Trellix

데이터시트

Trellix® 이메일 보안

포괄적인 이메일 위협 방어

이메일은 고객, 공급업체, 파트너, 그리고 동료 간의 연결 수단이며, 여전히 가장 효과적인 공격 경로입니다. 전체 사이버 공격의 90% 이상이 피싱으로 시작됩니다. 사이버 범죄자들은 사용자가 악성 URL을 클릭하거나 감염된 첨부파일을 열도록 유도하기 위해 정교한 사회공학 기법을 활용합니다. 기업들이 협업 플랫폼과 엔터프라이즈 애플리케이션을 확장하며 파트너십을 강화하는 과정에서, 공격자들은 이러한 대부분 보호되지 않은 공격 벡터를 적극적으로 악용하고 있습니다.

솔루션 개요

Trellix는 업계에서 가장 포괄적인 엔터프라이즈 커뮤니케이션 및 협업 보안 솔루션을 제공합니다. 이 솔루션은 온프레미스 또는 AWS 환경에, 주요 보안 이메일 게이트웨이 뒤에 인라인 또는 BCC 모드로 배치됩니다.

Trellix Email Security–Server는 랜섬웨어, 비즈니스 이메일 침해, 스피어 피싱, 자격 증명 탈취, 첨부파일 기반 공격 등을 내부 환경에 진입하기 전에 식별하고, 격리하며, 즉시 차단하는 업계 최고 수준의 탐지 기능을 제공합니다. 최신 URL 기반 공격도 실시간으로 차단하며, 대응 우선순위 설정과 조치를 가속화할 수 있도록 상황 정보까지 함께 제공합니다.

Email Security–Server는 Trellix의 학습형 적응 보안 생태계의 핵심으로, 전 세계 40,000개 이상의 기업 고객, 기술 파트너, 서비스 제공 네트워크로부터 수집된 위협 데이터를 상호 연관 분석하며, 알려진 위협은 물론 신종 위협에도 선제적으로 대응할 수 있도록 지원합니다.

또한 Trellix Intelligent Virtual Execution(IVX)과 결합되어 이메일 인프라, 엔터프라이즈 애플리케이션, 협업 플랫폼 전반에 걸쳐 안전한 협업 환경을 제공합니다.

주요 기능

우수한 위협 탐지

공격자들은 이메일 인프라 탐지를 피하기 위해 다단계 방식의 공격을 설계합니다. 예를 들어, 다단계 피싱 캠페인은 먼저 자격 증명을 탈취한 뒤, 이를 이용해 메일 서버에 로그인하고 조직 내로 피싱 메일을 배포합니다. 피싱은 거의 모든 사용자가 URL을 클릭하도록 속일 수 있어 공격자들에게 인기가 많으며, 랜섬웨어 역시 이메일을 통해 시작되고, 데이터 암호화를 위해 C2(명령 및 제어) 서버로의 콜백을 필요로 합니다.

고급 URL 방어

Trellix Email Security–Server는 여러 가지 고급 URL 방어 기술을 통해 악성 URL을 식별하고, 자격 증명 탈취 및 스피어 피싱 공격으로부터 조직을 보호합니다. 이 기능은 계속해서 진화하며, 피싱 사이트가 탐지를 회피하려는 최신 기법에 대응할 수 있도록 설계되었습니다.

고급 악성코드 방어

MalwareGuard는 바이너리 파일을 입력 받아 의심 점수를 산출하는 머신러닝 기반 도구입니다. 모든 PE(Portable Executable) 파일을 분석하여 점수 기반으로 악성 여부를 판단하고, 탐지 항목에 고유 이름을 지정합니다.

악성코드 탐지 엔진은 다음과 같은 항목에서 숨겨진 이메일 위협을 분석하고 격리합니다:

- EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4, ZIP/RAR/TNEF 등 다양한 첨부파일 유형
- 암호로 보호되거나 암호화된 첨부파일
- 이미지로 암호가 전달된 첨부파일
- 이메일, Microsoft 365 문서, PDF, 압축 파일(ZIP, ALZip, JAR), 및 기타 파일 유형(인코딩되지 않은 파일, HTML)에 포함된 URL
- URL을 통해 다운로드된 파일, 난독화 · 스푸핑 · 단축 · 동적 리디렉션된 URL
- 자격 증명 피싱 및 타이포스쿼팅 URL
- 알려지지 않은 Windows/macOS 운영체제, 브라우저, 애플리케이션 취약점
- 스피어 피싱 이메일에 포함된 악성 코드
- QR 코드

이메일 첨부파일과 URL을 실제로 실행(디토네이션)하여, 이전에 정상으로 보였던 파일이 무기화되었는지를 판별함으로써 조직을 피싱 및 랜섬웨어로부터 한층 더 강력하게 보호합니다. Trellix IVX는 시그니처에 의존하지 않는 동적이고 인텔리전스 기반의 분석 엔진으로, 실시간 다중 흐름(multi-flow), 다중 벡터(multi-vector) 분석을 통해 의심스러운 객체를 정밀하게 검사하고, 표적형 · 은폐형 · 신종 위협을 식별 및 차단합니다. 또한, 잠재적으로 악성인 객체가 실행될 때 사용된 단말기 환경을 모방할 수 있도록 가상머신 이미지(Guest Image)를 사용자 정의하여 구성할 수 있습니다.

Trellix Dynamic Threat Intelligence

- 시기적절하고 광범위한 위협 가시성 제공
- 탐지된 악성코드 및 첨부파일의 세부 기능 식별
- 위협 행위자의 활동을 추적하고, 대응 우선순위를 설정하며 대응 속도를 향상시킬 수 있는 상황 정보 제공
- 이메일에 포함된 URL을 re-write하여 사용자 보호
- 스피어 피싱 공격을 사후 식별하고, 악성 URL을 강조하여 피싱 사이트 접근 차단

진화하는 위협 환경에 대한 빠른 적응

Trellix Email Security – Server는 Trellix Dynamic Threat Intelligence(DTI) Cloud로부터 실시간 위협 인텔리전스를 받아 조직의 이메일 위협 방어 능력을 지속적으로 조정하고 강화할 수 있도록 지원합니다.

탐지, 조사, 대응의 통합

현대의 보안 위협은 그 어느 때보다도 빠르게 진화하고 있으며, 단편적인 기존 솔루션만으로는 보호가 어렵습니다.
Trellix Email Security – Server는 Trellix의 적응형 보안 생태계의 중심에서, 전 세계 고객, 파트너, 서비스 제공자 네트워크로부터 수집된 위협 데이터를 상시 모니터링하고 연관 분석합니다.

Trellix의 AI 알고리즘, 머신러닝 모델, 보안 분석 기술은 이 데이터를 활용해 공격자보다 빠르게 위협을 차단할 수 있도록 탐지 능력을 강화합니다.
Email Security – Server는 조직의 보안 운영 체계와 정렬된 통합 탐지 · 조사 · 대응 기능을 제공합니다. 보안 분석가는 새롭게 발견된 IOC를 기준으로 기존 이메일을 역추적해 침해의 근원을 신속하게 파악할 수 있으며, 전달 이후 무기화된 이메일을 회수(Claw-back)하여 사고 대응 속도를 높일 수 있습니다.
Trellix 고급 위협 분석 센터의 전문가들은 취약점 및 악성코드 캠페인, 그 배후의 국가 및 공격자들을 추적하며, 풍부한 상황 정보를 제공해 신속한 대응을 가능하게 합니다. Trellix XDR 또는 타사 SIEM/XDR 솔루션과 연계하면, 엔드포인트 · 네트워크 · 다양한 보안 신호를 기반으로 한 풍부한 메타데이터와 함께 이메일 경고를 연계 분석할 수 있어, 다단계 · 다중 벡터 공격으로부터의 실시간 보호를 실현합니다.

Table 1. Technical specifications

	EX 3600	EX 5600	EX 8600
성능*	시간당 최대 875개의 고유 첨부파일 분석	시간당 최대 2,200개의 고유 첨부파일 분석	시간당 최대 3,300개의 고유 첨부파일 분석
네트워크 인터페이스 포트	1 X 10/100/1000BASE-T port (Live Mode Analysis) 2 X 10/100/1000BASE-T port (SMTP interface ports)	2x 1GigE BaseT	4x SFP+ (supporting 10GigE Fiber, 10GigE Copper, 1GigE Copper), 2x 1GigE BaseT
관리 포트	1 X 10/100/1000BASE-T port	2x 1GigE BaseT	2x 1GigE BaseT
IPMI 모니터링	Included	Included	Included
VGA 포트 (후면 패널)	Included	Included	Included
USB 포트 (후면 패널)	USB2.0, USB3.2	2x USB3.1 Type A	2x USB3.1 Type A
시리얼 포트 (후면 패널)	DB9 (115,200 bps, No Parity, 8 Bits, 1 Stop Bit)	DB9 (115,200 bps, No Parity, 8 Bits, 1 Stop Bit)	DB9 (115,200 bps, No Parity, 8 Bits, 1 Stop Bit)
저장 용량	4x 4TB HDD, RAID 10, 3.5 inch, FRU	4x 4TB, RAID 10, HDD 3.5 inch, FRU	4x 4TB, RAID 10, HDD 3.5 inch, FRU
인클로저 형식	1RU, fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack
섀시 크기 (가로x깊이x높이)	17.2" X 19.98" X 1.7" (437 mm x 507 mm x 43 mm)	19"x26"x3.5" (482.6 x 660.4 x 88.9 mm)	19"x26"x3.5" (482.6 x 660.4 x 88.9 mm)
AC 전원 공급	Redundant (1+1), FRU, 400W with Input 1100-240VAC / 6.0 – 3.0A | 200-240VDC / 3.4- 3.2A, 50-60 Hz IEC60320- C14 inlet	Redundant (1+1),FRU,920W with Input 100-240V,11-4.4A, 50-60 Hz IEC60320-C14 inlet	Redundant (1+1),FRU,920W with Input 100-240V,11-4.4A, 50-60 Hz IEC60320-C14 inlet
DC 전원 공급	Not Available	Not Available	Not Available
최대 열 방출 전력	1024 BTU/hr	480 watts (1,637 BTU per hour)	580 watts (1,978 BTU per hour)
어플라이언스 단독 / 배송 시 무게	39.3 lbs	44.1 lbs (20.0 kg) / 67 lbs (30.4 kg)	44.1 lbs (20.0 kg) / 67 lbs (30.4 kg)
안전 규격 준수	EN IEC 62368-1:2018+A11:2020 UL 62368-1 CSA 22.2 No. 62368-1 CNS 15598-1 IS 13252 (Part-1)/IEC 60950-1	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
EMC(전자파 적합성) 규격 준수	EN 55032:2015/A11:2020, EN 55035:2017/A11:2020, EN 61000-3-2:2014, EN 61000-3-3:2013 BS EN 55032:2015 BS EN55035:2017 AS/NZS CISPR 32:2015 KS C 9832 KS C 9835 VCCI-CISPR 32:2016 FCC CFR 47 Part 15 CAN ICES-003 CNS 15936	FCC Part 15 ICES-003 Class 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 & V-3/2015	FCC Part 15 ICES-003 Class 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 & V-3/2015
환경 규제 준수	Directive 2011/65/EU CNS 15663	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU
작동 온도	5° to 35° C (41°F - 95°F)	5°C - 35°C (41°F - 95°F)	5°C - 35°C (41°F - 95°F)
작동 상대 습도	8% - 90% (non-condensing)	5% - 95% (non-condensing)	5% - 95% (non-condensing)
작동 고도	0 to 5000ft	0 to 5000ft	0 to 5000ft

Table 2. Trellix Virtual Execution smart grid 사양

	VX 12600
운영 체제 지원	Linux macOS X Microsoft Windows
성능	5100 attachments per hour
고가용성	N+1
관리포트 (후면 패널)	1x 1G/10G Base-T
클러스터 포트(후면 패널)	1x 1G/10G Base-T 4x 1G/10G SFP+
IPMI 포트 (후면 패널)	Included
전면 LCD & 키패드	No LCD
VGA 포트	Included
USB 포트 (후면 패널)	2x USB 3.1 ports
시리얼 포트 (후면 패널)	115,200 bps, no parity, 8 bits, 1 stop bit
드라이브 용량	4x 4TB 3.5" SAS3 HDD, RAID10, hot swappable, FRU
인클로저 형식	2RU, fits 19 inch rack
섀시 크기(가로x깊이x높이)	19in x 26 x 3.5 in (482.6 x 660.4 x 89 mm)
DC 전원 공급	Not available
AC 전원 공급	Redundant (1+1), FRU, 1000W/1200W with Input 100-127/200 - 240Vac, 15-12A/8.5-7A, 50-60 Hz IEC60320-C14 inlet
최대 전력 소비 (watts)	948 watts
최대 열 방출 (BTU/h)	3232 BTU/h
MTBF (h)	Coming soon
어플라이언스 단독 / 배송 시 무게(lb/kg)	44 lbs (20 kg) / 70 lbs (31.8 kg)
보안 인증	FIPS 140-2 Level 1, CC NDcPP v2.2e (pending)
안전 규정 준수	CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368, EN 62368 BS EN 62368
EMC 규정 준수	FCC Part 15 Class-A, CE (Class-A) CNS 13438 CISPR 32 VCCI-CISPR32
작동 고도	0 to 5000ft
환경 규정 준수	RoHS REACH
작동 온도	0-35°C (50-95°F)

Table 2. Trellix Virtual Execution smart grid 사양

	VX 12600
비작동 온도	-40°C-70°C (-40-158°F)
작동 상대 습도	8%-90% non-condensing
비작동 상대 습도	5%-95% non-condensing
작동 고도	1,524 m (5,000 ft)

Table 3. Trellix Email Security – Server Smart Node 가상 센서 사양

	EX 5500V	EX Int 2500V
운영 체제 지원	Microsoft Windows, Apple macOS X	Microsoft Windows, Apple macOS X
성능*	시간당 최대 1,250개의 고유 첨부파일 분석	시간당 최대 350개의 고유 첨부파일 분석
네트워크 모니터링 포트	2	1
네트워크 관리 포트	2	1
CPU 코어 수	8	8
메모리	16 GB	16 GB
저장 용량	384 GB	384 GB
네트워크 어댑터	VMXNet 3, vNIC	VMXNet 3, vNIC
하이퍼바이저 지원	VMware ESXi 6.0 or later	VMware ESXi 6.0 or later

Table 4. Trellix Virtual Execution models on VMware and Nutanix

Model	Throughput	Disk	vCPU	Memory	Network Interfaces	VM Number	VM Instance Type
IVX-VM300	3 subs/min 4320 files/day	1 TB - Thick Provisioning	16	32 GB	1 management port 4 cluster ports	16	VMware ESXi, Nutanix

* 모든 성능 수치는 시스템 구성 및 처리되는 트래픽 특성에 따라 달라질 수 있습니다.

더 자세한 정보는 trellix.com 에서 확인하실 수 있습니다.