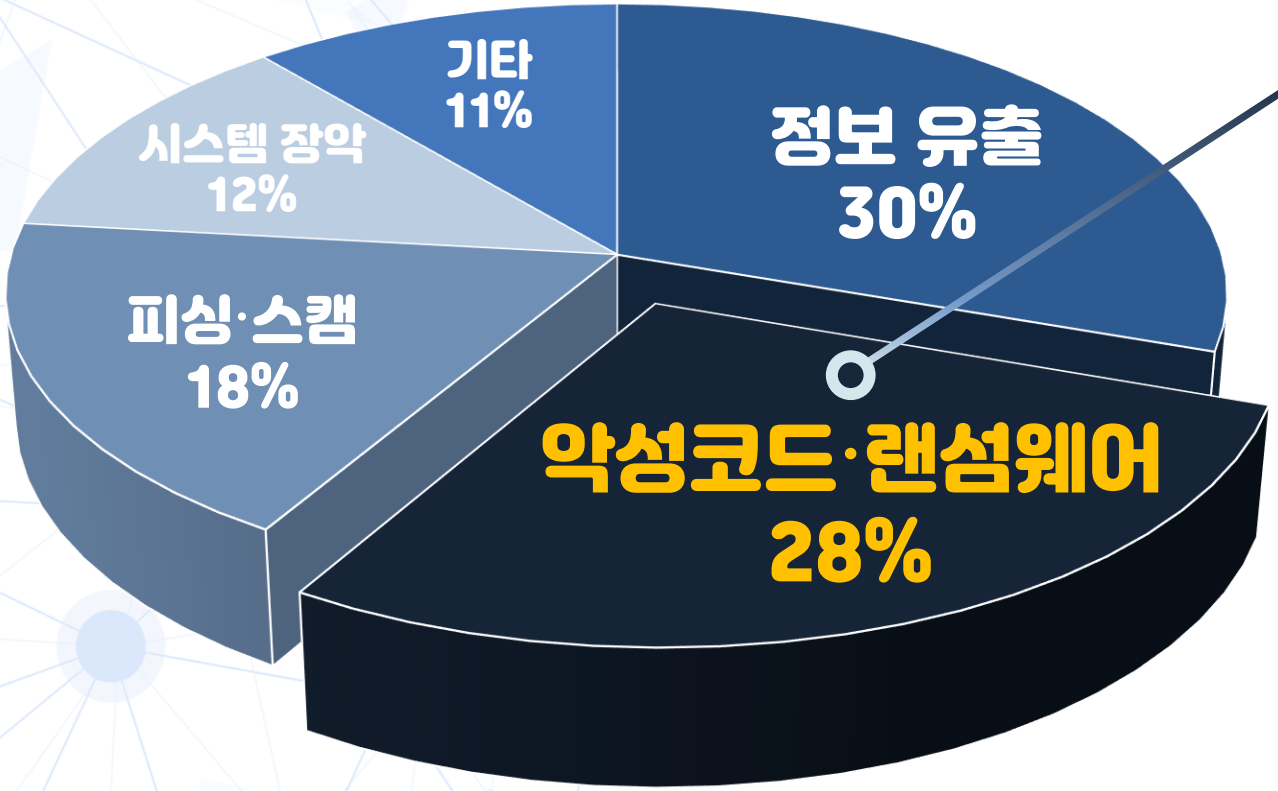
Eyeon Security

Information security company

01. End-Point 백신의 필요성

최근 5년간 랜섬웨어 관련하여 국내 피해 신고 건수는 14배 이상 증가하였습니다.

랜섬웨어는 몸값(Ransom)과 소프트웨어(Software)의 합성어로 해커 조직이 시스템이나 데이터를 암호화한 뒤 복구를 빌미로 금전을 요구하는 사이버 범죄입니다. 한국인터넷진흥원(KISA)에 접수된 침해 사고 접수 사례의 **28%가 랜섬웨어 의한 것**으로 확인되었습니다.



‘22년 상반기	‘23년 상반기
서비스형 랜섬웨어	대규모 랜섬웨어 공격
국내 기업 타깃형 랜섬웨어	디페이스 공격 악성코드 유포 ↑

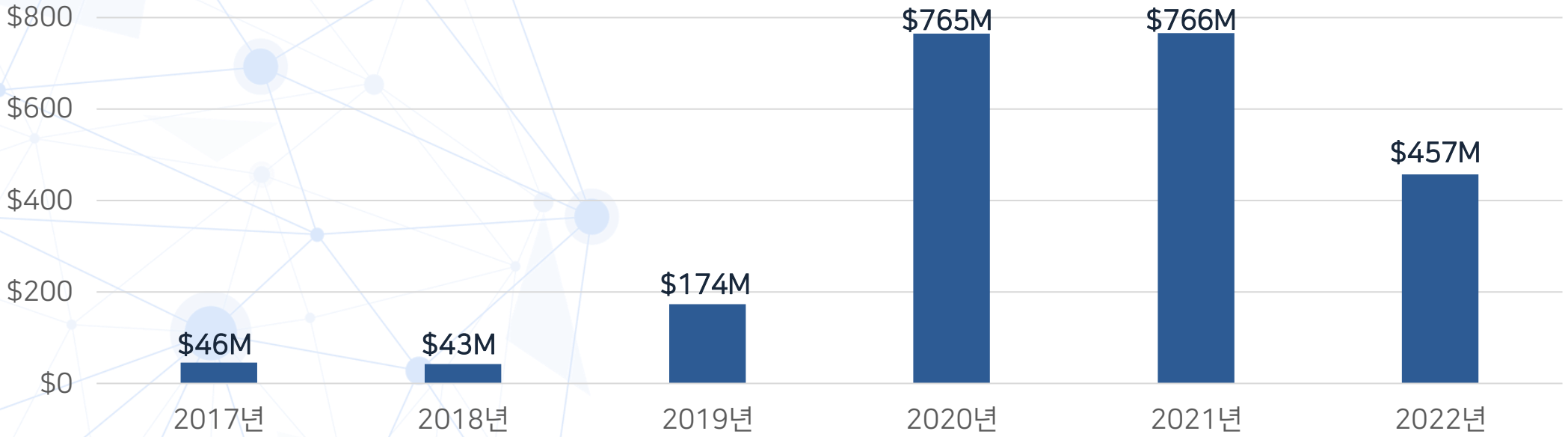
자료 출처 : 한국인터넷 진흥원

01. End-Point 백신의 필요성

랜섬웨어는 2017년부터 급속한 확산으로 기업에 큰 피해를 주었으며, 2022년까지 약 5,633억 원의 피해가 발생한 것으로 추정됩니다. 이를 줄이기 위해 **안티 랜섬웨어 백신과 같은 보안 솔루션 도입이 늘어나고** 있으며, 2022년부터 피해 사례는 10.4% 감소하고 피해액은 40.3% 으로 감소하였습니다.

그러나 랜섬웨어는 여전히 위협이 존재하며, 해커들이 새로운 공격 기법을 개발하고 있습니다. 따라서 기업은 계속해서 보안을 강화해야 합니다.

연도별 랜섬웨어 피해액, 2017 - 2022



자료 출처 : Chainalytic

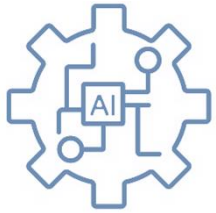
02. SentinelOne 백신 소개

SentinelOne은 AI 머신 러닝 기반으로 개발된 차세대 엔드포인트 보안 솔루션입니다.
시그니처 기반의 백신으로 탐지되지 않는 **랜섬웨어**, 알려지지 않은 악성코드 등 Zero-Day 공격에 효과적으로 대응하고, SentinelOne 엔드포인트 솔루션만의 특화된 랜섬웨어 피해 복구 기능으로 기업 정보 자산을 안전하게 보호합니다.

액셔너블 XDR

악의적인 행동을 식별하는 것만으로는 충분하지 않습니다. 크로스 플랫폼, 엔터프라이즈 데이터 분석을 통해 기계의 속도로 지능형 공격을 자율적으로 차단하고 치료합니다.

분산형 AI



위치와 연결에 관계없이 모든 엔드포인트 및 워크로드가 사이버 위협에 지능적으로 대응할 수 있도록 강력한 정적 AI 및 행동형 AI를 탑재하였습니다.

Storyline 특허 기술

하나의 일러스트 뷰에서 양성 및 악성 이벤트를 자동으로 연결하고 상호 연관시켜 분석가들이 필요한 컨텍스트를 더 빠르게 확보할 수 있습니다.

03.
SentinelOne 특징

AI 탐지 엔진

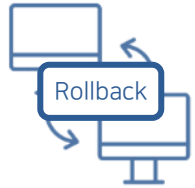
정적 / 동적 AI 엔진으로 알려지지 않은 위협 탐지

ActiveEDR®

악성코드가 수행한 프로세스, 레지스트리, 파일 등 14 항목을 기록/관리 및 분석

Storyline™

악성코드 시작부터 마지막까지 모든 과정을 분석 지원



강력한 대응 - 복구

EPP + EDR

센티널원 제공하는 모든 기능을 단일 에이전트로 통합, XDR로 확장

ONE Console

전세계 모든 지역에서 단일 콘솔로 통합 관리 제공

대응 조치

중지

위협과 관련된 모든 프로세스 중지

격리

위협 요소 및 실행 파일 암호화 및 이동

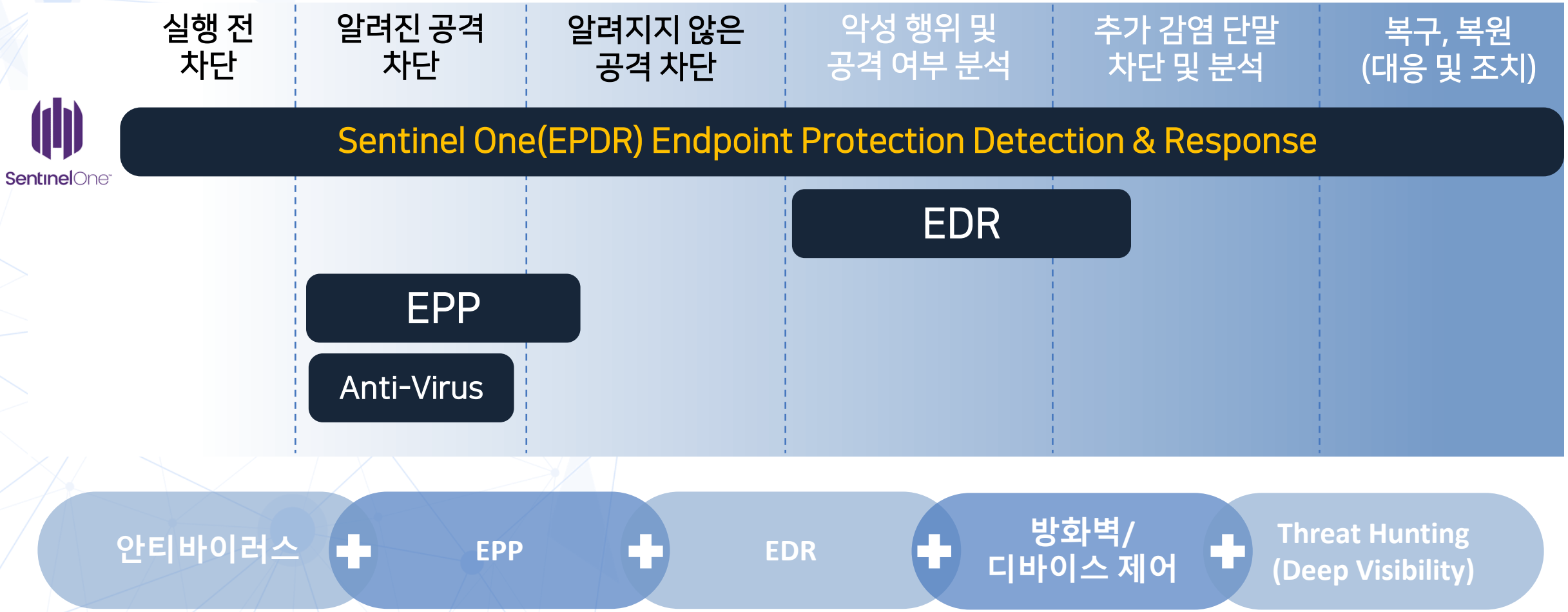
업데이트 적용

위협으로 인해 생성된 모든 파일 및 시스템 변경 삭제

복구

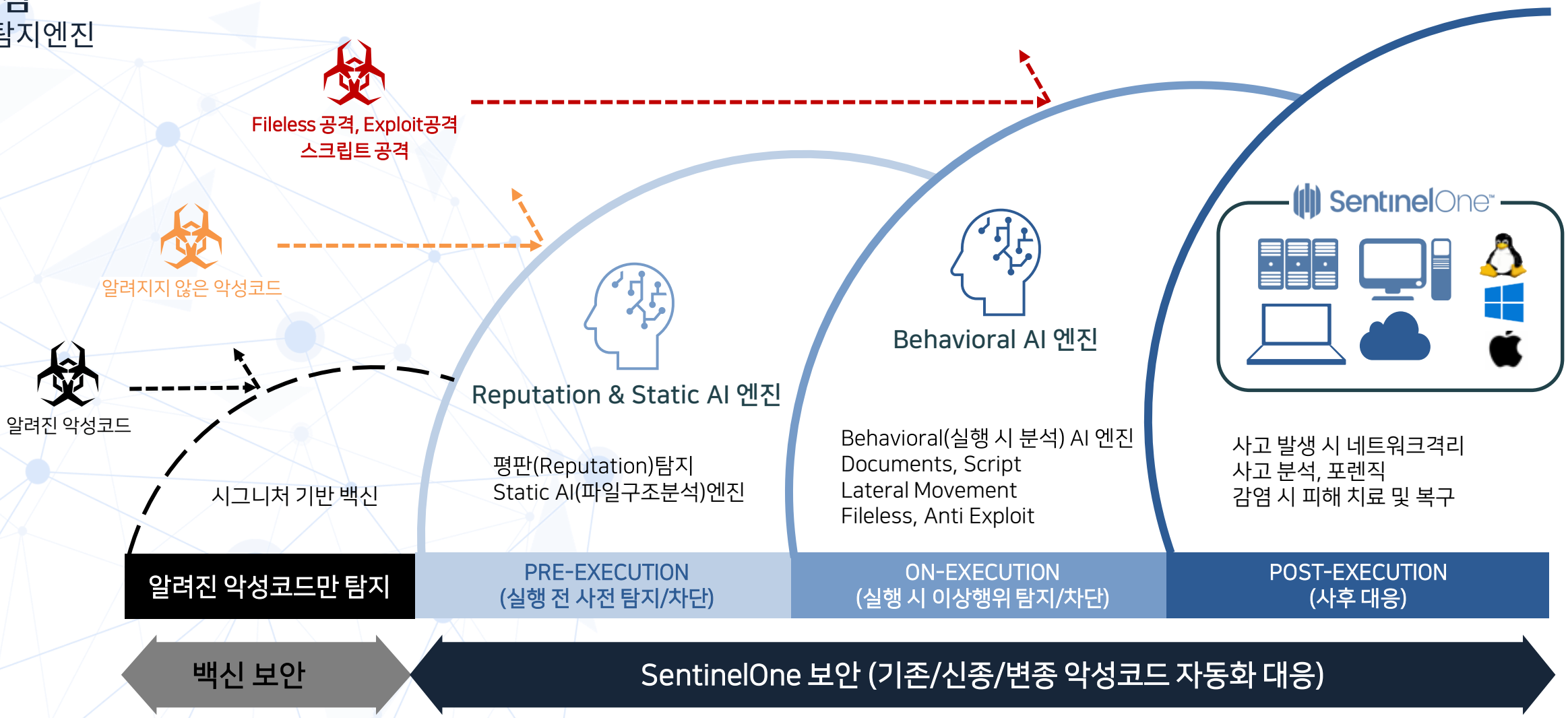
위협 요소로 인해 변경된 파일 및 구성 복원

04.
SentinelOne 범위



05. SentinelOne 장점
- 탐지엔진

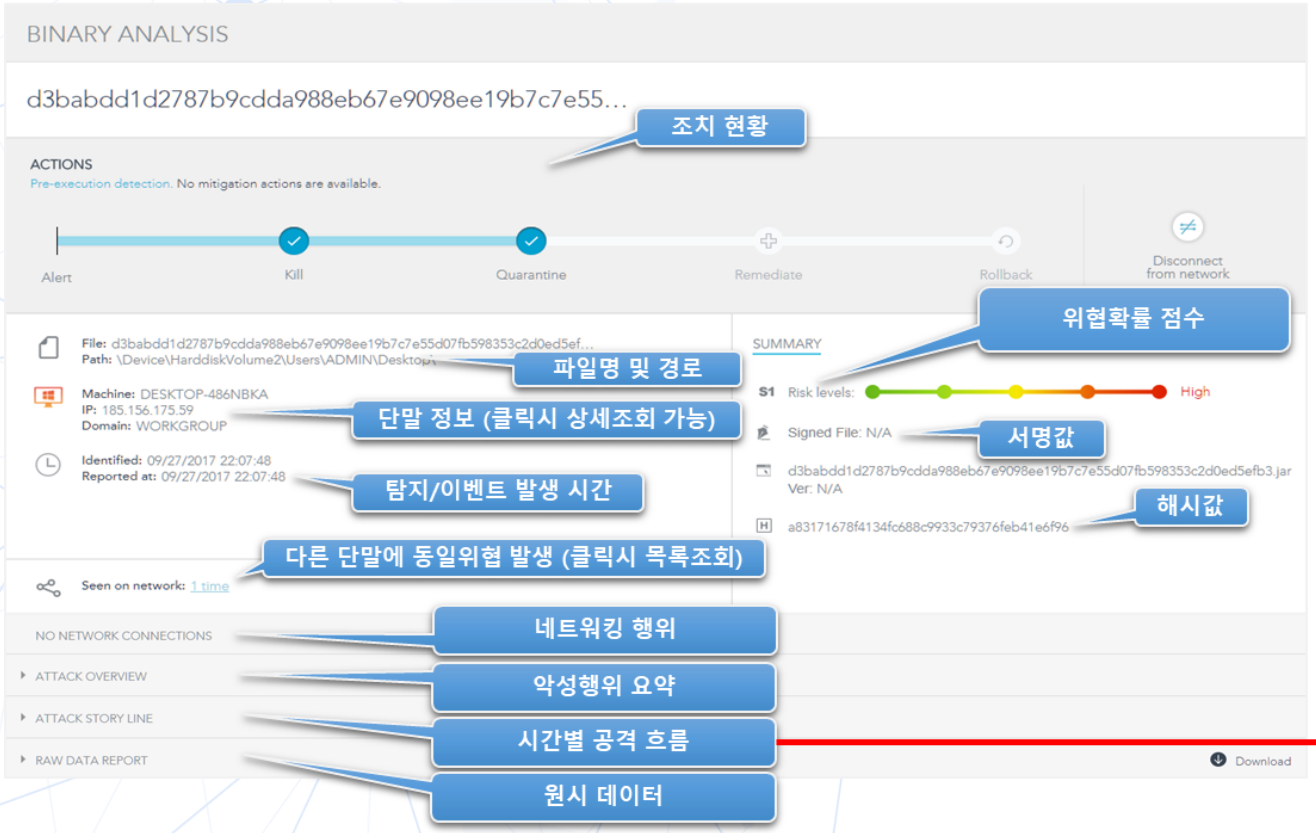
기존 백신은 알려진 악성코드만 탐지하여, 신종/변종 악성코드 감염에 대해 보호하지 못하였으나,
SentinelOne의 강력한 **기존/신종/변종/악성코드 자동화 대응**으로 다양한 공격 및 위험요인으로부터 보호할 수 있습니다.

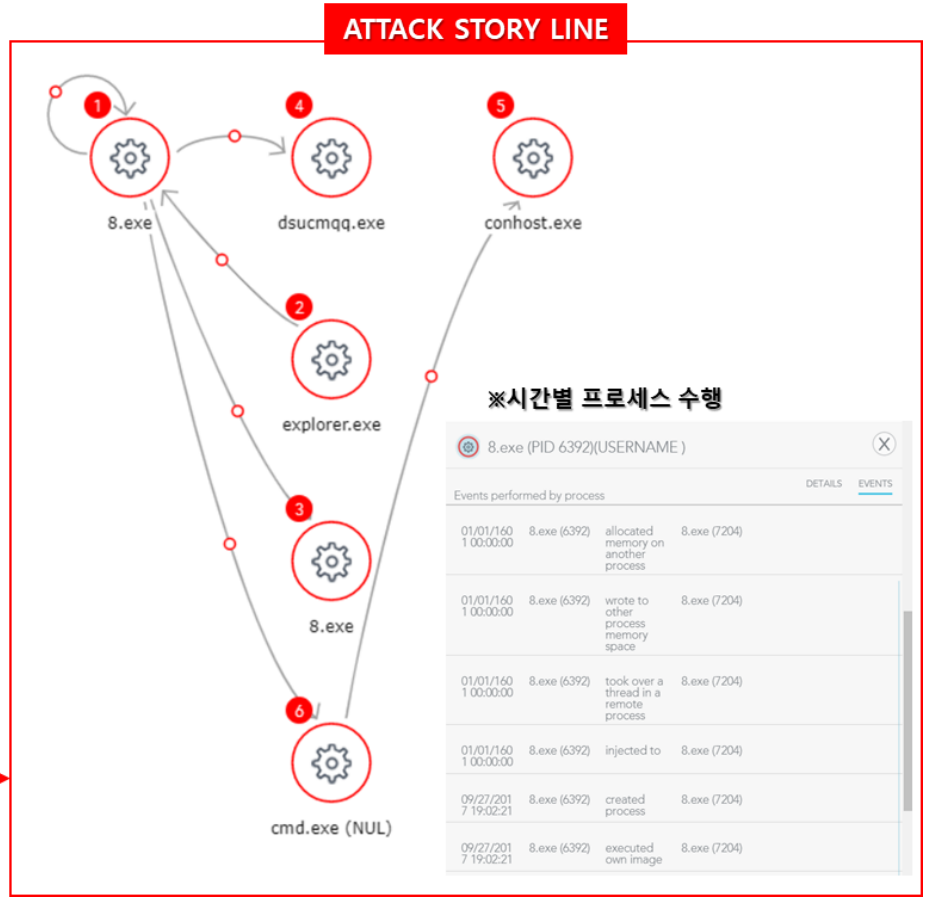


05. SentinelOne 장점

- 효율적인 사고 분석 및 원격 조치

기존에 수동적인 분석으로 원인파악이 장기간 소요 되어 2차 피해 발생 우려되었으나, **직관적인 화면을 제공하여 즉각적인 원인파악 및 조치** 할 수 있습니다.





05. SentinelOne 장점

- 원격대응으로 실시간 조치/관리

SentinelOne 의 원격 관리 기능(네트워크 격리, 재부팅, 복구 등)을 통하여 **Endpoint의 장애나 발생 위협에 대해 신속하게 대응**할 수 있기 때문에 업무를 효율적으로 수행할 수 있습니다.

- 네트워크 격리
- 파일 전수검사
- 파일/분석로그 수집
- 취약한 프로그램 확인
- PC 종료
- 재부팅
- 원격 명령(Shell)
- 사용자메시지 보내기

자동 조치 / 원격 대응으로 업무 효율성 증대

05. SentinelOne 장점
- 사고 후 조치대응 (복구 기능)

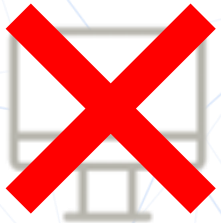
- Endpoint 의 랜섬웨어 감염 시 복구 기술 특허
- 윈도우 OS의 VSS(Volume Shadow Copy Service) 를 활용하여 주기적 백업 수행(환경에 따라 변경 가능)
- 랜섬웨어 감염 이전 시점으로 안전하게 복구(Rollback)

랜섬웨어 감염

데이터 암호화

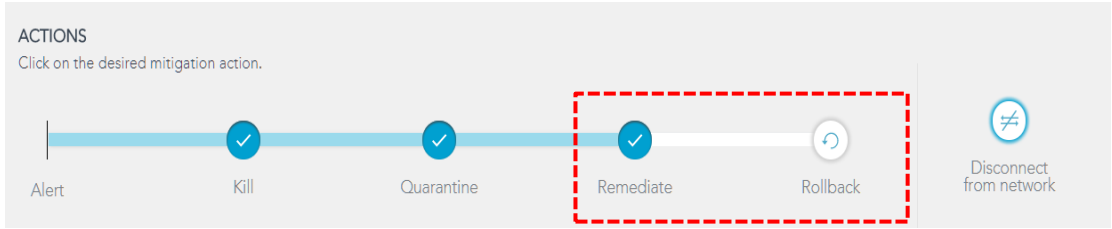
SentinelOne

기존 보안 장비



사용 불가로 인한 포맷

랜섬웨어 감염 전 백업(VSS) 이미지로 복구(Remediate & Rollback)



- Remediate : 악성코드에 의해 변경된 파일/레지스트리/설정 원상 복구
- Rollback : 윈도우 VSS를 이용하여 랜섬웨어 감염 이전 시점으로 복구

05. SentinelOne 장점

- 복구 기능

Threat Status: MITIGATED | AI Confidence Level: MALICIOUS | Analyst Verdict: True Positive | Incident Status: Unresolved

Mitigation Actions taken: KILLED 83/83 | QUARANTINED 53/53 | REMEDIATED 13114/13114 | ROLLED BACK 1212/1218

700 밀리초 이내에 **53개의** 파일을 성공적으로 격리했습니다 .
CSV 보고서 다운로드

31 초 이내에 **13114개의** 위협 생성을 성공적으로 수정 **했습니다** .
CSV 보고서 다운로드

2 시간 이내에 1212개의 위협 변경 사항을 성공적으로 롤백했습니다 .
CSV 보고서 다운로드

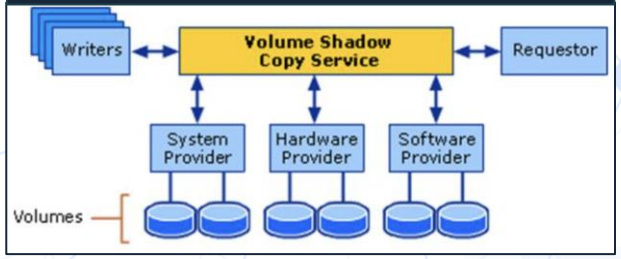
Rebooting
(스냅샷 Ⅰ 생성)

4시간 경과
(스냅샷 Ⅱ 생성)

4시간 경과
(스냅샷 Ⅲ 생성)

악성코드로 인한 데이터 손상시
(스냅샷 2 데이터를 이용하여 롤백 수행)

Windows Volume Shadow Service 활용

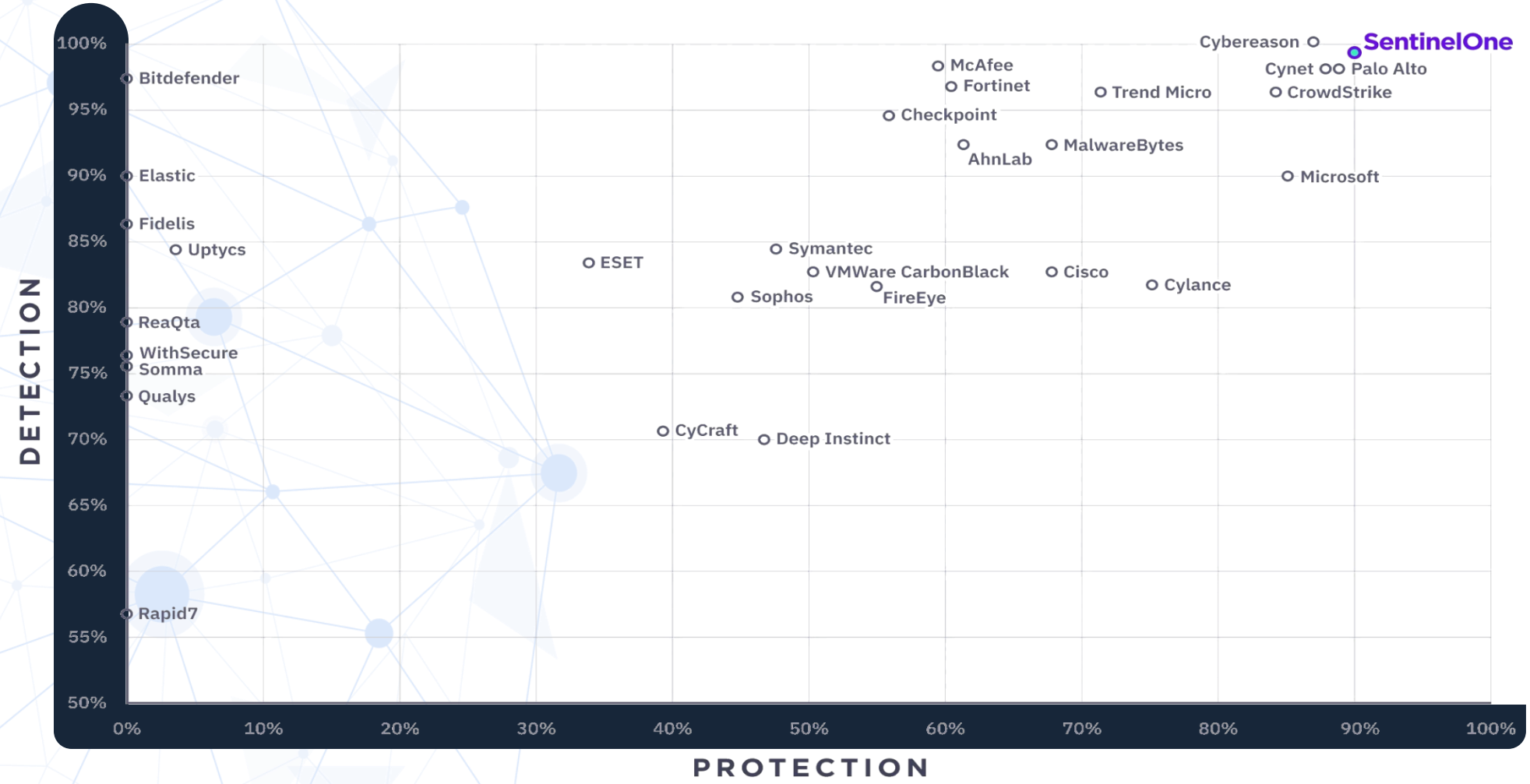


06. SentinelOne 특장점 요약

다양한 탐지엔진	손쉬운 운영	방화벽, Device제어	다양한 OS 지원
Reputation	Story Line(관련행위)	PC 방화벽 제어	Windows XP 제외 모든 OS
Static AI	감염 시 원 클릭 조치	감염 시 Network 격리	Windows 11
Behavioral AI	간편한 Agent 업데이트	블루투스 제어	맥 OS
Documents, Scripts	부서 별 다른 정책	USB 제어	리눅스
Lateral Movement	간편한 설치 / 제거	취약한 App 조회	모든 서버
Anti Exploit / Fileless	사용자 부담X	Remote shell 기능 지원	아마존 리눅스
Application Control	원격 조치		
Detect Interactive Threat	하나의 관리콘솔		

07.
외부 평판

MITRE 2022 Results : Overall Detection & Protection



08.
시스템 최소 요구사양

OS	유형	상세 버전
Windows	Windows Server Core	2012, 2016 (requires 3.0 or later), 2019
	Windows Server	2019, 2016, 2012 R2, 2012, 2008 R2 SP1
	Windows Storage Server	2016, 2012 R2, 2012
	Windows Client	32/64-bit ※ Windows 7 for up to 3 years after the Microsoft End Of Life declaration Windows 11, Monterey 지원
	Editions	Home, Pro, Pro for Workstations, Enterprise, Education, Pro Education, Enterprise LTSC, Embedded Supported without Agent UI: Windows 10 IoT Enterprise *Not supported: Mobile, Windows 10 IoT Core*
macOS	High Sierra,	macOS 10.13
	Mojave	macOS 10.14
	Catalina	macOS 10.15.1, 10.15.2, 10.15.3
	BigSur	macOS 11.x
	Monterey	macOS 12.x

OS	유형	상세 버전
Linux	CentOS	6.4+, 7.x, 8.4
	Red Hat Enterprise Linux (RHEL)	6.4+, 7.x, 8.4
	Ubuntu	14.04, 16.04, 18.04, 19.04, 19.10 20.04
	Oracle	6.9, 6.10, 7.x, 8.4
	Amazon	2017.03, 2018.03, AMI 2
	SUSE Linux Enterprise Server	12.x, 15.x
	Fedora	25, 26, 27, 28, 29, 30, 33
	Debian	8, 9, 10
	Virtuozzo	7
	Scientific Linux	6, 7

“

감사합니다.

영업/일반 문의 **02-2105-4400**

평일 9:00 ~ 18:00 (주말, 공휴일 휴무)

기술/장애 문의 **02-2105-4455, 02-2105-4400**

24시간

주소 : 서울특별시 서초구 서초대로 255 2층 (고덕빌딩) | 사업자등록번호 : 215-87-70318 | 통신판매업신고번호 : 제 2019-서울서초-2940호 | 영업 문의 : 02-2105-4400 | 기술문의 : 02-2105-4455