



**FORTINET®**

# 2024 글로벌 보안 트렌드와 포티넷의 방향성(FortiOS)

포티넷코리아



# INDEX



## 글로벌 보안 트렌드

2024 IDC의 아시아 지역 보안리더 설문 조사 결과  
2024 Cybersecurity의 Cloud Security Report

## 네트워크와 보안의 만남 SASE라는 트렌드

Fortinet  
FortiGate와 FortiOS





# IDC Asia 보안리더 설문조사



# 설문조사 목표

- 대한 사이버 보안 리더의 관점을 알아보기 위해
- 아시아 태평양의 사이버 보안 리더 **550명**
- **한국의 리더 50명**
- 기술 및 금융서비스업(각 14%), 에너지, 제조, 소매, 공공 부문(각 12%) 등 다양한 산업이 의료, 교육, 물류에 걸쳐 고르게 분포되어 있습니다.



# 보안의 당면 과제: 가장 일반적인 사이버 위협

01



피싱

02



랜섬웨어

03



패치 취약성

04



신원 도용

05



공급망 공격



50%



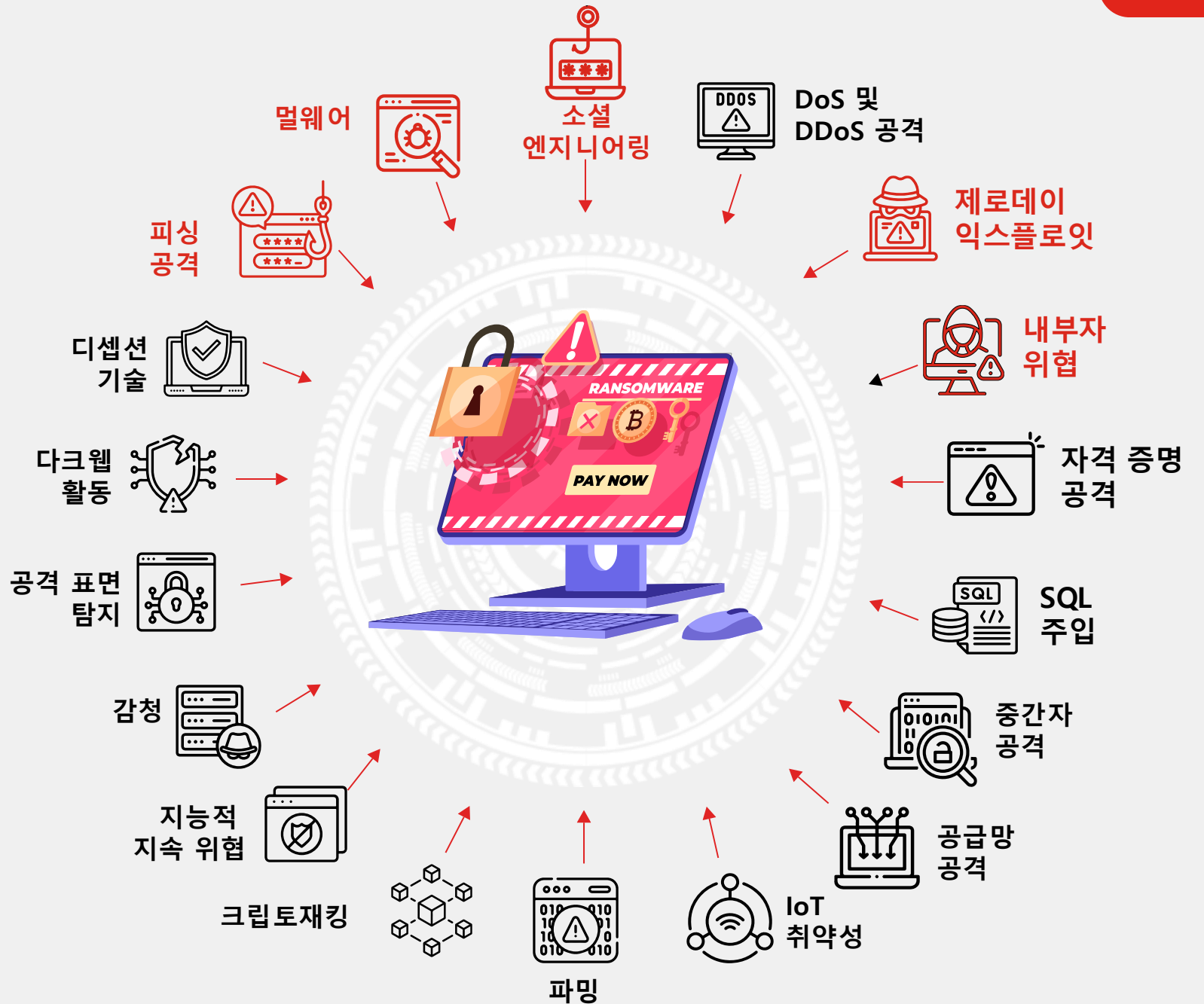
피싱 및 랜섬웨어를 가장 큰 우려 사항으로 생각하는 조직 비율

# 랜섬웨어의 급증

**100%**  
전년 대비

62%의 조직에서 랜섬웨어  
침해사고가 두 배로 증가했으며,

최소 **2배** 이상 증가



# 내부자 위협 및 원격 근무

**54%**의 응답자가 원격 근무로 인해 내부자 위협 인시던트가 증가했다고 생각



내부자 위협이 발생하는 가장 큰 이유 3가지



불충분한 교육



직원 관리부족



부적절한 소통이 랜섬웨어  
급증에 기여

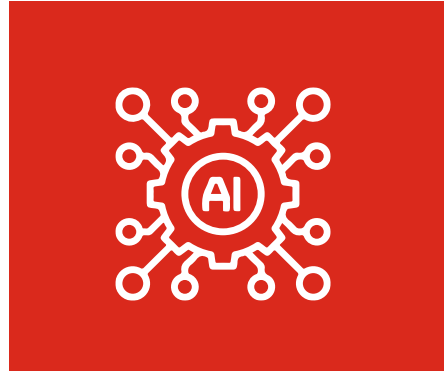
# 새로운 기술의 영향



클라우드  
기술



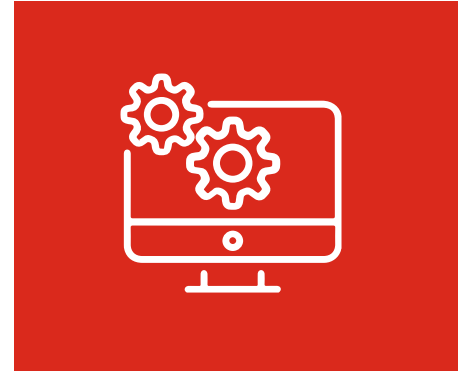
하이브리드  
근무



AI



엣지  
컴퓨팅



IT/OT 시스템  
통합

## IT 보안팀 리소싱

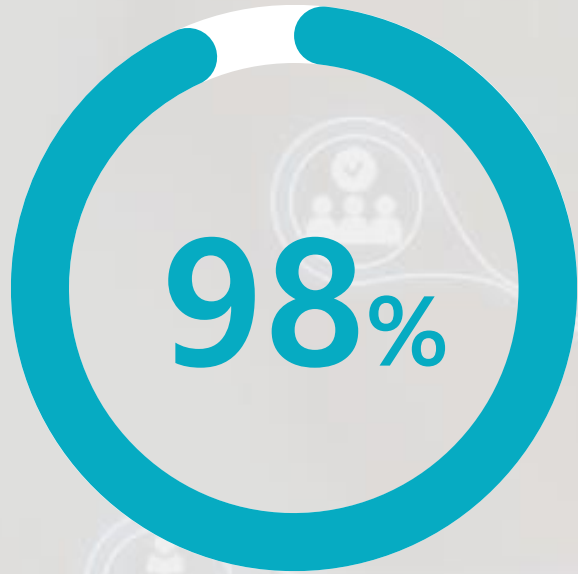


66%

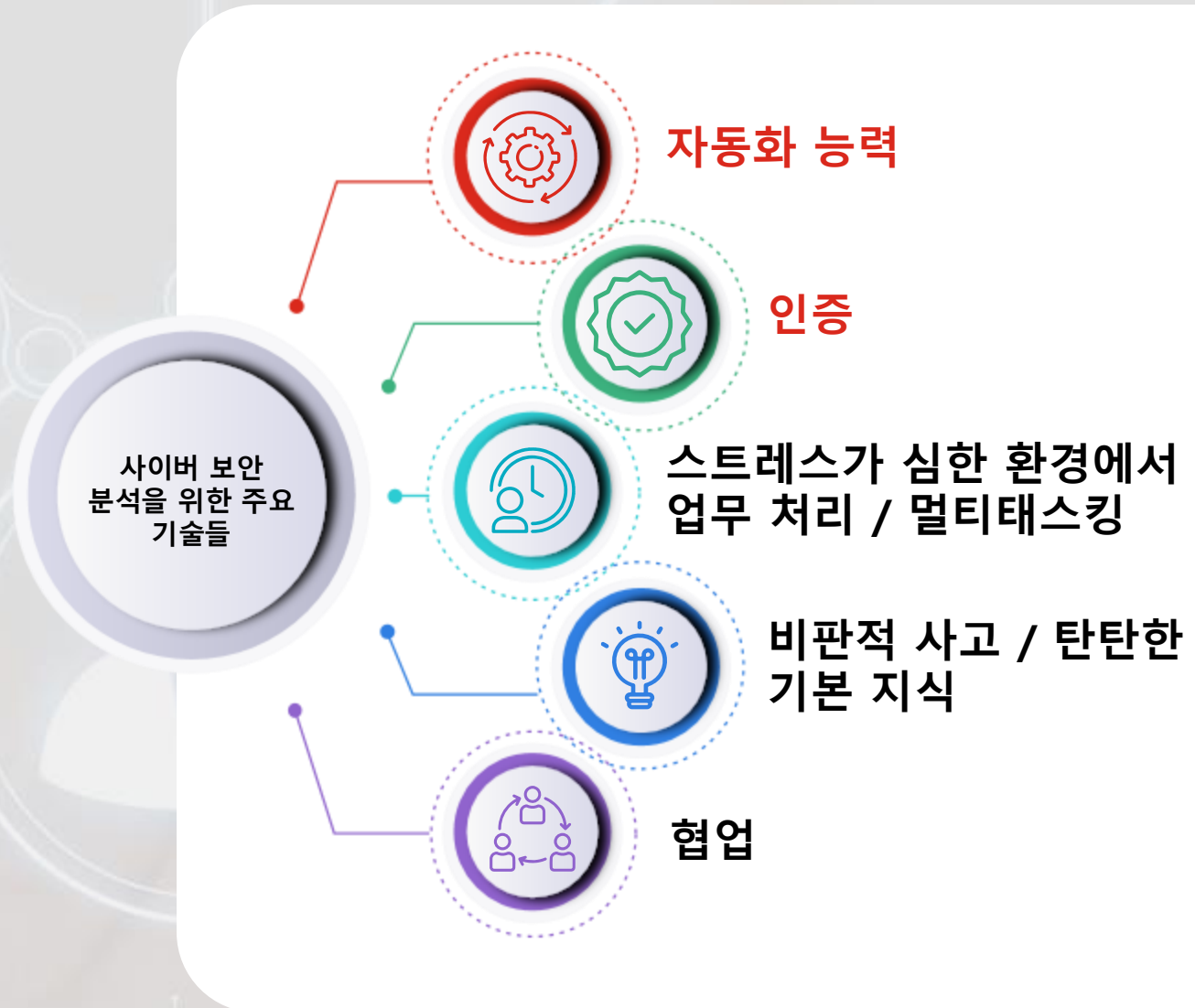
보안팀을 위한 전용 리소스가 **없**는 기업 비율



# 인재 및 기술 개발



응답자 중 **98%**가 팀원의 기술 수준을 유지하기 어렵다고 답변





# 2024 Cloud Security Report

*Cybersecurity INSIDERS*



# 2024 Cloud Security Report

Cybersecurity

## 개요 :

전 세계 927명의 사이버 보안 전문가를 대상으로 실시한 종합적인 설문조사를 바탕으로 클라우드 보안을 주도하는 현재 트렌드에 대한 중요한 인사이트를 제공합니다.

## 주요결과 :

- **멀티 클라우드 선호도:** 대다수의 조직(78%)이 유연성, 제어 및 다양한 클라우드 서비스의 고유한 이점을 결합하기 위해 하이브리드 및 멀티 클라우드 전략을 선택합니다.
- **클라우드 도입 장벽:** 보안 및 규정 준수 문제(59%)는 멀티 클라우드 전략의 빠른 도입을 가로막는 중요한 장애물입니다. 기술적 문제(52%)와 리소스 제약(49%)은 복잡한 멀티 클라우드 인프라 내에서 가시성과 정책 제어를 달성하는 데 상당한 어려움을 야기하며 강력한 클라우드 보안 전문 지식의 필요성을 강조합니다.
- **사이버 보안 인재 부족:** 응답자의 93%가 복잡한 멀티클라우드 환경을 보호할 자격을 갖춘 전문가를 찾는 데 어려움을 겪고 있다고 답할 정도로 기업은 사이버 보안 전문 인력 부족에 심각하게 직면해 있습니다. 이는 기업의 보안 태세와 전략적 노력에 직접적인 영향을 미칩니다. 이처럼 클라우드 보안 전문 지식의 지속적인 부족은 멀티 클라우드 전략을 더 빠르고 광범위하게 채택하는 데 방해가 됩니다.
- **통합 클라우드 보안 플랫폼 선호도:** 응답자의 95%는 클라우드 환경 전반에서 보안을 간소화하기 위해 단일 플랫폼을 선호합니다. 이는 보안 관리를 간소화 및 자동화하고, 인력 격차를 완화하며, 일관된 정책 시행 및 가시성을 통해 보안을 강화하여 여러 개의 서로 다른 보안 시스템을 관리하는 데 따른 비효율성을 해소하기 위함입니다.



▶ What is your organization's primary strategy for cloud deployment?



Hybrid cloud

43%



Multi-cloud

35%



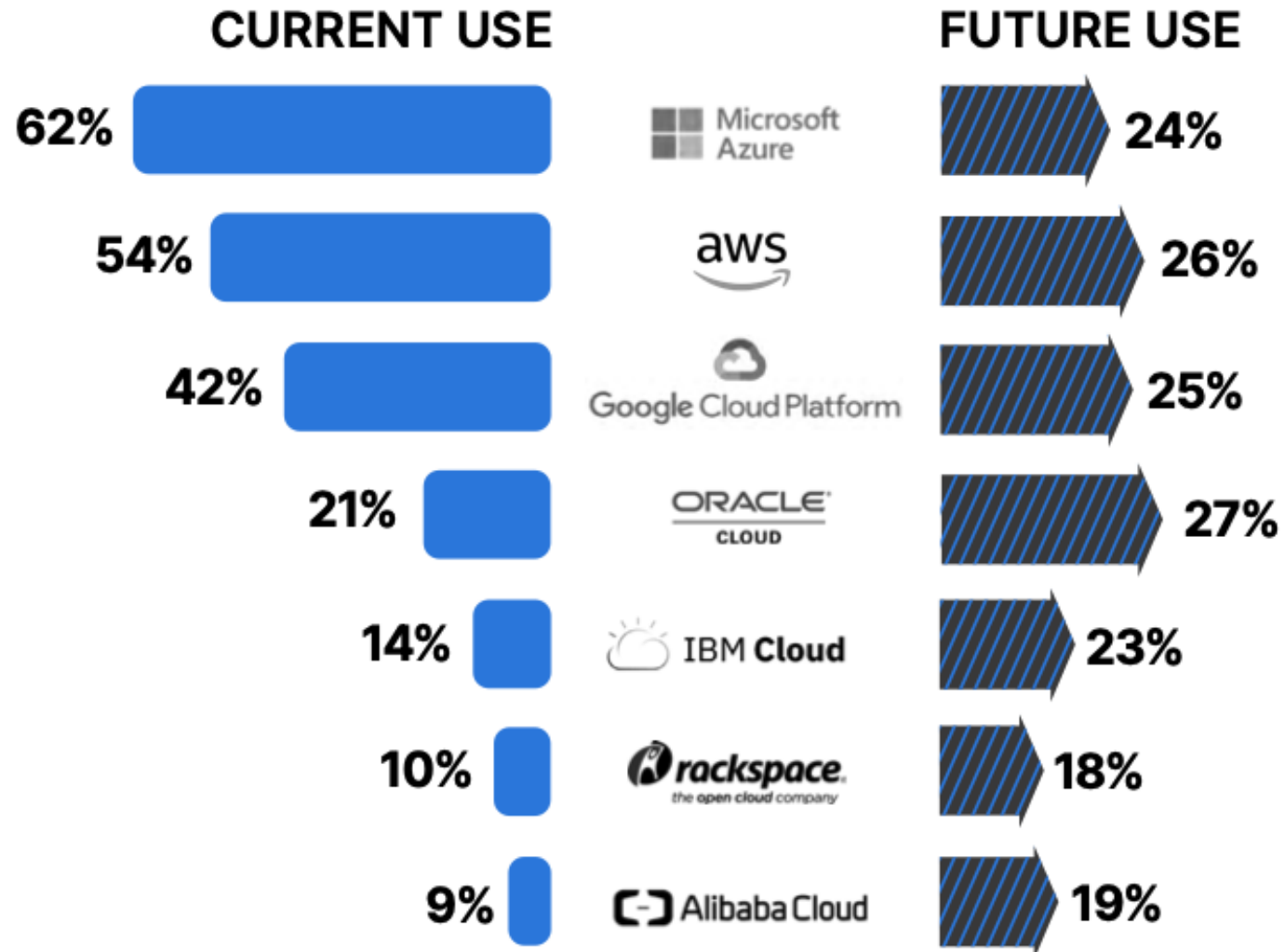
Single cloud

22%

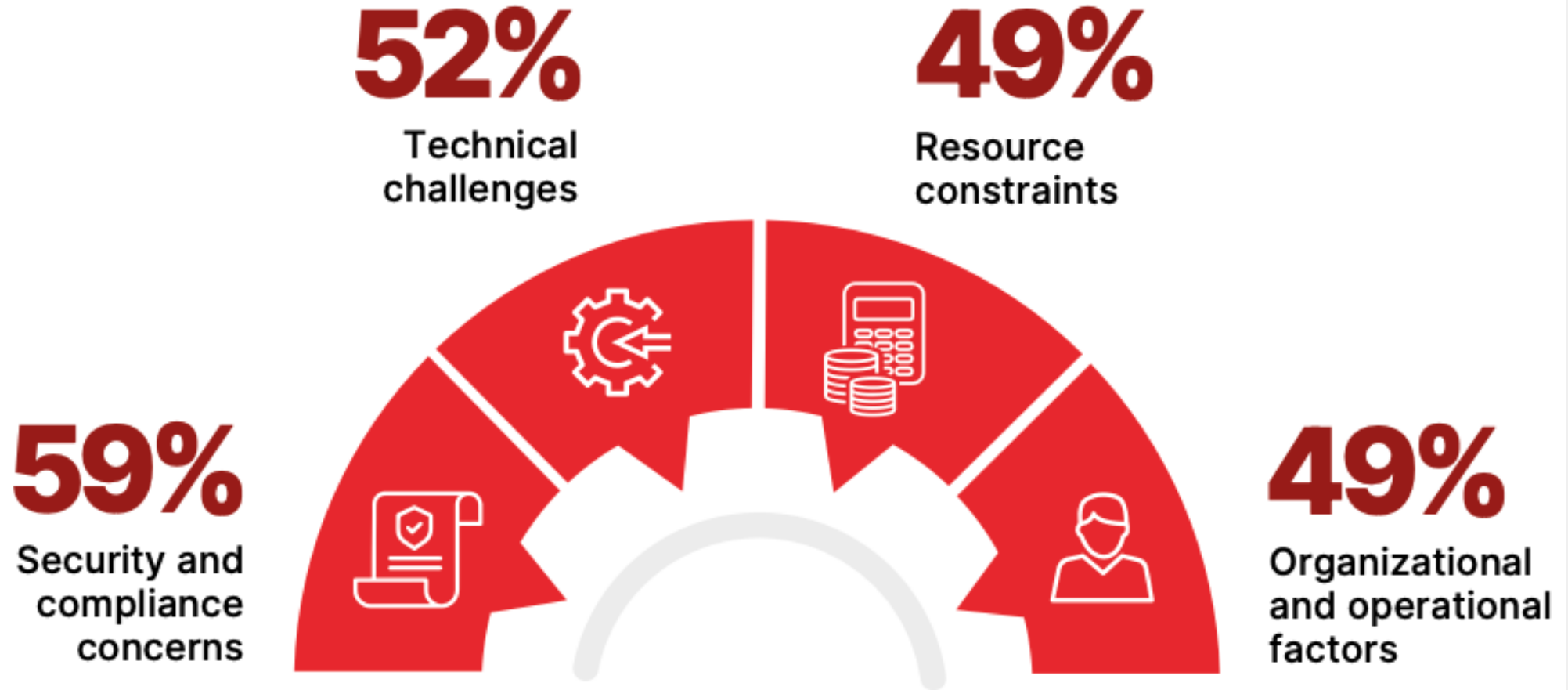
---

**78%** of organizations are using a multi-cloud or hybrid environment

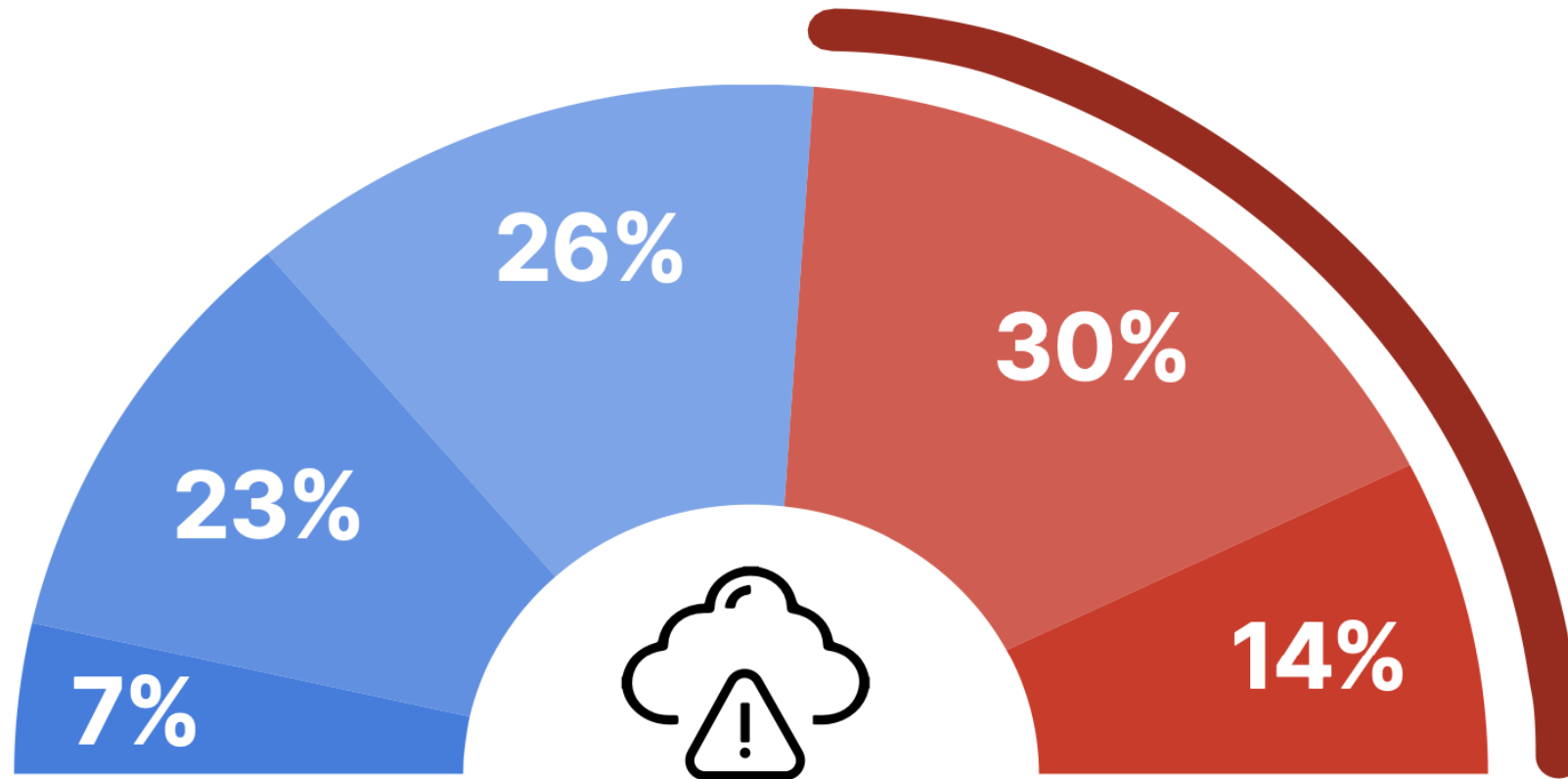
▶ What cloud IaaS provider(s) do you currently use or plan to use in the future?  
(select all that apply)



► **What are the primary barriers to cloud adoption in your organization?**  
(select all that apply)



▶ Compared to traditional, on-premises IT environments, would you say the risk of security breaches in a public cloud environment is higher or lower?



**44%**  
say public cloud risk is somewhat to significantly higher than on-premises

Significantly lower

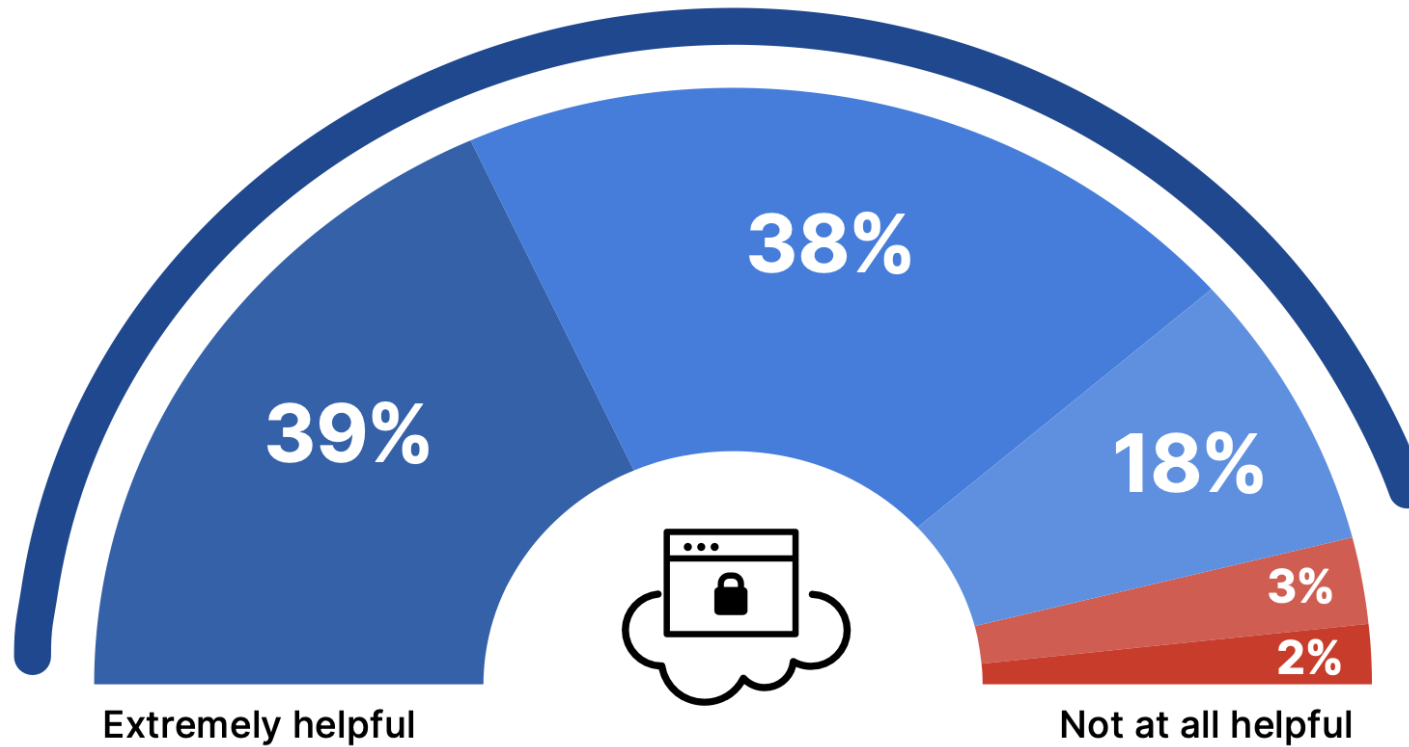
Significantly higher

■ Significantly lower   ■ Somewhat lower   ■ About the same   ■ Somewhat higher   ■ Significantly higher



▶ How helpful would it be to have a single cloud security platform with a single dashboard where you could configure all of the policies needed to protect data consistently and comprehensively across your cloud footprint?

**95%** of professionals consider the use of a single cloud security platform with a single dashboard to be moderately to extremely helpful



■ Extremely helpful   ■ Very helpful   ■ Moderately helpful   ■ Slightly helpful   ■ Not at all helpful





**Fortinet**



# 어디서나 사용자, 기기와 데이터를 보호하세요.

포티넷은 20년 이상 사이버 보안의 발전과 네트워크와 보안의 융합에 앞장섰습니다. 포티넷 보안 솔루션은 가장 많이 배포되었으며, 가장 많은 특허 출원을 통해 업계에서 가장 많은 검증을 거쳤습니다.

글로벌 기반  
**63.5만+**  
고객사

2023년 매출액  
**\$53억**  
(2023년 12월 31일 기준)

시가총액  
**\$540억**  
(2024년 2월 12일 기준)

광범위한 통합 포트폴리오  
**50개+**  
엔터프라이즈  
사이버 보안 제품

강력한 애널리스트 검증  
**33개**  
엔터프라이즈  
애널리스트 보고서 포함

업종 통합  
**\$10억+**  
ASIC에 대한 투자  
설계 및 개발

## FORTINET®

설립: 2000년 10월

설립자: Ken Xie 및 Michael Xie

본사 위치: 캘리포니아주 서니베일

포티넷 IPO(FTNT): 2009년 11월

상장: NASDAQ 100 및 S&P 500

편입 지수: 2022년 Dow Jones Sustainability World 및 North America 지수



# SD-WAN 분야의 압도적인 경쟁력

## Gartner SD-WAN MQ

Sep. 2024 Magic Quadrant for SD-WAN

**Fortinet Recognized as a Leader**  
**Five Years in a Row**

Figure 1: Magic Quadrant for SD-WAN



## Forrester SASE/ZTE Wave

Aug. 2023 Forrester Wave  
Zero Trust Edge Solutions

**Fortinet Recognized as a Leader**



## Gartner Peer Insights Customers' Choice

March 2024 Gartner SD-WAN Peer Insights

**Fortinet Receives Customers' Choice**  
**Five Years in a Row**



# 포티넷 시큐리티 패브릭 플랫폼

사이버시큐리티, 필요한 모든 곳에서





## Secure Networking

보안과 네트워킹을 통합하여 모든 에지와 장치를 보호



**1. 엔터프라이즈 방화벽**  
가트너가 평가한 업계 최고의 차세대 방화벽



**2. 보안 스위치**  
우수한 가시성과 NAC 기술을 내장한 매니지드 보안, 고성능 보안 스위치



**2. 무선 AP**  
우수한 무선 품질과 가시성, 사용자별 무선 접속 솔루션



**3. Rugged 제품 - OT보안**  
OT 등 혹독한 환경에서도 사용할 수 있는 Rugged 타입의 방화벽, 스위치, AP, 디셋터 등



**4. FG/FortiLAN 클라우드**  
SaaS 형태로 제공되는 다양한 포티넷 제품에 대한 원격 관리 서비스



**5. 통합 정책 관리 매니저**  
포티넷 제품 대상의 중앙 집중형 보안 정책 관리 및 프로비저닝 솔루션



**6. AIOps**  
AI와 ML 기술을 이용한 포티넷 유무선 서비스 및 SD-WAN 네트워크 품질 관리 솔루션



**7. 사용자 인증 관리**  
중앙 인증 관리 솔루션 (MFA, 로컬, AD / LDAP 연동, Radius 인증, SAML)



**8. 2FA 토큰**  
일회성 비밀번호 생성 및 푸시 알림 솔루션



**9. 트래픽 시뮬레이터**  
성능 시험 및 보안 테스트 (BAS, Breach Attack Simulation) 솔루션



**10. 개발자 FNDN**  
포티넷 제품 API 개발 정보와 툴을 제공하는 유료 개발자 커뮤니티 서비스



**11. 포티가드 시큐리티 서비스에서 제공하는 시그니처 업데이트 서비스**

- IPS 침입 탐지 방지
- AV 안티 바이러스 (악성코드 방지)
- 웹 URL 데이터베이스
- 안티 봇넷, C&C
- Geo IP 위치 정보
- 웹 방화벽 룰
- 클라우드 / 온-프레미스 샌드박스
- OT 산업용 프로토콜 분석
- IoT 사물인터넷 기기 탐지



## Unified SASE

어디서나 사용자와 기기와 애플리케이션을 보호



**12. SASE**  
원격 근무지 및 사용자의 접속 위치에 상관없이 사이버 공격으로부터 뛰어난 보호를 제공하는 클라우드 보안 솔루션



**13. 제로 트러스트 네트워크 접속 보안 ZTNA**  
원격 접속 제어, 애플리케이션 접속 정책과 단말기 리스크 제거를 위한 제로 트러스트 엔드포인트



**14. FortiClient - 패브릭 에이전트**  
엔드포인트 단말기 정보, IPSec / SSL VPN 접속 에이전트



**15. 시큐어 SD-WAN 솔루션**  
애플리케이션 기반의 NGFW 보안과 SD (Software Defined)-WAN 통합 솔루션



**16. 디지털 서비스 품질 모니터링 (DEM)**  
클라우드 워크로드 서비스와 온-프레미스 인프라의 성능 저하 및 장애 상태 모니터링 솔루션



**17. 시큐어 웹 게이트웨이**  
URL 프록시 서비스, 클라우드 워크로드에 대한 테넌트별 접속 제어 등의 애플리케이션 통제 솔루션



**18. 원격 브라우저 격리, RBI**  
웹 브라우저를 통한 악성코드 유입 차단하는 ATP 솔루션



**19. 방화벽 가상머신, FG-VM**  
퍼블릭 클라우드와 프라이빗 클라우드 워크로드 보호를 위한 가상머신 VM 방화벽



**20. 웹 방화벽, API 보안**  
OWASP 및 웹 API 애플리케이션 공격 탐지 및 방어 솔루션



**21. 클라우드 네이티브 방화벽 CNF for AWS**  
클라우드 네이티브, AWS 방화벽 매니저 서비스와 연동 지원하는 포티게이트 NGFW 방화벽, IPS 솔루션



**22. CASB**  
SaaS 애플리케이션 설정 오류로 인한 보안 홀과 데이터 유출 그리고 컴플라이언스 준수 여부 검사를 위한 SaaS 서비스



## Security Operations

SI 기반 보안 운영으로 대규모 위협을 탐지, 조사 및 대응



**23. 샌드박스**  
알려지지 않은 악성코드 탐지용 샌드박스 솔루션



**24. 이메일 보안 게이트웨이**  
시큐어 이메일 서버 및 게이트웨이를 통한 이메일 보안 솔루션



**25. EndPoint 탐지 및 대응, EDR**  
자동화된 엔드포인트 보호 및 인시던트 대응 관리 솔루션



**26. 악성코드 NDR**  
SI와 ML기술을 이용한 대용량 초고속 악성코드 탐지 솔루션



**27. 접근 관리 솔루션, PAM**  
OT 인프라 환경과 같은 보안수준이 높은 시스템 접속 사용자 접근 권한 관리 시스템



**28. 사이버 디셉션**  
허니팟 한계를 넘어서는 액티브한 보안 침입 탐지용 디셉션 솔루션



**29. 피싱 메일 시뮬레이션**  
실제 피싱 기술 기반으로 직원들에 대한 피싱 테스트



**30. 통합 로그 관리 솔루션**  
포티넷 제품 보안 로그 연관 관계 분석, 리포트 및 저장 관리 솔루션



**31. 보안 정보 및 이벤트 관리, SIEM**  
SIM(보안 정보 관리)과 SEM(보안 이벤트 관리) 솔루션



**32. 보안 오케스트레이션, 자동화 및 대응, SOAR**  
IT 인프라 보안 업무 프로세스 자동화 솔루션



**33. 디지털 리스크 보호 서비스, DRPS**  
기업의 브랜드 리스크 관리, 자산 및 데이터 보호 솔루션



**34. 클라우드 네이티브 프로텍션 CNP**  
멀티-클라우드 워크로드의 보안 위험과 컴플라이언스 준수 여부를 통합 관리 솔루션



**35. 동적 애플리케이션 보안 테스트, DAST**  
웹 애플리케이션의 동적 보안 테스트를 수행하여 공격자가 악용할 수 있는 취약성을 식별



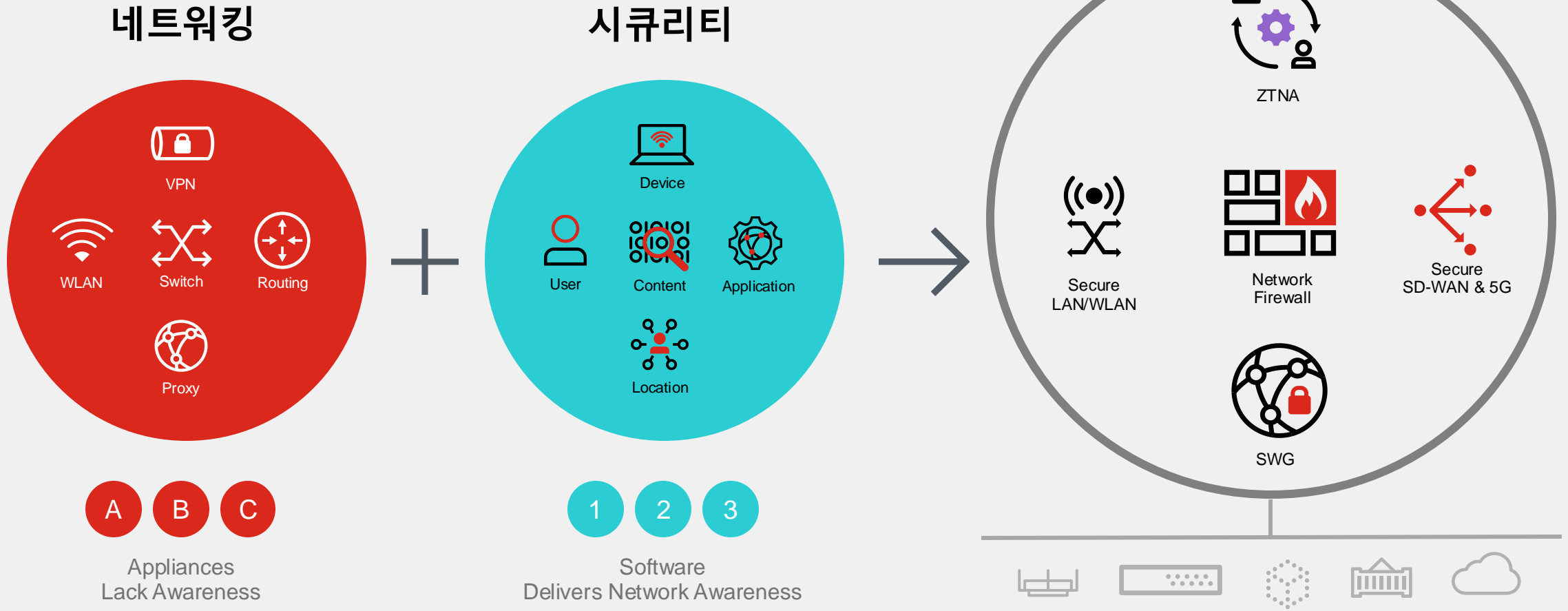
# FortiGate와 FortiOS



# 포티넷이 제안하는 컨버전스 접근방식

보안 기반 네트워킹으로 일관된 컨버전스 가능

## 보안 기반 네트워킹

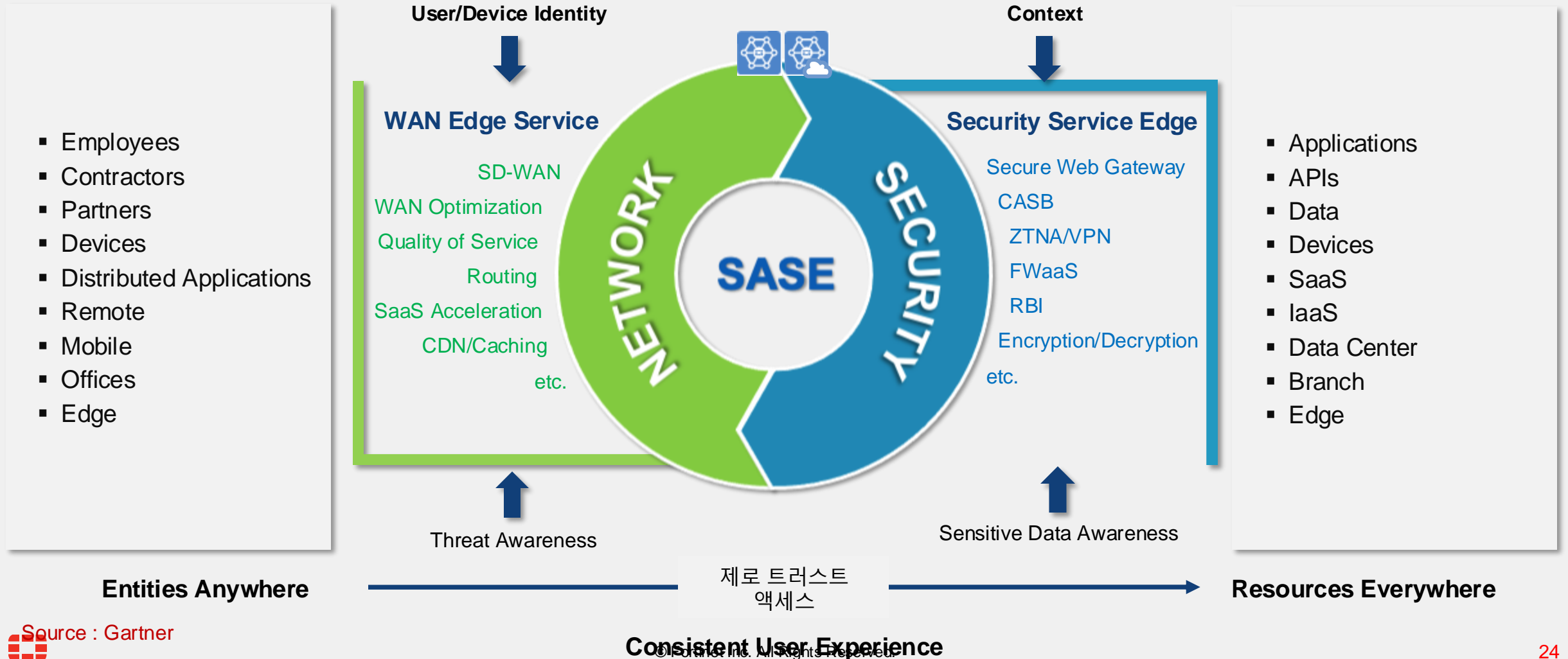


# 보안을 강화하기 위한 SASE 등장

어디서나 업무 할 수 있는 클라우드 제공 네트워크 및 보안 통합 솔루션

Gartner

일관성 있는 네트워크 및 보안 정책





# FortiOS를 중심으로 하는 보안 플랫폼 전략

중앙집중식 관리 . 분석

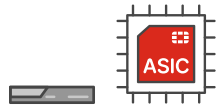


FortiManager



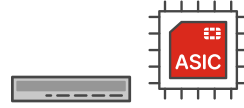
FortiAnalyzer

소규모



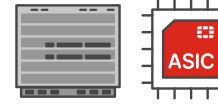
FortiGate  
40-90 Series

중간규모



FortiGate  
100-900 Series

대규모 / 데이터센터



FortiGate  
1000-7000 Series

VM / 클라우드 / FWaaS



Networking Operating System Everywhere



Firewall



VPN



NGFW



Segmentation



Distributed  
NGFW



DDoS



Low  
Latency



Integrated  
W/LAN



5G/LTE



HW SSL  
Inspection



Secure  
SD-WAN



Hyperscale



ZTNA



FortiGuard Labs  
AI-Powered  
Threat Intelligence

Device  
Security



North/South Inspection  
East/West Inspection  
SSL Inspection

Content  
Security



Anti-malware  
Detect Malicious Files

Web  
Security



Stop DNS-based Attacks  
Block Malicious URLs

Content  
Security

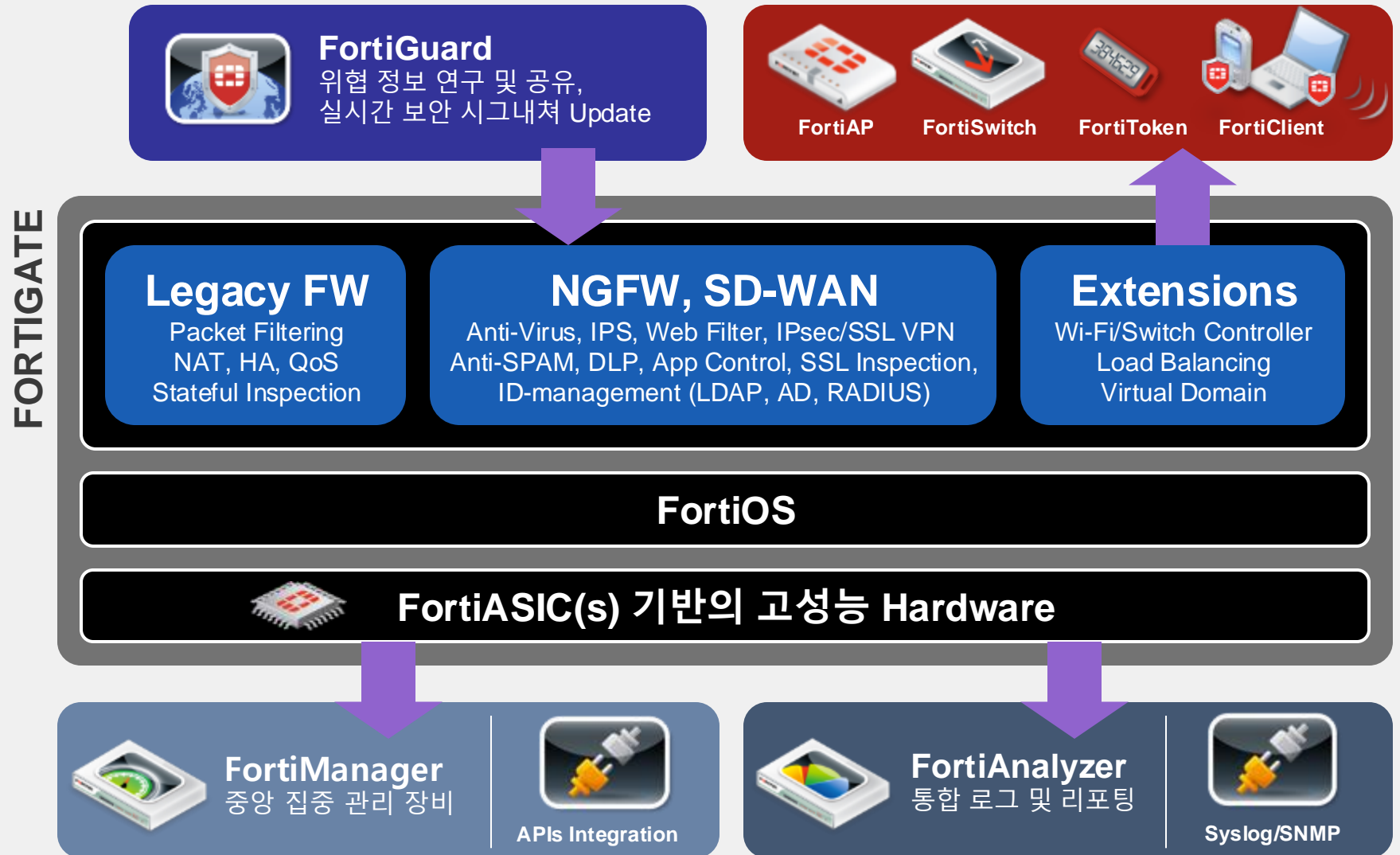


Prevent Data  
Exfiltration



# FortiGate – NGFW & SD-WAN

FortiGate는 자체 설계한 ASIC 기반의 **고성능 Hardware** 구조에, **최신 보안 위협 정보와 시그내쳐**를 통해 고객 비즈니스를 보호하며, **고도의 제어와 가시성**을 제공합니다.





# 전용 ASIC 기반의 고성능/저지연 방화벽

국산 등 경쟁사 방화벽  
아키텍처 멀티 CPU 최적화

## CPU Only

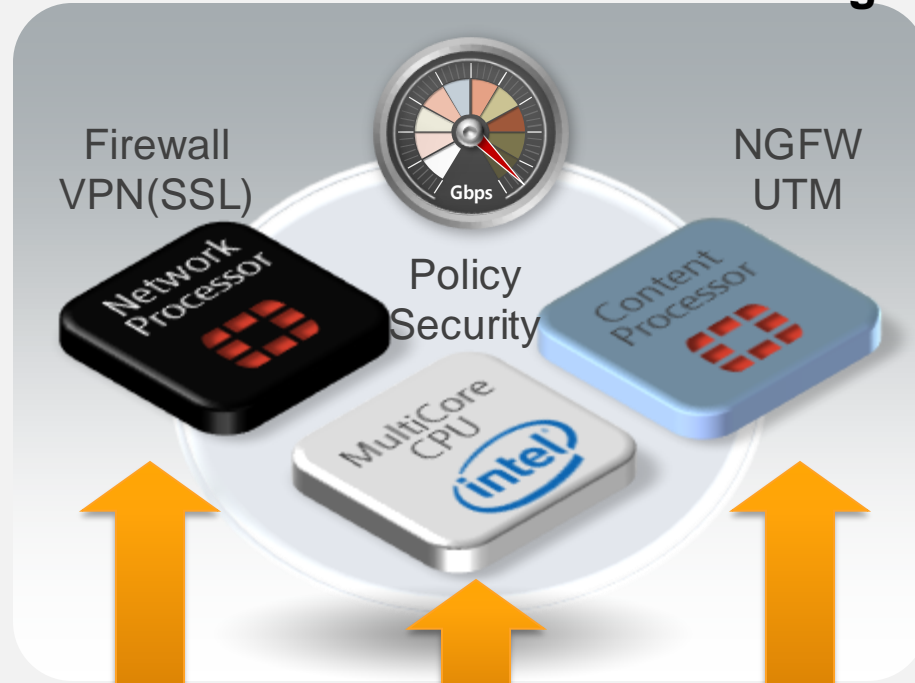


**CPU**  
방화벽 정책, 콘텐츠  
검사, 암호화 및 패킷  
처리

## 포티넷 방화벽 아키텍처

전용 ASIC 하드웨어 칩과 멀티 CPU 최적화  
방화벽 Latency 최소화 (2~3 $\mu$ s)

## Fortinet Parallel Path Processing



**Network Processor**  
방화벽 정책과 VPN  
트래픽의 H/W 가속

**CPU**  
방화벽  
정책 처리

**Content Processor**  
콘텐츠 검사 및 암호화  
H/W 가속



성능 개선



지연 감소



공간 절약



적은 전력





# FortiGate 120% 활용하기- Application control

일반 레거시 방화벽 기능도 좋지만, Application기반의 차세대 방화벽 기능을 사용해보세요.  
로그부터 달라집니다

The screenshot displays the FortiGate Application Control interface. On the left is a navigation menu with 'Application Signatures' highlighted. The main area features three donut charts: 'Category' (8019 Total), 'Technology' (8178 Total), and 'Risk' (8018 Total). Below these is a table of application signatures. A search bar is highlighted with a red dashed box.

Name	Category	Technology	Popularity	Risk
<b>Custom Application Signature 1</b>				
Windows.NT.6.3.Web.Surfing	Web Client			
<b>Application Signature 8,018</b>				
1kxun	Video/Audio	Client-Server	★★★★☆	■■■■□
1und1.Mail	Email	Browser-Based	★★★★☆	■■■■□

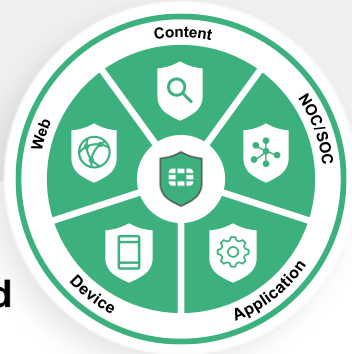
Priority	Details	Type	Action
1	KakaoTalk KakaoTalk_File.Transfer KakaoTalk_Voice.Chat	Application	Block
2	Instagram_File.Upload Instagram_Post	Application	Block
3	Naver.Mail_Attachment Naver.Mail_Send Naver.Cafe Naver.Mybox_Upload	Application	Block
4	Amazon.AWS_S3.Download Amazon.AWS_S3.Upload Amazon.AWS_S3	Application	Block





# FortiGate 120% 활용하기- FortiGaurd

옛날부터 지금까지도 변하지 않는 보안의 핵심 중에 하나는 TI(Threat Intelligence)를 활용하는 것입니다. AI 기반의 FortiGuard LABs의 TI 서비스를 활용하여 IPS,AV,Bot,URL,DNS등의 위협에 대한 다양한 보안 서비스를 활용해 보세요



## FortiGuard

### Content Security



### Web Security



### Device Security



### NOC/SOC

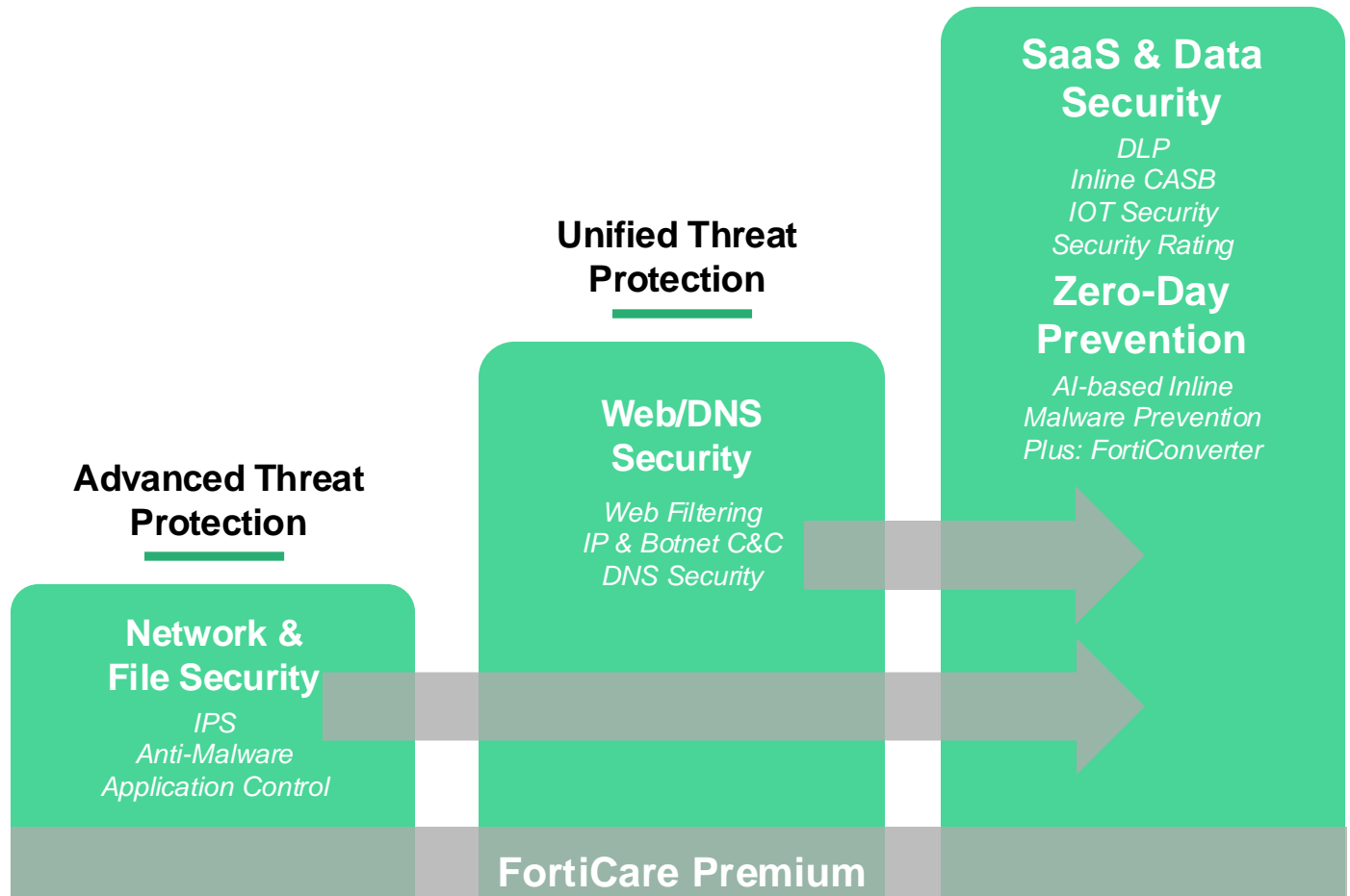


### Application Security



## FortiGate Bundles

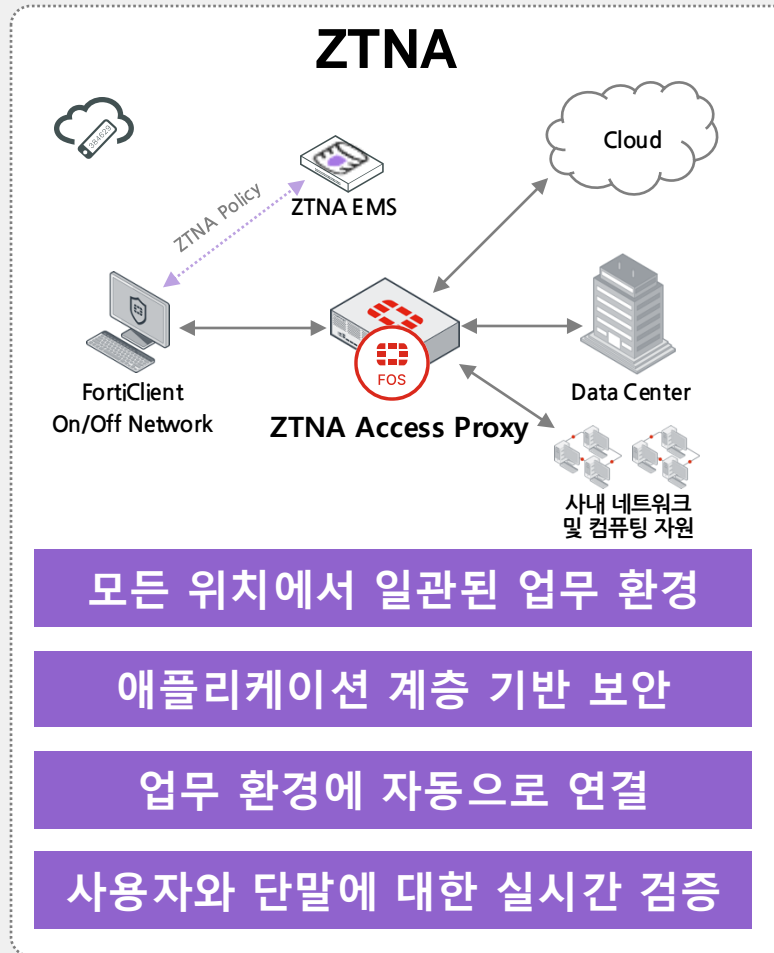
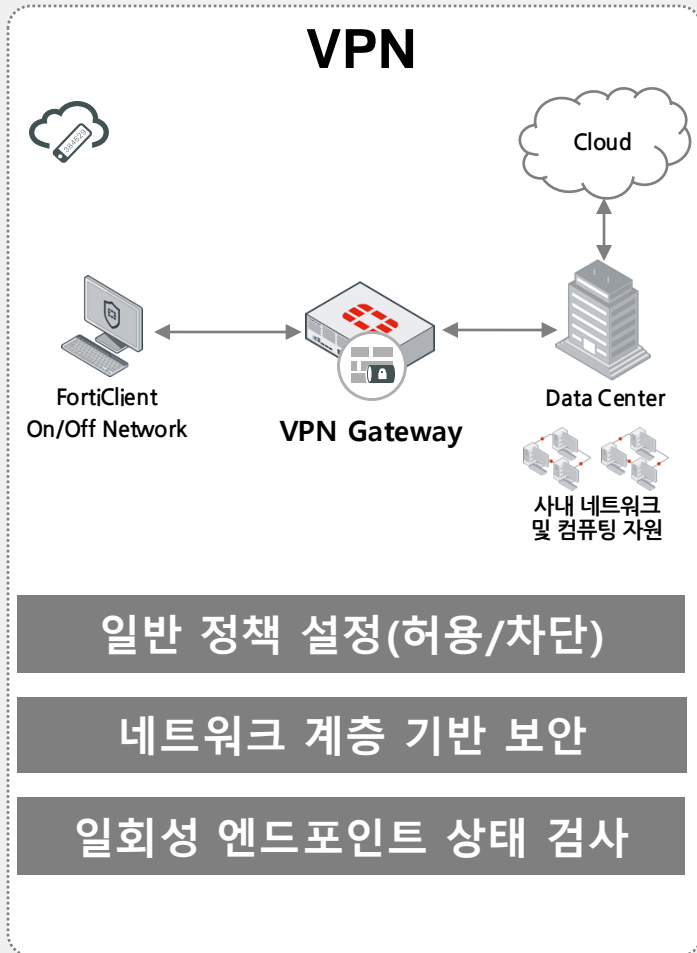
**NEW Enterprise Protection**





# FortiGate 120% 활용하기- ZTNA

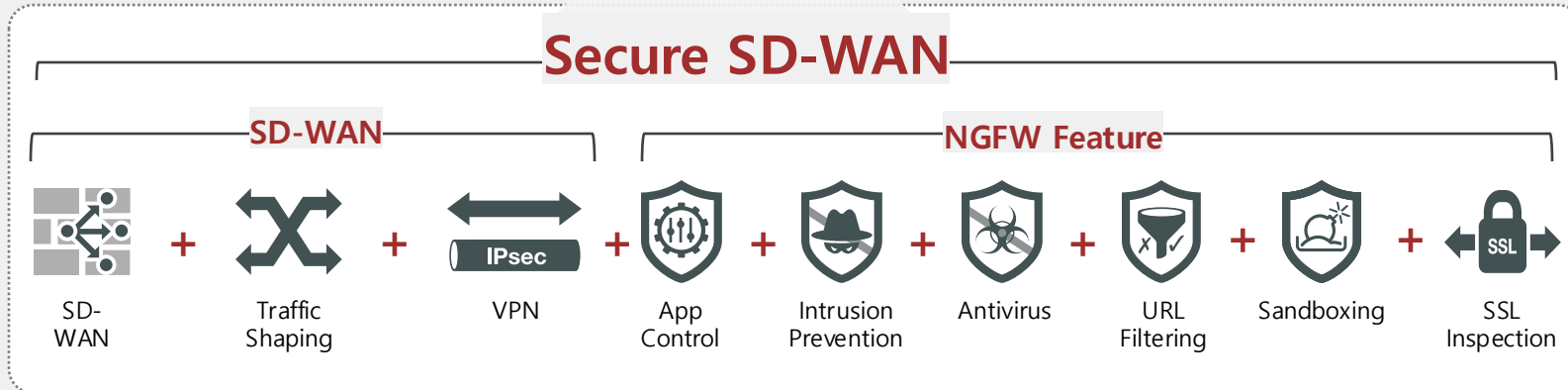
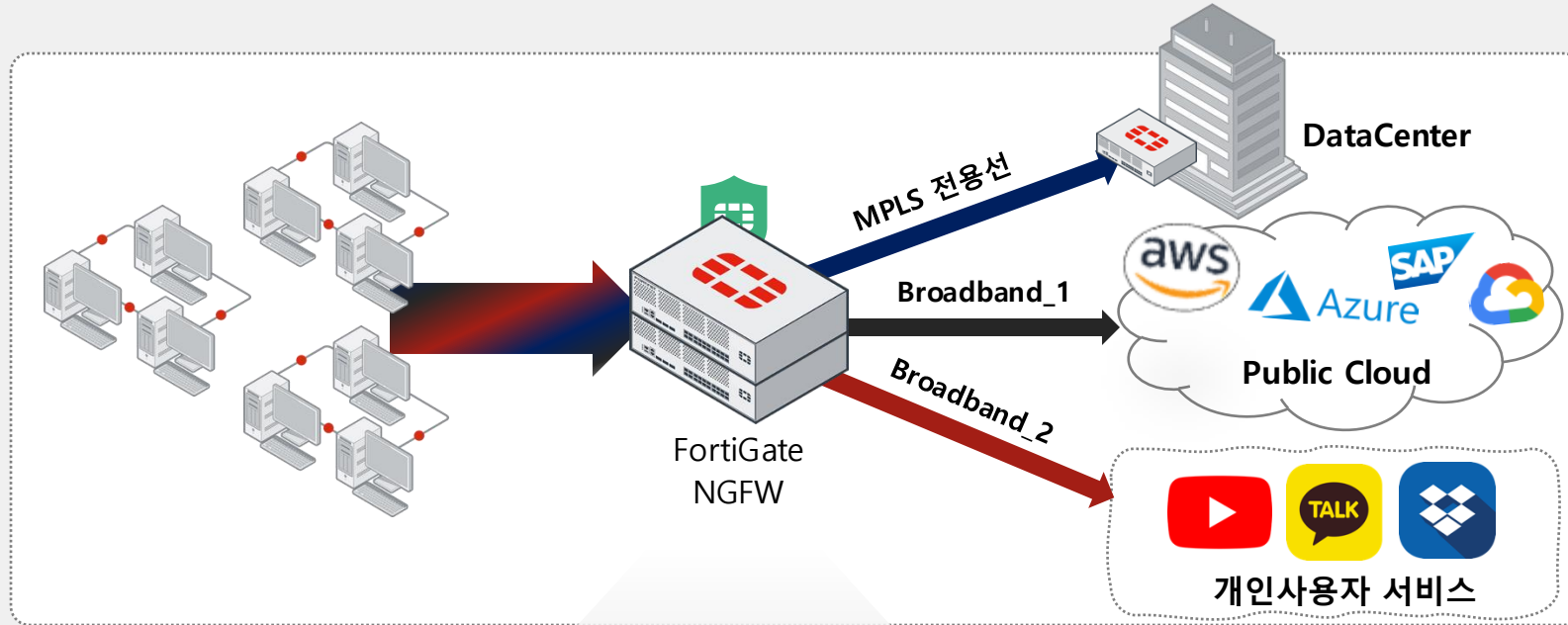
SSLVPN 기능을 쓰고 계신다면 제로트러스트 수준의 ZTNA 에이전트 기능도 활용해 보세요





# FortiGate 120% 활용하기- Secure SD-WAN

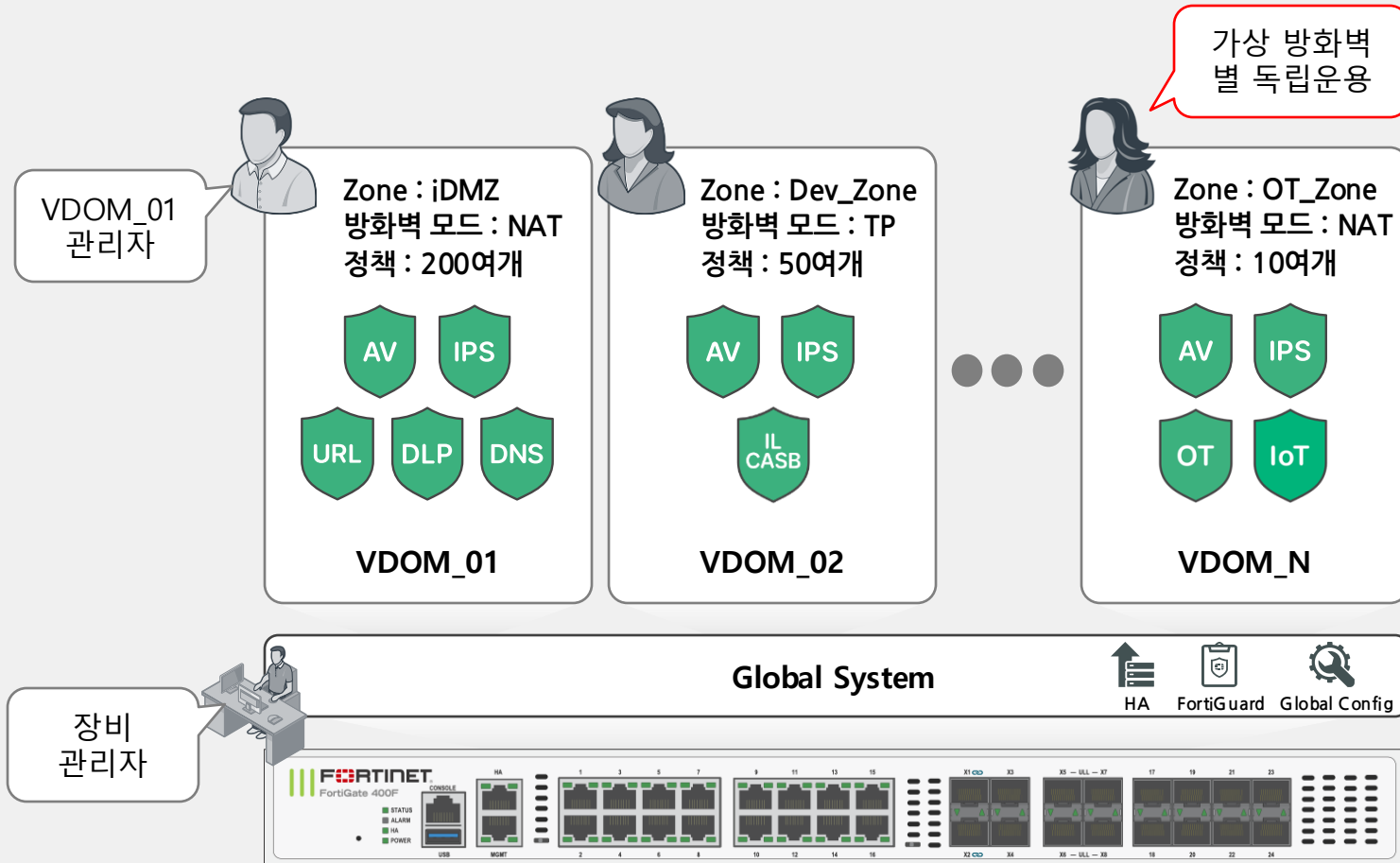
IPSec VPN 기능으로 여러 지점과 연결 되어 있다면, SD-WAN 기능을 무상으로 꼭 써보셔야 합니다





# FortiGate 120% 활용하기- 자체 가상화(VDOM)

다양한 포티넷 제품을 사용 하신다면 무상으로 모니터링 가능한 대쉬보드 제공기능 알고 계셨나요?

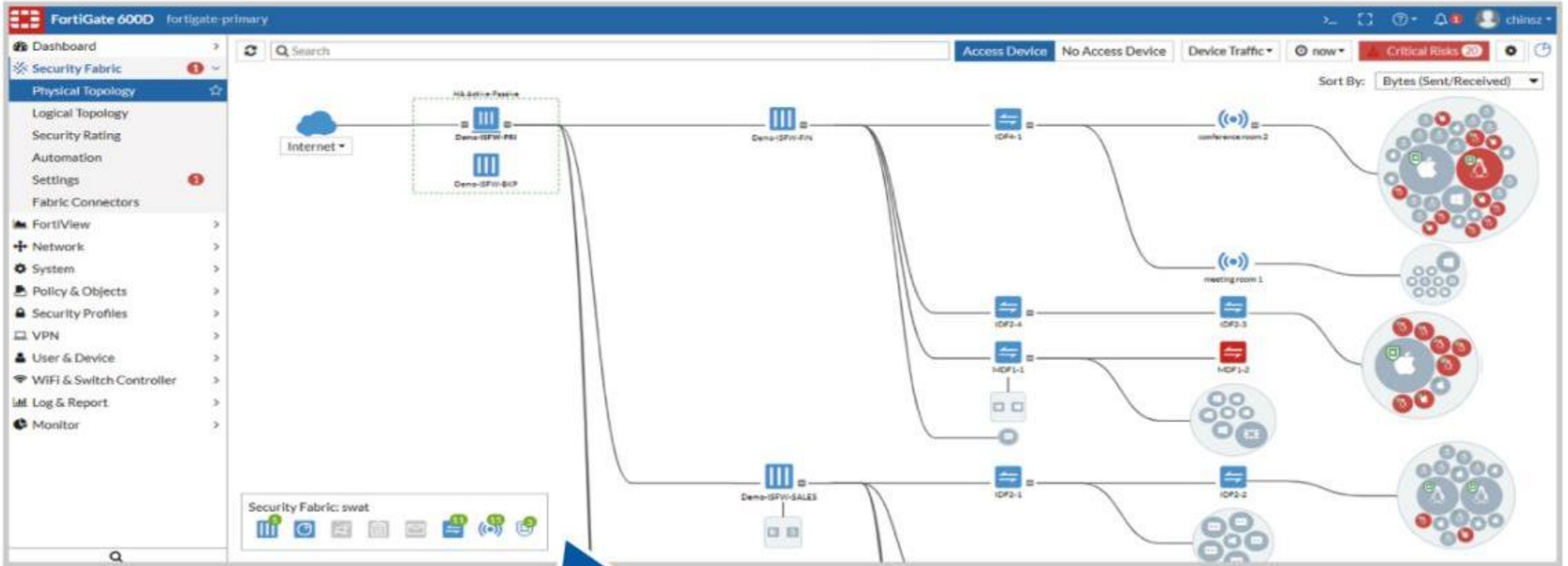






# FortiGate 120% 활용하기- 네트워크 가시성 대쉬보드

하나의 물리적인 방화벽을 여러대의 가상화 방화벽으로 설정하여, 무상으로 망분리 수준의



본사, IDC, 지사 및 영업점이나 원격 사무실 등을 한눈에!  
각 사무실의 전체 네트워크 현황을 한눈에!



# FortiGate 120% 활용하기- 운영 자동화 기능

FortiGate에서 특정 이벤트가 발생 하였을 때 Email/SMS 발송, 자동격리 등의 자동화 기능, 알고 계셨나요?



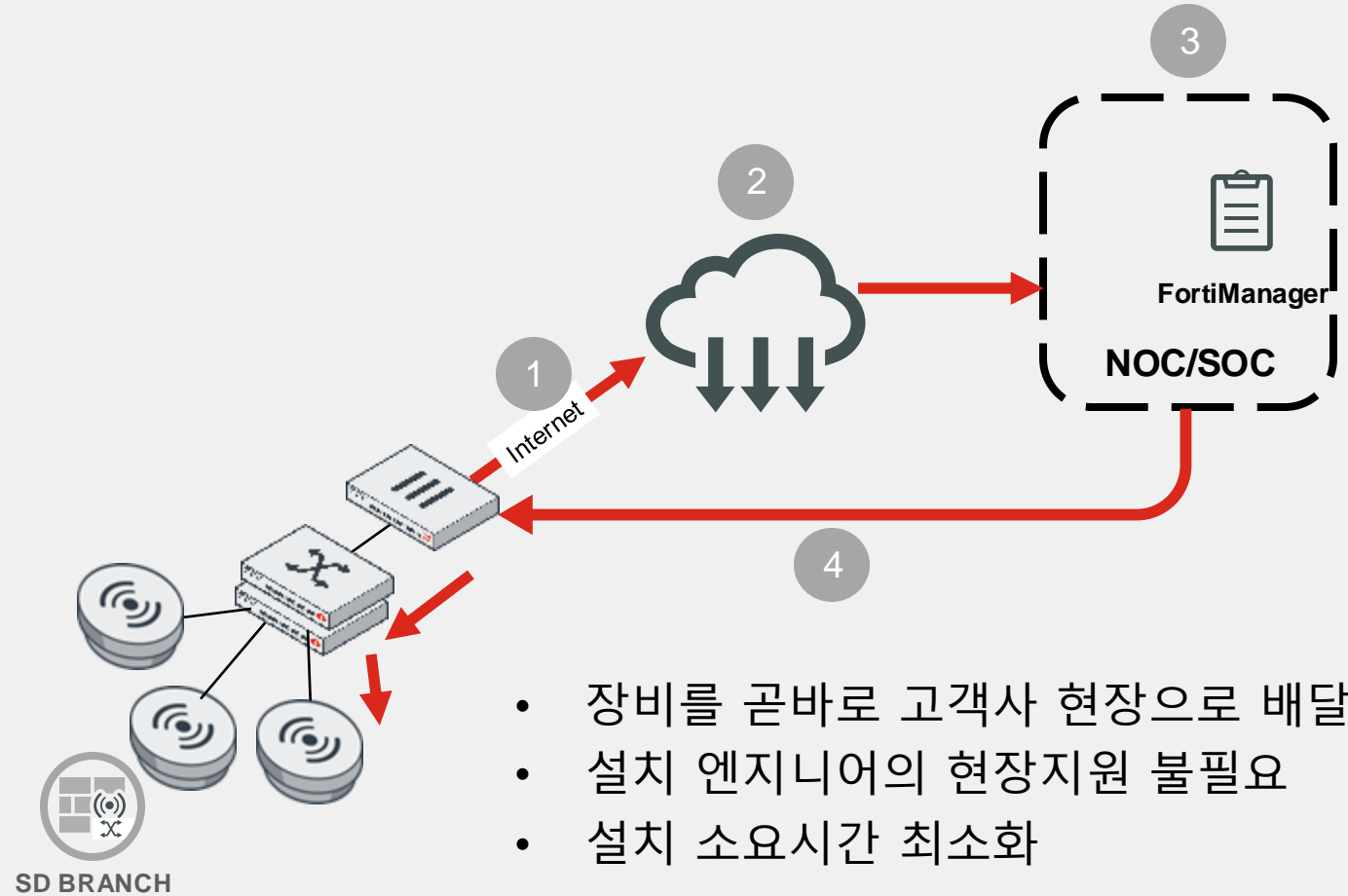
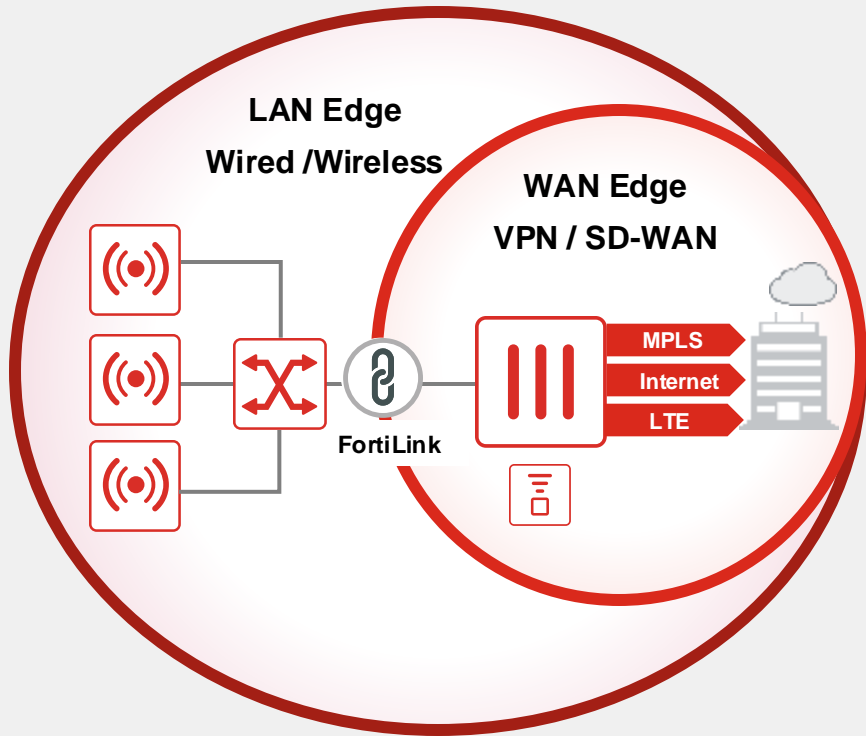
Name	Details
Anomaly Logs	An anomaly...
AV & IPS DB Update	AV & IPS DB update
Compromised Host	The an...
Configuration Change	
Conserve Mode	
Fabric Connector Event	
FDC_IP_BAN	EVENT insider_threat OT_Deceptor_KR_CBC
FortiOS Event Log	
Admin Login	Admin login successful
Auto Firmware upgrade	A federated upgrade was completed by the root FortiGate A federated upgrade could not be completed by the root Forti... Automatic firmware upgrade schedule changed
FortiAnalyzer Connection Down	FortiAnalyzer connection down
Network Down	Interface status changed
HA Fallover	
High CPU	
High CPU	
Incoming Webhook	
Incoming Webhook Call	
IPS Logs	
IPS Logs	
License Expiry	
Local Certificate Expiry	
Reboot	
Schedule	
Weekly Trigger	FWM Weekly

Name	Details	Trigger Count
Access Layer Quarantine		0
>_ CLI Script		0
>_ CLI Script - System Status		0
Email		0
Email Notification	to: yooj@fortinet.com	0
FortiClient Quarantine		0
FortiClient Quarantine		0
FortiExplorer Notification		0
FortiExplorer Notification		0
FortiNAC Quarantine		0
FortiNAC Quarantine		0
IP Ban		74
IP Ban		74
System Action		0
Backup Config Disk	ACTN Backup configuration	0
Reboot FortiGate	ACTN Reboot	0
Shutdown FortiGate	ACTN Shutdown	0





# FortiGate 120% 활용하기- ZTP



- 장비를 곧바로 고객사 현장으로 배달
- 설치 엔지니어의 현장지원 불필요
- 설치 소요시간 최소화



# Customer Briefing Center

## 포티넷 CBC 고객 솔루션 체험 센터

전세계 TOP3 사이버 보안 벤더인 포티넷에서 국내 고객 분들을 위해 마련한 솔루션 체험 센터로 방문하시는 고객분들의 요구사항에 따라 맞춤형 컨설팅을 제공합니다.



보안 중심 네트워크



다이나믹 클라우드 보안



AI 기반 보안 관제



제로 트러스트 액세스

### ✓ 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](http://www.fortinet-vcbc.com)

[www.fortinet.com/kr/corporate/cbc](http://www.fortinet.com/kr/corporate/cbc)



CBC 방문 신청하기



Virtual CBC 바로가기



# 감사합니다.



스크린 화면 또는 포티넷 부스의  
QR 코드 스캔을 통해  
설문 참여 부탁드립니다.

