데이터 시트

FortiSIEM®

현대 네트워크를 위한 통합 이벤트 상관 관계 및 위험 관리

가동 시간은 오늘날의 디지털 비즈니스에 매우 중요한 요소이며 최종 사용자는 애플리케이션의 문제가 성능과 관련된 것인지 아니면 보안과 관련된 것인지에 대해 상관하지 않습니다. 이러한 면에서 FortiSIEM이 유용합니다.

통합 NOC 및 SOC 분석(특허)

포티넷은 로그, 성능 메트릭, SNMP 트랩, 보안 알림, 구성 변경 등 다양한 정보원으로부터의 통합 데이터 수집 및 분석을 지원하는 아키텍처를 개발했습니다. 근본적으로, FortiSIEM은 과거에 SOC 및 NOC라는 서로 다른 사일로에서 모니터링되던 분석을 통합하여 비즈니스의 보안 및 가용성을 종합적으로 파악합니다. 모든 정보가 이벤트로 변환되며, 먼저 파싱된 후에 실시간 검색, 규칙, 대시보드 및 임시 쿼리를 모니터링하기 위해 이벤트 기반 분석 엔진으로 전송됩니다.

머신러닝/UEBA

FortiSIEM은 머신러닝을 사용하여 비정상적인 사용자 및 엔티티 행동(UEBA)을 탐지하기 때문에 관리자가 복잡한 규칙을 작성할 필요가 없습니다. FortiSIEM은 기존 방어를 통과하는 내부자 및 유입 위협을 식별하는 데 도움이 됩니다. 충실도가 높은 알림은 즉각적인 주의가 필요한 위협부터 우선적으로 처리하는 데 도움이 됩니다.

사용자 및 장치 위험 점수

FortiSIEM은 UEBA 규칙 및 기타 분석을 강화할 수 있는 사용자 및 장치 위험 점수를 매깁니다. 위험 점수는 사용자 및 장치와 관련된 여러 데이터포인트를 결합하여 계산됩니다. 사용자 및 장치 위험 점수는 통합된 엔티티 위험 대시보드에 표시됩니다.

하이라이트

- SOC 및 NOC 분석의 교차 상관 관계
- 실시간 네트워크 분석
- 곧바로 사용 가능한 보안 및 규정 준수
- 단일 IT 창구
- 클라우드 규모 아키텍처
- 자가 학습 자산 인벤토리(CMDB)
- 멀티테넌시
- MSP/MSSP 지원
- 가상 또는 물리적 어플라이언스로 사용

하이라이트

분산 실시간 이벤트 상관 관계(특허)

분산 이벤트 상관 관계는 어려운 문제입니다. 규칙을 트리거하기 위해 여러 노드가 부분적인 상태를 실시간으로 공유해야 하기 때문입니다. 많은 SIEM 공급업체들이 분산 데이터 수집 및 분산 검색 기능을 갖추고 있기는 하지만 포티넷만이 분산 실시간 이벤트 상관 관계 엔진을 갖춘 유일한 공급업체입니다. 복잡한 이벤트 패턴을 실시간으로 탐지할 수 있습니다. 이 특허 알고리즘을 통해 FortiSIEM은 다수의 규칙을 높은 이벤트 속도로 실시간 처리하여 탐지 시간을 단축할 수 있습니다.

실시간 자동 인프라 검색 및 애플리케이션 검색 엔진(CMDB)

신속한 문제 해결을 위해서는 인프라 컨텍스트가 필요합니다. 대부분의 로그 분석 및 SIEM 공급업체는 관리자가 컨텍스트를 수동으로 제공할 것을 요구하는데, 이러한 컨텍스트는 금방 과거의 것이 되며 작업자가 실수할 가능성이 높습니다. 포티넷은 장치나 애플리케이션이 무엇인지를 미리 알지 않아도 간단히 자격 증명을 사용하여 온프레미스 및 퍼블릭/프라이빗 클라우드에서 물리적 인프라와 가상 인프라를 모두 검색할 수 있는 지능형 인프라 및 애플리케이션 검색 엔진을 개발했습니다.

최신 CMDB(Centralized Management Database)를 사용하면 검색 조건에서 CMDB 객체를 사용하여 정교한 컨텍스트 인식 이벤트 분석을 수행할 수 있습니다.

동적 사용자 아이덴티티 매핑

로그 분석의 중요한 컨텍스트는 네트워크 아이덴티티(IP 주소, MAC 주소)를 사용자 아이덴티티(로그 이름, 전체 이름, 조직 역할)에 연결하는 것입니다. 이 정보는 사용자가 DHCP 또는 VPN을 통해 새 주소를 얻을 때 계속 변경됩니다.

포티넷은 동적 사용자 아이덴티티 매핑 방법을 개발했습니다. 사용자 및 해당 역할은 온프레미스 또는 클라우드 SSO 저장소에서 검색됩니다. 네트워크 아이덴티티는 중요한 네트워크 이벤트에서 식별됩니다. 그런 다음 지오아이덴티티가 추가되어 동적 사용자 아이덴티티 감사 추적을 형성합니다. 따라서 IP 주소 대신 사용자 아이덴티티를 기반으로 정책을 만들거나 조사를 수행할 수 있으므로 신속한 문제 해결이 가능합니다.

유연하고 빠른 맞춤형 로그 파싱 프레임워크(특허)

효과적인 로그 파싱에는 맞춤형 스크립트가 필요하지만, 특히 Active Directory, 방화벽 로그 등과 같은 대용량 로그의 경우 실행 속도가 느릴 수 있습니다. 반면에 컴파일된 코드는 실행 속도가 빠르지만 새로운 소프트웨어 릴리스가 필요하기 때문에 유연하지 않습니다. 포티넷은 고급 프로그래밍 언어처럼 작동하고 수정하기 쉬우면서도 효율성을 높이기 위해 런타임 중에 컴파일될 수 있는 XML 기반 이벤트 파싱 언어를 개발했습니다. 모든 FortiSIEM 파서는 이 특허 솔루션을 사용하여 대부분의 경쟁사 제품을 능가하며 노드당 10K EPS 이상으로 파싱될 수 있습니다.

비즈니스 서비스 대시보드 — 시스템을 서비스 보기로 변환

전통적으로 SIEMS는 서버, 애플리케이션, 데이터베이스 등 개별 구성요소를 모니터링하지만, 대부분의 조직에서 실제로 중요하게 여기는 것은 이러한 시스템이 제공하는 서비스입니다. FortiSIEM은 이제 개별 구성요소를 함께 제공되는 최종 사용자 경험과 연결함으로써 진정한 비즈니스 가용성을 확실하게 파악할 수 있습니다.

자동 사고 완화

사고가 발생할 때 자동 스크립트를 실행하여 위협을 완화하거나 없앨 수 있습니다. 기본 제공 스크립트는 포티넷, Cisco, Palo Alto, Window/Linux 서버를 비롯한 다양한 장치를 지원합니다. 기본 제공 스크립트는 사용자의 Active Directory 계정을 비활성화하고, 스위치 포트를 비활성화하고, 방화벽에서 IP 주소를 차단하고, WLAN 액세스 포인트에서 사용자 인증을 취소하는 등 다양한 작업을 실행할 수 있습니다. 스크립트는 FortiSIEM이 CMDB에서 이미 확보한 자격 증명을 활용합니다. 관리자는 자체 스크립트를 생성하여 사용 가능한 작업을 쉽게 확장할 수 있습니다.

보안 인텔리전스 주입

FortiGuard 위협 인텔리전스 및 IOC(Industrial Information) 그리고 상업용, 오픈 소스, 맞춤형 데이터 소스의 IT(Threat Intelligence) 피드가 보안 TI 프레임워크에 쉽게 통합됩니다. 이처럼 다양한 데이터 소스를 대통합함으로써 조직은 위협의 근본 원인을 빠르게 파악하고, 향후 이를 해결하고 방지하는 데 필요한 조치를 취할 수 있습니다. 여러 포티넷 제품을 위한 새로운 위협 완화 라이브러리를 사용하여 단계를 자동화할 수 있는 경우가 많습니다.

하이라이트

대기업 및 관리형 서비스 공급업체 지원 — "멀티테넌트 아키텍처"

포티넷은 기업 및 서비스 공급업체가 단일 콘솔에서 다수의 물리적/논리적 도메인 그리고 겹치는 시스템과 네트워크를 관리할 수 있도록 하는 고도의 맞춤형 멀티테넌트 아키텍처를 개발했습니다. 이러한 환경에서는 물리적 및 논리적 도메인 간에 그리고 개별 고객 네트워크 간에 정보를 상호 연관시키는 것이 매우 쉽습니다. 각각에 대한 고유한 보고서, 규칙 및 대시보드를 쉽게 만들어서 다양한 보고 도메인 및 고객에게 쉽게 배포할 수 있습니다.

이벤트 아카이브 정책을 도메인별 또는 고객별로 배포할 수도 있습니다. 세분화된 RBAC 제어를 통해 관리자 및 테넌트/고객에게 다양한 수준의 액세스 권한을 제공할 수 있습니다. 대규모 MSSP의 경우, Collector를 멀티테넌트로 구성하여 전체 배포 공간을 줄일 수 있습니다.

특징

신속한 보안 분석을 위한 실시간 운영 컨텍스트

- 지속적으로 업데이트되는 정확한 장치 컨텍스트 — 구성, 설치된 소프트웨어 및 패치, 실행 중인 서비스
- 시스템 및 애플리케이션 성능 분석 그리고 보안 문제를 신속하게 분류하기 위한 상황별 상호 관계 데이터
- 실시간 사용자 컨텍스트 그리고 IP 주소, 사용자 아이덴티티 변경 사항, 물리적 및 지리적 매핑 위치에 대한 감사 추적
- 인증되지 않은 네트워크 장치, 애플리케이션, 구성 변경 사항을 탐지

곧바로 사용 가능한 규정 준수 보고서

- 다음을 비롯한 다양한 규정 준수 감사 및 관리 요구를 지원하는 곧바로 사용 가능한 사전 정의된 보고서 — PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, SANS Critical Controls, COBIT, ITIL, ISO 27001, NERC, NIST800-53, NIST800-171, NESA
- GDPR 요구 사항을 충족하기 위해 관리자의 역할에 따라 PII(Personally Identifiable Information)를 관찰할 수 있음

성능 모니터링

- 기본 시스템/공통 메트릭 모니터링
- SNMP, WMI, PowerShell을 통한 시스템 레벨
- JMX, WMI, PowerShell을 통한 애플리케이션 레벨
- VMware, Hyper-V에 대한 가상화 모니터링 — 게스트, 호스트, 리소스 풀, 클러스터 레벨
- 스토리지 사용량, 성능 모니터링 — EMC, NetApp, Isilon, Nutanix, Nimble, Data Domain
- 전문화된 애플리케이션 성능 모니터링
- WMI와 Powershell을 통한 Microsoft Active Directory 및 Exchange
- 데이터베이스 — Oracle, MS SQL, MySQL via JDBC
- IPSLA, SNMP, CDR/CMR을 통한 VoIP 인프라
- 흐름 분석 및 애플리케이션 성능 — Netflow, SFlow, Cisco AVC, NBAR, IPFix
- 맞춤형 메트릭을 추가할 수 있는 능력
- 베이스라인 메트릭 및 커다란 편차 탐지

가용성 모니터링

- 시스템 업/다운 모니터링 — Ping, SNMP, WMI, 가동 시간 분석, 주요 인터페이스, 주요 프로세스 및 서비스, BGP/OSPF/EIGRP 상태 변경, 스토리지 포트 업/다운
- 가상 트랜잭션 모니터링을 통한 서비스 가용성 모델링 — Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, 경로 추적 및 일반 TCP/UDP 포트
- 유지 보수 기간을 예약하기 위한 유지 보수 달력
- SLA 계산 — "장상" 근무 시간 및 시간외 고려 사항

특징

강력한 확장형 분석

- 실시간으로 이벤트 검색 — 인덱싱할 필요 없음
- 키워드 및 이벤트 기반 검색
- 과거 이벤트 검색 — 부울 필터 조건이 있는 SQL 유사 쿼리, 관련 집계별 그룹화, 시각 필터, 정규식 일치, 계산식 — GUI & API
- 검색 및 규칙에서 검색된 CMDB 오브젝트, 사용자/아이덴티티, 위치 데이터 사용
- 보고서를 예약하고 결과를 이메일을 통해 주요 관계자들에게 제공
- 조직 전반에서 이벤트를 검색하거나 물리적 또는 논리적 보고 도메인까지 낮춰서 이벤트 검색
- 주요 위반자를 추적하기 위한 동적 감시 목록 — 어떠한 보고 규칙에서도 감시 목록을 사용
- 중단 시간 없이 Worker 노드를 추가함으로써 분석 피드 확장

베이스라인 지정 및 통계적 이상 징후 탐지

- 베이스라인 엔드포인트/서버/사용자 행동 — 시각 및 주중/주말 세분화
- 높은 유연성 — 어떠한 키 및 메트릭 집합도 "베이스라인 지정" 가능
- 통계적 이상 징후에 대한 기본 제공 및 맞춤형 트리거

외부 기술 통합

- IP 주소 조회를 위해 외부 웹사이트와 통합
- 외부 위협 피드 인텔리전스 소스를 위한 API 기반 통합
- 헬프데스크 시스템이 있는 API 기반 양방향 통합 — ServiceNow, ConnectWise, Remedy에 대한 원활하고 즉각적인 지원
- 외부 CMDB가 있는 API 기반 양방향 통합 — ServiceNow, ConnectWise, Jira, SalesForce에 대한 즉각적인 지원
- 강화된 분석 보고와의 통합을 위한 Kafka 지원 — 예: ELK, Tableau, Hadoop
- 프로비저닝 시스템과의 손쉬운 통합을 위한 API 지원
- 조직을 추가하고, 자격 증명을 만들고, 검색을 트리거하고, 모니터링 이벤트를 수정하기 위한 API 지원

실시간 구성 변경 모니터링

- 네트워크 구성 파일 수집(버전 지정된 저장소에 저장됨)
- 설치된 소프트웨어 버전 수집(버전 지정된 저장소에 저장됨)
- 네트워크 구성 및 설치된 소프트웨어의 변경 사항 자동 탐지
- 파일/폴더 변경 사항 자동 탐지 — Windows 및 Linux — 누가 무엇을 변경했는지에 대한 세부 정보
- 승인된 구성 파일의 변경 사항 자동 탐지
- FortiSIEM Windows 에이전트를 통해 Windows 레지스트리 변경 사항 자동 탐지

장치 및 애플리케이션 컨텍스트

- 스위치, 라우터, 무선 LAN 등의 네트워크 장치
- 보안 장치 — 방화벽, 네트워크 IPS, 웹/이메일 게이트웨이, 멀웨어 방지, 취약성 스캐너
- Windows, Linux, AIX, HP UX 등의 서버
- DNS, DHCP, DFS, AAA, 도메인 컨트롤러, VoIP 등의 인프라 서비스
- 웹 서버, 앱 서버, 메일, 데이터베이스 등의 사용자 대면 애플리케이션
- NetApp, EMC, Isilon, Nutanix, Data Domain 등의 스토리지 장치
- AWS, Box.com, Okta, Salesforce.com 등의 클라우드 앱
- AWS 등의 클라우드 인프라
- UPS, HVAC, Device Hardware 등의 환경 장치
- VMware ESX, Microsoft Hyper-V Scalable, Flexible Log Collection 등의 가상화 인프라

확장 가능하고 유연한 로그 수집

- 보안 로그를 매우 빠른 속도로 수집, 파싱, 정규화, 인덱싱, 저장
- 온프레미스와 클라우드 환경 모두에서 다양한 시스템 및 공급업체 API에 대한 즉각적 지원
- Windows 에이전트가 파일 무결성 모니터링, 설치된 소프트웨어 변경 사항 및 레지스트리 변경 사항 모니터링 등 확장성이 뛰어나고 이벤트가 풍부한 수집 기능을 제공
- Linux 에이전트가 파일 무결성 모니터링, syslog 모니터링, 맞춤형 로그 파일 모니터링을 제공
- GUI 내에서 파서를 수정하고 중단 시간 및 이벤트 손실 없이 실행 중인 시스템에 재배포
- 통합된 파서 개발 환경을 통해 새 파서(XML 템플릿)를 만들고 내보내기/가져오기 기능을 통해 사용자 간에 공유
- 위치에 관계없이 사용자 및 장치의 이벤트를 안전하고 안정적으로 수집

특징

알림 및 사고 관리

- 정책 기반 사고 알림 프레임워크
- 지정된 사고가 발생할 때 해결 스크립트를 트리거
- 외부 티켓팅 시스템과의 API 기반 통합 — ServiceNow, ConnectWise, Remedy
- 기본 제공 티켓팅 시스템
- 사고 보고서를 체계화하여 주요 비즈니스 서비스 및 애플리케이션에 가장 높은 우선 순위를 지정
- 복잡한 이벤트 패턴을 실시간으로 트리거
- 사고 탐색기 - 사고를 호스트, IP, 사용자에 동적으로 연결하여 모든 관련 사고를 빠르게 파악

다양한 맞춤형 대시보드

- 구성 가능한 실시간 대시보드 그리고 KPI를 보여주기 위한 "슬라이드쇼" 스크롤링
- 조직 및 사용자 간에 공유 가능한 보고서 및 분석
- 주요 문제를 빠르게 식별할 수 있도록 색상으로 구분
- 인메모리 계산을 통한 빠른 업데이트
- 비즈니스 서비스, 가상화된 인프라, 이벤트 로깅 상태 대시보드, 전문화된 앱을 위한 전문적인 레이어드 대시보드

외부 위협 인텔리전스 통합

- 외부 위협 피드 인텔리전스를 통합하기 위한 API — 멀웨어 도메인, IP, URL, 해시, Tor 노드
- 주요 위협 인텔리전스 소스에 대한 기본 통합 — Threat-Stream, CyberArk, SANS, Zeus, ThreatConnect
- 대형 위협 피드를 처리하기 위한 기술 — 점진적 다운로드 및 클러스터 내 공유, 네트워크 트래픽과의 실시간 패턴 매칭 모든 STIX 및 TAXII 피드가 지원

간단하고 유연한 관리

- 웹 기반 GUI
- 다양한 수준에서 GUI 및 데이터에 대한 액세스를 제한하기 위한 풍부한 역할 기반 액세스 제어
- 모든 모듈 간 통신이 HTTPS에 의해 보호
- FortiSIEM 사용자 활동의 전체 감사 추적
- 중단 시간 및 이벤트 손실을 최소화하는 손쉬운 소프트웨어 업그레이드
- 정책 기반 아카이브
- 부인 방지 및 무결성 확인을 위한 실시간 로그 해싱
- 유연한 사용자 인증 — 로컬, Microsoft AD 및 OpenLDAP을 통한 외부, Okta를 통한 Cloud SSO/SAML, Duo, RADIUS
- 원격 SSH 터널을 통해 FortiSIEM GUI에서 Collector 뒤로 원격 서버에 로그인

간편한 스케일아웃 아키텍처

- 다음 하이퍼바이저에서 온프레미스 및 퍼블릭/프라이빗 클라우드 구축에 대해 가상 머신으로 사용 — VMware ESX, Microsoft Hyper-V, KVM, Amazon Web Services AMI, Azure
- 다양한 수준의 성능으로 다양한 구축 옵션을 제공하는 여러 가지 물리적 어플라이언스 모델
- 여러 Collector를 구축함으로써 데이터 수집 확장
- FortiSIEM Supervisor에 연결할 수 없을 때 Collector가 이벤트를 버퍼링할 수 있음
- 여러 Worker를 구축함으로써 분석 확장
- Collector를 통해 원격 사이트로부터 이벤트를 수집하도록 기본 제공되는 부하 분산 아키텍처
- 로그 스토리지는 FortiSIEM 전용 NoSQL 데이터베이스 또는 최고의 확장성을 제공하는 Elasticsearch일 수 있음
- 높은 가용성 요구 사항을 충족하기 위해 Supervisor를 액티브/패시브 인스턴스로 구성

FortiSIEM 고급 에이전트

포티넷은 정보를 수집하기 위한 매우 효율적인 에이전트레스 기술을 개발했습니다. 하지만 파일 무결성 모니터링 데이터와 같은 일부 정보는 원격으로 수집하기에는 비용이 많이 듭니다.

FortiSIEM은 에이전트레스 기술을 Windows 및 Linux용 고성능 에이전트와 결합함으로써 데이터 수집을 대폭 향상시켰습니다.

특징

	에이전트레스 기술	고급 WINDOWS 에이전트	고급 LINUX 에이전트
에이전트레스			
검색	✓		
성능 모니터링	✓		
(저성능) 시스템, 앱, 보안 로그의 수집	✓		
에이전트			
(고성능) 시스템, 앱, 보안 로그의 수집		✓	✓
DNS, DHCP, DFS, IIS 로그		✓	
수집 로컬 파싱 및 시간 정규화		✓	
설치된 소프트웨어 탐지		✓	
레지스트리 변경 모니터링		✓	
파일 무결성 모니터링		✓	✓
고객 로그 파일 모니터링		✓	✓
WMI 명령 출력 모니터링		✓	
PowerShell 명령 출력 모니터링		✓	

사양



	FORTISIEM 500F "COLLECTOR"	FORTISIEM 2000F "SUPERVISOR 또는 WORKER"	FORTISIEM 3500F "SUPERVISOR 또는 WORKER"
하드웨어 사양			
CPU	Intel Xeon E3-1225V3 4C4T 3.20 GHz	Intel Xeon E5-2620V3 6C12T 2.40 GHz	2x Intel Xeon E5-2680V2 10C20T 2.80 GHz
Memory	DDR3 16GB(2x 8GB)	DDR4 32 GB(4x 8GB)	DDR3 64 GB(8x 8GB)
네트워크 인터페이스	4x GE RJ45 포트	4x GE RJ45 포트	2x GE RJ45 ports, 2x SFP ports
콘솔 포트	DB9	DB9	DB9
USB 포트	2x USB 2.0; 2x USB 3.0	2x USB 2.0; 2x USB 3.0	4x USB 2.0
저장 용량	3TB(1x 3TB)	36 TB(12x 3TB)	72 TB(24x 3TB)
사용 가능한 이벤트 데이터 스토리지		23.4 TB	55.7 TB
규격			
높이 x 너비 x 길이(인치)	1.7 x 17.2 x 19.8	3.5 x 17.2 x 25.6	7 x 17.2 x 26
높이 x 너비 x 길이(mm)	43 x 437 x 503	89 x 437 x 648	178 x 437 x 660
무게	31lbs(14kg)	58lbs(26.3kg)	93.74lbs(42.5kg)
폼팩터	1 RU	2 RU	4 RU
환경			
AC 전원공급장치	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
전력 소비(평균/최대)	132.3 W/150.3 W	285.7 W/310.5 W	528 W/586.6 W
방열	546.95 BTU/h	1093.55 BTU/h	2035.60 BTU/h
작동 온도	50-95°F(10-35°C)	50-95°F(10-35°C)	41-95°F(5-35°C)
보관 온도	-40-158°F(-40-70°C)	-40-158°F(-40-70°C)	-40-140°F(-40-60°C)
습도	8~90%(비응축)	8~90%(비응축)	8~90%(비응축)
규정 준수			
안전 인증	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

주문 정보

라이선싱 체계

FortiSIEM 라이선스는 상호 연관된 분석 네트워크 장치 검색을 위한 핵심 기능을 제공합니다. 장치에는 스위치, 라우터, 방화벽, 서버 등이 포함됩니다. 모니터링할 각 장치마다 라이선스가 필요합니다. 각 라이선스는 데이터 캡처 및 상관 관계, 알림 및 경보, 보고서, 분석, 검색 및 최적화된 데이터 저장소를 지원하며 10 EPS(Events Per Second)를 포함합니다. "EPS"는 각 장치에서 초당 생성되는 메시지 또는 이벤트 수를 정의하는 성능 측정값입니다. 필요하면 추가적인 EPS를 따로 구매할 수 있습니다. 라이선스는 "가입" 또는 "영구" 버전으로 구매할 수 있습니다.

제품	SKU	설명
FortiSIEM 하드웨어 제품		
FortiSIEM 500F	FSM-500F	FortiSIEM Collector 하드웨어 어플라이언스 FSM-500은 최대 5K EPS, 500 SNMP, 200 WMI(성능의 경우)/100 WMI(로그의 경우)를 지원합니다.
FortiSIEM 2000F	FSM-2000F	FortiSIEM 올인원 하드웨어 어플라이언스 FSM-2000F는 최대 15K EPS를 지원합니다 (모든 기능이 켜져 있음). 따로 구매해야 하는 장치 또는 EPS 라이선스는 포함되어 있지 않습니다.
FortiSIEM 3500F	FSM-3500F	FortiSIEM 올인원 하드웨어 어플라이언스 FSM-3500F는 최대 30K EPS를 지원합니다 (모든 기능이 켜져 있음). 따로 구매해야 하는 장치 또는 EPS 라이선스는 포함되어 있지 않습니다.
FortiSIEM Base 제품		
FortiSIEM 올인원 영구 라이선스	FSM-AIO-BASE	50개 장치와 500 EPS를 위한 Base 올인원 영구 라이선스입니다.
	FSM-AIO-XX-UG	올인원 영구 라이선스에 XX개 장치 및 EPS/장치를 추가합니다.
FSM-2000F용 FortiSIEM 올인원 영구 라이선스	FSM-AIO-2000-BASE	FortiSIEM FSM-2000F를 위한 100개 장치 및 1000 EPS 올인원 영구 라이선스입니다. 유지 보수 및 지원은 포함되지 않습니다.
FSM-3500F용 FortiSIEM 올인원 영구 라이선스	FSM-AIO-3500-BASE	FortiSIEM FSM-3500F를 위한 500개 장치 및 5000 EPS 올인원 영구 라이선스입니다. 유지 보수 및 지원은 포함되지 않습니다.
FortiSIEM 올인원 가입 라이선스	FC1-10-FSM98-180-02-DD	최소 XX개 장치, 10 EPS/장치를 관리하는 장치당 가입 라이선스입니다.
FortiSIEM 추가 제품		
FortiSIEM 엔드포인트 장치 영구 라이선스	FSM-EPD-XX-UG	올인원 영구 라이선스에 XX개 엔드포인트 및 2 EPS/엔드포인트 추가
FortiSIEM 엔드포인트 장치 가입 라이선스	FC[1-8]-10-FSM98-184-02-DD	최소 XX개 엔드포인트, 2 EPS/엔드포인트를 위한 엔드포인트당 가입 라이선스
1 EPS 영구 라이선스	FSM-EPS-100-UG	1 EPS 영구 추가
1 EPS 가입 라이선스	FC[1-10]-FSM98-183-02-DD	1 EPS 가입 추가
FortiSIEM 고급 에이전트(Windows & Linux) 영구 라이선스	FSM-AGT-ADV-XX-UG	영구 라이선스를 위한 XX개 고급 에이전트
FortiSIEM 고급 에이전트(Windows & Linux) 가입 라이선스	FC[1-8]-10-FSM98-182-02-DD	최소 XX개 고급 에이전트를 위한 에이전트당 가입 라이선스
IOC 서비스 가입 라이선스	FC[1-G]-10-FSM98-149-02-DD	(X 포인트) FortiSIEM IOC(Indicator of Compromise) 서비스. 1개 장치 또는 2개 엔드포인트 또는 3개 고급 에이전트가 1포인트에 해당합니다.
FortiSIEM 지원		
FortiSIEM에 대한 FortiCare 지원	FC[1-G]-10-FSM97-248-02-DD	24x7 FortiCare 계약(X 포인트). 1개 장치 또는 2개 엔드포인트 또는 3개 고급 에이전트가 1포인트에 해당합니다.
	FC-10-FSM04-311-02-DD	8x5 FortiCare 계약
	FC-10-FSM04-247-02-DD	24x7 FortiCare 계약

www.fortinet.com/kr

서울특별시 강남구 영동대로 325 에스타워 14 /15층 전화: 080-559-8989 Email: **kr-callcenter@fortinet.com**