FORTINET

AI 시대의 국가정책변화에 따른 포티넷의 FortiCNAPP 전략

포티넷코리아 / 김수영 상무

Agenda

- Cloud Security Challenge
- Introduction to New Lacework FortiCNAPP

The Challenge of Securing the Cloud

국정원 망분리 개선안 공개 및 금융권 망분리 개선안

< 단계별 세부 추진과제 >

1단계(24년 연내 추진)	2단계	3단계
❶ 생성형 AI 허용(규제샌드박스) : 생성형 AI를 활용하여, 가명정보'까지 처리할 수 있도록 규제특례 허용 * 추가정보 사용 없이는 특정 신용정보주체를 알아볼 수 없도록 가명처리된 개인신용정보	❹ 1단계까지의 규제특례 정규 제도화 : 샌드박스로 성과 검증'된 과제 → 규정 개정 등 제도화 추진 * ~'25.上 : 샌드박스 운영사례 성과검증	❼「디지털 금융보안법(가칭)」 제정 * 연구용역('24.3Q), 공청회(4Q)를 거쳐 연내 마련 추진 - 자율보안-결과책임의 보안체계 구축 : 목표·원칙중심으로 규제 전환 - 금융권 책임 강화 : 배상책임 강화, 실효성 있는 과징금 등 : CISO 권한 확대 및 CEO사회 보고의무 - 금융당국의 점검·이행명령 등 금융권 보안수준 제고 뒷받침
❷ 클라우드 이용 확대 (규제샌드박스)	❺ 규제특례 확대·고도화 : 개인신용정보 처리 등 리스크↑ 업무 → 강화된 보안대책 전제로 추가 허용	
❸ 연구·개발 분야 망분리 개선(감독규정 개정)	❻ 제3자 리스크 관리강화 등을 위한 정보처리 위탁제도 정비	

	현 행	개 선
데이터	개인신용정보 금지	가명정보 허용
프로그램 유형	협업툴, 인사관리 등 비중요업무 허용	고객관리(CRM), 업무자동화 등 추가 허용
단말기	유선 PC만 허용	모바일단말 허용

	현 행	개 선
연구개발망 업무망 간	물리적 망분리	논리적 망분리
연구개발망 전산실 간		개발 결과물 등 이관을 위한 예외 허용
데이터	개인신용정보 금지	가명정보 허용

기사

저무는 '망분리' 시대...'다층보안체계'로 국가 보안정책 대대적 변화 예고

By 이유지 · 2024년 9월 11일

보안성 확보를 이유로 정부·공공 분야 업무 환경에서 인터넷과 업무망을 분리해 사용해온 '망분리' 정책이 '다층보안체계(MLS)'로 전환된다.

정부는 그동안 획일적으로 적용해온 망분리 정책 대신에 공공 정보시스템과 데이터(정보)를 중요도에 따라 세 등급으로 분류해 그에 맞는 보안통제를 적용하는 방식을 내년부터 시행할 예정이다.

이에 따라 지난 2006년부터 시행돼온 정부·공공 망분리 정책이 사실상 폐지된다. 앞으로는 정부·공공기관 담당자들도 두 개의 PC를 사용할 필요 없이, 적절한 보호대책이 적용돼 있다면 민간 기업과 동일하게 업무용 단말에서 인터넷과 클라우드 서비스(SaaS), 챗GPT같은 생성형 인공지능(AI) 서비스도 이용할 수 있게 될 전망이다.

> 공공 망분리 대신 '다층보안체계'로...국가 보안 패러다임 대전환

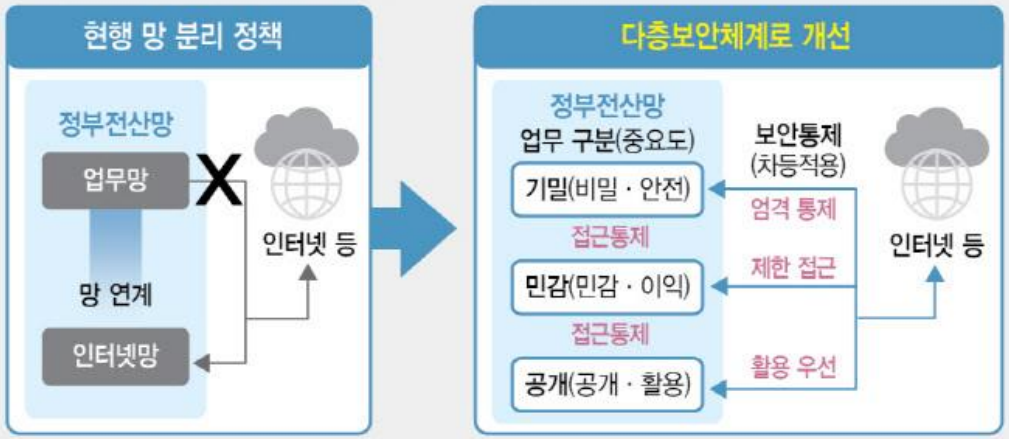
"공공기관 PC도 챗GPT 접속"…내년부터 망분리 규제

송고시간 | 2024-09-11 15:25

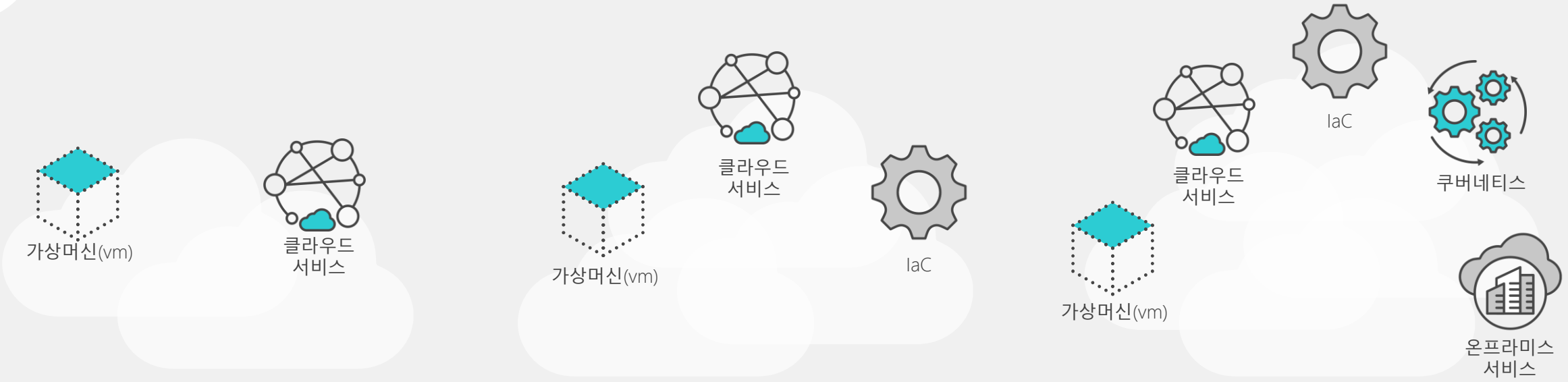
국정원 다층보안체계 전환 로드맵…정보 중요도 따라 3개 등급 분류
2026년부터 공공분야 암호모듈 국제표준암호 'AES' 허용

'사이버 서밋 코리아 2024' 콘퍼런스

망분리 정책에서 다층보안체계로 전환 개념도



클라우드의 진화 및 보안과제



부서별 워크로드

비즈니스 워크로드

Mission-Critical Workloads

조기채택 | **발전** | **하이브리드 멀티클라우드**

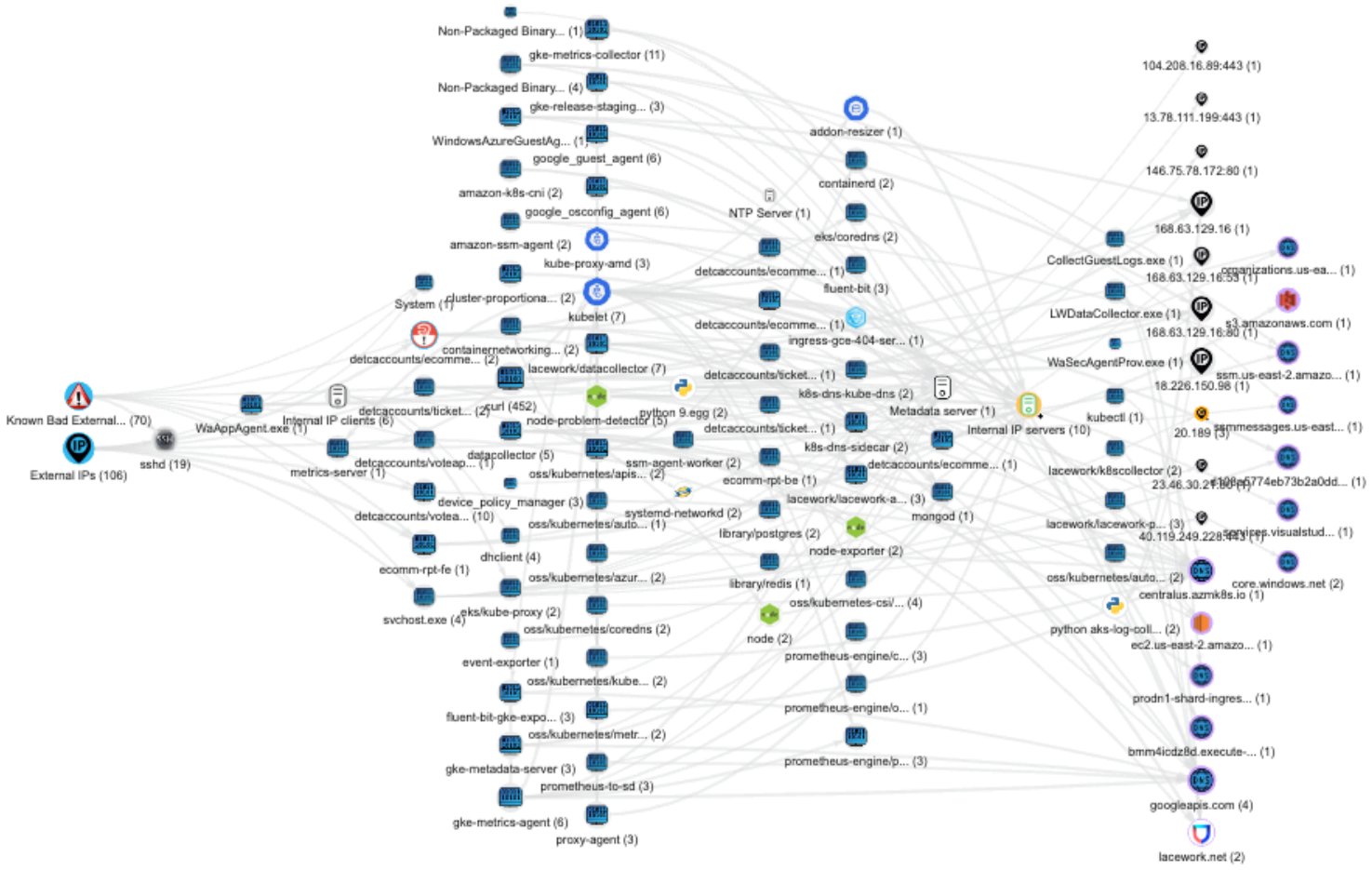
클라우드의 복잡성	어플리케이션, 클라우드서비스, 인스턴스, 권한
개발 속도	코드, 커밋, 인프라스트럭처, 네트워크
어플리케이션 종속성	오픈소스, 복잡한 종속성
코드 책임성	개발자가 컨테이너, 워크로드, 네트워크를 정의

- 기술이 완전히 다름
- 매년 새로운 기술 추가
- 책임공유모델
- 권한수준이 다름

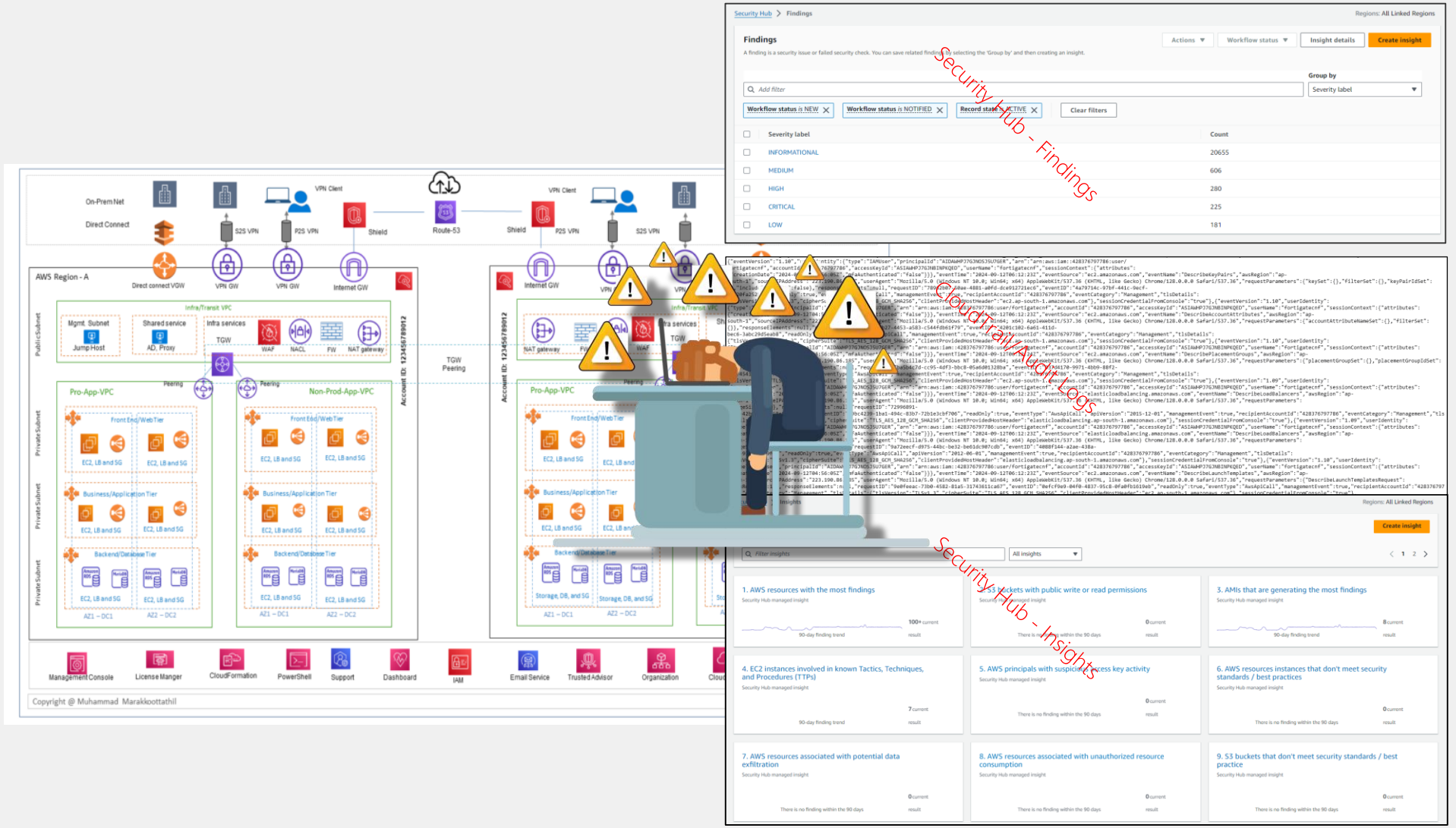
간단한 클라우드 배포도 매우 복잡

클라우드는 복잡하다.

- 200개의 클라우드 서비스 (AWS만 사용하는경우)
- 수백가지의 민감한 조치 가능
- 무제한의 공인 아이피 공간
- 비전문 개발자도 사용 가능한 서비스 제공



간단한 클라우드 배포도 매우 복잡



불편한 진실...

클라우드가 기존 사이버보안의 고정관념을 깨뜨리다.

50% 가 슈퍼유저 관리자이며, 클라우드 워크로드가 일반 사용자 보다 10배 더 많음

Source: Microsoft

18분마다 새로운 CVE가 발표되고 있음

Source: CVE.org

2031년까지 랜섬웨어로 인한 피해액은 **연간 약 2650억 달러** , **2초마다 새로운 공격이** 발생할 것으로 예상됩니다

Source: Cybersecurity Ventures

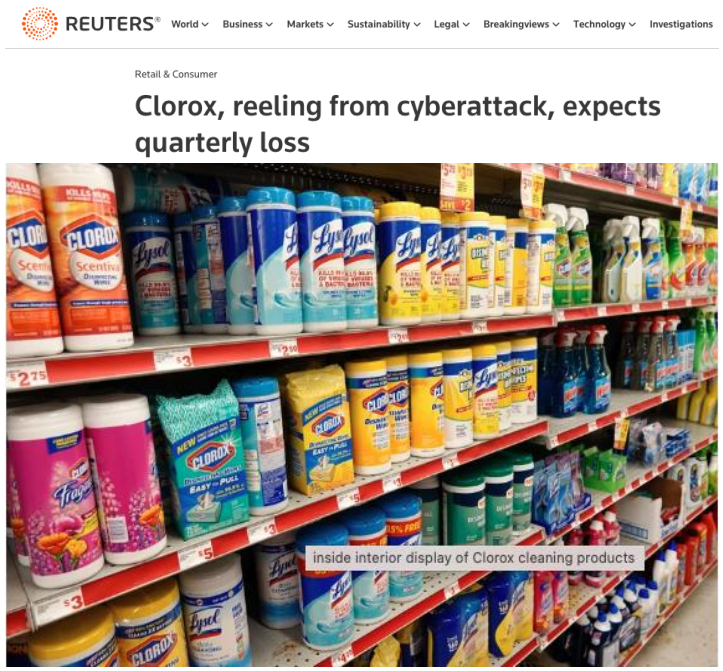
2022년의 41%의 직원에서 2027년까지 75% 직원이 **IT가시성 밖에서** 기술을 획득, 수정 또는 생성할 것입니다.

Source: Gartner

데이터 침해의 68%가 도난된 인증정보와 소셜엔지니어링에 의한 것입니다.

Source: Verizon

클라우드 침해는 비즈니스에 막대한 영향을 미칠 수 있습니다.



Social engineering: 3rd party help desk

Social engineering: IT support vendor

Social engineering: 3rd party customer support

클라우드 보안 태세를 강화하는 것만으로는 ID 관련 사고를 예방할 수 없습니다.

Introducing Lacework FortiCNAPP

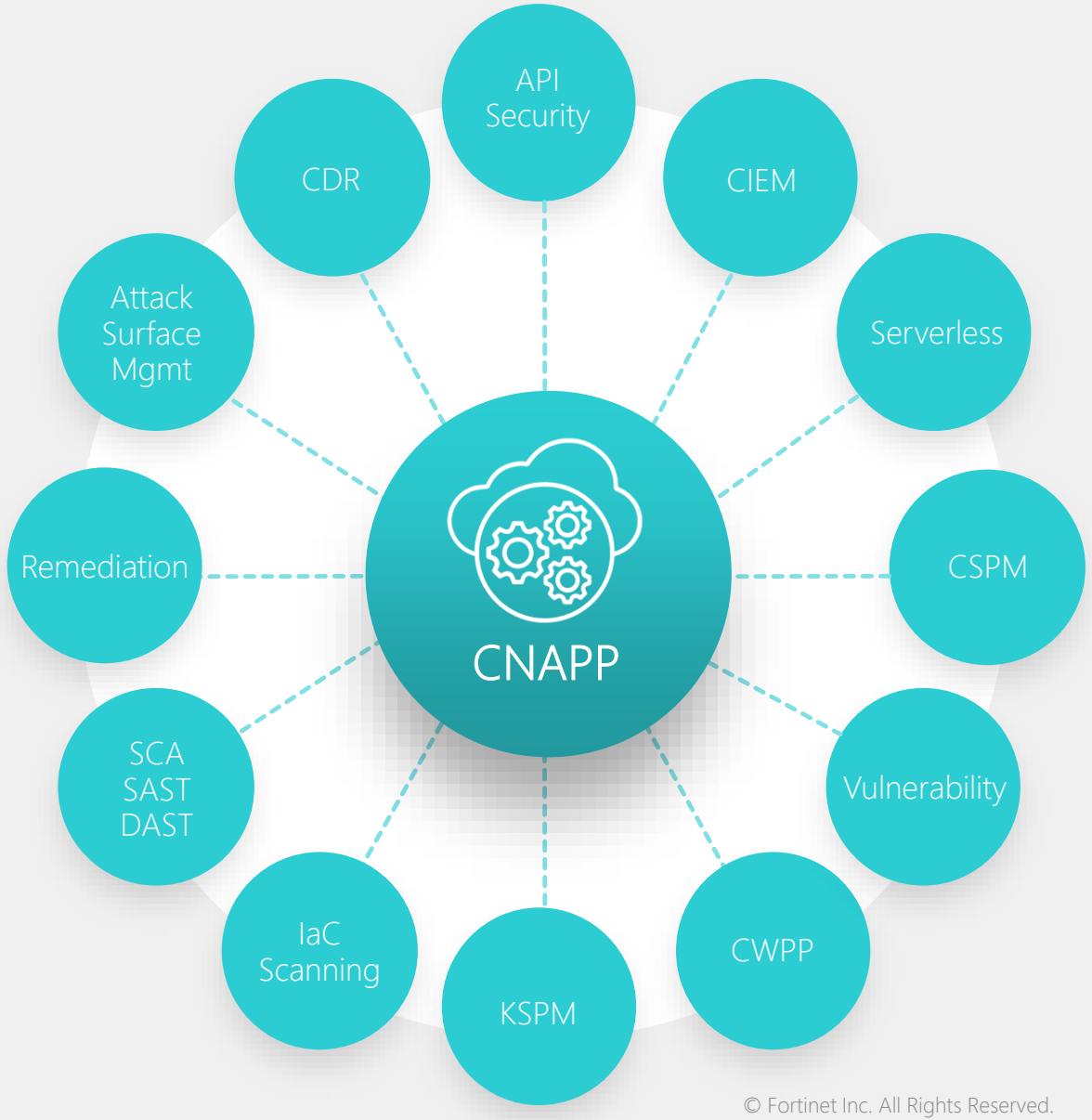
Enter: Cloud-Native Application Protection Platform (CNAPP)

가트너에서 만든용어

CNAPP:

"CNAPP(클라우드 네이티브 애플리케이션 보호 플랫폼)는 개발 및 프로덕션 전반에서 클라우드 네이티브 애플리케이션을 보호하고 보안을 유지하기 위해 설계된 긴밀하게 통합된 보안 및 규정 준수 기능 집합입니다.."

Gartner



Fortinet + Lacework FortiCNAPP

'24년 7월 10일, Lacework 인수로 업계에서 가장 포괄적인 사이버 보안 플랫폼 강화

> Both Fortinet and Lacework are driven by a culture of innovation and integration. By integrating Lacework's leading AI-powered cloud security platform, we're enhancing our Security Fabric platform to offer customers an even more comprehensive solution. This acquisition reinforces our commitment to delivering consistent security across on-premises and cloud environments.
>
> **- Ken Xie, Founder, Chairman of the Board, and CEO at Fortinet**

> Lacework, partnering closely with our customers, has built a world-class solution to the most complex and varied cloud cyber risks and threats. Our vision to connect across security silos enables teams to work together to produce better security outcomes more quickly. Integrated into Fortinet's platform, we can more deeply embrace these customers to truly solve for their end-to-end security challenges.
>
> **- Jay Parikh, CEO at Lacework**

온프레미스 및 클라우드 환경 전반에 걸쳐 일관된 보안을 제공하려는 우리의 약속을 강화합니다.

- Ken Xie, Founder, Chairman of the Board, and CEO at Fortinet

Fortinet의 플랫폼에 통합되면 고객의 엔드투엔드 보안 문제를 진정으로 해결할 수 있습니다.

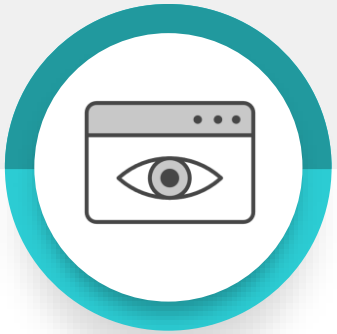
- Jay Parikh, CEO at Lacework

이 문제를 해결하는 방법

클라우드 네이티브 애플리케이션의 위험 및 위협 식별, 우선순위 지정 및 해결

공격 표면 최소화

개발 속도를 늦추지 않고 포괄적인 가시성을 확보하고 취약성, 잘못된 구성 및 과도한 권한을 선제적으로 줄이세요.



지속적으로 위험 모니터링

가상 머신, 컨테이너 및 쿠버네티스 워크로드를 지속적으로 평가하여 악용되기 전에 활성 위험을 해결합니다. 악용되기 전에 해결하세요.

위협 영향 감소

손상된 인증 정보 사용, 클라우드 랜섬웨어, 크립토마이닝 등 비정상적인 행동과 활성 위협을 신속하게 탐지, 조사 및 대응합니다.

부인할 수 없는 현실

클라우드 보안의 가장 큰 적은 시간이다.

65일
중대한 취약점에 대한 평균 MTTR

241일
평균 침해 탐지 및 억제 시간

5시간
공격자가 데이터를 유출하는 데 걸리는 평균 시간

Source: Edgescan: 2023 Vulnerability Statistics Report, IBM: 2023 Cost of a Data Breach, SANS: 2022 Ethical Hacking Survey

클라우드 보안을 어떻게 운영하고 계신가요?

가장 중요한 위험과 위협의 우선순위를 정하기 위한 주요 인사이트

가장 영향력이 큰 **리스크**를 어떻게 신속하게 완화할 수 있을까요?

잘못 구성된 서비스는 누구와 통신하고 있나요?

사람과 기계는 무엇에 액세스하고 있나요?

취약한 패키지는 어떻게 작동하나요?

이 리소스가 활성 위협과 연관되어 있나요?

가장 위험한 **위협**에 대한 MTTR을 어떻게 줄일 수 있나요?

이 애플리케이션의 동작이 변경된 이유는 무엇인가요?

잠재적인 영향은 얼마나 큰가요?

새로운 로그인, 프로세스 또는 사용자 자료인가요?

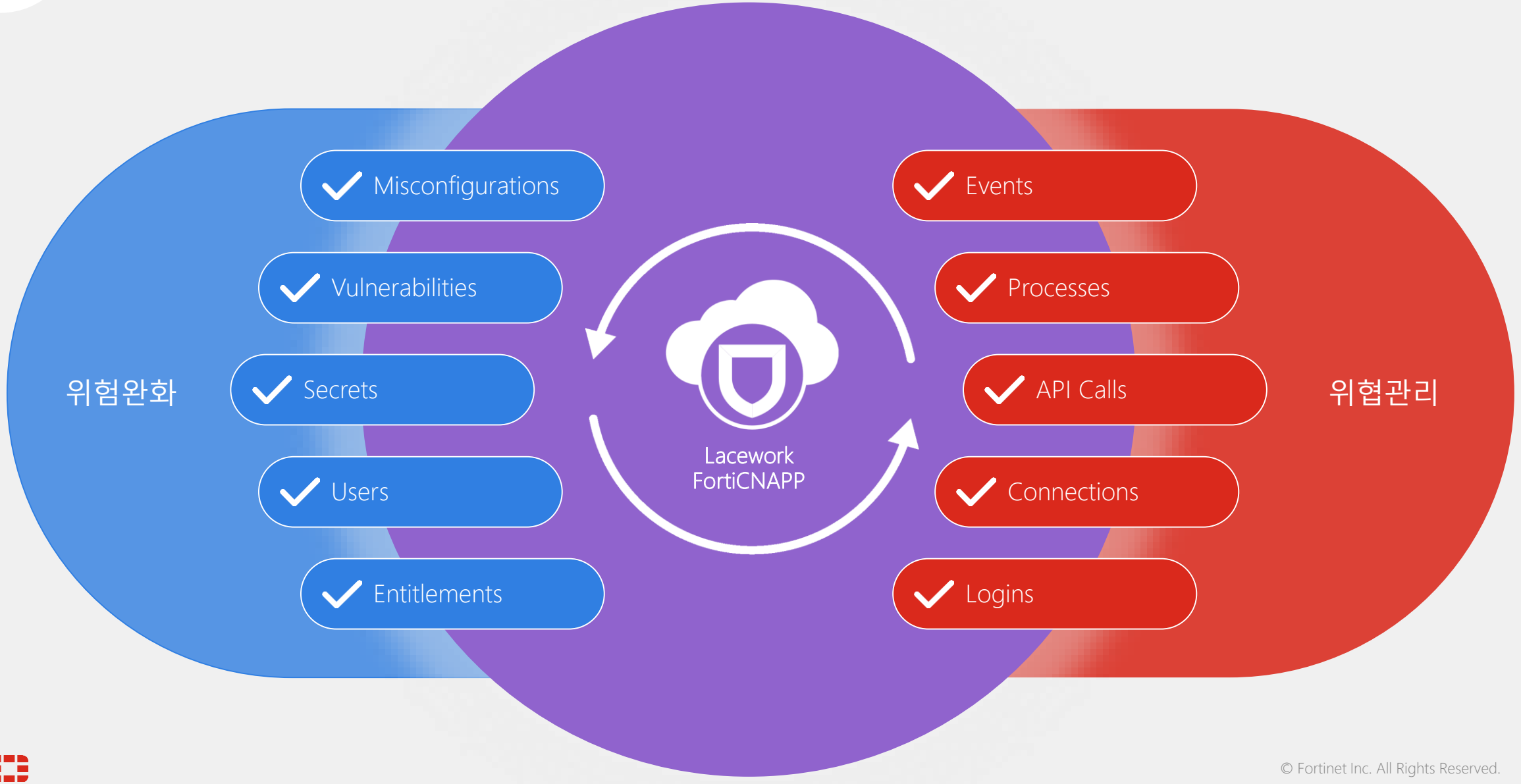
새로운 권한 에스컬레이션이 발생한 이유는 무엇인가요?

사일로화된 보안 도구만으로는 충분하지 않습니다

사일로화된 툴의 과제

- 6~10개의 클라우드 보안 툴을 관리하기에는 복잡하고 비용이 많이 듭니다.
- 부분적인 적용 범위를 가진 파편화된 툴로 인한 격차 발생
- 우선순위 지정을 위해 데이터를 정규화하는 데 매우 어렵고 시간이 많이 소요됨

우선순위를 정하려면 위험과 위협 컨텍스트를 결합해야 합니다.



효과적인 클라우드 네이티브 보안을 위해서는 통합된 접근 방식이 필요

Lacework FortiCNAPP: 코드부터 클라우드까지 고객의 환경을 이해하는 단일 플랫폼

수집

악용가능한 위험

Users | Misconfigs | Entitlements
Vulnerability | Secrets | ...

활성 위협

Connection | Processes | API Calls
User Login | Events | ...

이해

Lacework FortiCNAPP

데이터 자동 상관관계
분석기준이 되는 정상 동작
편차 및 이상 징후 식별

해결

Composite Risks

- Attack Paths
- Excessive Permissions
- Active Vulnerability

Composite threats

- Compromised Credentials
- Cryptojacking
- Ransomware

위험 완화
최소한의 노력으로
위험 최소화 및 완화

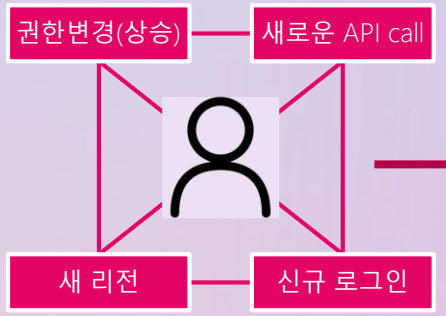
위협 관리
활성 위협을 신속하게
탐지하여 영향 최소화

분석 USE CASE

유출된 인증정보의 영향 탐지 및 최소화

탐지

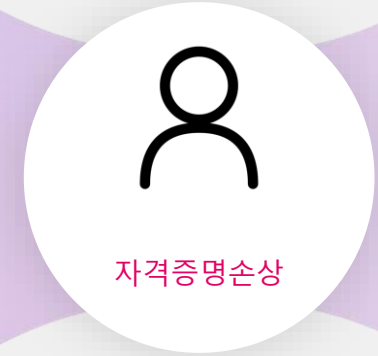
위협신호



실행중인 위협

- 불가능한 통신
- 인프라 탐색
- 계정 변조

Lacework
FortiCNAPP



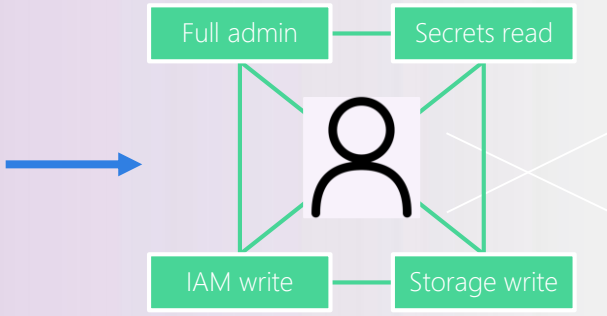
자격증명손상

대응

악용 가능한 위험

- 과도한 권한
- 유해성 조합
- 롤 연계(연결체인)

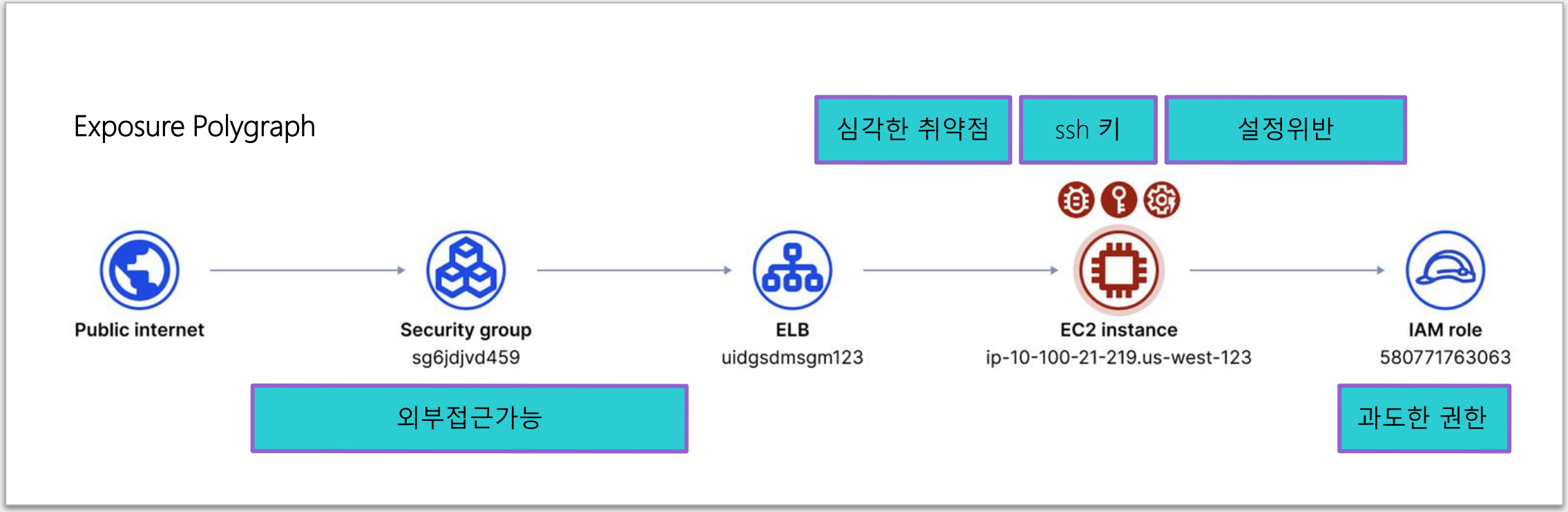
위험신호



향후 유사한 공격의 위험을
판단하여
공격을 신속하고 안전하게
차단하고 중지합니다.

분석 USE CASE

가장악용하기 쉬운 위험의 우선순위를 지정



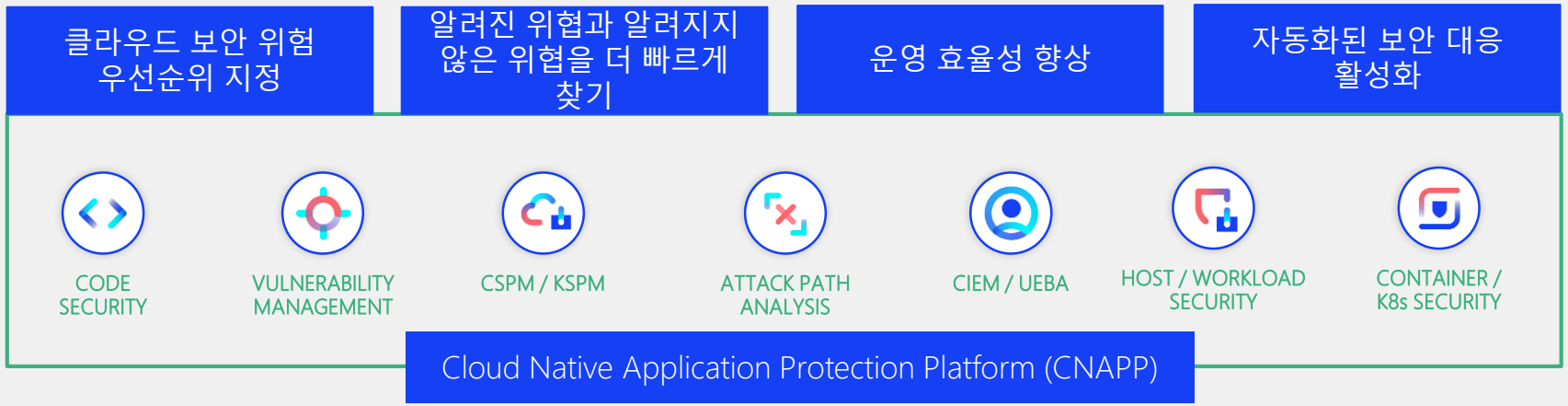
클라우드 이니셔티브 보안을 위한 Lacework FortiCNAPP의 적합성

고객 도전 과제 및 이니셔티브

클라우드 전환

어플리케이션 현대화

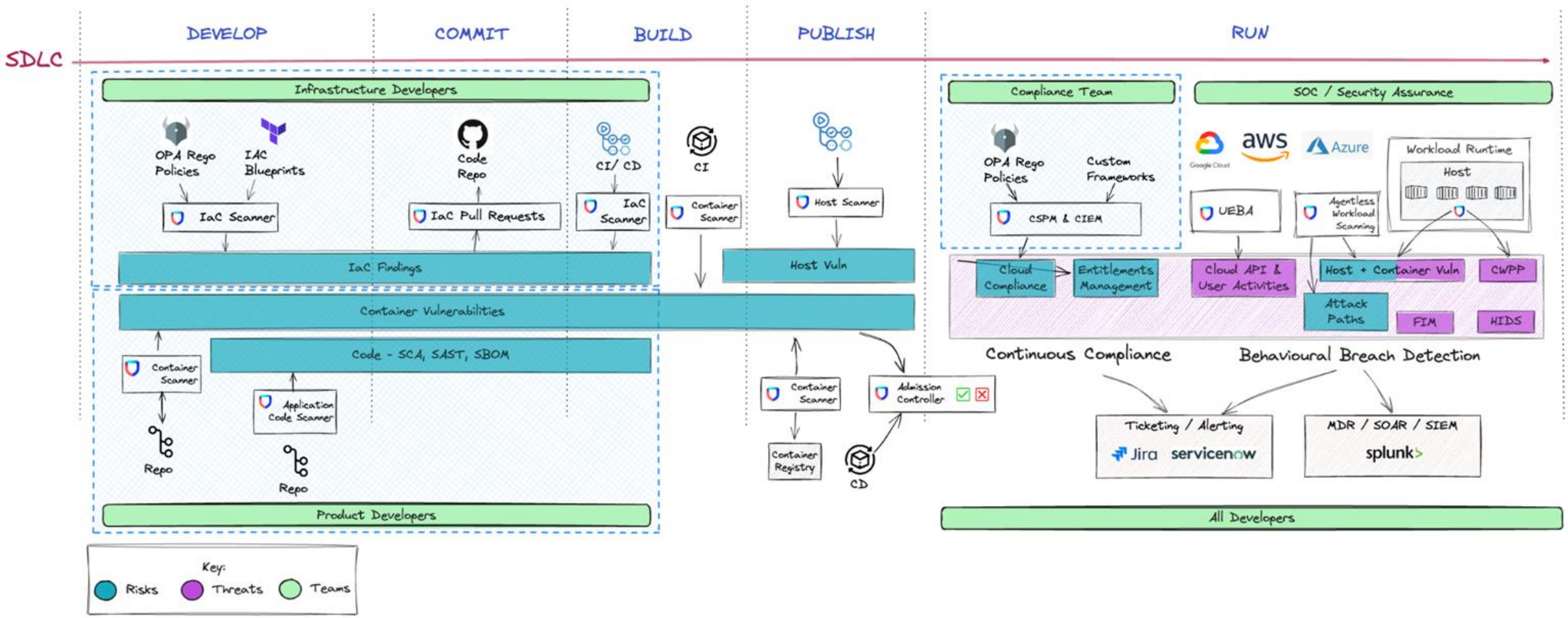
도구 통합



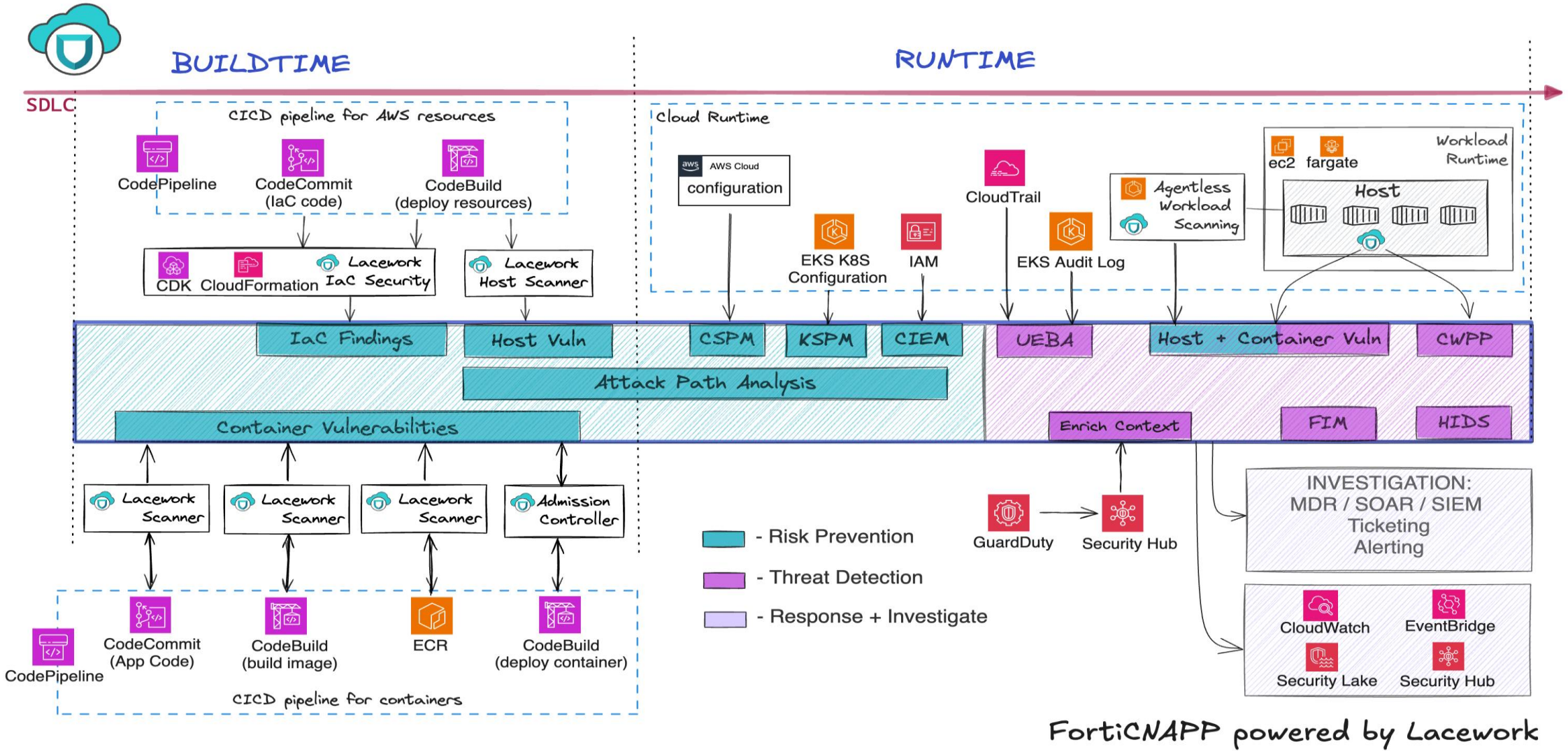
FortiCNAPP – USE CASE

FortiCNAPP를 통한 데브옵스전반의 클라우드 보안강화

고객 도전 과제 및 이니셔티브



AWS 사례



How Lacework FortiCNAPP이 금융 핀테크를 지원한 사례

lendingtree

업종 분야

금융

CSP

AWS, Google Cloud, Azure

챌린지

- 점점 더 복잡해지는 멀티클라우드 환경
- 컨테이너화된 워크로드에 대한 가시성 부족
- 지속적으로 변화하는 규제 표준을 따라잡기 어려움

솔루션

- 통합 플랫폼으로 멀티클라우드 자산을 완벽하게 지원
- 지속적인 가시성 및 위협 탐지
- 기본 제공 정책 및 보고서로 규정 준수 감사 간소화

결과

- 도구 통합을 통해 연간 20만 달러 절감
- 10시간에서 5분으로 조사 시간 단축 5분으로 단축-
- 경보 볼륨 98% 감소 5건/일

고객 성과 창출

100:1

일일 알림 횟수 감소

2 to 5

통합을 통한 클라우드
보안 도구 수 감소

80%

인시던트 및 알림의
신속한 조사

90%

수동 클라우드 보안
작업 감소

50%

SIEM 데이터 수집
비용 절감

0-Day

활성 위협 및 공격
탐지

Lacework FortiCNAPP 기술의 확장

Secure Networking

Firewall (FortiGate)

Management (FortiManager)

Switch (FortiSwitch)

Access Points (FortiAP)

5G (FortiExtender)

NAC (FortiNAC)

DDoS (FortiDDoS)

+MORE

Unified SASE

SD-WAN (FortiGate)

SSE/SASE (FortiSASE)

ZTNA (FortiClient)

DEM (FortiMonitor)

Virtual FW (FortiGate VM)

Cloud-native FW (FortiGate CNF)

WAF (FortiWeb)

SWG (FortiProxy)

+MORE

AI-Driven Security Operations

Analytics (FortiAnalyzer)

CNAPP (FortiCNAPP)

SIEM (FortiSIEM)

EDR (FortiEDR)

SOAR (FortiSOAR)

NDR (FortiNDR)

Mail (FortiMail)

EASM (FortiRecon)

FortiGuard SoCaaS

+MORE

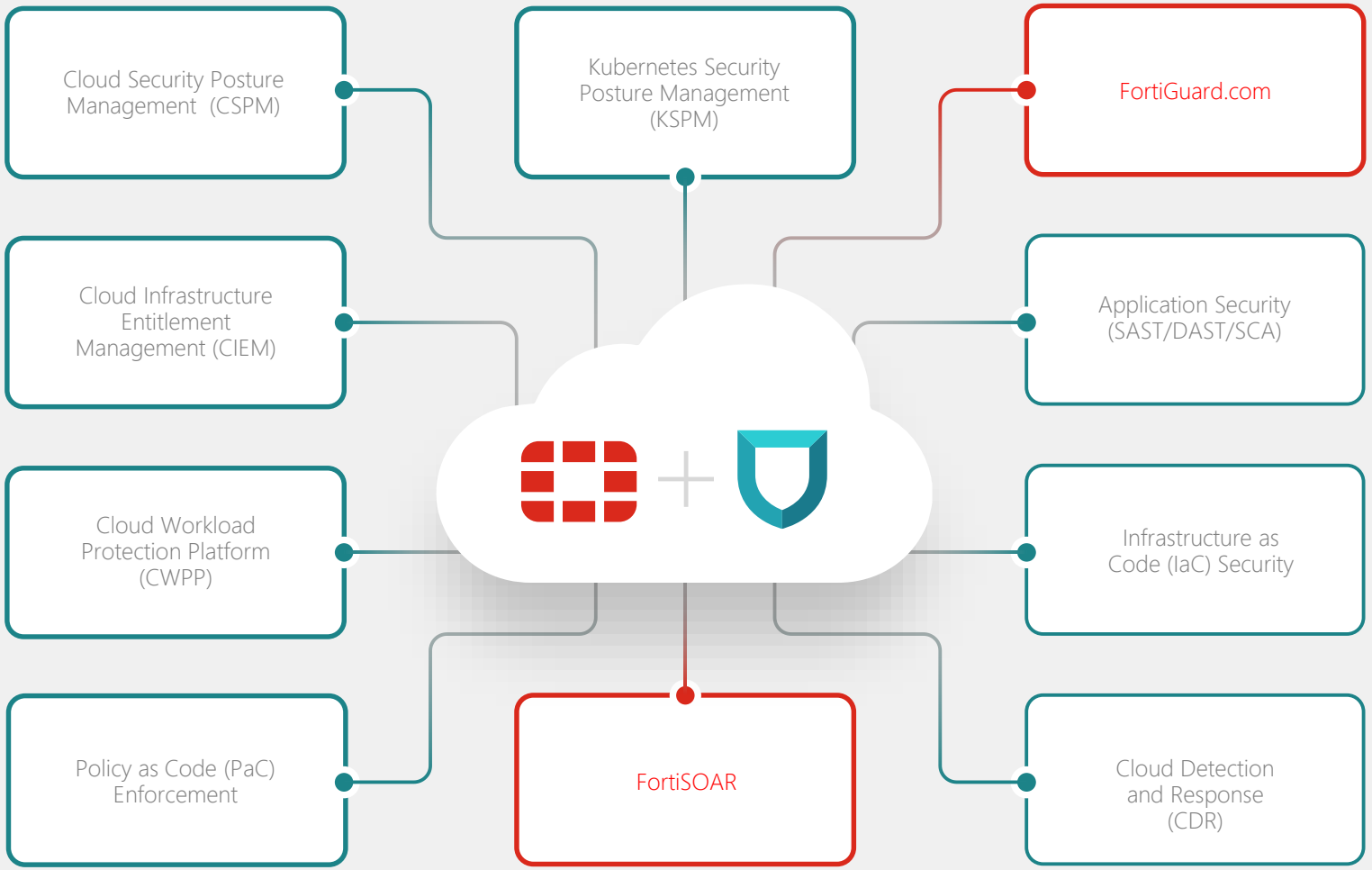
Fortinet + Lacework FortiCNAPP

가장 완벽한 AI 기반 클라우드 네이티브 애플리케이션 보호 플랫폼

모든 클라우드 보안 및 보안 CI/CD 애플리케이션 개발 요구 사항을 충족하는 단일 공급업체

하이브리드 및 멀티 클라우드 전반에서 애플리케이션 코딩, 배포, 실행에 이르는 모든 과정을 확인하고 보호

Lacework FortiCNAPP과 포티넷의 AI 기반 플랫폼으로 보안 간소화 및 포티넷의 AI 기반 플랫폼으로 보안을 간소화



FortiGuard Labs

VISIBILITY → INNOVATION → ACTIONABLE THREAT INTELLIGENCE

Telemetry

- Enforcement Partnerships
- CERTs
- CTA feeds
- OSINT
- Trusted Partnerships
- Darkweb Research

Firewalls (HW/VM/ SASE) 5.6M+

Web 250M+

Sandbox 1M+

Emails 100M+

Endpoints 3M+

FortiGuard Labs

- AI / Machine Learning
- Fortinet Distribution Network
- Detection and protection in milliseconds
- Federated Machine Learning
- Central Threat System

Lacework FortiCNAPP

SECURITY FABRIC PROTECTIONS

IPS, Application Control, Indicators of Compromise (IoCs), Phishing, Anti-Spam, Endpoint Vulnerability

AV, IPS, AV, IL SBX, IoT, BOT, OT, C2, IL CASB, URL, DNS

PROACTIVE RESEARCH

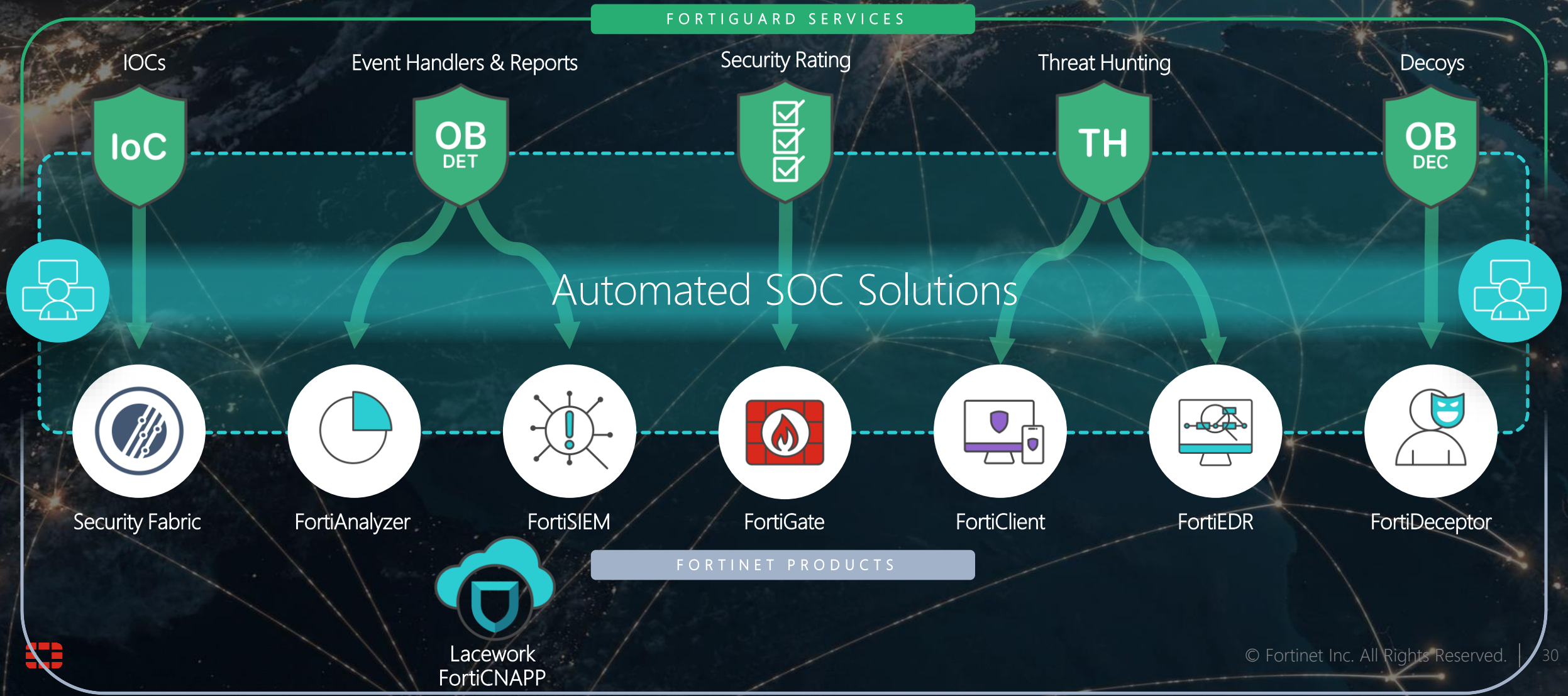
Adversary Playbooks, Security Blogs, Threat Intel Briefs, Zero Day research, Outbreak Alerts, Virtual Patches

THREAT INTELLIGENCE SERVICES

Penetration Testing, SOCaaS, Incident Response, RedTeam Assessment, Breach and Attack Simulation, Digital Forensics, Architecture Evaluation, Cybersecurity Workshops, FortiRecon, MDR

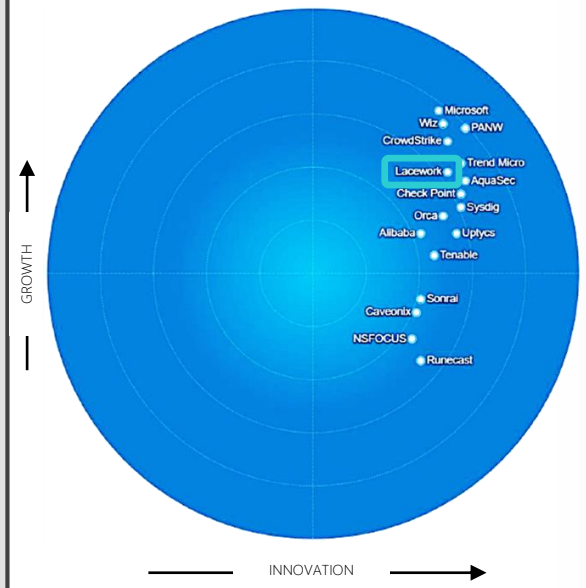
FortiGuard Outbreak Services

Monitoring for Indicators Across *Your* Network



CNAPP 글로벌 마켓리더

LEADER
Frost CNAPP Radar



Frost & Sullivan CNAPP Radar 2023

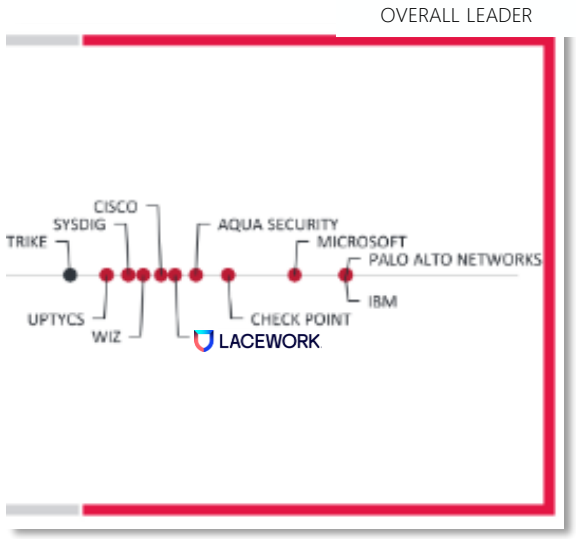
LEADER
G2 CNAPP GRID

G2 CNAPP Grid Report Spring 2024

LEADER
GigaOm CWS Radar

GigaOm Radar for Cloud Workload Security 2024

LEADER
KuppingerCole Compass



KuppingerCole CNAPP Leadership Compass 2024


FORTINET