데이터 시트

FireEye Email Security Server Edition

이메일 위협에 대한 지능적 , 확장 가능한 방어 시스템

요약

- 악성 첨부파일 , 자격 증명 피싱 URL, 스푸핑 , 제로데이 및 다단계 공격에 대한 포괄적인 이메일 보안 기능 제공
- Microsoft Windows 및 Apple Mac OS X 운영 체제 이미지에 대한 분석 지원
- 이메일을 분석하여 암호로 보호되고 암호화된 첨부 파일 및 악성 URL 을 비롯한 파일에 숨겨진 위협 탐지
- FireEye DTI 클라우드에서 실시간 위협 인텔리전스 획득
- 경보에 대한 상황적 통찰력을 제공하여 위협 우선 순위 지정
- 능동적 방어 모드 또는 모니터 전용 모드로 통합 또는 분산 MVX 서비스를 사용하여 온프레미스 설치

그림 1. EX 3500, EX 5500 및 EX 8500을 비롯한 통합 이메일 보안 어플라이언스.

개요

이메일은 데이터가 가장 많이 들어오는 지점이기 때문에 사이버 공격에 무엇보다 취약합니다. 조직들은 이메일 기반의 스팸 및 바이러스부터 표적화된 지능형 위협까지, 급증하는 보안 위험에 직면해 있습니다. 대부분의 지능적 위협은 이메일을 사용하여 자격 증명 피싱 사이트 및 무기화된 파일 첨부 파일에 연결된 URL을 전달합니다. 이메일은 고도의 타겟팅 및 사용자 정의가 가능하기 때문에 사이버 범죄의 주요 수단이 됩니다.

FireEye Email Security는 지능형 이메일 공격으로 인해 발생하는 침해의 위험과 피해를 최소화하는 데 목적을 두고 있습니다. 사내에서 구축된 FireEye Email Security – Server Edition은 URL 및 첨부 파일 기반 공격을 식별, 격리 및 즉시 중지하는 데 있어 업계를 선도하고 있습니다. Email Security는 진정한 확장형 빅 데이터 플랫폼을 사용하여 인텔리스전스 중심의 컨텍스트와 탐지 플러그인을 기반으로 악성 URL과 정상 URL을 탐지합니다. 시그니처리스 Multi-Vector Virtual Execution™(MVX) 엔진은 이메일 첨부 파일 및 다운로드 가능한 콘텐츠에 연결된 URL을 운영 체제, 애플리케이션 및 웹 브라우저의 포괄적인 크로스 매트릭스와 대조하여 분석합니다. 그리고 최소한의 노이즈로 위협을 식별하며, 오탐률은 0에 가깝습니다.

FireEye는 수백만 개의 센서를 통해 공격자 및 직접 침입 조사와 관련한 광범위한 위협 인텔리전스를 수집합니다. Email Security는 공격 및 공격자에 대한 이와 같은 실제 증거와 상황 인텔리전스를 활용하여 경보의 우선 순위를 정하고 위협을 실시간으로 차단합니다.

또한, FireEye Network Security 및 Endpoint Security와 통합하여 보다 광범위한 가시성으로 다중 벡터 공격을 실시간으로 방어합니다.

이메일 기반 위협에 대한 방어 시스템

온라인으로 많은 개인 정보를 수집할 수 있기 때문에, 사이버 공격자는 사회 공학을 이용하여 거의 모든 사용자가 URL을 클릭하거나 첨부 파일을 열도록 유도할 수 있습니다.

Email Security는 기존의 이메일 보안 시스템을 회피하는 인증 피싱, 발신자 사칭 및 스피어 피싱 공격에 대한 실시간 탐지 및 방어를 제공합니다. 알 수 없는 지능적 위협이 다음에 숨겨진 경우 전자 메일을 분석하고 검역(차단됨):

- 다음과 같은 첨부 파일 유형을 포함하지만 이에 국한되지는 않음: EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 및 ZIP/RAR/TNEF 아카이브
- 암호로 보호되며 암호화된 첨부 파일
- 암호화된 첨부 파일과 해당 암호가 이미지로 함께 첨부되어 있는 이메일
- 이메일, MS Office 문서, PDF 및 아카이브 파일(ZIP, ALZip, JAR)과 기타 파일 유형(Uuencoded, HTML)에 포함된 URL
- URL 및 FTP 링크를 통해 다운로드되는 파일
- 위장, 단축 및 동적으로 리다이렉팅되는 모호한 URL
- 인증 피싱 및 타이포스쿼팅 URL
- 알 수 없는 Microsoft Windows 및 Apple Mac OS X 운영 체제 이미지, 브라우저 및 애플리케이션 취약점
- 스피어 피싱 이메일에 내장된 악성 코드

랜섬웨어 공격은 이메일로 시작되지만 데이터를 암호화하려면 일반적으로 명령/제어 서버로 콜백해야 합니다. Email Security는 이와 같은 다단계 악성코드 캠페인을 식별하고 저지합니다.

뛰어난 위협 탐지

Email Security는 정상 트래픽으로 위장된 고급, 대상 및 기타 회피 공격을 식별하고 격리함으로써 비용이 많이 드는 위반 위험을 완화하는 데 도움이 됩니다. 일단 탐지되면, 이러한 공격은 즉시 중지되고, 분석되고, 식별자를 찍어 미래의 위협을 더 빨리 식별하도록 활용됩니다.

Email Security의 핵심에는 고급 URL 방어, MVX 엔진 및 MalwareGuard가 있습니다. 이러한 기술은 기계 학습과 분석을 사용하여 전통적인 서명과 정책 기반 방어를 회피하는 공격을 식별합니다.

고급 URL Defense의 핵심인 PhishVision은 딥러닝을 사용하여 신뢰할 수 있고 일반적으로 타겟팅된 브랜드의 스크린샷을 전자 메일의 URL에서 참조하는 웹페이지와 컴파일하고 비교하는 이미지 분류 엔진입니다. Kraken은 PhishVision과 협력하여 도메인 및 페이지 콘텐츠 분석을 적용하여 기계 학습을 강화하는 피싱 탐지 플러그인입니다. URL 감지의 또 다른 발전인 Skyfe는 특별히 제작된 완전히 자동화된 맬웨어 인텔리전스 수집 시스템입니다. 소셜 미디어 계정, 블로그, 포럼 및 위협 피드는 거짓 알람을 구별하기 위해 수집됩니다. 고급 URL Defense의 다면적인 특성은 Email Security에 의해 보호받는 조직이 자격 증명 수집 및 스피어 피싱 공격으로부터 비할 데 없는 방어 수단을 제공합니다.

MalwareGuard는 이진 파일을 입력으로 삼아 의심스러운 점수를 출력하는 기계학습 유틸리티입니다. 와이어에 표시되는 모든 휴대용 실행 파일(PE)은 MalwareGuard에 의해 분석됩니다. 결정은 MalwareGuard에 의해 촉발된 점수에 따라 이루어지며, 이름을 할당 받습니다.

MVX 엔진은 안전한 가상 환경에서 동적 시그니처리스 분석을 사용하여 제로데이, 다중 흐름 및 기타 우회 공격을 탐지합니다. 감염과 침해를 막기 위해 이전에 보지 못한 악용과 악성코드를 식별합니다.

회피 완화

Email Security는 원격 개체에 대한 요청을 회피하는 공격으로부터 보호하기 위해 제어된 실시간 모드 기능을 지원합니다. MVX 엔진은 여러 번 다운로드해야 하는 멀웨어를 탐지하고 샘플 바이너리가 요청하는 원격 개체를 반환합니다. 제어된 라이브 모드는 멀티스테이지 다운로드, 스피어 피싱 공격 및 지능형 랜섬웨어 침입에 대한 거짓 알람을 감소시킵니다.

공격자들은 또한 의심스러운 URL을 탐지하는 데 사용되는 기술을 피하려고 합니다. 고급 URL방어의 일환으로 피싱 사이트 탈피 완화도 꾸준히 진행되고 있습니다. 회피 완화는 고급 URL 방어의 일부로 지속적으로 강화됩니다. 또 다른 회피 완화인 게스트 이미지는 잠재적으로 악의적인 개체가 실행될 때 "사용된" 엔드포인트를 모방하도록 사용자 지정할 수 있습니다. 게스트 이미지가 엔드포인트 도메인, 도메인 사용자, 아웃룩 데이터 및 브라우저 기록을 재현하도록 보장함으로써 많은 탈루 기법이 방지됩니다.

통합으로 알림 처리 효율성 향상

Email Security는 모든 첨부 파일과 URL을 분석하여 오늘날의 지능형 공격을 정확하게 식별합니다. 알려진 위협 공격자에 대한 경보의 특성과 결합된 전체 FireEye 보안 에코시스템에서 제공하는 실시간 업데이트를 통해 중요한 경보의 우선순위를 정하고 그에 대한 조치를 취하며 지능형 이메일 공격을 차단하는데 필요한 상황 정보를 제공합니다. 최소한의 노이즈와 오탐률로 알려진 위협, 알려지지 않은 위협, 악성코드를 기반으로 하지 않은 위협을 식별하므로 실제 공격에 리소스를 집중하여 운영 비용을 절감할 수 있습니다. 리스크웨어 분류는 달갑진 않지만 덜 악의적인 활동(애드웨어, 스파이웨어 등)과 실제 침해 시도를 구분하여 경보 대응의 우선 순위를 정합니다.

진화하는 위협 환경에 신속하게 적응

Email Security는 FireEye 동적 위협 인텔리전스(DTI) 클라우드로부터 얻은 실시간 위협 인텔리전스를 활용하여 조직이 이메일 기반 위협의 선제적 방어 시스템을 지속적으로 조정하도록 지원합니다. 위협, 공격자, 시스템 및 피해자 심층 인텔리전스를 결합하여 다음을 수행합니다.

- 위협에 대한 보다 광범위한 가시성을 적시에 제공
- 탐지된 악성코드와 악성 첨부 파일의 역할 및 특징을 식별
- 우선 순위를 정해 신속하게 대응할 수 있도록 상황에 대한 통찰력 제공
- 공격자의 신원과 동기를 파악하고 조직 내에서 그들의 악성 활동 추적
- 이메일 내에 포함된 모든 URL을 다시 작성하여 악의적인 링크로부터 사용자 보호
- 스피어 피싱 공격을 소급 식별하고 악성 URL을 표시하여 피싱 사이트로의 액세스 차단

대응 워크플로우 통합

Email Security는 FireEye Helix 및 FireEye Central Management와 함께 원활하게 동작합니다.

- 보안 운영 플랫폼인 FireEye Helix의 구성 요소로서 전체 인프라에 대한 가시성을 제공합니다. FireEye Helix는 인텔리전스, 엔드포인트 상관관계 분석, 자동화 및 조사 관련 팁을 제공하여 이메일 경보 및 타사 경보를 강화합니다. FireEye Helix는 이러한 기능을 바탕으로 보이지 않는 위협을 드러내고 전문가의 의사 결정을 지원합니다.
- Central Management는 Email Security 및 Network Security에서 생성되는 경보의 상관관계를 분석하여 공격을 거시적으로 파악한 후 공격의 확산을 방지하는 차단 규칙을 설정합니다.
- Central Management는 공격 대상을 파악할 수 있도록 하는 역할 기반 태그 지정을 지원합니다.
- Central Management는 역할별 기준에 따라 경보에 대응하고 복구합니다.

추가 기능

맞춤화할 수 있는 YARA 기반의 룰

Email Security는 보안 분석가가 해당 조직을 표적으로 삼는 위협이 포함된 이메일 첨부 파일을 분석하는 규칙을 지정하고 테스트할 수 있게 합니다.

경영진 사칭 보호

Email Security – Server Edition은 중요한 직원이 스푸핑되는 것을 방지하기 위해 비즈니스 이메일 손상(BEC)을 차단할 수 있는 기능을 제공합니다. 내부 이메일 디스플레이 이름을 승인된 보낸 사람과 일치하는 승인된 목록과 비교하는 정책이 생성됩니다.

메시지 대기열, 경보 및 격리 관리

Email Security - Server Edition은 스캔하는 이메일 메시지에 대한 높은 제어력을 제공합니다. 능동적 방어 모드로 설치하는 경우, MTA 큐를 통해서 이동할 때 메시지를 추적 및 관리할 수 있습니다. 이메일 특성을 사용하여 메시지가 수신, 분석 및 넥스트 홉으로 전달되었는지 검색 및 검증하고, 시간 경과에 따라 직관적 대시보드를 통해 트렌드를 모니터링할 수 있습니다. 명백한 허용 및 차단 리스트는 이메일 처리에 대한 맞춤형 제어를 제공합니다. 일반적인 경보의 특성을 검색하거나 선택할 수 있습니다. 또한 경보 및 격리된 메시지를 일괄적으로 처리할 수 있습니다.

능동적 방어 모드 또는 모니터 전용 모드

Email Security는 능동적인 방어를 위해 이메일을 분석하고 위협을 격리할 수 있습니다. 모니터 전용으로 설치하는 경우, BCC 룰의 명확한 설정을 통해 이메일 사본들을 Email Security 시스템으로 보낸 후 분석할 수 있습니다.

유연한 설치 옵션

Email Security – Server Edition은 조직의 필요와 예산에 따라 다양한 설치 옵션을 제공합니다.

- **통합 이메일 보안:** 통합된 MVX 서비스를 사용하여 단일 사이트에서 이메일 수신 지점을 보호하는 독립 실행형, 올인원 하드웨어 어플라이언스. FireEye Email Security는 60분 내에 설치할 수 있고, 관리가 용이한 솔루션입니다. 규칙, 정책 또는 튜닝이 필요 없습니다.
- **분산 이메일 보안:** 중앙 공유 MVX 서비스를 사용하여 기업 내 이메일 수신 지점을 보호하는 확장 가능한 어플라이언스.
- **이메일 스마트 노드:** 이메일 트래픽을 분석하여 악성 트래픽을 탐지 및 차단하고 정확한 결과 분석을 위해 암호화된 연결로 MVX 서비스에 의심스러운 활동을 알리는 가상 센서.
- **MVX 스마트 그리드:** 투명한 확장성, 내장된 N+1 내결함성 및 자동 부하 조절을 제공하는 중앙에 위치한 탄력적 온-프레미스 MVX 서비스.

  통합 하드웨어 어플라이언스에서 MVX Smart Grid에 적용된 버스팅을 통해 메시지 처리량이 최고조에 달할 때 이메일 기반 위협 탐지 및 분석에 추가 용량을 활용할 수 있습니다.
- **FireEye 클라우드 MVX:** 이메일 스마트 노드에서 트래픽을 분석하여 개인 정보 보호를 보장하는 MVX 서비스 구독입니다. 의심스러운 객체만 암호화된 연결을 통해 MVX 서비스에 전송됩니다. 여기에서 정상으로 밝혀지는 객체는 폐기됩니다.

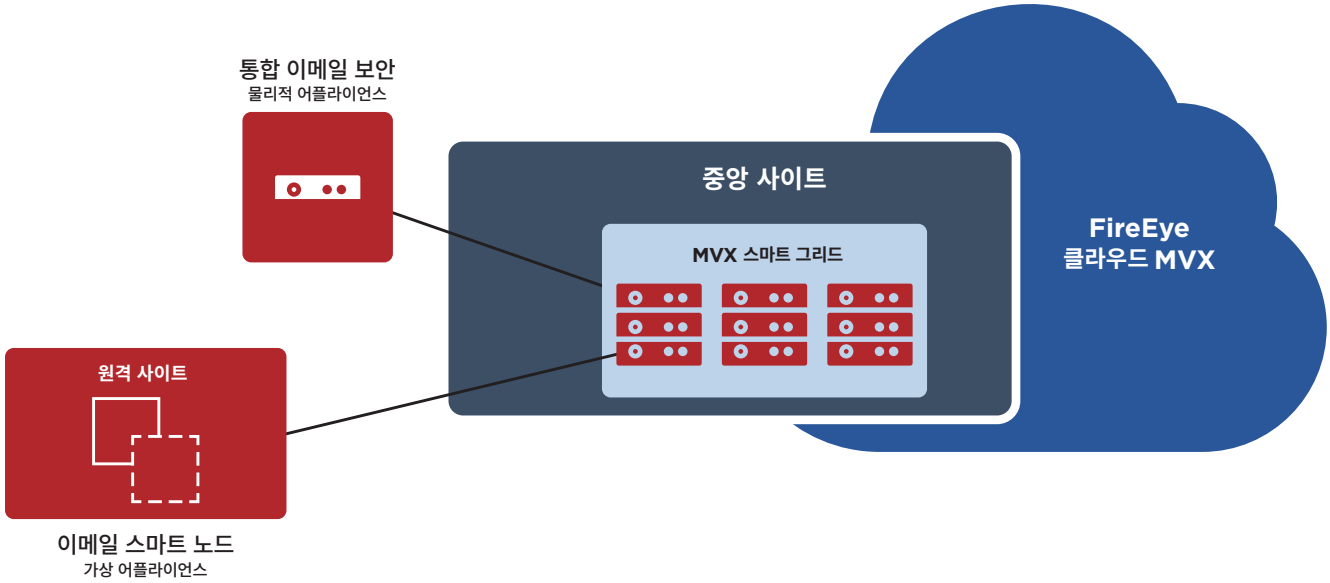

그림 2. 이메일 보안을 위한 분산 및 버스팅 배치 모델.

표 1. 기술 사양.

	EX 3500	EX 5500	EX 8500
성능*	시간당 각 첨부 파일 최대 700개	시간당 각 첨부 파일 최대 1,800개	시간당 각 첨부 파일 최대 2,650개
네트워크 인터페이스 포트	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+(10GigE 섬유, 10GigE 구리, 1GigE 구리), 2x 1GigE BaseT
관리 포트	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI 모니터링	포함	포함	포함
VGA 포트(후면 패널)	포함	포함	포함
USB 포트(후면 패널)	4x USB 타입 A 후면	2x USB 타입 A 전면, 2x USB 타입 A 후면	2x USB 타입 A 전면, 2x USB 타입 A 후면
시리얼 포트(후면 패널)	115,200bps, 패리티 없음, 8비트, 1 정지 비트	115,200bps, 패리티 없음, 8비트, 1 정지 비트	115,200bps, 패리티 없음, 8비트, 1 정지 비트
저장 용량	4x 2TB, RAID 10, HDD 3.5인치, FRU	4x 2TB, RAID 10, HDD 3.5인치, FRU	4x 2TB, RAID 10, HDD 3.5인치, FRU
엔클로저	1RU, 19인치 랙에 적합	2RU, 19인치 랙에 적합	2RU, 19인치 랙에 적합
섀시 크기(WxDxH)	437 x 650 x 43.2mm (17.2 x 25.6 x 1.7인치)	438 x 620 x 88.4mm (17.24 x 24.41 x 3.48인치)	438 x 620 x 88.4mm (17.24 x 24.41 x 3.48인치)
AC 전원 장치	이중화(1+1) 750와트, 100~240 VAC, 9~4.5A, 50~60Hz, IEC60320-C14 인렛, FRU	이중화(1+1) 800와트, 100~240 VAC, 9~4.5A, 50~60Hz, IEC60320-C14 인렛, FRU	이중화(1+1) 800와트, 100~240 VAC, 9~4.5A, 50~60Hz, IEC60320-C14 인렛, FRU
DC 전원	해당 없음	해당 없음	해당 없음
최대 열량 전력	245와트(시간당 836BTU)	456와트(시간당 1,556BTU)	530와트(시간당 1,808BTU)
MTBF(h)	54,200시간	57,401시간	53,742시간
어플라이언스만/발송 중량, kg(lbs)	13.6kg(30.0lbs)/18.6kg(41.0lbs)	20.0kg(44.1lbs)/29.6kg(65.3lbs)	20.2kg(44.4lbs)/29.8kg(65.6lbs)
안전 규제 준수	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
EMC 준수	FCC 파트 15 ICES-003 클래스 A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 및 V-3/2015	FCC 파트 15 ICES-003 클래스 A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 및 V-3/2015	FCC 파트 15 ICES-003 클래스 A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 및 V-3/2015
보안 인증	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
환경 준수	RoHS 지침 2011/65/EU, REACH, WEEE 지침 2012/19/EU	RoHS 지침 2011/65/EU, REACH, WEEE 지침 2012/19/EU	RoHS 지침 2011/65/EU, REACH, WEEE 지침 2012/19/EU
작동 온도	0~35°C(32~95°F)	0~35°C(32~95°F)	0~35°C(32~95°F)
작동 상대 습도	40°C에서 10~95%, 비응결	40°C에서 10~95%, 비응결	40°C에서 10~95%, 비응결
작동 고도	3,000m/9,842ft	3,000m/9,842ft	3,000m/9,842ft

* 모든 성능 수치는 시스템 설정과 처리 중인 이메일 트래픽 프로파일에 따라 달라집니다. 어플라이언스 크기는 시간당 각 첨부 파일 수에 따라 달라집니다.

표 2. FireEye MVX 스마트 그리드 사양.

	VX 5500	VX 12500
OS 지원	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
성능*	시간당 각 첨부 파일 최대 480개	시간당 각 첨부 파일 최대 1,250개
고가용성**	N+1	N+1
관리 포트(후면 패널)	1x 10/100/1000Mbps BASE-T 포트	1x 10/100/1000Mbps BASE-T 포트
클러스터 포트(후면 패널)	3x 10/100/1000Mbps BASE-T 포트	1x 10/100/1000Mbps BASE-T 포트, 2x 10Gbps BASE-T 포트
IPMI 포트(후면 패널)	포함	포함
전면 LCD 및 키패드	해당 없음	포함
VGA 포트	포함	포함
USB 포트(후면 패널)	4x 타입 A USB 포트	2x 타입 A USB 포트
시리얼 포트(후면 패널)	115,200bps, 패리티 없음, 8비트, 1 정지 비트	115,200bps, 패리티 없음, 8비트, 1 정지 비트
드라이브 용량	2x 2TB 3.5 SAS HDD, RAID 1, 핫 스왑 가능, FRU	4 x 4TB 3.5인치 SAS3 HDD, RAID 1, FRU
엔클로저	1RU, 19인치 랙에 적합	2RU, 19인치 랙에 적합
섀시 크기(WxDxH)	17. 437 x 650 x 43.2mm(2x25.6x1.7인치)	437 x 851 x 89mm(17.2x33.5x3.5인치)
DC 전원	해당 없음	해당 없음
AC 전원 장치	이중화(1+1) 750와트, 100-240VAC, 8-3.8A, 50-60Hz, IEC60320-C14, 인렛, 핫 스왑 가능, FRU	이중화(1+1) 800W: 100-127V, 9.8A-7A 1000W: 220-240V, 7-5A, 50-60Hz, FRU IEC60320-C14 인렛, FRU
최대 전력 소비	285와트	760와트
최대 열 방산	시간당 972BTU	시간당 2,594BTU
MTBF	54,200시간	38,836시간
어플라이언스만/발송 중량	15kg(33lb)/21.8kg(48lb)	21kg(46lb)/40.2kg(90lb)
보안 인증	FIPS 140-2 레벨 1, CC NDPP v1.1	FIPS 140-2 레벨 1, CC NDPP v1.1
규제 준수 안전	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

* 모든 성능 수치는 시스템 설정과 처리 중인 트래픽 프로파일에 따라 달라집니다.

** 적절한 이중화 하드웨어 구성 사용 시.

표 3. FireEye Email Security 스마트 노드, 가상 센서 사양.

	EX 5500V
OS 지원	Microsoft Windows, Apple macOS X
성능*	시간당 각 첨부 파일 최대 1,250개
네트워크 모니터링 포트	2개
네트워크 관리 포트	2개
CPU 코어	8개
메모리	16GB
드라이브 용량	384GB
네트워크 어댑터	VMXNet 3, vNIC
하이퍼바이저 지원	VMWare ESXi 6.0 이상

* 모든 성능 수치는 시스템 설정과 처리 중인 트래픽 프로파일에 따라 달라집니다 .

FireEye에 대한 자세한 정보: **www.FireEye.com**

FireEye Korea
서울 특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@fireeye.com

FireEye, Inc. 소개
FireEye는 인텔리전스 기반의 보안 회사입니다. FireEye는 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영의 완벽한 확장을 지원합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다.