FireEye
SECURITY REIMAGINED

FireEye Network Threat Prevention Platform

웹 기반의 사이버 공격에 대처하는 위협 방어 플랫폼

데 이 터 시 트 :

SECURITY REIMAGINED

주요 기능

- 인라인(차단/모니터 모드) 또는 대역 외(TCP 재설정 모드/모니터 모드)로 설치하고, IPv6 트래픽에 대한 보안 분석을 활성화
- PDF, Flash, 멀티미디어 형식, ZIP/RAR/TNEF 아카이브를 포함하는 모든 의심스러운 웹 객체를 분석하고 아웃바운드 악성코드를 차단하여 데이터 유출을 무력화
- FireEye Threat Prevention Platform(위협 방어 플랫폼)과 통합하여 혼합된 스피어 피싱 공격을 차단
- FireEye Dynamic Threat Intelligence(동적 위협 인텔리전스, DTI)를 통해서 위협 인텔리전스를 로컬에 설치된 전체 FireEye 시스템과 글로벌 FireEye 고객 기반에 배포
- 로컬 인증에 추가하여 다른 회사의 원격 AAA 네트워크 서비스에 대한 접근을 지원
- 역할 기반 접근 제어(RBAC) 와 감사 기록을 제공
- 윈도우즈 및 맥 OS X 환경에 대한 지원 포함
- FireEye Network에 대한 IPS 추가 라이센스를 사용하여 시그니처 기반과 비-시그니처 기술을 통합함으로써 자동으로 오탐을 줄이고 운영 비용을 억제
- 자동화된 노이즈 감소 능력을 사용하여 IPS 운영 비용을 억제

NX 2400, NX 4420, NX 7420, NX 10000
(사진 없음: NX 1400, NX 4400, NX 7400)

요약

The FireEye® Network Threat Prevention Platform은 제로데이 웹 익스플로잇, 드롭퍼(바이너리), 다중 프로토콜 콜백을 식별 및 차단하여 조직들이 본부는 물론, 지사, 원격 및 이동 사무실에 설치된 다양한 시스템에 대한 지능형 위협 방어를 확대하는 것을 지원합니다. Intrusion Prevention System(침입 방어 시스템, IPS) 기술을 사용하는 FireEye Network는 추가로 지출을 최적화하고, 오탐을 상당히 줄이고, 알려졌거나 알려지지 않은 위협에 대해 보안을 제공하는 동안 법규를 준수할 수 있습니다.

사이버 범죄자들은 웹을 주 위협 벡터로 사용하여 이메일에 들어 있는 제로데이 익스플로잇과 악성 URL을 전달하고 데이터를 유출합니다. FireEye Network는 드라이브바이 다운로드와 웹 및 이메일이 혼합된 공격을 중단시키도록 설계되었습니다. 또한, FireEye Network는 네트워크 외부에서 발생하는 감염을 방어합니다.

웹 기반의 공격을 차단하는 실시간 위협 방어

FireEye Network는 인터넷 접점에 인라인으로 설치하여 웹 익스플로잇과 아웃바운드 다중 프로토콜 콜백을 차단할 수 있습니다. FireEye Multi-Vector Virtual Execution™ (다중 벡터 가상 실행, MVX)를 사용하는 FireEye Network는 제로데이 공격을 확인하고, 실시간 위협 인텔리전스를 생성하고, 동적 콜백 목적지를 캡쳐합니다. 이 플랫폼은 모니터 모드에서 사고 대응 메커니즘에 신호를 보냅니다. FireEye Network는 대역 외 방어 모드에서 TCP, UDP 또는 HTTP 연결을 대역 외에서 차단하기 위해 TCP를 재설정합니다.

웹과 이메일 위협 벡터에 대한 혼합 공격을 방어

FireEye 플랫폼은 웹, 스피어 피싱 이메일, 제로데이 익스플로잇을 사용하는 혼합된 지능형 공격을 방어합니다. 고객들은 FireEye Network, FireEye Email 및 FireEye Central Management를 사용하여 악성 URL을 실시간으로 방어할 뿐만 아니라, 산재된 혼합 공격으로 연결하는 능력을 보유합니다.

알려지지 않은 제로데이 공격을 방어

FireEye Network는 취약점 악용, 메모리 오염 및 다른 악성 활동을 추적하는 다양한 브라우저, 플러그인, 애플리케이션, 운영 환경에 대해 의심스러운 바이너리와 웹 객체를 실행하는 비-시그니처 FireEye MVX 엔진을 사용합니다. 공격이 발생하면, FireEye MVX 엔진은 콜백 채널을 캡쳐하고, 차단 룰을 동적으로 생성하고, 이 정보를 다시 FireEye Network 플랫폼으로 전송합니다.

맞춤화할 수 있는 YARA 기반의 룰

보안 분석가는 맞춤화된 YARA 룰의 지원을 받아 위협을 분석해야 하는 웹 객체를 지정할 수 있습니다.

사고에 대한 우선 순위 결정을 능률화

안티바이러스 벤더들이 FireEye Network 플랫폼이 중단시킨 악성코드를 탐지할 수 있는지 확인하기 위해 FireEye AV 제품군을 사용하여 각 악성 객체를 분석합니다. 따라서 고객들은 사고 대응의 우선 순위를 더 효과적으로 결정할 수 있습니다.

Dynamic Threat Intelligence

FireEye Network가 분석 결과에 따라 동적으로 생성하는 실시간 위협 인텔리전스는 모든 FireEye 제품이 로컬 네트워크를 보호하는 데 도움이 될 수 있습니다. 이 인텔리전스는 Dynamic Threat Intelligence™ (동적 위협 인텔리전스, DTI) 클라우드를 통해서 전세계에서 공유하여 모든 가입자에게 새로 출현한 위협에 대해 통지할 수 있는 콜백 정보와 통신 특성이 포함됩니다.

룰에 대한 튜닝이 필요 없고 0에 가까운 오탐률

FireEye Network는 60분 이내에 설치되고 튜닝이 절대적으로 필요 없는 관리가 용이한 클라이언트리스 플랫폼 그룹입니다. 이 플랫폼은 TAP/SPAN 을 통한 대역 외 설치, 인라인 모니터링 또는 능동적인 인라인 차단을 포함하는 유연한 설치 모드를 제공합니다.

능동적인 페일 오픈 (fail open) 지원

FireEye Network는 능동적 페일 오픈 스위치와의 통합을 지원하여 링크 다운타임을 방지하고, 전원 또는 링크 고장 시, 설치된 인라인 하드웨어에 대해 지속적인 가용성을 제공합니다. 능동적 페일 오픈 스위치는 하트비트 기술을 활용하여 FireEye Network 장치의 가용성을 모니터하고, 고장이 발생하는 경우에는 우회로 자동 전환됩니다.

IPS 지원

IPS 기술을 사용하는 FireEye Network는 지능형 위협 방어 시스템을 기존의 보안 시스템과 통합하여 투자비용을 줄여줍니다. FireEye Network는 경보 검증을 자동화하고, MVX의 능력을 활용하여 오탐을 줄이고, 노이즈 내에 숨겨진 공격을 파악하여 OPEX(운영 비용)를 억제하고, 탐지하지 못한 사고가 비즈니스에 노출되는 것을 줄입니다. FireEye Network는 MVX가 제공하는 비-시그니처 보안을 기존 IPS 기술의 시그니처 기반 보안으로 보완하여 보안을 확대하고 컴플라이언스를 가능하게 합니다.

기술 사양

	NX 900	NX 1400	NX 2400	NX 4400/4420	NX 7400/7420	NX 7500	NX 9450	NX 10000	NX 10450
사용자 수	50	100	500	2,500	10,000	10,000	20,000	40,000	40,000
OS 지원	마이크로소프트 윈도우즈	마이크로소프트 윈도우즈	마이크로소프트 윈도우즈	마이크로소프트 윈도우즈	마이크로소프트 윈도우즈	마이크로소프트 윈도우즈 맥 OS X	마이크로소프트 윈도우즈	마이크로소프트 윈도우즈	마이크로소프트 윈도우즈
성능 *	최대 10Mbps	최대 20Mbps	최대 50Mbps	최대 250Mbps	최대 1Gbps	최대 1Gbps	최대 2Gbps	최대 4Gbps	최대 4Gbps
네트워크 모니터링 포트	2x 10/100/1000 BASE- T 포트	2x 10/100/1000 BASE- T 포트	4x 10/100/1000 BASE- T 포트	4400: 4x 10/100/ 1000 BASE- T 포트 4420: 4x 1000 BASE-SX 광섬유 포트 (LC 멀티모드)	7400: 4x 10/100/1000 BASE- T 포트 7420: 4x 1000 BASE-SX 광섬유 포트 (LC 멀티모드)	4x 10/100/1000 BASE- T 포트	4x SFP+, 4xSFP 포트, 1000baseSX (LC MMF), 1000baseLX (LC, SMF), 1000baseT (RJ45, UTP5)	2x 10GBASE - SR/SW 850nm 고정 인터페이스: 10GbaseSX (LC MMF)	8 x SFP+ (4 x 1000base and 4 x 10Gbase), 1000baseSX/ 10GbaseSR (LC, MMF), 1000baseLX/ 10GbaseLR (LC SMF), 1000baseT (RJ45, UTP5), 10GbaseCu (5m 직접 연결 케이블)
네트워크 포트 작동 모드	인라인 모니터, 페일 오픈, 페일 클로즈 또는 Tap/Span, HW 우회	인라인 모니터, 페일 오픈, 페일 클로즈 또는 Tap/Span, HW 우회	인라인 모니터, 페일 오픈, 페일 클로즈 또는 Tap/Span, HW 우회	인라인 모니터, 페일 오픈, 페일 클로즈 또는 Tap/Span, HW 우회	인라인 모니터, 페일 오픈, 페일 클로즈 또는 Tap/Span, HW 우회	인라인 모니터, 페일 오픈, 페일 클로즈 또는 Tap/Span, HW	인라인 모니터 또는 Tap/Span	인라인 모니터, 페일 오픈, 페일 클로즈 또는 Tap/Span, HW 우회	인라인 모니터 또는 Tap/Span
관리 포트(후면 패널)	2x 10/100/1000 BASE-T 포트	2x 10/100/1000 BASE- T 포트	2x 10/100/1000 BASE- T 포트	2x 10/100/1000 BASE- T 포트	2x 10/100/1000 BASE- T 포트	2x 10/100/1000 BASE- T 포트	2x 10/100/1000 BASE- T 포트	2x 10/100/1000 BASE- T 포트	2x 10/100/1000 BASE- T 포트
IPMI 포트(후면 패널)	포함	포함	포함	포함	포함	포함	포함	포함	포함
전면 LCD 및 키패드	해당없음	포함	포함	포함	포함	포함	포함	포함	포함
PS/2 키보드 및 마우스, DB15 VGA 포트(후면 패널)	포함	포함	포함	포함	포함	포함	포함	포함	포함
USB 포트(후면 패널)	2x 타입 A USB 포트	2x 타입 A USB 포트	2x 타입 A USB 포트	2x 타입 A USB 포트	2x 타입 A USB 포트	4x 타입 A USB 포트	2x 타입 A USB 포트	2x 타입 A USB 포트	2x 타입 A USB 포트
시리얼 포트 (후면 패널)	115,200bps, 패리티 없음, 8 비트, 1 정지 비트	115,200bps, 패리티 없음, 8 비트, 1 정지 비트	115,200bps, 패리티 없음, 8 비트, 1 정지 비트	115,200bps, 패리티 없음, 8 비트, 1 정지 비트	115,200bps, 패리티 없음, 8 비트, 1 정지 비트	115,200bps, 패리티 없음, 8 비트, 1 정지	115,200bps, 패리티 없음, 8 비트, 1 정지 비트	115,200bps, 패리티 없음, 8 비트, 1 정지 비트	115,200bps, 패리티 없음, 8 비트, 1 정지 비트
드라이브 용량	단일 500 GB HDD, 내부, 고정	단일 500 GB HDD, 내부, 고정	단일 500 GB HDD, 내부, 고정	2x 600 GB HDD, RAID 1, 2.5인치, FRU	2x 600 GB HDD, RAID 1, 2.5인치, FRU	4x 900 GB HDD, RAID 10, 2.5인치, FRU	4x 900 GB HDD, RAID 10, 2.5인치, FRU	2x 800 GB SSD, RAID 1, 2.5인치, FRU	4x 800 GB SSD, RAID 10, 2.5 인치, FRU
엔클로저	1RU, 19인치 랙에 맞음	1RU, 19인치 랙에 맞음	1RU, 19인치 랙에 맞음	1RU, 19인치 랙에 맞음	2RU, 19인치 랙에 맞음	2RU, 19인치 랙에 맞음	2RU, 19인치 랙에 맞음	2RU, 19인치 랙에 맞음	2RU, 19인치 랙에 맞음
섀시 크기 WxDxH	16.8" x 14" x 1.7" (427 x 356 x 43mm)	17.2" x 24.1" x 1.70" (437 x 612 x 43.2mm)	17.2" x 24.1" x 1.70" (437 x 612 x 43.2mm)	17.2" x 27.8" x 1.70" (437 x 706 x 43.2mm)	17.2" x 28.0" x 3.41" (437 x 711 x 86.5mm)	17.2" x 28" x 3.41" (437 x 711 x 86.6mm)	17.2" x 27.9" x 3.5" (437 x 709 x 89mm)	17.2" x 27.9" x 3.5" (437 x 709 x 89mm)	17.2" x 27.9" x 3.5" (437 x 709 x 89mm)
DC 전원	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음

기술 사양

	NX 900	NX 1400	NX 2400	NX 4400/4420	NX 7400/7420	NX 7500	NX 9450	NX 10000	NX 10450
AC 전원	단일, 비-FRU, 내부 200와트 @ 100-240VAC 3-1.5A, 50-60Hz IEC60320-C14 인렛	단일, 비-FRU, 내부 500와트 @ 100-240VAC 5-2.5A, 50-60Hz IEC60320-C14 인렛	단일, 비-FRU, 내부 500와트 @ 100-240VAC 5-2.5A, 50-60Hz IEC60320-C14 인렛	이중화 (1+1) 750와트, 100-240 VAC 9-4.5A, 50-60Hz IEC60320-C14 인렛, FRU	이중화 (1+1) 750와트, 100-240 VAC 9-4.5A, 50-60Hz IEC60320-C14 인렛, FRU	이중화(1+1) 750와트, 100-240 VAC 9-4.5A, 50-60Hz IEC60320-C14 인렛, FRU	이중화 (1+1) 1200와트, 100-140 VAC, 14.7-10.5A 1400와트, 180-240 VAC, 9.5-7.2A, 50-60Hz, FRU IEC60320-C14 인렛, FRU	이중화 (1+1) 1200와트, 100-140 VAC, 14.7-10.5A 1400와트, 180-240 VAC, 9.5-7.2A, 50-60Hz, FRU IEC60320-C14 인렛, FRU	이중화 (1+1) 1200와트, 100-140 VAC, 14.7-10.5A 1400와트, 180-240 VAC, 9.5-7.2A, 50-60Hz, FRU IEC60320-C14 인렛, FRU
최대 전력 소비(와트)	136와트	208와트	210와트	305와트	501와트	479와트	550W	962와트	850W
최대 열 방산 (BTU/h)	464 BTU/h	710 BTU/h	717 BTU/h	1041 BTU/h	1709 BTU/h	1634 BTU/h	1881 BTU/h	3282 BTU/h	2908 BTU/h
MTBF (h)	94,700 h	67,500 h	55,200 h	37,000 h	58,900 h	58,900 h	52,469 h	50,200 h	40,275 h
어플라이언스만 / 발송 중량(lb.) (kg)	11lb. (5kg) / 20lb. (9kg)	24lb. (11kg) / 39lb. (18kg)	24lb. (11kg) / 39lb. (18kg)	31lb. (14kg) / 46lb. (21kg)	42lb. (19kg) / 58lb. (26kg)	43lb. (19.5kg) / 59lb. (27kg)	51lb. (23kg) / 66lb. (30kg)	51lb. (23kg) / 66lb. (30kg)	51lb. (23kg) / 66lb. (30kg)
안전 인증	IEC 60950 EN 60950 CSA 60950-00 CE 마킹	IEC 60950 EN 60950 CSA 60950-00 CE 마킹	IEC 60950 EN 60950 CSA 60950-00 CE 마킹	IEC 60950 EN 60950 CSA 60950-00 CE 마킹	IEC 60950 EN 60950 CSA 60950-00 CE 마킹	IEC 60950 EN 60950 CSA 60950-00 CE 마킹	IEC 60950-1 EN 60950-1 CSA 60950-1 CE 마킹	IEC 60950-1 EN 60950-1 CSA 60950-1 CE 마킹	IEC 60950-1 EN 60950-1 CSA 60950-1 CE 마킹
EMC/EMI 인증	FCC (파트 15 클래스-A), CE (클래스-A), CNS, AS/NZS, VCCI(클래스 A)	FCC (파트 15 클래스-A), CE (클래스-A), CNS, AS/NZS, VCCI(클래스 A)	FCC (파트 15 클래스-A), CE (클래스-A), CNS, AS/NZS, VCCI(클래스 A)	FCC (파트 15 클래스-A), CE (클래스-A), CNS, AS/NZS, VCCI(클래스 A)	FCC (파트 15 클래스-A), CE (클래스-A), CNS, AS/NZS, VCCI(클래스 A)	FCC (파트 15 클래스-A), CE (클래스-A), CNS, AS/NZS, VCCI(클래스 A)	FCC (파트 15 클래스-A), CE (클래스-A), CNS, AS/NZS, VCCI(클래스 A)	FCC (파트 15 클래스-A), CE (클래스-A), CNS, AS/NZS, VCCI(클래스 A)	FCC (파트 15 클래스-A), CE (클래스-A), CNS, AS/NZS, VCCI(클래스 A)
규제 준수	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE
작동 온도	10°C에서 35°C (추가 차이를 고려하여 0°C와 40°C 사이에서 시험)	10°C에서 35°C (추가 차이를 고려하여 0°C와 40°C 사이에서 시험)	10°C에서 35°C (추가 차이를 고려하여 0°C와 40°C 사이에서 시험)	10°C에서 35°C (추가 차이를 고려하여 0°C와 40°C 사이에서 시험)	10°C에서 35°C (추가 차이를 고려하여 0v°C와 40°C 사이에서 시험)	10°C에서 35°C (추가 차이를 고려하여 0°C와 40°C 사이에서 시험)	10°C에서 35°C	10°C에서 35°C	10°C에서 35°C
비작동 온도	-40°C에서 70°C	-40°C에서 70°C	-40°C에서 70°C	-40°C에서 70°C	-40°C에서 70°C	-40°C에서 70°C	-40°C에서 70°C	-40°C에서 70°C	-40°C에서 70°C
작동 상대 습도	8%-90% (비응축)	8%-90% (비응축)	8%-90% (비응축)	8%-90% (비응축)	8%-90% (비응축)	8%-90% (비응축)	10%-85% (비응축)	10%-85% (비응축)	10%-85% (비응축)
비작동 상대 습도	5%-95% (비응축)	5%-95% (비응축)	5%-95% (비응축)	5%-95% (비응축)	5%-95% (비응축)	5%-95% (비응축)	5%-95% (비응축)	5%-95% (비응축)	5%-95% (비응축)
작동 고도	0m - 3000m (1000m 당 1°C 의 온도 저하)	0m - 3000m (1000m 당 1°C 의 온도 저하)	0m - 3000m (1000m 당 1°C 의 온도 저하)	0m - 3000m (1000m 당 1°C 의 온도 저하)	0m - 3000m (1000m 당 1°C 의 온도 저하)	0m - 3000m (1000m 당 1°C 의 온도 저하)	5.000ft	5.000ft	5.000ft

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

IPS 기술 사양

	NX 900	NX 1400	NX 2400	NX 4400/4420	NX 7400/7420	NX 7400	NX 9450	NX 10000	NX 7400
IPS 성능	10Mbps	20Mbps	50Mbps	250Mbps	1Gbps	1Gbps	2Gbps	4Gbps	4Gbps
동시 연결	4K	7.5K	15K	80K	500K	500K	1M	2M	2M
신규 연결(초 당)	200/Sec	375/Sec	750/Sec	4K/Sec	10K/Sec	10K/Sec	20K/Sec	40K/Sec	40K/Sec
패킷(초 당)	600/Sec	1200/Sec	4K/Sec	20K/Sec	90K/Sec	90K/Sec	105K/Sec	120K/Sec	120K/Sec

능동적 페일 오픈 스위치 기술 사양

	AFO 1G 스위치	AFO 10G 스위치
크기(W x D x H)	8.75" x 11.0" x 1.35" (22.2 x 27.9 x 3.4cm)	6.5" x 14.0" x 1.125" (16.5 x 35.6 x 2.8cm)
관리 포트	(1) DB9 시리얼 콘솔, (1) RJ45 Cat5e 포트 (10/100)	(1) DB9 시리얼 콘솔, (1) RJ45 Cat5e 포트 (10/100)
네트워크 포트	(2) RJ45 Cat5e 포트 (10/100/1000)	(1) 쿼드 LC 커넥터
모니터링 포트	(2) RJ45 Cat5e 포트 (10/100/1000)	(2) XFP 포트
AC 전원 입력	100~240VAC, 0.5A, 47-63Hz	100~240VAC, 1.0 A, 47-63Hz
작동 온도	10°C에서 40°C	10°C에서 40°C

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

FireEye Korea | 서울특별시 강남구 테헤란로 440 포스코센터 서관 11층 | 02.559.073 | korea.info@fireeye.com | www.fireeye.kr

FireEye