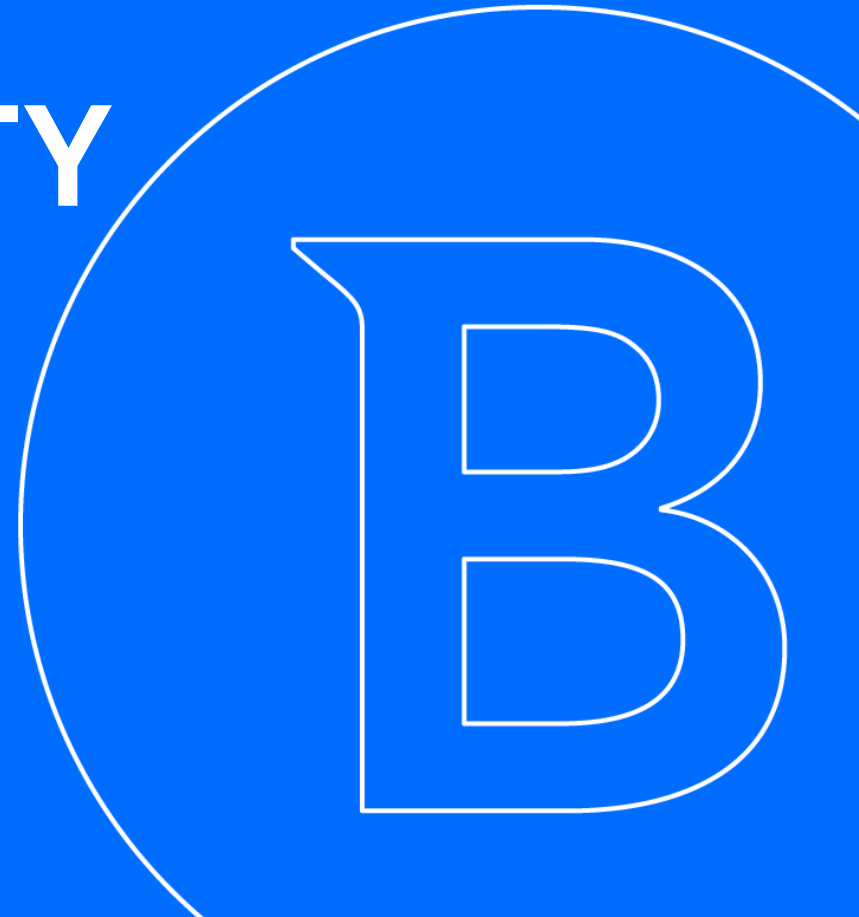


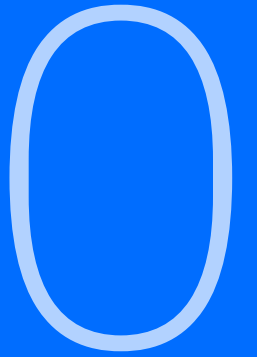
Bitdefender[®]
Cybersecurity
Built For Resilience

비트디펜더 그라비티존 시큐리티 제품 소개서

GRAVITYZONE SECURITY

For Business





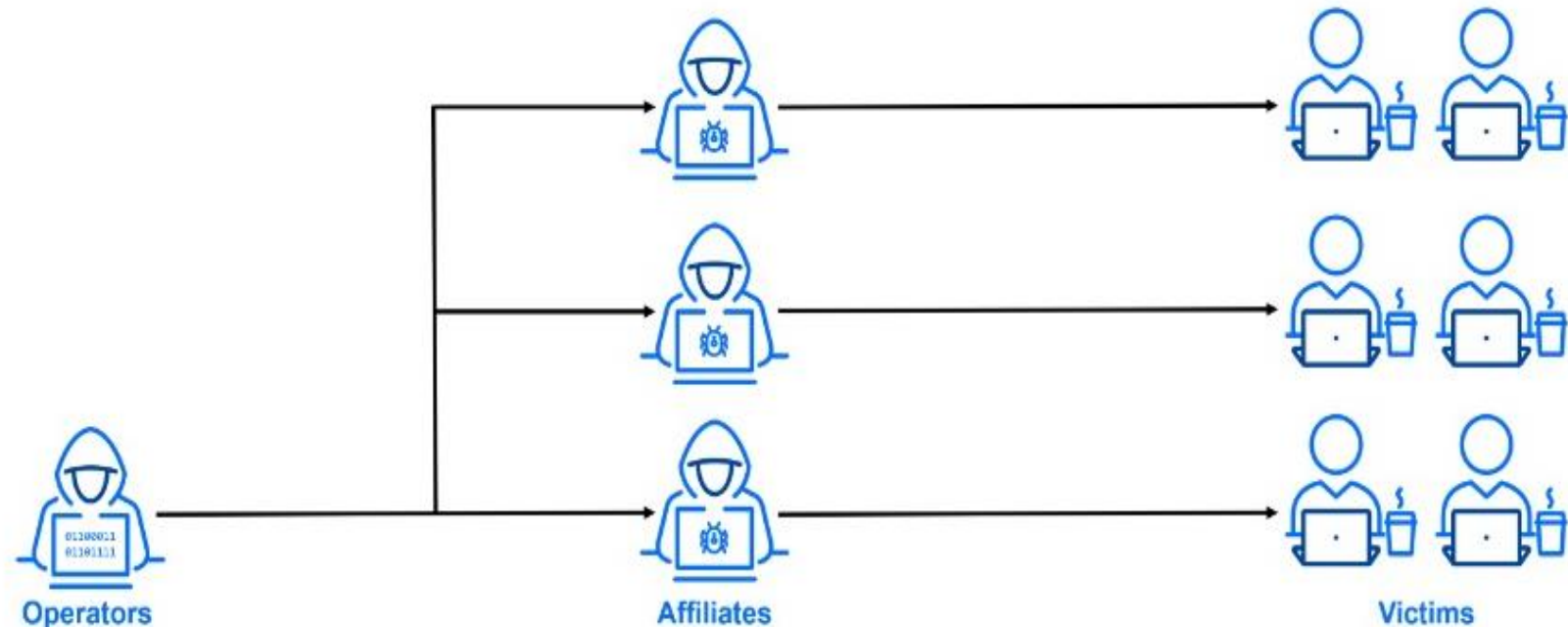
● 보안 백서

랜섬웨어 차단: Bitdefender를 사용한 공격 벡터 및 완화 전략에 대한 기술 심층 분석

RaaS(Ransomware-as-a-Service) 모델의 도입으로 가속화된 랜섬웨어의 진화는 방어 전략에 대한 지속적인 재평가를 필요로 합니다. 이 백서는 최신 랜섬웨어 킬 체인을 분석하여 각 단계에서 공격자의 방법을 노출합니다. RaaS가 공격자의 행동을 어떻게 변화시켰는지, 그리고 다계층 심층 방어 아키텍처가 랜섬웨어 위협에 대처하는 가장 효과적인 방법인 이유를 살펴보겠습니다.

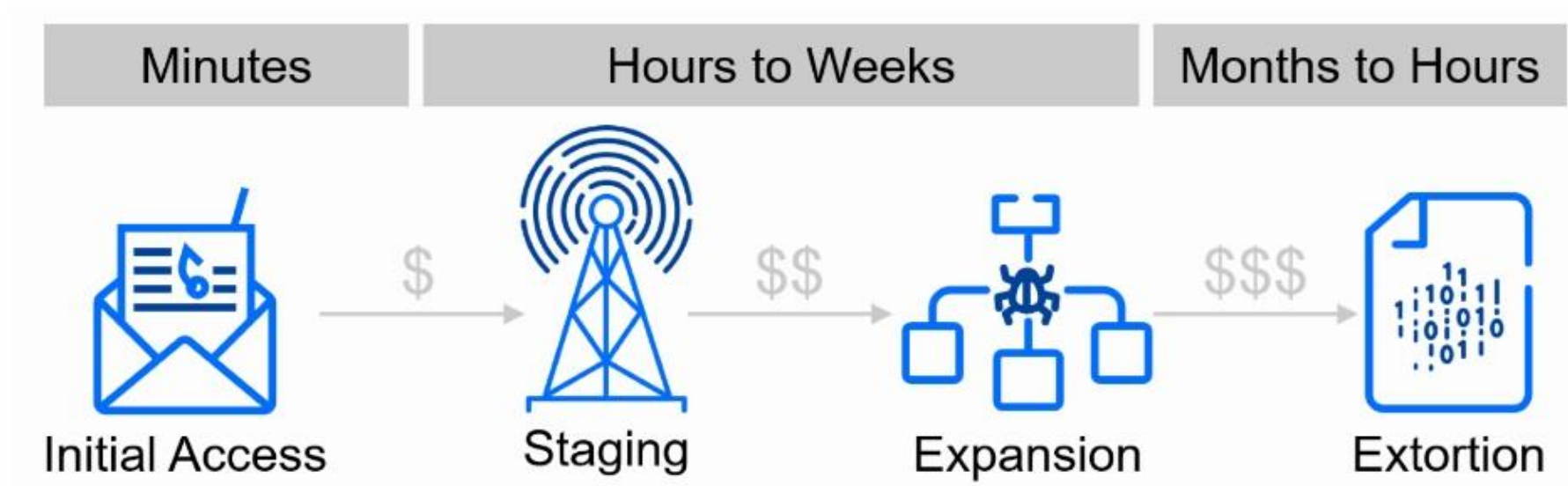
랜섬웨어 플랫폼 제공자 : 랜섬웨어 코드 구축 및 인프라 관리와 피해 복구 비용등을 협상하는 운영자

공격자 : 초기 액세스에서 랜섬웨어 배포까지 실제 해킹을 수행하는 공격자

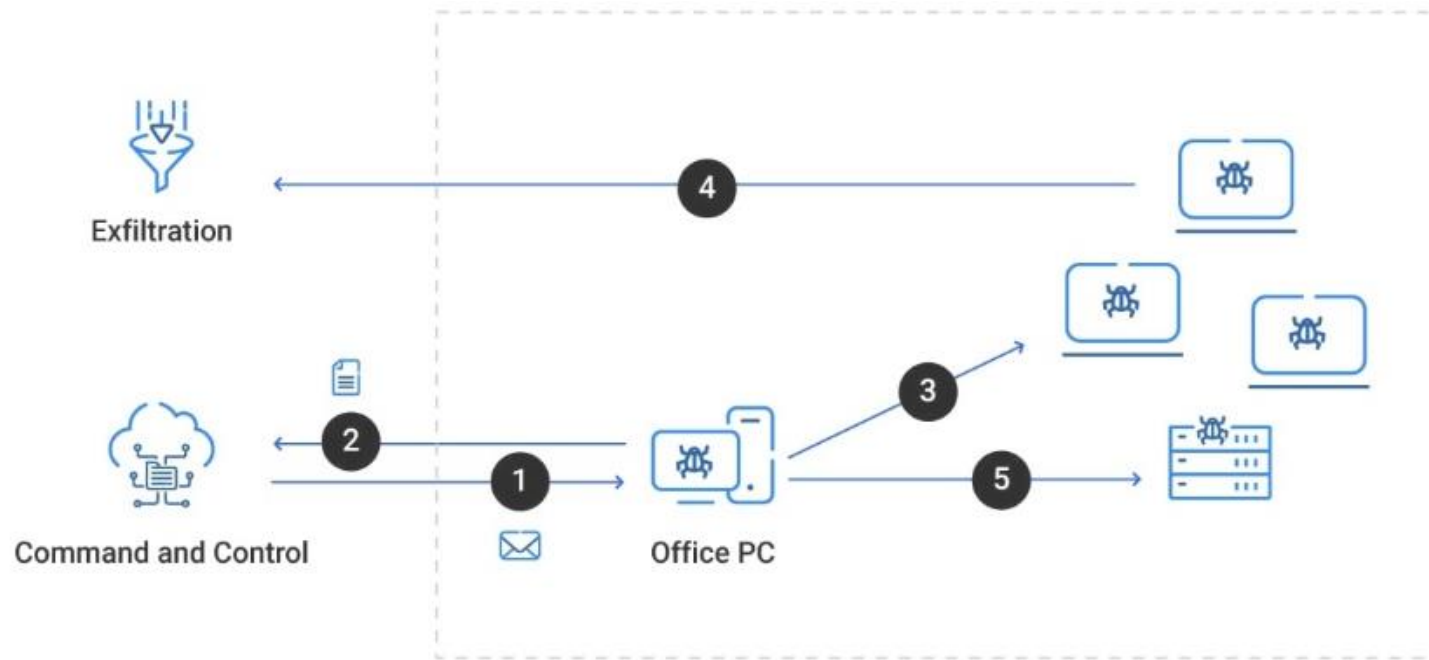


랜섬웨어의 끊임없는 진화로 다양한 규모의 기관에서 피해가 발생 할 수 있으며 확장 공급망을 이용하여 액세스 권한을 잠재적으로 탈취하는 교묘한 수법을 활용으로 인해 유연한 방어 전략이 필수적으로 요구되고 있습니다.

단일 시스템을 타겟으로 하는 공격이 아닌 네트워크를 대상으로 하는 지속적이고 치밀한 공격 작업



랜섬웨어 공격의 여러 단계를 이해하면 공격을 완전히 차단하거나 발생하는 동안 탐지 및 대응할 수 있는 기회를 식별 할 수 있습니다.



1

피싱 이메일

2

리버스 셸
(Revers Shell)

3

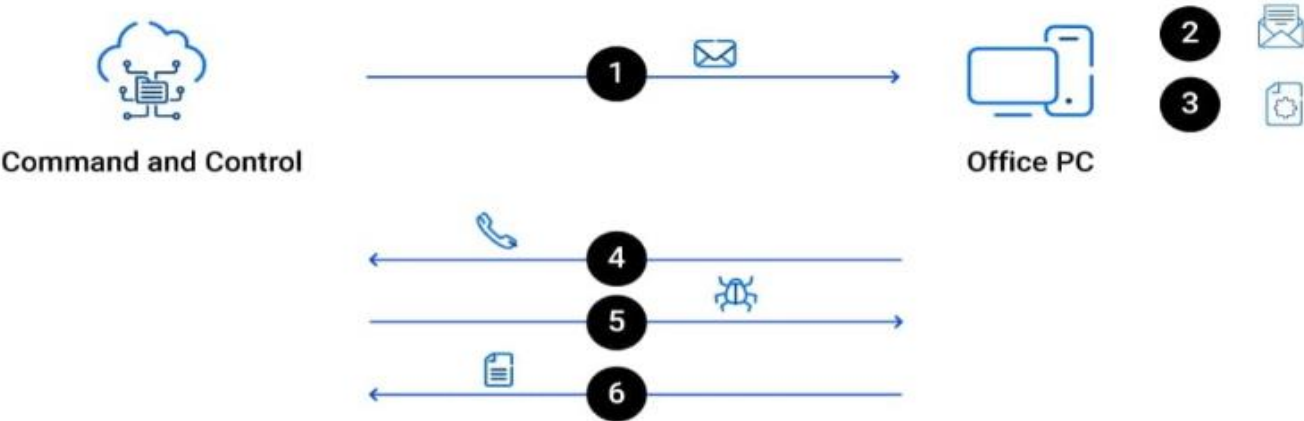
횡적 이동
(Lateral Movement)

4

데이터 유출

5

랜섬웨어 배포



직접 공격 방식 절차



스피어피싱과 같은 표적 수법을 사용하여 수신자를 속이거나 악성 URL, 감염된 첨부 파일을 통해 공격을 하는 단순하지만 효과적인 전술로 LLM기술에 발전으로 더 교묘해진 방법에 피해가 발생 할 수 있습니다.

Initial Access

Staging

Expansion

Extortion

공격 절차

1

더 많은 시스템
액세스 시도

2

권한에 대한 지속성을
유지하기 위한 매커니즘 설정

3

익스플로잇을 통한
제어권 탈취 시도

4

다양한 공격 시도에
대한 흔적 지우기

최초 네트워크 접근 후 다양한 인프라 및 환경 요소를 통한 영역 장악 시도의 중점을 두고 더 큰 위협의 도구를 사용

대응 방법

1

네트워크 분리 및
그룹 세그먼트 체계화

2

위협 이벤트 및 의심스러운
이벤트 검토 및 위협 헌팅 수행

3

중요 시스템에 대한
권한 관리 및 액세스 제어 관리

4

로깅 활성화 및
데이터 기록에 대한 점검



초기 액세스 권한을 획득 후 다양한 작업을 시도하여 공격을 고도화 하고 확장하는 단계

1

제어권 장악

관리 계정 및 손상된 도메인
컨트롤러, 하이퍼 바이저 등

2

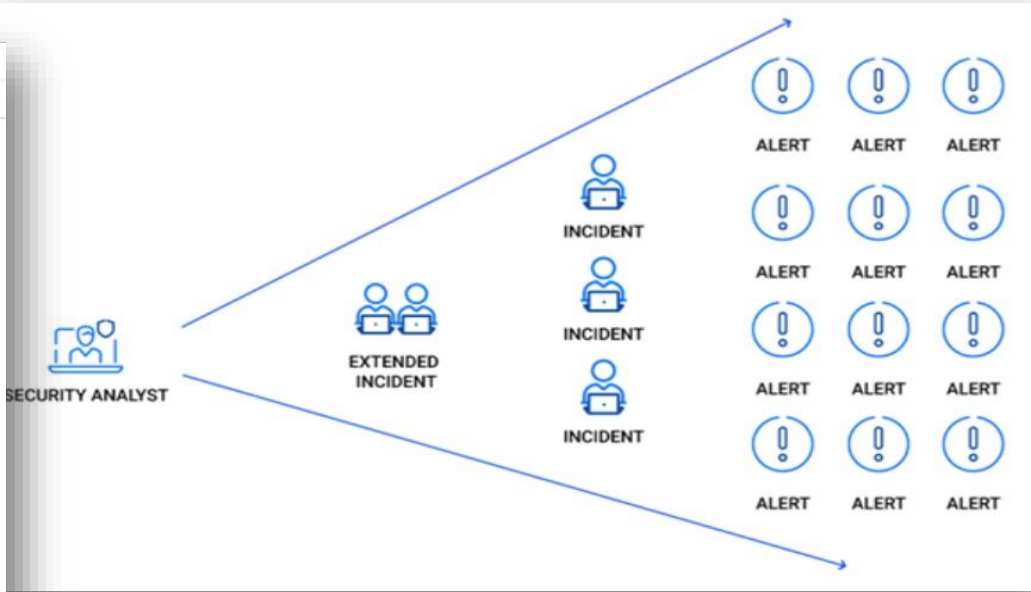
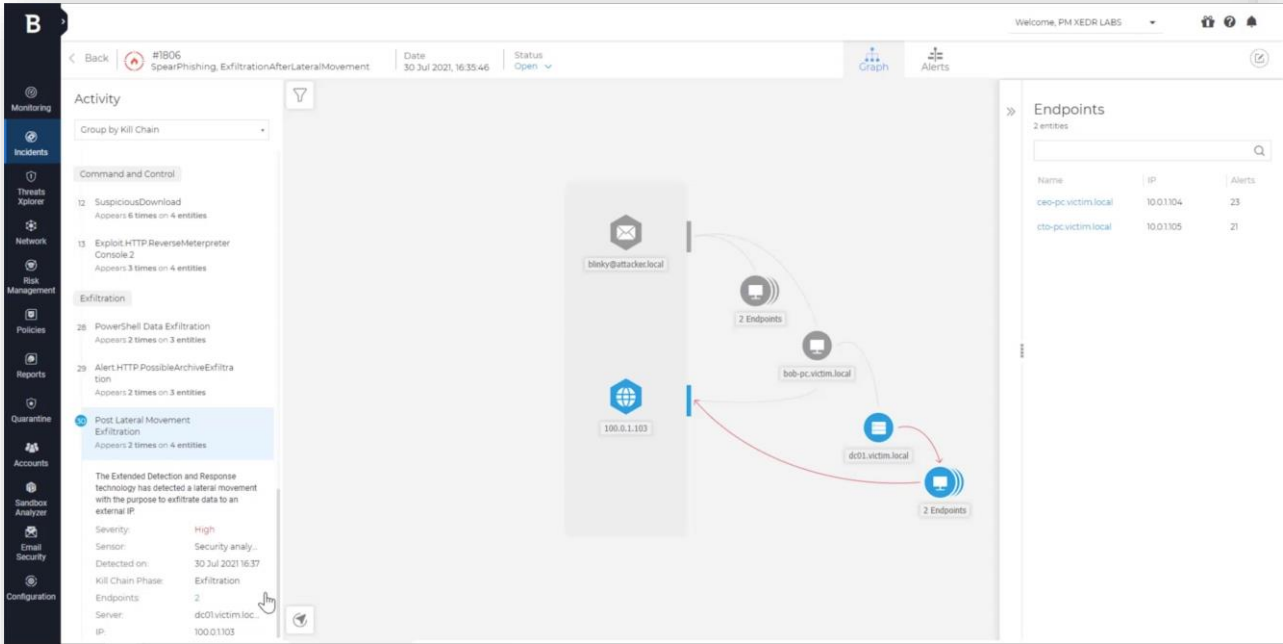
유출 데이터 파악

개인 정보 / 지적 재산 / 기밀 정보 등

3

방어 평가

대응되고 있는 사이버
보안 상태에 대한 정보 수집





대부분 이 단계에서 데이터 유출 또는 랜섬웨어 배포 등이 이루어지는 등 대규모 피해가 발생 할 수 있습니다.

1

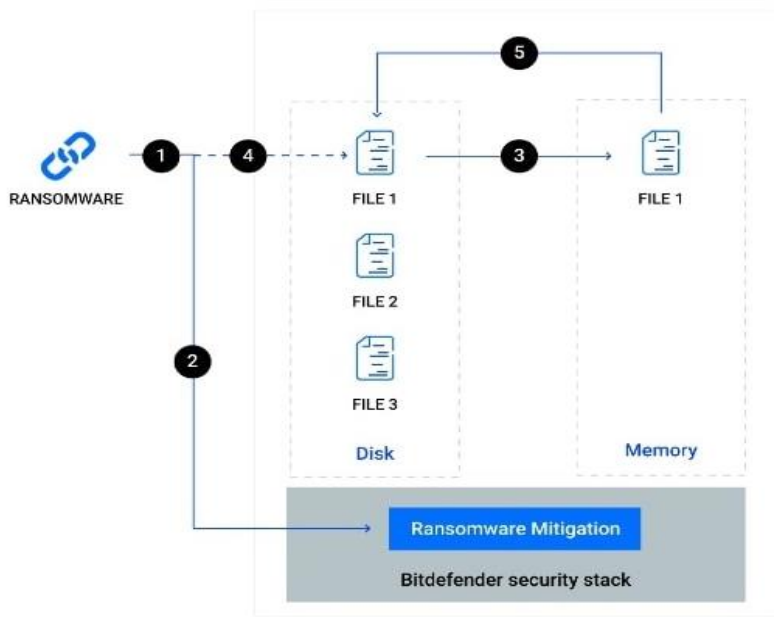
FTP 프로토콜 또는 공용 클라우드 스토리지를 사용해 데이터 전송

2

탐지 최소화를 위해 작은 배치 형태로 반출하여 초기 대응이 어려울 수 있음

3

원격관리 도구를 사용하여 랜섬웨어 배포를 통한 파일 암호화 처리



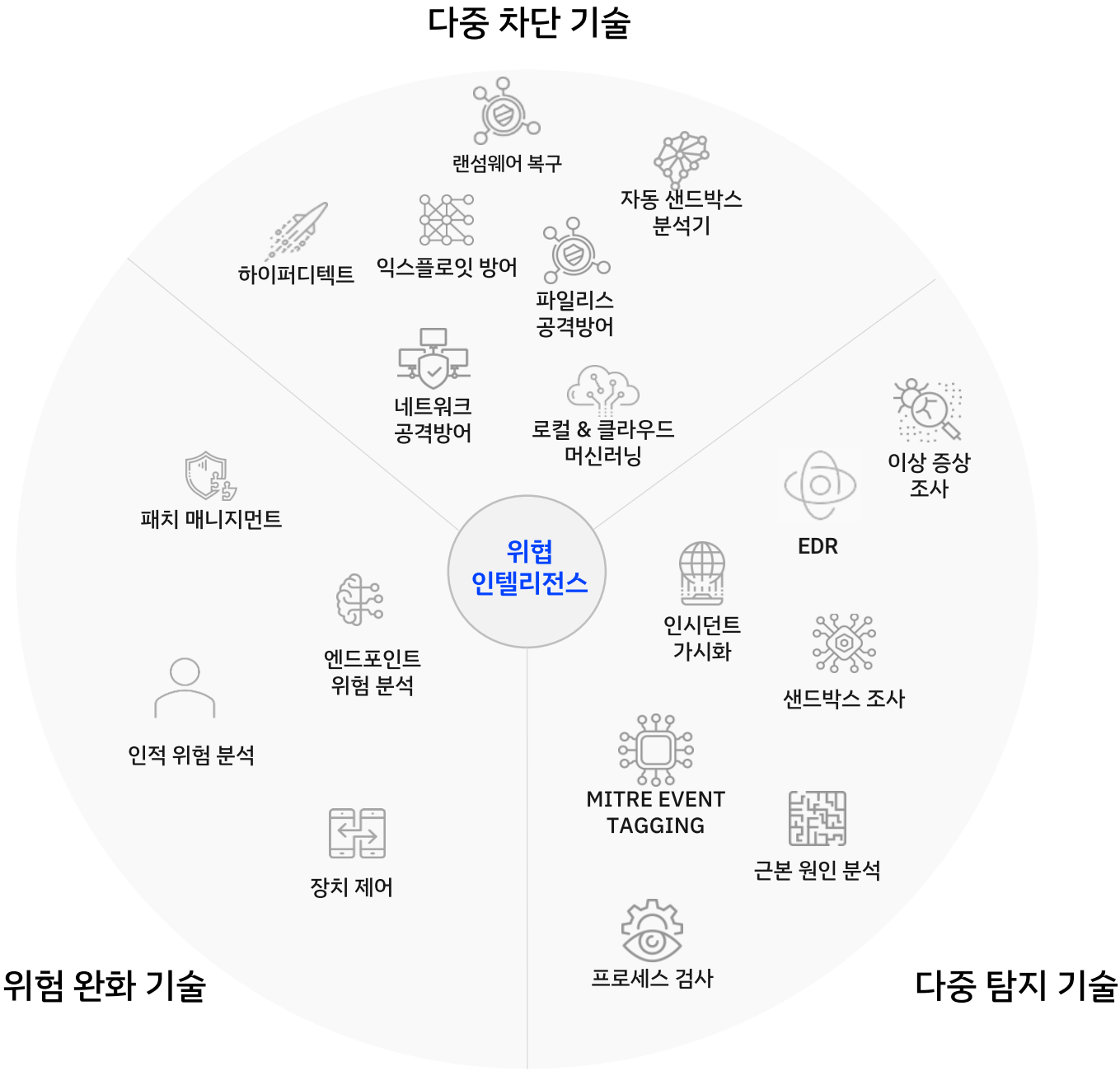
대응 방법

1. 파일 암호화 시도
2. 요청을 가로채고 알고리즘이 랜섬웨어 유무를 감시
3. 가능성이 높은 경우 파일의 인메모리 백업 생성
4. 랜섬웨어 암호화 시도
5. 원본 파일은 인메모리 백업 복사본을 사용하여 복구



Ransomware Prevention

Gravityzone AntiRansome 플랫폼	
대응 기술	상세 내용
다중 차단 기술	AV / 익스플로잇 / 네트워크 공격 / 머신 러닝 / 파일리스
다중 탐지 기술	EDR / XDR / 샌드박스
적응형 방어 기술	ATC / 프로세스 감시
위험 완화 기술	ERA / 콘텐츠 제어 / 패치관리



AGENDA

1

- 회사 소개

About Bitdefender

2

- 제품 소개

GravityZone 제품 소개

GravityZone 라인업

3

- 기능 및 특징점

GravityZone EPP&EDR

GravityZone Cloud

GravityZone Mobile

4

- 수상

평가

수상

1

● 회사 소개

ABOUT BITDEFENDER

Global Leader in Cybersecurity Software

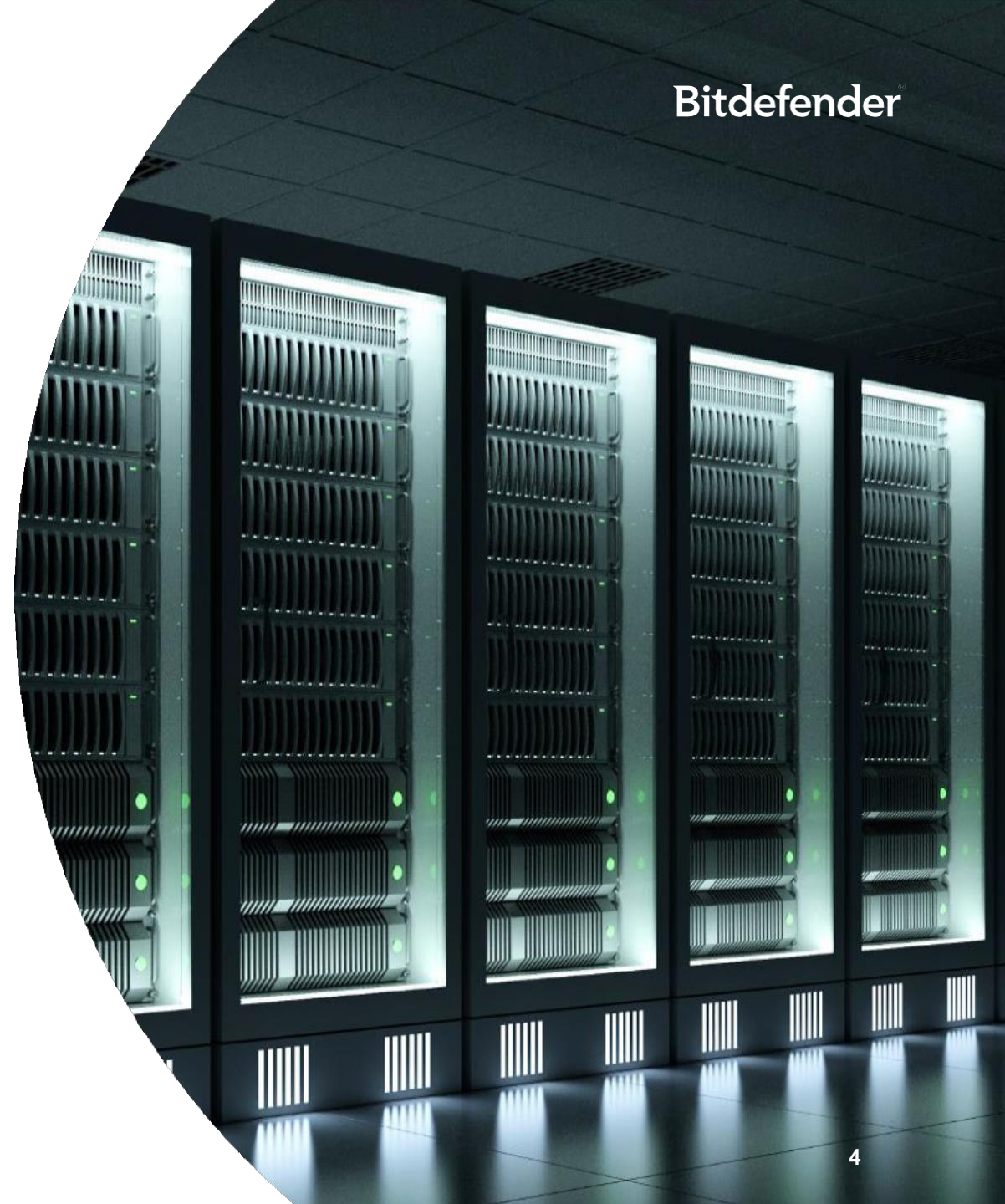
세계적인 사이버 보안 회사 비트디펜더

@endpoint @network @cloud

1600+ 전 세계 임직원
800+ R&D 기술지원

20K+ 전 세계 비즈니스 파트너
150+ OEM 파트너

전 세계 보안 솔루션의 38% 이상 비트디펜더 기술 사용



2

● 제 품 소 개

GravityZone?

GravityZone 제품 소개

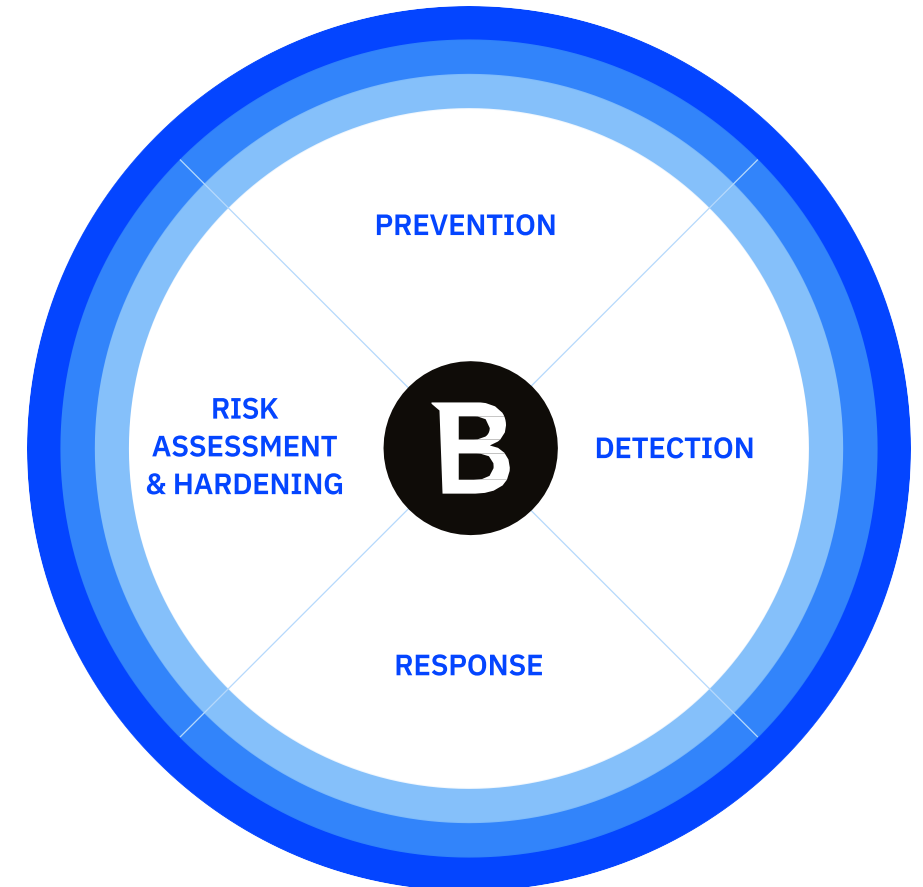
GravityZone 라인업

Bitdefender GravityZone

Unified Prevention, Detection & Response Platform

단일화되고 간편한 관리를 통해 엔드포인트, 생산성 앱, 네트워크 및 클라우드 환경 전반을 지원하는 보안 솔루션

- 페더급 에이전트 기반을 통해 유연한 운영(Windows, Linux, Mac)
- 단일 설치본 제공으로 멀티 인프라 적용(물리적, 가상 엔드포인트, 컨테이너, 클라우드)
- 확장 센서를 통해 엔드포인트를 넘어 탐지 및 대응을 확장
- 엔드포인트 보호 플랫폼 중 업계 최고의 예방 및 탐지
- 단일 에이전트를 통해 풀스택 EPP/EDR 기능 제공
- 인프라 전반에 걸친 센서 확장을 통해 대응 범위 확대
- 클라우드 보안 (CWS)와 클라우드 형태 관리 (CSPM)을 모두 통합
- 추가 설치가 필요하지 않은 확장 가능한 Add On 제공



Bitdefender GravityZone Blueprint

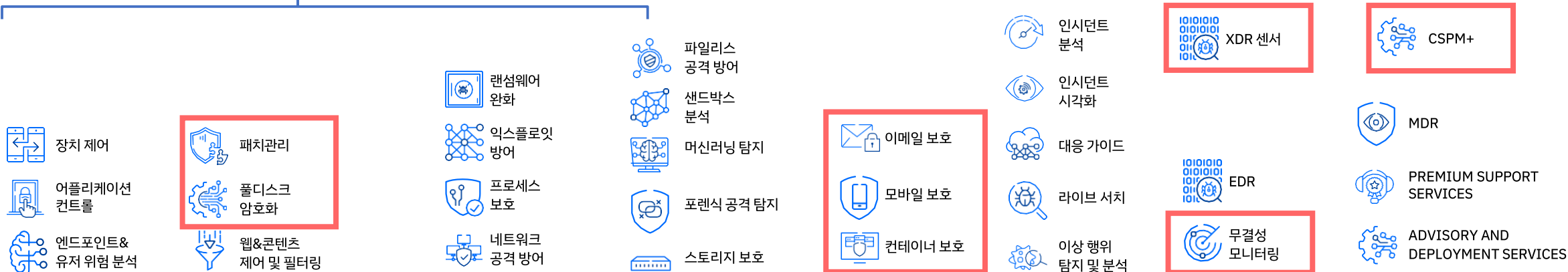
포괄적인 예방 및 보호를 통해 조기 공격 차단 및 전통적인 탐지에 의존하지 않습니다.

Managed Detection and Response Premium/Enterprise

Business Security Enterprise

Business Security Premium

Business Security



예방

보호

탐지 및 대응

데이터 상관관계
분석 및 유지

로컬 & 클라우드
머신러닝

멀웨어
보호

앱 이상
탐지

위협
인텔리전스

구성 설정
관리

취약점 자동 점검
및 패치

자동화 및
최적화

대시보드 및
보고서

외부 API
통합 지원

GRAVITYZONE PLATFORM

ENDPOINT | CLOUD | NETWORK | MOBILE | IDENTITY | PRODUCTIVITY | IOT DEVICES

3

• 기능 및 특징점

About GravityZone

GravityZone EPP&EDR

GravityZone Cloud

GravityZone Mobile

GravityZone EPP & EDR

Add-ons:

- Patch Management (취약점 패치 관리)
- Full Disk Encryption (폴 디스크 암호화)
- Security for Storage (스토리지 보호)
- Email Security (M365/Gmail)
- Security for Containers (컨테이너 보호)
- MDR 관제 서비스 (24x7)
- 무결성 모니터링
- 모바일 위협 탐지 (MTD)
- 엔드포인트 탐지 및 대응 (EDR)
- CSPM+

랜섬웨어 방어 및 완화

프로세스 검사 및 고급 위협 제어

HyperDetect & 샌드박스 분석기

파일리스 공격 방어

Security for Exchange

네트워크 공격 방어

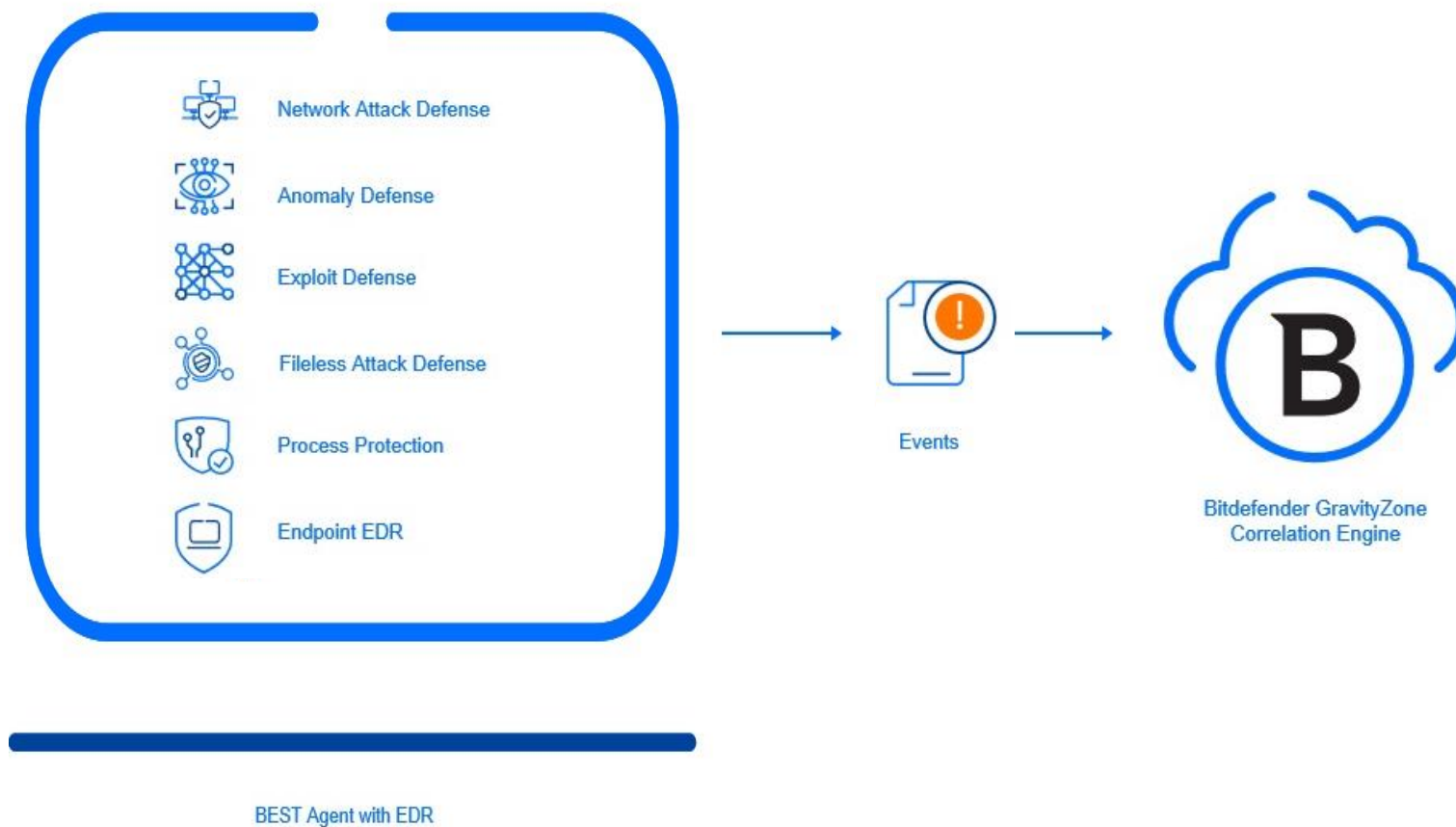
가상화 보호

AV / 매체 제어 / 콘텐츠 제어

엔드포인트 위협 분석

GravityZone EPP & EDR

중앙 상관 관계 엔진을 통해 위협 상황을 지속적으로 모니터링하고 분석하여 위협 위기 대응 능력을 구현



RaaS(Ransomware-as-a-Service)로 인한 피해를 최소화하고
조직 단위로 전파되는 위협을 차단 하는 GravityZone EDR 아키텍처

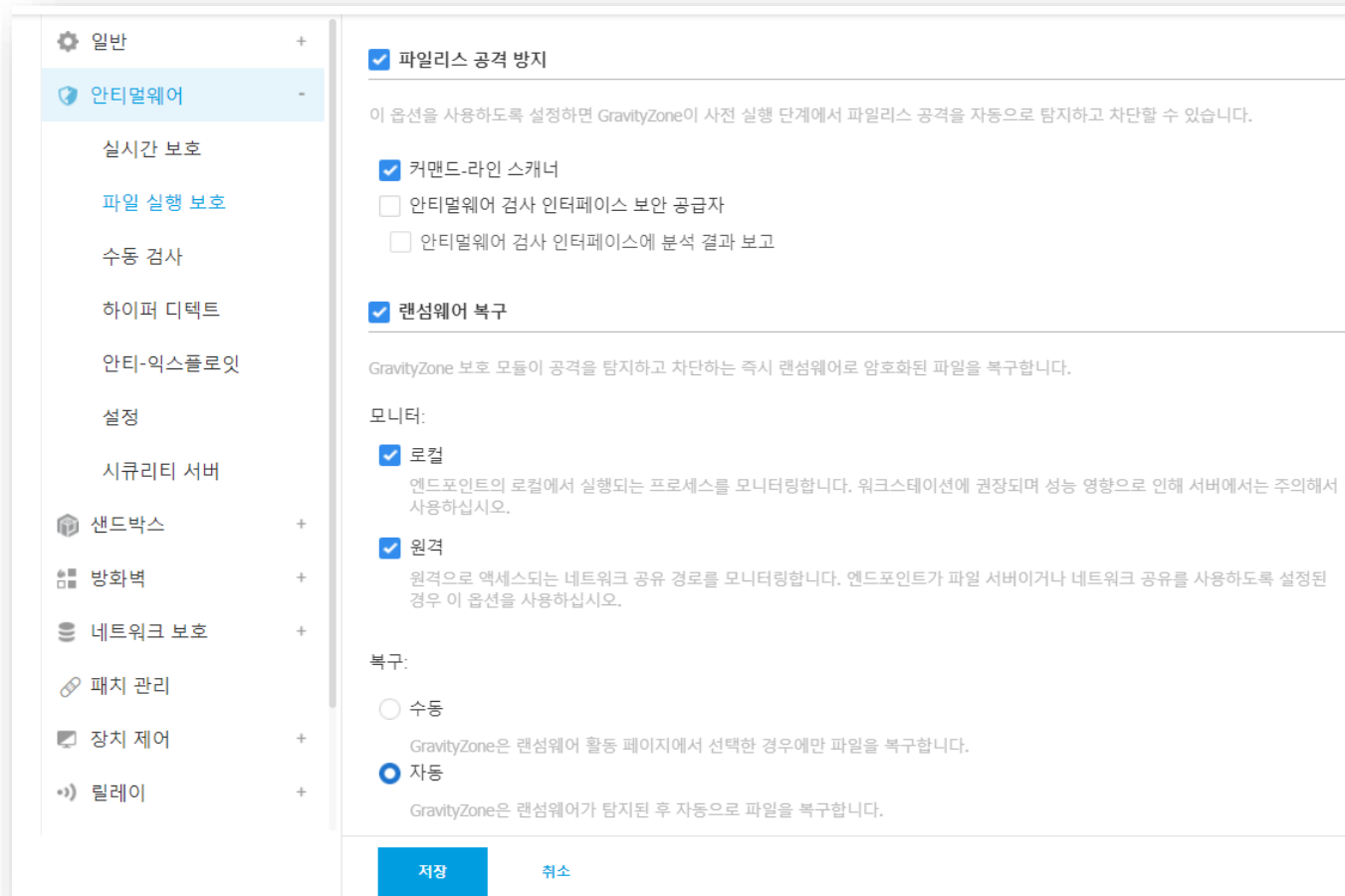


Ransomware Mitigation

랜섬웨어 복구 기능을 통해 차단된 랜섬웨어 공격이 발생한 이후 파일을 다운타임 없이 복구

랜섬웨어의 영향을 받은 암호화된 파일을 신속하게 복구

- 데이터 보호를 위한 변조 방지, 안전한 백업 복사본
- 비트디펜더에 의해 보호되지 않는 엔드포인트에서 오는 공격을 보호
- 랜섬웨어 복구에 대한 추가 비용이 없어 합리적으로 고급 보안 기능 사용 가능



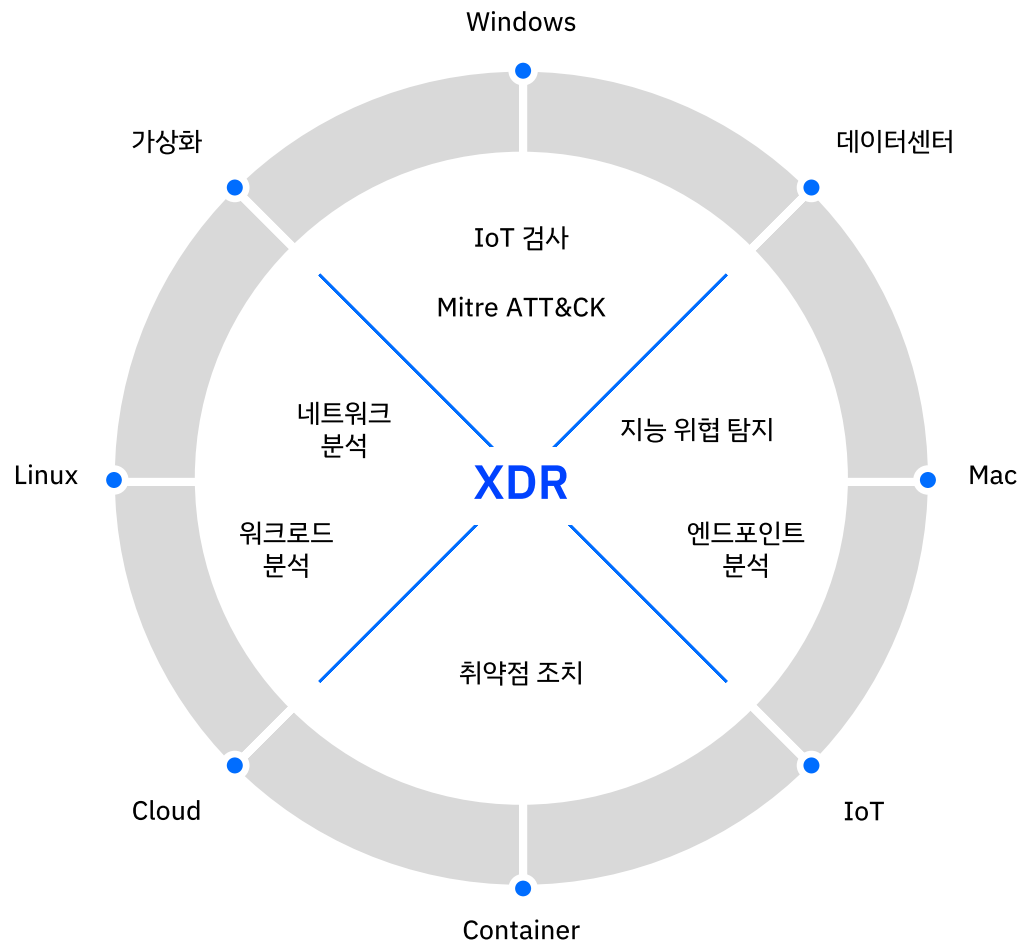
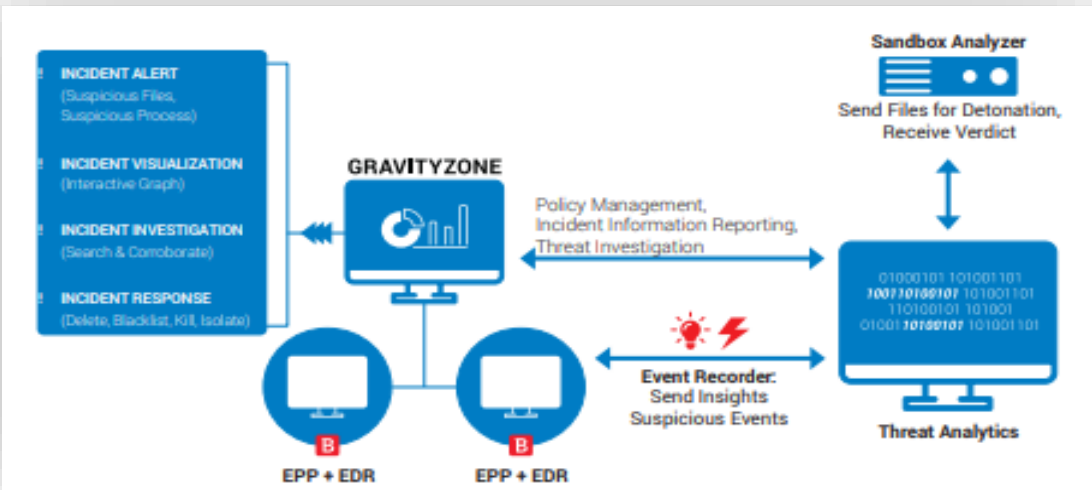
랜섬웨어 복구 기능은 의심스러운 프로세스에 의해 감염되기 전에 파일의 실시간 백업을 생성하여 고급 랜섬웨어 공격중에도 데이터 손실 위험을 완화합니다.

원격 공격이 차단되면 해당 공유에 대한 랜섬웨어 공격에서 감시하는 파일 유형에 접근하기 위해 원격 시스템의 IP가 2시간 동안 차단됩니다.

XDR

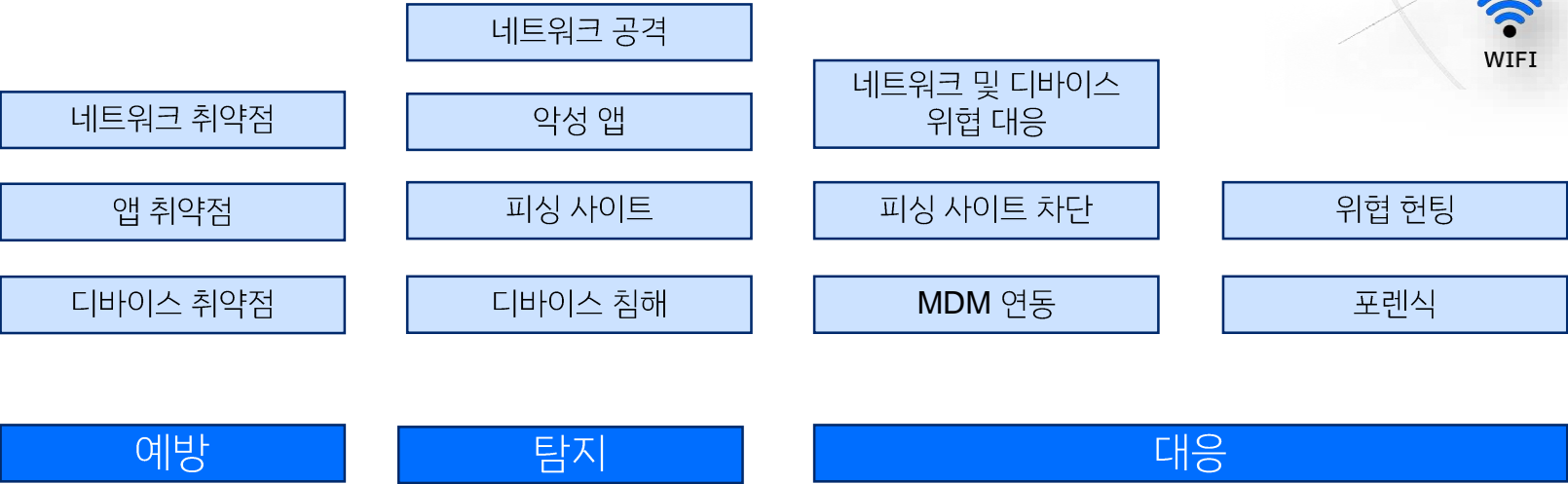
하이브리드 인프라(워크스테이션, 서버, 컨테이너, 다양한 OS)의 여러 엔드포인트 및 네트워크에 대한 교차 이벤트를 수집하고 상관관계를 분석합니다.

- 취약점을 제거하고 반복 공격의 위험을 제거 조치
- 엔드포인트 방지 메커니즘을 회피하는 활동 감지
- 네트워크 전체 인시던트가 환경에 미치는 영향을 보고 분석 및 최소화
- 초기 단계 공격을 발견할 수 있도록 특정 손상 지표(IoC) 및 의심스러운 요소 검색



GravityZone Mobile Security

- 온디바이스 머신러닝 기술을 통해 위협 모니터링
- 애플리케이션 관리를 통해 규정준수 및 모니터링 정책 지정
- 클라우드 기반 심층 분석을 통해 취약점 분석
- 온디바이스 기반 피싱방지 및 로컬VPN을 통한 트래픽 보호
- 디바이스 취약점 모니터링 및 MITRE 매핑을 제공하여 가시성 확보

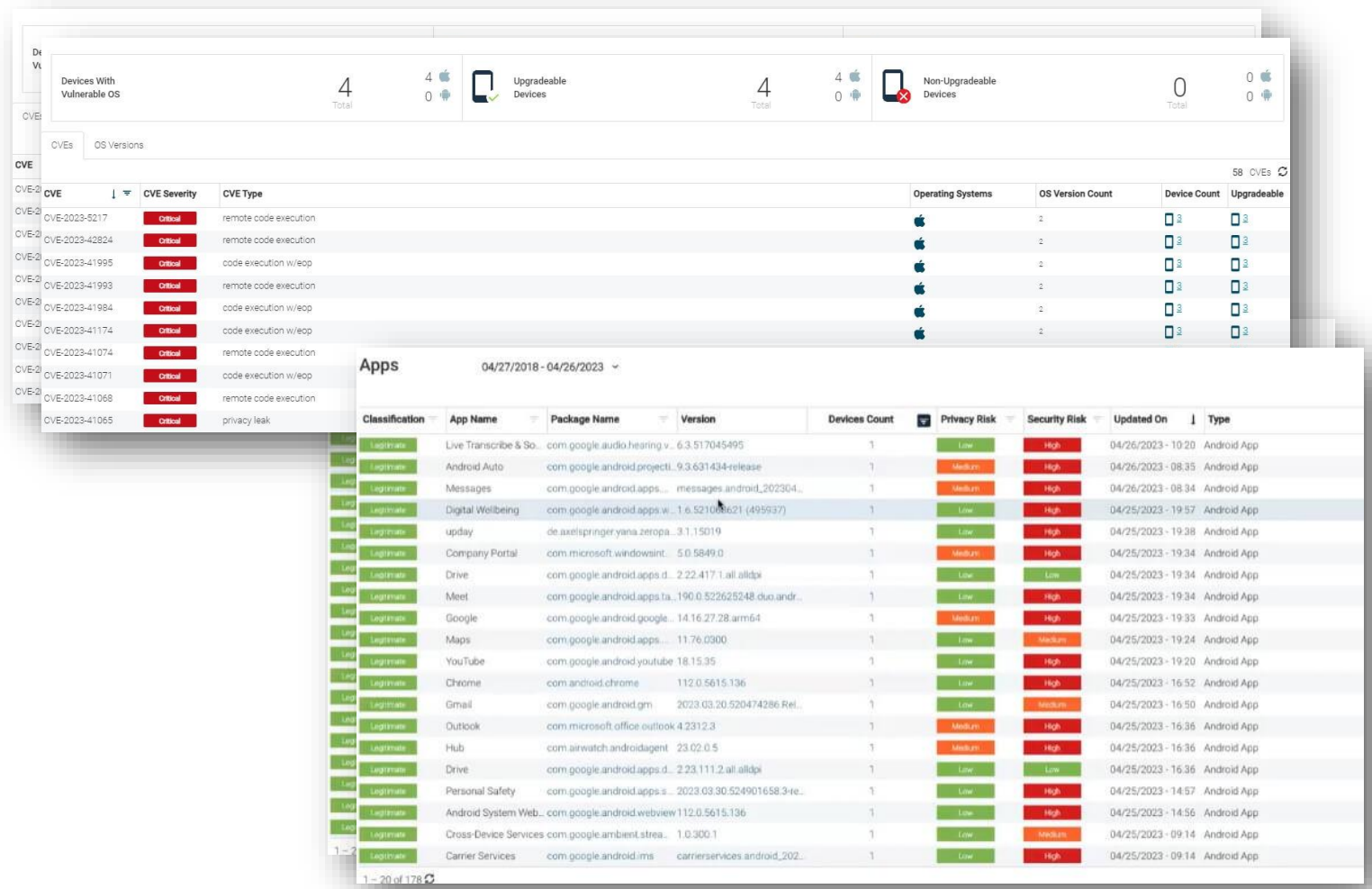




디바이스 취약점 관리

디바이스 환경에 대한 취약점 탐지

- OS 취약점 보고서를 통해 보안 조치를 강화 하고 잠재적 위협을 보다 철저하게 식별
- 앱 로그 보고서를 통해 보안 취약 사항 관리





디바이스 탐지 및 대응

디바이스 환경에 위협 헌팅 및 이벤트
모니터링

- 모바일 위협 헌팅을 통해 지속적인 위협 모니터링 결과를 상세히 보고 받으며 Mitre 태깅을 지원
- 포렌식 데이터 수집을 통해 앱 동작, 네트워크 연결 및 시스템 활동에 대한 정보를 캡처 형태로 제공하여 해당 이벤트를 재구성 및 취약점 식별을 통한 관리 제공

The screenshot displays the Bitdefender Mobile Security management interface. On the left, a table lists various security events detected on mobile devices. The table columns include Severity, Type, Threat Name, Group, User, Device ID, and App. The events are categorized by severity (Elevated, Low) and type (Singular). Threat names include 'Vulnerable iOS Version', 'Detection Inactive', 'Inactive App', 'Unsecured WiFi Network', and 'Location Permission Required: IOS'. The right panel provides a detailed view of a specific event titled 'Phishing protection - Link Tapped'. This panel includes a 'MITRE Tactics' section with links to 'Initial Access', 'Credential Access', and 'Network Effects'. Below this, a 'Details' section lists attributes such as Severity (Elevated), Timestamp (08/30/2023 - 13:16), Threat Type (Singular), Mitigation Date (08/30/2023 - 13:16), User (grzegorznocon), Device ID (10FE1613-F), Group (Default Group), OS (iOS), OS Version (16.7), and Jailbroken status (No). An 'Incident Summary' section describes the event as 'Detected abnormal activity. Continuing to monitor. Nicpon-domAP'. The bottom of the panel shows a map with a location pin and the text 'Last Known GPS'.

Severity	Type	Threat Name	Group	User	Device ID	App
Elevated	Singular	Vulnerable iOS Version	Default Group	grzegorznocon+...	A9EF6112-B48C-4...	Bitdefender Mobile Security
Elevated	Singular	Detection Inactive	Default Group	grzegorznocon+...	A77360BE-0FDF-4...	Bitdefender Mobile Security
Elevated	Singular	Inactive App	Default Group	grzegorznocon+...	A77360BE-0FDF-4...	Bitdefender Mobile Security
Elevated	Singular	Inactive App	Default Group	grzegorznocon+...	A9EF6112-B48C-4...	Bitdefender Mobile Security
Elevated	Singular	Detection Inactive	Default Group	grzegorznocon+...	A9EF6112-B48C-4...	Bitdefender Mobile Security
Elevated	Singular	Detection Inactive	Default Group	grzegorznocon+...	950FBA19-C4F6-4...	Bitdefender Mobile Security
Elevated	Singular	Inactive App	Default Group	grzegorznocon+...	950FBA19-C4F6-4...	Bitdefender Mobile Security
Elevated	Singular	Vulnerable iOS Version	Default Group	grzegorznocon+...	32FE4B46-D149-4...	Bitdefender Mobile Security
Elevated	Singular	Vulnerable iOS Version	Default Group	grzegorznocon+...	A77360BE-0FDF-4...	Bitdefender Mobile Security
Elevated	Singular	Detection Inactive	Default Group	grzegorznocon+...	A9EF6112-B48C-4...	Bitdefender Mobile Security
Elevated	Singular	Inactive App	Default Group	grzegorznocon+...	A9EF6112-B48C-4...	Bitdefender Mobile Security
Elevated	Singular	Inactive App	Default Group	grzegorznocon+...	950FBA19-C4F6-4...	Bitdefender Mobile Security
Elevated	Singular	Detection Inactive	Default Group	grzegorznocon+...	950FBA19-C4F6-4...	Bitdefender Mobile Security
Elevated	Singular	Detection Inactive	Default Group	grzegorznocon+...	A77360BE-0FDF-4...	Bitdefender Mobile Security
Elevated	Singular	Inactive App	Default Group	grzegorznocon+...	A77360BE-0FDF-4...	Bitdefender Mobile Security
Low	Singular	Unsecured WiFi Network	Default Group	grzegorznocon+...	32FE4B46-D149-4...	Bitdefender Mobile Security
Elevated	Singular	Inactive App	Default Group	grzegorznocon+...	A77360BE-0FDF-4...	Bitdefender Mobile Security
Elevated	Singular	Detection Inactive	Default Group	grzegorznocon+...	A77360BE-0FDF-4...	Bitdefender Mobile Security
Low	Singular	Unsecured WiFi Network	Default Group	grzegorznocon+...	32FE4B46-D149-4...	Bitdefender Mobile Security
Elevated	Singular	Detection Inactive	Default Group	grzegorznocon+...	950FBA19-C4F6-4...	Bitdefender Mobile Security
Elevated	Singular	Inactive App	Default Group	grzegorznocon+...	950FBA19-C4F6-4...	Bitdefender Mobile Security
Elevated	Singular	Detection Inactive	Default Group	grzegorznocon+...	A9EF6112-B48C-4...	Bitdefender Mobile Security
Elevated	Singular	Inactive App	Default Group	grzegorznocon+...	A9EF6112-B48C-4...	Bitdefender Mobile Security
Low	Singular	Vulnerable, Non-upgradeable iOS Version	Default Group	grzegorznocon+...	32FE4B46-D149-4...	Bitdefender Mobile Security
Elevated	Singular	Location Permission Required: IOS	Default Group	grzegorznocon+...	10FE1613-F2D8-4...	Bitdefender Mobile Security
Low	Singular	Unsecured WiFi Network	Default Group	grzegorznocon+...	32FE4B46-D149-4...	Bitdefender Mobile Security
Low	Singular	Unsecured WiFi Network	Default Group	grzegorznocon+...	32FE4B46-D149-4...	Bitdefender Mobile Security
Elevated	Singular	Inactive App	Default Group	grzegorznocon+...	32FE4B46-D149-4...	Bitdefender Mobile Security

GravityZone Cloud Security

지속적인 워크로드 보호

단일 콘솔 가시성 및 보고

클라우드 전반에 걸쳐 일관된 정책 시행
모든 주요 퍼블릭 및 프라이빗 클라우드와
기본적으로 통합

뛰어난 성능

대기시간에 미치는 영향 최소화

최적의 사용자 경험과 ROI 향상
VDI 수 최대 55% 향상
어플리케이션 응답 속도 36% 향상

효율적인 인프라 운영

모든 VMS 단일 콘솔 관리

보안 워크플로우 자동화
비영구 VDI 라이선스

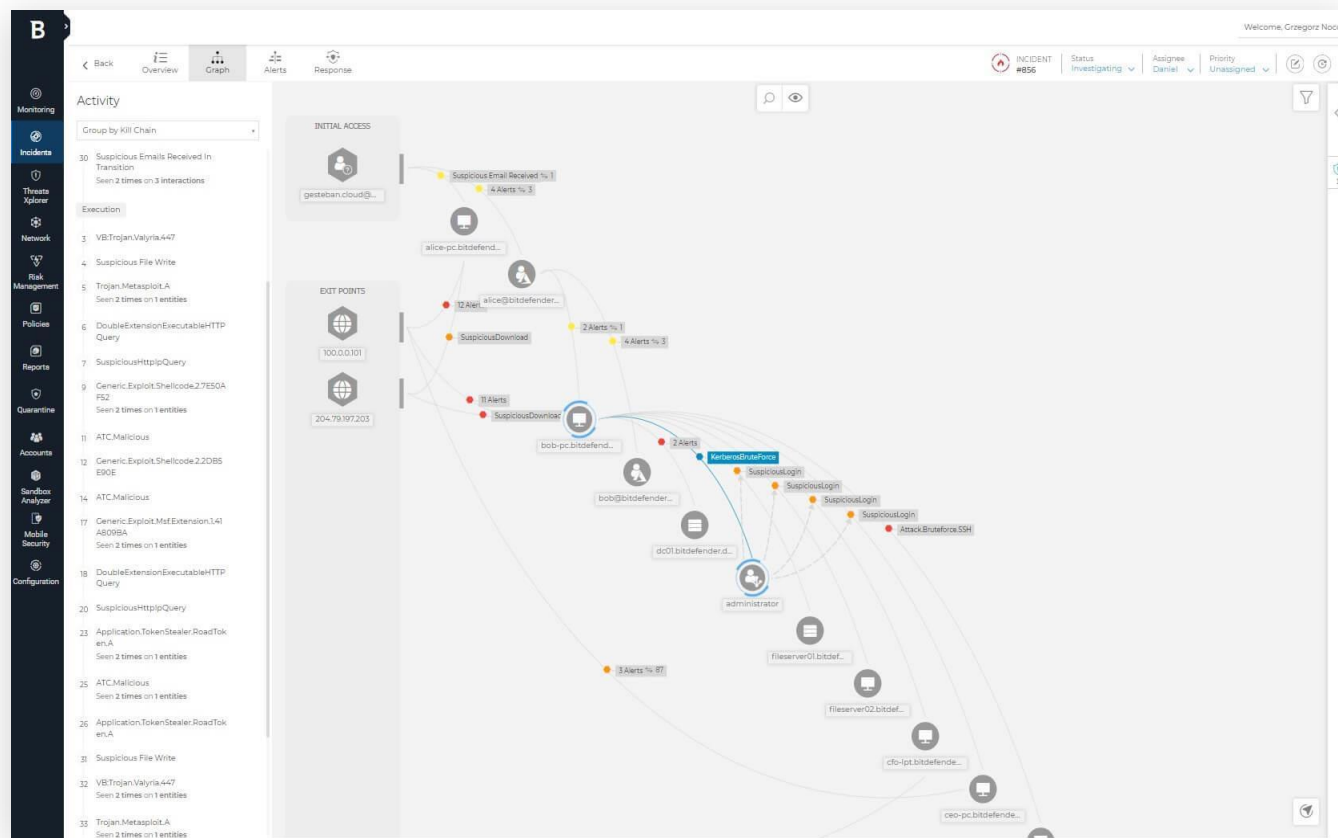




클라우드 위협 검색

클라우드 관리 환경에 대한 위협 탐지

- 다양한 위협 탐지 기능을 클라우드 인프라로 확장
- GravityZone Issent Advisor를 사용하여 공격 시각화 및 드릴링 제공
- 엔드포인트 외 다양한 인프라에 대한 위협 정보와 상관관계 분석
- 단일 콘솔을 통한 통합 운영











가속화된 규정 준수

실행 가능한 규정 준수 지침

- 30분 이내 보고하도록 설정
- NIST, GDPR, ISO27001, PCI DSS 등에 대한 보고서 제공
- 규정 준수 위반 사항에 대한 정보 자동 식별



Standards			GDPR				
Section	Section no.	Scoring					
▼ Controller and processor	IV	82%  9440 Pass, 2041 Fail, 47 Suppressed					
▶ Data protection by design and by default: Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	IV.025.001	65%  1213 Pass, 635 Fail, 6 Suppressed					
▼ Data protection by design and by default: The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.	IV.025.002	98%  7449 Pass, 113 Fail, 2 Suppressed					

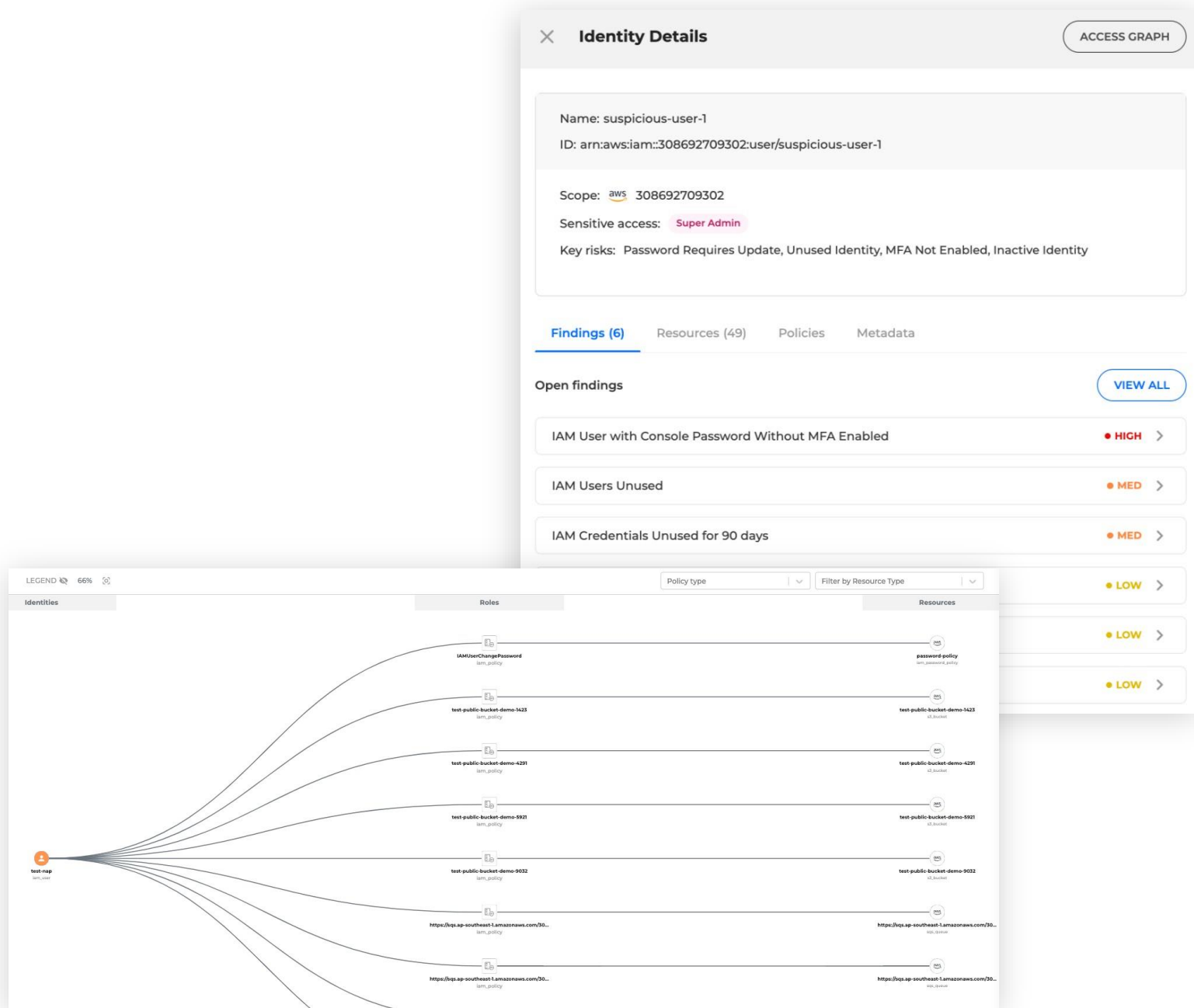
Bitdefender GravityZone Cloud Security Compliance Report		Organization: Internal CSPM+ Demo Standard: EU General Data Protection Regulation (GDPR)	
Article	Paragraph	Description	Checks Status Scoring Check Breakdown
IV - Controller and processor			
25	1	Data protection by design and by default: Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	183 checks: 93 Pass / 90 Fail 53 Secure Transport Not Enabled: 14 Pass / 48 Fail / 0 Suppressed AWS CloudFront to Custom Origin Traffic Not Encrypted: 0 Pass / 2 Fail / 0 Suppressed AWS ALB (ELBv2) Listener Not Encrypted: 4 Pass / 2 Fail / 0 Suppressed EBS Volume Encryption Not Enabled: 0 Pass / 9 Fail / 0 Suppressed CloudFront Distribution Viewer Protocol Policy Encryption Not Enabled: 0 Pass / 2 Fail / 0 Suppressed NLB (ELBv2) Listener Not Secure: 1 Pass / 0 Fail / 0 Suppressed
25	2	Data protection by design and by default: The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.	744 checks: 710 Pass / 34 Fail AWS S3 Bucket with Public Full Control Permission: 62 Pass / 0 Fail / 0 Suppressed Storage Bucket Publicly Accessible: 6 Pass / 1 Fail / 0 Suppressed AWS S3 Bucket with Authorized Full Control Permission: 62 Pass / 0 Fail / 0 Suppressed CloudTrail S3 Bucket MFA Delete Not Enabled: 0 Pass / 1 Fail / 2 Fail / 0 Suppressed CloudWatch Log Metric Filter and Alarm for AWS Management Console Authentication Failures Not Enabled: 0 Pass / 1 Fail / 0 Suppressed AWS S3 Server Access Logging Not Enabled: 1 Pass / 61 Fail / 0 Suppressed CloudWatch Log Metric Filter and Alarm for Route Table Changes Not Enabled: 0 Pass / 1 Fail / 0 Suppressed CloudWatch Log Metric Filter and Alarm for Network Gateway Changes Not Configured for All Log Entries: 0 Pass / 1 Fail / 0 Suppressed CloudWatch Log Metric Filter and Alarm for Network Gateway Changes Not Enabled: 0 Pass / 1 Fail / 0 Suppressed Log Metric Filter and Alarm for Audit Configuration Changes Not Enabled: 0 Pass / 1 Fail / 0 Suppressed CloudWatch Log Metric Filter and Alarm for Unauthorized API Calls Not Enabled: 0 Pass / 1 Fail / 0 Suppressed
30	1	Records of processing activities: Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 45(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; Records of processing activities: Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller; (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 45(1), the documentation of suitable safeguards; Records of processing activities: The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	290 checks: 7 Pass / 192 Fail (1 suppressed) 58 checks: 2 Pass / 56 Fail (1 suppressed) 200 checks: 7 Pass / 192 Fail (1 suppressed) 197 checks: 105 Pass / 92 Fail
30	2	Security of processing: Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the level of security appropriate to the risk that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.	755 checks: 713 Pass / 42 Fail
30	3	Security of processing: The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is authorised to do so in law.	744 checks: 744 Pass / 32 Fail
32	1	Security of processing: The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is authorised to do so in law.	744 checks: 744 Pass / 32 Fail
32	2	Security of processing: The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is authorised to do so in law.	744 checks: 744 Pass / 32 Fail
32	4	Security of processing: The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is authorised to do so in law.	744 checks: 744 Pass / 32 Fail



ID 및 액세스 관리

클라우드에 대한 최소 권한 제공

- 위험하고 과도한 권한을 가진 ID 식별
- 접근 범위 제안
- 직관적인 매핑을 통해 권한에 대한 시각화



4

● 수상

APPENDIX

평가
수상

검증된 사이버 보안 리더십

비트디펜더는 보안 효율성 및 우수성 등을 꾸준히 인증받고 있습니다.



Highest level of detection for all major steps in 2023 MITRE Engenuity ATT&CK Enterprise Evaluations

First in AV-Comparatives enterprise tests, far more than any vendor



AV-Comparatives 2023



Highest Overall Performer in AV-Comparatives Endpoint Prevention & Response Report



35 consecutives VBSpam + awards

산업 및 동종 업계 인증 내역

FORRESTER®

Named a Leader in The Forrester Wave™: Endpoint Security, Q4 2023

Named Among Notable Vendors Managed Detection And Response Services Landscape In Europe, Q3 2023

Gartner®

Named a Representative Vendor for the second consecutive time in the 2023 Gartner® Market Guide for Managed Detection & Response Services.



Named a Customers' Choice for EMEA in the 2023 Gartner Peer Insights™ for Voice of the Customer for Endpoint Protection Platforms



CRN Partner Program Guide Award for MDR 2023



AV-TEST

성능

매일 사용하는 컴퓨터 속도에 대한 제품의 평균 영향

6.0

성능 점수 :: 6.0 만점에 6.0

보호

맬웨어 감염(바이러스, 웜 또는 트로이 목마 등)으로부터 보호

100%

보호 점수 :: 6.0 만점에 6.0

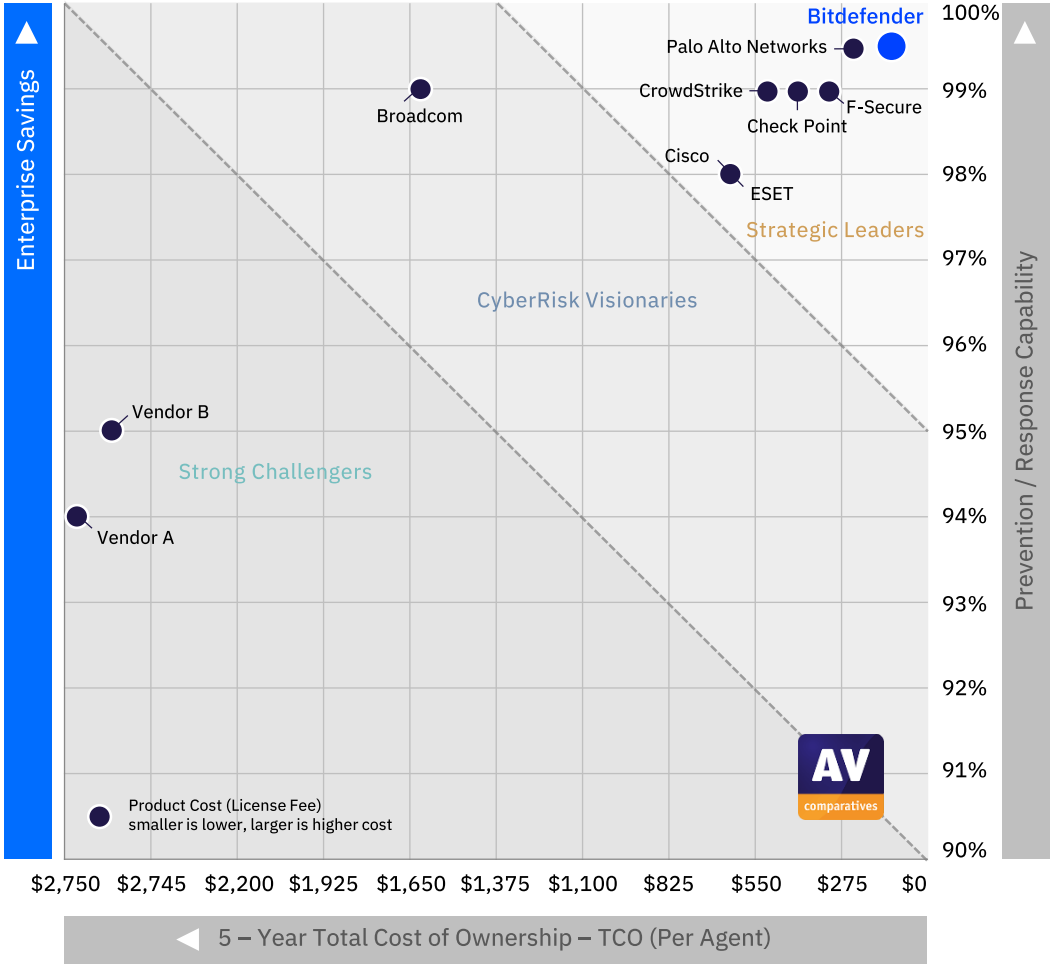
사용성

전체 컴퓨터의 사용성에 대한 보안 소프트웨어의 영향

6.0

사용성 점수 :: 6.0 만점에 6.0

* AV-TEST > Tests > Bitdefender : <https://www.av-test.org/en/antivirus/business-windows-client/>



AV Comparatives

제품	5년 제품 비용	능동 대응	수동 대응	통합 예방 대응 능력	5년 TCO
Bitdefender	\$100	99.0%	100%	99.5%	\$100
Symantec	\$113	98.0%	100%	99.0%	\$1,734
Check Point	\$180	98.0%	100%	99.0%	\$392
Cisco	\$158	96.0%	100%	98.0%	\$582
Crowd Strike	\$249	98.0%	100%	99.0%	\$461
ESET	\$170	96.0%	100%	98.0%	\$594
F-Secure	\$106	98.0%	100%	99.0%	\$318
Palo Alto Networks	\$210	99.0%	100%	99.5%	\$210

180 + Technology Licensing Partners



Bitdefender[®]

180 + Technology Licensing Partners



GravityZone

고객 사례





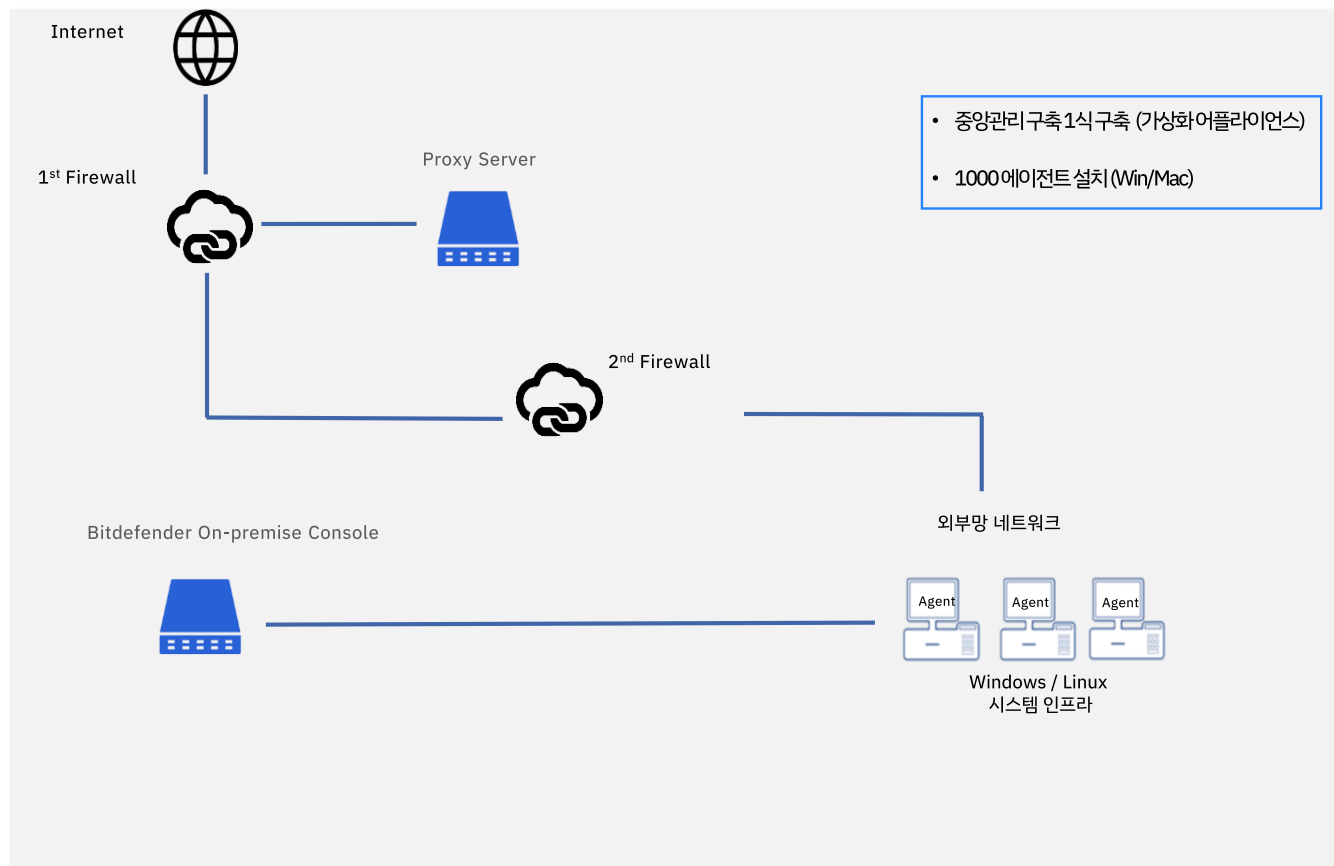
고객 도입 사례

고객사

- A사

운영제품

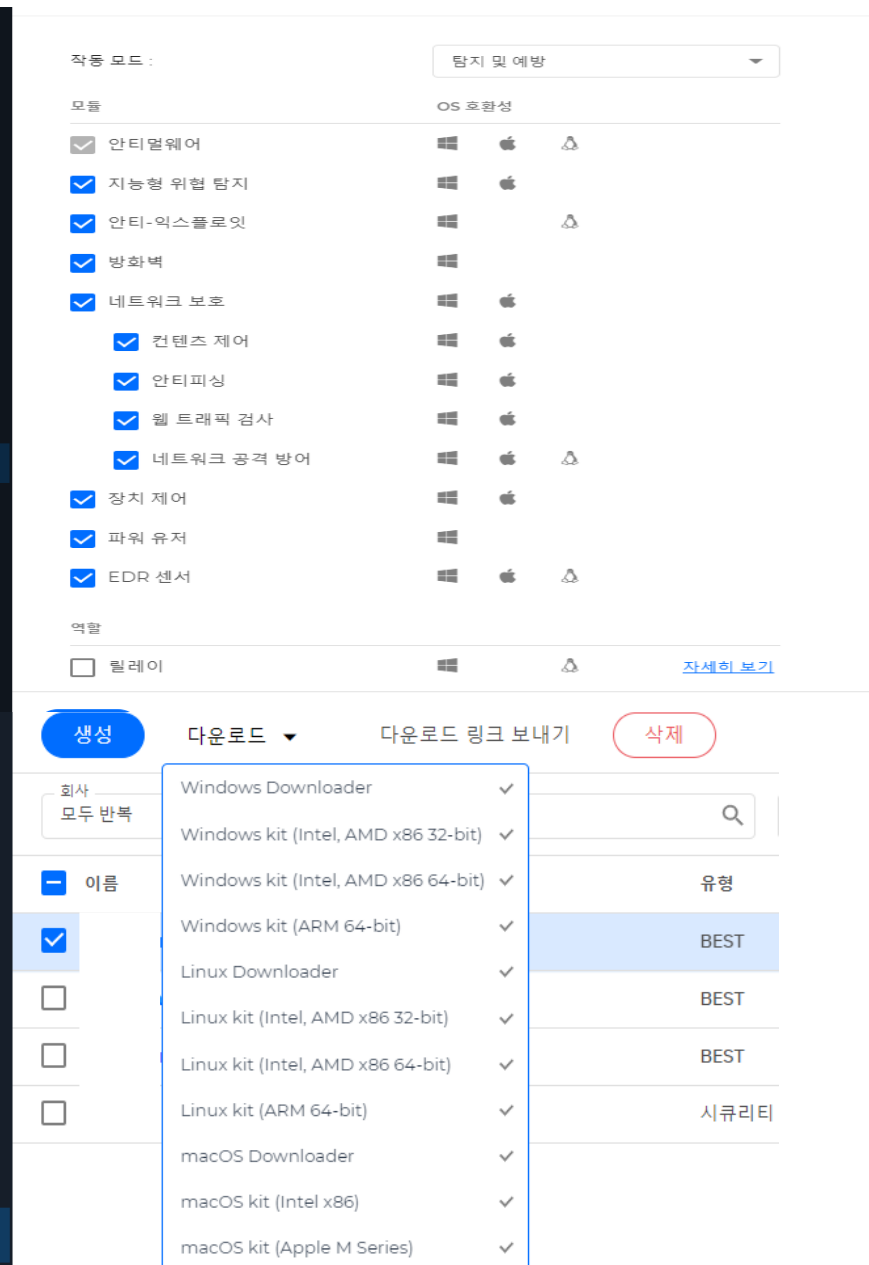
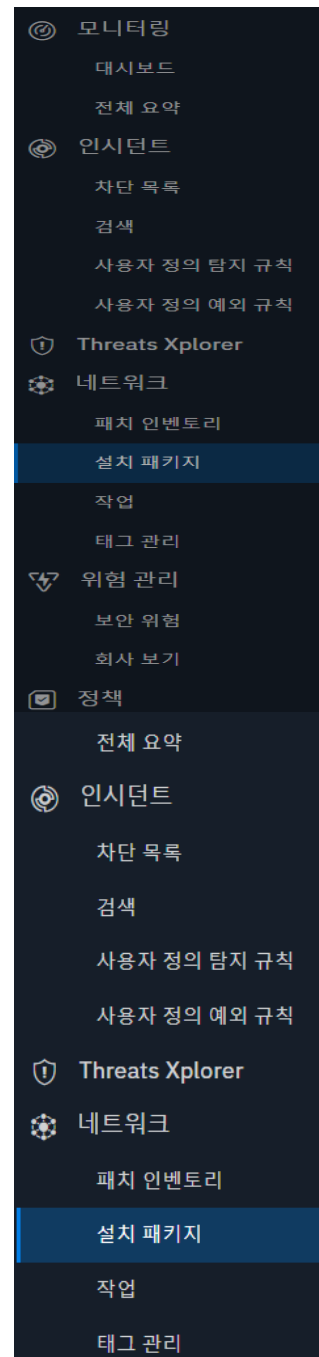
- GravityZone Enterprise Security
- GravityZone Patch Management
- Windows / Mac OS 통합 패치관리
- Windows / Mac 통합 EPP & EDR 운영





통합 OS 설치 패키지

- 사내에 사용하는 엔드포인트를 통합 지원하여 추가적인 작업없이 패키지 설정하여 각 Windows, mac, Linux OS에 맞는 링크를 통해 다운, 설치가 가능합니다.
- 별도의 요청없이 사내 환경에 맞는 정책을 미리 설정하여 설치 패키지를 만들어 각 그룹에 맞는 효과적인 보안에 도움이 됩니다.





파일 실행 보호

- 모듈간의 연계를 통해 잠재적인 위협 및 지능형 위협에 대해 강력한 보호를 해줍니다.
- 단순 쉘도우 카피가 아닌 비트디펜더만의 암호화 기술로 랜섬웨어 공격에서도 안전하게 데이터를 보호할 수 있습니다.

☒ 지능형 위협 탐지

감염된 어플리케이션에 대한 기본 작업:

☐ - 높음

중간 - 대부분의 시스템에 권장

☒ - 중간

이 옵션은 Bitdefender 지능형 위협 탐지 모듈의 탐지율을 중간으로 설정하여 일부 오탐을 포함한 경고가 나타날 수 있습니다.

☐ - 낮음

☒ 파일리스 공격 방지

이 옵션을 사용하도록 설정하면 GravityZone이 사전 실행 단계에서 파일리스 공격을 자동으로 탐지하고 차단할 수 있습니다.

☒ 커맨드-라인 스캐너

☐ 안티멀웨어 검사 인터페이스 보안 공급자

☐ 안티멀웨어 검사 인터페이스에 분석 결과 보고

☒ 랜섬웨어 복구

GravityZone 보호 모듈이 공격을 탐지하고 차단하는 즉시 랜섬웨어로 암호화된 파일을 복구합니다.

모니터:

☒ 로컬

엔드포인트의 로컬에서 실행되는 프로세스를 모니터링합니다. 워크스테이션에 권장되며 성능 영향으로 인해 서버에서는 주의해서 사용하십시오.

☐ 원격

원격으로 액세스되는 네트워크 공유 경로를 모니터링합니다. 엔드포인트가 파일 서버이거나 네트워크 공유를 사용하도록 설정된 경우 이 옵션을 사용하십시오.



안티 익스플로잇

- 취약점 공격에 대한 보호기능을 통해 프로그램의 보안 패치나 업데이트가 되기 전의 보안 격차를 줄여주어 보안에 효율적인 도움을 줍니다.

일반

안티멀웨어

실시간 보호

파일 실행 보호

수동 검사

Anti-Tampering

Hyper Detect

안티-익스플로잇

설정

시큐리티 서버

샌드박스

방화벽

네트워크 보호

패치 관리

장치 제어

무결성 모니터링

밀레이

Exchange 보호

안티-익스플로잇

안티-익스플로잇은 브라우저, Microsoft Office 또는 Adobe Reader와 같이 일반적으로 사용하는 어플리케이션의 알려진 취약점과 알려지지 않은 취약점을 대상으로 하는 공격 시도뿐만 아니라 커널 모드 이후의 탐색 시도에도 실시간 보호 기능을 제공합니다.

Windows 어플리케이션 추가

시스템 전체 탐지

Windows 탐지

프로세스 검사

권한 상승

LSASS 보호

프로세스 종료

보고 전송

보고만

Linux 탐지

자격 증명 모니터링

Ptrace 모니터링

네임스페이스 모니터링

메모리 손상 모니터링

SUID 모니터링

보고 전송

보고 전송

보고 전송

보고 전송

보고 전송

미리 정의된 Windows 어플리케이션

추가 Windows 어플리케이션

저장

취소

© 2024 BitdefenderKorea. All rights reserved.



샌드박스

- 샌드박스 분석 기능을 탑재하여 실제적인 위협을 판단할 수 있습니다.
- 다른 모듈과의 연계를 통해 오탐율을 줄일 수 있습니다.
- MITRE ATT&CK 기술 연동으로 고도화된 공격기법을 분석 할 수 있습니다.

샌드박스

샘플 제출

검색:

샘플 이름 또는 해시 검색

검색

필터 숨기기 ^

분석 결과

☐ 삭제
☐ 감염됨
☐ 지원 안 함

심각도 점수

1009080706050403020100

높음중간낮음

100 ~ 0

제출 유형

☐ 직접
☐ 엔드포인트 센서

제출 상태

☐ 완료
☐ 대기
☐ 실패

ATT&CK 기술(0 선택됨)

정보

MITRE 태그 검색

☐ Obfuscated Files or Information: Software Pa...
☐ Query Registry

26 FEB 2024

직접 제출: igyu

✓ 삭제

하이퍼디텍트_샘플.exe
직접 제출 11:09, 26 Feb 2024

심각도 점수:
● 0

파일 및 프로세스
관련됨: 1

제출처
N/A

분석 환경:
클라우드 샌드박스

보기 >

MD5: 하이퍼디텍트_샘플.exe ~ N/A

ATT&CK 기술: Defense Evasion – Obfuscated Fil...[항목 삭제](#)

직접 제출: igyu

! 감염됨

setup_clover@3.5.4.exe
직접 제출 11:09, 26 Feb 2024

심각도 점수:
● 80

파일 및 프로세스
관련됨: 5

제출처
N/A

분석 환경:
클라우드 샌드박스

보기 >

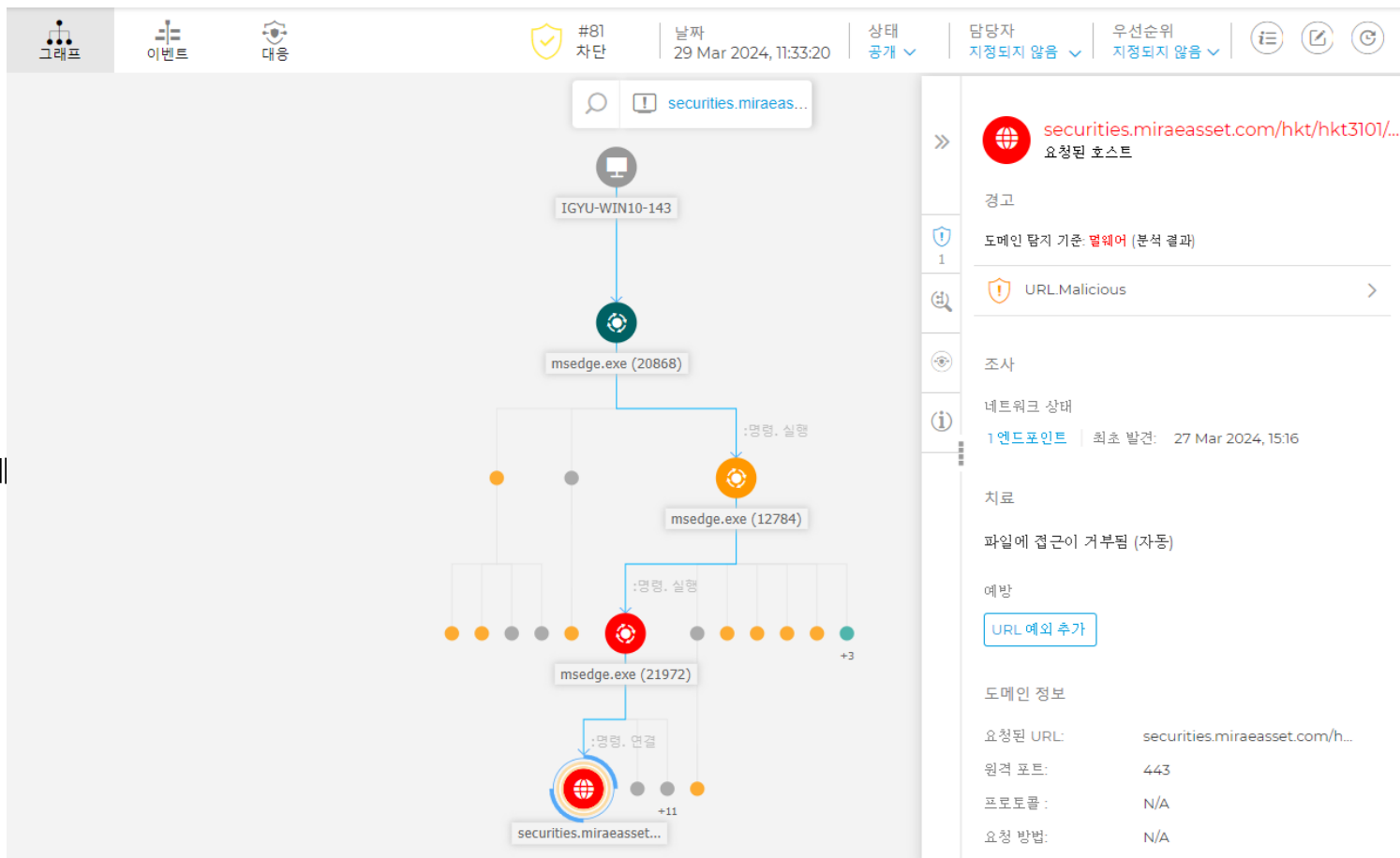
MD5: setup_clover@3.5.4.exe ~ N/A

[항목 삭제](#)



인시던트

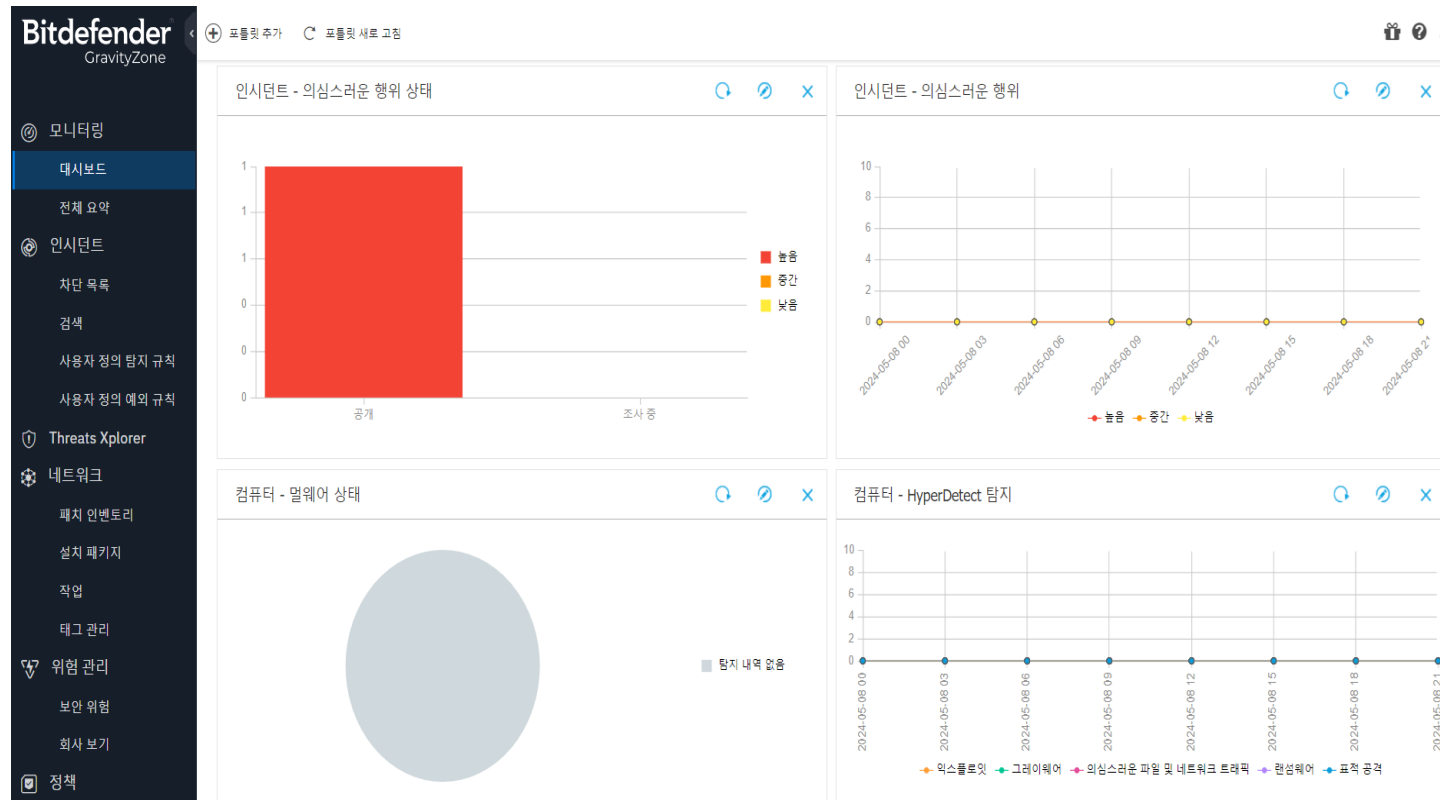
- 공격에 대한 내용을 그래프를 통해 가시성을 확보하고 공격에 대한 경로를 쉽게 파악할 수 있습니다.
- 대응 탭을 통해 해당 공격에 대한 대응법 안내로 비전문가도 어렵지 않게 대응 할 수 있어 추후 공격에 대한 대비가 가능합니다.





모니터링 대시보드

- 대시보드를 통해 사용중인 장치의 상태를 실시간으로 확인하여 위협에 대한 빠른 대응이 가능합니다.
- 포틀릿 추가와 커스텀을 통하여 원하는 이슈들에 대한 확인이 가능하여 관리상 불필요한 리소스를 줄여줍니다.





보고서 생성 및 알림

- 원하는 항목에 대한 보고서를 CSV, pdf로 받아 볼 수 있습니다.
- 수동 및 예약 보고서를 통해 수동 및 예약을 통해 각 항목에 대한 보고서를 볼 수 있습니다.
- 원하는 이벤트에 대한 알림을 설정하여 해당 이벤트에 대한 내용을 확인 할 수 있습니다.

보고서 생성

정보

유형: HyperDetect 탐지

이름: * HyperDetect 탐지

설정

지금

예약됨

보고 간격:

전송:

HyperDetect 탐지

Top 10 감염 엔드포인트

TOP 10 탐지 멀웨어

가상 머신 네트워크 보호 상태

네트워크 보호 상태

네트워크 인시던트

네트워크 패치 상태

데이터 보호

멀웨어 상태

방화벽 활동

파일 첨부:

☐ pdf (요약 정보)

☐ CSV (세부 정보)

☐ 압축 파일

알림 사용

알림

☒

멀웨어 아웃브레이크

☒

라이선스 만료

☒

라이선스 사용 제한 도달

☒

라이선스 제한 도달 예정

☒

사용 가능한 업데이트

☒

인터넷 연결

☒

SMTP 연결

☒

데이터베이스 백업

☒

인증 감사

☒

인증서 만료

표시 여부

☒ 컨트롤 센터에 표시

☒ syslog 서버에 로그인

☐ 이메일로 보내기

환경설정

☐ 임계값 설정 사용

Bitdefender.

Trusted.
Always.

Bitdefender Kora

070-5056-1000

www.bitdefenderkorea.co.kr

