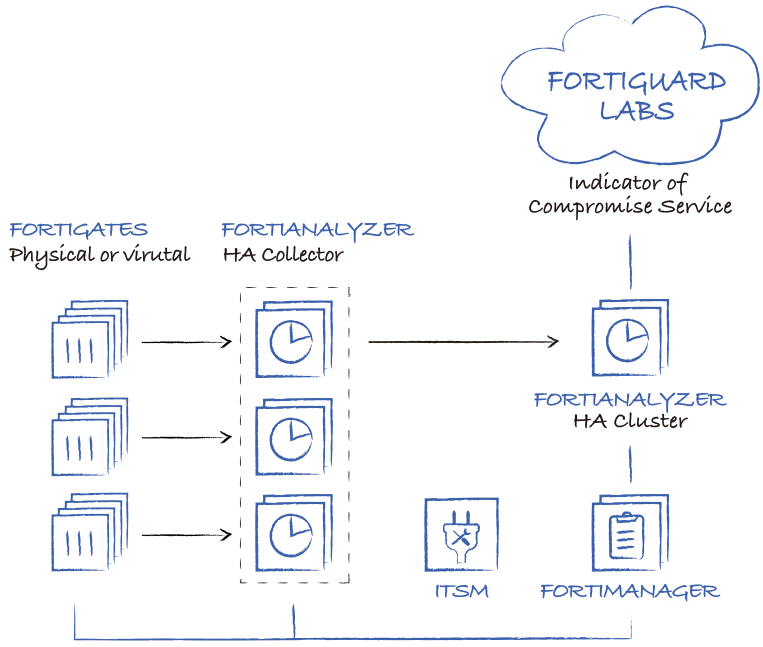
DATA SHEET

FortiAnalyzer

보안 중심의 분석 및 로그 관리

FortiAnalyzer는 전체 공격면에 대한 **단일 대시보드 오케스트레이션, 자동화 및 응답**을 통해 위험을 줄이고 조직의 전반적인 보안을 개선함으로써 지능형 위협에 대한 깊이 있는 통찰력을 제공합니다.

Fortinet의 보안 패브릭과 통합된 FortiAnalyzer는 공격면을 넓히는 최근의 새로운 기술들을 좀 더 간편하게 분석하고 모니터링할 수 있게 해주며 종합적인 가시성을 제공함으로써 위협을 식별하고 제거할 수 있게 도와줍니다.



지능형 위협 탐지 및 상관관계는 보안 및 네트워크 팀이 인프라 전반의 네트워크 보안 위협을 즉각적으로 식별하고 대응할 수 있도록 해줍니다.

자동화된 워크플로 및 규정 준수 보고서는 보안 및 네트워크 팀이 워크플로를 가속화하고 규정 준수 감사에 도움을 줄 수 있도록 맞춤형 대시보드, 보고서, 고급 워크플로 핸들러를 제공합니다.

확장 가능한 로그 관리는 FortiGate, FortiClient, FortiManager, FortiSandbox, FortiMail, FortiWeb, FortiAuthenticator, Generic Syslog 등으로부터 로그를 수집합니다. 개별 단위로 또는 특정 작업에 최적화된 상태로 배포되며 보존 요구 사항에 따라 스토리지가 확장됩니다.

주요 기능

종합적인 가시성

- 이벤트 상관관계, 위협 탐지, IOC(Indicator of Compromise) 서비스가 위협을 탐지하고 식별하는 시간을 줄임

Fortinet 보안 패브릭 통합

- 더 심층적인 가시성과 중요한 네트워크 통찰력을 위해 FortiClient, FortiSandbox, FortiWeb, FortiMail의 로그와 상관관계 분석

엔터프라이즈급 고가용성

- 재해 복구를 위해 지리적으로 분산시킬 수 있는 FortiAnalyzer DB(최대 4노드 클러스터)를 자동으로 백업함

보안 자동화

- REST API, 스크립트, 커넥터 및 자동화 스티치를 통해 복잡성을 줄이고 자동화를 활용함으로써 보안 대응을 촉진함

멀티테넌시 및 관리 도메인(ADOM)

- 규정을 준수하고 효과적으로 작동하는 ADOM을 활용하여 고객 데이터를 분리하고 도메인을 관리함

유연한 배포 옵션 및 아카이브 스토리지

- 어플라이언스, VM, 호스티드 또는 클라우드의 배포를 지원함. AWS, Azure 또는 Google을 사용하여 로그를 보조 스토리지로 아카이브함

주요 기능

Security Operations Center (SOC)

FortiAnalyzers SOC 관리 센터는 로그 및 위협 데이터에 대해 실행 가능한 보기를 제공함으로써 전체 네트워크를 보호할 수 있게 도와줍니다. 보안 패브릭에 쉽게 통합할 수 있도록 단일 대시보드 인터페이스를 통해 제공되는 사전 정의된 맞춤형 대시보드를 사용하는 중앙 집중식 모니터링, 위협 인지, 이벤트 및 네트워크 활동을 통해 네트워크, 웹사이트, 애플리케이션, 데이터베이스, 서버, 데이터 센터를 보호하십시오.

사고 감지 및 대응

FortiAnalyzer의 자동화된 사고 대응 기능은 이벤트 관리와 손상된 엔드포인트 식별에 중점을 두고 관리 및 분석을 개선합니다. 향상된 기본 및 맞춤형 이벤트 핸들러를 사용하여 악의적인 활동과 의심되는 활동을 즉시 감지할 수 있습니다. 이벤트가 FOS 자동화 프레임워크와 통합되어 있어 엔드포인트 격리와 블랙리스트 IP 같은 작업이 자동화됩니다. ITSM 플랫폼과의 통합을 통해 사고 감지 및 추적은 물론 증거 수집 및 분석도 간소화되기 때문에 보안 운영 센터에서 간극을 해소하고 보안 태세를 강화하는 데 도움이 됩니다.

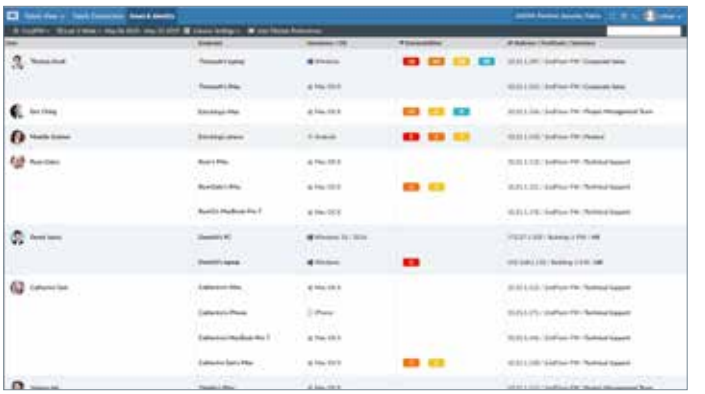
이벤트 핸들러는 빠른 감지, 자동화된 상관관계, 사고 관리와 연결된 교정을 통해 Fortinet 보안 패브릭 전반에서 로그 분석 및 위협 식별을 간소화합니다. FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox 장치 및 syslog 서버를 위한 이벤트 핸들러를 만드십시오.

로그에서 추출하고 이벤트에서 표시할 메시지를 정의하고 이메일 주소, Webhook, SNMP 커뮤니티 또는 syslog 서버를 통해 이벤트 핸들러에 대한 알림을 보내십시오.



침해 지표(Indicators of Compromise)

IOC(Indicators of Compromise) 요약은 의심스러운 웹 사용 위해를 최종 사용자에게 보여 줍니다. 최종 사용자의 IP 주소, 호스트 이름, 그룹, OS, 전체 위협 등급, 맵 보기, 위협 수 등의 정보가 제공되며 보기 위협 세부 정보로 드릴다운할 수 있습니다. 분석가들은 위협 탐지를 위해 과거 로그를 재검사하고 새로운 정보를 바탕으로 위협을 식별할 수 있습니다. IOC를 생성하기 위해 FortiAnalyzer는 각 최종 사용자의 웹 필터, DNS 및 트래픽 로그를 위협 데이터베이스와 대조합니다. 위협 일치가 발견되면 최종 사용자에게 위협 점수가 부여됩니다. FortiAnalyzer는 최종 사용자의 위협 점수를 집계하여 최종 사용자의 전반적인 IOC를 결정합니다. IOC 요약은 로컬 위협 데이터베이스를 FortiGuard 위협 데이터베이스와 동기화된 상태로 유지하기 위해 FortiGate 장치 및 FortiAnalyzer 서브스크립션부터 생성되며 FortiGuard에 전달됩니다.



보고서

FortiAnalyzer는 곧바로 사용할 수 있는 39개 이상의 기본 템플릿을 제공하며, 알맞은 보고서를 찾아내는 데 도움을 주는 샘플 보고서도 있습니다. 보고서 기능을 사용하여 로그로부터 맞춤형 데이터 보고서를 생성할 수 있습니다. 자동화된 이메일 알림, 업로드 및 관리하기 쉬운 달력 보기를 통해 필요할 때 또는 일정에 맞춰 보고서를 실행하십시오. 보고서를 작성할 때 바로 사용할 수 있는 300개가 넘는 기본 차트 및 데이터 세트로 맞춤형 보고서를 작성하십시오. PDF, HTML, CSV, XML 등 다양한 보고서 형식으로 작성할 수 있습니다.

주요 기능

타사 통합을 위한 로그 전달

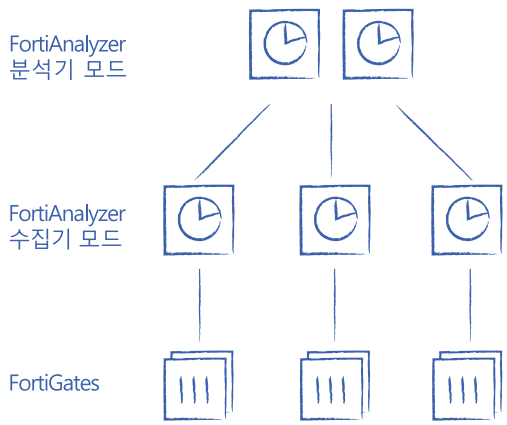
로그를 FortiAnalyzer 유닛에서 다른 FortiAnalyzer 유닛, syslog 서버 또는 CEF(Common Event Format) 서버로 전달할 수 있습니다. 클라이언트는 로그를 다른 장치로 전달하는 FortiAnalyzer 유닛입니다. 서버는 로그를 받는 FortiAnalyzer 유닛, syslog 서버 또는 CEF 서버입니다. 로그를 다른 유닛이나 서버로 전달하는 것 외에도 클라이언트는 로그의 복사본을 보존합니다. 로그의 로컬 복사본은 아카이브된 로그의 데이터 정책 설정을 따릅니다. 로그는 수신될 때 실시간으로 또는 거의 실시간에 가깝게 전달됩니다. 전달되는 콘텐츠 파일로는 DLP 파일, 안티바이러스 격리 파일, IPS 패킷 캡처가 있습니다.

분석기-수집기 모드

서로 다른 FortiAnalyzer 유닛에서 분석기 모드 및 수집기 모드로 배포하고 유닛이 서로 연동되어 로그 수신, 분석, 보고의 전반적인 성능을 향상시키도록 할 수 있습니다. FortiAnalyzer가 수집기 모드일 때는 연결된 장치의 로그를 분석기에 전달하고 로그를 아카이브하는 것이 기본 작업입니다. 분석기는 데이터 분석 및 보고서 생성에 집중할 수 있도록 로그 수신 작업을 수집기에 넘깁니다. 따라서 수집기의 로그 수신 성능이 극대화됩니다.

유연한 할당량 관리의 멀티테넌시

관리 도메인(ADOM)에 따른 시간 기반의 아카이브/분석 로그 데이터 정책, 정의된 정책을 바탕으로 하는 자동화된 할당량 관리, 정책 구성 및 사용 모니터링을 안내하는 추세 그래프가 제공됩니다.



FortiAnalyzer-VM

FortiAnalyzer-VM은 네트워크 로깅, 분석 및 보고를 단일 시스템에 통합하여 네트워크 전반에서 향상된 보안 이벤트 지식을 제공합니다. 가상화 기술을 활용하는 FortiAnalyzer-VM은 FortiAnalyzer 하드웨어 어플라이언스의 소프트웨어 기반 버전이며 여러 가상화 플랫폼에서 실행되도록 설계되었습니다. FortiAnalyzer 하드웨어 어플라이언스의 모든 기능을 제공합니다.

FortiAnalyzer-VM은 크고 작은 조직에 중앙 집중식 보안 이벤트 분석, 포렌식 조사, 보고, 콘텐츠 아카이빙, 데이터 마이닝, 악성 파일 격리 및 취약성 평가를 제공합니다. Fortinet 어플라이언스 및 타사 장치에서 지리적 및 시기적으로 분산된 보안 데이터의 중앙 집중식 수집, 상관관계, 분석 기능은 통합된 보안 태세 보기를 간편하게 제공합니다.

사양

FORTIANALYZER VIRTUAL APPLIANCES	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
Capacity and Performance							
GB/Day of Logs	1 incl.*	+1	+5	+25	+100	+500	+2,000
Storage Capacity	500 GB	+500 GB	+3 TB	+10 TB	+24 TB	+48 TB	+100 TB
Devices/VDOMs (Maximum)	10,000	10,000	10,000	10,000	10,000	10,000	10,000
FortiGuard Indicator of Compromise (IOC)	✓	✓	✓	✓	✓	✓	✓
Hypervisor Requirements							
Hypervisor Support	VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/6.7, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+ and Open Source Xen 4.1+, KVM on Redhat 6.5+ and Ubuntu 17.04, Nutanix AHV (AOS 5.10.5), Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI), Alibaba Cloud (AliCloud)						
Network Interface Support (Minimum / Maximum)	1 / 4						
vCPUs (Minimum / Maximum)	2 / Unlimited						
Memory Support (Minimum / Maximum)	4 GB / Unlimited						

* Unlimited GB/Day when deployed in collector mode

사양





	FORTIANALYZER 200F	FORTIANALYZER 300F	FORTIANALYZER 400E
Capacity and Performance			
GB/Day of Logs	100	150	200
Analytic Sustained Rate (logs/sec)*	3000	4500	6,000
Collector Sustained Rate (logs/sec)*	4500	6,750	9,000
Devices/VDOMs (Maximum)	150	180	200
Max Number of Days Analytics**	40	28	30
Options Supported			
FortiGuard Indicator of Compromise (IOC)	✓	✓	✓
Hardware Specifications			
Form Factor	1 RU Rackmount	1 RU Rackmount	1 RU Rackmount
Total Interfaces	2 x RJ45 GE	2 x RJ45 GE, 2 x SFP	4 x GE
Storage Capacity	4 TB (1 x 4 TB)	8 TB (2 x 4 TB)	12 TB (4 x 3 TB)
Usable Storage (After RAID)	4 TB	4 TB	6 TB
Removable Hard Drives	No	No	✓
RAID Levels Supported	N/A	RAID 0/1	RAID 0/1/5/10
RAID Type	N/A	Software	Software
Default RAID Level	N/A	1	10
Redundant Hot Swap Power Supplies	No	No	No
Dimensions			
Height x Width x Length (inches)	1.75 x 17.0 x 15.0	1.75 x 17.0 x 15.0	1.7 x 17.2 x 19.8
Height x Width x Length (cm)	4.4 x 43.2 x 38.1	4.4 x 43.2 x 38.0	4.3 x 43.7 x 50.3
Weight	17.1 lbs (7.8 kg)	18.9 lbs (8.6 kg)	31 lbs (14.1 kg)
Environment			
AC Power Supply	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Power Consumption (Average / Maximum)	49W / 114W	65W / 130W	93W / 133W
Heat Dissipation	390 BTU/h	445 BTU/h	456 BTU/h
Operating Temperature	32–104° F (0–40° C)	32–104° F (0–40° C)	41–95°F (5–35°C)
Storage Temperature	95–158° F (-35–70° C)	95–158° F (-35–70° C)	-40–140°F (-40–60°C)
Humidity	20 to 90% non-condensing	20 to 90% non-condensing	8– 90% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 9,842 ft (3,000 m)
Compliance			
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.
**is the max number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

사양





	FORTIANALYZER 800F	FORTIANALYZER 1000E	FORTIANALYZER 2000E
Capacity and Performance			
GB/Day of Logs	300	600	1,000
Analytic Sustained Rate (logs/sec)*	8,250	18,000	30,000
Collector Sustained Rate (logs/sec)*	12,000	27,000	45,000
Devices/VDOMs (Maximum)	800	2,000	2,000
Max Number of Days Analytics**	30	30	30
Options Supported			
FortiGuard Indicator of Compromise (IOC)	✓	✓	✓
Hardware Specifications			
Form Factor	1 RU Rackmount	2 RU Rackmount	2 RU Rackmount
Total Interfaces	4 x GE, 2 x SFP	2 x GE	4 x GE, 2 x SFP+
Storage Capacity	16 TB (4 x 4 TB)	24 TB (8 x 3 TB)	36 TB (12 x 3 TB)
Usable Storage (After RAID)	8 TB	18 TB	30 TB
Removable Hard Drives	✓	✓	✓
RAID Levels Supported	RAID 0/1/5/10	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60
RAID Type	Hardware / Hot Swappable	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	10	50	50
Redundant Hot Swap Power Supplies	No	✓	✓
Dimensions			
Height x Width x Length (inches)	1.75 x 17.44 x 22.16	3.5 x 17.2 x 25.2	3.5 x 17.2 x 25.6
Height x Width x Length (cm)	4.4 x 44.3 x 56.3	8.9 x 43.7 x 68.4	8.9 x 43.7 x 64.8
Weight	28.6 lbs (13.0 kg)	52 lbs (23.6 kg)	58 lbs (26.3 kg)
Environment			
AC Power Supply	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Power Consumption (Average / Maximum)	108W / 186W	192.5W / 275W	293.8W / 354W
Heat Dissipation	634 BTU/h	920 BTU/h	1840 BTU/h
Operating Temperature	32–104° F (0–40° C)	41–95°F (5–35°C)	50–95°F (10–35°C)
Storage Temperature	95–158° F (-35–70° C)	-40–140°F (-40–60°C)	-40–158°F (-40–70°C)
Humidity	20 to 90% non-condensing	8–90% non-condensing	8–90% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)
Compliance			
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.
**is the max number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

사양




	FORTIANALYZER 3000F	FORTIANALYZER 3700F
Capacity and Performance		
GB/Day of Logs	3,000	8,300
Analytic Sustained Rate (logs/sec)*	42,000	100,000
Collector Sustained Rate (logs/sec)*	60,000	150,000
Devices/VDOMs (Maximum)	4,000	10,000
Max Number of Days Analytics**	30	60
Options Supported		
FortiGuard Indicator of Compromise (IOC)	✓	✓
Hardware Specifications		
Form Factor	3 RU Rackmount	4 RU Rackmount
Total Interfaces	4 x GE, 2 x SFP+	2 x SFP+, 2 x 1GE
Storage Capacity	48 TB (16 x 3 TB – 48 TB max)	240 TB (60 x 4 TB SAS HDDs)
Usable Storage (After RAID)	42 TB	216 TB
Removable Hard Drives	✓	✓
RAID Levels Supported	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60
RAID Type	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	50	50
Redundant Hot Swap Power Supplies	✓	✓ ***
Dimensions		
Height x Width x Length (inches)	5.2 x 17.2 x 25.5	7 x 17.2 x 30.2
Height x Width x Length (cm)	13.2 x 43.7 x 64.8	17.8 x 43.7 x 76.7
Weight	76 lbs (34.5 kg)	118 lbs (53.5Kg)
Environment		
AC Power Supply	100–240V AC, 50–60 Hz, 11.5 Amp Maximum	100–240V AC, 60–50 Hz
Power Consumption (Average / Maximum)	449 W / 541W for 12 HDD	850 W / 1423.4W
Heat Dissipation	1846.5 BTU/h	4858 BTU/h
Operating Temperature	50–95°F (10–35°C)	50–95°F (10–35°C)
Storage Temperature	-40–158°F (-40–70°C)	-40–158°F (-40–70°C)
Humidity	8–90% non-condensing	8% to 90% (non-condensing)
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,000 ft (2133 m)
Compliance		
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.
** is the max number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.
*** 3700F must connect to a 200V - 240V power source.

주문 정보

Product	SKU	Description
FortiAnalyzer 200F	FAZ-200F	Centralized log and analysis appliance — 2 x RJ45 GE, 4 TB storage, up to 100 GB/day of logs.
FortiAnalyzer 300F	FAZ-300F	Centralized log and analysis appliance — 2 x RJ45 GE, 8 TB storage, up to 150 GB/day of logs.
FortiAnalyzer 400E	FAZ-400E	Centralized log and analysis appliance — 4 x GE RJ45, 12 TB storage, up to 200 GB/day of logs.
FortiAnalyzer 800F	FAZ-800F	Centralized log and analysis appliance — 4 x GE, 2x SFP, 16 TB storage, up to 300 GB/day of logs.
FortiAnalyzer 1000E	FAZ-1000E	Centralized log and analysis appliance — 2 x GE RJ45, 24 TB storage, dual power supplies, up to 650 GB/day of logs.
FortiAnalyzer 2000E	FAZ-2000E	Centralized log and analysis appliance — 4 x GE RJ45, 2 x SFP+, 36 TB storage, dual power supplies, up to 1,000 GB/day of logs.
FortiAnalyzer 3000F	FAZ-3000F	Centralized log and analysis appliance — 4 x GE RJ45, 2 x SFP+, 48 TB storage, dual power supplies, up to 3,000 GB/day of logs.
FortiAnalyzer 3700F	FAZ-3700F	Centralized log and analysis appliance — 2 x SFP+, 2 x 1GE slots, 240 TB storage, up to 8,300 GB/day of logs.
FortiAnalyzer-VM	FAZ-VM-BASE	Base license for stackable FortiAnalyzer-VM; 1 GB/Day of Logs and 500 GB storage capacity. Unlimited GB/Day when used in collector mode only. Designed for all supported platforms.
	FAZ-VM-GB1	Upgrade license for adding 1 GB/Day of Logs and 500 GB storage capacity.
	FAZ-VM-GB5	Upgrade license for adding 5 GB/day of logs and 3 TB storage capacity.
	FAZ-VM-GB25	Upgrade license for adding 25 GB/day of logs and 10 TB storage capacity.
	FAZ-VM-GB100	Upgrade license for adding 100 GB/day of logs and 24 TB storage capacity.
	FAZ-VM-GB500	Upgrade license for adding 500 GB/day of logs and 48 TB storage capacity.
	FAZ-VM-GB2000	Upgrade license for adding 2 TB/Day of Logs and 100 TB storage capacity.
	FortiAnalyzer AWS On-Demand	https://aws.amazon.com/marketplace/pp/B01N5K7210/ref=portal_asin_url
	FortiAnalyzer Azure On-Demand	https://azuremarketplace.microsoft.com/en-us/marketplace/apps/fortinet.fortianalyzer
FortiAnalyzer - Backup to Cloud Service	FC-10-FAZ00-286-02-DD	One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.
FortiGuard Indicator of Compromise (IOC) Subscription	FC-10-[Model code] -149-02-DD	1 Year Subscription license for the FortiGuard Indicator of Compromise (IOC).



FORTINET CBC
(CUSTOMER BRIEFING CENTER)

포티넷 CBC (고객 솔루션 체험센터)가
새로운 모습으로 여러분을 찾아갑니다.

포티넷 CBC (고객 솔루션 체험센터)가 국내 최초로 OT 보안 데모 시설을 갖추고 새로이 오픈을 합니다.

클라우드 보안부터 다양한 사이버 보안 솔루션과 보안 패브릭을 직접 시연하고 귀사의 비즈니스와 IT 요구사항에 맞춤화된 1:1 기술 컨설팅을 받으실 수 있습니다.

VISIT TODAY

포티넷 CBC 문은 언제나 열려있습니다.
방문을 원하시는 고객분들은
언제든지 연락 주시기 바랍니다.

kr-callcenter@fortinet.com
080-559-8989

FORTINET

포티넷 코리아
서울특별시 강남구 영동대로 325 해암빌딩 14 /15층
전화 : 080-559-8989 이메일 : kr-callcenter@fortinet.com
홈페이지 : http://fortinet.com/kr
페이스북 : https://www.facebook.com/fortinetsouthkorea