DOOSAN

cybereason

온프레미스 환경에서도 강력한 보안을 구현하는 사이버리즌

사이버리즌의 독보적인 시장 입지

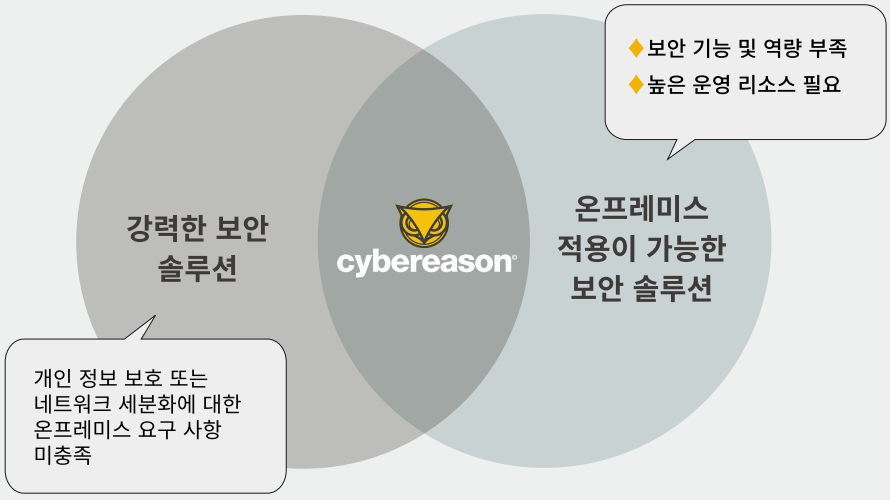
레거시 보안으로 위기에 처한 기업들

규정과 업계 표준 등 다양한 이유로 퍼블릭 클라우드 인프라 사용이 제한되는 조직의 보안팀은 대부분 레거시 엔드포인트(Endpoint) 보안 기술을 사용하고 있습니다. 그러나 레거시 기술은 지능형 보안 위협이 등장하기 이전에 만들어진 과거 기술로 효율적인 보안 운영에 필요한 최소 요구 사항을 충족하지 못합니다.

복잡하고 새로운 최신 위협에 대응하기 위해서는 효율적인 보안이 필요하며, 이를 구현하기 위해서는 클라우드 인프라가 필요합니다.
하지만 클라우드 인프라 사용이 제한된 조직은 최신 보안 위협을 어떻게 대비할 수 있을까요?

사이버리즌의 독보적인 시장 입지

여러 보안 회사에서 출시하는 보안 솔루션은 강력한 보안 기능을 갖추고 있지만 아래와 같은 한계점 또한 가지고 있습니다.



- 사이버리즌은 더 많은 보안 가치를 제공합니다.
- 어떤 환경에도 EPP 및 EDR의 모든 이점을 구현할 수 있습니다.

보안업계는 오프라인 환경 엔드포인트에 퍼블릭 클라우드와 SaaS(software as a service) 솔루션 적용이 어렵다는 입장입니다. 심지어 대부분의 보안 기업은 온프레미스 보안을 클라우드 퍼스트 전략의 장애물로 여기며 업데이트를 거의 제공하지 않고 있습니다. 결국 온프레미스 보안은 유지보수 기술 수준에 멈춰 있을 수 밖에 없습니다.

사이버리즌 솔루션 특장점

- 프라이빗 및 에어갭(외부 인터넷과 완전히 격리된) 네트워크 환경을 위한 **최신 엔드포인트 보안을 제공합니다.**
- 경고 중심이 아닌 공격 전체 스토리와 상관 관계를 완전히 파악해 **MalOps™으로 차단합니다.**
- 탐지 및 대응 시간을 93% 개선해 **더 빠르게 공격을 식별하고 종료합니다.**
- 해결 방안 추천으로 조사에 소요되는 시간을 최소화하여 **단 몇 분 만에 문제를 해결합니다.**

DOOSAN | 두산디지털이노베이션 | Doosan Digital Innovation | ddi.marketing@doosan.com

최신 기술로 효과적인 온프레미스 보안 구현

많은 기업들이 레거시 엔드포인트 보안을 고수하는 이유는 데이터 경계와 세분화를 명확히하고 중요한 네트워크를 보호하기 위해서 입니다. 하지만 레거시 엔드포인트 보안 적용이 기업 보안의 취약점이 되어서는 안됩니다. 사이버리즌은 엔드포인트 NGAV 및 EDR 솔루션을 포함한 최고 수준의 보안 기술로 온프레미스 및 에어갭 환경에서 최신 위협에 대응합니다.

비즈니스 가치

- 최신 기술로 예방, 탐지 및 대응하여 오탐을 줄이고 랜섬웨어와 같은 사이버 보안 공격으로 중요 오프라인 및 프라이빗 네트워크의 비즈니스가 중단되는 상황을 최소화 합니다.
- 프로세스 자동화와 AI 기반 분석으로 보안 운영 효율성을 개선하고 위협 분류, 조사 및 대응 시간을 단축합니다.
- 보안 기술 격차를 해소해 기업의 모든 보안 분석가가 복잡한 쿼리 작성 없이 공격의 세부 정보를 신속하게 분석할 수 있습니다. 이후 단 한번의 클릭으로 조사부터 영향 받은 장치에 대한 문제 해결까지 진행합니다.
- 100% 오프라인 구축으로 데이터를 간소화하고 인프라 규정을 준수합니다. 즉, 네트워크의 취약성을 노출시킬 수 있는 외부 액세스를 제한하면서 모든 데이터 유지가 가능합니다.
- 간소화된 구축 프로세스로 구축 위험성을 줄이고 가시성을 빠르게 확보합니다.
- 기존 인프라 도구와 통합하여 모니터링, 조사 및 분류를 중앙 집중식으로 관리합니다.

온프레미스 환경에서도 강력한 보안을 구현하는 사이버리즌

사이버리즌의 차세대 안티바이러스(NGAV)는 9개 보안 계층으로 더 뛰어난 방어력을 선보입니다.

사이버리즌은 다계층(Multi-layered) NGAV 접근 방식으로 공격을 방어하는 유일한 보안 플랫폼입니다. 총 9개 계층으로 이루어진 차세대 안티바이러스는 독립적이면서도 상호 보완적인 구성으로 악의적인 공격 행위를 체계적으로 차단합니다.

[1 계층] 엔드포인트 제어
: USB 및 네트워크 무단 연결 차단과 전체 디스크 암호화

USB 저장 장치 및 휴대폰 사용을 제한해 공격 표면을 줄이고 방화벽 정책을 세워 전체 디스크를 암호화합니다.

[2 계층] 멀웨어 차단: 상용화된 멀웨어 차단

위협 인텔리전스 및 휴리스틱(경험) 기반 탐지로 알려진 멀웨어를 차단합니다.

[3 계층] AI 기반 멀웨어 차단: 새로운 멀웨어 차단

AI를 활용해 기업 전체에서 발생하는 악성 행위를 탐지하여 공격자를 추적하고 알려지지 않은 멀웨어까지 차단합니다.

[4 계층] 익스플로잇 차단
: Windows 취약성에 대한 가상 패치(Virtual Patching)

익스플로잇 차단 기술로 엔드포인트가 공격을 받기 전에 미리 차단할 뿐만 아니라 제로데이 취약점을 악용한 익스플로잇 공격까지 방어합니다.

[5 계층] 행위 기반 문서 보호: 악성 매크로 차단

사용자가 문서를 열 때 문서를 분석하여 매크로 등 악성 코드가 실행되지 않도록 보호합니다.

[6 계층] 파일리스 멀웨어 차단
: 메모리 내 명령어 및 스크립트 기반 공격 차단

Powershell 엔진, .Net, JScript 및 VBScript의 동작을 검사하여 공격자가 악성 코드를 메모리에 삽입하는 것을 차단합니다.

[7 계층] 행위 기반 실행 차단: 리빙 오프 더 랜드(LOL) 기법 차단

사이버리즌은 고객의 행위에서 수집된 정보를 활용하여 킬 체인에서 합법적인 실행파일을 악용해 위장하는 LOLBins 공격을 탐지하고 차단합니다.

[8 계층] 악성 페이로드 차단
: Cobalt Strike, Emotet과 같은 악성 페이로드 예방

메모리에 축적되는 코드를 모니터링하고 BSA(Binary Similarity Analysis) 기술 및 유사성 분석으로 Cobalt Strike Beacon 또는 Metasploit Meterpreter와 같은 알려진 악성 페이로드의 특성을 보이는 코드를 식별하고 차단합니다.

[9계층] 랜섬웨어 사전 예방(PRP): 암호화 차단 및 파일 복원
*PRP: Predictive Ransomware Protection

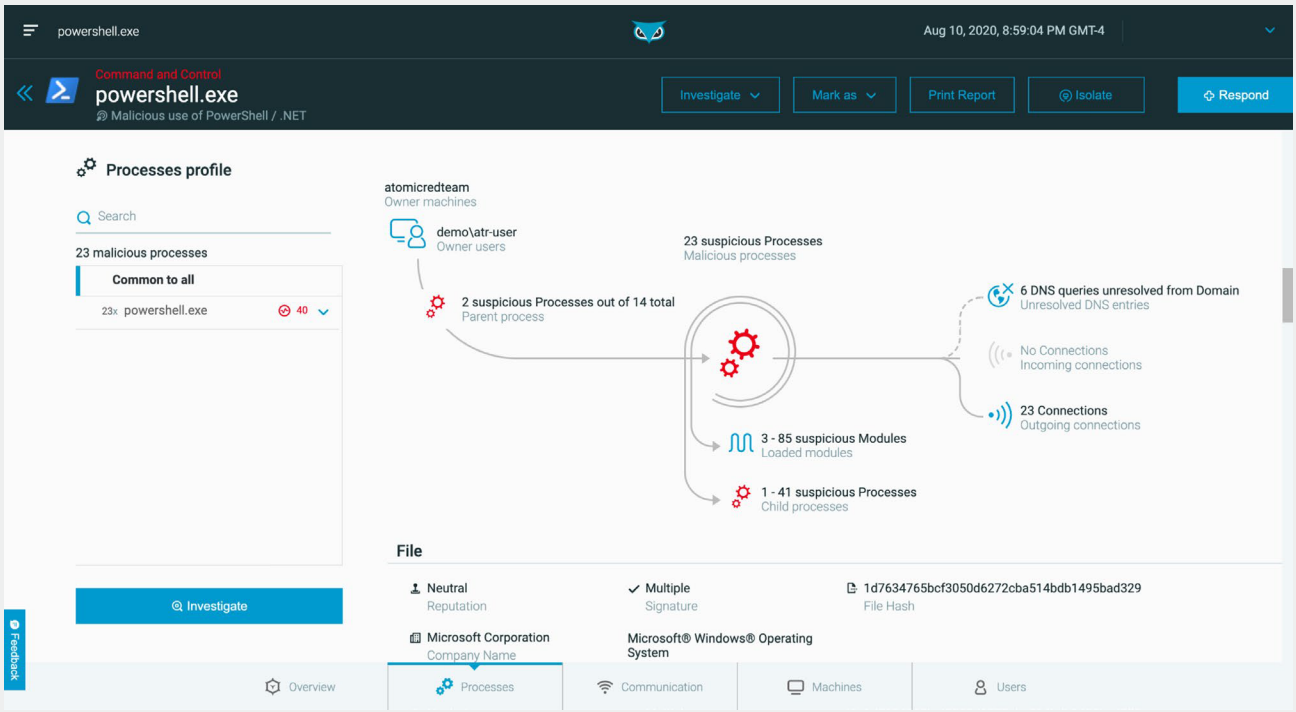
앞선 8개의 계층들로 대부분의 랜섬웨어를 차단한 후 가장 정교한 랜섬웨어 공격 행위는 마지막 보호 계층에서 식별해 보안을 더욱 강화합니다.

필요한 경우, 빠른 복구 기능으로 암호화된 특정 파일을 손상되지 않은 상태로 롤백(되돌리기)할 수 있으며 사이버리즌 PRP는 독점 특허 기술로 랜섬웨어 행위를 실시간으로 식별, 예방 및 차단합니다.

온프레미스 환경에서도 강력한 보안을 구현하는 사이버리즌

AI 기반 온프레미스 엔드포인트 탐지 및 대응(EDR)으로 악성 공격을 예측하고 차단합니다.

사이버리즌 온프레미스 EDR은 악성 행위가 시작되기 전에 사전에 인식하고 노출시켜 빠르게 종식시킵니다. AI에 기반한 사이버리즌 보안은 악의적인 행위를 노출시켜 차단하도록 설계되었으며 하나의 에이전트, 콘솔, 팀으로 모든 엔드포인트를 방어합니다.



MalOp는 경고 알림 뿐만 아니라 공격 스토리의 전체적인 맥락을 가시화합니다. 사이버리즌은 전체적인 스토리 파악으로 공격을 예측하는 정보, 빠른 해결 속도, 공격 차단에 도움되는 인사이트를 제공합니다.

■ 정확한 공격 차단

자동화와 단 한번의 클릭으로 시스템 전반에서 일어나는 공격을 종식시켜 보안 분석의 생산성을 높입니다.

■ 혁신적인 속도

공격자보다 더 빠르게 분석 및 대응하여 단 몇 분 만에 상용화된 공격, 표적 위협 뿐만 아니라 새로운 위협까지 제거합니다.

■ 포괄적인 가시성 확보

엔드포인트, 디바이스, 사용자 ID, 애플리케이션 및 클라우드 등 공격 영향을 받은 근본적인 원인을 시작으로 전체 공격 스토리를 가시화해 악의적인 작업을 추적하고 종료합니다.

온프레미스 환경에서도 강력한 보안을 구현하는 사이버리즌

사이버리즌 온프레미스 구축 요건

사이버리즌 온프레미스 서버 설치는 VMware vSphere ESXi 버전 6.5 이상을 지원하며,
온프레미스, 프라이빗 클라우드 및 로컬 데이터 센터에 대해 다양한 옵션을 선택할 수 있습니다.

문의: ddi.marketing@doosan.com

사이버리즌 온프레미스 엔드포인트 센서 버전 23.1 적용 가능 운영체제

WINDOWS	MAC	LINUX
Windows XP*	Yosemite (10.10)*	Amazon Linux (All versions before 2017)*
Windows Vista*	El Capitan (10.11)*	CentOS 6, 7, 8
Windows 7 SP1	macOS Sierra (10.12)	RedHat Enterprise Linux 6, 7, 8
Windows 8	macOS High Sierra (10.13)	Oracle Linux 6, 7, 8
Windows 8.1	macOS Mojave (10.14)	Debian 8, 9, 10
Windows 10	macOS Catalina (10.15)	Amazon Linux AMI 2017.03
Windows 11, 21, H2	macOS BigSur 11	Amazon Linux 2
Windows Server 2003*	macOS Monterey 12	Ubuntu 14 LTS, 16 LTS, 18.04 LTS
Windows Server 2008*		Ubuntu 20.04 LTS, 20.10
Windows Server 2019		
Windows Server 2016		
Windows Server 2012 R2		
Windows Server 2012		
Windows Server 2008 R2 SP1		
Windows Server 2022		

두산디지털이노베이션

두산디지털이노베이션은
사이버리즌의 APAC 대표
파트너사로 엔드포인트, 클라우드
및 전체 엔터프라이즈 에코시스템
사이버 보안에 앞장서고 있습니다.

사이버리즌 보안 플랫폼은 선제적 방어,
탐지 및 대응으로 현대 랜섬웨어 및
고도화된 공격을 종식시킵니다.
사이버리즌 MalOp™은 공격 영향을
받는 모든 장치, 사용자 및 시스템에
전체 맥락이 포함된 공격 정보를
정확하고 빠르게 제공합니다.

- DDI 사이버보안 바로가기
- DDI에 문의하기 바로가기