



The bridge to possible

Secure Networking

Track A

황성규 상무

시스코 코리아 보안사업부

CISCO *Connect*

#CiscoConnect



SECURE

침해 사고 소개 (VPN, MFA, ZeroTrust, 보이스피싱, Chrome)



Software Vulnerability Information Reputation Center Library Support Incident Response Careers Blog Podcasts About



Cisco Talos shares insights related to recent cyber attack on Cisco

By Nick Biasini

RELATED CONTENT

Video: How propaganda can spread on social media via memes, fake news
OCTOBER 14, 2022 09:10

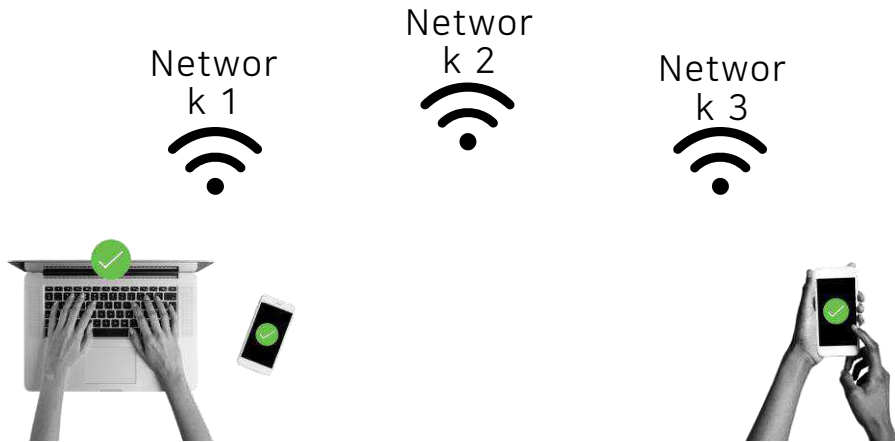
In this video, we'll look at a few examples of what essentially equates to propaganda spreading across social media, leading to false stories, headlines, posts and the continued degradation of the meaning of "truth."

Attackers target Ukraine using GoMet backdoor
JULY 21, 2022 08:07

Executive summary Since the Russian invasion of Ukraine began, Ukrainians have been under a nearly constant barrage of cyber attacks. Working jointly with Ukrainian organizations, Cisco Talos has discovered a

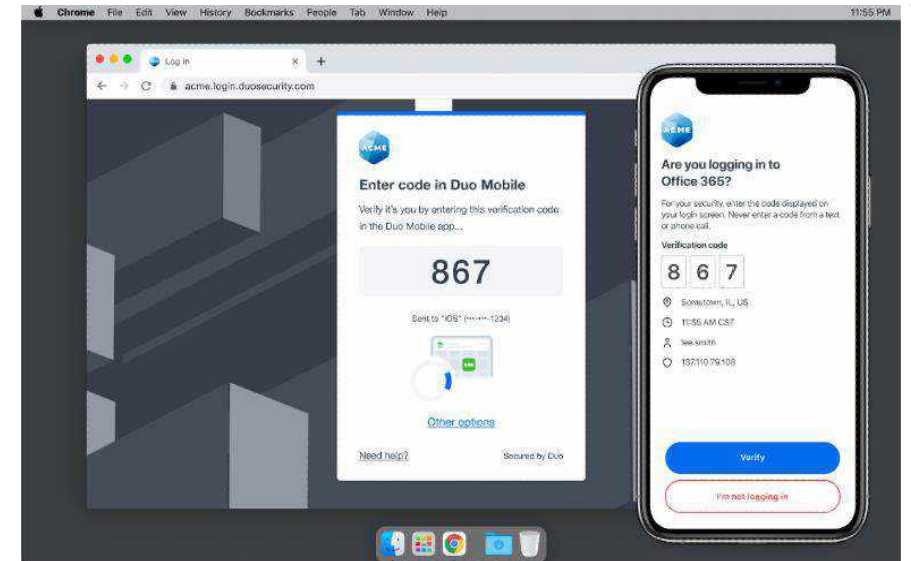
이후 강화한 접근 보안 정책

인증환경의 리스크를 산정하여 그에 맞는 인증 단계로 유도 (Risk Based Authentication)



WiFi 환경 변화 감지, ML 적용

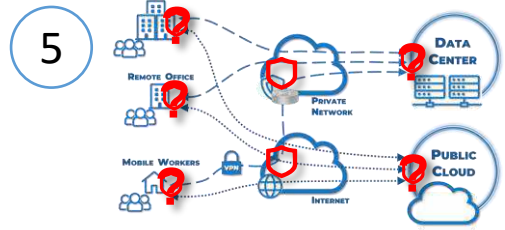
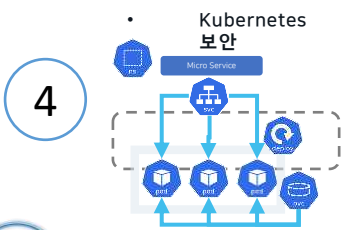
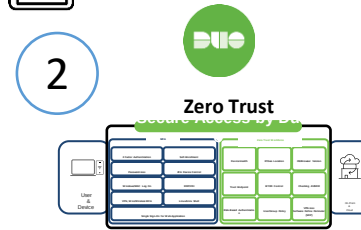
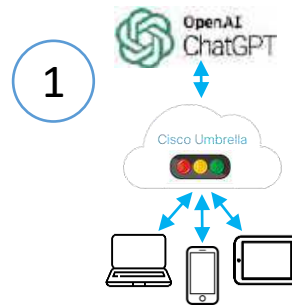
- Password-Less VPN 적용
- 2MFA 보이스피싱 시도를 막기 위한 IT 운영팀과 신청자 상호인증 방법도 적용



사용자의 접속 환경 분석 결과로 추가 검증

Track 세션 소개

1. 최신 보안 트렌드와 대응 전략
2. 사이버 보안의 핵심은 제로 트러스트!
3. 점차 지능화되는 사이버 위협, 지킬 것인가? 당할 것인가?
4. 비즈니스에서 승리하기 위한 애플리케이션 관점의 보안 및 관리 비결
5. Hybrid Cloud 환경에서 Secure Enterprise Network 구현
6. 메가존클라우드의 Cisco Meraki 기반 구독형 IT매니지드 서비스 F:it





SECURE의 계속되는 혁신 (2023년 상반기)

APPLE 과 Cisco Secure Access의 보안 협력

- Cisco CSA 를 통한 강력하고 빠른 아이폰/맥북 단말 보안 릴레이 네트워킹 지원

Generative AI 기술 도입

- 방화벽 정책 설정 도우미
- XDR 보안 분석 도우미

신규 보안 솔루션 인수 (2023년)

- Valtix - 멀티클라우드 보안 정책 단일화
- ArmorBlox - AI, 자연어처리 기능으로 이메일 보안 강화
- LightSPIN - CSPM 강화

NGFW 신규 모델 출시 (Firepower 4200, V7.4)



The bridge to possible

감사합니다

CISCO *Connect*

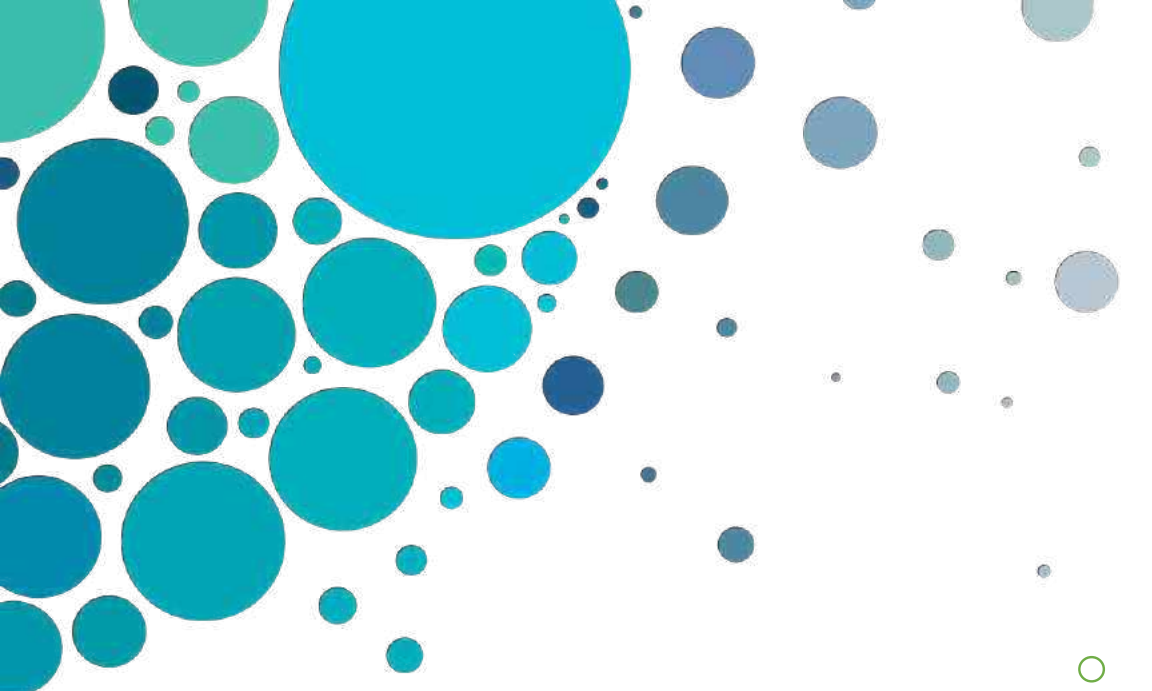
#CiscoConnect



The bridge to possible

최신 보안 트렌드와 대응 전략

김영근 프로 | 시스코코리아



Agenda

- 취약한 MFA로 인한 사이버 보안 위협
- Generative AI 기술로 인한 데이터 유출 위협
- 세션 요약

#1 취약한 MFA로 인한 사이버 보안 위험



**2FA Compromise Led to
\$34M Crypto.com Hack**



**The Uber Hack Shows
Push Notification 2FA Has a
Downside: It's Too Annoying**

VentureBeat

**Russian hackers exploited
MFA and 'PrintNightmare'
vulnerability in NGO breach,
U.S. says**



**MFA Fatigue: How
Hackers Breached Uber,
Microsoft, and Cisco**

IT WORLD CANADA

**Oktapus phishing campaign exploit
MFA to compromise 130 companies**

Forbes

**New Gmail Attack
Bypasses Passwords
and 2FA To Read All Email**



**Cybercriminals Launching
More MFA Bypass Attacks**

MFA 인증 우회를 목표로 하는 공격 기법

ATTACK TACTICS



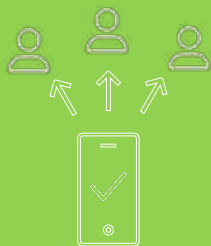
Push Bomb



SIM Swap Attacks



Domain Name Redirection & Spoofing



Push Spray



Endpoint OTP Attacks



OTP Phishing

Microsoft 365 타깃 공격 - ATP29

활동 시기
2022년 여름

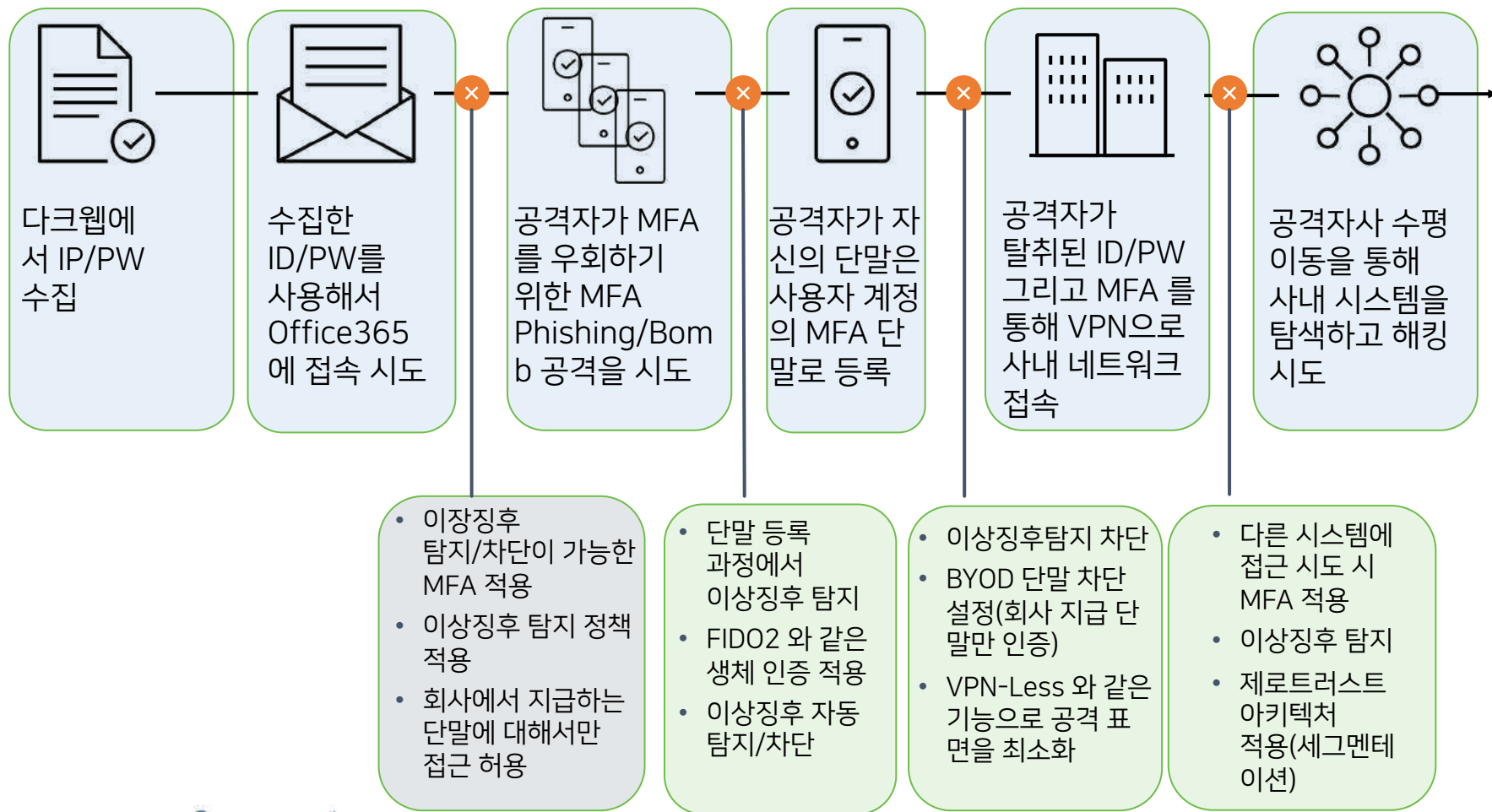


공격자 정보

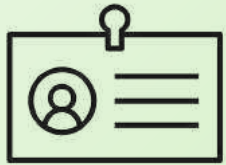
ATP29/Cozy Bear. Russian
nation state

공격 기술

- 무차별 대입 공격- [MITRE ID T1110](#)
- 공격자 단말 대리 등록 - 공격대상의 신분으로 위장하여 공격자의 단말을 이중 인증 기기로 등록 - [MITRE ID T1098.005](#)
- MFA 요청 생성 MFA 인증을 우회하기 위하여 피로도 공격을 유발하는 지속적인 인증 요청 시도 - [MITRE ID T1621](#)

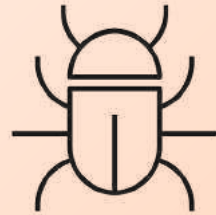


인증 프로세스를 강화하는 것은 선택이 아닌 필수



아이덴티티는
새로운 경계
보안입니다.

+



공격자는 ID
관리의 약점을
적극적으로
악용합니다

+



조직의 80%가
인증에 대해 추가
보안이
필요합니다.

2023 Cisco's Cybersecurity Readiness
Index

인증 위협을 차단하기 위한 Cisco Secure Access DUO

액세스 관리의 문제점과 해결 방안



검증되고 안전한 액세스 관리 솔루션의 조건

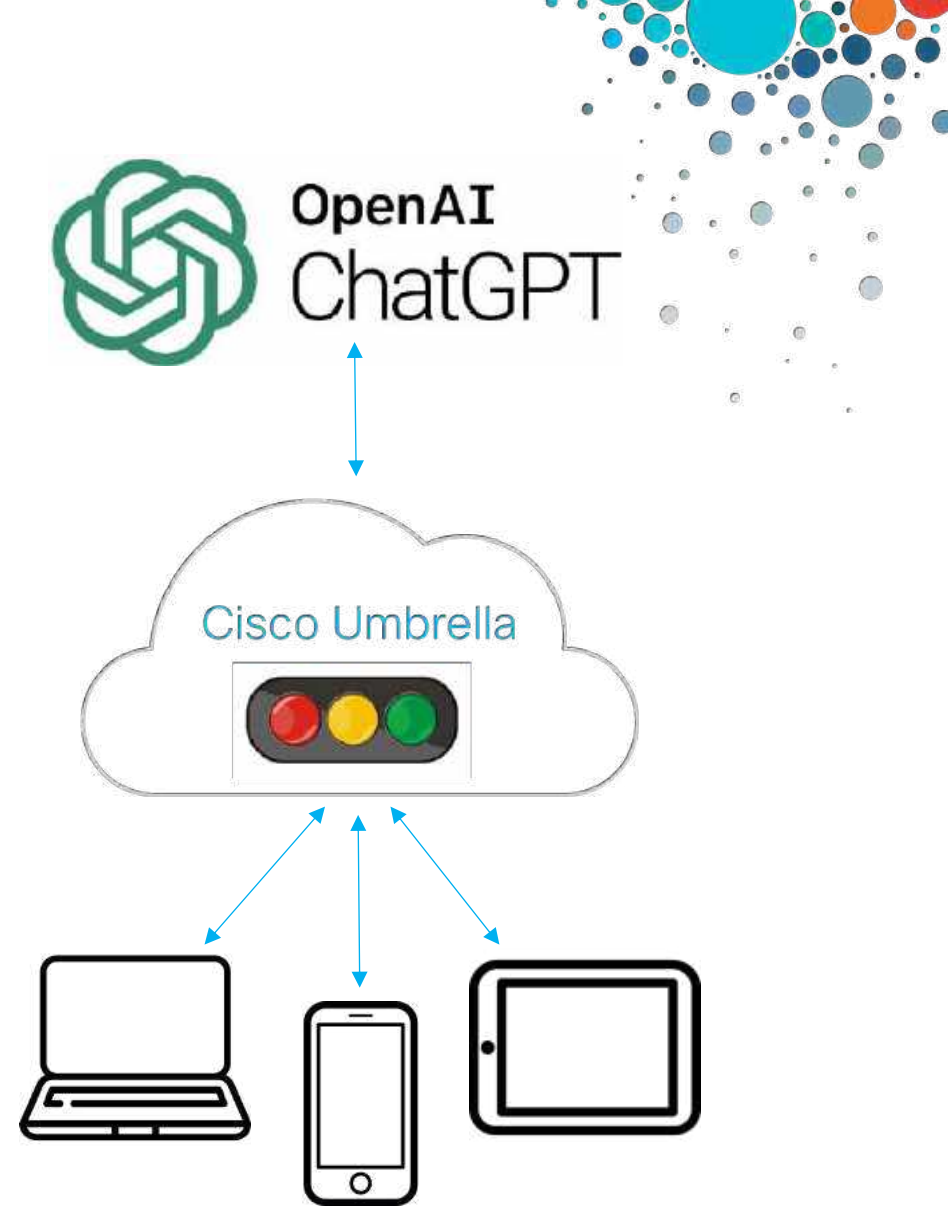


#2 Generative AI 기술로 인한 새로운 위협



Generative AI 와 내부자 위협

- 기밀 데이터 유출 및 컴플라이언스 문제
 - 개인정보 유출
 - 민감 정보에 대한 무의식적인 업로드
 - 신규 앱을 통한 알려지지 않은 기밀 정보 유출
- 소스 코드 및 기업 자산 유출 위험
- Generative AI 3rd Party 로 위장한 악성 코드 배포 위험



Cisco Umbrella 기능 - CASB!



CASB 솔루션을 통한 ChatGPT 통제 방안

새도우 IT 탐지 기술

OpenAI, Generate AI, Bard 등 승인 받지 않은 앱/어플리케이션을 탐지하고 자동 차단

신규 OpenAI 기술을 활용하고자 하는 경우에는 IT보안팀의 검토 필요

보안 담당자들은 인텔리전스 정보를 통해 해당 앱이 정상적인 앱인지, 배포자는 누구인지를 확인 후 승인

어플리케이션 통제

사내 접근 정책을 적용하여, OpenAI를 사용할 수 있는 그룹과 사용할 수 없는 그룹으로 나누어서 정책 설계

OpenAI 웹/어플리케이션에 대한 사용량 통계 정보를 제공

데이터 유출 방지

OpenAI, Generate AI, Bard 등의 포털에 기업 데이터, 개인정보, PII, 소스코드에 대한 키워드 탐지/차단

클라우드 저장소에도 동일하게 민감 정보 업로드 여부를 확인하고 탐지/차단

클라우드 악성 코드 차단

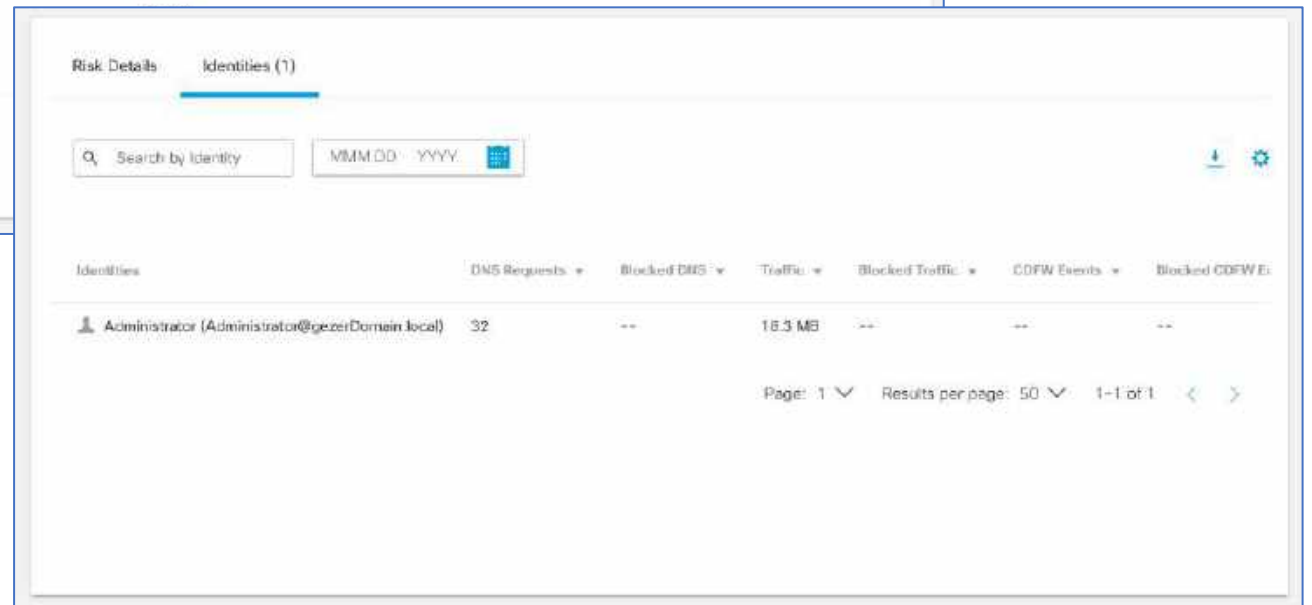
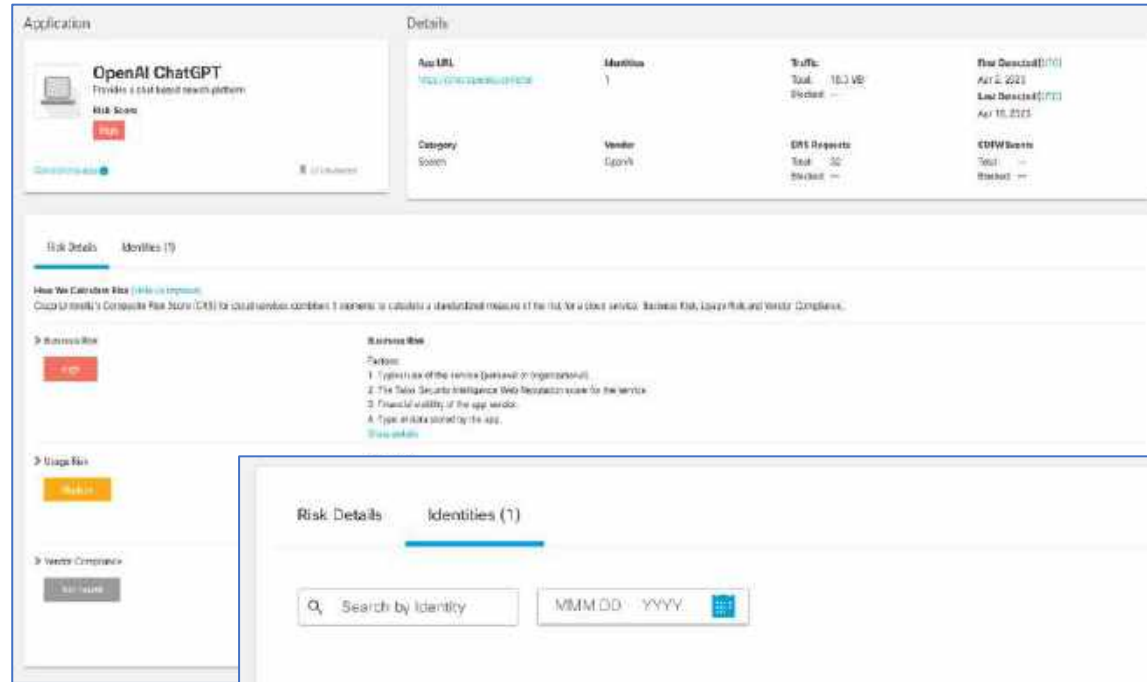
OpenAI 도구로 위장한 악성 앱을 사전에 탐지/차단

알려지지 않은 신규 앱에 대한 평판, 인텔리전스 정보를 제공.

정상적인 앱으로 위장한 악성 코드 확산 방지 및 사전 차단

Generative AI 위협 대응 - 어플리케이션 탐지

- 기업에서 사용하고 있는 모든 앱에 대해서 검색 기능을 제공.
- ChatGTP 와 같은 OpenAI 관련 툴은 Business Risk 를 검토하여 High 로 조정
- ID 별 사용량 및 접속 일시에 대한 확인 가능
- 보안 정책으로 고위험 앱에 대한 접근을 사전 통제 가능



Generative AI 위협 대응 – OpenAI 사용 제한

- 기업/그룹망에서 ChatGPT 사용을 원천적으로 차단
- 연구소 인원만 허용하는 그룹정책 적용
 - 연구소 인원은 ChatGPT 사용 가능
 - 영업직 인원은 ChatGPT 사용 불가
 - 동일 네트워크에서도 사용자에 따른 정책 적용 가능

The screenshot displays two configuration windows in the Cisco Connect interface. The top window, titled 'Default Settings', is configured with 'Applied To: DNS Policy', 'Items Allowed: 0', and 'Items Blocked: 7'. It shows the setting name 'Default Settings' and a search for 'chatgpt' in the 'Applications To Control' list, where 'OpenAI ChatGPT' is listed with an unchecked checkbox. The bottom window, titled 'My Application settings', is configured with 'Applied To: Web Policy' and 'Last Modified: Feb 23, 2023'. It shows the setting name 'My Application settings' and the same 'OpenAI ChatGPT' application in the control list, also unchecked. Both windows include 'CANCEL' and 'SAVE' buttons. A 'DELETE' button is visible at the bottom left of the interface.

Generative AI 위협 대응 - 기밀 정보 유출 탐지

- ChatGPT 사용은 허용하되, 기밀 데이터 유출 시도를 탐지/차단
- 기밀정보 예시
 - 기밀 정보(예: 법률 문서, 기업 정보)
 - PII
 - 개인정보
 - 지적 재산권
 - 카드정보
 - 소스 코드

실시간 규칙 수정

적용을 트리거하는 기준을 설정하려면 이 규칙을 구성합니다. Umbrella는 이 규칙의 ID 및 대상과 일치하는 아웃바운드 웹 요청의 콘텐츠를 검사합니다. 데이터 위반이 탐지되면 이 규칙의 작업 설정이 자동으로 적용됩니다.

규칙 이름

Chat GPT

설명 (선택 사항)

심각도

High(높음)

데이터 분류

선택한 데이터 분류를 검색할 위치를 선택합니다.

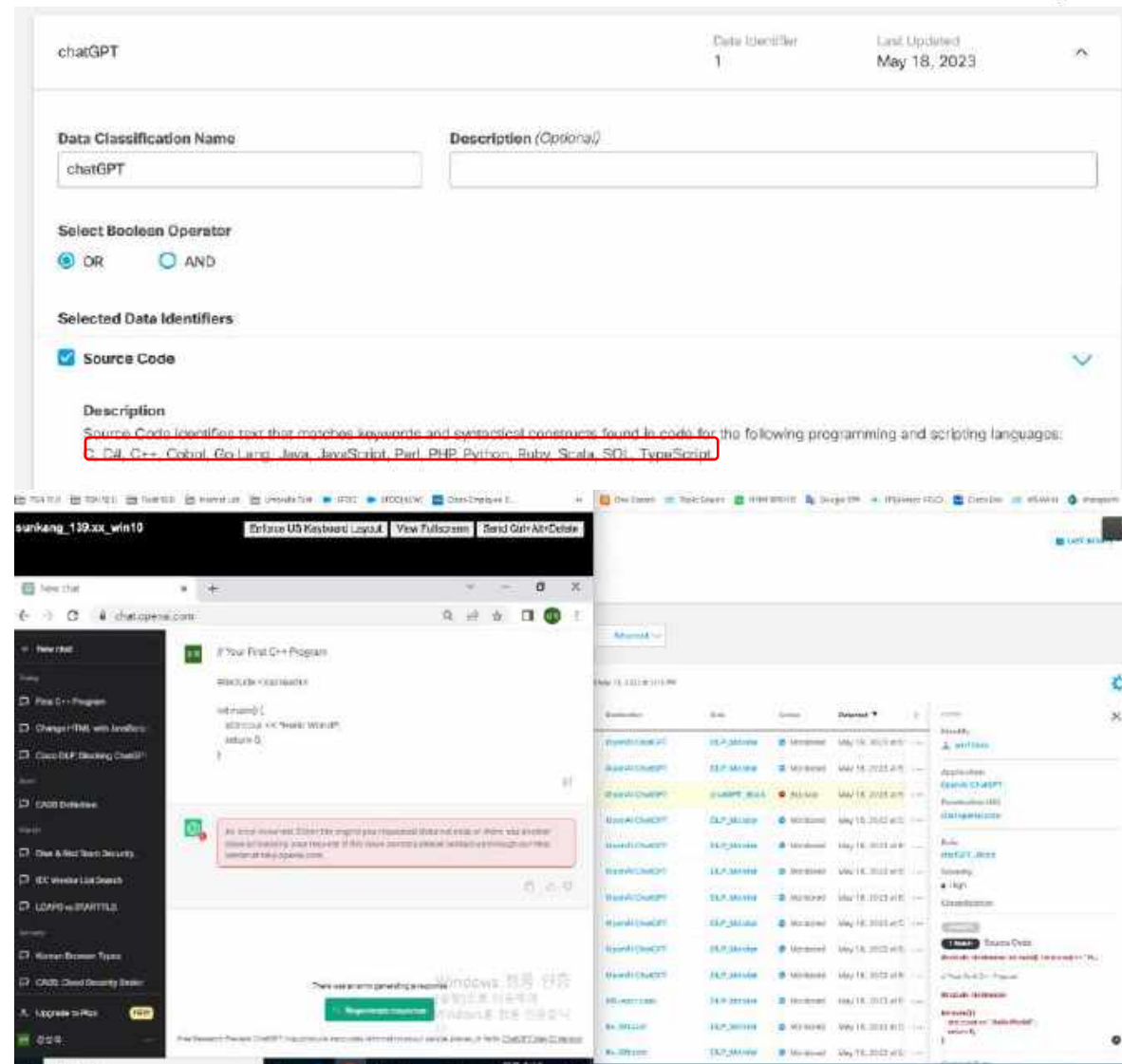
☒ 콘텐츠 ☐ 파일 이름 ☐ 콘텐츠 및 파일 이름

이 규칙에 추가할 데이터 분류를 선택합니다.

Q	분류 검색	
☒	안녕하세요	미리보기
☒	주민번호	미리보기
☒	주민번호, 대외비	미리보기
☒	hello	미리보기
☐	Built-in GDPR Classification	미리보기
☐	Built-in HIPAA Classification	미리보기
☐	Built-in PCI Classification	미리보기

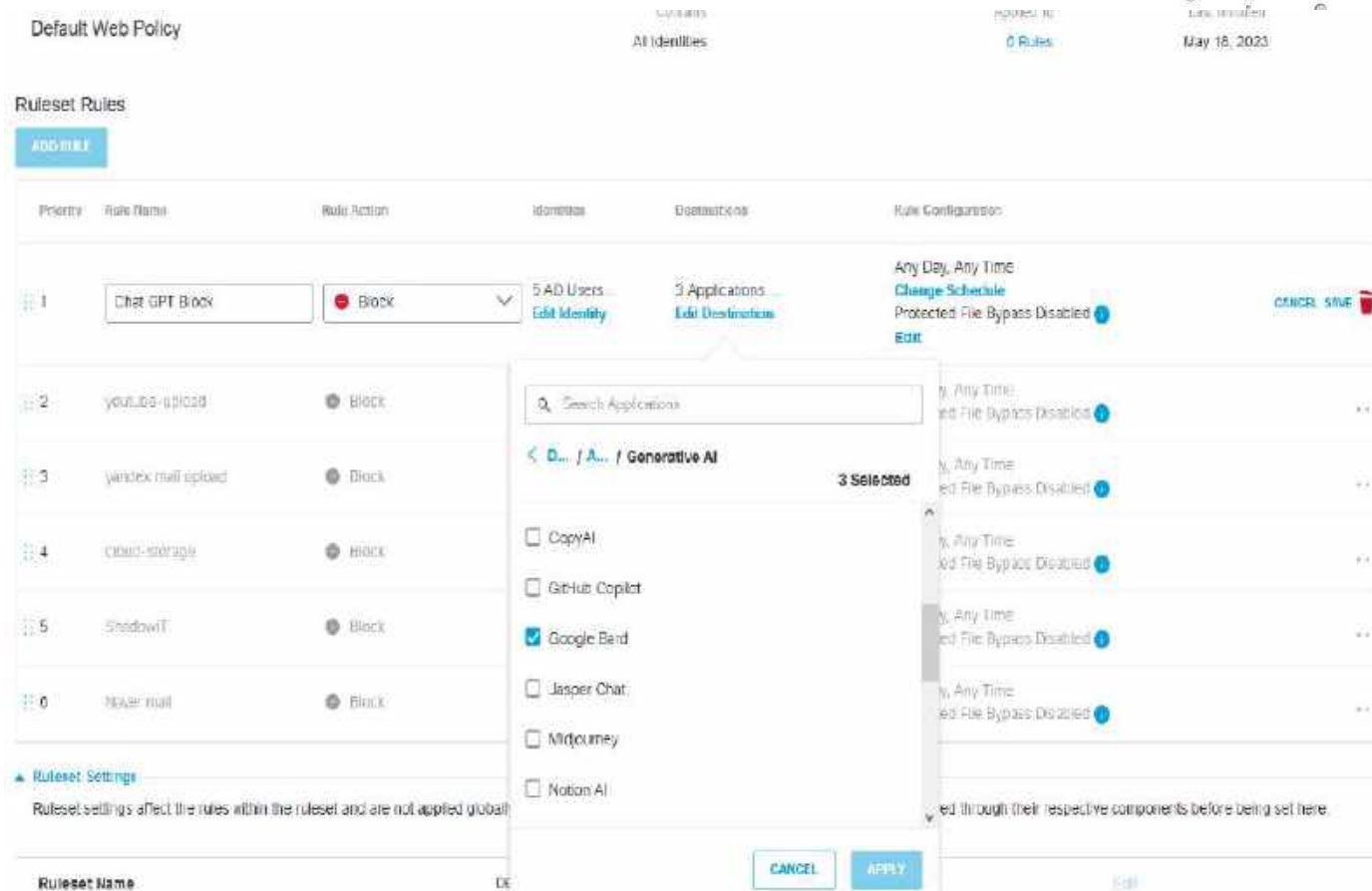
Generative AI 위협 대응 - 소스 코드 유출 탐지

- ChatGPT 사용은 허용하되, 소스 코드 입력 시, 사전 차단
- 지원되는 소스 코드
 - C, C#, Cobol, Go Lang, JavaScript, Ruby, SQL, TypeScript
 - 지원되는 소스 코드는 지속 업데이트 중



Generative AI 위협 대응 - 신규 오픈소스 AI 도구 탐지

- Cisco Talos 조직을 통해 신규 오픈소스 AI 도구에 대한 정보 주기적 업데이트
- 웹 분류에서 "Generative AI"를 통해 신규 AI 도구를 자동으로 차단 설정 가능
- 전 세계에서 파생될지 모르는 신규 오픈소스 AI에 대한 분석을 시스코 탈로스로 위임 가능



세션 요약

하이브리드 환경에서의 인증 보안

하이브리드 업무 형태로의 전환 과정에서 아이덴티티에 대한 위협이 지능적으로 변화하고 있습니다.

일반적인 MFA(Multi-Factor Authentication)가 아닌 이상징후를 탐지할 수 있는 보다 강력한 인증 보안 제품을 검토할 때입니다.

새로운 기술을 활용하기 위한 검증된 보안

많은 언론에서 Generative AI 를 통해 새로운 기술 도약의 기회가 왔다는 이야기를 하고 있습니다.

새로운 기술이 안전하게 사용되기 위해서는 검증된 보안 아키텍처를 빠르게 적용하고 기술이 안전하게 보호되어야 합니다.



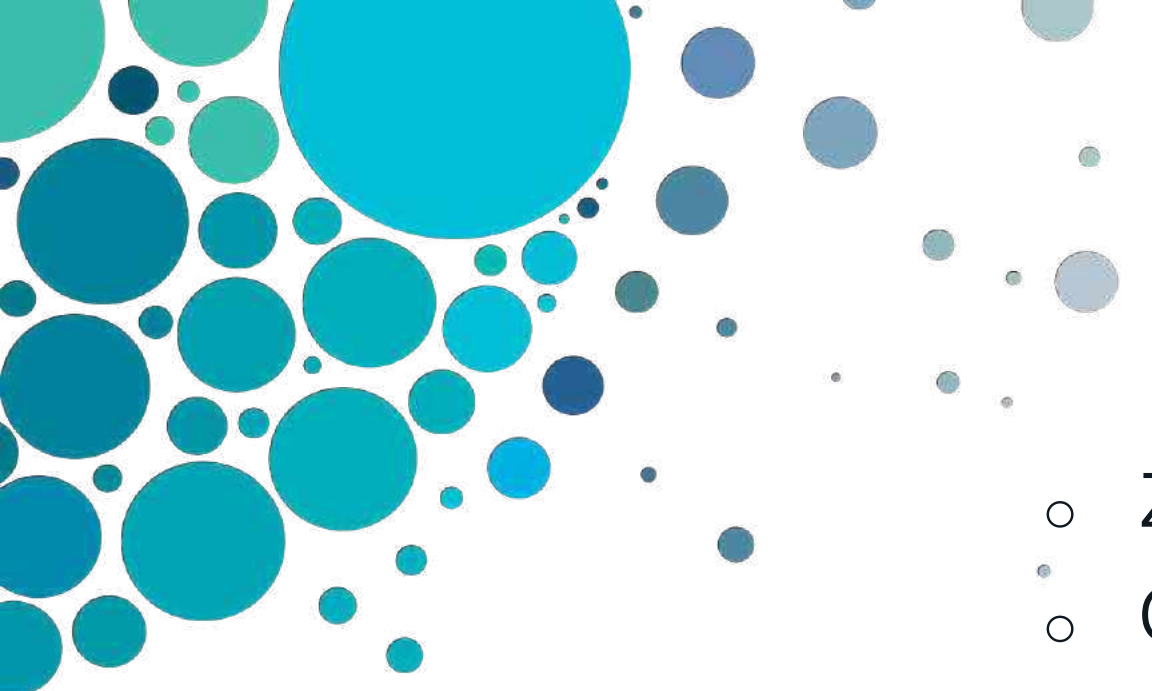


The bridge to possible

사이버 보안의 핵심은 제로 트러스트!

시스코와 함께하는 성공적인 제로 트러스트

이진현 프로 | 시스코코리아 보안 솔루션 아키텍트



Agenda

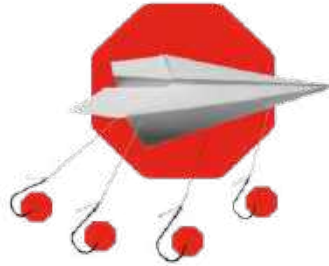
- Zero Trust
- Cisco Secure Access
- Passwordless + Seamless Auth
- Summary

제로 트러스트, 왜 필요할까요?



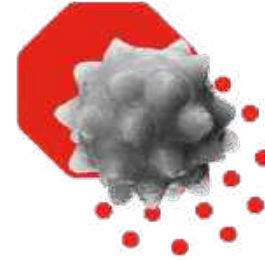
공격 표면의 증가

애플리케이션이 클라우드로 이동함에 따라, 더 쉽게 접근이 가능하여 공격에 노출 됨



>80% 계정 탈취 공격

취약한 비밀번호, 비밀번호의 재사용, **크레덴셜 스테핑**과 같은 계정 탈취 공격 증가



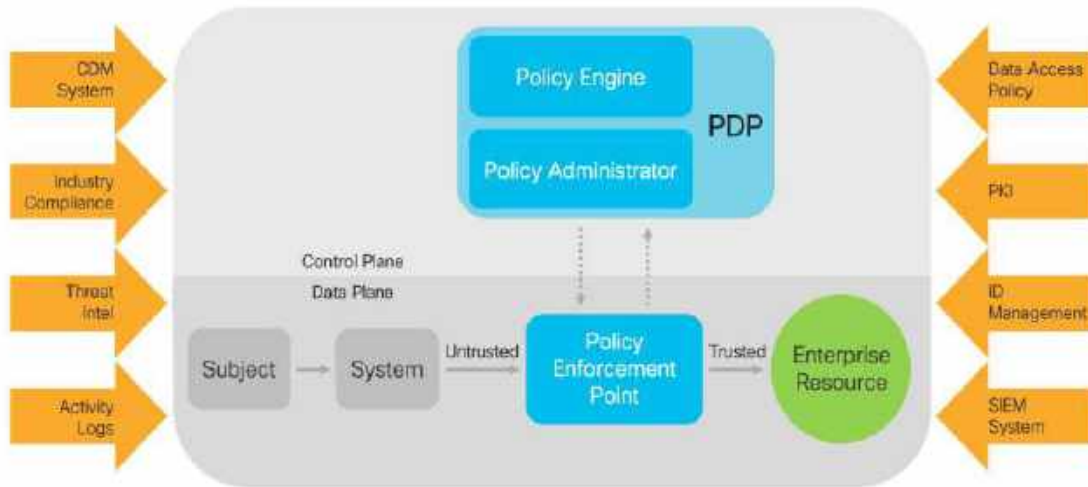
보안 방어 우회 공격

MFA 우회, 디바이스 자산 정보 부족 비정상적인 행위 탐지 및 일관된 정책 부재로 인한 보안 위협

보안에 대한 새로운 접근 방법 - **"Zero Trust"** - 기반의 애플리케이션 보호 필요

Zero Trust Network Access (ZTNA)

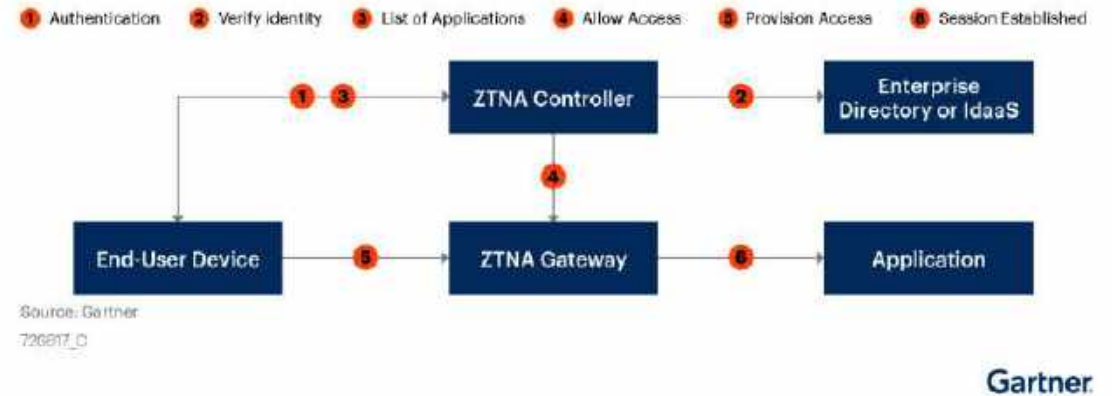
NIST



NIST: 800-207 Zero Trust Architecture

Gartner

Conceptual Model of Endpoint-Initiated ZTNA



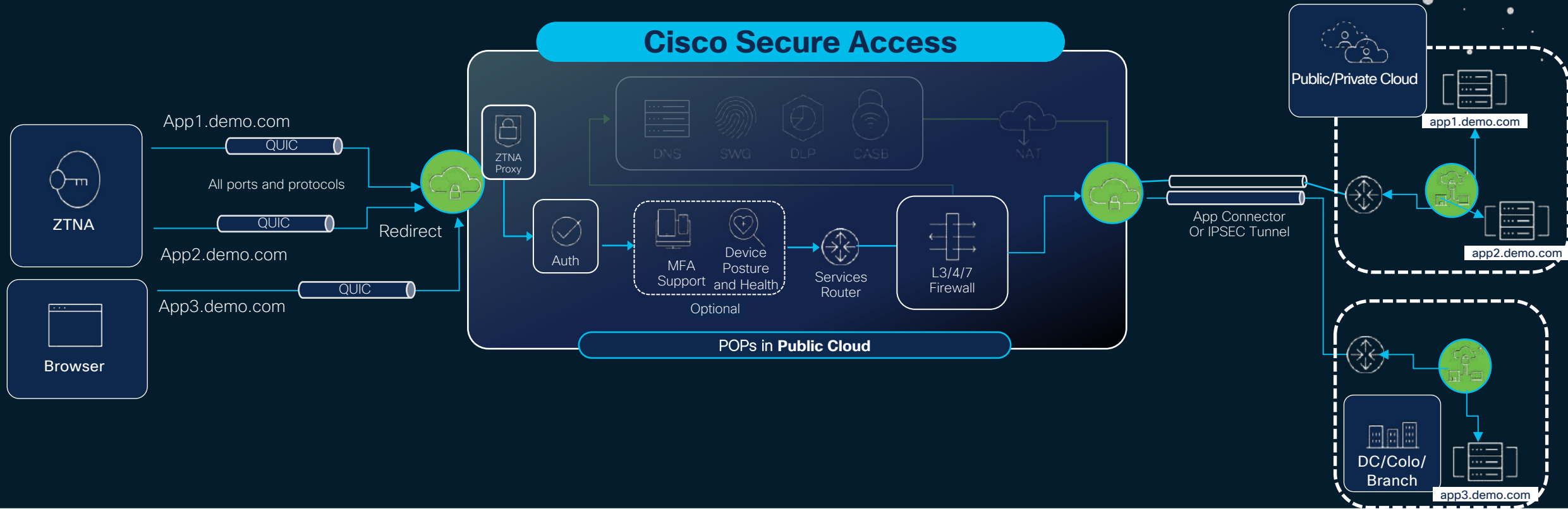
Gartner : Market Guide for Zero Trust Network Access

Never Trust Authentication & Authorization Per-session base grant Continuous verification
Identify & Context Policy & Visibility VPN-Less Software Defined Perimeter

New!! “Cisco Secure Access”



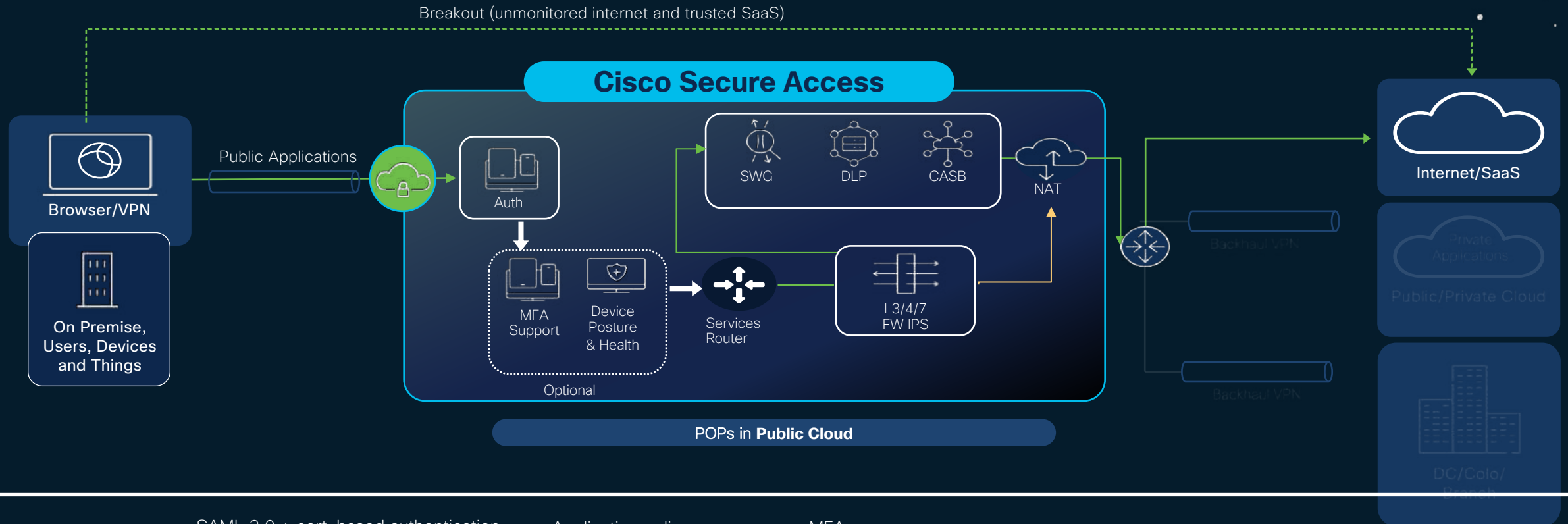
ZTNA Architecture - Private App



Benefits

- 사용자 경험 개선
- 모든 디바이스와 애플리케이션 적용
- QUIC & MASQUE 이용한 성능 제공
- 애플리케이션 단위의 보안
- 단일 플랫폼을 통한 관리와 모니터링
- Routing / Network 변경 없이 적용
- App Bypass 기능 제공

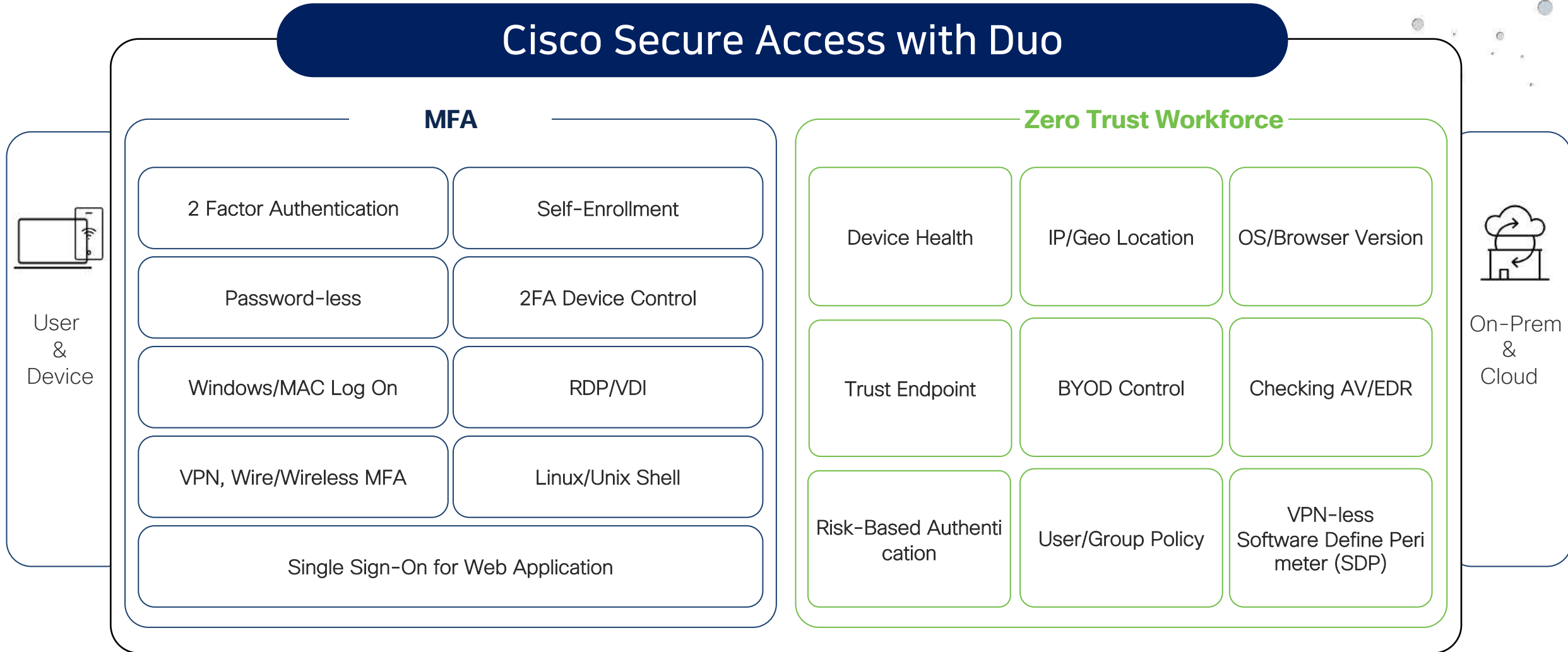
ZTNA Architecture - Internet/SaaS



Capabilities

- SAML 2.0 + cert-based authentication
- Posture verification (optional)
- IPS
- Single in-line inspection
- Application policy
- SWG
- DLP
- CASB
- AV/Malware
- MFA
- SSO
- Device Health

제로 트러스트의 핵심 - Duo

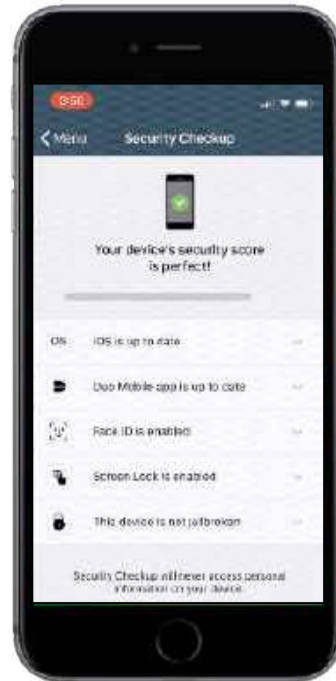


Device and Risk Base Authentication

애플리케이션 접속 시 디바이스의 상태를 확인하여 안전한 디바이스만 접속을 허용



- Corp managed asset status
- Disk encryption
- Firewall enabled
- Device password
- OS patch level (Win 10)
- Third party agents
- OS type & versions
- Browser type & versions
- Flash & Java plugins versions
- OS, browser and plugins status



ACCESS PATTERN

AUTH PATTERN

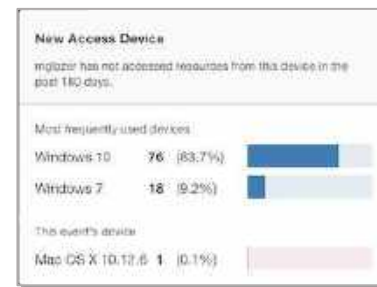
RISK SIGNAL ANALYSIS

DEVICE TRUST

LOCATION

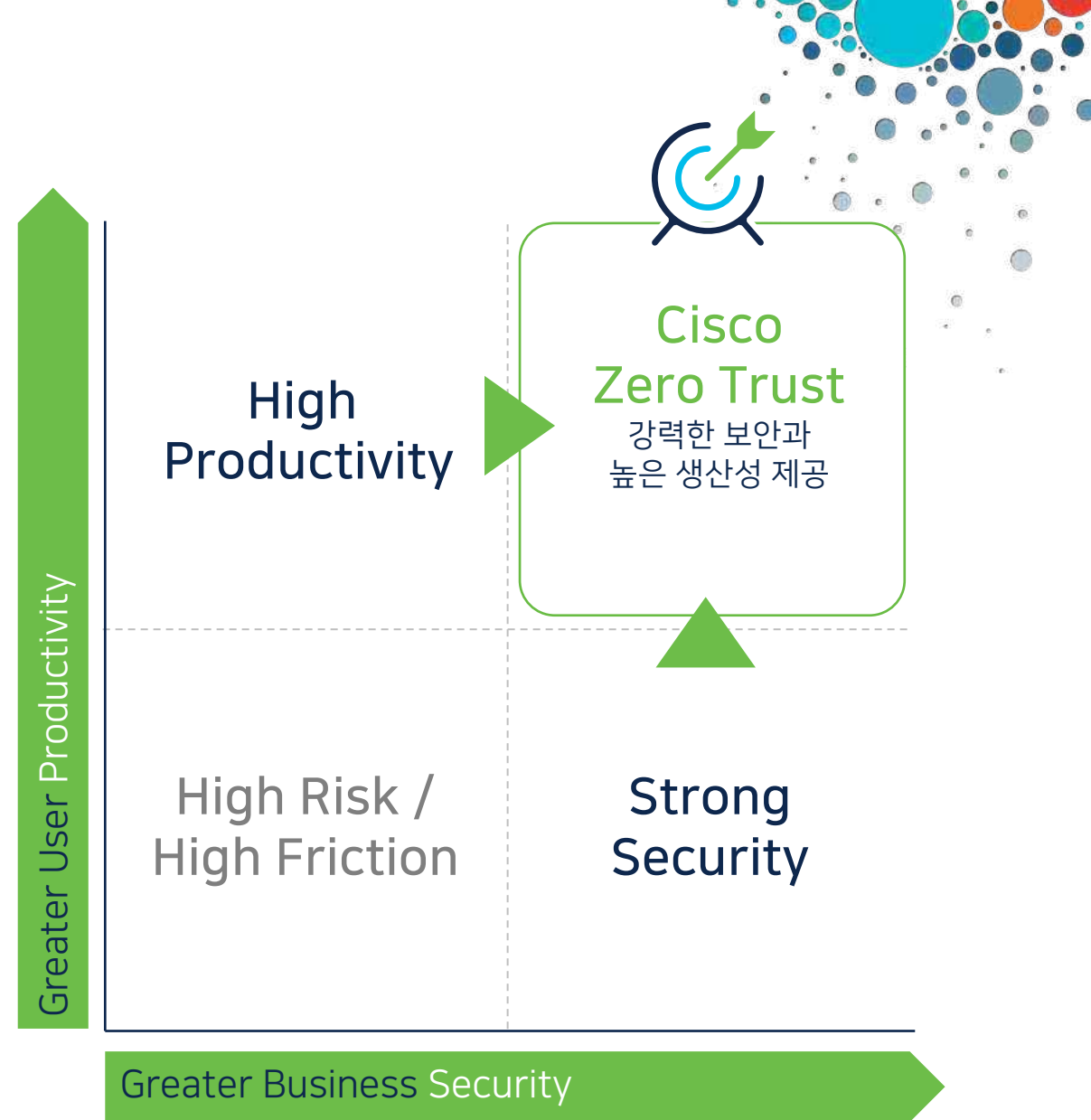
WI-FI FINGERPRINT

KNOWN ATTACK PATTERN

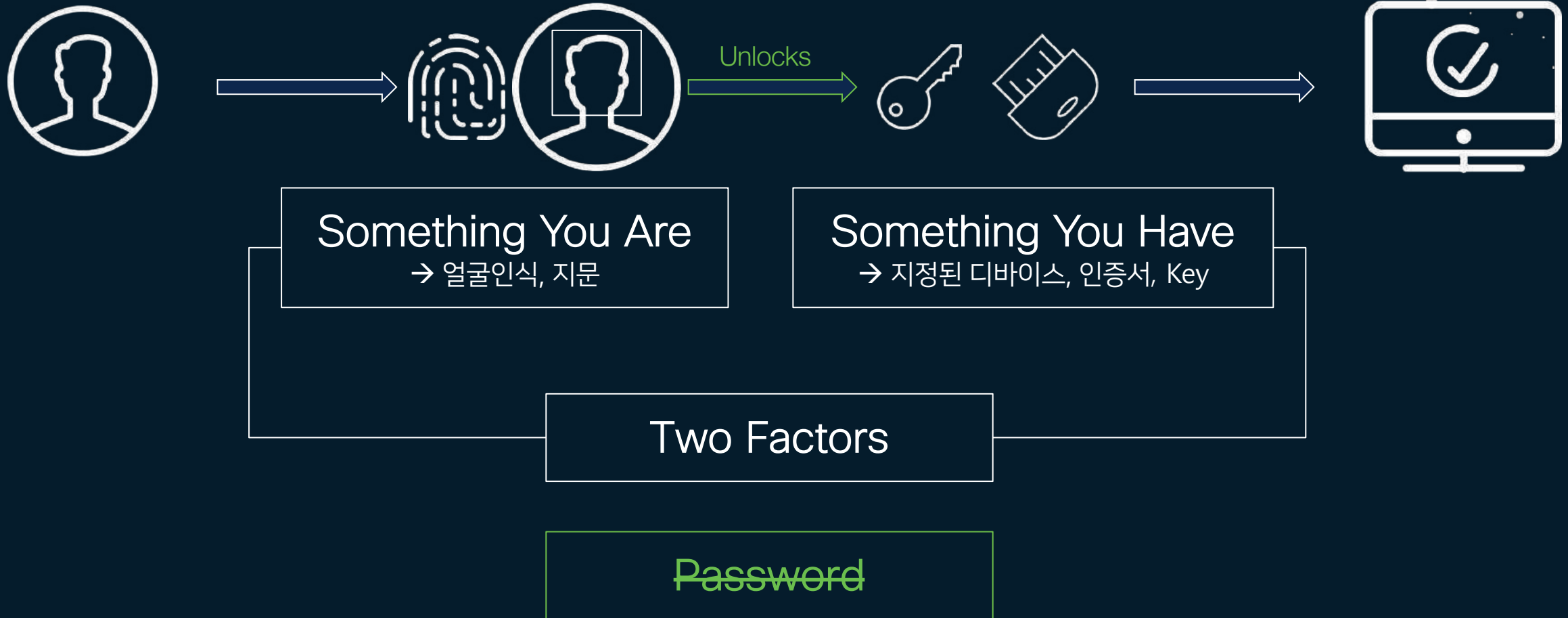


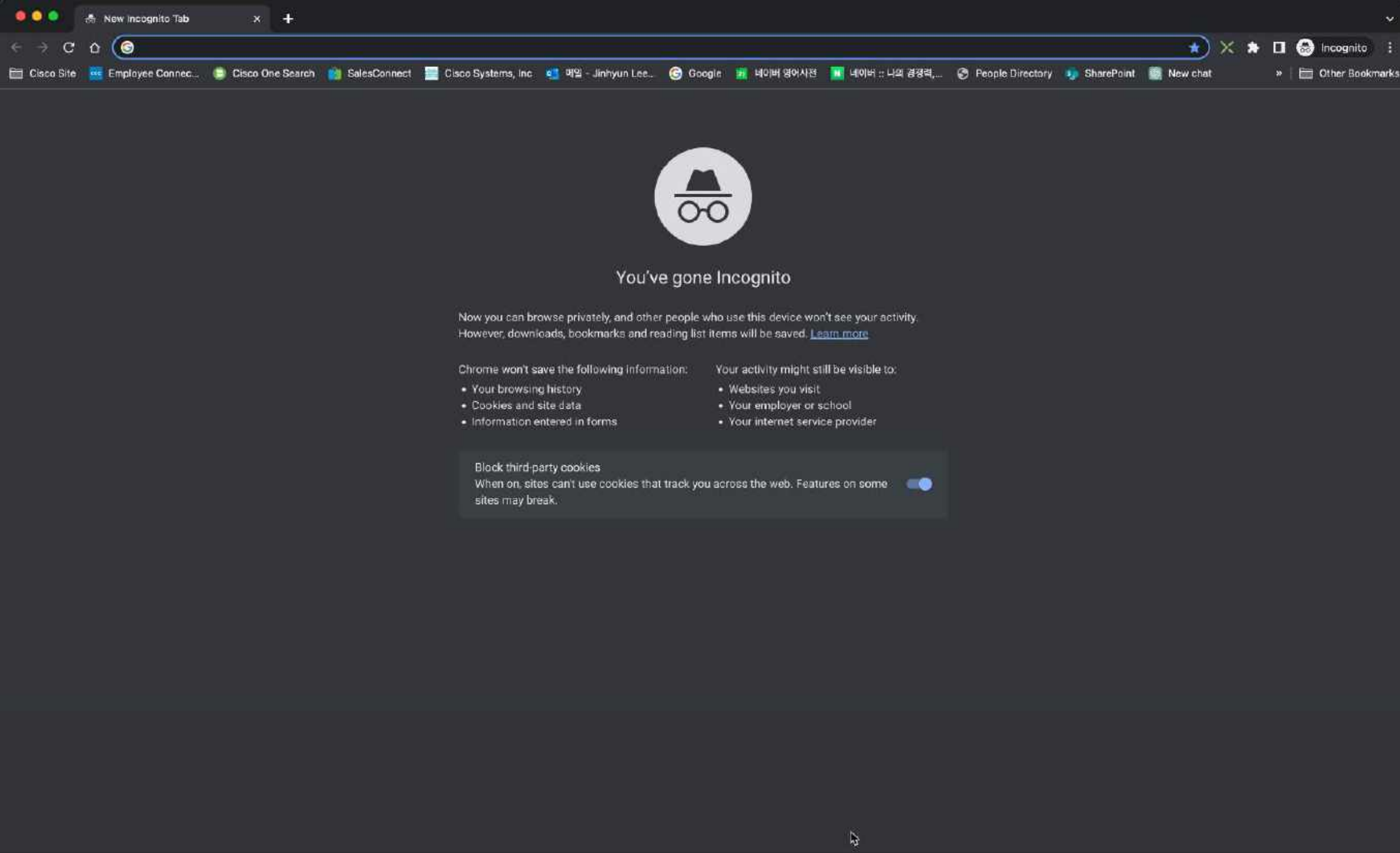
보안 vs 생산성

절대 타협되지 않는 숙제



Goodbye Password - 패스워드리스





You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved. [Learn more](#)

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies

When on, sites can't use cookies that track you across the web. Features on some sites may break. ☒



You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved. [Learn more](#)

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies

When on, sites can't use cookies that track you across the web. Features on some sites may break. ☒

Seamless Authentication

1

애플리케이션 접속에 대한
사용자 인증과 디바이스
로그인



2

디바이스의 보안성 확인



3

애플리케이션 접속 별
보안 정책 적용



단 한번의 인증을 통해 모든 애플리케이션에 대한 Single Sign-On과 보안 정책을 모두 적용



Lee

Sign-in options



Summary

✓ Cisco Secure Access

- 제로 트러스트를 위해 시스코가 새롭게 제공하는 클라우드 기반의 보안 플랫폼

✓ Passwordless + Seamless Authentication

- 오직 시스코만 제공해 드리는, 강력한 보안과 사용자의 편의성까지 모두 제공하는 새로운 제로 트러스트의 패러다임



The bridge to possible

감사합니다.

CISCO *Connect*

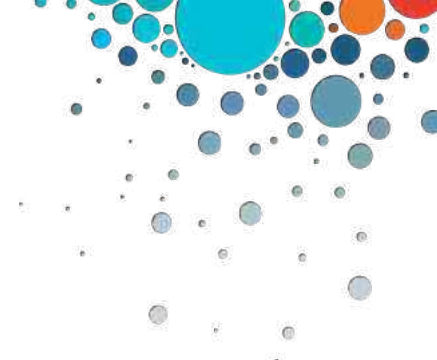
ALL IN

#CiscoConnect

점차 지능화 되는 사이버 위협, 지킬 것인가? 당할 것인가?

김종현 이사 | 시스코코리아

하이브리드, 멀티 벤더, 멀티 벡터 환경



누구나 내부자가
될 수 있습니다

+30%

도난된 크리덴셜
또는 악의적 내부자와
관련된 사고의 비율

어디서든 공격이
시작될 수 있습니다

45%

클라우드에서 발생한
침해 사고의 비율
19%는 비즈니스 파트너사의
보안 침해로 인해 발생

알림으로 인한 피로가
더 심해집니다

37%

알림 증가, 복잡성 증가로
업무 난이도가 높아진다고
응답한 IT 및 보안 운영
전문가 응답

공격 표면이
확장됩니다

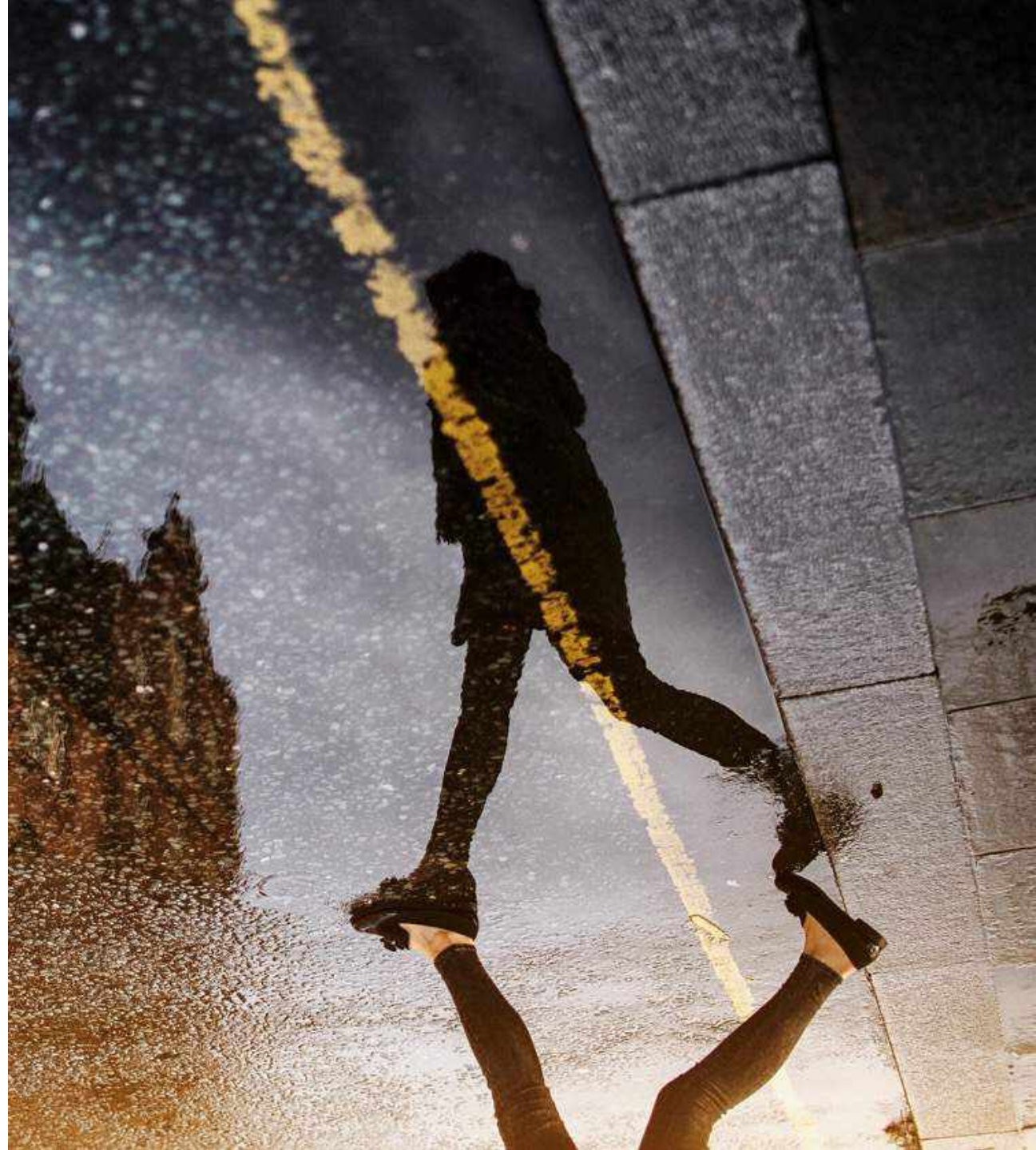
22%

하이브리드 업무로 인한
데이터 유출의 평균 비용
증가율

과거에는 국가 보안에만
영향을 미쳤던 TTP
(Tactics, Techniques
and Procedures)가
이제는 일반 공격자들의
손에 들어갔습니다.



미래의 위협에
대응하기 위해서는
현재의 탐지
및 대응 방식을
바꿔야 합니다.



XDR은 보안 운영 문제를 자신 있게 해결

우리가 위험에 **가장 많이**
노출 되는 곳은 어디입니까?
공격을 **조기에** 탐지하는 데
얼마나 능숙합니까?

1 더 빠른 감지

영향에 따른 우선순위 지정

2

공격의 **전체 범위**와
진입 벡터를 얼마나 빨리
이해할 수 있습니까?

3 조사 시간 단축

대응 가속화

4

모든 자산에 대한 **완전한**
가시성을 확보하고
있습니까? 장치와 장치를
사용하는 사람을 **확실하게**
식별할 수 있습니까?

5 자산 컨텍스트 확장

비즈니스에
가장 큰 영향을 미치는
공격의 우선 순위를 **정**하고
있습니까?

얼마나 빨리 **자신** 있게
대응할 수 있습니까?
SecOps는 얼마나
자동화할 수 있나요?
대응 시간을 **단축**하고
있습니까?

올바른 XDR 활용의 가치

90%

인시던트당 분석가의
노력 감소

높은
퍼포먼스

90%

SecOps 효율성 향상

빠른 응답

85%

공격 체류 시간 단축

더 나은 보안

50%

데이터 유출 위험 및
비용 감소

수익 개선

"그것은 일을 더 쉽고 빠르게 만들 것이며, 우리는 그 어느 때보다 우리 환경에서 훨씬 더 많은 일이 일어나는 것을 보게 될 것입니다."

- 마이클 디그루트(Michael Degroote), 모호크 인더스트리(Mohawk Industries)

XDR의 역할



여러 보안 도구에서
텔레메트리 수집



균질화된 데이터에 분석을
적용하여 악의적 행위 탐지



해당 공격에 대한
대응 및 시정





공격자:
Turla



// 닉네임

Snake

Venomous Bear

Uroburos

Group 88

Waterbug

실제 공격에 대한 분석(Turla)

대부분의 공격은 다음과 같은 순서로 진행됩니다...



T1055: 프로세스 주입(Process Injection)

T1570: 측면 도구 전송(Lateral Tool Transfer)

T1566: 스피어 피싱(Spear phishing)

T1189: 의도하지 않은 보안 침해 (Drive-by Compromise)

T1087: 계정 검색: 도메인 계정(Account Discovery: Domain Account)

T1048: 시스템 네트워크 연결 검색(System Network Connections Discovery)

벤더 A

벤더 C

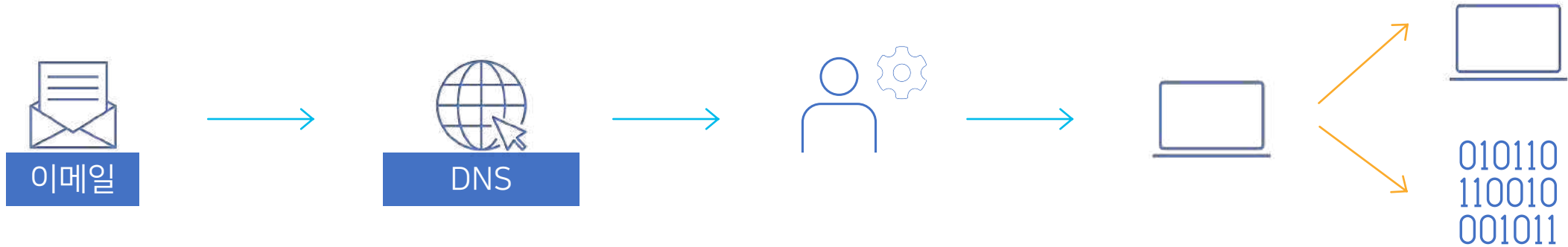
벤더 E

벤더 G

벤더 D

랜섬웨어와 같은 지능형 위협 차단

대부분의 공격은 다음과 같은 순서로 진행됩니다...



전체 공격 체인을 심층적으로 파악하는 솔루션이 필요합니다.

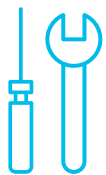


Cisco XDR

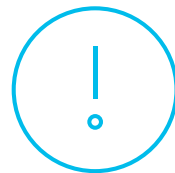


Cisco Security Cloud 플랫폼 상에 구축

XDR 솔루션의 새로운 위협에 대응



보안 도구는
공격자에게 초점



잠재적 오탐을 검증된
인시던트로 전환



초기 침해, 측면 이동,
권한 상승, 데이터
유출에 초점

Cisco의 보안

The most comprehensive integrated cybersecurity platform on the planet gets even better

Started with foundational security solutions

Began acquiring new technologies and innovating at a rapid pace

Unified networking and security

2007

Network Segmentation
Email Security
Web Security Gateway

2009

Cloud Web Security Gateway

2011

Network Access Control

Unified Threat Management

Malware Analysis
Endpoint Detection and Response
NGIPS
DC Networking

2013

Enterprise Firewall
Security Services VPN

Cloud Security
Traffic Analytics
Workload Protection

2015

CASB
Network Security Policy

2017

SD-WAN
SD-Access
Application Performance Management
Cloud Analytics

2019

Access Management
Threat Response

SECURE X

2021

Cloud Email Security Supplements

2023



Cisco XDR

Network telemetry becomes foundations for XDR outcomes

지난 6년간 60억 달러 이상의 M&A



400명 이상의 위협 연구원(Talos)



비교 할 수 없는 플랫폼

SAFE Reference Architecture

TALOS

Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

Duo Secure Access | Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN

Posture

Telemetry

Threat

Query



ThousandEyes (Visibility)

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo



DNS-layer security



SSL decryption



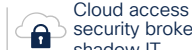
Secure web gateway Remote browser Isolation



L7 firewall + IPS



Data loss prevention



Cloud access security broker/ shadow IT Cloud malware detection

SDWAN



SDWAN



SDWAN by Viptela



Secure Firewall



ThousandEyes



Cloud DDoS

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security



Network Edge



SDWAN



SDWAN by Viptela



Secure Firewall



ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT



Industrial Router



Industrial Firewall



Industrial Switch/AP



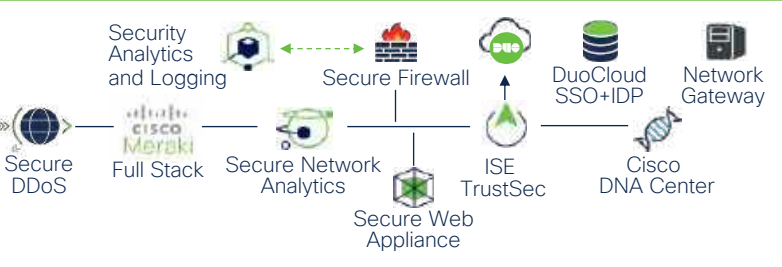
Cyber Vision



ISE TrustSec

ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility



Application Security

ZERO TRUST WORKLOAD

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack



App Visibility | Detection | Response



시스코의 XDR 전략



최첨단 위협 탐지

다중 벡터 탐지:
네트워크, 클라우드, 엔드포인트,
이메일 등 애셋 인사이트, 위협
인텔리전스로 인시던트 강화
멀티 벤더 환경에 최적화



실질적으로 중요한 조치를 더 빠르게 실행

중대성을 기준으로 위협의 우선
순위 지정
조사를 간소화하는 통합
컨텍스트
근거에 기반한 권장 사항



생산성 향상

중요한 문제에 집중하고
노이즈를 필터링
제한된 리소스를 최대한
활용하여 가치 극대화
작업 자동화 및 전략 작업에 집중



복원력 구축

보안 격차 해소
실용적인 인텔리전스를 통해
다음에 일어날 일을 예측
지속적이고 정량화 가능한
개선으로 나날이 강화

Cisco XDR을 통한 간소화



Cisco Security 플랫폼 상에 구축

개방형 확장
가능 플랫폼

명확한
우선순위 지정

자동화 및
대응 지침

간소화된 조사

보안 운영
분석가

CISO

인시던트
대응자

귀사 SOC

효과적인 XDR의 특징

네이티브 및 타사
제어점으로부터의 텔레메트리



엔드포인트



네트워크



이메일



클라우드



ID



방화벽



Cisco XDR
개방형 및 위험 기반



분석 및 상관관계



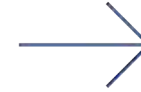
간소화된
조사



자동화
및 대응



간소화된 조사를 통해
탐지부터 대응까지 걸리는
시간 단축



알림의 우선순위를 지정하여
가장 큰 피해를 입히는 위협에
SOC 노력을 집중 투입



자동화된 대응 조치를 통한
신속한 위협 완화 및 사전
예방적 조치

위협 정보

애셋 및
사용자 컨텍스트

MITRE

보안 운영을 간소화하여 생산성을 높이고 최첨단 위협에 대한 복원력을 유지

XDR 구성 요소 및 결과



XDR 활용 사례

즉시 주의를 기울일 수 있도록
가장 중요한 보안 이벤트에 집중



우선 순위가 지정된 사고 대응

침입 발생과 공격자 발견 사이의
시간 단축



온디맨드 위협 헌팅

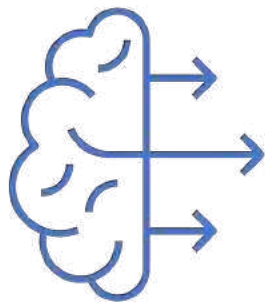
XDR 활용 사례

다양한 인텔리전스로 향상된 탐지 기능

59.93.19.92 	Malicious	IP Addr...	2023-03-31T09:10:13.6... 2023-04-30T09:10:13.6...	TALOS IP B...	High
59.97.169.111 	Malicious	IP Addr...	2023-03-31T09:10:13.6... 2023-04-30T09:10:13.6...	TALOS IP B...	High
b0c57.binan... 	Malicious	Domain	2023-03-31T08:46:51.4... 2023-04-07T08:46:51....	ZeroDot1 C...	Medium



다른 사람...



- 공개 및 비공개 인텔리전스 소스를 사용하여 더 나은 위협 식별 달성
- 환경 및 요구 사항에 따라 고유한 피드를 만들고 사용자 지정

판단

지표

피드

이벤트

XDR 활용 사례

상관 관계 알람을 통해 공격을 더 빨리 확인

• 2023-03-13T16:...	High	Suspicious SMB and RDF
• 2023-03-13T16:...	High	Suspicious Endpoint Acti
• 2023-03-13T16:...	High	Malicious Process Detec

Priority **1000** Status **New**

Malicious Process and Suspicious SMB/RDP...

Reported by **Cisco Secure Cloud Analytics**
14 hours ago

Assigned **BM** **JF**

MITRE **.....**

Alert types

- Malicious Process Detected
- Suspicious SMB and RDP activity

Alerts

1. Malicious Process Detected - #6
2. Suspicious SMB and RDP activity - #35

Sources

- virtualmachines/win-vic-2
- virtualmachines/kali

Chaining Patterns - Tactics

Execution (TA0002) → **Lateral Movement** (TA0008)

Chaining Patterns - Techniques

Masquerading (T1036) → **Remote Services** (T1021)

시간에 따른 경고 상관 관계

시간이 지남에 따라 상관 관계가 있는 경고에서 새로운 인시던트를 자동으로 생성하고 다단계 공격의 더 큰 그림을 보여줍니다.

공격 체인 매핑

MITRE 전술 및 기법을 사용하여 공격 체인 연결 및 공개

XDR 활용 사례

인시던트를 단계별로 추적

점진적 공개

인시던트를 조사하는 것은 SOC 분석가를 압도하지 않고 필요에 따라 관련 데이터를 공개하는 점진적인 경험입니다

Priority	Name
1000	Malicious Process and Suspicious SMB/RDP Activity Detect
1000	Unusual External Server for This is localhost

풍부한 인시던트 세부 정보

인시던트는 자산, 지표, 관찰 가능 개체 등을 포함한 여러 소스에서 수집된 데이터로 보강됩니다. 위험 점수와 함께 자세히 설명된 관련 MITRE ATT&CK 전술 및 기술

Priority **1000** Status **New**

Malicious Process and Suspicious SMB/RDP...

Reported by **Cisco Secure Cloud Analytics (rsa)**
15 hours ago

Assigned **BM** **JF**

MITRE **.....**

Priority score breakdown

1000

100
Detection Risk

10
Asset Value at Risk

Short description

This feature is currently under active development

Long description

Alert Chain
fb56eea65af173cd7288d510722e4f8f7e5c8613

Description

View Incident Detail

MITRE | ATT&CK

View all Tactics

Tactics

TA0002: Execution 100

The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

TA0008: Lateral Movement 66

Orientation

```
graph LR; NT_AUTHORITY_NETWORK[NT AUTHORITY\NETWORK] --- C_WINDOWS_SYSTEM[C:\Windows\System32\svchost.exe]; SYSTEM[SYSTEM] --- C_WINDOWS_SYSTEM; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_WIN_VLC_2[virtualmachines/win-vc-2]; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_WIN_DC_0[virtualmachines/win-dc-0]; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_WIN_VLC_6[virtualmachines/win-vc-6]; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_KALI[virtualmachines/kali]; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_WIN_VLC_2; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_WIN_DC_0; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_WIN_VLC_6; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_KALI; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_WIN_VLC_2; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_WIN_DC_0; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_WIN_VLC_6; C_WINDOWS_SYSTEM --- VIRTUALMACHINE_KALI;
```

4 Assets

View Assets

virtualmachines/win-vc-2

6 events

virtualmachines/win-dc-0

5 events

virtualmachines/win-vc-6

4 events

virtualmachines/kali

1 event

31 Observables

View Assets

NT AUTHORITY\SYSTEM

C:\Windows\System32\svchost.exe

svchost.exe

SYSTEM

XDR 활용 사례

영향력에 따른 우선순위 지정

XDR 탐지결과

- 여러 소스의 인시던트에 대한 단일 보기
- 가장 중요한 인시던트에 초점을 맞춘 향상된 인시던트 보기
- 비즈니스 영향 및 자산 가치에 따라 우선 순위가 지정된 인시던트

742

92
Detection
Risk

8
Asset
Value at Risk

Incidents

62 Incidents

33 New Incidents

8 Open Incidents

Search

62 matching results

Filters

☐	Priority	Name	Source
☐	1000	Malicious Process and Suspicious SMB/RDP Activity - Doc Test Do ...	Cisco Secure Clou...
☐	1000	Unusual External Server for This is localhost	Cisco Stealthwatc...
☐	1000	AWS Inspector Finding for This is localhost	Cisco Stealthwatc...
☐	1000	Command and Control DNS Activities	Umbrella
☐	928	Formula Test.Mar27.Critical.TTP(58).AssetValue[8]	FormulaTest
☐	928	F1.03-06d.Critical.TTP(58).AssetValue[10]	FormulaTest
☐	835	Attack Graph Test - 109 Observables	FormulaTest
☐	800	F1.03-06a.Critical.TTP(50).AssetValue[NULL]	FormulaTest
☐	765	New Internal Device for This is localhost	Cisco Stealthwatc...
☐	765	Azure Permissive Security Group for TD&R RSA	Cisco Secure Clou...
☐	742	F1.03-08.Critical.TTP(58).AssetValue[8]	FormulaTest

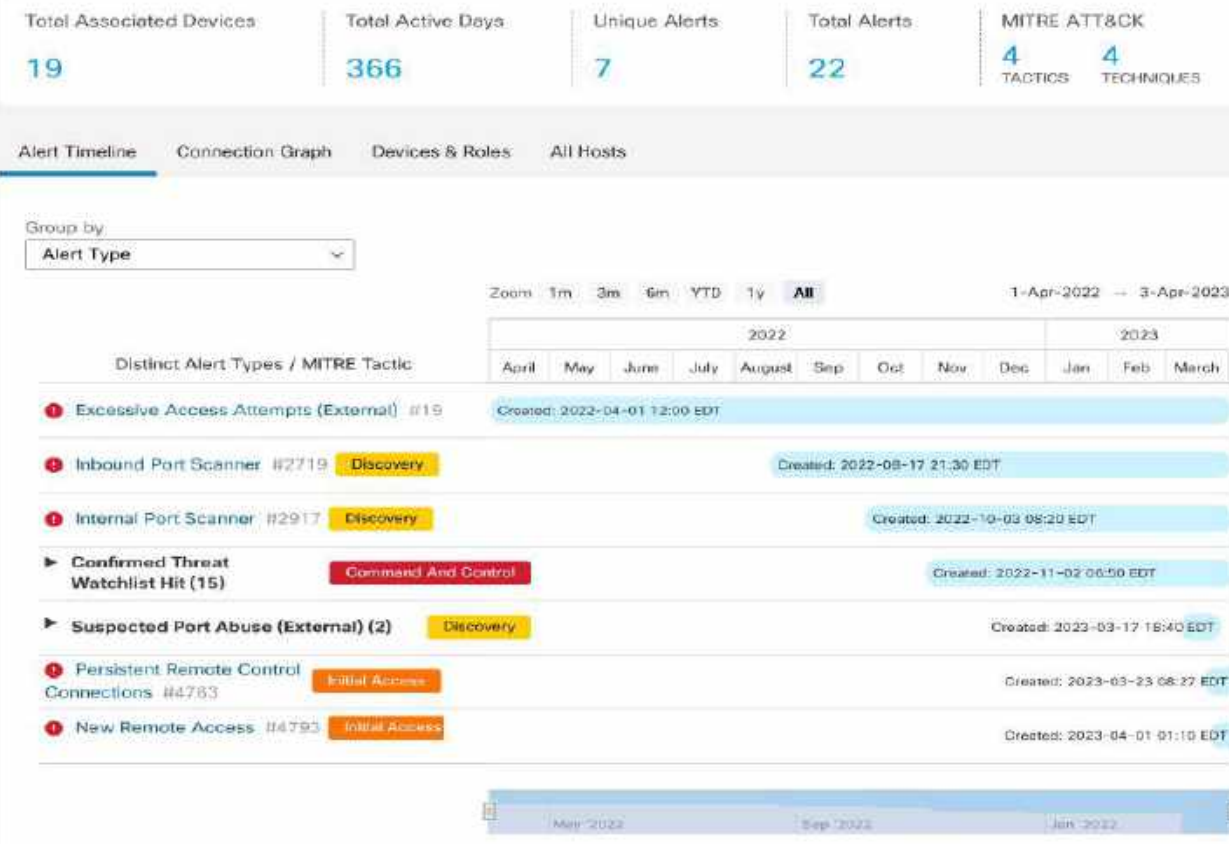
XDR 활용 사례

조사 시간 단축

XDR 탐지결과

- 인시던트의 대화형, 시각적 표현
- 그룹 관련 인텔리전스에 대한 이벤트 상관 관계 및 공격 체이닝
- 가장 중요한 인시던트에 대한 자동화된 보강을 통해 인텔리전스를 즉시 수집할 수 있습니다.

Alert Chain at a Glance

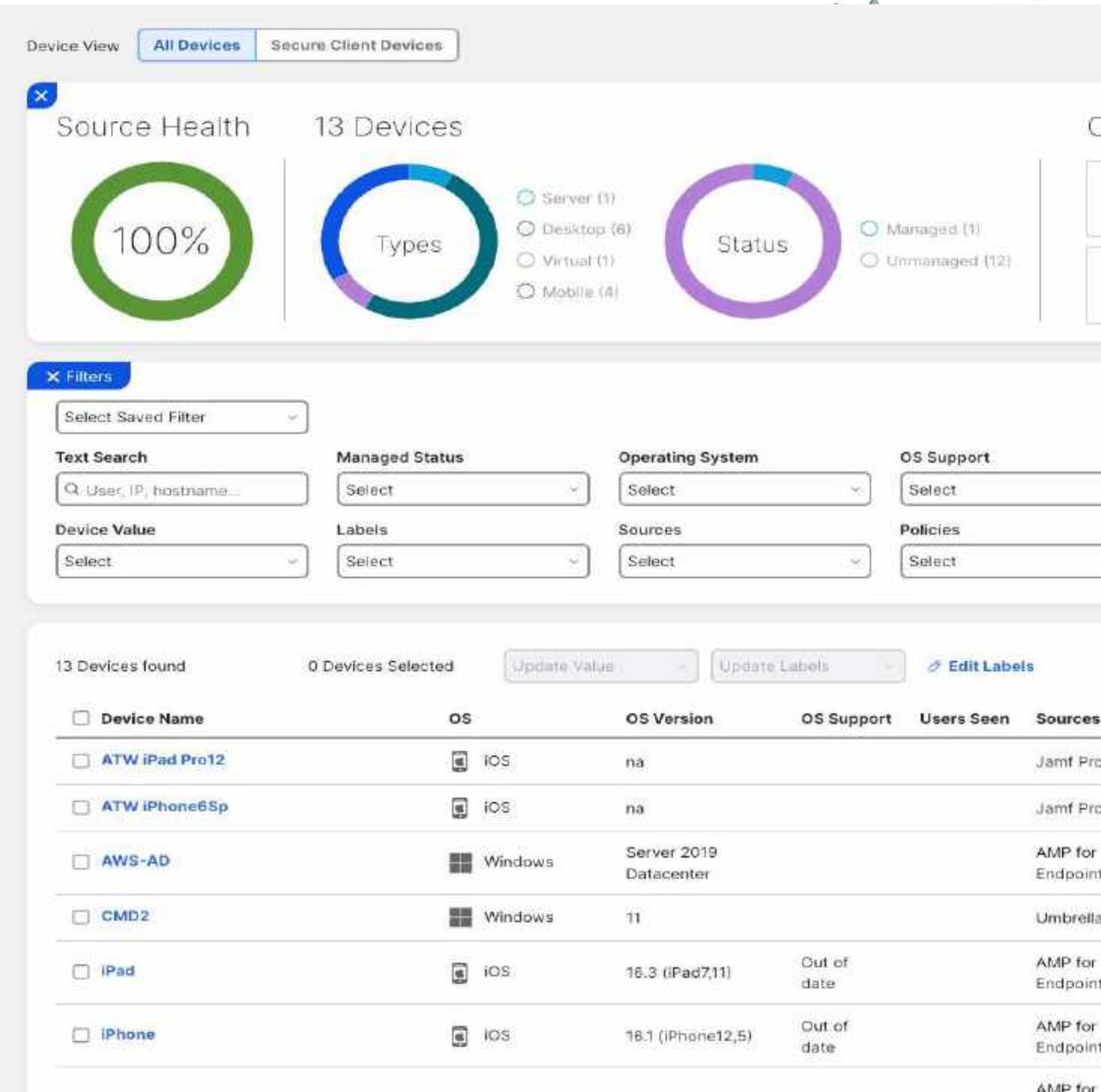


XDR 활용 사례

자산 컨텍스트 확장

XDR 탐지결과

- 여러 소스에서 집계된 자세한 자산 정보
- 자산 인벤토리와 보안 컨텍스트 결합
- 자산 가치에 따라 보다 정확한 사고 우선순위 지정 가능
- 대상과 자산 구분



사용자가 어디에 있든 요구 사항을 충족하는 XDR



XDR은 팀이 보안 대응을 위해 신속한 포지셔닝

통합

통합 플랫폼으로
솔루션 및 기술 통합



오케스트레이션

AI 및 ML을 통한 우선 순위가
지정된 탐지 및 대응 지원



최적화

베이스라인 기반의
선제적 실행을 통한
보안의 발전 및 미세 조정



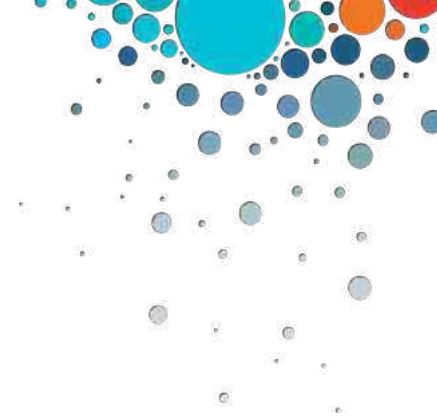
에코시스템 구축

환경의 모든 부분에서 데이터를
집계하고 보강하며 원격 분석하는
에코시스템 구축

자동화

사람의 개입을
최소화하는
탐지 및 대응 워크플로
자동화

Summary



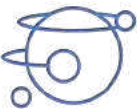
멀티 벤더, 멀티 벡터 환경에 최적화된 개방적이고 유연한 접근 방식



위협 상관관계 및 명확한 우선순위 지정으로 사용자가 가장 중요한 문제를 파악할 수 있도록 지원



가이드 기반의 신속한 대응으로 위협을 신속하게 해결하고 분석 효율을 향상



필수 네트워크 인사이트를 통해 사용자 환경에 대한 이해도 향상



The bridge to possible

감사합니다.

CISCO *Connect*

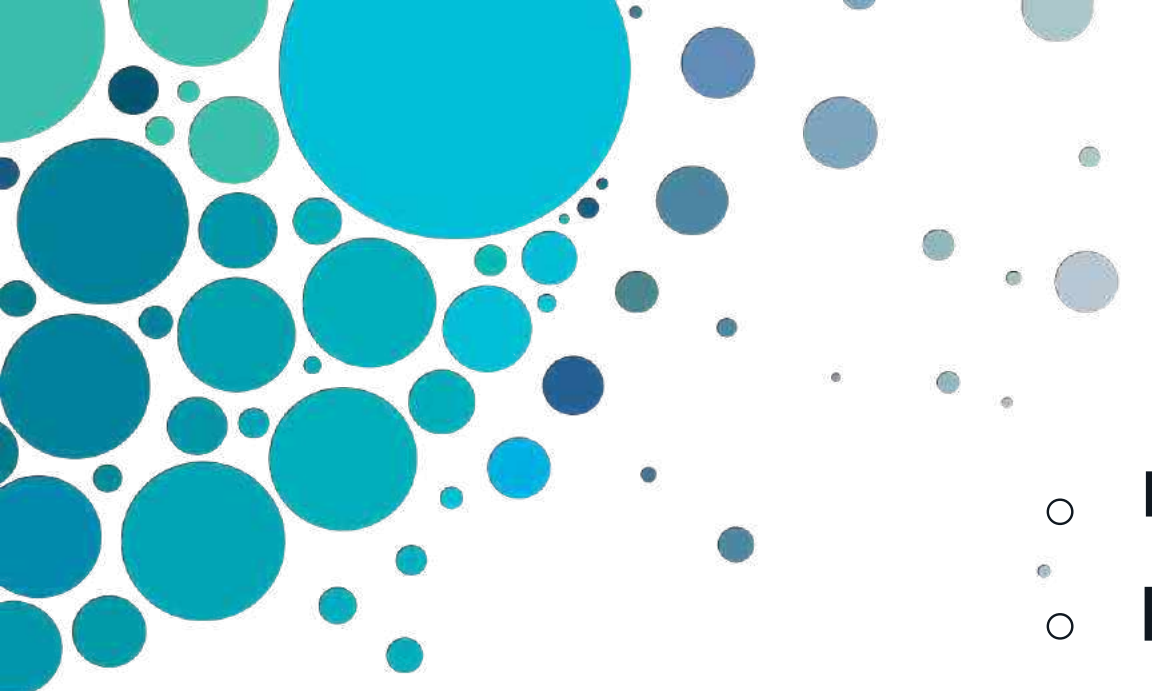
#CiscoConnect



The bridge to possible

비즈니스에서 승리하기 위한 애플리케이션 관점의 보안 및 관리 비결

박한진 이사 | 시스코코리아



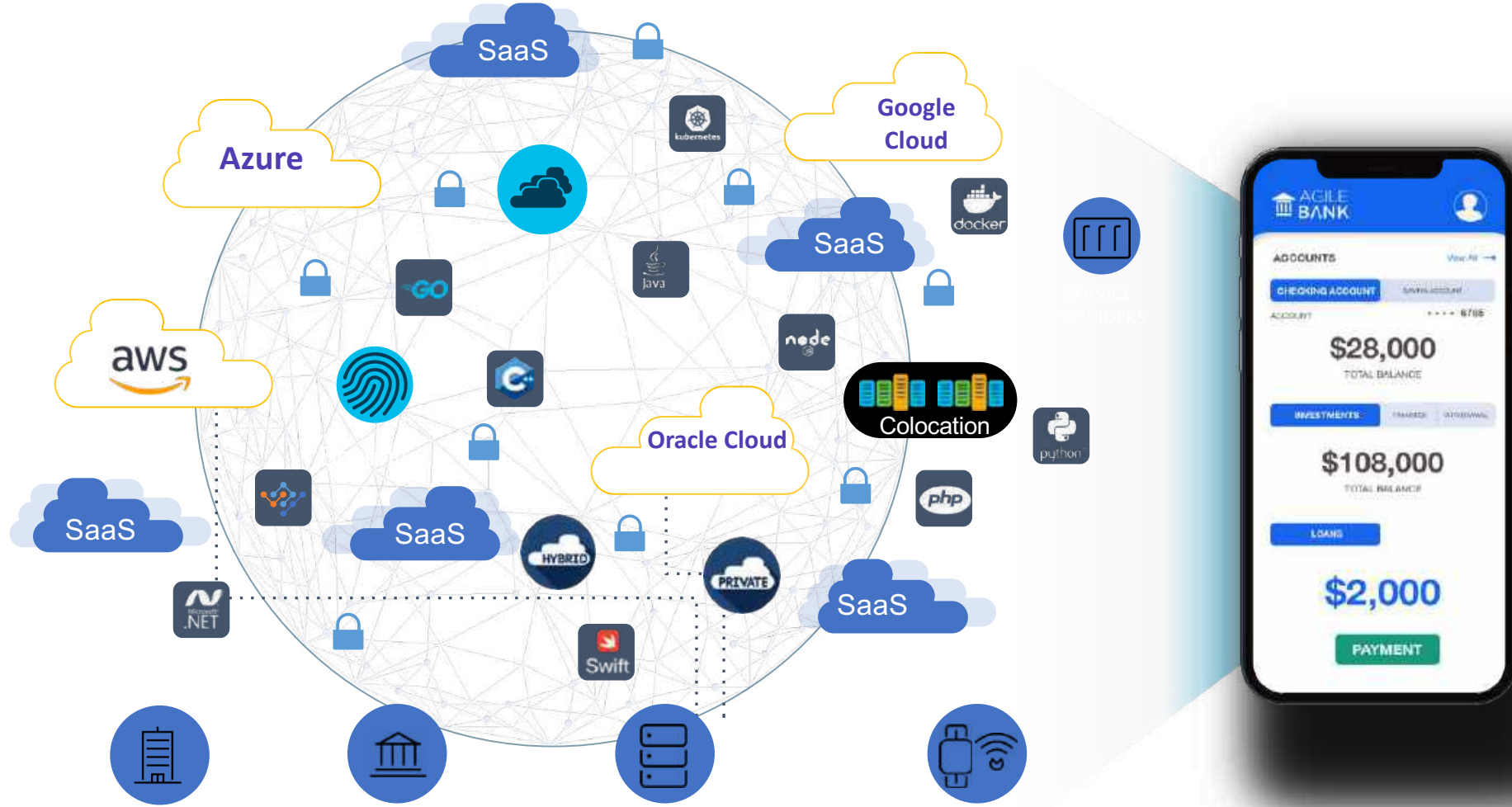
Agenda

- 비즈니스와 컨테이너
- Kubernetes 가시성
- Kubernetes 보안
- Summary

비즈니스와 컨테이너



더 편리하고, 더 빠르고, 더 안전한 것을 원합니다.



CNCF 2022 설문 조사 결과

Does your organization use Kubernetes?

49% 이상이 K8S 사용 중



END USERS

64%

Using in production

25%

Piloting / evaluating



NON-END USERS

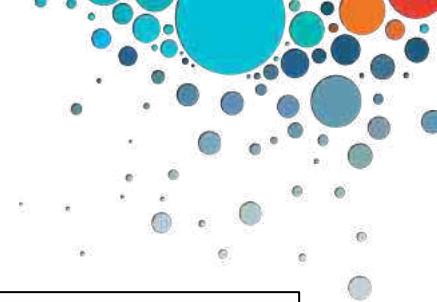
49%

Using in production

20%

Piloting / evaluating

CNCF 2022 설문 조사 결과



How are containers used within your organization?

79%가 운영에서 사용

Used for **most or all** production applications and business segments throughout the organization

44%

Used for **a few** production applications and business segments in the organization

35%

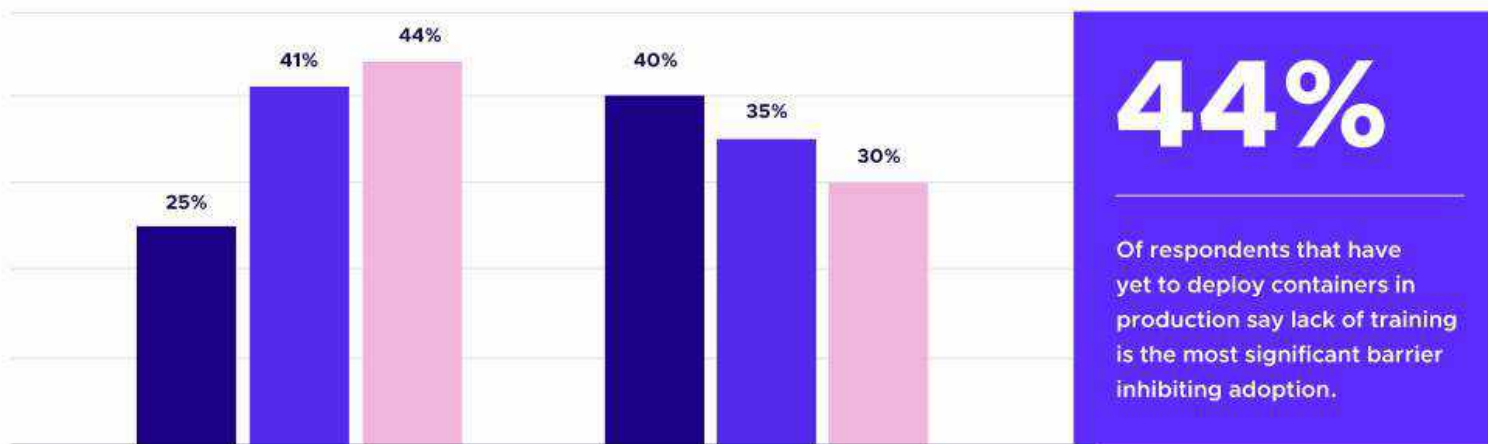
Piloting or actively evaluating

9%

CNCF 2022 설문 조사 결과

What are your challenges in using / deploying containers?

The biggest challenges responders reported, in using and deploying containers, are a lack of training and security. In fact, lack of training is the most significant barrier inhibiting adoption. It is the top challenge cited by 44% that have yet to deploy containers in production, and 41% of those that use containers on a limited basis. Once containers are used for nearly all applications, then security becomes the top challenge.



LACK OF TRAINING

Complexity

SECURITY

가시성

Containers used for **most or all** production applications and business segments throughout the organization

Used for **a few** production applications and business segments throughout the organization

Containers are being **piloted or actively evaluated**

보안

Kubernetes 가시성



Kubernetes를 운영하기 위한 기본 요소

다양한 보안 요소들

영구 저장소

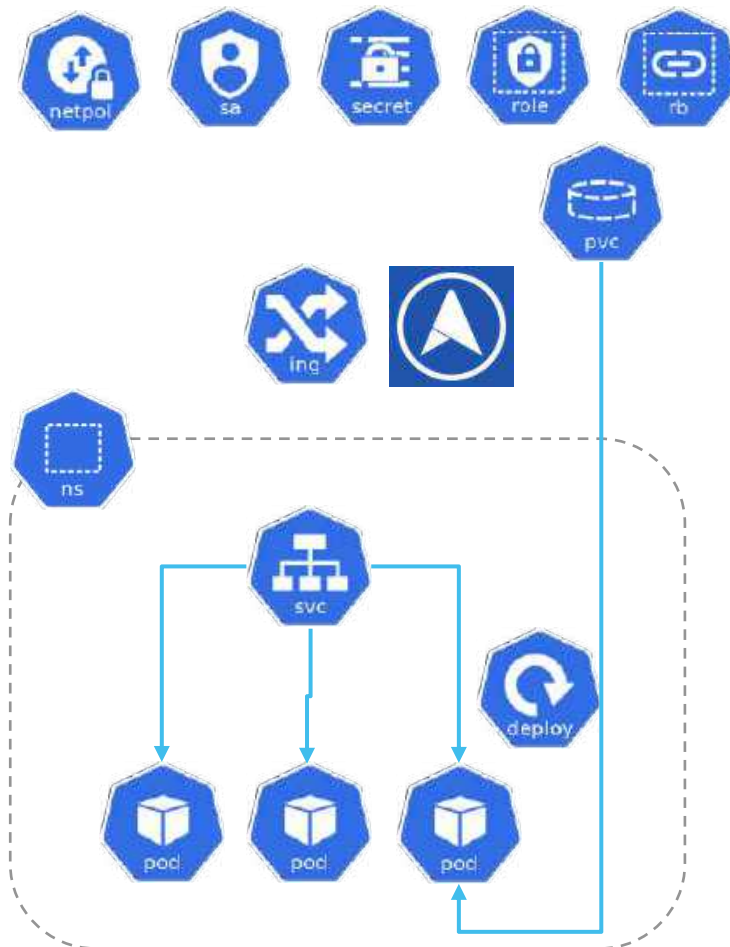
외부서비스 연결 필요

리소스 격리를 위한 논리 그룹

라우팅을 위한 서비스

가용성을 위한 복제구성

서비스를 위한 POD



NetworkPolicies , ServiceAccount,
configmap,Secret , Role , Rolebinding

Persistent Volumes,
Persistent Volume Claims

Ingress , External LB

Namespace

ClusterIP , NodePort,
LoadBalancer, ExternalName

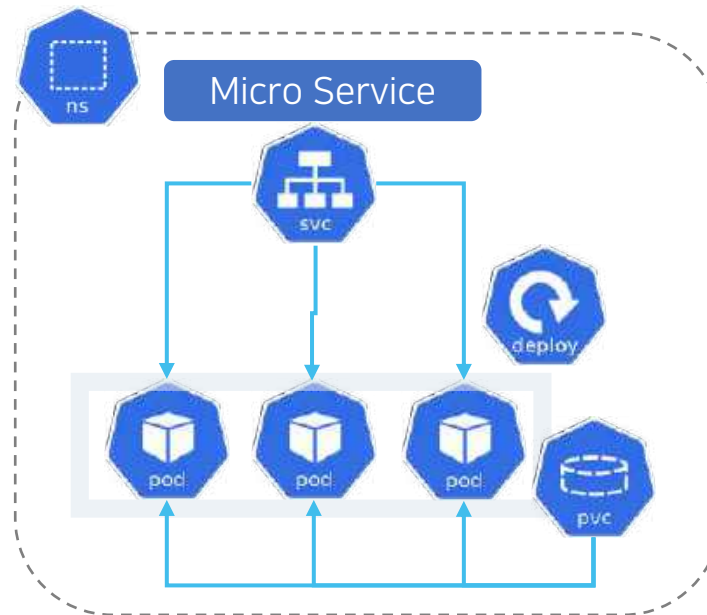
ReplicaSet, Deployments,
StatefulSets, DaemonSets

Pods (Single or Multi Containers)

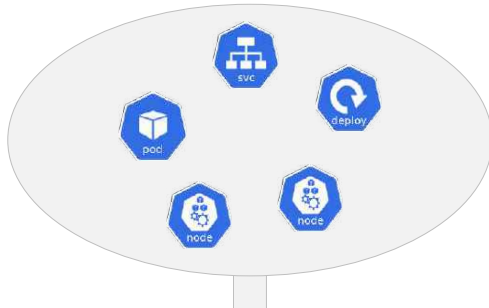
Kubernetes는 어렵다?

```
#kubectl get namespaces
~~
#kubectl get service -n ns
~~
#kubectl describe service -n ns svc01
~~
~~
~~
~~
#kubectl edit service -n ns svc01

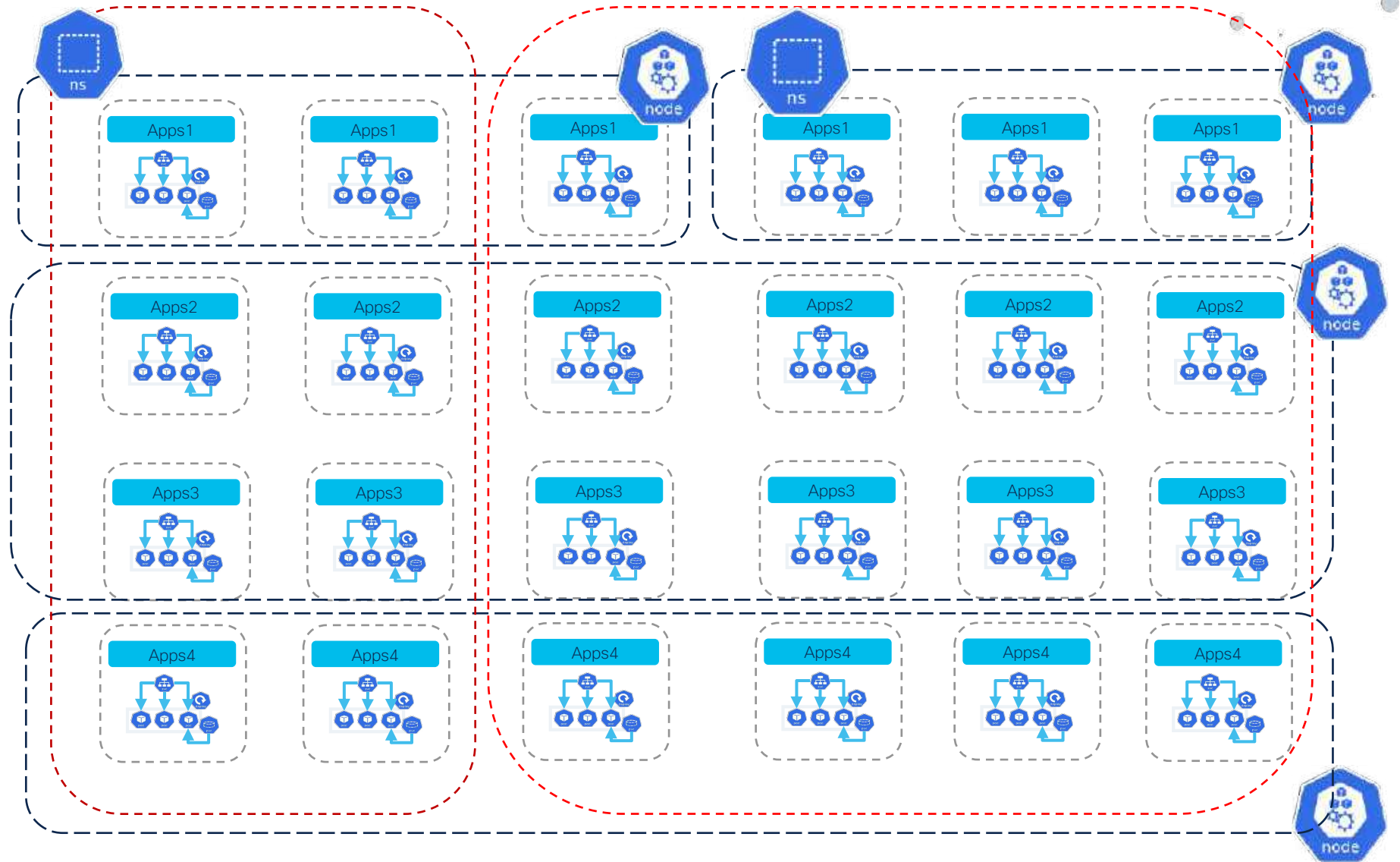
#kubectl get deployments -n ns
~~
#kubectl describe deployments -n ns
~~
~~
~~
#kubectl get pods -o wide -n ns
~~
#kubectl describe pvc -n ns pod-pvc
~~
~~
~~
#kubectl get pvc -n ns pod-pvc -o yaml
> 123.yaml
```



Kubernetes는 복잡하다?

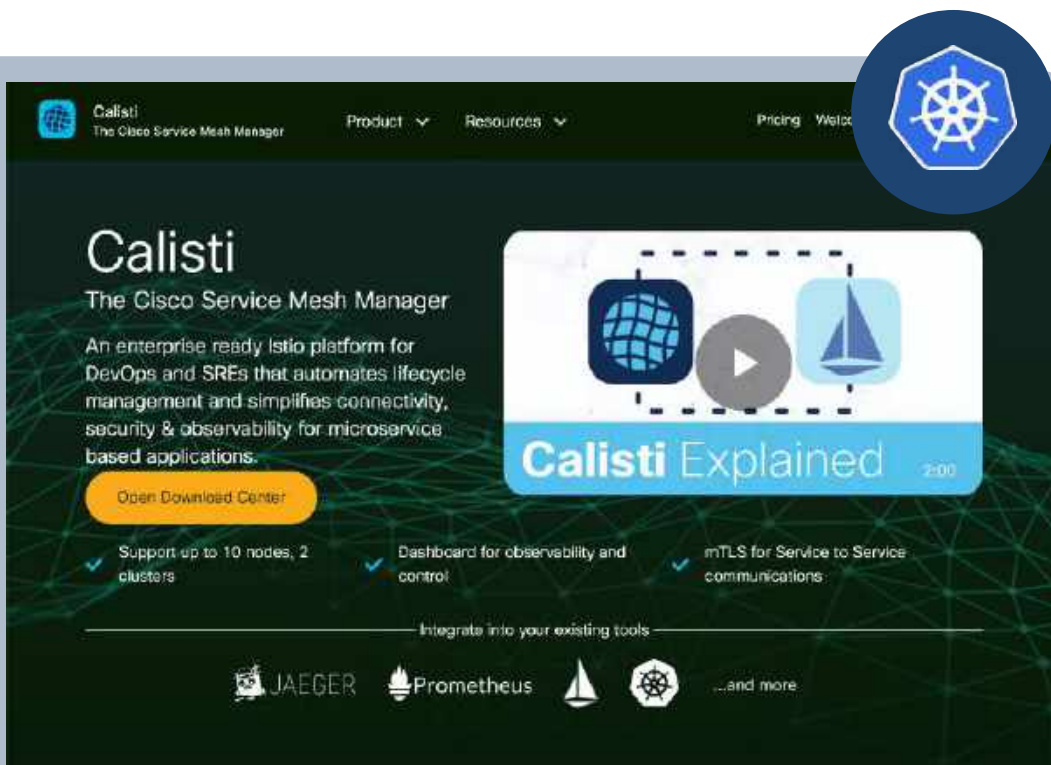


```
#Kubecttl get service  
~~  
#Kebestl get deployments.app  
~~  
#Kubecttl get namespaces  
~~  
#Kubecttl get pods  
~~
```



Calisti - Cisco Service Mesh Manager

Service Mesh - 컨테이너 환경에서의 가시성 확보 및 다양한 관리 효율성 제공



Operationalize the service mesh

POD 간 상세한 서비스 가시성 제공

컨테이너 환경의 트래픽 관리

서비스 간의 mTLS 통신 제공

2개 클러스터 10개 nodes까지 무료 !

Kubernetes의 가시성 제공

The screenshot displays the Cisco Connect SMM-DEMO interface. On the left, the 'analytics-v1' deployment is selected, showing its namespace (smm-demo), cluster (kubernetes), kind (Deployment), app (analytics), version (v1), and replicas (1). Below this, the 'Pods' section shows a single pod named 'analytics-v1-6556d95866-m4ggl' with 2 containers. The 'Events' and 'Metrics' sections are also visible. On the right, the 'DEPLOYMENT' details for 'analytics-v1' are shown, including the 'spec' section which is highlighted with a yellow box. The 'spec' section contains the following YAML configuration:

```
172 type: RollingUpdate
173 template:
174   metadata:
175     annotations:
176       app.kubernetes.io/version: 0.1.4
177       istio.io/rev: cp-v115x.istio-system
178     creationTimestamp: null
179     labels:
180       app: analytics
181       version: v1
182   spec:
183     containers:
184       - env:
185         - name: WORKLOAD
186           value: PI
187         - name: PI_COUNT
188           value: '1000'
189         image: ghcr.io/banzaicloud/allspark:0.1.7
190         imagePullPolicy: Always
191         name: analytics
192         ports:
193           - containerPort: 8080
194             protocol: TCP
195           - containerPort: 8082
196             protocol: TCP
197           - containerPort: 8083
198             protocol: TCP
199         resources:
```

전체적인 서비스 흐름 파악

실시간 통신 확인

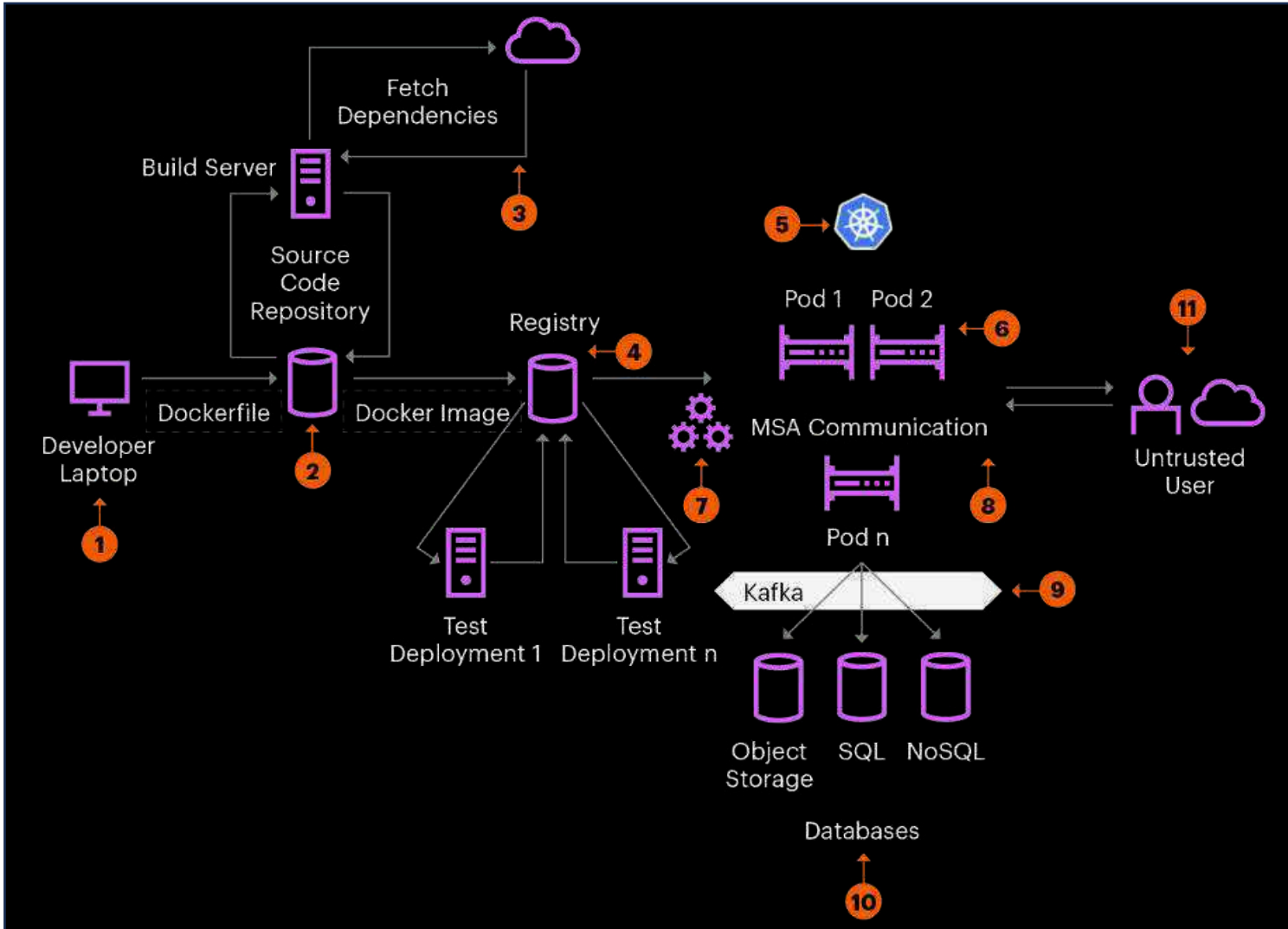
서비스/런타임 health 확인

클릭을 통한 Yaml 파일 확인

Kubernetes 보안

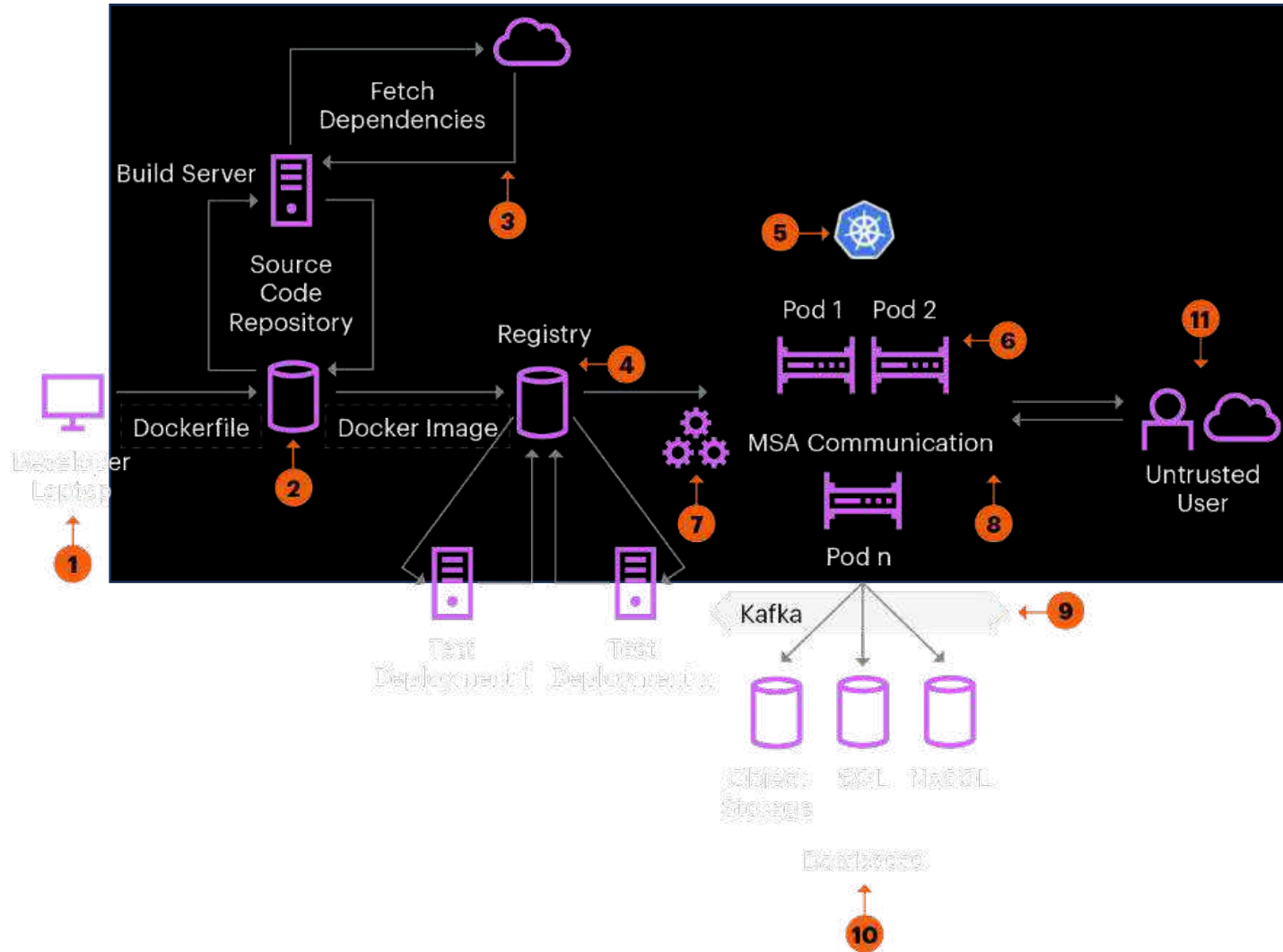


컨테이너 라이프사이클의 위협 요소 by Gartner



1. 개발 시스템
2. Git 기반 저장소
3. 의존성 검색
4. 이미지 레지스트리
5. 보안되지 않은 오케스트레이터 플랫폼
6. 호스트-컨테이너간의 관리
7. 빠른 변화율
8. MSA 통신 및 네트워크 분리
9. 프로세스 간 통신
10. 데이터베이스 수 증가
11. 애플리케이션 계층 공격

컨테이너 라이프사이클의 위협 요소 by Gartner



1. 개발 시스템
2. Git 기반 저장소
3. 의존성 검색
4. 이미지 레지스트리
5. 보안되지 않은 오케스트레이터 플랫폼
6. 호스트-컨테이너간의 관리
7. 빠른 변화율
8. MSA 통신 및 네트워크 분리
9. 프로세스 간 통신
10. 데이터베이스 수 증가
11. 애플리케이션 계층 공격

Cisco Panoptica

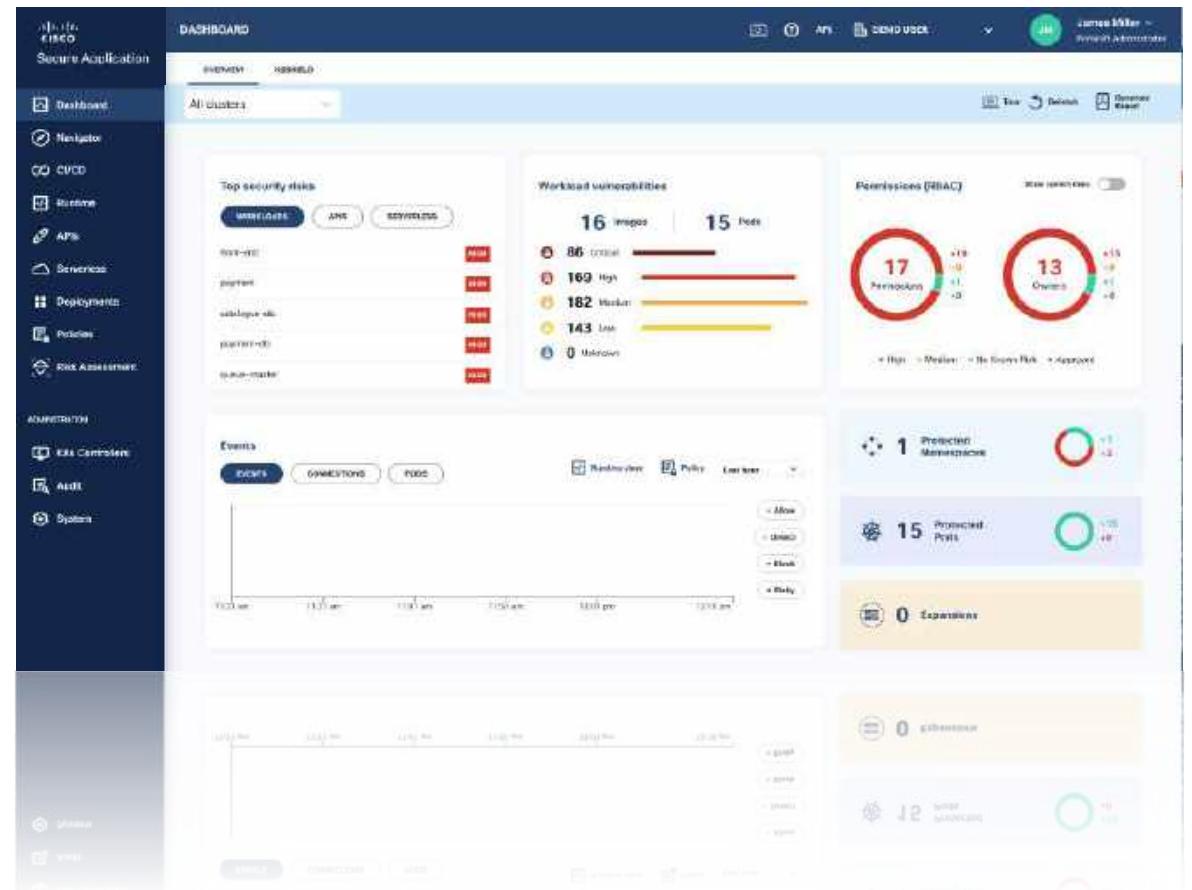
클라우드 네이티브 앱의 모든 것을 위한 **단일 환경**에서 관리

응용 프로그램의 모든 요소에 대한
취약점 제시

컨테이너, 이미지, SBOM, CI/CD,
서버리스 및 API 에 대한 **제어 및 관리**

보안취약점 및 사용자 정의 정책을 통한
워크로드 수정 및 우선순위 지정

기업을 위한 **보안 정책 및 규정 준수**를
정의하고 시행합니다



배포의 시작 - Registry의 이미지 관리

The screenshot displays the Panoptica CI/CD interface. The left sidebar contains navigation links: Dashboard, Navigator, CI/CD (highlighted), Runtime, APIs, Serverless, Deployments, Policies, Risk Assessment, and Compliance. The main content area is titled 'Images' and shows the URL 'docker.io/dcartesresearch/teastore-image'. Below this, there are tabs for 'VULNERABILITIES' (selected), 'IMAGE LAYERS', 'CIS BENCHMARK', 'PACKAGES & LICENSES', and 'EXPOSURE'. The 'VULNERABILITIES' tab shows a table of findings. The first finding is a critical vulnerability (CVSS 9.1) with the ID CVE-2021-35942, which is fixable. The second finding is a critical vulnerability (CVSS 9.8) with the ID CVE-2021-3177, which is not currently fixable. The interface also includes a 'Fixable only' filter and a 'Columns' button to toggle between 'Properties' and 'Consequences' views.

FINDINGS	NAME	FIX AVAILABILITY	DESCRIPTION
9.1 critical	CVE-2021-35942	Fix available	The wordexp function in the GNU C Library (aka glibc) through 2.33 may crash or read arbitrary memory in parse_param (in posix/wordexp.c) when called with an untrusted, crafted pattern, potentially resulting in a denial of service or disclosure of information. This occurs because atoi was used but strtoul should have been used to ensure correct calculations.
9.8 critical	CVE-2021-3177	No fix is currently available	Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _types/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely.

배포의 시작 - Registry의 이미지 관리

The screenshot displays the Panoptica CI/CD interface. The sidebar on the left contains navigation links: Dashboard, Navigator, CI/CD (highlighted), Runners, APIs, Serverless, Deployments, Policies, Risk Assessment, and Compliance. The main content area is titled 'Images' and shows details for the image `docker.io/dcartesresearch/teastore-image`. The 'Image Layers' tab is selected, showing a list of layers with their commands and vulnerability counts. The second layer is highlighted with a yellow box.

Layer	Command	Total	Critical	High	Medium	Low	Info
1	<code>COPY target/*.war /usr/local/tomcat/webapps/ # buildkit</code>	12	0	8	3	1	0
2	<code>set -eux; savedAptMark="\$(apt-mark showmanual)"; apt-get update; apt-get install -y --no-install-recommends gnupg dirmngr wget ca-certificates ; ...</code>	241	29	70	38	104	0
3	<code>set -eux; nativeLines="\$(cat /etc/catalina.sh grep -v '^#'); nativeLines="\$(echo "\$nativeLines" grep 'Apache Tomcat Native'); nativeLines="\$(echo "\$nativeLines" sort -u)"; ...</code>	0	0	0	0	0	0
4	<code>RUN /bin/sh -c sed -i 's/JDK_JAVA_OPTIONS.*\$/ /usr/local/tomcat/bin/catalina.sh # buildkit</code>	0	0	0	0	0	0
5	<code>set -eux; if ! command -v gpg > /dev/null; then apt-get update; apt-get install -y --no-install-recommends gnupg dirmngr ; rm -f ...</code>	0	0	0	0	0	0
6	<code>COPY kieker.monitoring.properties /kieker/config/kieker.monitoring.properties # buildkit</code>	0	0	0	0	0	0
7	<code>apt-get update && apt-get install -y --no-install-recommends git mercurial openssh-client subversion procps && rm -rf /var/lib/apt/lists/*</code>	0	0	0	0	0	0
8	<code>RUN /bin/sh -c rm /usr/local/tomcat/conf/server.xml # buildkit</code>	0	0	0	0	0	0
9	<code>RUN /bin/sh -c rm /usr/local/tomcat/lib/tomcat-websocket.jar # buildkit</code>	0	0	0	0	0	0

서비스의 안정성 - Runtime 관리

The screenshot displays the Panoptica Runtime management interface. The left sidebar contains navigation options: Dashboard, Navigator, CI/CD, Runtime (highlighted), APIs, Serverless, Deployments, Policies, Risk Assessment, and Compliance. The main panel is titled 'RUNTIME' and includes tabs for WORKLOADS, CONNECTIONS, EVENTS, and NAMESPACES. A 'Last 5 minutes' filter is selected. Below the filters, a table lists various workloads with their associated risk levels and security threats.

WORKLOAD	WORKLOAD RISK	SECURITY THREATS	ENVIRONMENT	CLUSTER	STATUS	START TIME	RESULT	API TOKEN INJECTION	PROTECTED
teastore-webui	High risk	Identified, Protected, Clusters & Namespaces, Environment, Workload	teastore	kubernetes	Active	6:36:52 PM Apr 20th, 2023	Block	—	Unprotected
smm	High risk	Identified, Protected, Clusters & Namespaces, Environment, Workload		kubernetes	Active	3:12:10 PM Mar 7th, 2023	Block	—	Unprotected
smm	High risk	Identified, Protected, Clusters & Namespaces, Environment, Workload		kubernetes	Active	3:12:10 PM Mar 7th, 2023	Block	—	Unprotected
smm-tracing	High risk	Identified, Protected, Clusters & Namespaces, Environment, Workload		kubernetes	Active	3:12:10 PM Mar 7th, 2023	Block	—	Unprotected
smm-authentication	High risk	Identified, Protected, Clusters & Namespaces, Environment, Workload		kubernetes	Active	3:12:10 PM Mar 7th, 2023	Block	—	Unprotected
smm-web	High risk	Identified, Protected, Clusters & Namespaces, Environment, Workload		kubernetes	Active	3:12:10 PM Mar 7th, 2023	Block	—	Unprotected
smm-federation-gateway	High risk	Identified, Protected, Clusters & Namespaces, Environment, Workload		kubernetes	Active	3:12:10 PM Mar 7th, 2023	Block	—	Unprotected
smm-federation	High risk	Identified, Protected, Clusters & Namespaces, Environment, Workload		kubernetes	Active	3:12:10 PM Mar 7th, 2023	Block	—	Unprotected

서비스의 안정성 - Runtime 관리

The screenshot displays the Panoptica Runtime management interface. The left sidebar contains navigation links: Dashboard, Navigator, CI/CD, Runtime (highlighted), APIs, Serverless, Deployments, Policies, Risk Assessment, Compliance, ADMINISTRATION, Audit, and System. The main content area is titled 'RUNTIME' and shows the 'Workloads' section. A specific workload, 'teastore-webui', is selected, and its 'DETAILS & RISK' tab is active. The workload risk is indicated as 'High risk'. A list of risk factors is shown, including vulnerabilities, root access, public-facing status, SSH access, privilege escalation, template modifications, and unidentified workloads. The workload details section shows it is running on the 'kubernetes' cluster in the 'teastore' namespace, with the rule 'Restrict unidentified workloads' applied, resulting in a 'Block' action. The workload is marked as 'UNPROTECTED'. The workload trust section shows it has unidentified images and is not identified by the registry. The workload licenses section lists various licenses such as 2lib, APL-3.0, BSD-4-Clause, etc.

panoptica <

RUNTIME

< Workloads

teastore-webui

DETAILS & RISK | POD TEMPLATE | SECURITY CONTEXT | API | LICENSES

Workload risk: **High risk** Edit

- The workload has a vulnerability of severity HIGH or CRITICAL
- The workload can run as root
- The workload is public-facing
- The workload is accessible using SSH (port 22 is open)
- The workload can escalate its privileges
- The workload template has been modified
- The workload is unidentified

You may edit the ignore risk rules on the [Risk Management page](#). Please note that it will take few minutes to update the risk table.

Workload licenses:

2lib APL-3.0 BSD-4-Clause GPL-1.3-only LGPL-2.1-only BSD-3-Clause BSD-2-Clause GPL-2.0-only GPL-3.0-only Artistic-2.0 Apache-2.0 CC0-1.0 MIT GFDL-1.2-only

Workload details

CLUSTER	NAMESPACE	ENVIRONMENT
kubernetes	teastore	teastore

RULE NAME	RULE ACTION	VIOLATION REASON
Restrict unidentified workloads	Block	

UNPROTECTED X

Workload trust

- The workload has unidentified Images
- The workload was identified
- The image registry is untrusted

Kubernetes CIS Benchmark

panoptica

Dashboard

Navigator

CI/CD

Runtime

APIs

Serverless

Deployments

Policies

Risk Assessment

Compliance

COMPLIANCE

Set up Panoptica

UPGRADE ACCOUNT

API

HP

Han Jin Park Administrator

Kubernetes CIS Benchmark summary

89% Scanned clusters compliance

1 out of 1 clusters scanned

1 Clusters with action items

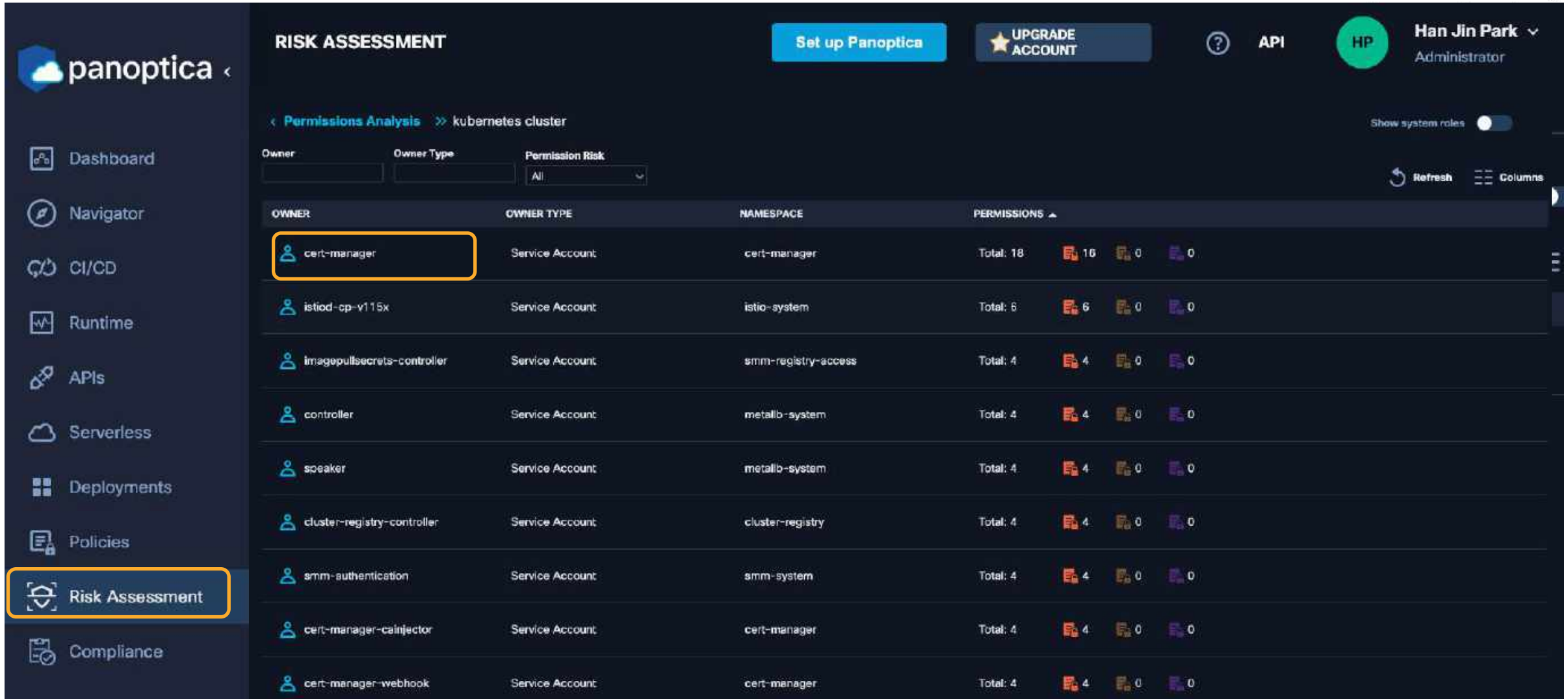
TEST	COMPLIANCE	RESULTS	ACTION ITEMS
1. Control Plane Security Configuration	82%	42 9 0	11
1.1. Control Plane Node Configuration Files	94%	18 1 0	2
1.2. API Server	75%	18 6 0	8

RECOMMENDATION	COMPLIANCE	TYPE	REMEDIATION
1.2.1. Ensure that the --anonymous-auth argument is set to false (Manual)	0%	NA	Edit the API server pod specification file /etc/kubernetes/manifests/kube-apiserver.yaml on the control plane node and set the below parameter. --anonymous-auth=false
1.2.2. Ensure that the --token-auth-file parameter is not set (Automated)	100%	NA	Follow the documentation and configure alternate mechanisms for authentication. Then, edit the API server pod specification file /etc/kubernetes/manifests/kube-apiserver.yaml on the control plane node and remove the --token-auth-file=<filename> parameter.
1.2.3. Ensure that the --DenyServiceExternalIPs is not set (Automated)	100%	NA	Edit the API server pod specification file /etc/kubernetes/manifests/kube-apiserver.yaml on the control plane node and remove the 'DenyServiceExternalIPs' from enabled admission plugins.

CISCO Connected

CIS: Center for Internet Security

Kubernetes RBAC



The screenshot displays the Panoptica Risk Assessment interface. The left sidebar contains navigation links: Dashboard, Navigator, CI/CD, Runtime, APIs, Serverless, Deployments, Policies, Risk Assessment (highlighted), and Compliance. The main content area is titled 'RISK ASSESSMENT' and shows a 'Permissions Analysis' for a 'kubernetes cluster'. A table lists various service accounts and their permissions. The 'cert-manager' entry is highlighted with a yellow box.

RISK ASSESSMENT

Set up Panoptica | UPGRADE ACCOUNT | ? API | HP Han Jin Park Administrator

< Permissions Analysis >> kubernetes cluster

Show system roles

Owner: [] Owner Type: [] Permission Risk: All

Refresh Columns

OWNER	OWNER TYPE	NAMESPACE	PERMISSIONS
cert-manager	Service Account	cert-manager	Total: 18 16 0 0
istiod-cp-v115x	Service Account	istio-system	Total: 6 6 0 0
imagepullsecrets-controller	Service Account	smm-registry-access	Total: 4 4 0 0
controller	Service Account	metalib-system	Total: 4 4 0 0
speaker	Service Account	metalib-system	Total: 4 4 0 0
cluster-registry-controller	Service Account	cluster-registry	Total: 4 4 0 0
smm-authentication	Service Account	smm-system	Total: 4 4 0 0
cert-manager-cainjector	Service Account	cert-manager	Total: 4 4 0 0
cert-manager-webhook	Service Account	cert-manager	Total: 4 4 0 0

Kubernetes RBAC

The image shows the Panoptica Risk Assessment interface. The left sidebar contains navigation links: Dashboard, Navigator, CI/CD, Runtime, APIs, Serverless, Deployments, Policies, Risk Assessment (highlighted), and Compliance. The main content area is titled 'RISK ASSESSMENT' and has three tabs: 'RUNTIME SCANS', 'PERMISSIONS (RBAC)' (highlighted), and 'RISK MANAGEMENT'. The 'PERMISSIONS (RBAC)' tab shows a breadcrumb trail: '< Permissions Analysis >> kubernetes cluster >> cert-manager owner >> cert-manager-controller-challenges role'. Below this is a table with columns: RESOURCES, RESOURCE NAMES, API GROUPS, VERBS, RISK, and RISK REASONS. The table lists several resources with their associated risks. The 'Risk Assessment' sidebar item and the 'Permissions (RBAC)' tab are highlighted with orange boxes. The table content is also highlighted with an orange box.

RESOURCES	RESOURCE NAMES	API GROUPS	VERBS	RISK	RISK REASONS
challenges, challenges/status		acme.cert-manager.io	update, patch	No known risk risk	
challenges		acme.cert-manager.io	get, list, watch	No known risk risk	
issuers, clusterissuers		cert-manager.io	get, list, watch	No known risk risk	
secrets		core	get, list, watch	High risk	Allows access to secrets that can result in exposure of private credentials, passwords, private encryption keys, etc.
events		core	create, patch	High risk	Allows to access all cluster events which can result in disclosure of sensitive information, falsely changing event content or removal of important information
pods, services		core	get, list, watch, create, delete	High risk	Allows to create, delete and even modify running workloads in the cluster which can result in changing of desired workload behavior Allows to modify network routes which can result in unauthorized communication or DoS
Ingresses		networking.k8s.io	get, list, watch, create, delete, update	High risk	Allows to modify network routes which can result in unauthorized communication or DoS

API Security

panoptica

APIS

Set up Panoptica

UPGRADE ACCOUNT

API

Han Jin Park Administrator

DASHBOARD RISK FINDINGS INTERNAL APIS THIRD-PARTY APIS TOKENS GATEWAYS API POLICY PROFILE

Internal APIs

Refresh

Specs & diffs

69 Total APIs

0 No data

- APIs with specs
- APIs without specs
- Zombie operations
- Shadow operations
- Rogue operations
- Valid operations

Top risky findings

FINDING NAME	RISK	CATEGORY
--------------	------	----------

Top risky APIs

- carta
- catalogue
- user
- analytics
- analytics
- analytics

Risk findings

0 No data

Risk Findings Trend

No data to display

Critical High Medium Low No known risk

API Security

The screenshot displays the Panoptica API Security interface. On the left is a dark sidebar with navigation links: Dashboard, Navigator, CI/CD, Runtime, APIs (highlighted), Serverless, Deployments, Policies, Risk Assessment, Compliance, ADMINISTRATION, Audit, and System. The main content area is titled 'apis' and shows details for the 'carts:80' API, last updated on Oct 24th, 2022. Below this are tabs for API DETAILS, SPECS, and RISK FINDINGS (active). Under RISK FINDINGS, there are sub-tabs for SECURITY POSTURE, BFLA, TEST, and TRACE ANALYSIS. A 'Categories List' shows 'server-workload-security' with a warning icon, highlighted by an orange box. The right panel, titled '3 Medium risk findings', lists three issues, each with a title, occurrence count, source, description, and mitigation. The first finding, 'The workload template has been modified' (1 Occurrence), is highlighted with an orange box. The second finding, 'The workload can escalate its privileges' (1 Occurrence), is also highlighted. The third finding, 'The workload is accessible using SSH (port 22 is open)' (1 Occurrence), is highlighted. Each finding has a 'Download finding's JSON' button. The top right of the interface includes links for 'Set up Panoptica', 'UPGRADE ACCOUNT', and a user profile for 'Han Jin Park'.

panoptica

apis

Dashboard
Navigator
CI/CD
Runtime
APIs
Serverless
Deployments
Policies
Risk Assessment
Compliance

ADMINISTRATION
Audit
System

apis

carts:80
Last update: 10:10:56 PM Oct 24th, 2022

API DETAILS SPECS **RISK FINDINGS**

SECURITY POSTURE BFLA TEST TRACE ANALYSIS

Categories List

server-workload-security ⚠️

3 Medium risk findings

The workload template has been modified 1 Occurrence

Download finding's JSON

Source: workload_security
Description: The workload template has been modified
Mitigation: Address this issue in the API server workload image

The workload can escalate its privileges 1 Occurrence

Download finding's JSON

Source: workload_security
Description: The workload can escalate its privileges
Mitigation: Address this issue in the API server workload image

The workload is accessible using SSH (port 22 is open) 1 Occurrence

Download finding's JSON

Source: workload_security
Description: The workload is accessible using SSH (port 22 is open)
Mitigation: Address this issue in the API server workload image

Set up Panoptica
UPGRADE ACCOUNT
API
Han Jin Park Administrator

API Security - Third-Party

The screenshot displays the Panoptica API Security dashboard. The left sidebar contains navigation links: Dashboard, Navigator, CI/CD, Runtime, APIs (highlighted with an orange box), Serverless, Deployments, Policies, Risk Assessment, Compliance, and an ADMINISTRATION section with Audit and System links. The main header includes the Panoptica logo, a 'Set up Panoptica' button, an 'UPGRADE ACCOUNT' button, a help icon, the 'API' tab, and a user profile for 'Han Jin Park' (Administrator). The main content area is titled 'APIS' and features a navigation bar with tabs: DASHBOARD, RISK FINDINGS, INTERNAL APIS, THIRD-PARTY APIS (highlighted with an orange box), TOKENS, GATEWAYS, and API POLICY PROFILE. Below the tabs, there is a 'New API' button and a table of API entries. The first entry, 'https://www.linuxfoundation.org/', is highlighted with an orange box and shows a total of 10 security findings: 0 Critical, 3 High, 0 Medium, 7 Low, and 0 No known risk. Below the table, the details for 'https://www.linuxfoundation.org/' are shown, including a 'Last update' timestamp and a 'Download JSON' button. The details section is divided into 'API DETAILS', 'SPECS', 'SECURITY POSTURE', and 'API ENDPOINTS'. The 'SECURITY POSTURE' tab is active, showing 'Client Workloads' and 'Compliant to' sections. A 'Top Risk Categories' bar chart is also present, with 'Network' and 'Application' categories highlighted by an orange box. The chart shows 'Network' with a risk level of 3 (High) and 'Application' with a risk level of 4 (Medium).

API Security Dashboard - Third-Party APIs

API List:

API NAME	SECURITY FINDINGS	CLIENT WORKLOADS	POLICY COMPLIANCE	SPECS
https://www.linuxfoundation.org/	Total: 10 0 Critical, 3 High, 0 Medium, 7 Low, 0 No known risk		✓	

API Details for https://www.linuxfoundation.org/

Last update: 12:19:33 PM Jun 2nd, 2023

API Details Section:

- Client Workloads:**
- Compliant to:** Select...
- Top Risk Categories:**

Risk Level Legend:

- Critical (Red)
- High (Orange)
- Medium (Yellow)
- Low (Light Green)
- No known risk (Dark Green)

Top Risk Categories Chart:

Category	Risk Level
Network	High (3)
Application	Medium (4)

API Security - Third-Party

The screenshot displays the Panoptica API Security dashboard. The left sidebar contains navigation links: Dashboard, Navigator, CI/CD, Runtime, APIs (highlighted with an orange box), Serverless, Deployments, Policies, Risk Assessment, Compliance, and an ADMINISTRATION section with Audit and System links. The main content area is titled 'APIs' and shows the URL 'https://www.linuxfoundation.org/'. The 'SECURITY POSTURE' tab is selected and highlighted with an orange box. Under the 'Categories List', the 'network' category is highlighted with an orange box. The dashboard reports '3 High risk findings'. One finding is expanded, showing details for 'TLS Version' with '3 Occurrences'. The finding details include the source 'shodan', a description that the protocol is deprecated, and a mitigation to use a secured one. An 'Additional Info' section is highlighted with an orange box, listing affected endpoints and specific asset/module details.

APIs

SECURITY POSTURE

Categories List

- network
- application

3 High risk findings

TLS Version 3 Occurrences

Source shodan

Description The protocol used is deprecated or no more recommended.

Mitigation Disable this protocol and use a secured one.

Occurrences

#1 Additional Info

- Affected endpoint: 199.60.103.31:443
- title: Asset
value: "199.60.103.31:443"
- title: Module
value: "https-simple-new"
- title: Description
value: "Weak SSL version"
- title: Version

API Security - Third-Party

The screenshot displays the Panoptica API Security dashboard. The left sidebar contains navigation links: Dashboard, Navigator, CI/CD, Runtime, APIs (highlighted with an orange box), Serverless, Deployments, Policies, Risk Assessment, Compliance, and an ADMINISTRATION section with Audit and System links. The main content area is titled 'APIs' and shows the URL 'https://www.linuxfoundation.org/'. The 'SECURITY POSTURE' tab is selected and highlighted with an orange box. Below this, a 'Categories List' shows 'network' and 'application' (highlighted with an orange box). The 'application' category shows '4 Low risk findings'. One finding is expanded, showing 'Missing required headers' with '4 Occurrences'. The finding details include: Source (shodan), Description (One or more required security headers are not set...), Mitigation (Ensure your policy correctly implements the required headers.), and Occurrences. The 'Occurrences' section is highlighted with an orange box and shows two items: '#1 Additional Info' with affected endpoint '199.60.103.31:443' and title 'Asset' with value '199.60.103.31:2083', and '#2 Additional Info' with title 'Description' and value 'At least one security header is required'.

panoptica

APIs

https://www.linuxfoundation.org/

Last update: 12:19:33 PM Jun 2nd, 2023

API DETAILS SPECS **SECURITY POSTURE** API ENDPOINTS

Categories List

network

application

4 Low risk findings

Missing required headers 4 Occurrences

Download JSON

Download finding's JSON

Source shodan

Description One or more required security headers are not set. These headers are important for preventing attacks and must be checked for use and correct configuration.

Mitigation Ensure your policy correctly implements the required headers.

Occurrences

#1 Additional Info

Affected endpoint: 199.60.103.31:443

title: Asset
value: "199.60.103.31:2083"

title: Description
value: "At least one security header is required"

#2 Additional Info

CISCO Connected

K8Sheld를 통한 MITRE ATT&CK Framework

The screenshot displays the Panoptica K8Sheld dashboard. The left sidebar contains navigation links: Dashboard, Navigator, CI/CD, Runtime, APIs, Serverless, Deployments, Policies, Risk Assessment, Compliance, ADMINISTRATION, Audit, and System. The main dashboard area is titled 'DASHBOARD' and includes a 'K8SHIELD' tab. Key metrics shown are: LAST UPDATE (Jun 5th 2023, 13:15), 1 CLUSTER (All clusters), and 14/14 COMPROMISED NAMESPACES (kubernetes/bookinfo +13). A table below lists various MITRE ATT&CK techniques and their status:

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIALS ACCESS	DISCOVERY	LATERAL MOVEMENT	IMPACT
✓ PUBLIC FACING PRIVILEGED WORKLOAD	⚠ CONTAINER SERVICE	⚠ WRITABLE HOSTPATH MOUNT	⚠ PRIVILEGED PODS/ ROOT PODS	⚠ CLEAR CONTAINER LOGS	⚠ EXPOSE KUBERNETES SECRETS	✓ EXPOSED KUBERNETES DASHBOARD	⚠ CLUSTER INTERNAL NETWORKING	⚠ DATA DESTRUCTION
✓ EXPOSED KUBERNETES DASHBOARD	⚠ DEPLOY CONTAINER	⚠ KUBERNETES CRONJOB CREATION	⚠ PRIVILEGES ESCALATION ENABLED	⚠ DEPLOY CONTAINER	⚠ SERVICEACCOUNT ACCESS	⚠ CONTAINER RESOURCE DISCOVERY	✓ ACCESS TILLER ENDPOINT (HELM 2)	
⚠ VULNERABLE WORKLOADS	⚠ SSH SERVER RUNNING INSIDE CONTAINER		⚠ RESTRICT ADMIN BINDING ABILITY	⚠ DELETE KUBERNETES EVENTS			✓ EXPOSED KUBERNETES DASHBOARD	
⚠ UNAUTHORISED REGISTRIES USAGE			✓ MULTIPLE CLUSTER ADMINS				⚠ CORE DNS POISONING	
✓ SUSPICIOUS DEPLOYMENT			⚠ ACCESS THE KUBERNETES API SERVER					
⚠ COMPROMISED IMAGES IN REGISTRY			⚠ WRITABLE HOSTPATH MOUNT					

Summary



컨테이너 더이상 피할 수는 없습니다.



복잡한 K8S 에서 손쉽게 서비스 가시성을 확보하세요.



K8S 의 다양한 보안이슈를 단일 환경에서 관리합니다.



Cisco는 고객의 Containerization 을 함께 도와드립니다.



2개 클러스터 10개 노드까지 무료로 체험해보세요.
(<https://www.calisti.app>, <https://www.panoptica.app>)



The bridge to possible

감사합니다.

CISCO *Connect*

ALL IN

#CiscoConnect



The bridge to possible

메가존클라우드의 Cisco Meraki 기반 구독형 IT매니지드 서비스 F:it

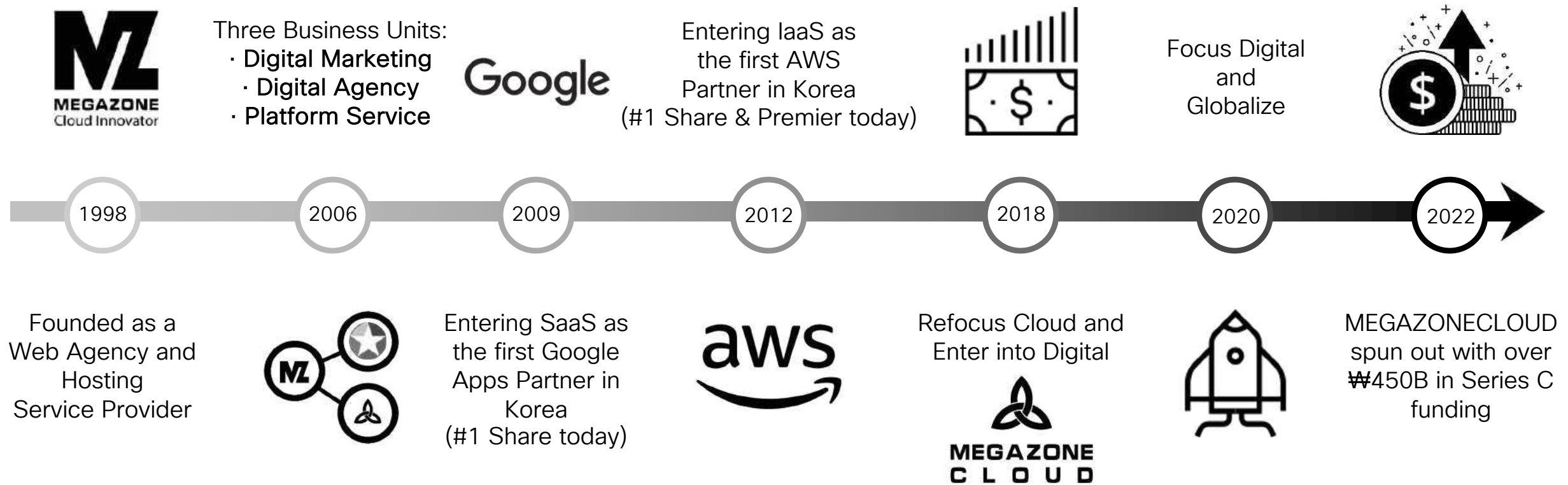
오영찬 팀장 | 메가존클라우드
홍순권, 머라키 팀 이사 | 시스코코리아



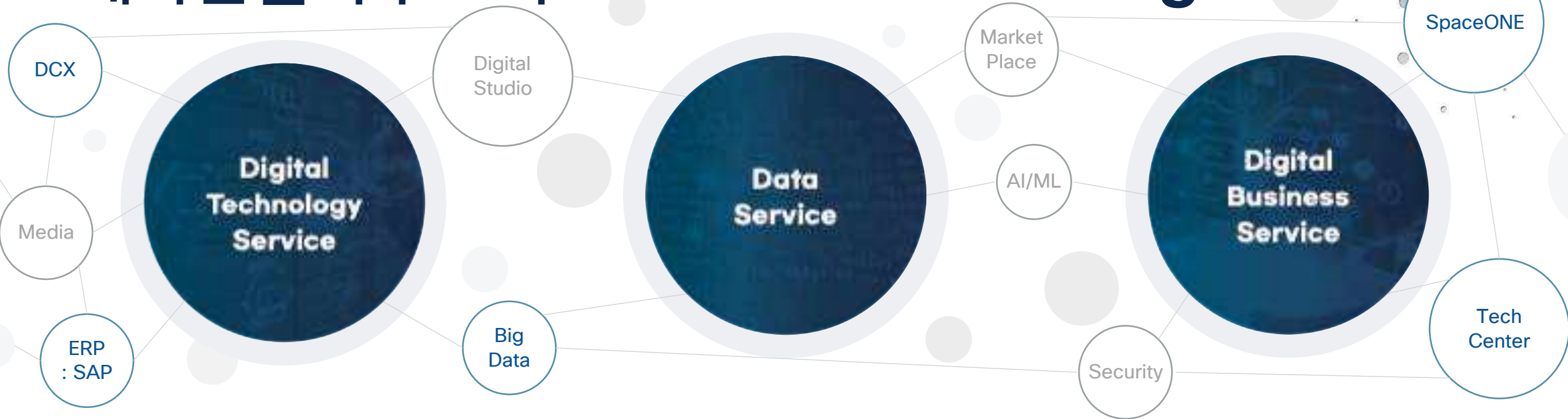
Agenda

- 메가존클라우드 소개
- IT 소비의 변화와 **Pain Points**
- **F:it your IT as you want**
- **IT/IOT** 관리의 새로운 패러다임
Cisco Meraki
- 메가존클라우드 **Offering**의 확장
- **Conclusion**

25년 간의 디지털 혁신 과정에서의 변화



메가존클라우드의 Business & Offerings



Infrastructure

디지털 혁신을 위한 최적화된 인프라

- Managed Service
- Mass Migration Service
- Cloud Security Service
- DMZ Stack & VMC on Cloud
- Graphcore & SQream

Platform

디지털 혁신 가속화를 위한 모던
어플리케이션 개발/운영/관리 플랫폼

- SpaceONE
- Megazone PoPs
- CloudPlex
- Rescale & Elastic

Application

신속한 디지털 비즈니스 의사결정 및
관리를 위한 비즈니스 어플리케이션

- SAP on Cloud
- Salesforce/Zendesk : Mega CX

Data

데이터 가치 실현을 위한
데이터 플랫폼 구축

- Data Business Service
- Big Data
- DW/Data Lake
- AI/ML

메가존클라우드의 Business & Offerings

Digital Technology Service



Data Service



Digital Business Service



메가존클라우드의 Business & Offerings

Hyper Billing

1,500+ install-base with
AWS, Google, Microsoft
& major CSP
Cost Management Solution



Multi-Cloud Management
Platform which extends into
IDC inventories with Single
Pane of Glass enabling IaC -
based infrastructure operation



F:it your IT as you want

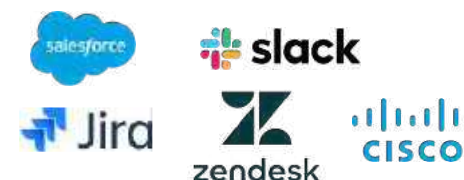
F:it's business philosophy is
to assure the highest quality
product, total client
satisfaction, timely delivery of
solutions and the best
quality/price ratio found in the
industry.



...



Enterprise SaaS
management platform
helping customers with an
increasing application
deployment



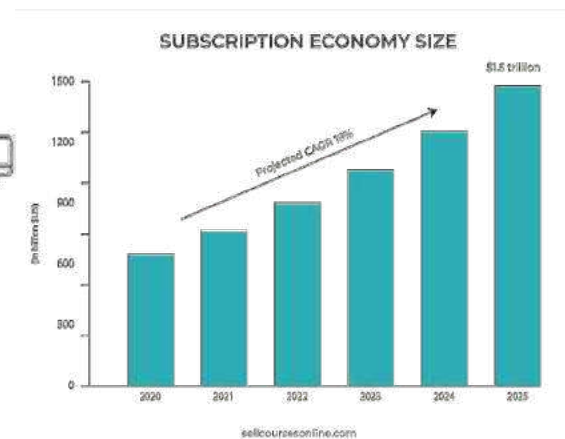
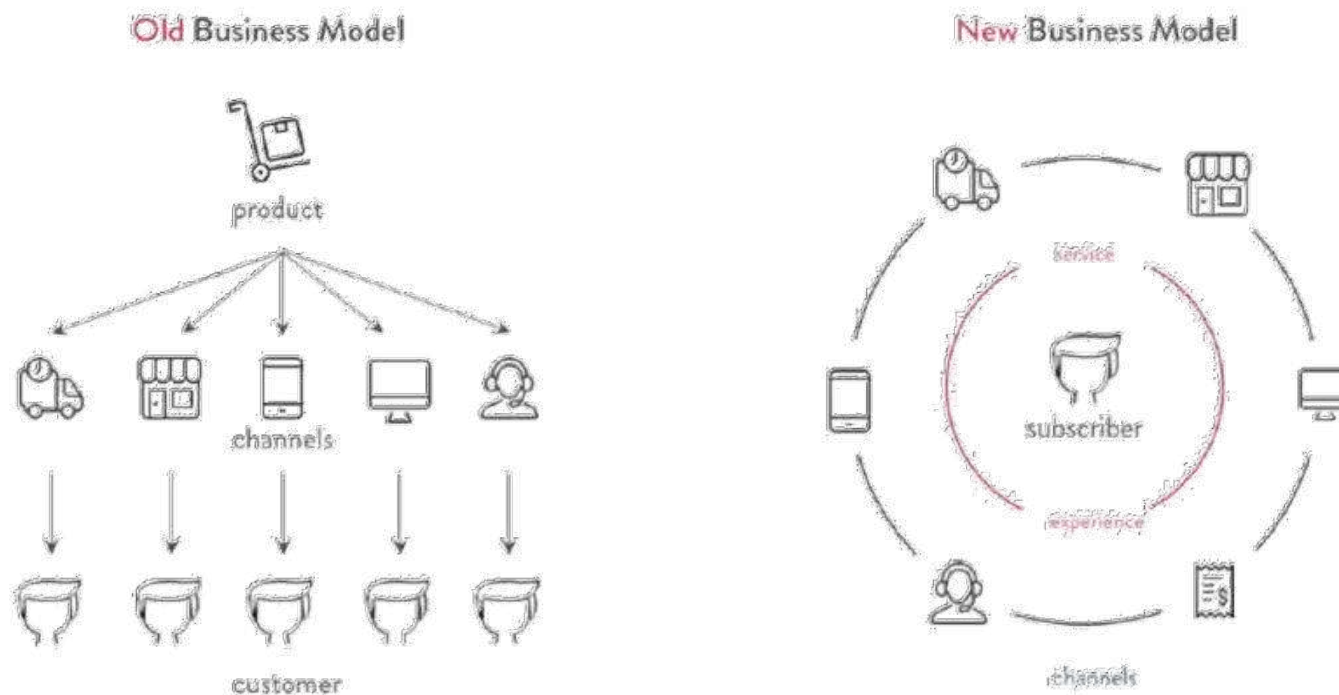
...

IT 소비 방식의 변화

- 소비자가 상품을 구매하고 '소유'하던 구조에서, 돈을 지불하고 상품을 '이용·경험'하는 방향으로 소비 구조의 전환이 관찰되고 있습니다. 코로나19 이후 재택근무, 비대면 등 소비자 라이프 스타일 패턴 변화로 다양한 서비스에 대한 구독시장이 B2C를 넘어 B2B시장에도 확대되고 있습니다.

▶▶ 소유경제 vs 구독경제

A NEW WAY OF THINKING



고객의 Pain Points

네트워크 장애 문제

- 네트워크 장애, 성능 저하 조치의 어려움
- IT 담당자의 부재 또는 업무 부하



CISCO Connect

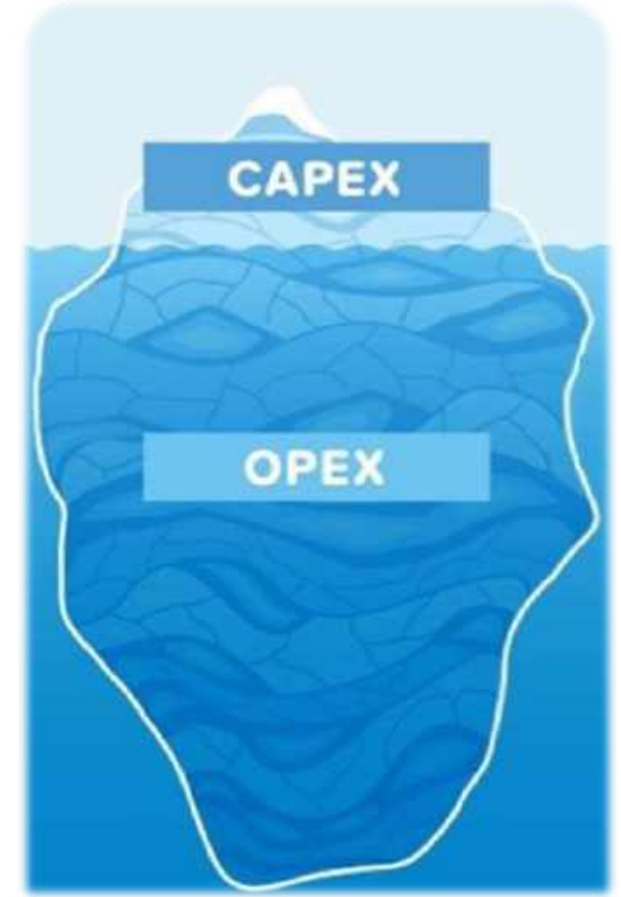
복잡한 HW/SW 구매 절차

- 최적의 솔루션 결정 문제
- 솔루션 업체별 별도 계산서 처리



TCO 절감 문제

- CAPEX 절감을 위한 구독 모델 고려
- OPEX 절감을 위한 솔루션 Search



F:it your IT as you want

F:it은 메가존클라우드가 제공하는 구독기반 All-in-One IT 서비스입니다.
기업에서 고민하고 있는 IT 인프라에 대한 모든 것을 매니지드 서비스와 함께 구독형태로 제공합니다.
기업의 모든 IT 고민을 F:it을 통해 한번에 해결할 수 있습니다.



원하는대로 F:it, 당신의 IT



F:it 코디네이터
[매니지드 서비스]

구매는 쉽게, 관리는 편하게.
어디에서든지 로그인 한번이면 끝!



F:it 24/7
[연중 무휴 서비스 센터]



F:it Subscription
[유연한 월과금 정책]

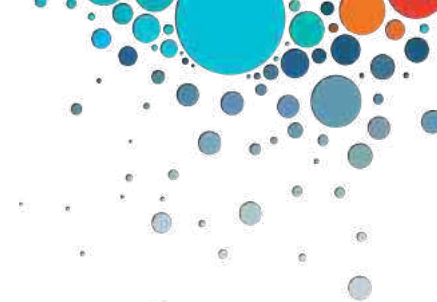
F:it E-Commerce
[IT 구독 스토어]

F:it Board
[구독 관리 대시보드]



F:it Recommender
[업종별 패키지 추천 기능]





F:it your IT as you want

F:it의 핵심가치는 고객의 요구사항에 Fit한 새로운 서비스를 제공해드리는 것입니다.
기업의 IT와 관련된 모든 어려움을 구독 기반의 All-in-One IT 서비스로 해결할 수 있는 것이죠.
신속하고 유연한 구매와 전문가의 매니지드 서비스를 더한 매력있는 F:it으로 당신의 마지막 IT 서비스가 되겠습니다.

Full-Managed :it 매니지드 서비스

F:it은 IT 전문가를 통해 관리 및 운영에 대한 부담을 덜고 핵심 업무에 집중할 수 있도록 도와드립니다.

24/7 서비스 지원을 제공하여 비즈니스의 생산성과 효율성을 높입니다.

Fast :it 신속한 업무 환경 구축

F:it은 이커머스 스토어를 제공함으로 어디서나 쉬운 방법으로 IT 인프라를 구매, 결정할 수 있는 환경을 제공합니다.

전문가의 지식과 경험을 활용하여 안정적이고 효율적인 IT 인프라를 구축합니다.

Fascinating :it 매력적인 추천 방식

F:it은 알고리즘 기반의 업종별 패키지 상품 추천을 통해 IT 최신 트렌드를 제공하여 매력적입니다.

IT 요구 사항에 따라 필요한 서비스를 유연하게 선택하여 비용을 최적화할 수 있습니다.

Flexible :it 유연한 구독

F:it은 비즈니스가 확장되거나 축소되더라도 필요에 맞게 IT 인프라를 조정할 수 있어 유연합니다.

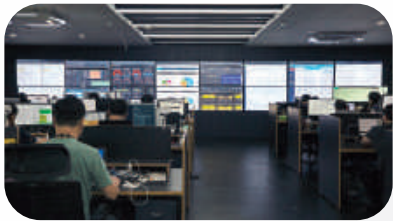
유연한 구독 모델을 통해 필요에 따라 비용을 조절할 수 있습니다.

First & Final : IT의 시작과 끝

원하는대로 F:it, 당신의 IT

Why Megazone Cloud

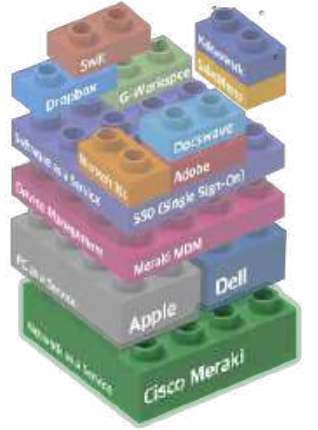
- 메가존클라우드 국내 최대의 Managed Service 기업



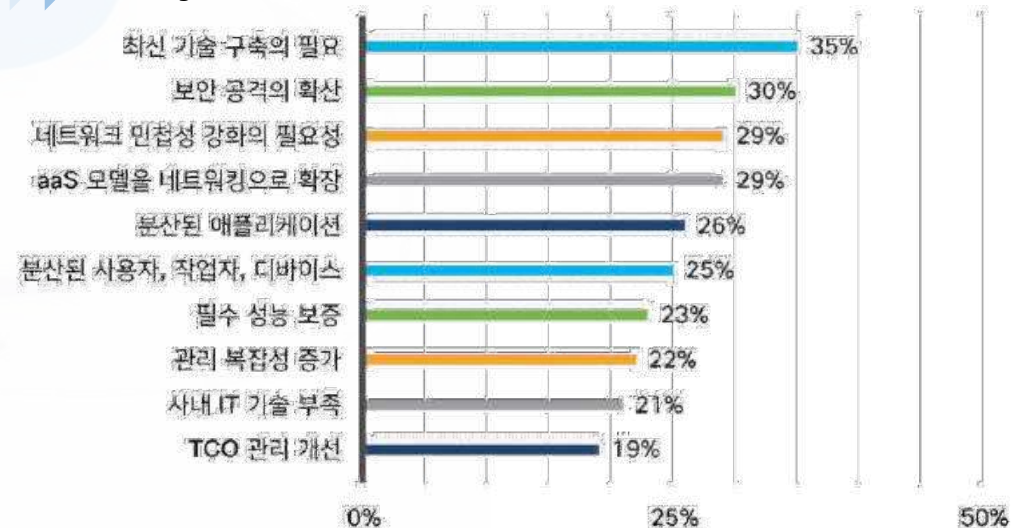
- 24/7/365 운영되는 Cloud Operation Center로 고객 서비스 모니터링 및 장애 대응
- 고객의 요구에 맞는 솔루션과 전문 엔지니어 직접 지원
 - 2,500+ 인력과 100+ ISV 전문 지원 기술 보유
- 고객의 Digital Transformation을 위한 Cisco와의 MOU
 - Meraki, AppDynamics, Duo, SD-WAN, Umbrella 등의 Cisco Cloud 솔루션 기술력 보유

Why F:it

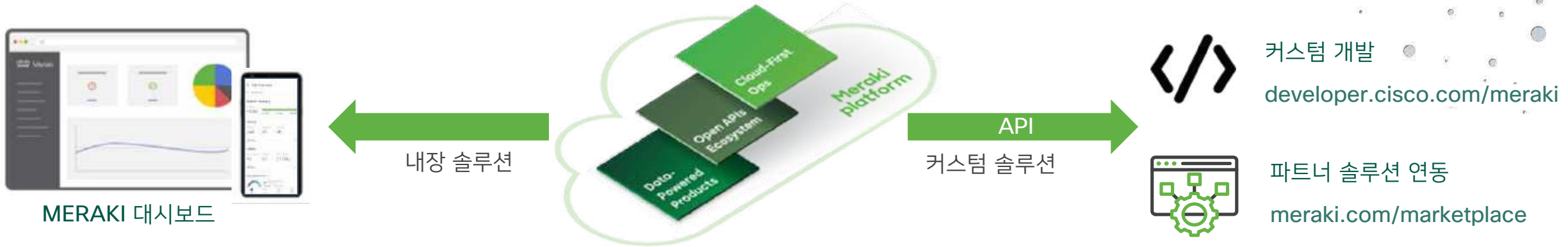
- All-in-One 오피스 IT 구독 서비스 제공
 - Internet → Network → Device → Software
- Lean IT 기업의 전문 기술 인력 지원
- 구독으로 CAPEX 절감, 예측 가능한 OPEX 확인

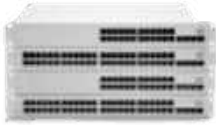


Why Network as a Service



Meraki 플랫폼: IT 와 IoT Full Portfolio



 MR 무선랜	 MS L2/L3 스위치	 MX UTM + SD-WAN	 SM 모바일 단말기 관리	 MV 스마트 카메라	 MT IoT 센서
자동무선상태 분석+ 최적화 어플리케이션 별 분석+관리 ML기반 무선성능 측정 (Meraki Health)	네트워크 단말에 대한 관리 제로터치 업데이트 자동설정을 위한 API	Site to Site Auto VPN App, WAN, VoIP Health 등에 대한 성능 측정 성능기반 경로 선택 Cisco Talos 및 Umbrella 연동	단말설정 및 접근권한 부여 App 및 업데이트 배포 도난/분실 기기 추적 분실 기기에 대한 초기화	AI를 활용한 분석 기능을 통해 다양한 업무 활용 영상접근 통제로 개인정보 보호 모션 및 일정 기반 저장 등을 통해 영상 저장 최적화	온도(냉동시설도 지원)/습도/누수/도어 개폐 등등의 전용 센서 다양한 알람 옵션 지원 최대 5일간의 센서 자체 정보 저장

언제 어디서나 심플한

전 세계에서 신뢰받는 Platform의 힘



640K+
고객수



99.99%
Cloud SLA

3.5M+

고객 네트워크

10M+

온라인 상태의
Meraki 장비들

190+

플랫폼 이용
중인 나라들

3.5B+

월간 API 이용

153M+

일일 End User
단말

98%

WW Meraki
라이선스 갱신율

100K+

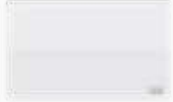
Top 5 고객들이 각자 이용 중인 Meraki 장비들

285K+

하나의 글로벌 고객사에서 운용하는 AP장비들

The Meraki platform

단일 대시보드를 통해 통합 모니터링 및 관리 지원



MR

Wireless



MX

Security
Appliances
& SD-WAN



MI

App Insight



MG

Cellular Gateway



MS

Switches



SM

EMM / MDM



MV

Smart Cameras



MT

IOT Sensors



Cat9xxx

CAT SW



Cisco Secure
Connect

Coming soon

???

What's next?



Journey of Meraki

그리스어, 영혼, 창의력, 사랑으로 만들어진 것

2006

클라우드 네트워킹 솔루션
최초 개발

2012

Cisco 인수 (현금 12억 달러)

2017

IT 포트폴리오를 IOT까지
범위 확장

TODAY

17년 이상의 확장성 및
보안을 지원하는 클라우드
아키텍처 설계 및 운영 노하우

CISCO *Connect*

Meraki는 클라우드 관리를 통해
보다 쉽고 간편한 운영 및 강력한 보안,
지능형/자동화 기반 업무 환경을 지원



Be Brave

I BELIEVE THAT WE WILL WIN

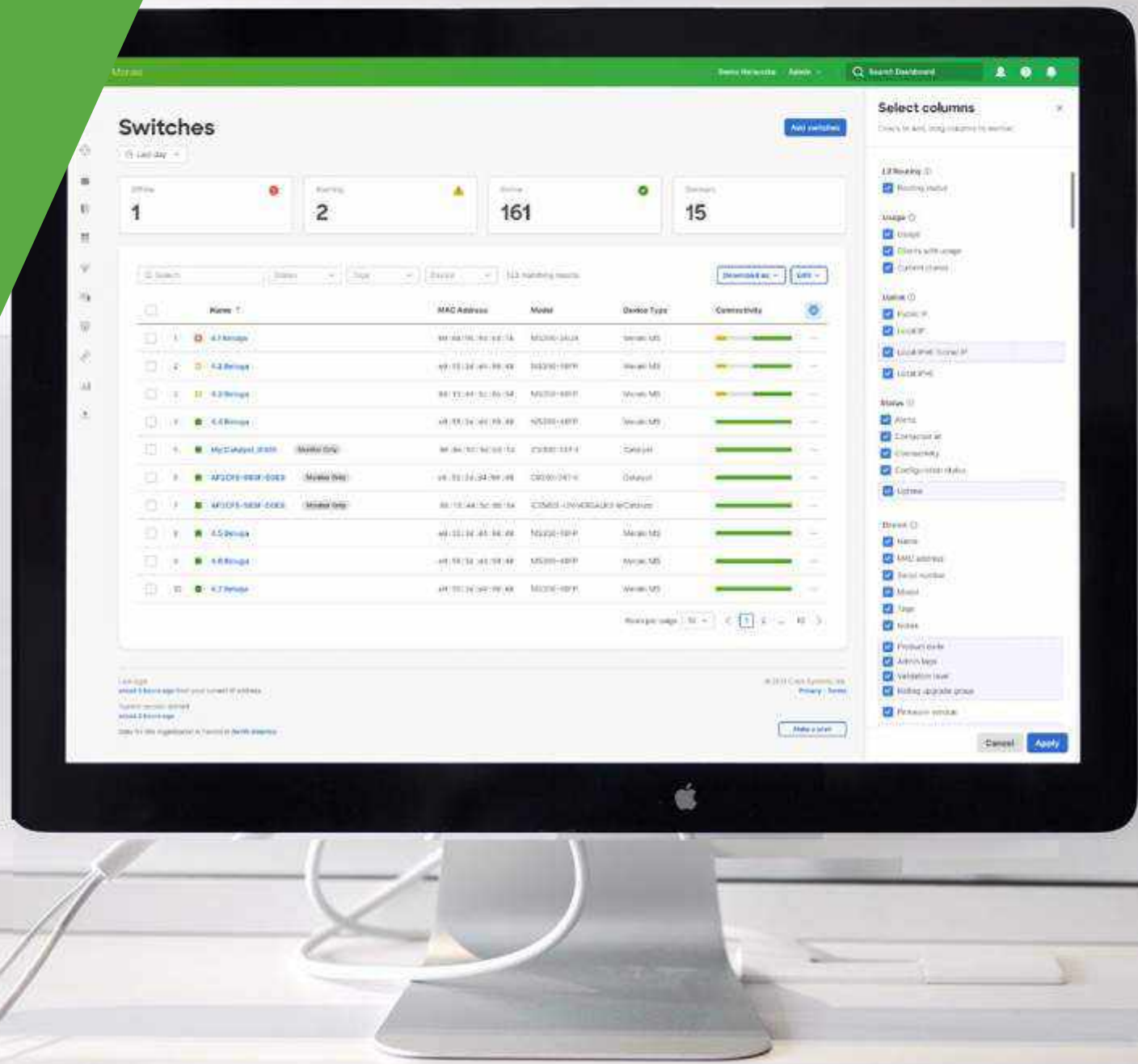
The next decade for Meraki Cloud

- Next Gen Cloud Architecture design
- 10x scale
- Global Expansion
- Higher performance
- Powering new Cisco product lines



Meraki dashboard, 그 혁신적인 변화

- 인텔리전스의 일상화
- 향상된 고객 경험
- 간편하고 일관적인 고객 인터페이스
- 향상된 성능
- 확장가능하고 능동적인 인사이트 제공



One Cisco



Cisco+ **Secure Connect**



TALOS ThousandEyes

Cisco Umbrella Cisco **Catalyst**

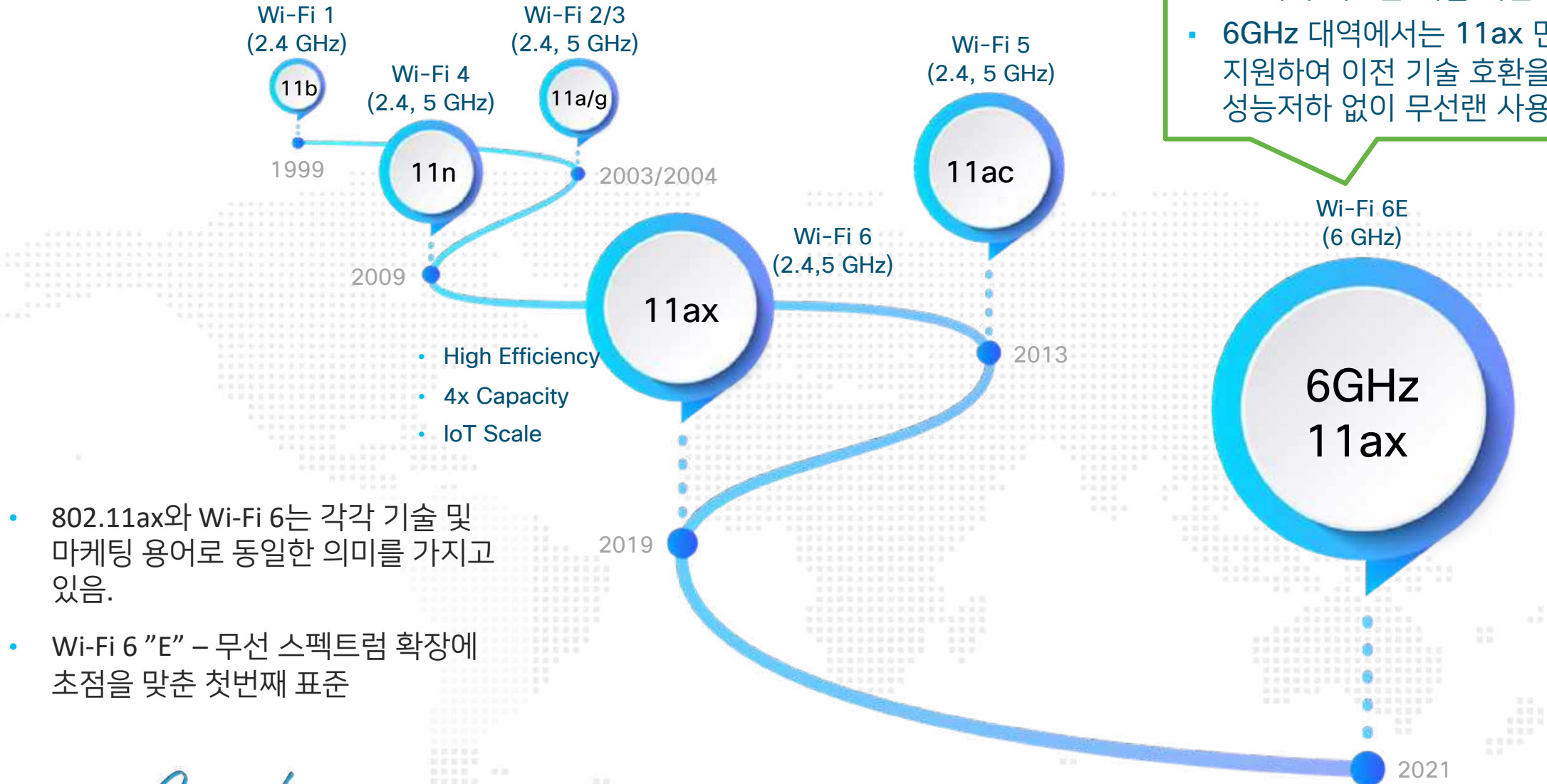


- Meraki dashboard is Cisco's Platform
- We are One Cisco sales team
- Demo Meraki to all customers

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco **IMPACT**

Wi-Fi 기술의 진화



- 802.11ax와 Wi-Fi 6는 각각 기술 및 마케팅 용어로 동일한 의미를 가지고 있음.
- Wi-Fi 6 "E" – 무선 스펙트럼 확장에 초점을 맞춘 첫번째 표준

Cisco Meraki Wi-Fi6E 플랫폼

1

완전히 새로운 무선랜 대역
6GHz(5925 to 7125MHz) - 한국 기준
기존 대비 2~3배 이상의 채널 수 지원

2

안전한 보안 통신
무선랜 사용을 위해 향상된 무선 구간
암호화(WPA3, OWE) 필수 사용 필요

3

청정 무선 환경
무선 간섭에서 Free한 무선 대역 지원으로
기존 Wi-Fi 밀집 환경에서도 성능 보장

4

보다 넓은 채널 지원
80MHz, 160MHz 등 와이드 채널 본딩 지원
기존 Wi-Fi6 대비 2배 속도* 지원

5

신규 단말 선별 지원
신규 Galaxy 폰 등 6E 지원 단말 only 지원
기존 저속 단말로 인한 무선성능저하 방지

6

기존 Wi-Fi 6 AP와 혼용 구성 지원
기존 Wi-Fi6와 같이 혼용 시 간섭없이 동작
고속 무선랜 필요 환경에 선별 구성 지원

Cisco Wireless 무선랜 (Wi-Fi6E)

동일한 하드웨어 플랫폼 - 2개의 관리 모드



Cisco Meraki WiFi6E 제품군

WiFi 6E

중소 규모 사업장에 적합한 효율성 제공 모델



CW9162I-MR

- 2x2(2.4GHz) + 2x2 (5GHz)+ 2x2(6GHz)
- 2.5 Gbps mGig
- 전원 옵션: PoE, DC Power
- IoT ready + Bluetooth 5.x
- USB - 4.5 W
- 범용 성능 AP



CW9164I-MR

- 2x2(2.4GHz) + 4x4 (5GHz)+ 4x4(6GHz)
- 2.5 Gbps mGig
- 전원 옵션 : PoE, DC Power
- IoT Ready + Bluetooth 5.x
- USB - 4.5 W
- 고성능 AP



CW9166I-MR

- 4x4(2.4GHz) + 4x4 (5GHz)+ 4x4(6GHz) 또는 4x4(2.4GHz) + 4x4 (5GHz)+ 4x4(5GHz) (XOR 5/6)
- 5 Gbps mGig
- 전원 공급: PoE, DC Power
- IoT ready + Bluetooth 5.x
- USB - 4.5W
- 초고성능 AP

중요 업무 수용을 위한
높은 가용성 제공 모델



MR57

- 4x4(2.4GHz) + 4x4 (5GHz)+ 4x4(6GHz) 또는 4x4(2.4GHz) + 4x4 (5GHz)+ 4x4(5GHz) (XOR 5/6)
- 5 Gbps mGig 이중화
- 전원 Failover 지원 *
- IoT ready + Bluetooth 5.x
- USB - 9W
- 초고성능 AP

*향후 지원 예정

30W PoE+에서도 모든 무선성능 제공(6 GHz @ LPI)

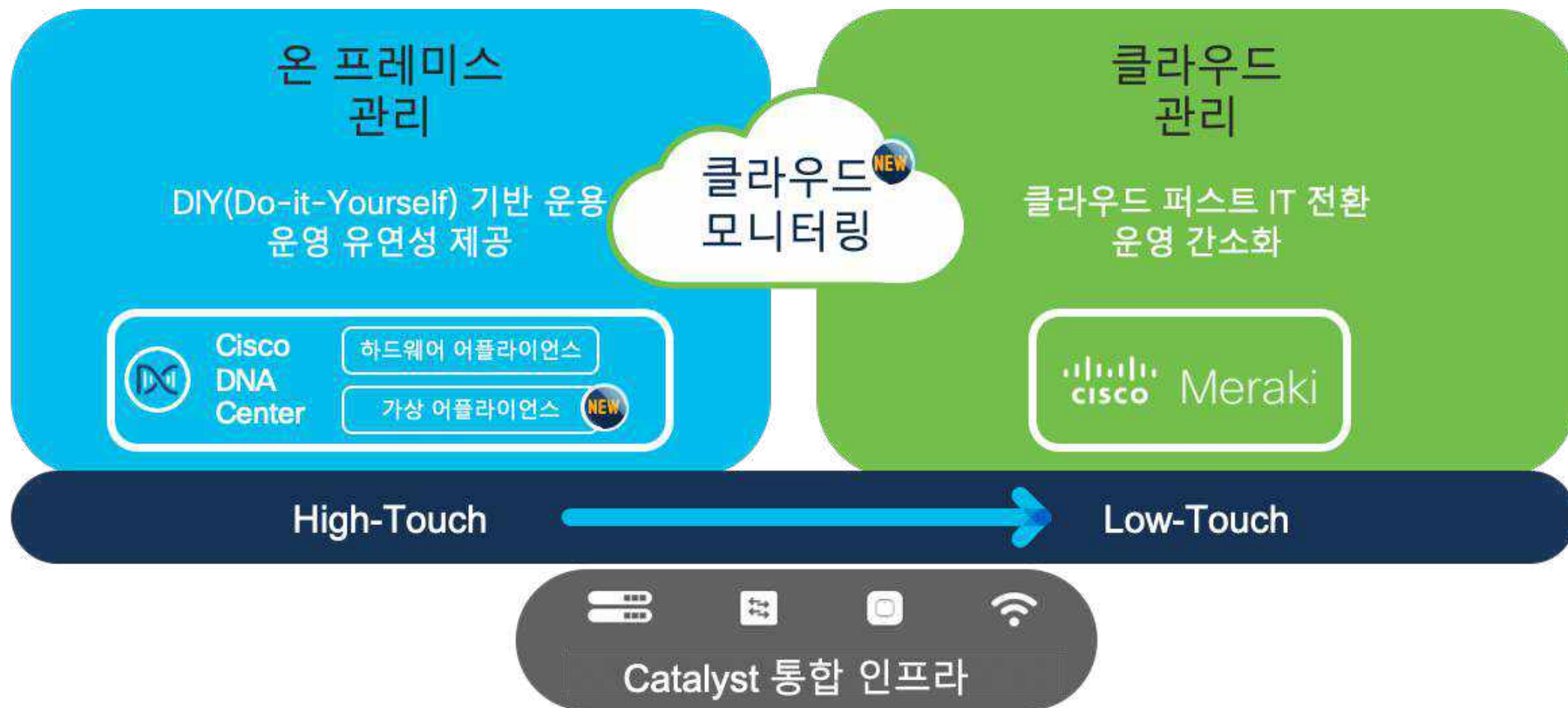
별도의 스캐닝 Radio

공용 브라켓 제공

WIDS/WIPS 기능(AirMarshal)

USB*

Catalyst 클라우드 모니터링으로의 확장



지원 제품 및 소프트웨어



지원 모델
Catalyst
9200/L/CX
9300/L/X
9500

소프트웨어
IOS-XE 17.3.1 ~
17.9.2

라이선스
DNA Advantage
DNA Essentials*

* DNA Essentials 라이선스 사용시 어플리케이션 및 사용량 정보는 지원되지 않음

Meraki MX 보안 제품군

SMALL BRANCH



MX64/W

Up to 50 users
250 Mbps FW throughput
Wi-Fi & PoE



MX67/68

Up to 50 users
600 Mbps FW throughput
Wi-Fi & PoE



MX67C/68CW

Up to 50 users
600 Mbps FW throughput
Wi-Fi & PoE
CAT 6 LTE modem



MX75

Up to 50 users
1 Gbps FW throughput
WAN PoE

VIRTUAL



Small

VPN THROUGHPUT

200 Mbps

Medium

500 Mbps

Large

1 Gbps

MEDIUM TO LARGE BRANCH



MX84

Up to 200 users
500 Mbps FW
throughput



MX85

Up to 250 users
1 Gbps FW
throughput



MX95

Up to 500 users
2 Gbps FW
throughput



MX100

Up to 500 users
750 Mbps FW
throughput



MX105

Up to 750 users
3 Gbps FW
throughput

CAMPUS OR CONCENTRATOR



MX250

Up to 2,000 users
4 Gbps FW
throughput



MX450

Up to 10,000 users
6 Gbps FW
throughput

Meraki 플랫폼 기반 솔루션 연동



CISCO 솔루션



Cisco Umbrella



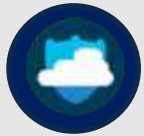
Cisco DNA Spaces



Cisco ISE



Cisco AnyConnect



Cisco AMP



Cisco SNORT IDS/IPS



Cisco Duo



Cisco Stealthwatch

MERAKI 솔루션



APIs + 에코파트너 솔루션

250+ Apps , 1,000+ 적용 사례

Hybrid Work

공용 데스크, 유동 사무실 관리 등

Smart Spaces

자산 추적, IoT센서 등

Safe Environments

접촉 추적, 안전한 인원 관리 등

Analytics

이동인구 분석 등

Marketing

게스트 Wi-Fi, 온라인 to 오프라인 등

+ 50 추가 카테고리

ThousandEyes 연동

Coming Soon



소형 지점



MX67/68



MX75

중대형 지점



MX85



MX95



MX105

본사 / DC



MX250



MX450

Cisco+ Secure Connect Now

Coming Soon

- 통합된 터키 기반으로 쉽고 빠르게 설정 가능한 SASE as-a-service 솔루션
- Meraki 플랫폼을 기반으로 한 직관적인 대시보드를 통해 손쉬운 운영 지원
- 통합 SASE 솔루션 제공으로 언제 어디서나 안전한 하이브리드 업무환경 지원
- Meraki/Viptela SD-WAN 기반 SASE 연동, SSE 기능 지원



USE CASE

스마트 업무 환경을 위한 필수 솔루션

MR, MV 및 MT 로 만드는 스마트 업무환경

CISCO *Connect*

MT 센서
환경 정보 모니터링



MR 무선랜 AP
위치 기반 서비스



MV
스마트 카메라
다양한 비디오 분석 기능



쉽고 간편한 운용 설계

Meraki MV 스마트 카메라

주요 차별화 기능

- 스마트 서치 및 공유 Tool 기반의 쉽고 빠른 이벤트 분석
- 모션 및 일정 기반 저장, 클라우드 저장 옵션을 이용한 영상 저장 최적화
- 세밀한 권한 제한을 통한 영상 접근 통제 및 영상 Audit 로그 제공으로 개인정보 보호
- 머신러닝 및 AI를 이용한 내장 분석 기능으로 단순한 감시 이상의 다양한 업무 활용 지원

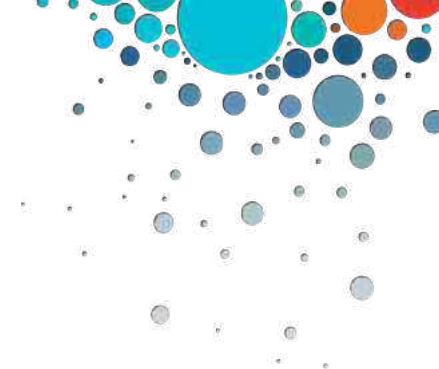


카메라 내장 스토리지 및 영상처리
기능으로 추가 인프라 구성 최소화 및
확장성 극대화

클라우드 기반 중앙집중 관리
및 모니터링을 통해
어디에서나 보안 검증을 통한
접속 가능

내장 무선 기능으로
설치 및 구성 단순화

MV 스마트 카메라 라인업



쉬운 설치	360° FISHEYE	다용도	다용도	더 많은 정보, 더 큰 스토리지 용량
 MV12 시리즈 Wide or narrow FoV 1080P video 128-256GB storage	 MV32 360° fisheye 8.4MP sensor 256GB storage	 MV22 시리즈 Varifocal lens Wide to narrow FoV Up to 4MP video 256-512GB storage	Outdoor  MV72 36-112° FoV 1080P video 256GB storage	Outdoor  MV72X 36-112° FoV 4MP video 512GB storage

모든 비즈니스 니즈에 부합하는 MT Sensor



MT10

온도 및 습도



MT11

온도 탐지 센서
(냉동 시설용)



MT12

누수 센서



NEW!

MT14

공기 청정도



MT20

도어 개폐 센서



NEW!

MT30

스마트 자동화 버튼



AA 건전지로
5년간 동작



Bluetooth® Low Energy



최대 5일간 센서 자체
정보 저장



다양한 알람 옵션 지원

메가존클라우드 Offering의 확장



SpaceONE
멀티 클라우드 관리를 하나로
SpaceONE

클라우드 자원 통합 관리
비용 분석 및 자원 최적화
장애 관리 및 알림 자동화
사용자 및 접근 권한 관리

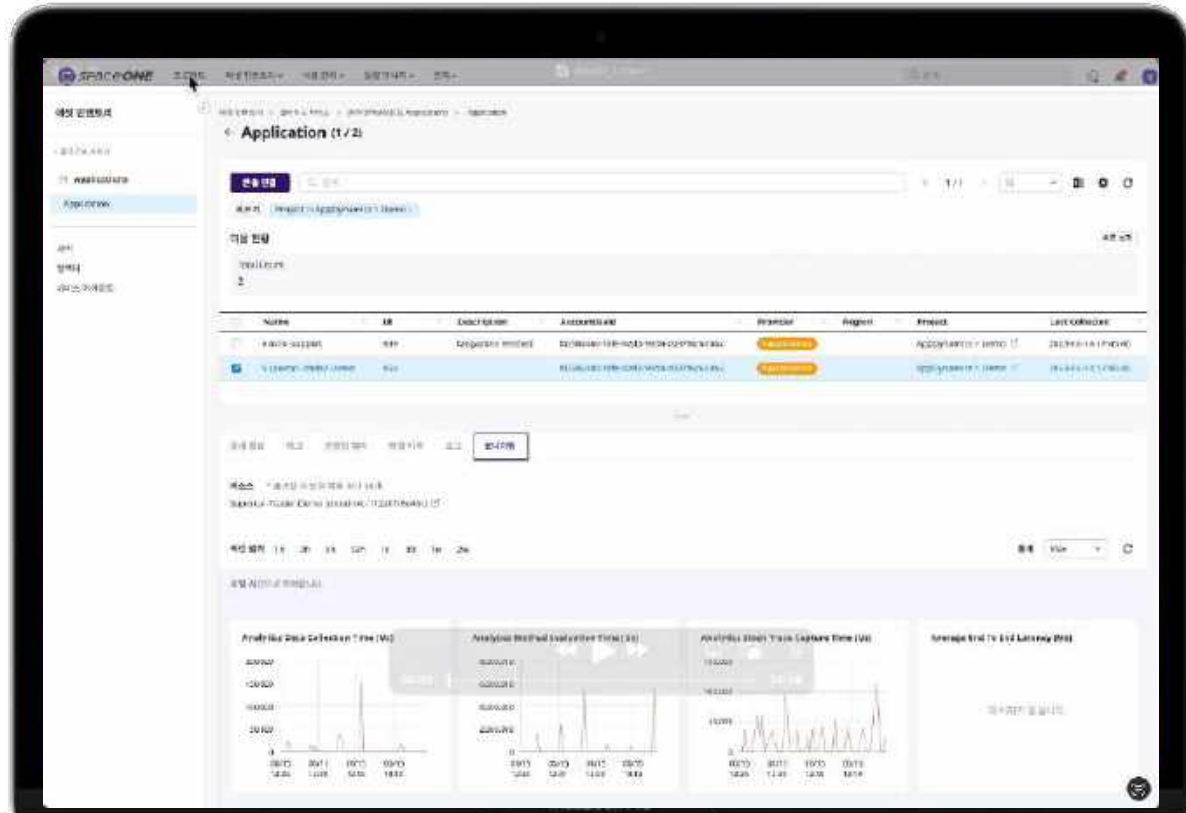
관리 중인 리소스 수: 600k+
연동된 클라우드 계정 수: 800+
지원 API 수: 500+

+ AppDynamics가 통합된 효율적 FSO 제공

CISCO *Connect*

Cisco AppDynamics Integration

- AppDynamics가 제공하는 통합 가시성(FSO)과의 강력한 결합
- Application과 Business의 상태를 명확하게 실시간으로 확인
- 메트릭, 스냅샷 관리 및 애널리틱스 이벤트 활용

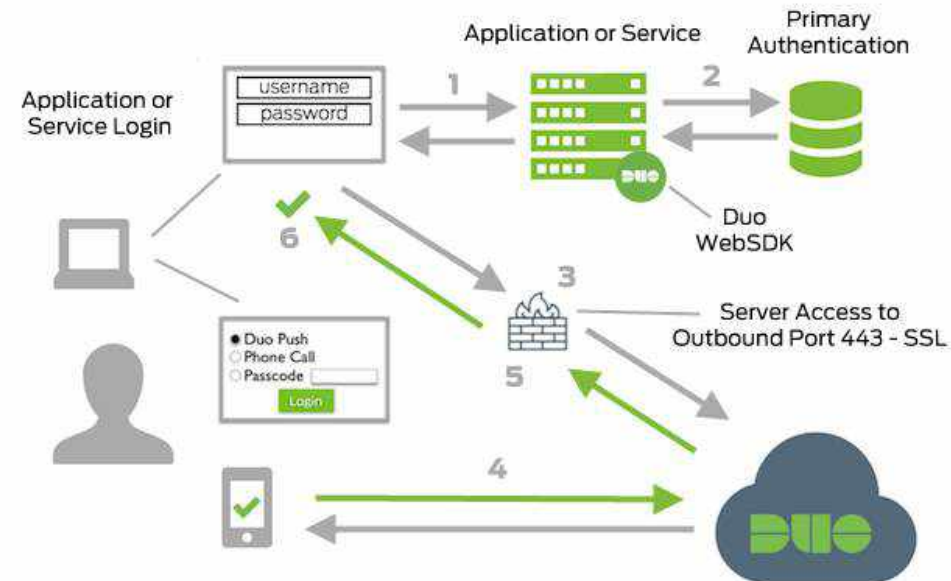


메가존클라우드 Offering의 확장



Duo Integration

- 강력한 Duo의 MFA 인증 기능을 통합하여 Megazone PoPs의 사용자 경험을 향상
- Duo Web SDK 연동으로 Duo의 MFA 및 Security Policy 통합 개발 중



Conclusion

✓ 메가존클라우드 Offerings

- All-in-One IT Managed Service인 F:it with **Meraki**
- 멀티클라우드 관리 플랫폼인 SpaceONE with **AppDynamics**
- SaaS 통합 관리 플랫폼 Megazone PoPs with **Duo**

✓ Meraki 5가지 주요 기술 특징점



신뢰성 있고 안전한
클라우드 관리구조 및
차세대 대시보드



AI/ML 기반
스마트한 무선랜
성능 관리



클라우드 모니터링
지속적 확장



보안 및 기타
Cisco 솔루션
연동 강화



지속가능한
환경을 고려한
장비 및 기능 지원



The bridge to possible

감사합니다.

CISCO *Connect*

#CiscoConnect

CISCO *Connect*

ALL IN

#CiscoConnect