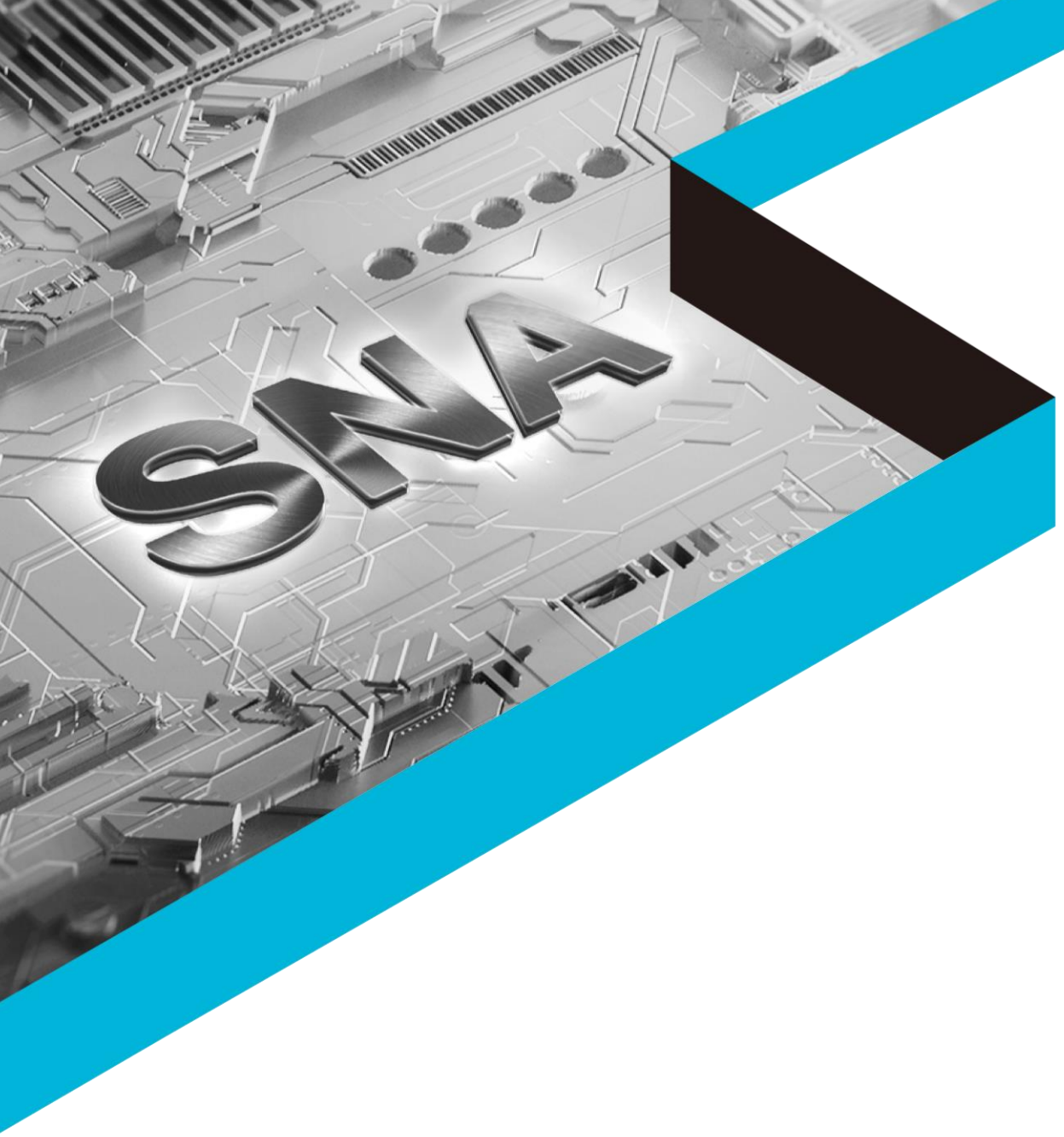



(주)에스엔에이

# 총판 비즈니스 제품 소개서

2023.July

# Contents

Chapter 1

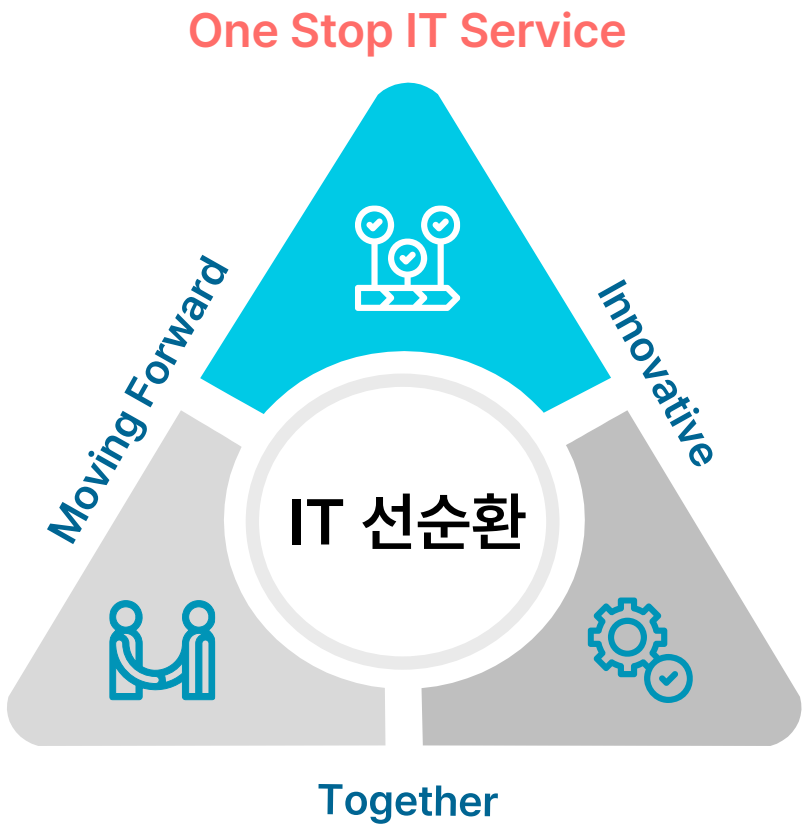
# About SNA

# 회사 일반 현황

## Together + Innovative + Moving forward = 선순환 !

2001년도에 설립된 SNA는 하드웨어 판매와 기술지원 서비스 등의 비즈니스를 20년간 이어온 기업으로 2019년부터 소프트웨어 총판 비즈니스로 사업 영역을 확대하여 성장을 이어오고 있습니다.

| | |
|---|---|
| 회사명 | (주)에스엔에이 |
| 대표자 | 이 원 호 |
| 회사 설립 연도 | 2001년 4월 |
| 사업분야 | 컴퓨터 및 주변기기 / 도소매 / 서비스 / 소프트웨어 개발 및 판매 |
| 주소 | 서울특별시 성동구 성수일로55 (성수동1가, SK테크노빌딩 302~5/308호) |
| 전화번호 | 02- 511-7060 |
| FAX번호 | 02- 497-1585 |
| 직원 수 | 83명(한국 63명, 필리핀 10명, 베트남 10명) |
| 홈페이지 | https://www.snainfo.com |
| 해외지사 | 베트남, 필리핀 해외 지사 |
| 전년도 매출 | 2022년 매출 460억 |



# 회사 연혁

에스엔에이는 20년 노하우를 기반으로 하드웨어와 소프트웨어 분야에서 폭넓은 경험을 가지고 있습니다.

## 2001

- (주)에스엔에이정보 법인 설립
- 삼성전자주식회사 거래처 등록
- 코오롱정보통신(주) 협력업체 등록
- IBM GARS 파트너 등록
- LGNSYS(주)파트 공급업체 등록
- 대우정보시스템 협력 업체 등록
- SK C&C(주)협력업체 등록
- LGNSYS(주)협력업체 등록
- SK 네트웍스(주)협력업체 등록

## 2011

- IBM Value 파트너등록
- SNA Global Philippines 지사설립
- SNA Vietnam 지사설립

## 2013

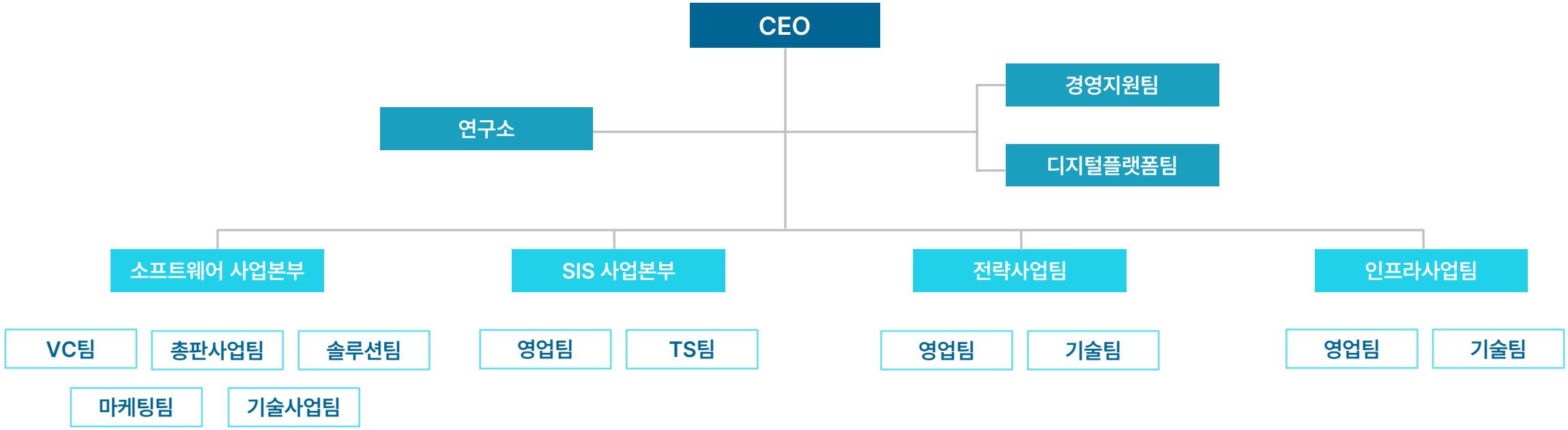
- '(주)에스엔에이'로 사명 변경
- HPE 파트너 등록
- SGA(퓨어스토리지)파트너등록
- DELL & EMC 파트너등록
- 포티넷코리아파트너 등록
- 한국레드햇파트너 등록
- CISCO 협력업체 등록
- 화웨이코리아파트너 등록

## 2018 2023

- SK Shieldus 탄소중립협업 협약 체결
- ABLESTOR 파트너 계약 체결
- DAWON I&C 총판 체결
- 자사솔루션 Onrrow 론칭
- NHN다이퀘스트 협약 체결
- TheJOIN 협약 체결
- 조달 제품 등록 (틸론 외 3개 솔루션)
- 약 20여개 솔루션 밴더와 총판/파트너쉽 체결
- TSV & QSV 자사 서버 조달 등록
- TANIUM 파트너 등록
- 쿼드마이너 총판 등록
- 틸론 VDI 총판 등록
- Kakao Most Valuable 파트너 등록
- ORACLE DBMS 파트너 등록
- W사업부, 총판 사업부 신설
- LG 히다찌 파트너 등록

# SNA 조직도

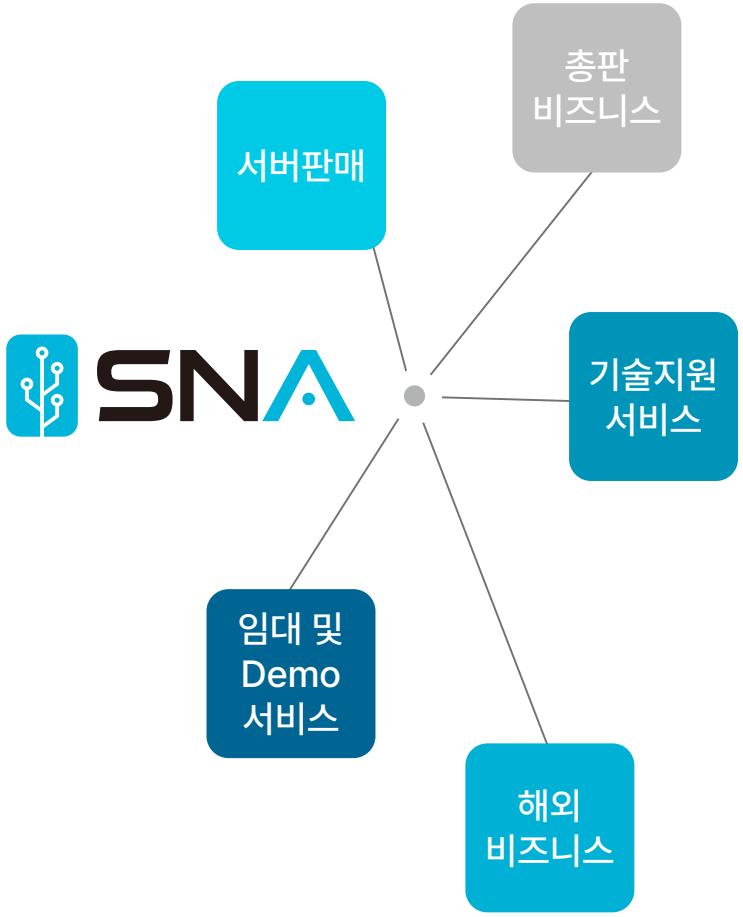
에스엔에이(SNA)는 하드웨어 조직으로 시작하여 2019년 소프트웨어 사업본부를 신설하여 조직을 확장하고 있습니다.
2023년에는 솔루션팀을 신설하였고, 연구소를 신규로 신설 진행 중입니다.




➡ 2023년 ESG 프로젝트 TFT : 총판 사업팀 + SIS사업 본부 + 인프라사업팀

# SNA Business

에스엔에이는 하드웨어 판매, 임대 및 데모, 통합유지보수, 인프라 구축(이전사업, 보안폐기) 컨설팅, 솔루션 유통, 글로벌 비즈니스 등
맞춤형 One Stop IT 서비스를 제공합니다.




## 서버 판매

시스템 : 약다양한 제조사와의 파트너 계약 체결 / 제조사 별 다양한 상품 보유
2000대 재고 보유 / 파트 : 약 100,000개 재고 보유

## 총판 비지니스

전문 엔지니어 및 컨설턴트 보유 / 20여개 이상의 밴더사와 총판쉽 체결
조달 총판 업무 지원

## 임대 및 Demo 서비스

시스템 구성 컨설팅 지원 / 전담 엔지니어의 시스템 구축 및 기술지원
시스템 : 약 3300대 & 파트 : 약 36,000개 재고 보유
하드웨어 장애 시 무상 부품 교체

## 기술지원 서비스

다양한 밴더 별 기술지원 인력 보유 / 24x7x365 기술지원 및 유지보수
전산센터 이전 사업 / 보안 폐기 서비스

## 해외 비지니스

SNA 글로벌 필리핀 / SNA 글로벌 베트남
상품판매, 시스템 구축, 기술지원, 유지보수

Chapter 2

# About Solution

# 총판 비즈니스 제품 라인

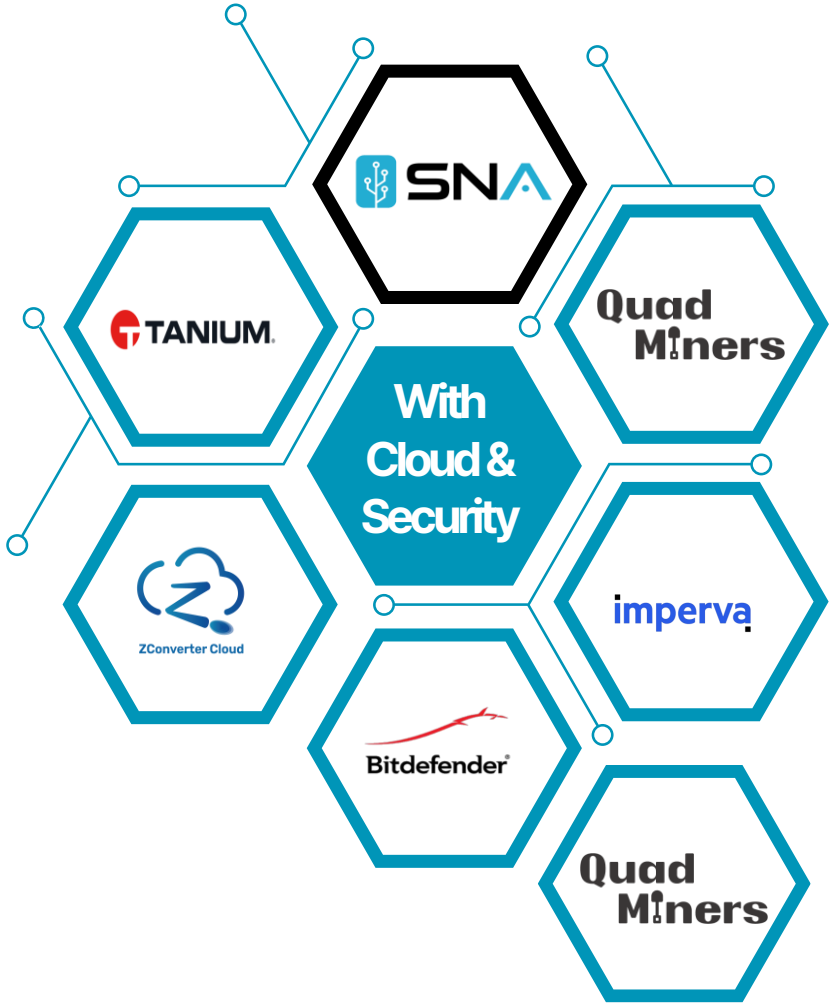
빠르게 변화하는 IT환경, 비지니스 패러다임의 변화 등 급변하는 미래를 함께할 SNA의 파트너사

Chapter 2

# With Cloud & Security

- 에스엔에이 / Onrrow
- 쿼드마이너 / Network Blackbox
- 쿼드마이너 / QUADX
- 비트디펜더 / Gravity Zone
- 태니엄 / TANIUM
- 임퍼바 / Imperva
- 제트컨버터클라우드 / Cloud migration

# With Cloud & Security - 통합인증솔루션(SSO)



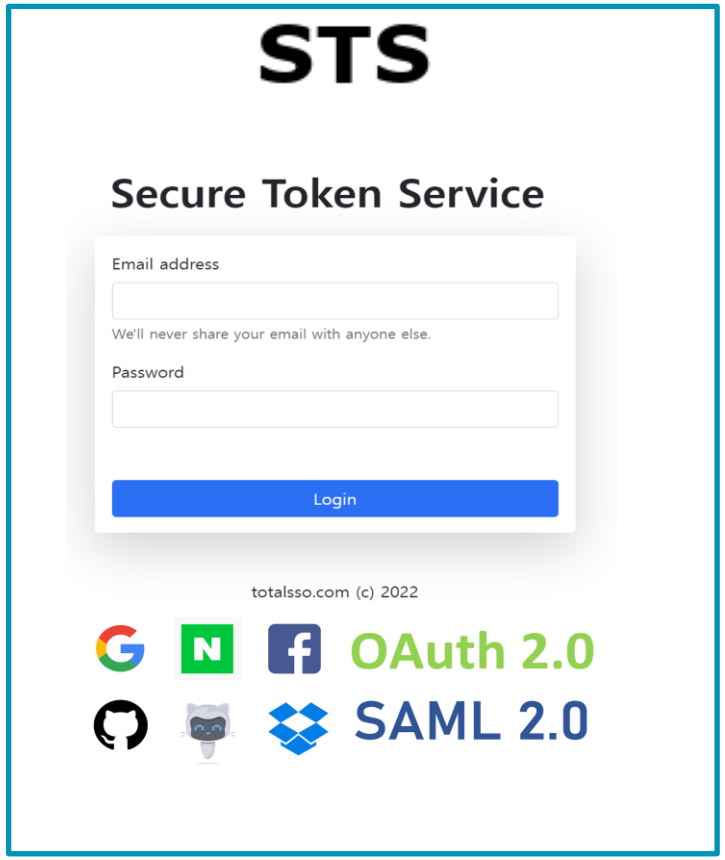

SNA 통합 인증 솔루션 (SSO)

ONRROW 클라우드 및 온프라미스 환경의 통합인증 및 계정관리를 쉽고 빠르게 지원하는 Access & Identity 솔루션 입니다

| | |
|---|---|
| 제조사 | (주)에스엔에이 (SNA) |
| 제품명 | Onrrow |
| 제품구성 | SaaS형 서비스, 구축형 서비스 |
| 제품 특장점 | 인증 시장이 포화 상태인 가운데, SMB 시장에서 인증 관련 인프라를 직접 운영하기 어렵고 Major 밴더사 제품의 경우 도입과 유지 비용이 높다는 문제점들이 야기되었습니다.<br><br>SNA의 Onrrow는 Major 밴더와 동일 기능을 제공하지만, 초기 도입비용과 유지 비용을 낮춰 쉽고 편하게 사용할 수 있도록 진입 장벽을 낮췄습니다.<br><br>또한, 국내 개발 제품으로 다양한 고객의 니즈를 반영한 커스터마이징이 가능하다는 강점을 가지고 있습니다. |

# With Cloud & Security - 통합인증솔루션(SSO)

## 개요

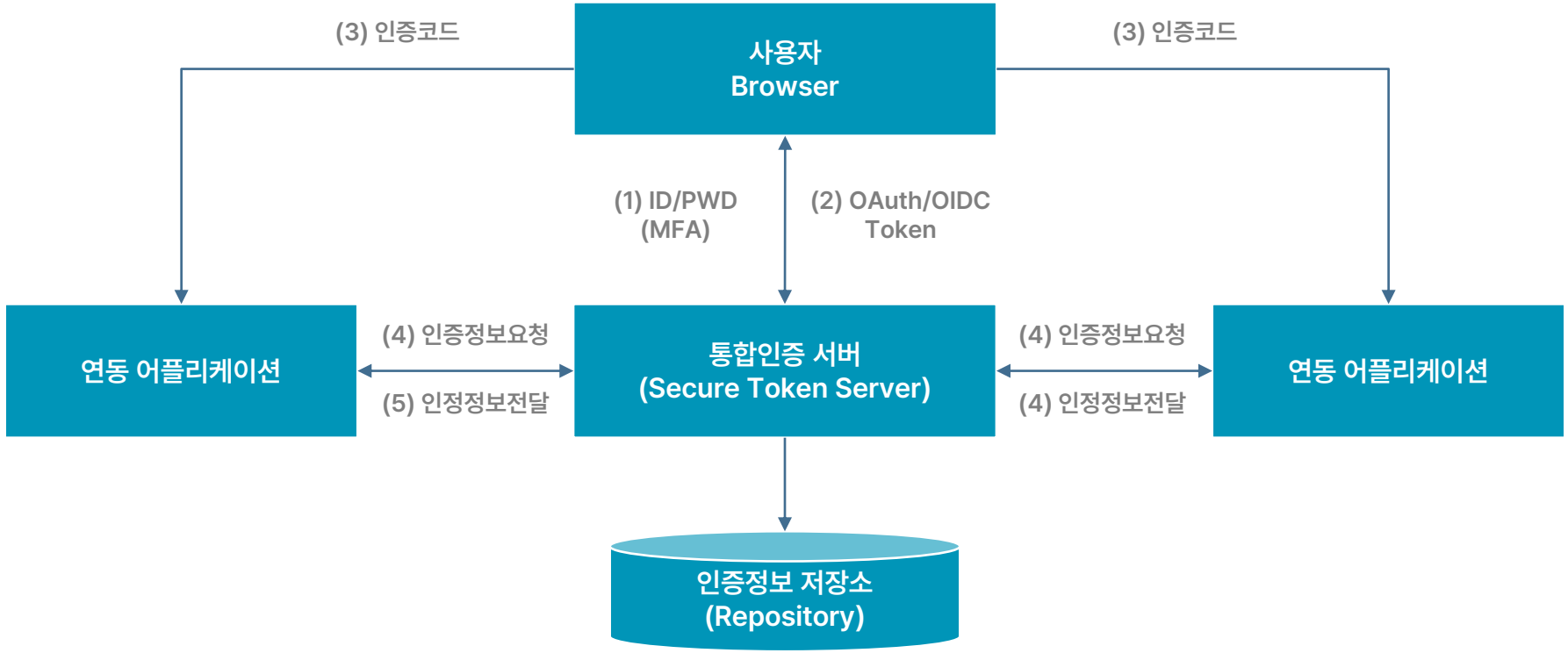



- **기존 방식의 인증방식이 아닌 Secure Token 방식**
- **표준 인증 기술 지원**
  - QAuth 2.0 / OIDC 지원
- **표준 계정관리 기술 지원**
  - SCIM 2.0 지원
- **다년간 Major 제품 취급을 통한 기술력 확보**
  - CA IAM / Oracle IAM / IBM IAM
- **Simple 인증 / 계정 제품의 필요성으로 자체 제품 개발**
  - 커스터마이징 용이

# With Cloud & Security - 통합인증솔루션(SSO)

## 논리적 아키텍처

통합인증 기능을 제공하는 Secure Token Server 를 통해 인터넷 표준 인증 기술인 OAuth2.0/OIDC 기반으로 가장 보편화되고 검증된 통합인증을 제공하며, 특정 솔루션에 종속되지 않는 표준 프로토콜로 자체 개발된 어플리케이션 뿐만 아니라 SaaS 형으로 제공되는 많은 클라우드 어플리케이션 연동을 지원 합니다.



# With Cloud & Security - 통합인증솔루션(SSO)

## 주요기능

'Onrrow'는 사용자의 인증 뿐 아니라 API 인증 또한 지원하며 OAuth/OIDC, JWT 보안 토큰을 활용하여 표준화된 인증 기능을 수행합니다. 또한 사내/외 사용자 정보 관리를 위한 표준 방식인 SCIM 을 지원하여 계정통합관리에 일관된 방식으로 확장 관리할 수 있습니다.

### 인증 기능

- 웹을 통한 OAuth2.0/OIDC 기반 사용자 인증 제공
- Any Browser 지원
- API 서버 등 단일 인증 필요시 ID/PWD 기반 RestAPI 인증 제공
- 로그인 페이지 UI 변경 제공
- 다양한 SaaS 인증 연동

### API 기능

- 사용자 정보 관리용 RestAPI 제공
- 각종 로그 수집용 RestAPI 제공

ONRROW

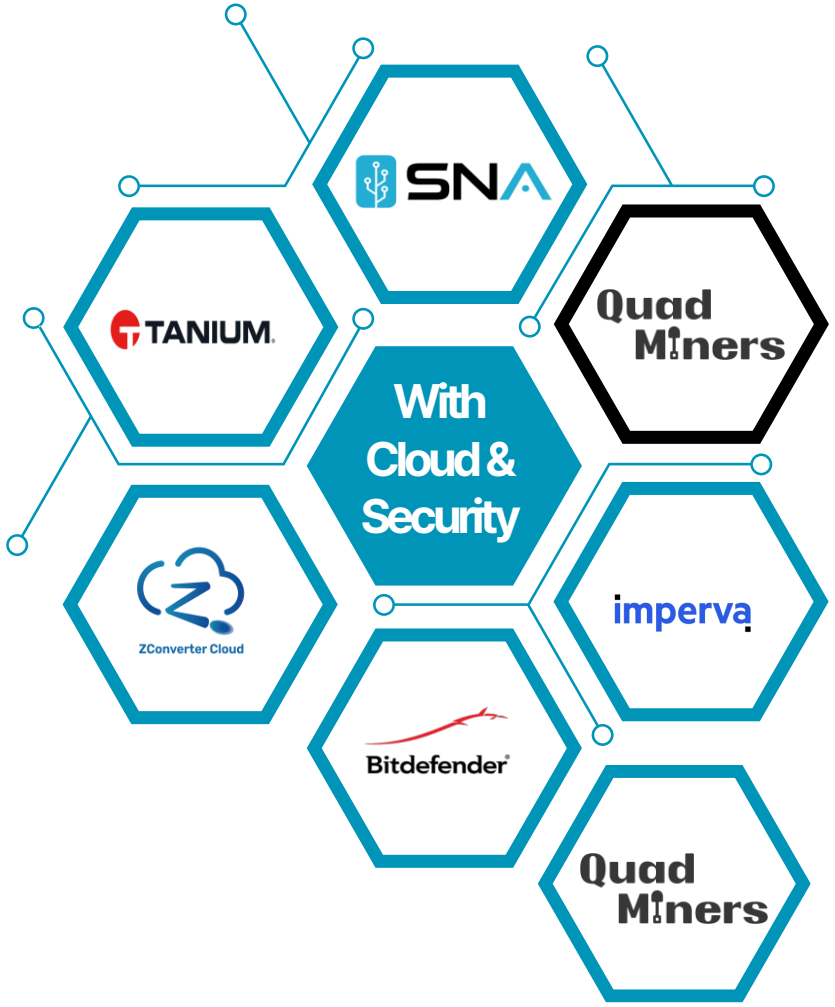
### 개발자 지원

- OAuth2.0/OIDC 기반 Legacy 연동을 위한 Sample Code 제공
- 필요시 직접 개발 지원
- 암호화 토큰 (JWT) 라이브러리 제공 (Java/.NET)

### 다중 인증 지원

- 3rd Party MFA (FIDO) 연동을 위한 인터페이스 제공다양한 업체의 MFA 연동 지원 (별도 연동 필요)

# With Cloud & Security – 네트워크 탐지 및 대응




Quad Miners

## 네트워크 탐지 및 대응(NDR)

NETWORK BLACKBOX

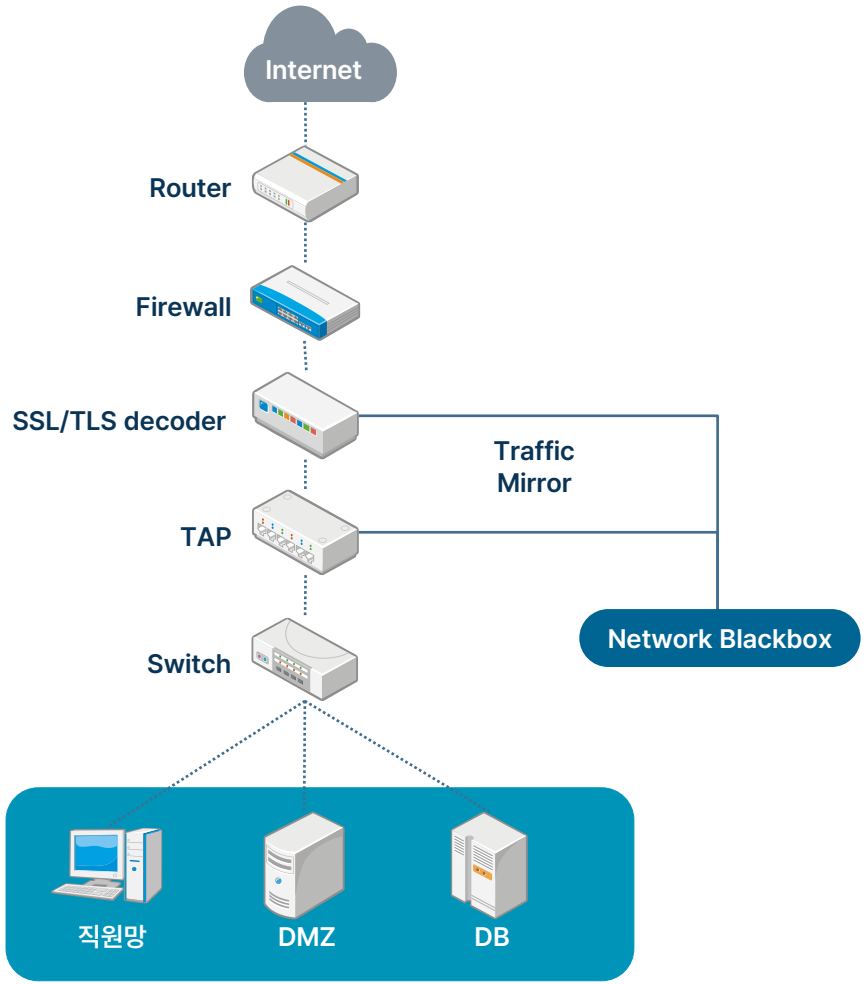
모든 패킷을 저장하고 분석하여 실시간 이상징후를 탐지하고 내·외부 위협에 대한 명확한 분석을 제공합니다.

| | |
|---|---|
| 제조사 | (주)쿼드마이너 (Quadminers) |
| 제품명 | Network Blackbox |
| 제품구성 | • AIO 구성<br>(Sensor, Data Node, Management All-in-One)<br>• Expand 구성<br>(네트워크 환경에 따라 Multi Data Node 추가) |
| 제품 특장점 | • 위협/이상 행위 탐지<br>다양한 이상행위에 대한 룰을 정의하여 탐지할 수 있습니다.<br>25,000+ Rule기반 위협탐지를 제공합니다.<br><br>• 컨텐츠 추출<br>메일, 파일, 게시판, 검색 등 다양한 컨텐츠를 추출하고<br>분석/재현합니다.<br><br>• 네트워크 포렌식<br>페이로드부터 플로우 영역까지 네트워크 및 패킷 전반에 대한<br>분석이 가능하며, 풀-패킷을 통한 명확한 증적 자료를<br>제공합니다.<br><br>• 3rd Party 연동<br>API/EAI/JDBC 등 다양한 인터페이스를 통해 고객사에서<br>보유하고 있는 다양한 솔루션과 연계를 통한 상세분석 기능을<br>제공합니다. |

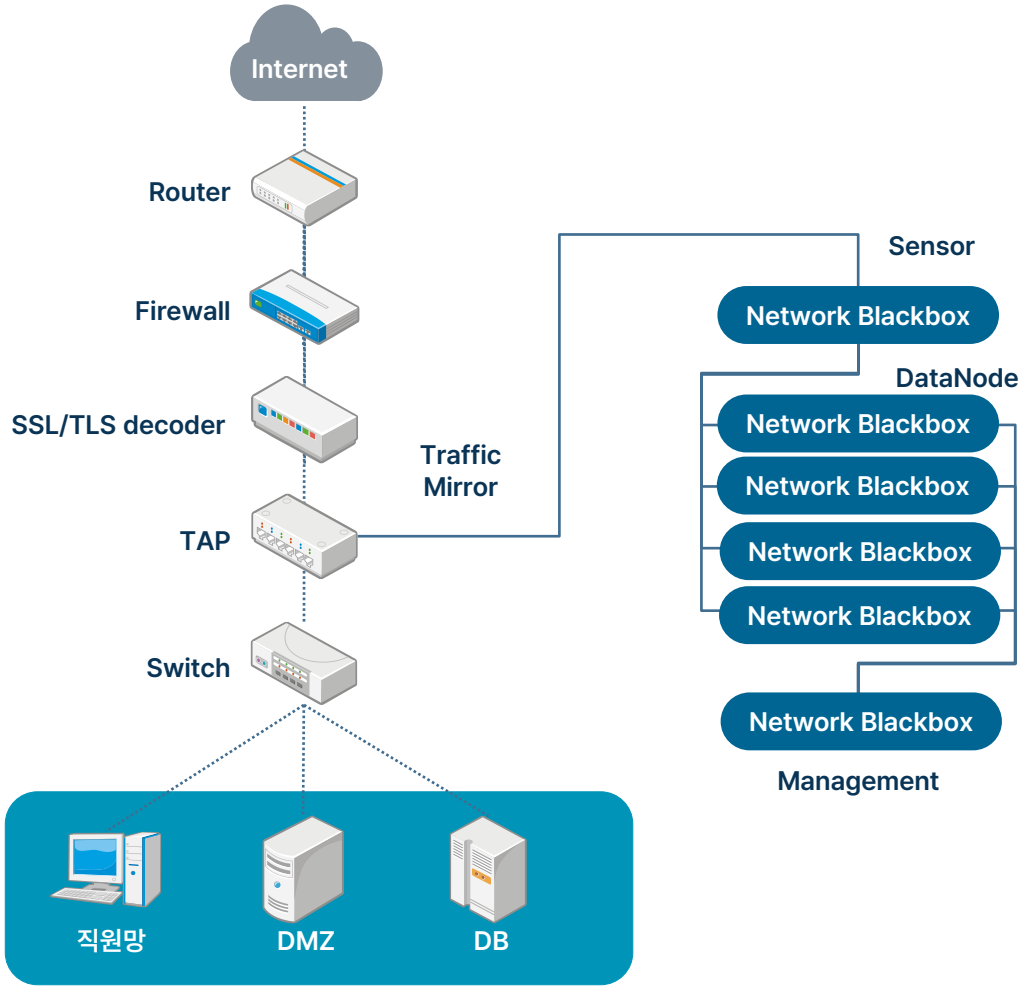
# With Cloud & Security – 네트워크 탐지 및 대응

## 구성안

### AIO(All-in-One) 구성



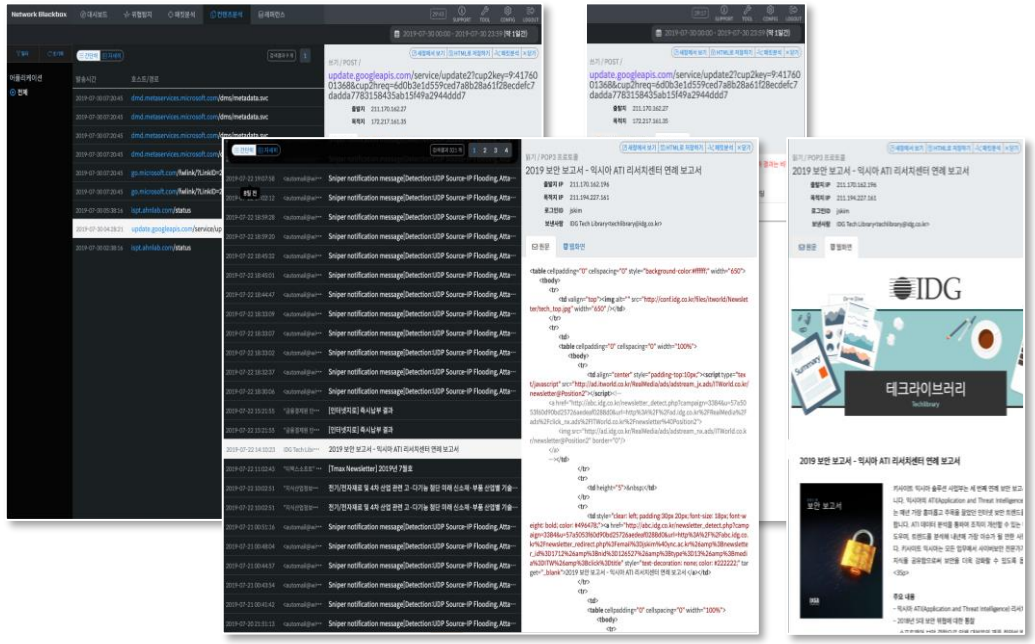

### Expand 구성



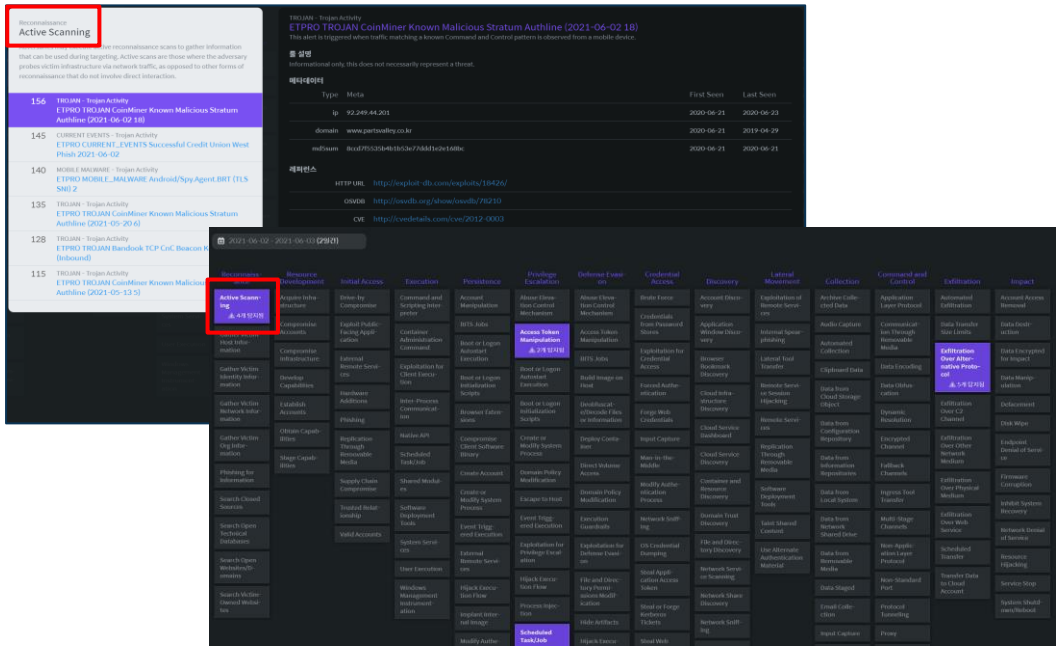
# With Cloud & Security – 네트워크 탐지 및 대응

## 대시보드

### 컨텐츠 추출 및 분석




### MITRE ATTACK & 위협 탐지 현황



# With Cloud & Security – 네트워크 탐지 및 대응

## 경쟁사 비교자료

| 구분 | 쿼드마이너(KR) | N사(KR) | D사(UK) | V사(US) |
|---|---|---|---|---|
| 벤더 국내 현황 | **인원 2배 증가<br>매출 3.5배 증가** | 인원 및 매출 감소 | 한국지사 축소<br>(18명 -> 7명) | 한국지사 미설립<br>(지원미비) |
| 풀패킷 저장 | **O** | X | X | X |
| 리빌딩 기능제공 | **O** | X | X | X |
| 탐지모델 커스텀 지원 | **O** | △ | O | O |
| 시각화 | **O** | X | O | O |
| 원본파일분석 | **O** | X | X | X |
| 머신러닝 | **지도학습 기반** | △ | 비지도학습 기반 | 지도학습 기반 |
| 전후 데이터 추적 | **O** | △ | △ | X |
| 타솔루션 연계 | **O** | △ | X<br>(탐지이벤트 로그만 전달) | X<br>(탐지이벤트 로그만 전달) |
| 확장성 | **O** | O | △ | △ |
| 국내 대형  구축사례 | **O** | X | O | △ |

# With Cloud & Security – 네트워크 탐지 및 대응

## 기대 효과

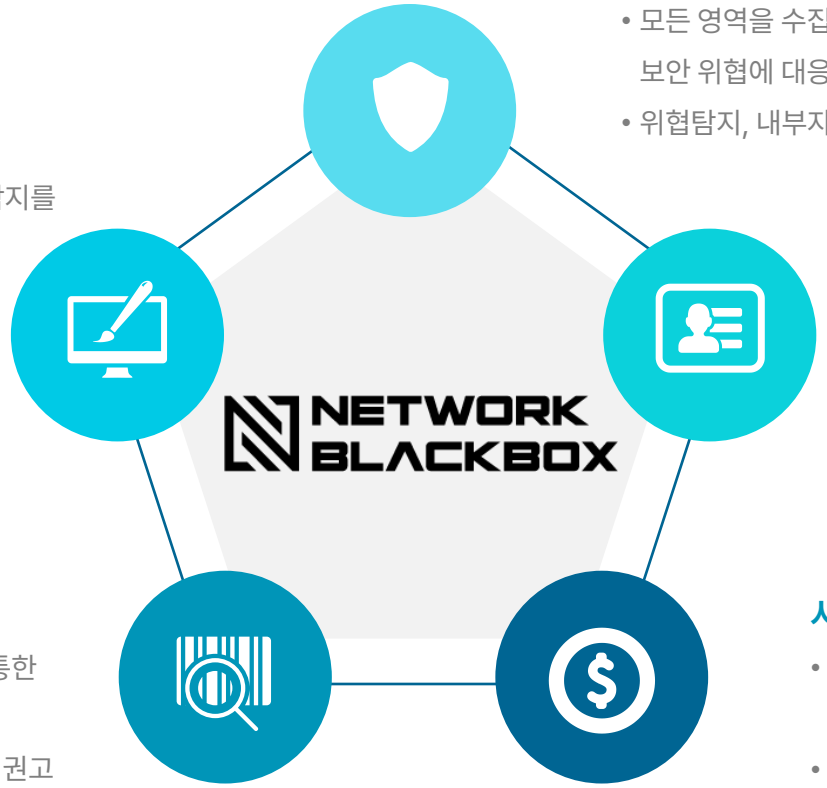
명확한 분석, 대응관리, 통합, 시간/비용 절감, 유출탐지 등 많은 보안 이점을 통해 보다 안전한 기업 네트워크의 운영이 가능합니다.

### 전방위 보안 강화

- 모든 영역을 수집하고 저장, 분석하기 때문에 모든 종류의 사이버 보안 위협에 대응
- 위협탐지, 내부자료유출, 네트워크 포렌식까지 전방위 보안 강화

### 내 · 외부 위협에 대한 명확한 분석

- 트래픽 분석을 통한 내 · 외부 보안 위협에 대한 이상징후 탐지를 통해 보안사고 사전예방
- 전체 트래픽 저장/분석을 통한 네트워크 가시성 확보
- 주요 위협에 대한 룰 설정을 통해 즉각적인 모니터링




### 내부자료 및 개인정보 유출 탐지

- 다양한 컨텐츠 추출 및 트래픽 분석을 통한 내부자료유출 및 개인정보유출에 대한 모니터링을 통해 주요 정보 유출에 대한 최소화 예방

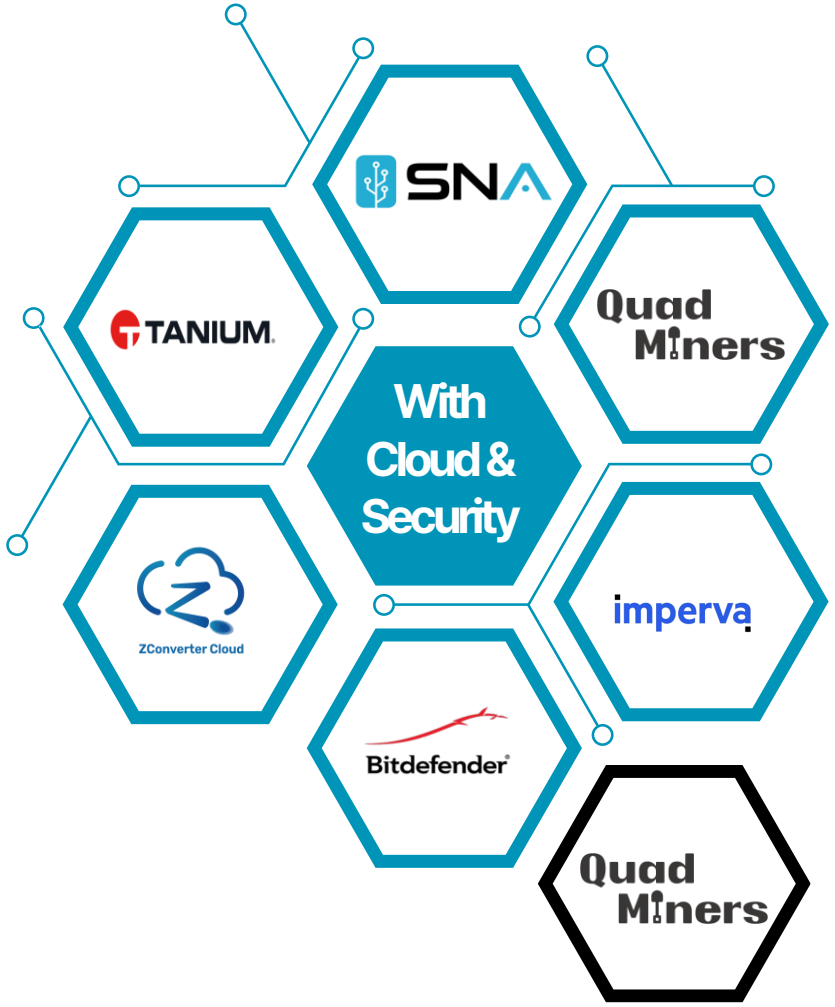
### 악성 트래픽 분석 및 대응관리 수립

- 악성 트래픽 상세 분석 후 Blacklist 및 Whitelist 관리를 통한 모니터링 F/W, IDS 등 기존 보안장비와의 연동
- 악성파일 정보를 백신업체에 전달하여 정책 추가 업데이트 권고

### 사후 추적의 시간/비용 절감

- 보안사고 발생 후 저장된 트래픽을 통해 명확한 사건 분석과 증적 자료 수집에 대한 시간과 비용의 절감
- 패킷 재조합을 통한 사용자 화면 재구성 및 증적(화면, 파일 등) 자료 확보

# With Cloud & Security - Next Generation SIEM




Quad Miners

## Next Generation SIEM

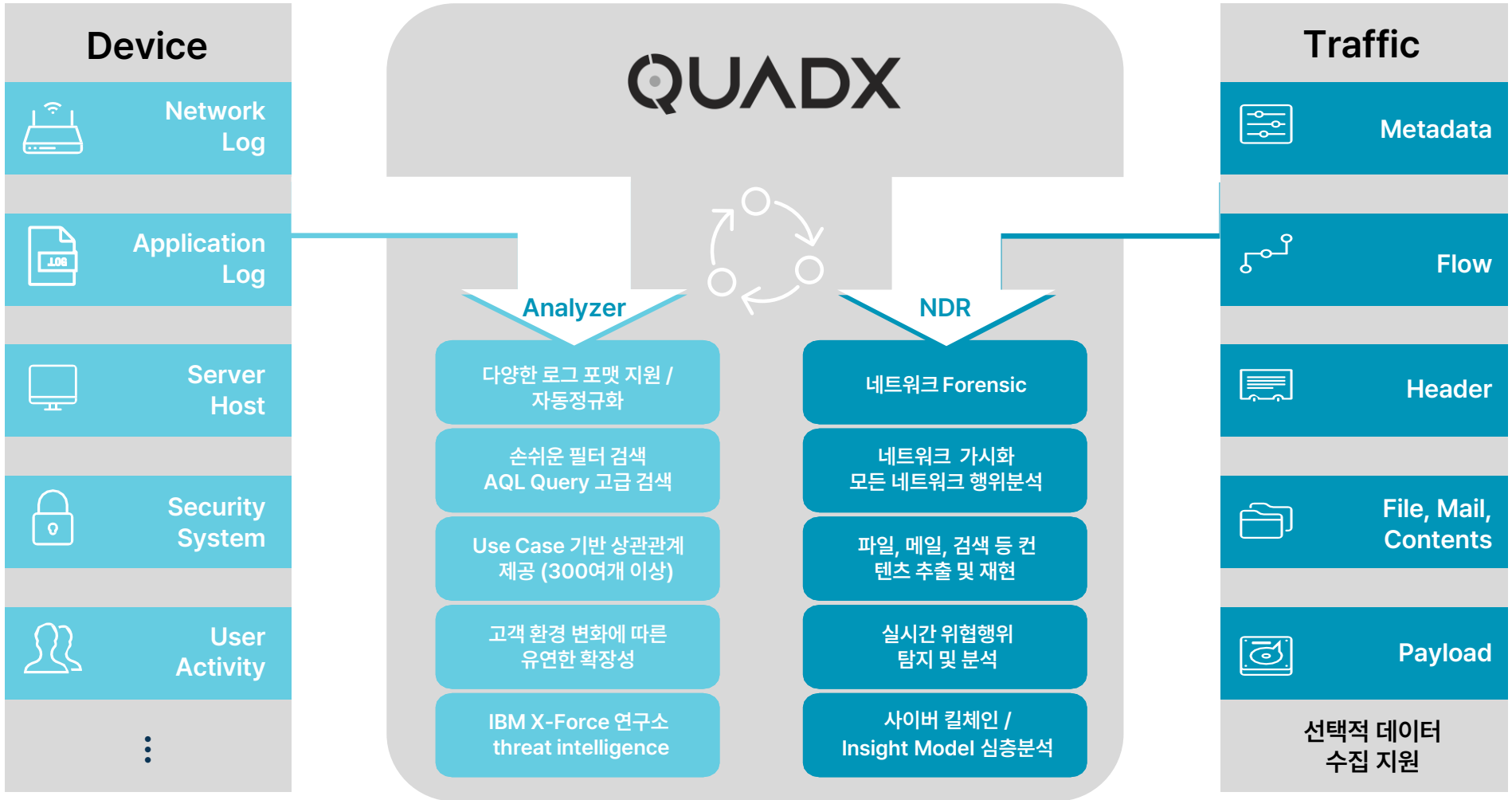
QUADX

기업내에 흐르는 모든 네트워크 통신 전체를 함께 분석하여 모든 종류의 사이버 보안 위협을 탐지하고 대응하는 차세대 SIEM 솔루션입니다.

| | |
|---|---|
| 제조사 | (주)쿼드마이너 (Quadminers) |
| 제품명 | QUADX |
| 제품구성 | QUADX NDR, QUADX Analyzer |
| 제품 특장점 | 모든 데이터에 가시성을 확보하여 위협을 탐지하고 분석할 수 있는 환경을 구성하고 쉬운 연계 및 데이터 분석을 통해 위협 정보 등 새로운 위협을 탐지하는 기능을 제공합니다.<br><br>• 전체 가시성<br>정규화 / 카테고리 / 추가 분석 정보 / 모든 영역의 정보 수집<br><br>• 위협 탐지 우선순위<br>MITRE ATT&CK / 분석 모델링 / 경보 연관성 / 글로벌 위협 정보<br><br>• 자동화된 분석<br>AI / 데이터 분석 / 머신러닝<br><br>• 통합 대응<br>플레이북 연계 / 자동화 연계 |

# With Cloud & Security - Next Generation SIEM

## 구성안



# With Cloud & Security - Next Generation SIEM

## Quad Miners와 IBM의 Collaboration

QUADX
NDR

- Integration
- 가시성
- 지도학습 기반 인공지능
  DPI (Deep Packet Intelligence)
- 심층적인 네트워크 트래픽 분석
  DPA (Deep Packet Analyzer)
- Full Packet
  DPR (Deep Packet Repository) & Big Data

Quad Miners

+

QUADX
Analyzer

SENSE ANALYTICS™

**행위 기반**
- 패턴 인식
- 사용자와 엔티티 프로파일링
- 통계적 분석
- 아노말리 탐지

**문맥 기반**
- 비즈니스 컨텍스트
- 엔티티와 사용자 컨텍스트
- 외부 위협 상관분석

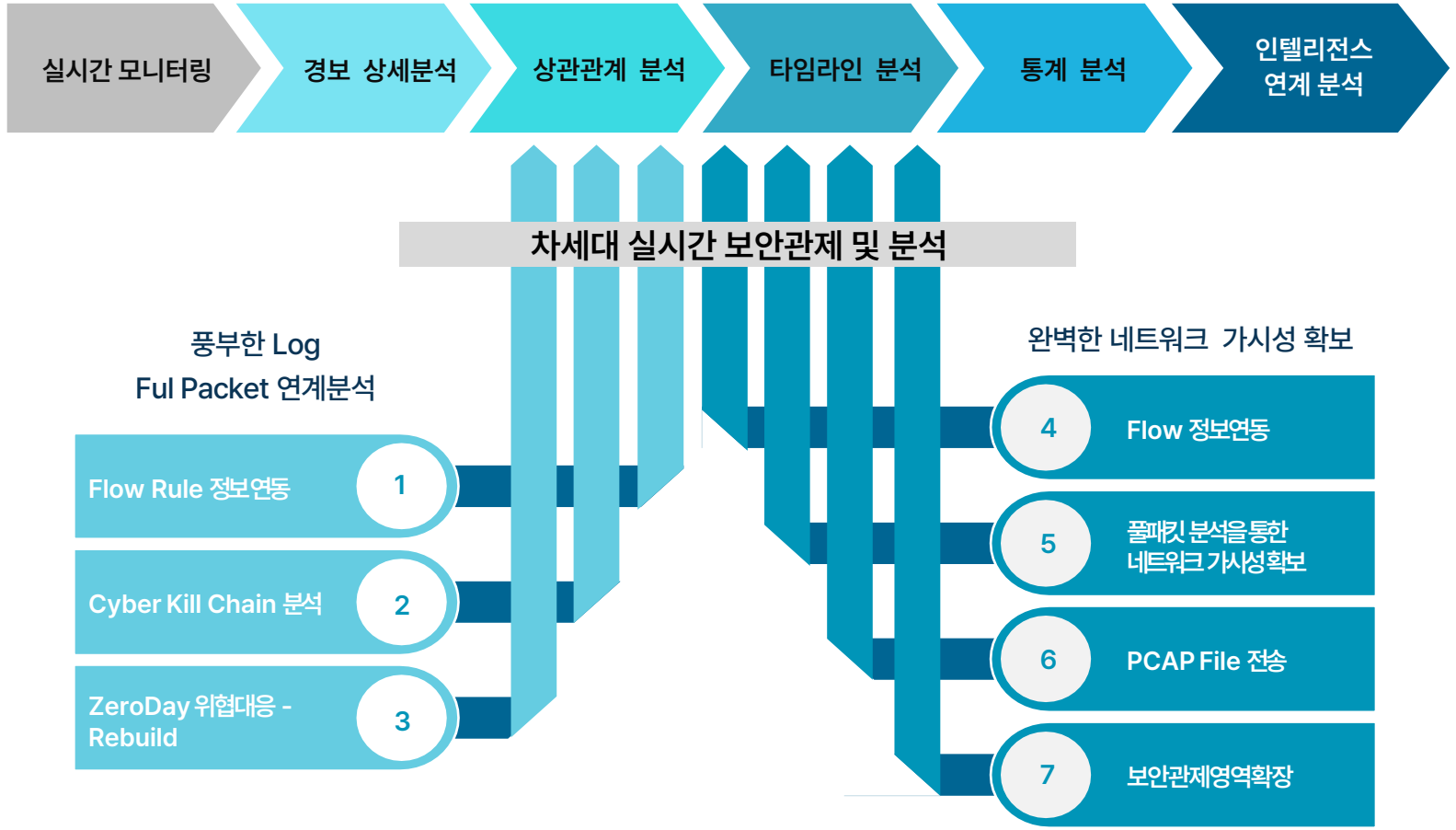
**시간 기반**
- 히스토리컬 분석
- 실시간 분석
- 위협 사냥
- 임계값 기반 룰

IBM Security

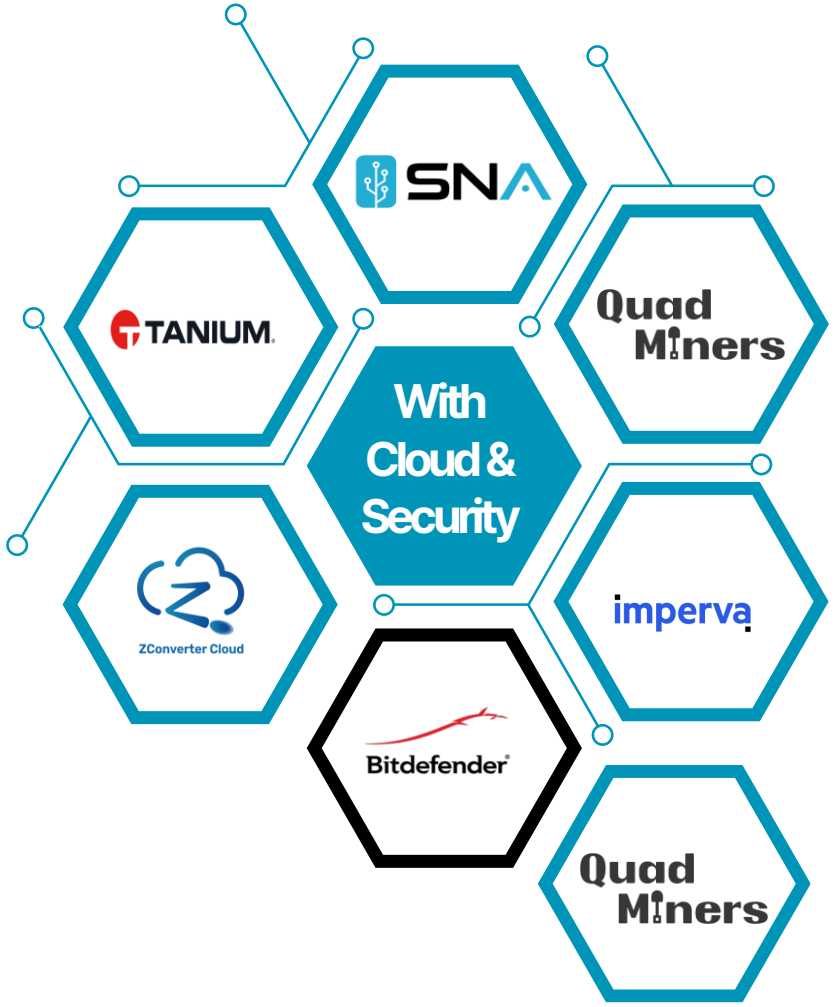
## 기대 효과

**QUADX는 담당자분들이 궁금해하는 Why라는 질문에 대한 답을 즉시 제공합니다. 이를 통해 보안위협 대응 시간을 50% 이상 줄일 수 있습니다.**

풀패킷 기반의 차세대 관제 솔루션 QUADX는 기존의 보안장비들을 우회해서 들어오는 내・외부 위협을 찾아내며 분석에 필요한 명확한 증적 자료를 제공하여 차별화된 네트워크 가시성을 제공합니다.



# With Cloud & Security – 백신 솔루션




Bitdefender

## 백신 솔루션

**GravityZone Business Security**

앤드포인트의 취약점을 점검하여 자동으로 조치하며 우수한 탐지 성능으로 완벽하게 보호합니다.

| | |
|---|---|
| 제조사 | 비트디펜더 (비트디펜더 코리아 (bitdefenderkorea.co.kr)) |
| 제품명 | GravityZone |
| 제품구성 | GravityZone Control Center, GravityZone Client |
| 제품 특장점 | • 중요 데이터 보호<br>- 해커가 민감한 기록이나 직원정보를 도용하지 못하도록 차단<br>- 간편한 비즈니스 보안 이벤트 분석<br>- 개인정보 보호 규정 준수<br><br>• 각종 보안 위협으로부터 해방<br>- 바이러스, 루트킷, 멀웨어, 피싱, 지능형 공격 차단<br>- 안티 랜섬웨어, 안티 익스플로잇, 콘텐츠 제어, 매체 제어<br>- 1시간마다 시그니처 자동 업데이트 : 사용자 비활성화 불가<br><br>• 간편한 설치 및 관리<br>- 이메일 주소 하나로 클라우드 콘솔 즉시 사용<br>- 네트워크 찾기를 통한 원격 설치<br>- 이미 설치된 안티바이러스 솔루션 자동 제거 |

# With Cloud & Security – 백신 솔루션

## 특징 및 차별성

GravityZone은 최고의 보호 및 최고의 성능, 통합적인 보안 및 효율적인 관리, 완벽한 제어&관리 및 비즈니스 생산성 향상을 보장합니다.

### 네트워크 공격 방어

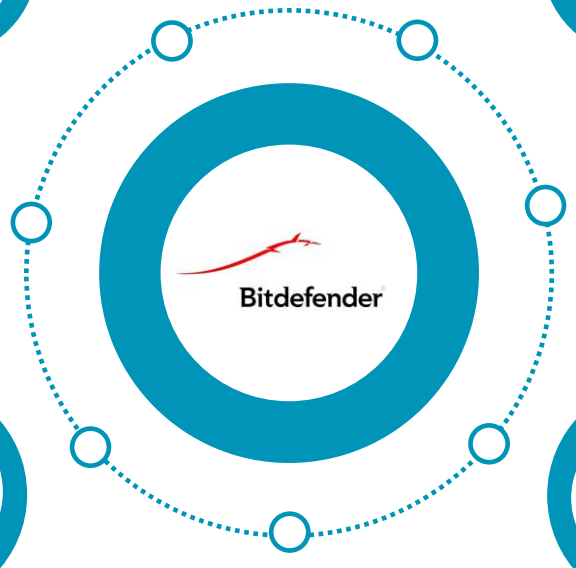
네트워크 취약점을 악용하여 시스템에 접근하려는 공격에 대한 새로운 수준의 보호 기능을 제공합니다.

### 앤드포인트 위협 관리 시스템 – 내 PC 지키미

앤드포인트의 취약점을 효과적으로 식별, 평가, 개선하는 것은 보안 관리자 및 사용자의 업무 부담을 최소화하고 조직의 앤드포인트 보안 수준을 극대화 합니다.

### 앤드포인트를 위한 다계층 보호 방식

네트워크 취약점을 악용하여 시스템에 접근하려는 공격에 대한 새로운 수준의 보호 기능을 제공합니다.




### 수년에 걸쳐 완성된 AI와 머신러닝

비트디펜더는 선도적인 기술을 완벽하게 완성한 경험이 있으며 그 결과는 독립적인 평가 기관으로부터 명확하게 검증 되었습니다.

### 웹 기반 중앙 관리 – 하드웨어 불필요(클라우드 콘솔 제공)

GravityZone 중앙 관리 솔루션은 모든 보안 기능을 하나의 콘솔로 중앙 집중관리토록 하며, On-premise 타입으로 사내에 직접 구축하거나 비트디펜더가 제공하는 안전한 클라우드를 통해 즉시 사용할 수 있습니다.

### 가장 큰 보안 인텔리전스 클라우드

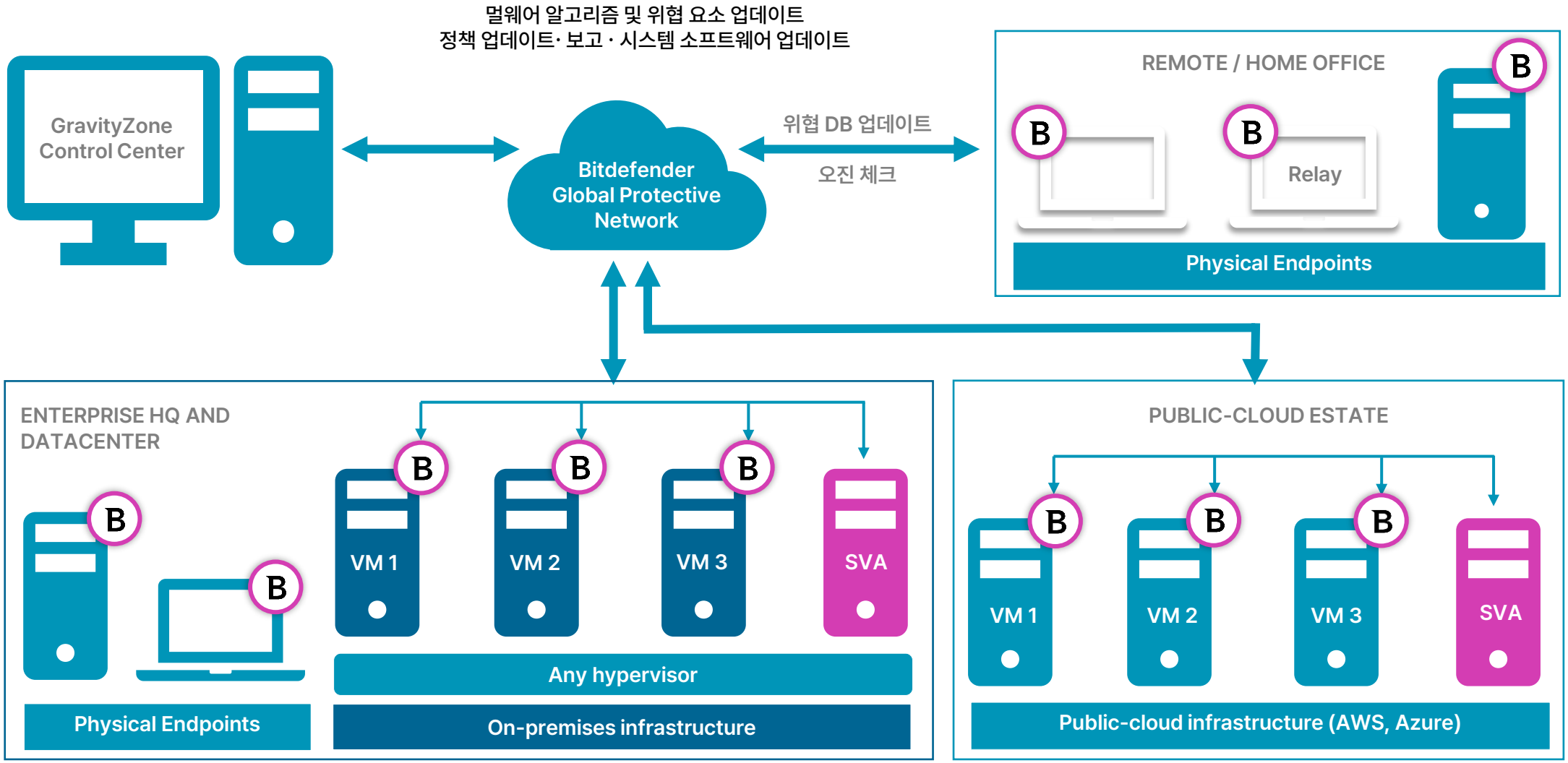
5억대 이상의 시스템을 보호하는 Bitdefender Global Protection Network는 하루 110억 건의 쿼리를 수행하고 머신 러닝 및 이벤트 상관 분석을 사용하여 사용자의 속도 저하 없이 위협을 탐지하고 차단합니다.

### 프로세스 행위 모니터링

제트 트러스트 모델에서 작동하며 사용자 모드 및 커널 필터를 사용하여 OS에서 실행 중인 프로세스를 지속적으로 모니터링 합니다.

# With Cloud & Security – 백신 솔루션

## 구성안



# With Cloud & Security – 백신 솔루션

## Bitdefender 계층화 된 차세대 앤드포인트 보호 플랫폼

일반적인 안티-멀웨어 솔루션은 이미 구성된 보호 모듈로 설치 패키지를 제공하지만, Bitdefender GravityZone은 고객이 필요한 보호 모듈을 직접 선택하여 구성할 수 있으며, 이미 앤드포인트에 설치가 완료된 상태일지라도 언제든지 보호 모듈을 추가하거나 제거할 수 있습니다.

### TRADITIONAL ANTI MALWARE

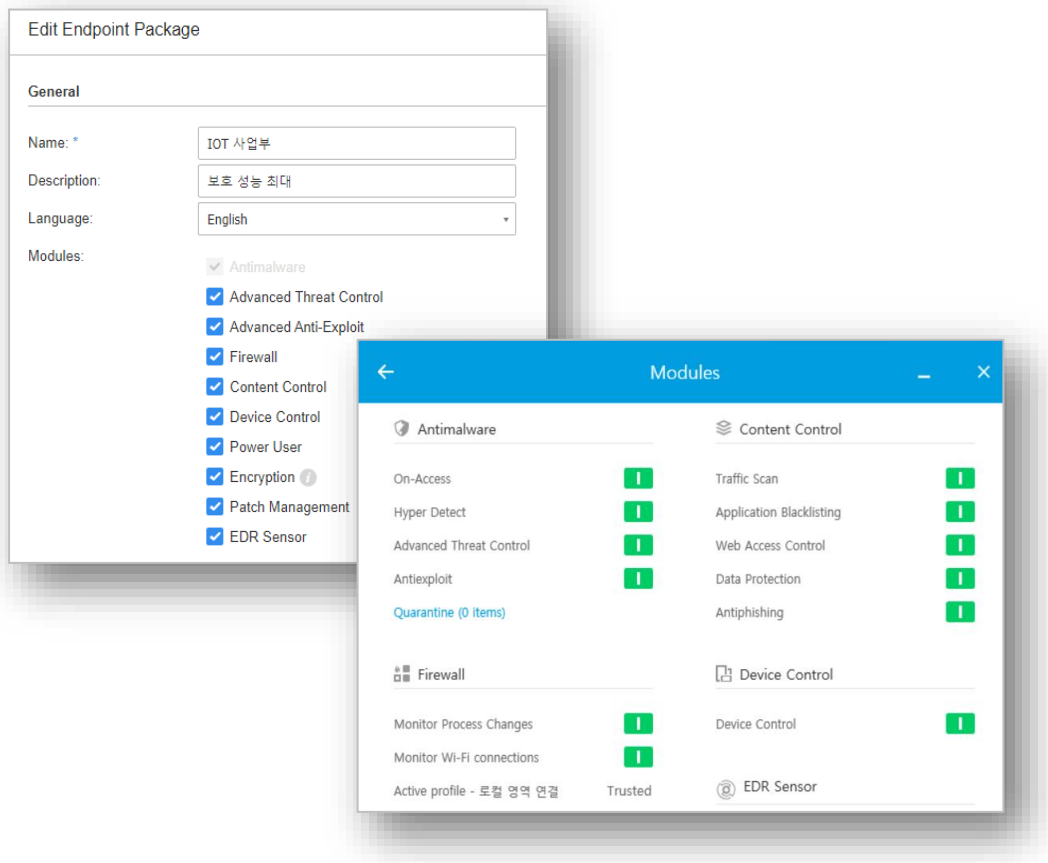
**안티-멀웨어 회사가 제공하는 설치 패키지를 그대로 사용해야 합니다.**

개발 회사가 기본적으로 구성한 안티-멀웨어, 방화벽, 매체제어, 웹 보호 등의 보호 모듈이 탑재된 상태에서 불필요하거나 다른 앤드포인트 솔루션과 중복된 보호 모듈을 제거 또는 새롭게 추가하기 어렵기 때문에 일반 기기와 저사양 기기 또는 특수 단말기를 구분하여 적용하기 어렵습니다.

### BITDEFENDER NEXT-GEN

**고객 환경에 맞게 필요한 보호 모듈을 직접 구상할 수 있습니다**

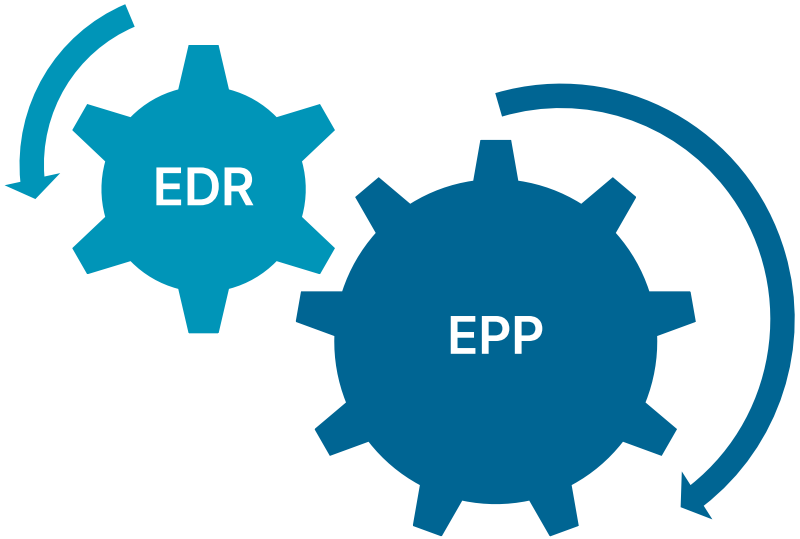
설치하려는 앤드포인트에 포함될 다음 기능들을 각각 개별적으로 선택하여 구성할 수 있으며, 이미 설치된 상태일지라도 언제든지 다시 구성할 수 있습니다.
안티-멀웨어, 잠재적 위협 차단, 안티-익스플로잇, 방화벽, DLP, 매제제어 , 디스크 암호화, 패치관리자(PMS), EDR 센서, 고급사용자 모드, 설치 언어 등



# With Cloud & Security – 백신 솔루션

## Bitdefender 계층화 된 차세대 EPP & EDR

차세대 방화벽, IPS, 네트워크 분석 장비(Sandbox), 안티바이러스 등 여러 개의 독립형 보안 솔루션으로 고도화된 정교한 위협 요소를 분석하려면  과도한 로그량, 이기종 운영 관리의 한계, SSL 암호화 트래픽 분석 한계, 오탐 발생 가능성 등이 존재하고, 위협 행위에 대한 연관 관계와 감염 경로를 분석하기 어렵기 때문에 빠른 시간 내에 효율적으로 대응하는 것은 사실상 불가능에 가깝습니다.




### EPP + EDR 솔루션 통합의 장점

- 정확한 탐지로 EDR 솔루션의 핵심 과제인 경고 누적 피로로부터 해방
- 정확한 분석 정보로 대응 노하우 및 보안 리소스 요구 사항 감소
- 보안팀이 실질적 보안 위협에 집중하도록 높은 정확성 제공
- 탁월한 운영 효율성과 높은 ROI 제공
- 독립형 보안 솔루션과의 연계 오용 방지
- 시간이 지남에 따라 진화된 보안 태세(위협 정보 향상) 유지

* EDR(Endpoint Detection & Response): 앤드포인트에서 발생하는 위협 행위에 대해 지속적인 모니터링과 함께 대응 방법을 제공하는 보안 솔루션으로 앤드포인트의 위협을 탐지, 분석, 차단, 격리, 치료하는 기능을 제공하며 안티바이러스 솔루션과 연계하여 가장 효율적인 대응 방법을 제시합니다.

* EPP(Endpoint Protection Platform)

# With Cloud & Security – 백신 솔루션

## 기대 효과

### 01
### 간단한 설치

며칠이 걸리지 않습니다, 몇 분이면 됩니다.
자동 설정키트가 데스크톱에서 데이터센터와
클라우드까지 설치를 간편하게 해줍니다.

### 02
### 보안 공백 없음

환경 인지형 에이전트가 물리적, 가상화, 클라우드
등 모든 형태의 앤드포인트를 보호합니다

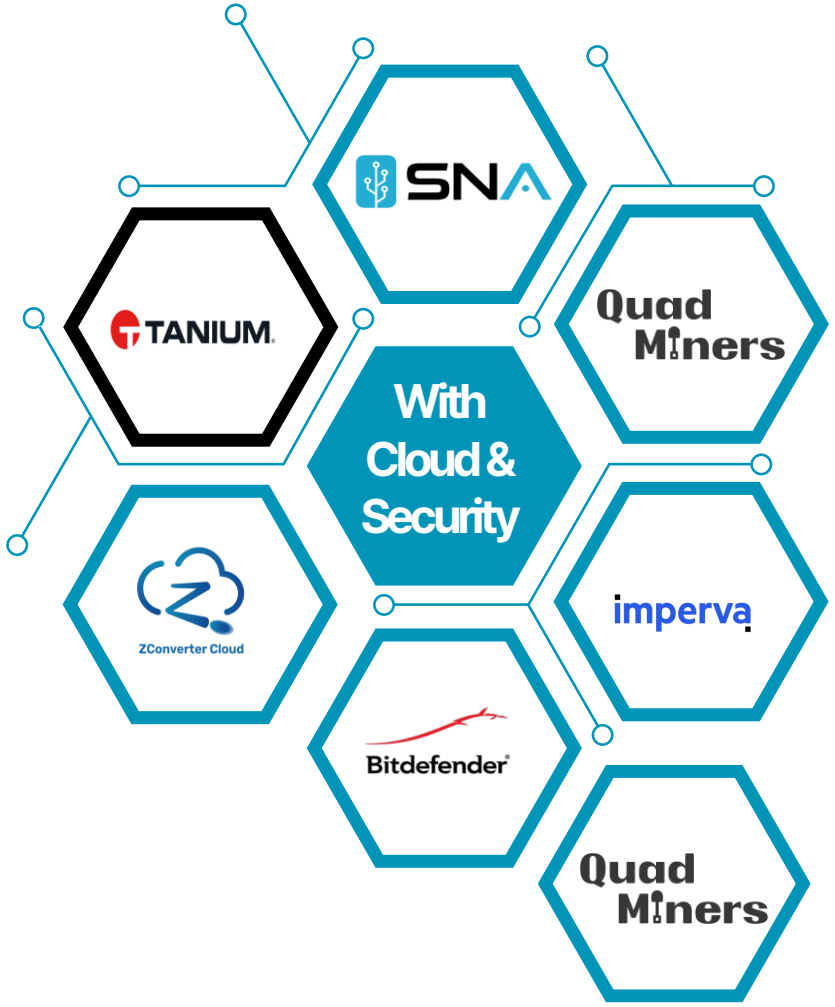

### 03
### 공격에 대한 보다 빠른 면역 체계

비트디펜더의 BRAIN (Bitdefender Reflective
Artificial Intelligent Networks) 기술은 세계
어느 곳에서 발생하는 새로운 위협도 3 초 안에
탐지하여 모든 앤드포인트를 보호합니다.


### 04
### 가상화 및 물리적 수행 자원
### 최적화와 위험 관리

데이터센터의 모든 앤드포인트 뿐만이 아니라
모든 컴퓨터에 대한 보안 업무를 개별 컴퓨터에서
하지 않고 가상 보안 장치가 수행하게 합니다.

# With Cloud & Security - Endpoint 보안 관리 플랫폼




## TANIUM의 통합 앤드포인트 관리
(Unified Endpoint Management)

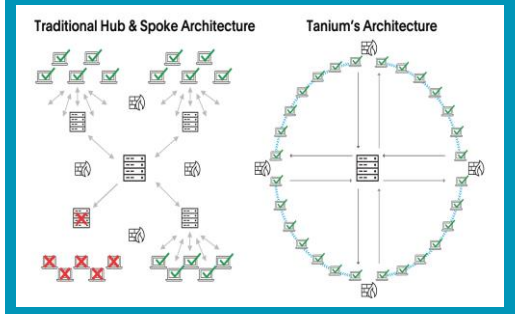
TANIUM

모든 사용자, 서버, 클라우드 앤드포인트를 관리할 수 있는 빠르고 유연한 통합 솔루션

| | |
|---|---|
| 제조사 | 태니엄 (TANIUM) |
| 제품명 | TANIUM |
| 제품구성 | Tanium Server, Tanium Agent |
| 제품 특장점 | • Inventory : 비인가 자산 파악, 인가 자산 관리<br>• Monitor : 단말 사용자의 행위 분석 및 서버 성능 모니터링<br>• Remediate : OS 및 SW 패치 관리, 단말의 일반/보안설정 변경 여부 파악 및 강제화<br>• Contextualize : 소프트웨어 자산간 종속성 매핑<br>• Identify : 비인가 자산 파악, 취약점 및 잘못된 구성, 설정 파악<br>• Protect : 보안 설정의 중앙 통제<br>• Recover : 위협에 대한 능동적 치료, 보안 설정의 복원 강제화<br>• Respond : 보안 위협 및 증적의 조사 및 추적<br>• Detect : 공격 징후 및 위협에 대한 탐지, 전사적 잠복 현황 파악 |

# With Cloud & Security - Endpoint 보안 관리 플랫폼

## 주요 특징

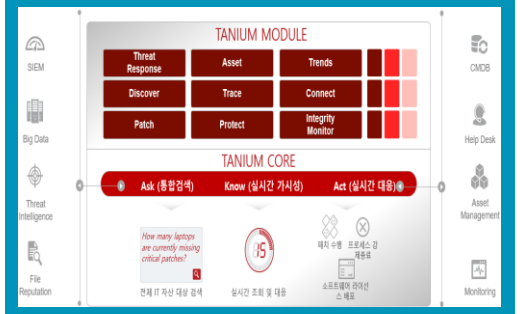



### 통신 아키텍처 (Linear Chain Architecture)

"문제의 원인은 통신 구조로 인해 발생되기 때문에 Tanium은 Linear Chain Architecture를 개발 하였습니다."

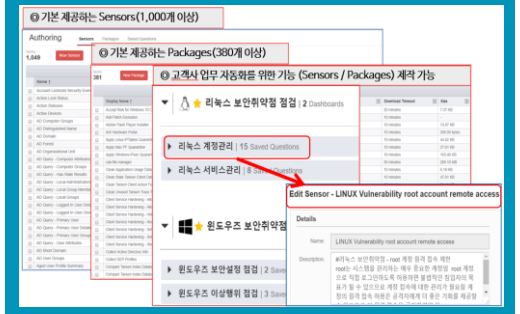

### 가시성 & 실시간 대응

"Tanium Core의 핵심 사용자 ASK, KNOW, ACT 인터페이스로 IT 및 보안 운영의 가시성과 실시간 대응방안을 제공합니다."




### 개방형 플랫폼 및 Tanium Module

"Tanium Core의 핵심 기능을 개방형 개발 플랫폼화하여 활용에 제약사항이 없습니다."




### 오픈된 소스로 기능 개발 (Sensor/Package)

"다양한 OS(Windows, Linux, Mac, Unix)에서 동작하는 기능의 소스가 오픈되어 기업마다 특화된 요구사항을 수정하여 적용할 수 있습니다."

# With Cloud & Security - Endpoint 보안 관리 플랫폼

## Tanium 활용 – 보안 및 IT 운영 업무 프로세스

**실시간 가시화를 통한 상황에 따른 우선순위 판단**

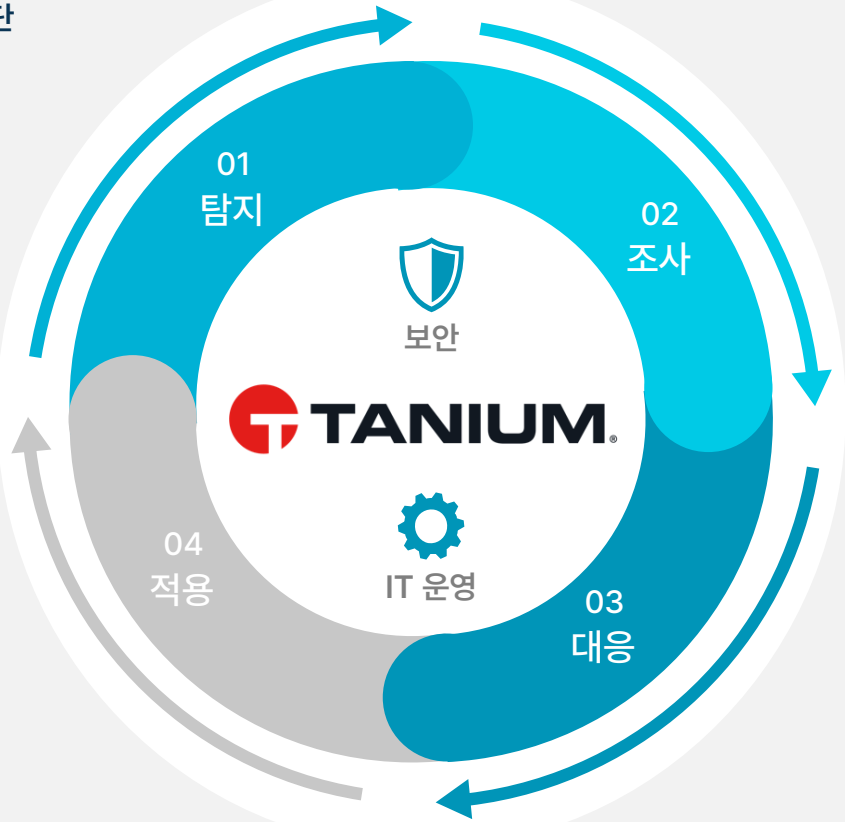
3rd PART HELP DESK SIEM IOCs

실제 이슈에 대해 빠르고 정확하게 집중

**운영 내에 보안환경 수준을 통합**

- ✓ IT 자산 관리
- ✓ 컨피거레이션 관리
- ✓ 패치 관리
- ✓ 위험관리 및 규제준수

전사적인 비용 효율적이고 신뢰할 수 있는 보안 적용




**대규모 환경에서 빠르고, 정확한 조사 완수**


신속한 응답: 무엇이, 어디에서, 어떻게 일어났는가?
현재 상황은 어떤가?

**대규모 엔드포인트에 대한 실시간 대응**


문제에 대한 신속하고 정확한 조치

# With Cloud & Security - Endpoint 보안 관리 플랫폼

## 업무 영역별 국내 활용 사례

| 영역 | 기존 업무 방식 | Tanium이 제공하는 업무혁신 | 비즈니스 목표 |
|---|---|---|---|
| 자산 관리 | 정기적 자산확인(년 1회)<br>자산의 DB화 | 실시간 미관리 자산 발견<br>미관리 자산을 자동적 관리 자산화 | 100% 실시간 자산관리 |
| OS 패치 | 정기적 패치 배포<br>사용자 주도의 패치 설치 | 보안이슈 발생 시 즉시/전체 패치 배포<br>대용량 패치파일 전사 배포 | 긴급 패치 배포<br>자동화 배포 |
| S/W 관리 | S/W 설치 후 확인<br>설치현황 DB화 | 실시간 S/W 현황 확인<br>미허가 S/W 실행 방지 및 자동 삭제 | 100% 실시간<br>확인 및 조치 |
| 계정 관리 | OS 설치 시 규정 적용/확인<br>서버 관리자의 수작업 | 전체 시스템 계정 내역 실시간 확인<br>계정 설정 시 적용 자동화 | 100% 실시간 계정 확인<br>및 적용 자동화 |
| 컴플라이언스 | 정기적 확인(년 1회)<br>컴플라이언스 이슈 시 확인 | 실시간 컴플라이언스 이슈 확인<br>컴플라이언스 자동 적용 | 100% 실시간<br>컴플라이언스 적용 |
| 보안 이슈 | 보안 이슈 발생 시 1회 점검<br>보안밴더에 종속적인 점검 | 보안 이슈 발생 후 지속적인 점검<br>고객 주도적으로 보안 점검 가능 | 보안 설정<br>적용 자동화 |

# With Cloud & Security - Endpoint 보안 관리 플랫폼

## 업무 영역별 국내 활용 사례

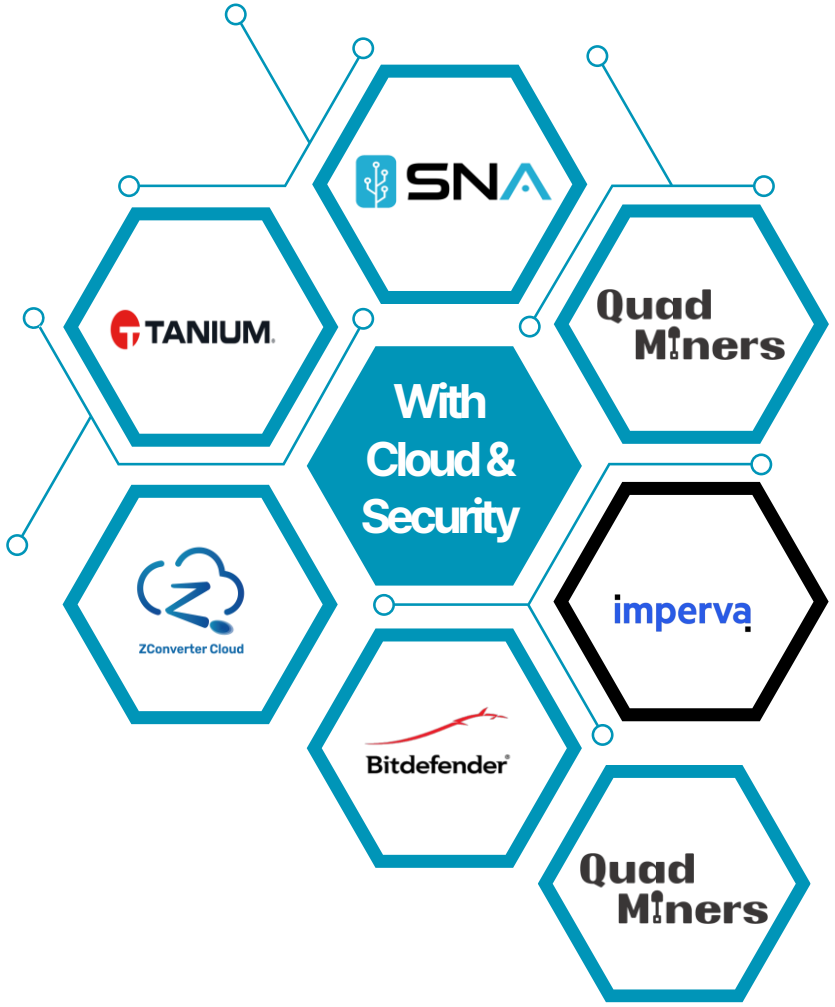
| | |
|---|---|
| **Threat Response** | • 보유중인 IOC, Yara 정보를 Tanium에 포팅하여 이상행위 탐지<br>• KISA로부터 제공받은 C&C IP로 과거 3개월간 회사 내 PC에서 접속한 기록 확인<br>• 자체 보안설정 적용 또는 컴플라이언스 현황 자동화<br>• Anti-Virus에서 판단한 의심파일을 자체 Sandbox로 자동 이관하여 더블체킹 |
| **Discover** | • 분산된 사업장별로 사용중인 PC, 서버, OA기기, 산업용기기 현황파악<br>• 미관리 자산에서 미허가 포트 오픈(80, 443, 445 등) 현황 확인 |
| **Patch** | • Windows Security Only 패치 자동 배포 설치<br>• Adobe, Java 최신 버전 자동 업그레이드<br>• Mac OS 강제 업그레이드 |
| **Trace** | • 서버 의심 프로세스 포렌식 수행<br>• 회사 내 랜섬웨어 공격 루트 파악(의심 PC, 공격대상 PC, 의심 프로세스 확인 |
| **Connect** | • SIEM으로 PC 상태(프로세스, 보안설정 현황) 데이터 전송 후 관제 수행<br>• Tanium으로 실시간 현황 정보를 BI도구(Tableau, Qlik)로 확인 |
| **Open API** | • HR & PC 관리 DB와 연동하여 PC 소유자, 사용자, 로그인한 사용자 차이 확인 |

# With Cloud & Security - Endpoint 보안 관리 플랫폼

## 앤드포인트 보안 시스템 비교자료

| 구분 | 일반적인 앤드포인트 보안 시스템 | Tanium 앤드포인트 보안 시스템 |
|---|---|---|
| 분석 및 대응 | **보안 솔루션별 개별 탐지/대응**<br>• Anti-Virus/ NAC/ PC관리 등 개별 앤드포인트의 대응 영역(Coverage)의 차이로 통합적인 분석/대응 불가<br>• 사이버안전센터에서 침해사고 발생 시 앤드포인트 통합보안관리가 불가함(개별 앤드포인트에 수동으로 관리) | **시그니처 기반이 아닌 이상행위 기반 탐지**<br>• 기존 시그니처 방식 기술(안티바이러스 등)의 한계를 극복한 새로운 행위기반의 악성코드 탐지 기술(IOC)<br><br>**위협 유입 경로 분석 및 대응**<br>• 악성코드 유입경로 분석을 통한 사전/사후 대응력 향상<br>• 악성코드 감염 시 신속한 분석 및 대응 가능<br>• 악성코드로 인한 피해 최소화 |
| 운영 | **다수의 엔드포인트 에이전트 설치에 따른 보안 운영 부담 증가**<br>• Anti-Virus/ NAC/PC관리 등 다수의 개별 앤드포인트 에이전트 설치에 따른 관리 부담 증가 | **Tanium을 운영하는 글로벌 기업에서 대규모 앤드포인트를 안정적으로 운영 중**<br>• Tanium은 대규모 앤드포인트 환경을 위해 개발된 솔루션으로 10,000 ~ 1,000,000대 환경에서도 안정적으로 운영 가능<br>• 기존 앤드포인트 솔루션의 근본적인 한계를 해결(Linear Chain Architecture)<br><br>**Tanium의 다양한 모듈을 통한 통합 관리**<br>• Tanium은 EDR, Patch, 자산, 취약점 진단 관리 등 다양한 모듈을 통해 하나의 솔루션에서 통합적으로 앤드포인트를 관리 및 운영<br>• SIEM, 인사 DB 등의 연계를 통해 기존 통합 보안 관제<br>• 시스템(SIEM)과 결합된 통합 보안 관리 시너지 효과 |
| 도입비용 | **개별 솔루션 별 중복 기능에 따른 비용 부담 증가**<br>• 기존 단위 보안 솔루션 별 중복 기능에 따른 솔루션 활용도 저하에 따른 운영 효율성 저하 | **도입비용 최소화**<br>• Tanium을 통해 기존 사용중인 솔루션을 대체하여 초기 비용 부담 최소화(기존 사용중인 패치관리, PC관리, 취약점 진단관리 대체) |

# With Cloud & Security - WAAP




imperva

## Next Generation SIEM

imperva

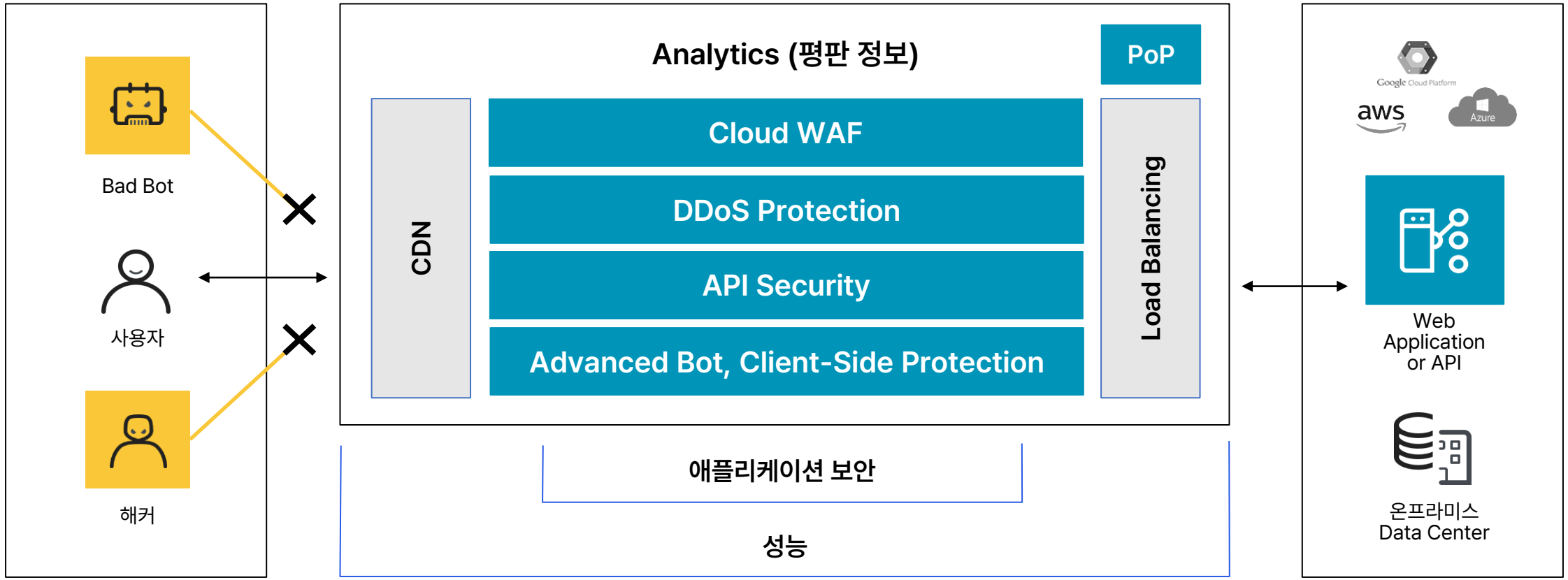
'Imperva'는 사이버 공격과 내부 위협으로부터 고객의 주요 비즈니스 데이터 및 어플리케이션을 보호하는 보안 솔루션 입니다.

| | |
|---|---|
| **제조사** | **임퍼바 (Imperva)** |
| **제품명** | **Imperva WAAP(Web Application & API Protection)** |
| **제품구성** | 웹 방화벽, DDoS 대응, 봇 관리, 크리덴션-계정탈취, API 보안 |
| **제품 특장점** | • 애플리케이션 보안<br>- 애플리케이션과 API를 자동으로 보호<br>- DDoS, 봇 및 공급망 공격으로부터 애플리케이션 보호<br><br>• 네트워크 보안<br>- 최적의 가용성, 액세스 및 대역폭 보장<br>- 파괴적인 봇 공격으로부터 애플리케이션 보호<br><br>• 데이터 보안<br>- 온프레미스 및 클라우드 환경 전반에 걸쳐 민감한 데이터 보호<br>- 규정 준수 및 감사 보고 간소화<br><br>• 클라우드 네이티브 보안<br>- DevOps에 뒤지지 않는 보안 제공<br>- 애플리케이션 및 데이터 저장소를 완벽하게 보호 |

# With Cloud & Security - WAAP

## 구성도

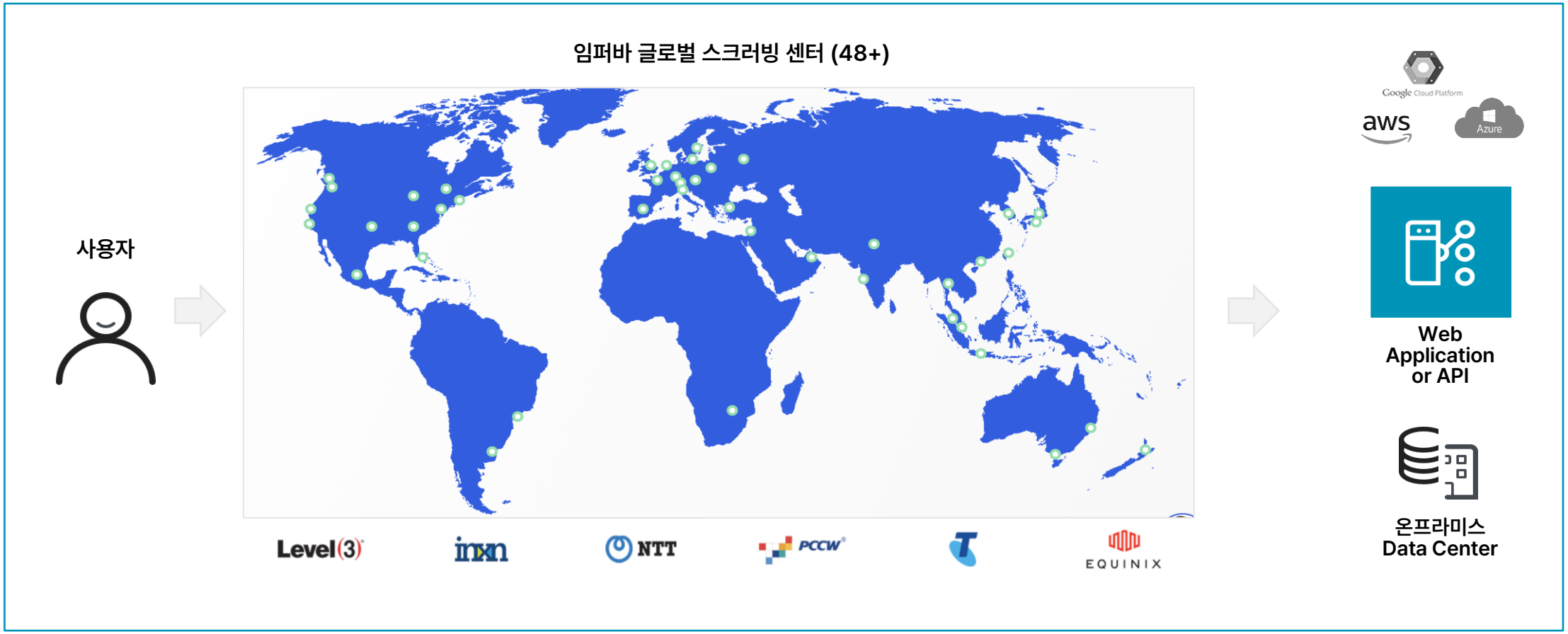
다양한 환경에서 운영중인 Application들을 WAAP를 통하여 통합 운영합니다.



# With Cloud & Security - WAAP

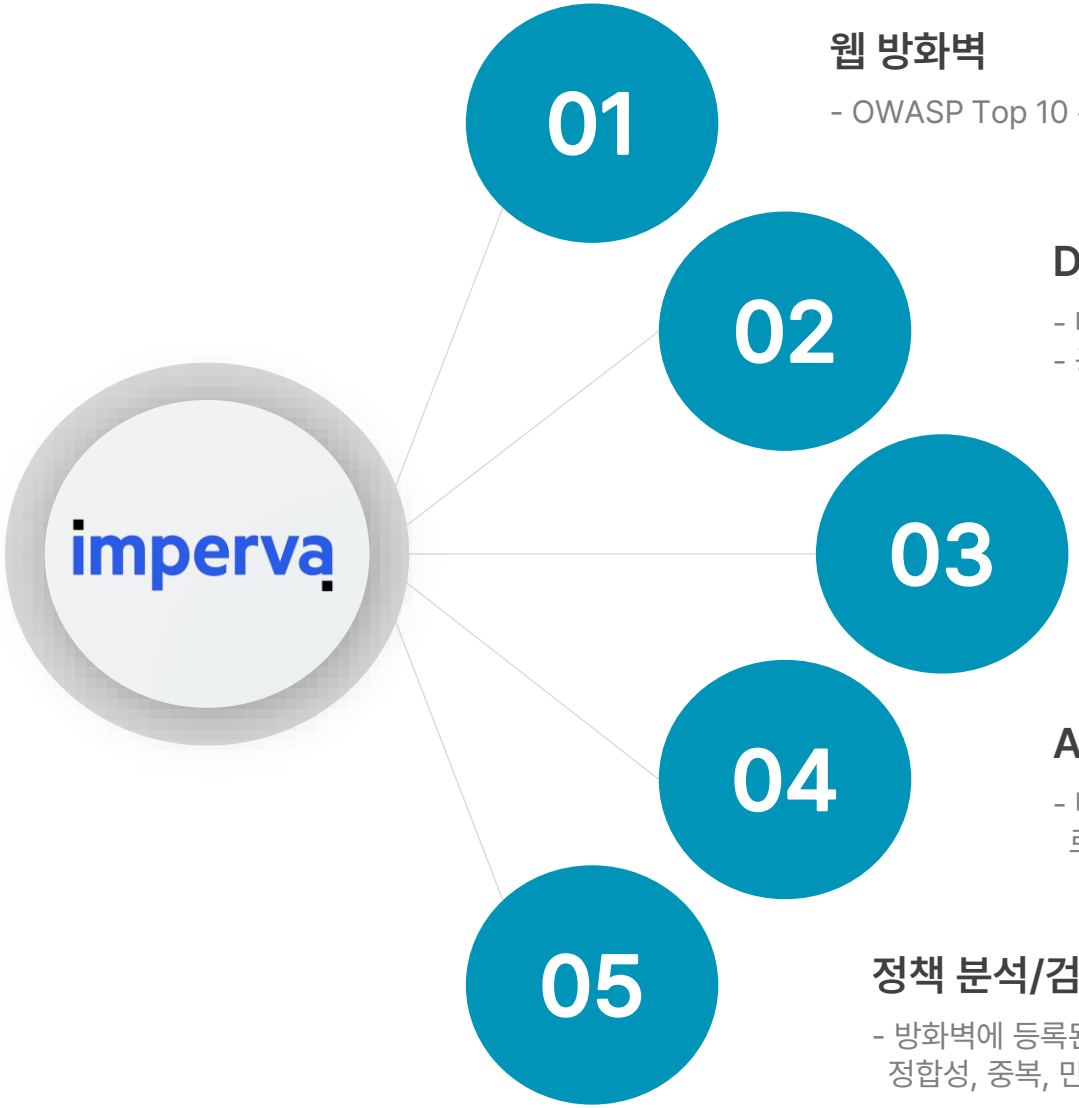
## 글로벌 인프라를 활용한 서비스 가용성 보장

- 국내 및 글로벌 48+곳의 스크러빙 센터 운영 및 T1 회선 사업자 계약을 통한 서비스 지연 시간 최소화
- 삼중 Mesh 구성을 통한 서비스 안정성 & 가용성 보장(99.99%)



# With Cloud & Security - WAAP

## 주요 기능




### 웹 방화벽

- OWASP Top 10 취약점 및 최신 앱 어플리케이션 위협에 대한 방어 서비스 제공

### DDoS 대응

- 대용량 디도스 및 어플리케이션 디도스 공격 대응
- 공격 차단 횟수 및 방어 용량 제한 없음

### 봇 관리

- 클라이언트 분류, 임계치, CAPTCHA 삽입, MFA를 이용한 기본 봇 방어
- 핑거 프린트, 머신 러닝 등을 활용한 자동화된 봇 위협 대응

### ATO(크리덴셜, 계정탈취)

- 다크웹을 통한 수집된 로그인 정보를 봇이 로그인 필드에 반복적으로 입력하여 로그인하여 개인정보를 수집하는 형태의 계정 도용 공격 차단

### 정책 분석/검증

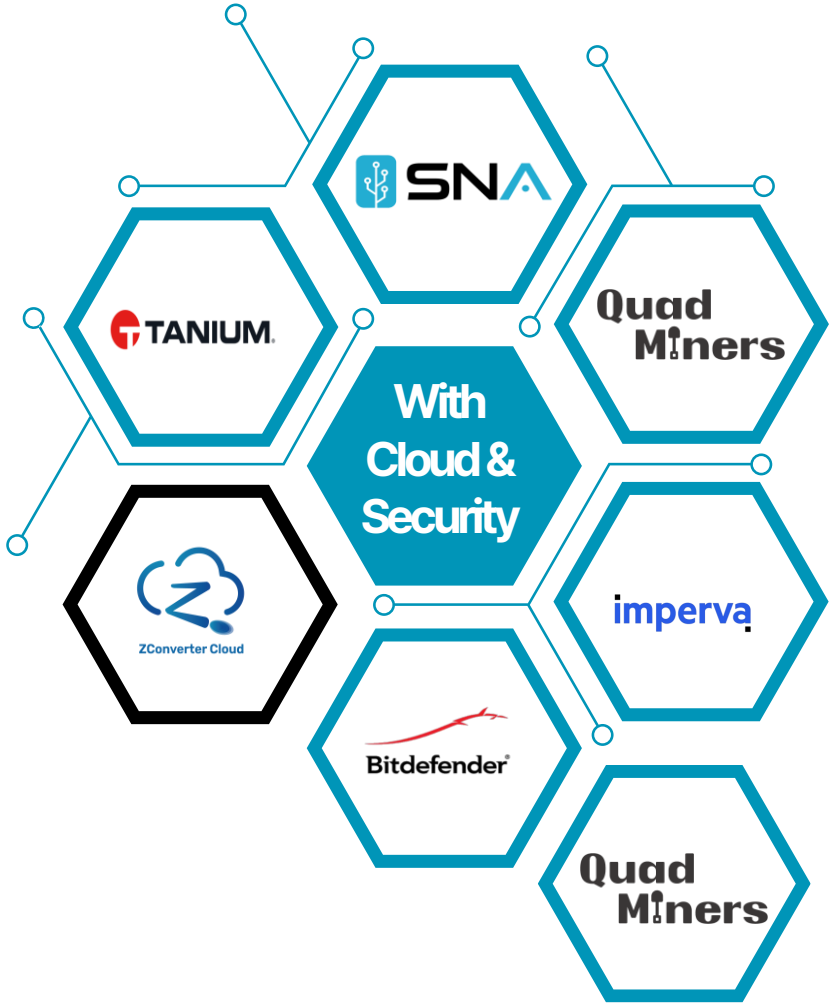
- 방화벽에 등록된 정책과 과거 신청정보의 유사도를 확인하여 위험성을 파악하고 정합성, 중복, 만료 등의 분석결과를 리포팅

# With Cloud & Security - WAAP

## 주요 기능별 라이선스 현황

| WAAP 보안 패키지 & 제공 기능 | App Protect Essentials | App Protect Professional | App Protect Enterprise | App Protect 360 |
|---|---|---|---|---|
| Cloud WAF (클라우드 웹방화벽) | o | o | o | o |
| Bot Protection<br>- Client classification, Rate limiting, CAPTCHA insert, Multi-factor authentication (기본 봇 방어) | o | o | o | o |
| DDoS - Website Protection (디도스 방어) | o | o | o | o |
| API Security (API 보안) | o | o | o | o |
| Content Delivery Network (CDN) | o | o | o | o |
| Application Delivery - Edge Delivery Rules | o | o | o | o |
| Reporting and Analytics (통합 리포팅 & Attack Analytic) | o | o | o | o |
| Services - Advanced Reporting | o | o | o | o |
| DNS Protection(DNS 보안) | o | o | o | o |
| Advanced Bot Protection - Account Takeover Detection (크리덴셜 탐지) | | o | o | o |
| Client Side Protection - Detection | | o | o | o |
| DDoS - Advanced Website Protection (고급 디도스 대응) | | o | o | o |
| Services - Proactive monitoring | | o | o | o |
| Advanced Bot Protection (w/ ATO Mitigation, 고급 봇 방어/크리덴셜 차단) | | | o | o |
| Client Side Protection - Mitigation | | | o | o |
| Application Delivery - Edge Load Balancing (엣지로드밸런싱-GSLB) | | | o | o |
| Runtime Protection (RASP – 런타임 애플리케이션 보안) | | | | o |
| WAF Gateway (설치형 WAF-GW 지원) | | | | o |

# With Cloud & Security – Cloud Migration




## ZConverter Cloud 클라우드 마이그레이션

ZConverter Cloud

온프레미스 환경과 클라우드 환경 간의 자유로운 마이그레이션을 지원하는 솔루션

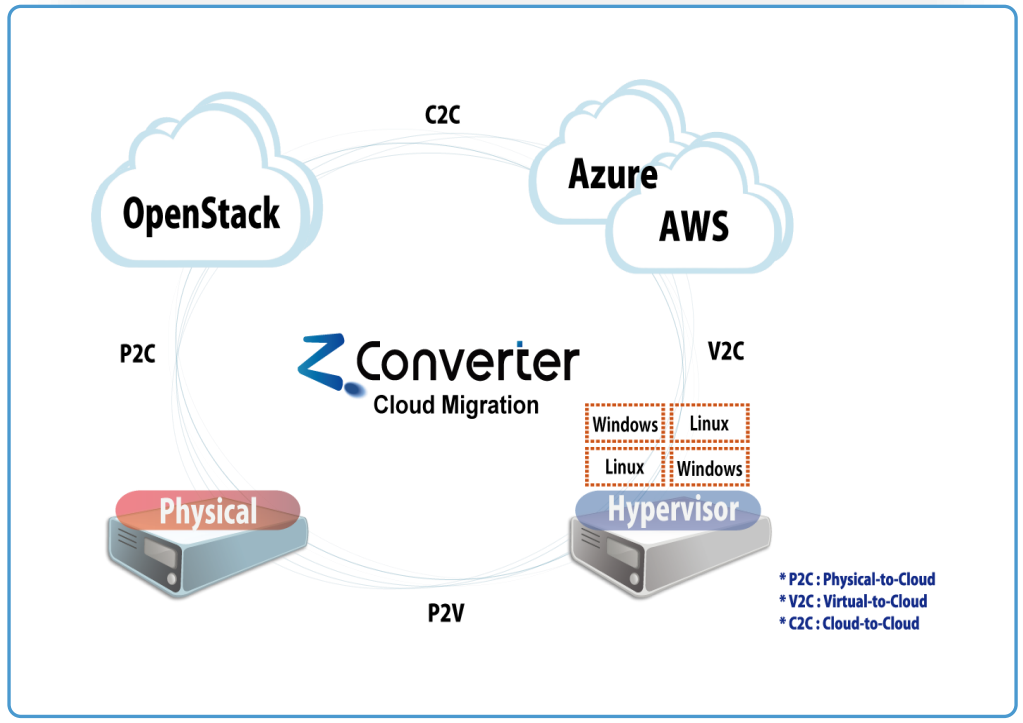
| | |
|---|---|
| 제조사 | (주)제트컨버터 클라우드 (Zconverter Cloud) |
| 제품명 | ZConverter (Cloud Migration) |
| 제품구성 | • 클라우드 기반 재난복구 솔루션<br>• 사내 또는 클라우드 워크로드를 보호하기 위한 OS, 데이터 백업 및 복구 솔루션 |
| 제품 특장점 | • 클라우드 마이그레이션<br>ZConverter 클라우드 마이그레이션 SaaS는 온프레미스 환경과 클라우드 환경(오픈스택, 클라우드스택, 마이크로소프트 Azure 및 아마존 AWS)간의 자유로운 마이그레이션을 지원합니다.<br><br>• 레거시 환경과 유연성<br>기존에 운용하던 프라이빗 클라우드를 퍼블릭 클라우드로 옮기거나, 또는 퍼블릭 클라우드에서 다른 종류의 퍼블릭 클라우드로의 이동도 가능합니다.<br><br>• Zconverter만의 특허 기술<br>ZConverter 클라우드 마이그레이션의 경우 현존하는 거의 90%의 클라우드 플랫폼들에 대해 완벽히 자동화된 마이그레이션을 지원합니다. |

# With Cloud & Security – Cloud Migration

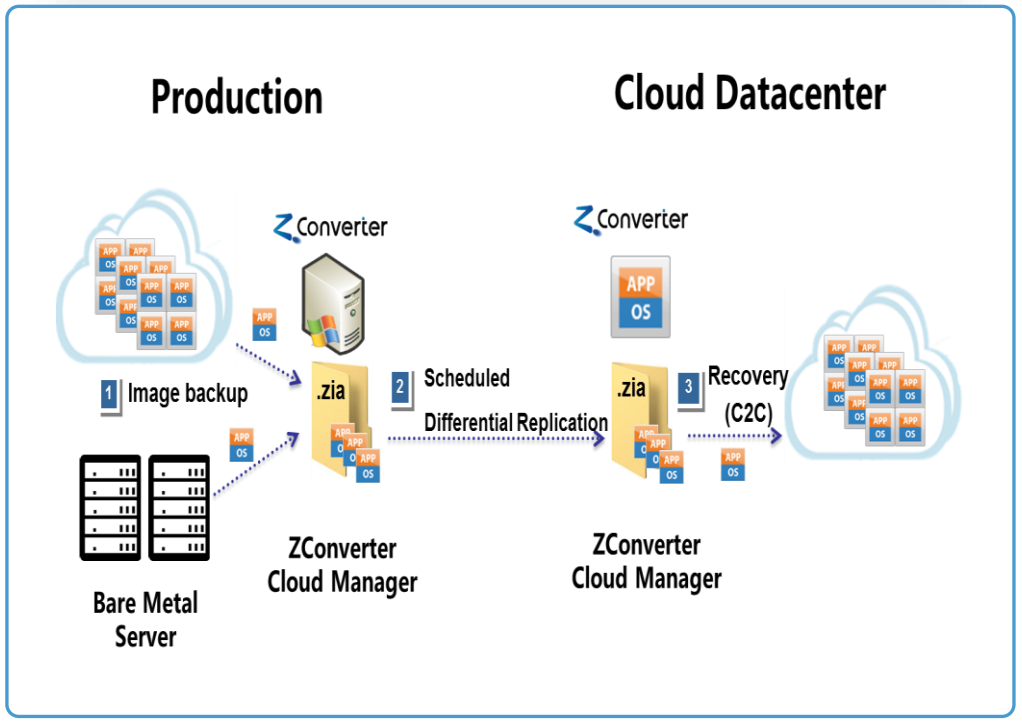
## 구성안

물리환경(IBM/HP/DELL)과 가상화 환경(VMware/KVM/Xen/Hyper-V) 또는 클라우드 환경(AWS/Azure/GCP/IBM/Alibaba/Oracle 등) 모두에 대한 OS레벨의 마이그레이션을 지원합니다.

### 물리, 가상, 클라우드 서버 마이그레이션




### Cloud DRaaS(Diaster Recovery as Service Process



# With Cloud & Security – Cloud Migration

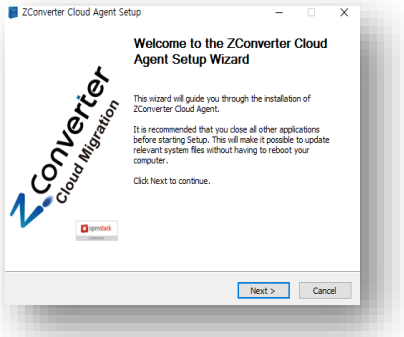
## Zconverter 기술적 이점

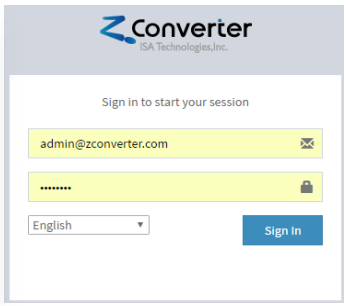
| | |
|---|---|
| **Migration & DR 서비스 원천기술 보유** | • OS 이미징 원천기술 보유 (경쟁사는 가상디스크 변환 오픈소스 사용)<br>• 이기종 복구 원천기술 보유 (경쟁사는 이기종 환경 간 별도의 드라이버 작업 필요) |
| **다양한 인프라 지원** | • 온프레미스 / 가상화 환경 지원<br>• 프라이빗 클라우드 환경 지원<br>• 퍼블릭 클라우드 환경 지원<br>• 네트워크 단절환경 / 다중 네트워크 환경 지원 |
| **운영 관리** | • 운영환경의 부하 최소화(No Reboot)<br>• 운영서비스 중지 없이 라이브 환경의 서비스 지원(Live backup/Live replication)<br>• SaaS형태의 서비스 지원(서비스 구성 편의성 증대) |
| **편의성** | • 멀티 클라우드 마이그레이션 절차 단일화<br>• 멀티 클라우드 DR 절차 단일화<br>• 멀티 클라우드 백업 절차 단일화 |
| **기술 지원** | • 제조사 엔지니어/개발자레벨 지원 제공<br>• 제조사의 한국어 레벨의 기술지원<br>• 커스터마이제이션 서비스 지원 |

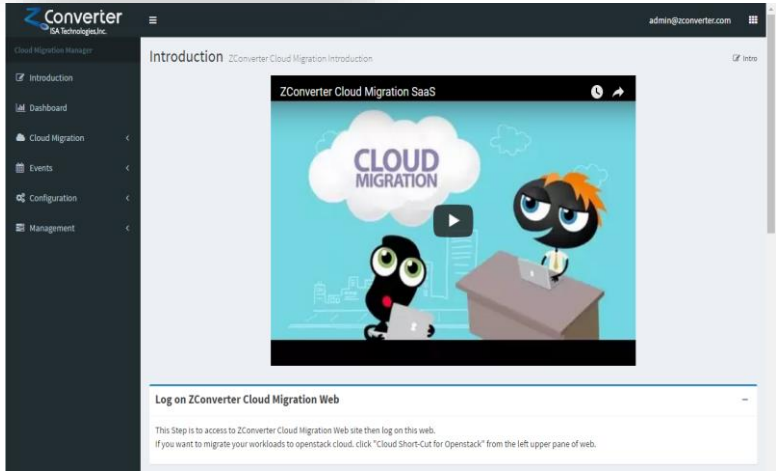
# With Cloud & Security – Cloud Migration

## 포털 및 대시보드

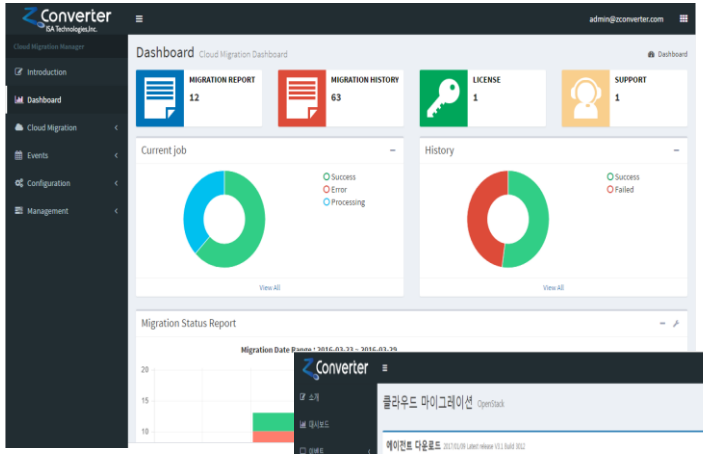
### Zconverter Cloud Migration 포털

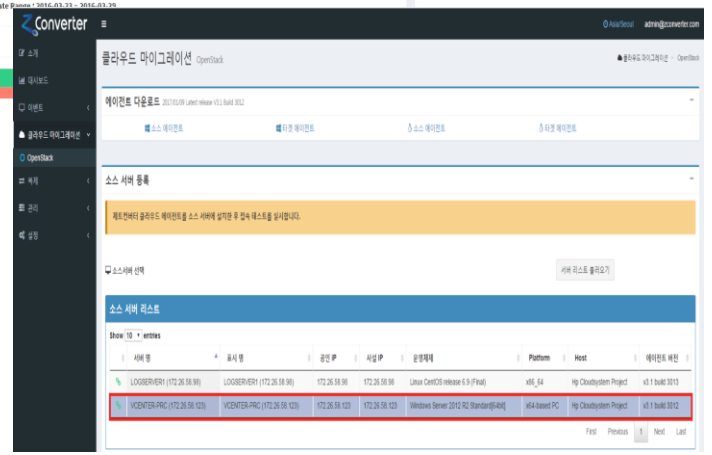



### 웹페이지 대시보드



# THANKS

SNA는 2023년에도 최선을 다하겠습니다


전화 문의 | 02-511-7060

홈페이지 | www.snainfo.com

제품 문의 | sna_sales@snainfo.com

기술 문의 | sna_tech@snainfo.com

마케팅 문의 | marketing@snainfo.com