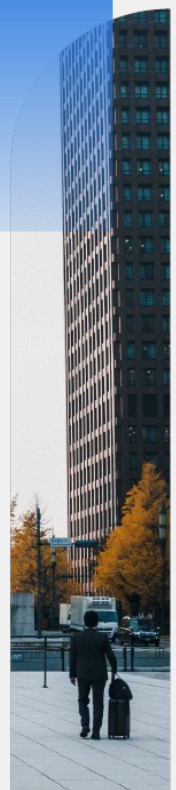
FORTINET

제로트러스트의 첫걸음, 무엇이 중요한가?

박현범 차장 / 포티넷 코리아
Systems Engineer

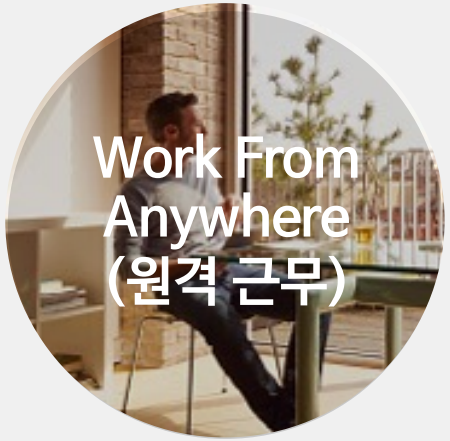


가속화되는 디지털포메이션

그 어느 때보다도 급증하고 있는 보안 리스크

Increase the Attack Surface

- 새로운 엣지 출현
- 새로운 어플리케이션 개발
- 새로운 에코시스템 적용



Remote Workers are a target for cybercriminals

- 가성비 위주의 보안 등급 낮은 라우터, IP 공유기 사용
- VPN 망 스플릿 기술 사용
- 새로운 원격 근무 환경 취약점에 대한 대응 기술과 보안 인식 부족

Higher Bandwidth Higher Risks

- 분산 아키텍처 (멀티 MEC)
- 사이버 공격 전파 속도 증가
- 보안 침해 사고 대응 속도 느려짐 (수동 작업)

Increased Risk

- 데이터 정합성
- 산업 규제와 컴플라이언스 준수 대상의 확대
- 데이터 프라이버시 보장 이슈

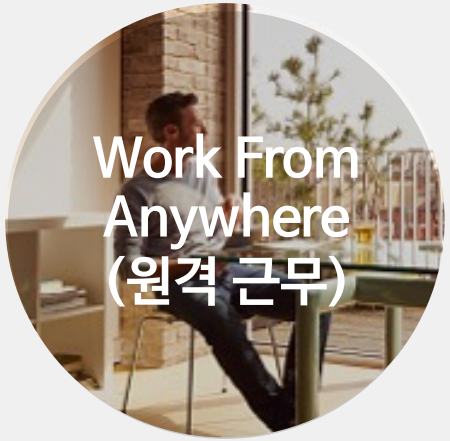
© Fortinet Inc. All Rights Reserved.

가속화되는 디지털포메이션

그 어느 때보다도 급증하고 있는 보안 리스크

Increase the Attack Surface

- 새로운 엣지 출현
- 새로운 어플리케이션 개발
- 새로운 에코시스템 적용



Remote Workers are a target for cybercriminals

- 가성비 위주의 보안 등급 낮은 라우터, IP 공유기 사용
- VPN 망 스플릿 기술 사용
- 새로운 원격 근무 환경 취약점에 대한 대응 기술과 보안 인식 부족

Higher Bandwidth Higher Risks

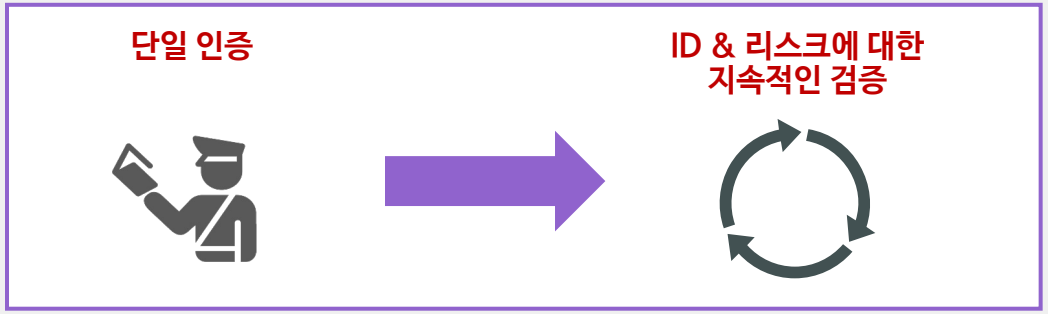
- 분산 아키텍처 (멀티 MEC)
- 사이버 공격 전파 속도 증가
- 보안 침해 사고 대응 속도 느려짐 (수동 작업)

Increased Risk

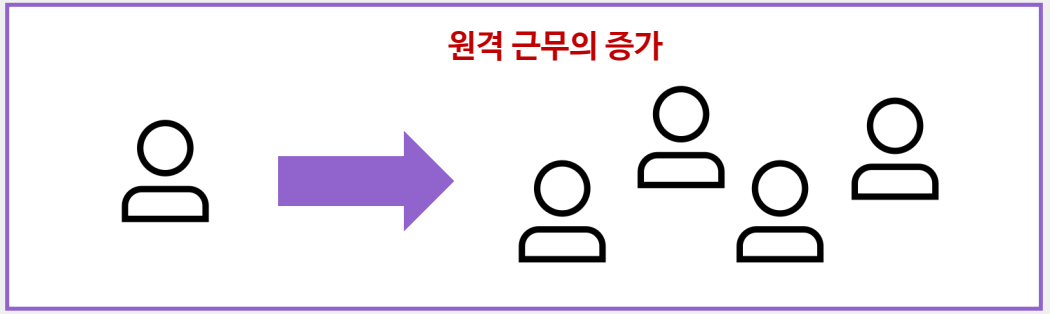
- 데이터 정합성
- 산업 규제와 컴플라이언스 준수 대상의 확대
- 데이터 프라이버시 보장 이슈

© Fortinet Inc. All Rights Reserved.

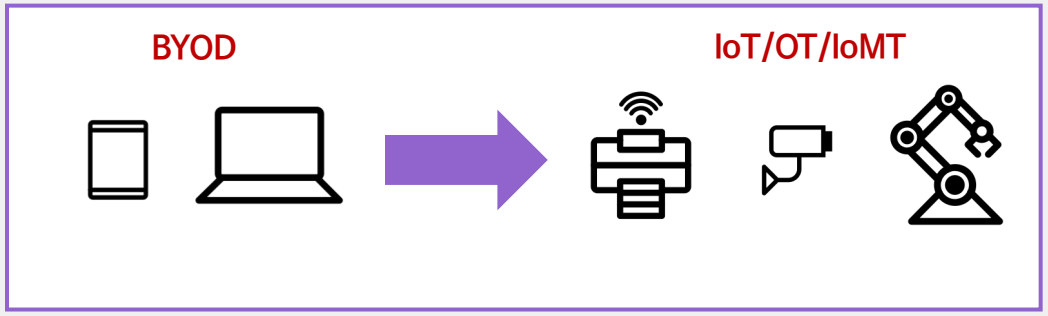
엔터프라이즈 액세스 동향



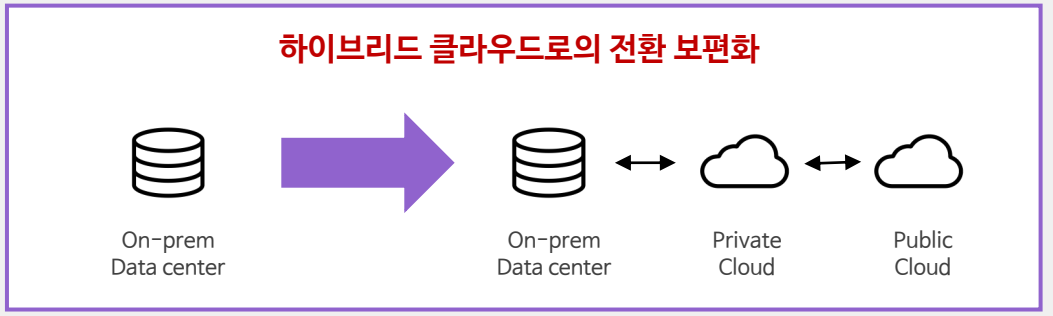
2024년까지 애플리케이션 액세스의 70%가 MFA를 사용(현재 10%)



2022년 말까지 4% 재택근무에서 30% 재택근무로 인력 전환



2025년에는 12B의 IoT 기기가 설치

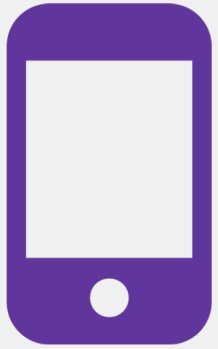


하이브리드 IT 사용이 Gartner 고객 사이에서 더욱 보편화되고 있음

1 Gartner Magic Quadrant for Access Management, 12 August 2019
2 Global Workplace Analytics
3 Gartner IoT Forecast
4 Gartner Magic Quadrant for Public Cloud Managed Services, 4 May 2020

© Fortinet Inc. All Rights Reserved.

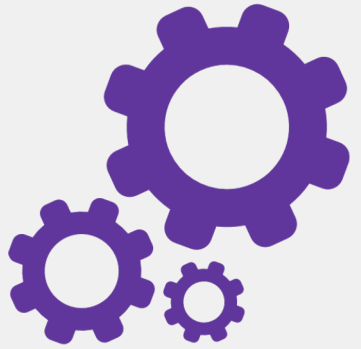
제로 트러스트 모델이 다시 주목받는 이유



사용자, 디바이스, 애플리케이션과 데이터가 기업의 경계와 통제 영역을 벗어나고 있음

디지털 혁신으로 견인되는 새로운 비즈니스 프로세스로 인해 공격에 대한 취약성도 증가

기업 보안 경계 내부로 정교한 표적 위협이 침투함에 따라 '신뢰하되 검증'하는 방식이 필수



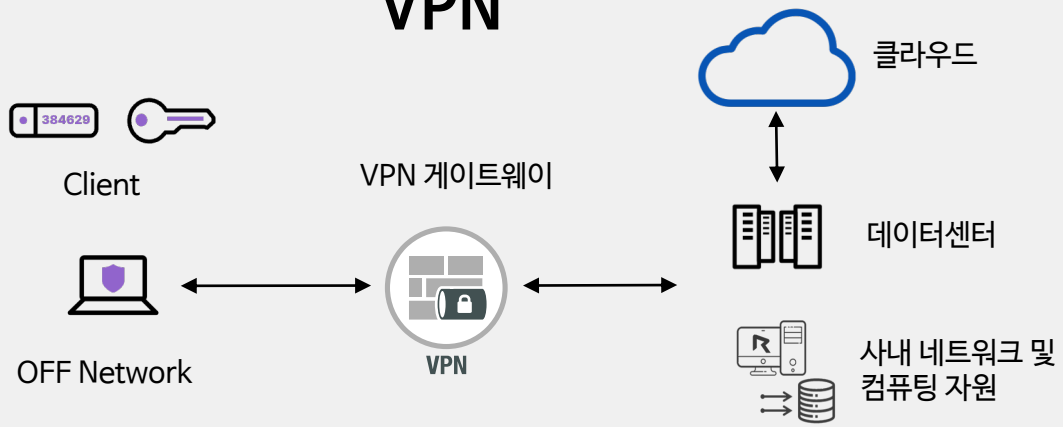
기존의 보안 경계는 복잡하고 리스크가 높으며 오늘날의 비즈니스 모델에 적합하지 않음

© Fortinet Inc. All Rights Reserved.

VPN에서 ZTNA로 변화되어야 하는 이유

VPN 대비 ZTNA 사용시 이점

VPN

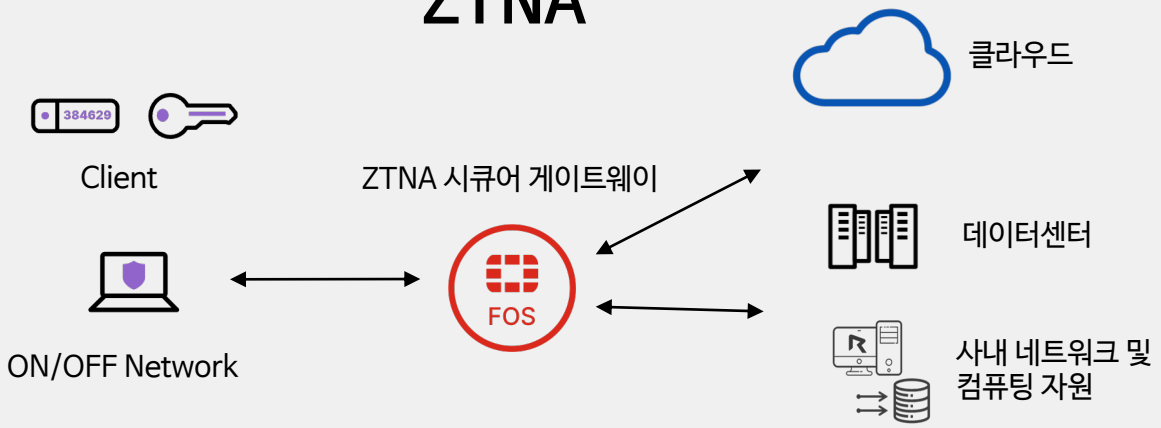


일회성 신뢰 확인

전체 네트워크 액세스

일반 정책 설정(허용/차단)

ZTNA



지속적인 신뢰 확인

특정 애플리케이션 액세스

사용자/단말기 상황 별 정책 설정

- VPN 설정이나 사용자 상호 작용이 없이 트래픽 보호를 위해 모든 세션을 암호화
- ZTNA 시큐어 게이트웨이(시큐리티 패브릭에 내장)
  - ✓ 세션당 상태 체크
  - ✓ 지속적인 상태 재점검 및 시행

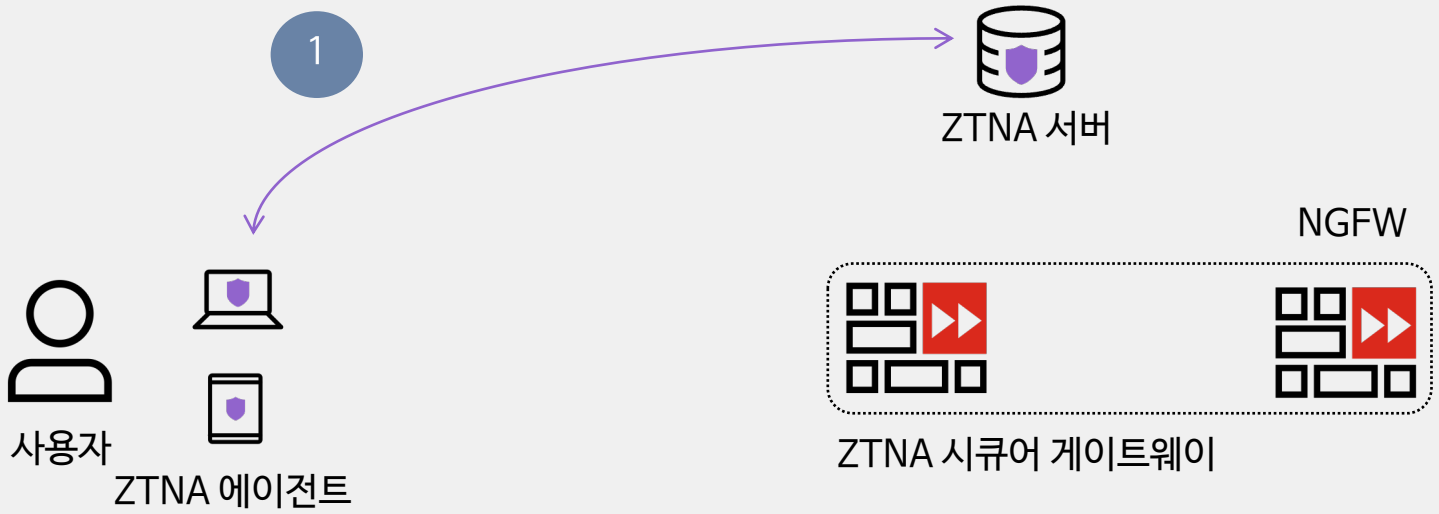
© Fortinet Inc. All Rights Reserved.

VPN에서 ZTNA로 변화되어야 하는 이유

ZTNA 텔레메트리

무엇을 할까요?

ZTNA 에이전트는 ZTNA 구성을 위해 ZTNA 서버에 연결
- ZTNA 터널을 어디로 연결할지
- 상태 확인을 위한 단말기 등록, 인증서 제공



클라우드
애플리케이션

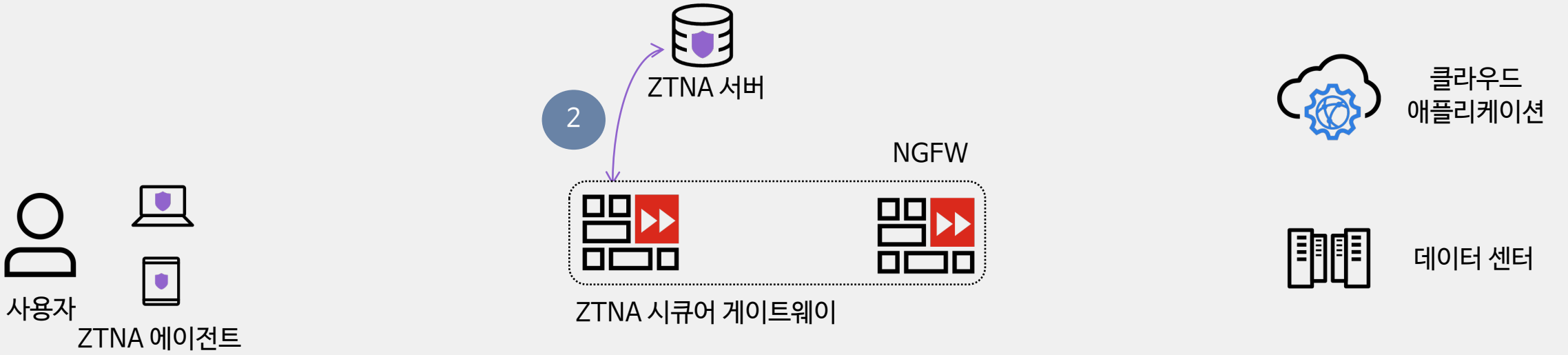
데이터 센터

사내 네트워크 및
컴퓨팅 자원

© Fortinet Inc. All Rights Reserved.

VPN에서 ZTNA로 변화되어야 하는 이유

정보 동기화(싱크)



무엇을 할까요?

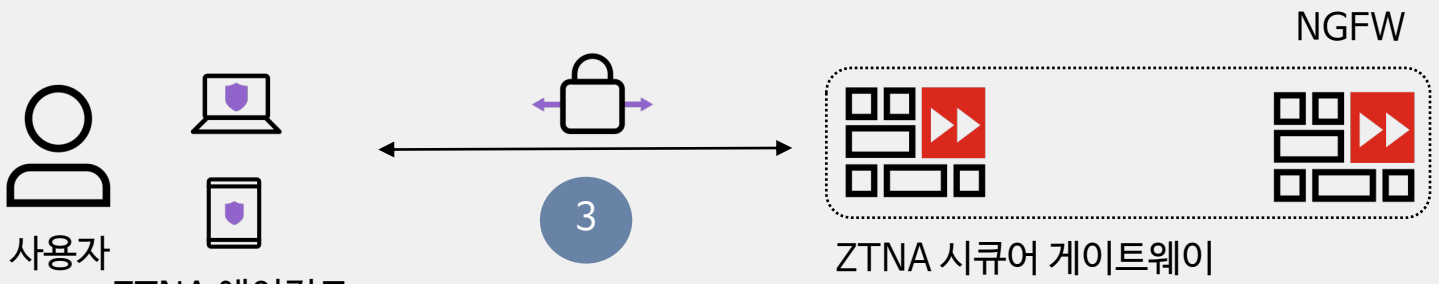
ZTNA 서버가 ZTNA 터널 수신을 위해 ZTNA 시큐어 게이트웨이와 연동

- 디바이스 ID 및 상태 확인을 위해 인증서 전달
- ZTNA 시큐어 게이트웨이에 ZTNA Tag를 추가

© Fortinet Inc. All Rights Reserved.

VPN에서 ZTNA로 변화되어야 하는 이유

터널 및 디바이스 상태 확인 : 인증 강화를 위해 OTP 등 MFA 인증



무엇을 할까요?

사용자가 앱을 실행하면 ZTNA 에이전트가 자동으로 ZTNA 시큐어 게이트웨이에 연결

클라우드 애플리케이션

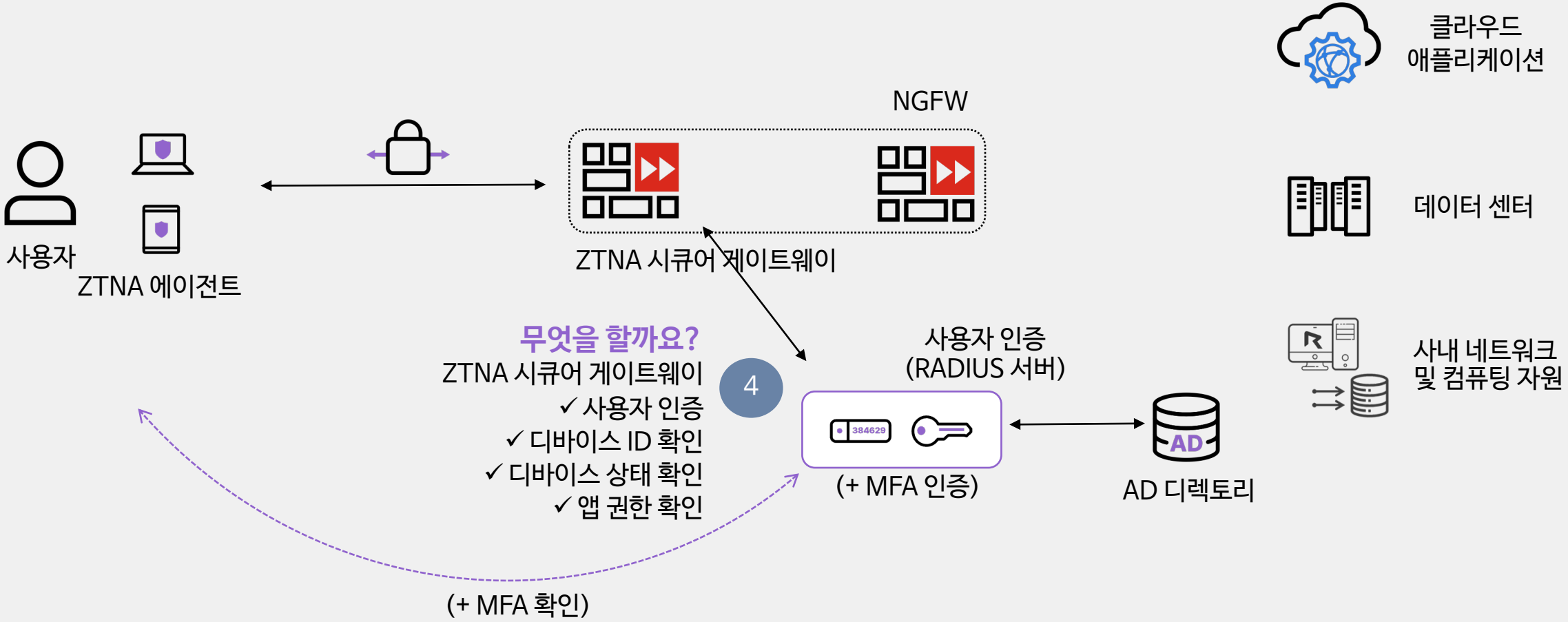
데이터 센터

사내 네트워크 및 컴퓨팅 자원

© Fortinet Inc. All Rights Reserved.

VPN에서 ZTNA로 변화되어야 하는 이유

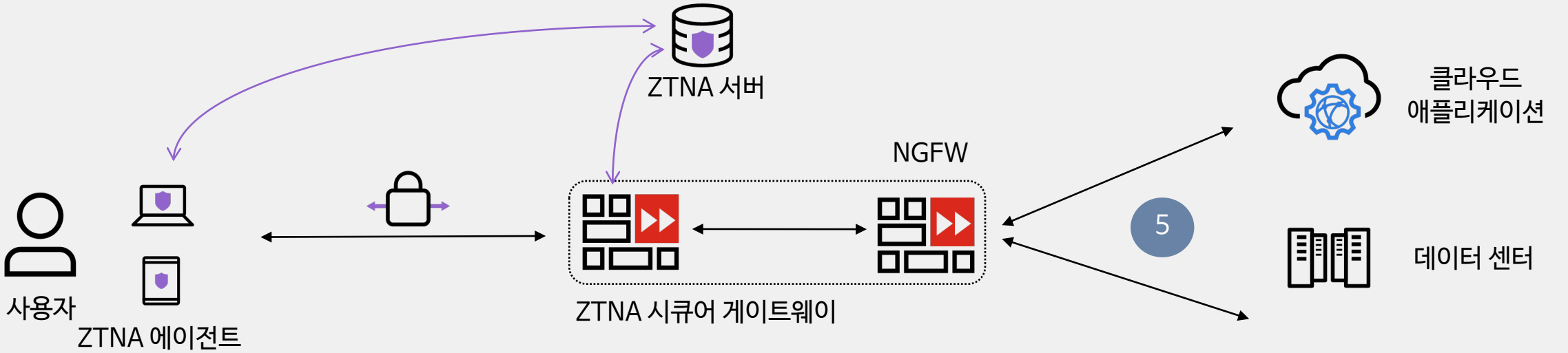
터널 및 디바이스 상태 확인 : 인증 강화를 위해 OTP 등 MFA 인증



© Fortinet Inc. All Rights Reserved.

VPN에서 ZTNA로 변화되어야 하는 이유

애플리케이션 인지 및 제어 정책 적용



무엇을 할까요?

ZTNA 게이트웨이가 애플리케이션에 연결되어 해당 서비스가
어디에 있든 사용자는 세션에 액세스 가능
- 지속적인 단말기 상태 확인
- ZTNA 시큐어 게이트웨이에 정보 업데이트

© Fortinet Inc. All Rights Reserved.

잠깐! 여기서 우리가 놓치고 있는것은 무엇일까?

APT 제품을 우회하는 공격자들


어나니머스

라자루스


샤오치잉

킬넷

탈취된
정상 사용자의 계정

시스템의 내장된
정상 프로그램 사용

누구나 알 수 있는
알려진 취약점 활용

합법적인
침투 테스트 도구 사용

제로 트러스트, 요약해보면?

보안기술이나 제품이 아닌
보안모델링을 하기 위한
규칙/원칙일 뿐

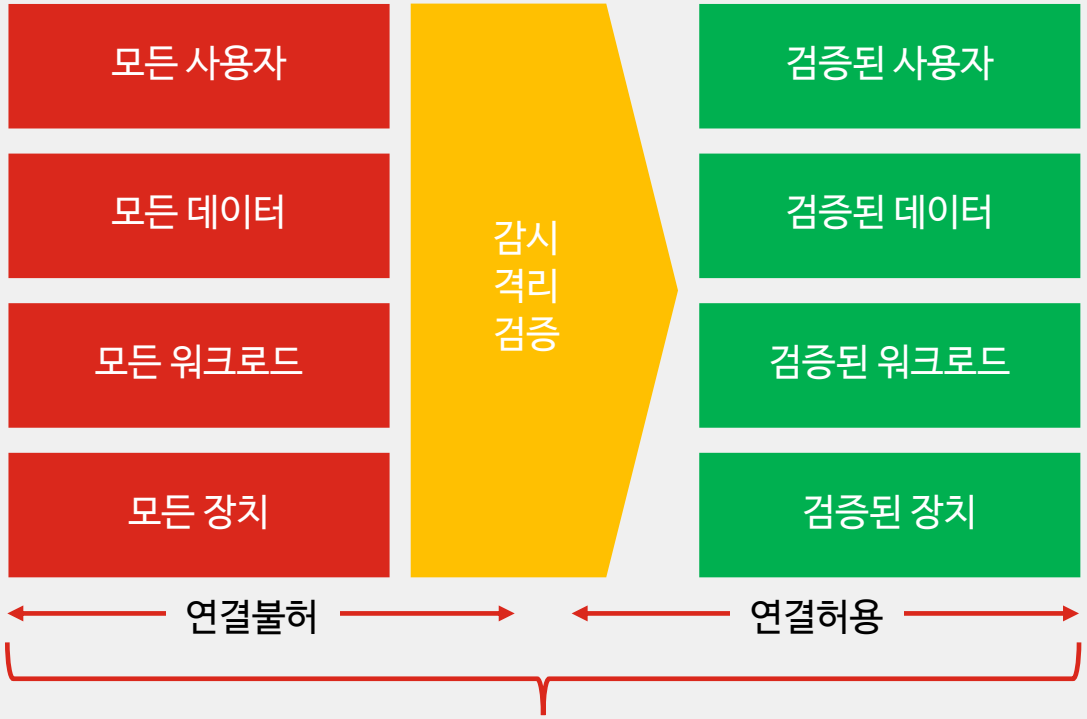
내부 통제에 집중하기 전에
먼저 해야 할 일이 있다

먼저 해야 할 일, **무엇**일까?

© Fortinet Inc. All Rights Reserved.

제로 트러스트 개념 다시 잡기 (1/3)

제로 트러스트 개념



신뢰성이 확인된 컴포넌트만 연결을 허용하여 보안성 강화

제로 트러스트 적용 절차

단계	적용절차	세부방안
1단계	악성 데이터 확인/분류	• 악성데이터 〉 제거 • 유해데이터 〉 검사
2단계	악성 트래픽 경로 파악	• 네트워크 엣지 파악 • URI 기반 경로 파악
3단계	제로 트러스트 설계	• 네트워크 세그먼테이션 • 클라우드/SDN 기반 가상화
4단계	지능형 정책 생성	• 워크플로우 자동화 • 보안 실행 최적화
5단계	제로 트러스트 모니터링	• 모든 변경항목 검증 • Any/Any 정책 제거

Source: John Kindervag (forrester research), “5 Steps to a Zero Trust Network”, 2015.3

© Fortinet Inc. All Rights Reserved.

제로 트러스트 개념 다시 잡기 (2/3)

제로 트러스트 기술요소

구분	기술요소	구현 방안
데이터 격리 측면	CDR	• 오브젝트 파싱/비정상 구조 제거 • 스크립트 추출, 리어셈블링
	웹/이메일 랜더링	• 웹/이메일 화면 랜더링 • 컨텐츠 격리 공간 실행
트래픽 감시 측면	EDR	• 이벤트 감시, 휴리스틱 적용 • 분석, 조사, 조치 3단계 적용
	In-band Network	• 패킷헤더 구조화 • Leaf-spine 아키텍처
신뢰성 검증 측면	OTP	• Challenge-Response • Time/Event-Synchronous
	FIDO	• FIDO 1.0; 토큰/공개키 • FIDO 2.0; 외부인증

제로 트러스트 VS 일반 네트워크

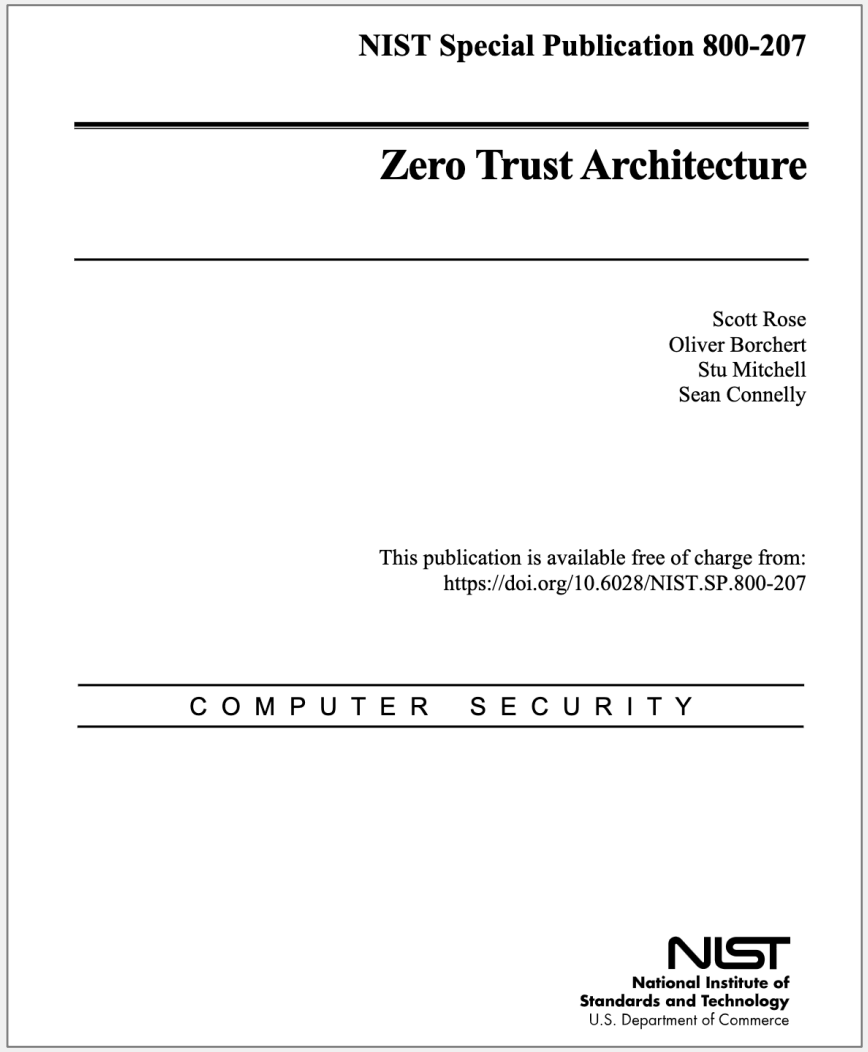
비교항목	제로 트러스트	일반 네트워크
신뢰성 부여 기준	신뢰성 검증 여부	네트워크 위치
보안 정책	적응형 보안 정책	보안장비 정의된 정책
보호 대상	모든 컴포넌트	장치와 데이터

내/외부 관계없이 모든 사용자나 시스템의 연결에 대해 검증 후 신뢰하는 네트워크 보안 모델

Source: John Kindervag (forrester research), “5 Steps to a Zero Trust Network”, 2015.3

© Fortinet Inc. All Rights Reserved.

제로 트러스트 개념 다시 잡기 (3/3)



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- 모든 데이터 소스와 컴퓨팅 서비스는 리소스 이다
- 모든 통신은 위치나 장소에 관계없이 안전해야 한다
- 개별 리소스에 대한 접근은 세션단위로 허용한다
- 리소스에 대한 접근은 동적인 정책에 의해 결정된다
- 소유 자산과 관련된 모든 보안상태를 모니터링한다
- 접근이 허용되기 전에 인증과 인가가 실행되야 한다
- 자산의 네트워킹은 보안상태 개선을 위해 수집한다

Source: CSA - NIST - SP 800-207

© Fortinet Inc. All Rights Reserved.

제로 트러스트의 첫걸음 → Discover

FORTINET

Zero Trust Access Consulting Services

Service Overview

To stay ahead of a rapidly evolving threat landscape, organizations must adopt security architecture and operations that enable a comprehensive and measured approach to cybersecurity. Fortinet offers Zero Trust Access Consulting Services to partner with business leaders, helping organizations be at their best through this ever-changing environment.

Fortinet experts discover existing security posture elements through a vendor-agnostic approach, align findings to business goals, strategic objectives, and compliance requirements, and guide existing projects and future planning toward framework maturity. These collective tasks and outcomes empower organizations to achieve a holistic security architecture resilient enough to withstand continuous change in the threat landscape.

Advisory Team Proficiency

- ✓ Dedicated access to experienced professionals who possess decades of industry security experience and direct connection to additional experts inside Fortinet
- ✓ Our team can provide customers with Zero Trust Access advisory services during the entire lifecycle of their projects
- ✓ Best-in-class methodologies and framework alignment with studied application from our existing customer base

Domains

- Network Access Control (NAC)
- OT / IOT Device Profiling
- Identity & Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Endpoint Posture
- Dynamic Access
- BYOD
- Device Discovery

Simple and Flexible Engagement

Per-day remote service (FP-10-SA001)

- **Discover** network attached devices across the network
- **Align** existing systems and processes to security) and business goals
- **Guide** templated or customized reference security architectures

Deliverables:

- ✓ **Network Device Inventory report**
- ✓ **Best practices recommendations**
- ✓ **Access Control policy review**
- ✓ **Zero Trust Access reference architecture**
- ✓ **Implementation guidance**

Key Business Outcomes

Design & Architecture: Zero Trust Acess Architecture based on best practices. Tailored for customer's business goals

- End to end consistent user & endpoint secure access
- Architectures designed be resilient and to meet business goals

Minimize Attack Surface: Review of existing endpoint access policies to ensure the exposed attack surface is as minimal as possible.

- Secure access strategy and policy review
- Endpoint discovery and inventory
- Assess hygiene and posture

Security Framework Integration: Working with existing security framework to best leverage all threat intelligence.

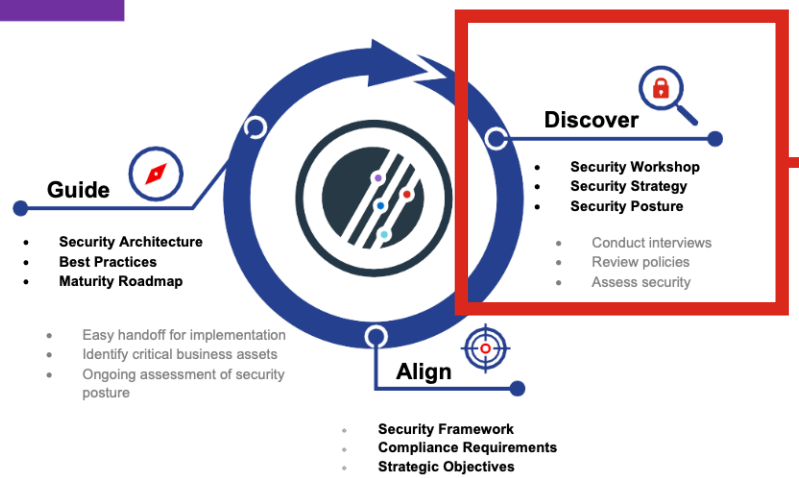
- Security Fabric integration at all levels possible
- Integrated & actionable threat intelligence

Why Fortinet?

Fortinet is the #1 global cybersecurity company, with more than 20 years of experience in protecting assets, detecting malicious actors, mitigating threats, and leading the way on industry evolution.

Fortinet delivers the Security Fabric, a broad, integrated, and automated cybersecurity framework that weaves together all facets of operational and functional security.

FortiGuard Labs Global Threat Research and Response organization leverages tested artificial intelligence and machine learning technologies to remain on the cutting edge of threat intelligence.



보호해야 될 대상
즉, 내/외부 자산 정의

현재 적용되어 있는
규정과 보안규칙 점검

© Fortinet Inc. All Rights Reserved.

Discover Assets 재정의

현재 우리가 집중하는 자산 범위는?

원격 위치에서 회사 인프라에 접근 가능한
개인 PC / 인증에만 집중

제로 트러스트를 위한 자산 범위는?

웹 서버

데이터베이스

가상머신

컨테이너

산업용 IoT

쉐도우 장치

외부자 관점에서
데이터를 가진 모든 자산으로 확대 필요

© Fortinet Inc. All Rights Reserved.

그래서 우리는 ASM에 주목한다!

CAASM

Gartner ‘enables organizations to see all assets (internal and external) through API integrations with existing tools, query against the consolidated data, identify the scope of vulnerabilities and gaps in security controls, and remediate issues.’

The advantage of this approach is that it leverages the assets you already have.

- 조직의 기존 도구를 API 통한 통합 자산 관리
- 내외부의 자산을 식별하여 사이버 관계도 매핑
- 보안이슈를 탐지하고 직접적으로 조치 실행

〉〉 이미 알고 있는 자산을 기반으로 하는 접근의 장점

〉〉 보안이슈 발견 후, 직접 해결 가능한 기능 필요

EASM

A way to discover and document external-facing assets that may be potential breach-points into an organization’s network.

Specifically, EASM helps organizations gain more visibility into the applications, cloud services, and systems that are visible in the public domain - which therefore may also be visible to an attacker.

- 조직의 외부, 인터넷에 연결된 자산에 중점
- 특히 퍼블릭 클라우드와 퍼블릭 도메인에 효과적
- 때때로 ASM과 EASM를 동일한 의미로 사용

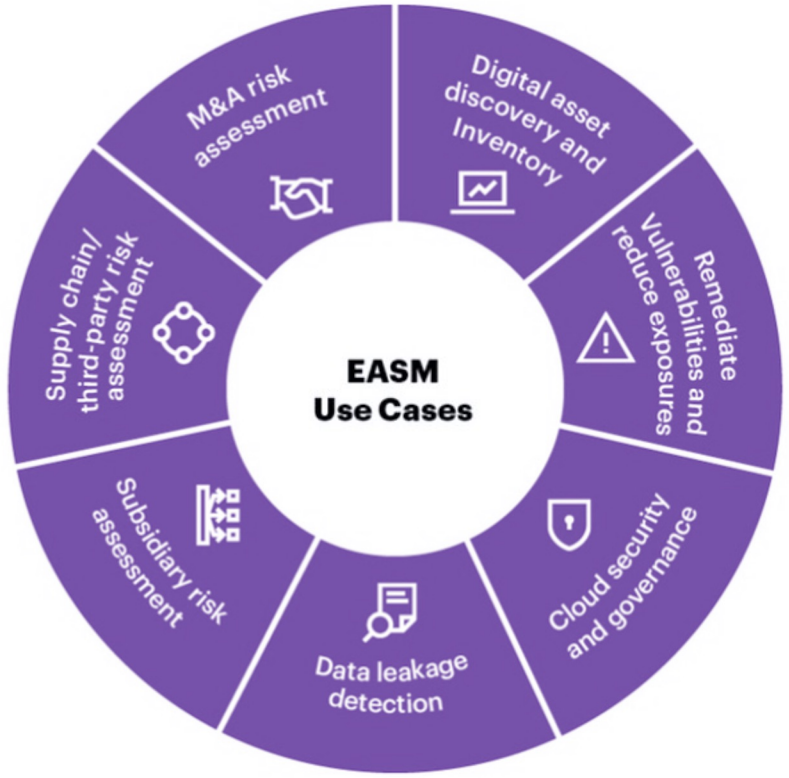
〉〉 공격자의 시선으로, 외부에서 내조직을 바라보는 방식

〉〉 인텔리전스와 함께 적용시, 우선순위 선정 효과적

© Fortinet Inc. All Rights Reserved.

CAASM 〈 EASM, 우선순위가 높은 이유는?

Common Use Cases for External Attack Surface Management



Source: Gartner
737807_C

EASM 기대 효과

- 클라우드, 엔드포인트 등 엄청난 양의 취약성이 확장됨에 따라 취약성 관리 프로그램의 한계점 확인

  (※SW취약점은 공격자가 악용할 수 있는 벡터 중 하나일 뿐)

- 공격 가능성의 우선순위를 정하고, 패치 대상과 위치, 로깅 및 모니터링을 추가할 위치, 자산 삭제/이관 등 의사결정 도움
- 보안사고 대응에 대한 전술, 기술 및 절차를 갖추어 기본적으로 보안사고가 발생하지 않도록 미연에 방지

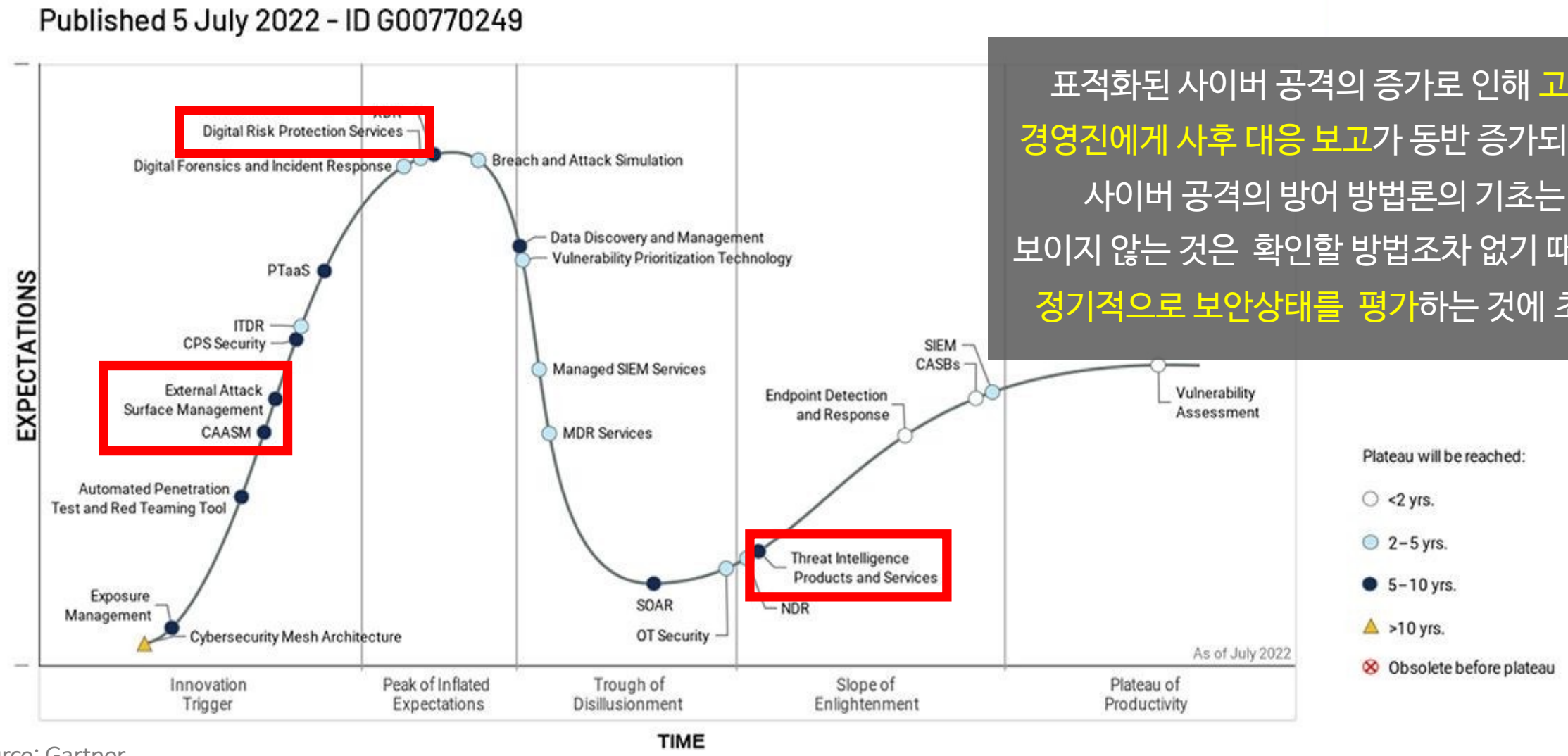
보안적용은 큰범위 → 작은범위 순차적용

즉, 외부 → 내부로 보안홀을 점진적으로 줄여가는 방식의 Management 선호

Source: Gartner

© Fortinet Inc. All Rights Reserved.

그런데 왜 이제 ASM? 과거의 기술 아닌가?



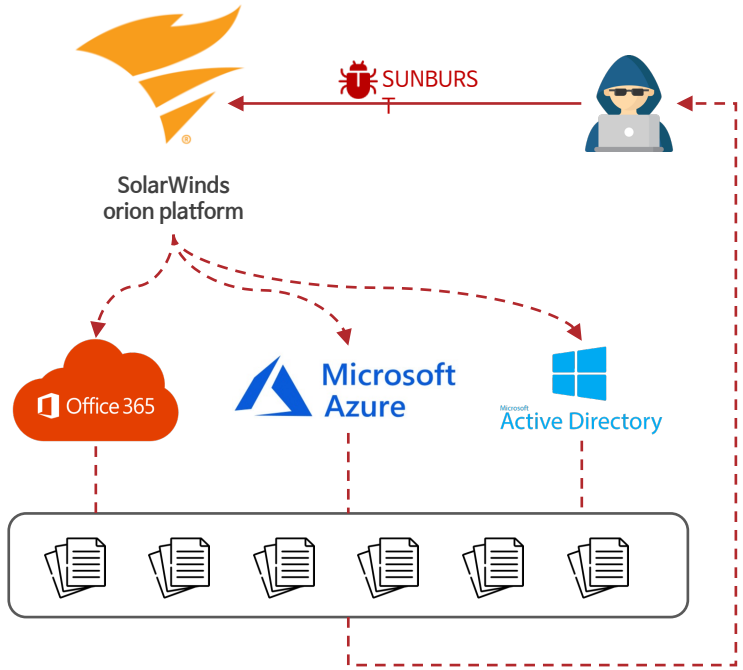
표적화된 사이버 공격의 증가로 인해 고위 경영진에게 사후 대응 보고가 동반 증가되었고, 사이버 공격의 방어 방법론의 기초는 보이지 않는 것은 확인할 방법조차 없기 때문에 정기적으로 보안상태를 평가하는 것에 초점

Source: Gartner

© Fortinet Inc. All Rights Reserved.

ASM이 트랜디해진 이유, 멀리갈 필요가 없다

Solawinds



암시적으로 안전하다는 가정하에
종종 간과되는 공급망 공격

Colonial pipeline

RDP 프로토콜을 통해
정보유출 및 랜섬웨어 감염

공격자는 알려지지 않거나
중요하지 않은것으로 간주되는
경로를 선택

》 등잔 밑이 어둡다는 뜻

© Fortinet Inc. All Rights Reserved.

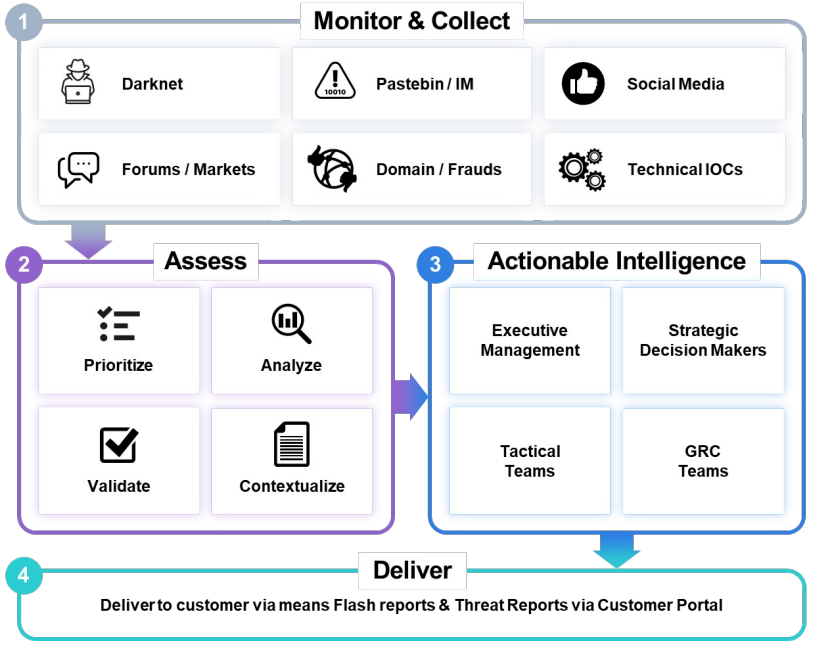
ASM을 포함한 DRPS 솔루션 – FortiRecon

➢ 증가하는 위협 환경에서 보안을 강화하기 위한 차세대 인텔리전스 서비스

FortiRecon Overview

External Attack Surface Management (EASM)

Brand Protection (BP)

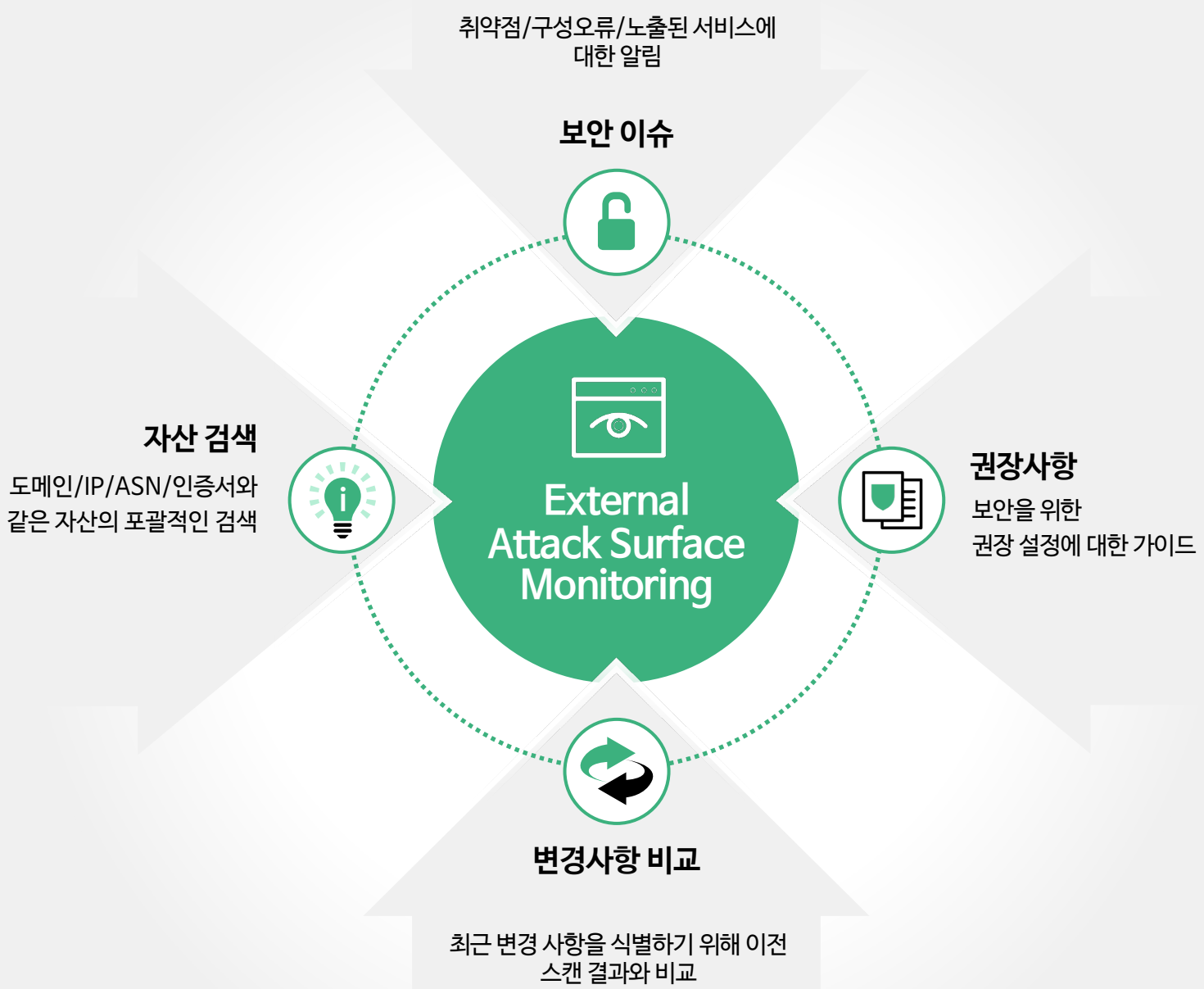


Adversary Centric Intelligence (ACI)

© Fortinet Inc. All Rights Reserved.

포티리콘 EASM은?

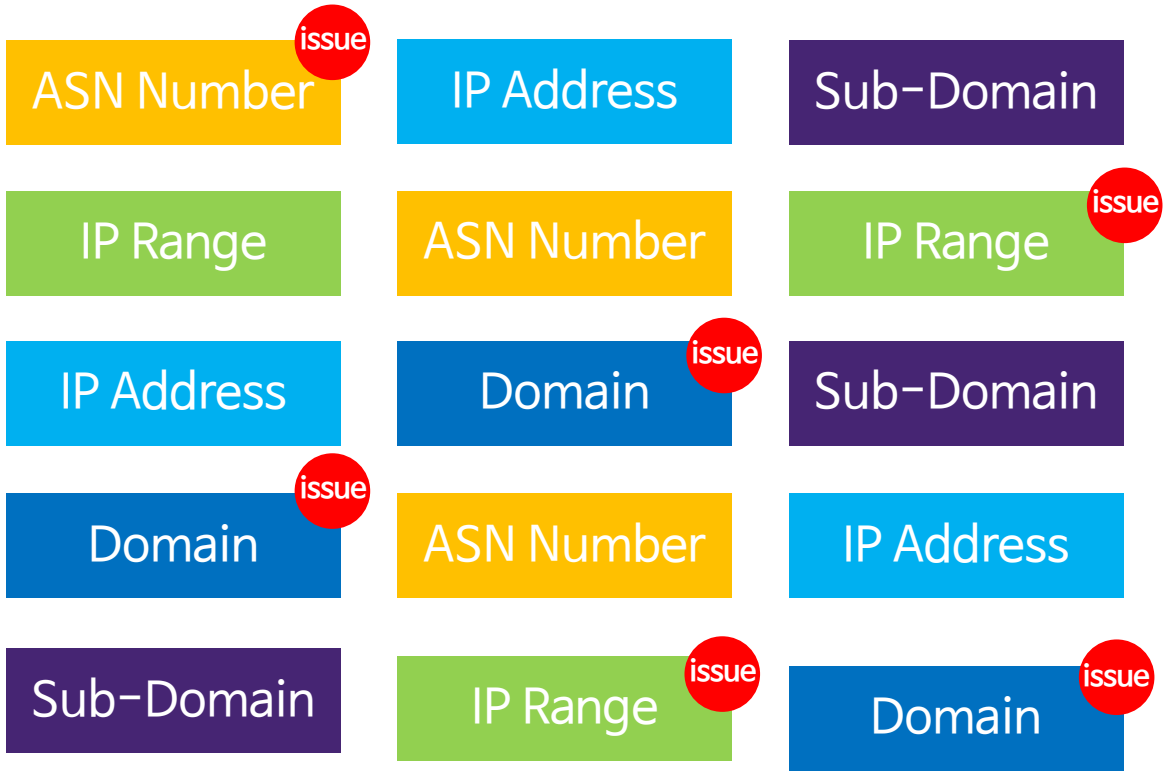
FortiRecon EASM (External Attack Surface Management)은 조직 및 자회사에 대한 외부 외부 보기를 제공하여 노출된 알려진 기업 자산과 알려지지 않은 기업 자산 및 관련 취약성을 식별하여 가장 중요한 문제 해결의 우선 순위를 정하는 데 도움이 됩니다. EASM은 악의적인 행위자가 악용할 수 있는 서버, 자격 증명, 퍼블릭 클라우드 서비스 구성 오류 및 타사 파트너 소프트웨어 코드 취약성을 식별하는데 도움이 됩니다.



© Fortinet Inc. All Rights Reserved.

포티넷 EASM 동작방식

➢ 모니터링 자산등록(Asset Discovery)



➢ 보안 이슈 탐지(Security Issues)

심각성 기준으로 분류 가능

CRITICAL HIGH MEDIUM LOW

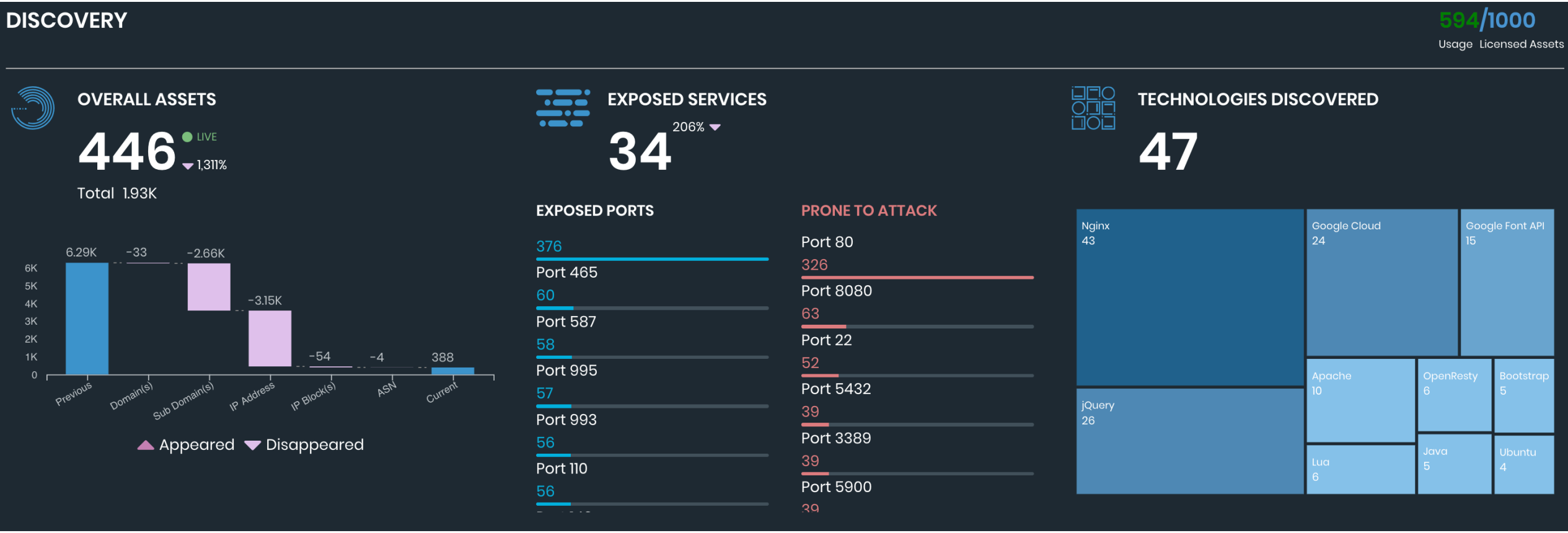
[MIS-CONFIG] [CREDENTIAL]

[VULNERABILITIES] [SERVICES]

[EXPOSED PORT] [PRONE TO ATTACK]

© Fortinet Inc. All Rights Reserved.

포티넷 EASM 활용 사례 1



- 전체 자산의 증감 추이 제공
- 발견된 자산/서비스 정보 제공
- 발견된 기술 정보 제공
  (서비스 구성에 사용된 어플리케이션)

➢ Discovery Assets 전반적인 가시성 제공

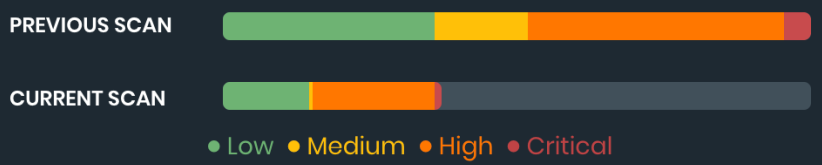
© Fortinet Inc. All Rights Reserved.

포티넷 EASM 활용 사례 2

ISSUES

TOTAL ISSUES

2.41K 169%



SEVERE ISSUES

22

ISSUE NAME	ASSETS	SEVERITY
Exposed Elastic Search Service ...	29	Critical
Exposed VNC Service	26	Critical
Exposed PostgreSQL Service	18	Critical
Exposed Mongo DB Service	1	Critical
Exposed SSH Service	1269	High

WIDELY EXPLOITED VULNERABILITIES

04

ISSUE NAME	ASSETS	SEVERITY
Mis-configured .git/.svn expose...	1	Critical
CVE-2022-0001	1	High
CVE-2022-0002	1	High
CVE-2022-0003	1	High

- 노출된 서비스 정보
- 노출된 서비스 포트
- 평판시스템에서 감지된 자산
- 보안이슈의 증감 추이
- 안전하지 않은 어플리케이션 구성
- CVE 취약점이 발견된 자산
- 현재/과거 스캐닝 결과 비교

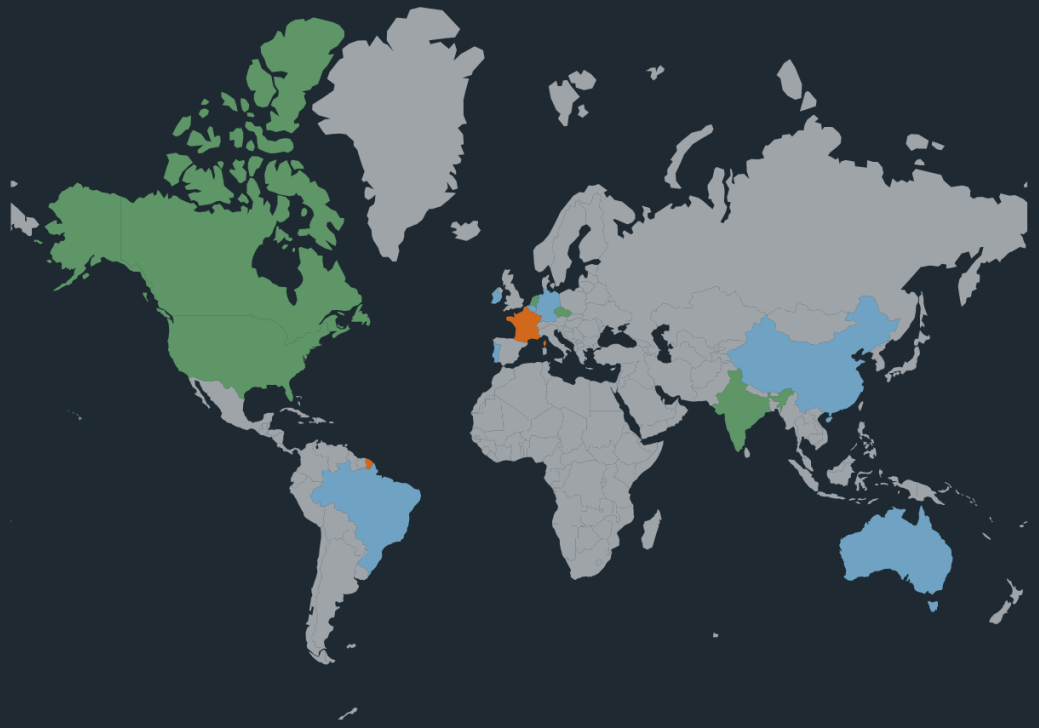
© Fortinet Inc. All Rights Reserved.

포티넷 EASM 활용 사례 3

ASSET DISTRIBUTION

ASSET LOCATIONS

14

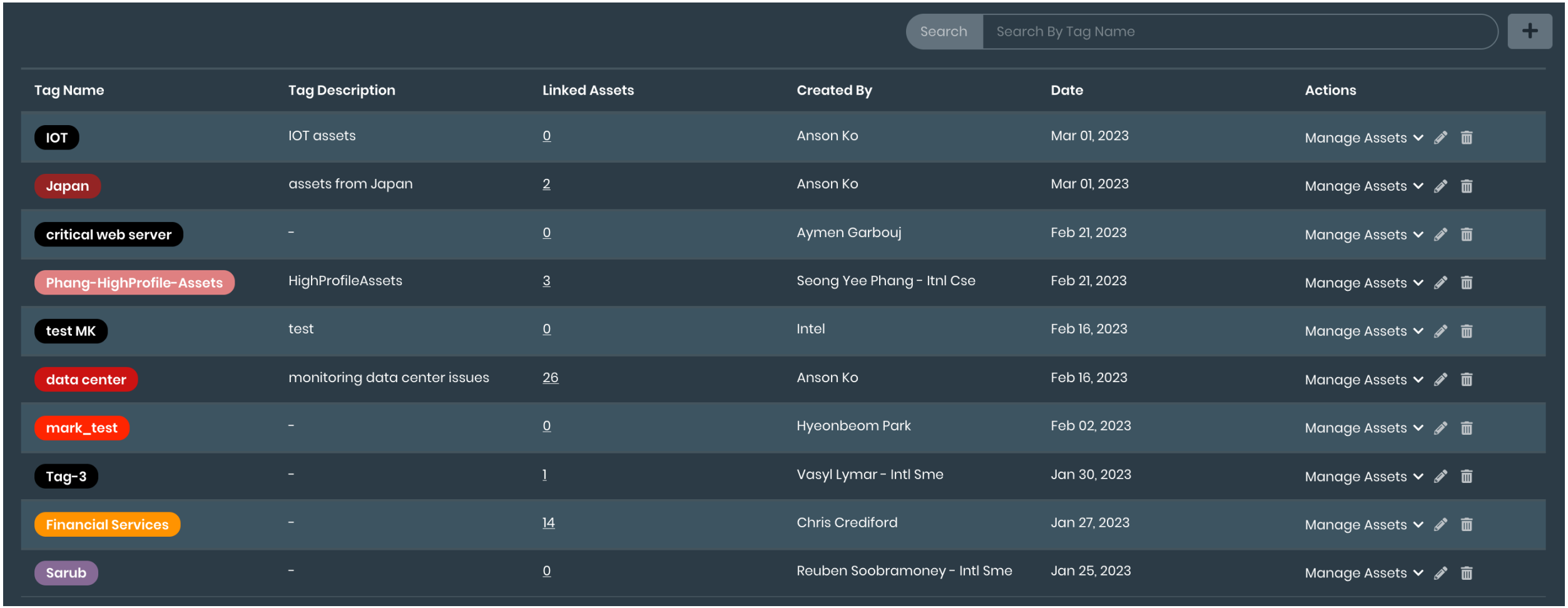


COUNTRY	ASSETS	ISSUES
United States	59	15
France	53	4 24
Canada	9	1
Portugal	2	No Issue
Australia	2	No Issue
China	2	No Issue
Ireland	1	No Issue
Belgium	1	No Issue

- 우선순위 지정을 위한 맵
- 분산된 환경의 보안이슈 가시성 확보
- 사용자 친화적 직관적인 뷰어

© Fortinet Inc. All Rights Reserved.

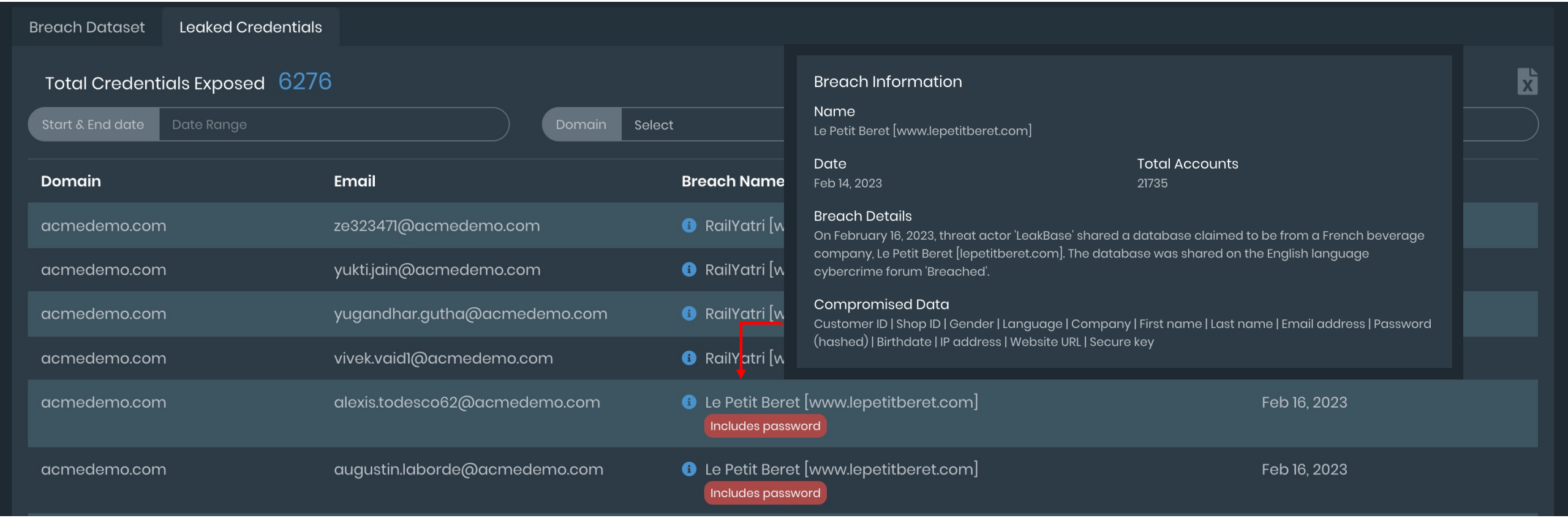
포티넷 EASM 활용 사례 4



- 태깅을 통한 2차 자산 관리
- 유관 시스템과 유연한 연동성 확보
- SOC 및 MSSP 확장된 사용성

© Fortinet Inc. All Rights Reserved.

포티넷 EASM 활용 사례 5

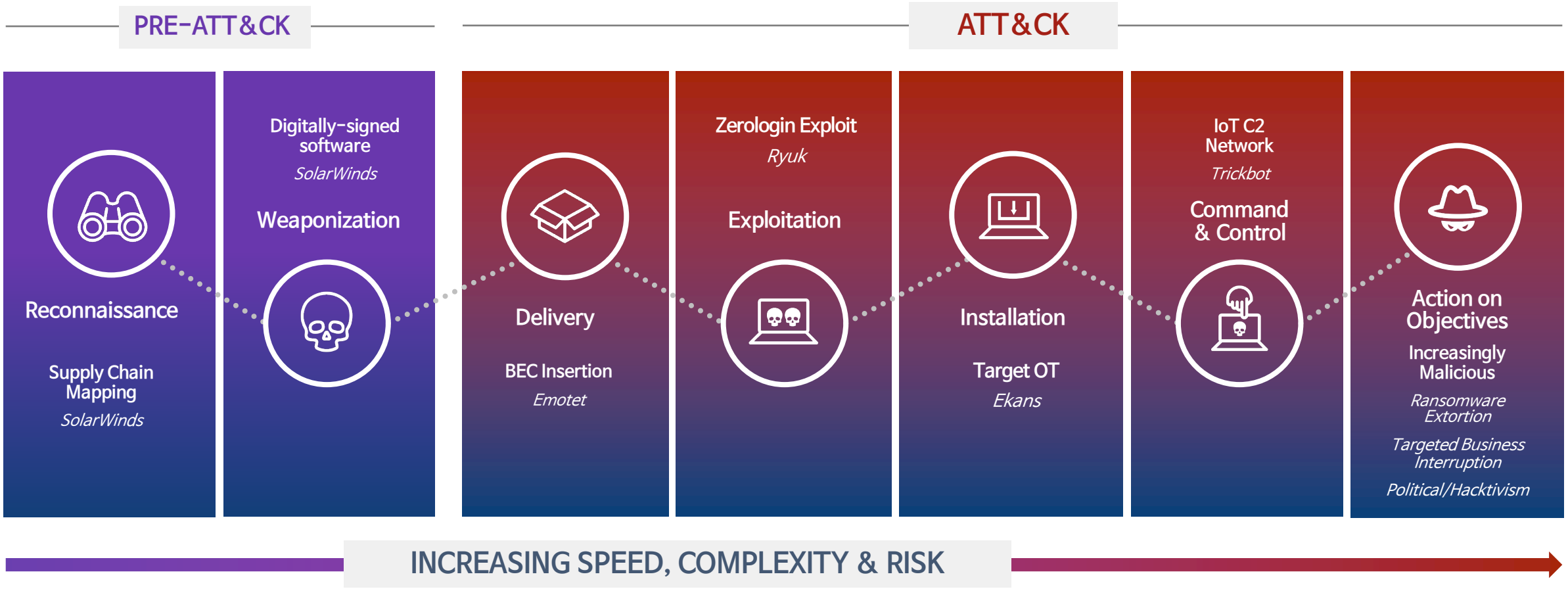


- 노출된 자격증명의 사용자 정보 제공
- 노출된 자격증명의 공격그룹에 대한 요약정보 제공
- 다크웹/딥웹 포럼/블로그와 관련된 리포트 링크
- 노출된 자격증명과 관련된 인텔리전스 리포트 링크

© Fortinet Inc. All Rights Reserved.

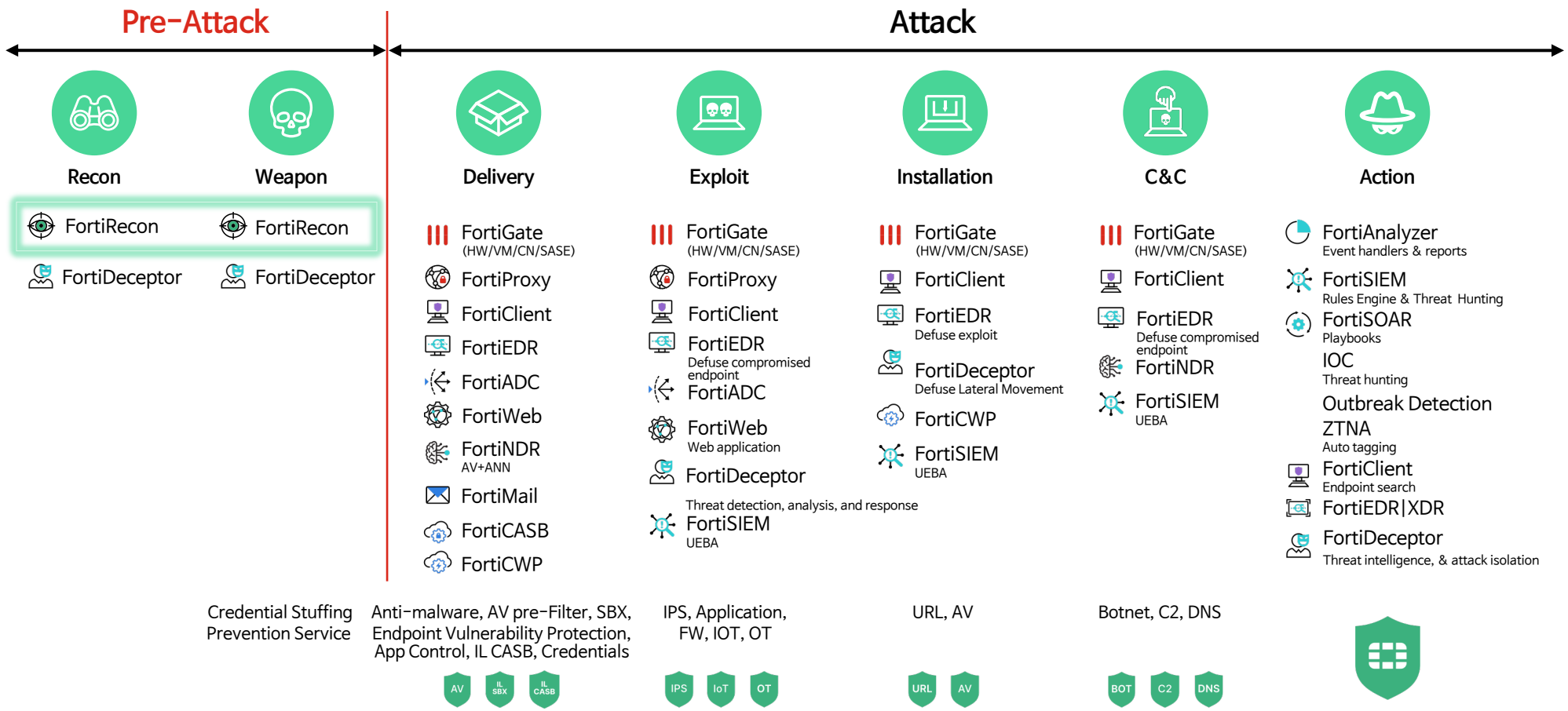
외부공격표면과 사이버킬체인의 관계성

➢ 사이버킬체인 전반에 걸쳐진 보안툴과의 유기적인 활동성 필요



© Fortinet Inc. All Rights Reserved.

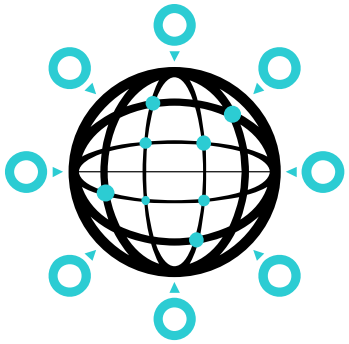
포티넷 사이버킬체인 매트릭스



© Fortinet Inc. All Rights Reserved.

진정한 제로 트러스트 모델을 위하여

외부자 관점의 제로 트러스트



EASM in FortiRecon

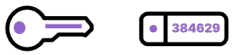
- ✓ 포티넷 – FortiRecon의 EASM은 **알려지거나 알려지지 않은 기업의 노출된 자산**을 리얼타임으로 탐지하는 솔루션
- ✓ **외부자 관점으로 접근하여** 기업 자산의 **취약점 및 위험 상태**를 웹포탈 형태로 제공
- ✓ 악의적인 행위자(해커)가 **악용 할 수 있는 서버, 자격증명, 퍼블릭클라우드 서비스 구성 오류 및 소프트웨어 코드 취약성을 식별**하여 문제 해결의 우선순위 지정에 도움

Cyber Hygiene 통한
제로 트러스트 모델링 적용 준비

내부자 관점의 제로 트러스트

포티게이트

클라이언트 / EMS 중앙관리



FortiAuthenticator /
FortiToken

- ✓ 포티넷의 ZTNA 솔루션은 FortiClient 및 FortiGate 사용 고객이라면, **추가 비용 없이 소프트웨어 업그레이드만으로 사용** 가능(FOS 7.0 이상)
- ✓ 사내 네트워크에 있는 모든 장치가 누구, 언제, 무엇인지에 대한 **완전한 가시성과 제어를 제공**
- ✓ 포티게이트는 **세션과 사용자 행동을 지속적으로 모니터링**하여 데이터, 애플리케이션 및 리소스가 계속 보호되고 있는지 확인

가장 확실한 방법,
지속적인 사용자 검증을 통한 제로 트러스트 구현

© Fortinet Inc. All Rights Reserved.

FORTINET

Customer Briefing Center
포티넷 CBC 고객 솔루션 체험 센터

전세계 TOP사이버 보안 벤더인 포티넷에서 국내 고객 분들을 위해 마련한 솔루션 체험 센터로 방문하시는 고객분들의 요구사항에 따라 맞춤화된 컨설팅을 제공합니다.

보안 중심 네트워크 | 다이나믹 클라우드 보안 | AI 기반 보안 관제 | 제로 트러스트 엑세스

☑ 포티넷CBC에 방문해야 하는 이유?

- 디지털 트랜스포메이션에 필요한 IT보안 요구 사항을 알아보고 최적의 해결 방안을 제시합니다.
- 고객의 비즈니스 목표에 맞추어 당사 기술 전문가와 1:1 맞춤 컨설팅이 가능합니다.
- 축적된 수많은 레퍼런스로 고객의 다양한 상황에 맞는 완벽한 보안 솔루션을 제공합니다.
- 보안 솔루션을 시각적으로 확인할 수 있는 라이브 데모를 직접 체험할 수 있습니다.

포티넷 CBC는 언제나 여러분께 열려있습니다. 지금 방문 신청해주세요!

www.fortinet-vcbc.com www.fortinet.com/kr/corporate/cbc

CBC 방문 신청하기

Virtual CBC 바로가기


FORTINET