Trellix

Cyberworld

Trellix 电子邮件安全(EX) 服务器版

全面的企业通信和协作安全

电子邮件连接客户、供应商、合作伙伴和同事，而且是最容易受到网络攻击的媒介。超过90%的企业攻击始于网络钓鱼电子邮件。攻击者利用有针对性的社交工程，诱骗用户点击恶意 URL，打开不安全的附件。随着公司扩展协作平台和企业应用程序来深化合作伙伴关系，攻击者也开始利用这一基本不受保护的攻击媒介。

解决方案概述

Trellix 提供业界最全面的企业通信和协作安全解决方案。Trellix 电子邮件安全服务器版以内联或密件抄送模式部署在主要安全电子邮件网关后面，还支持 AWS 裸机实例，最大限度地降低了代价高昂的违规风险。

亮点

- 支持对Microsoft Windows 和 Apple macOS X 操作系统镜像的分析。
- 检查电子邮件中是否存在隐藏在受密码保护的文件、加密附件和URL中的威胁。
- 使用集成或分布式IVX服务进行本地部署。
- 元数据流式传输到第三方 SIEM 解决方案。
- 支持自定义 YARA 规则以提高威胁检测效率。

Trellix电子邮件安全服务器版提供业界领先的、出色的检测功能，能够在勒索软件、商业电子邮件泄露、鱼叉式网络钓鱼、凭据窃取和基于附件的攻击进入您的环境之前识别、隔离并立即阻止这些攻击。Trellix电子邮件安全服务器版解决方案可识别、隔离和阻止最新的URL攻击，提供上下文情报，以确定优先级并加快响应速度。

集成的调查和响应
确保与您的整体安全运维计划保持一致

Trellix 电子邮件安全服务器版通过与其他 Trellix 扩展检测和响应 (XDR) 产品集成，可以更广泛地了解多向量混合攻击，从而进行实时保护。

使用 Trellix 中央管理系统查看实时警报、创建智能自定义规则并生成报告。

Trellix 电子邮件安全与 Trellix IVX (Intelligent Virtual Execution) 相结合，提供了全面的企业通信和协作安全解决方案，涵盖电子邮件基础设施、企业应用程序和协作平台，确保人们能够在企业中安全地协同工作。

电子邮件安全服务器版是 Trellix 学习和自适应生态系统的重要组成部分，它提供重要的第二层保护，保护电子邮件基础设施。Trellix 持续监察威胁形势，关联从全球40,000多家企业客户、技术合作伙伴和服务供应商网络收集的威胁数据，确保您始终领先于已知和新兴威胁。

主要功能

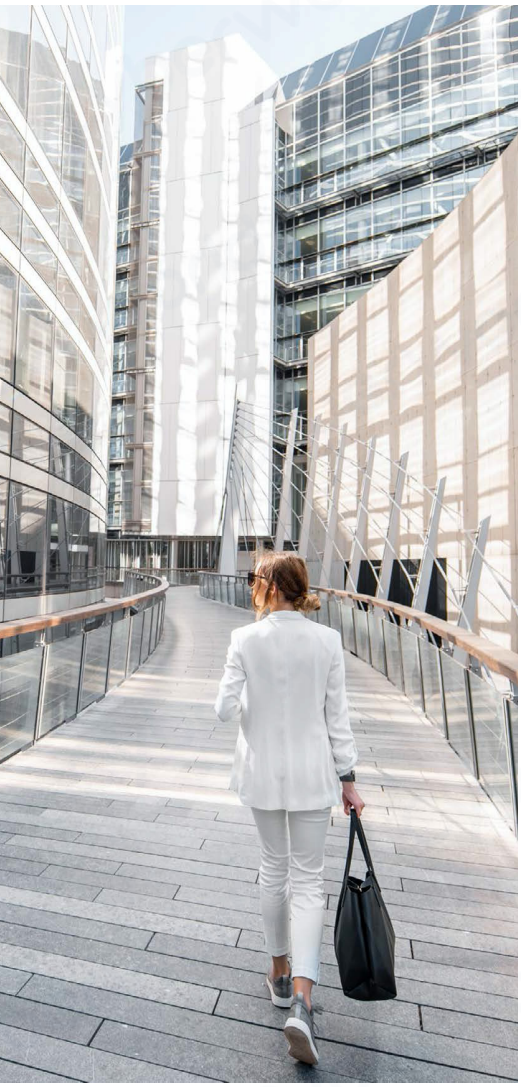
出色的威胁检测

攻击者使用多阶段攻击活动，旨在规避电子邮件基础设施供应商。例如，在多阶段网络钓鱼攻击中，攻击者首先窃取凭据，然后使用被盗凭据登录邮件服务器，并在整个企业内分发网络钓鱼电子邮件。网络钓鱼在攻击者中很受欢迎，因为可以通过有针对性的社交工程来诱骗任何用户点击URL。虽然勒索软件攻击始于电子邮件，但需要回调命令和控制服务器才能加密数据。

先进的 URL 防御技术

电子邮件安全服务器版提供多种先进的URL防御技术来识别恶意URL，保护您的企业免受凭据窃取和鱼叉式网络钓鱼攻击。

该解决方案中的 Advanced URL Defense、MalwareGuard 和 IVX 引擎会分析并隔离被阻止的电子邮件，以查找其中隐藏的未知或高级威胁：



- 附件类型包括EXE、DLL、PDF、SWF、DOC/DOCX、XLS/XLSX、PPT/PPTX、JPG、PNG、MP3、MP4 和 ZIP/RAR/TNEF 档案。
- 受密码保护和加密的附件。
- 通过图像发送的带有密码的加密附件。
- 嵌入在电子邮件、Microsoft 365 文档、PDF、存档文件(ZIP、ALZip、JAR)和其他文件类型(未编码、HTML) 中的 URL 。
- 通过 URL(包括 FTP 链接)下载的文件。
- 混淆、欺骗、缩短和动态重定向的 URL 。
- 凭据式网络钓鱼和仿冒 URL 。
- 未知的 Microsoft Windows 和 Apple macOS X 操作系统镜像、浏览器和应用程序漏洞。
- 鱼叉式网络钓鱼电子邮件中嵌入的恶意代码。

Advanced URL Defense 的多个功能可帮助您的企业实现无与伦比的防御，以抵御凭据窃取和鱼叉式网络钓鱼攻击。Advanced URL Defense 不断发展并增强了对网络钓鱼站点的规避缓解措施，以保护您的企业免受试图规避检测可疑 URL 技术的攻击者的威胁。

恶意软件防护

MalwareGuard是一款机器学习实用程序，它将二进制文件作为输入内容，并输出可疑性分数。它会检查网络上的每个可移植可执行(PE)文件。根据分数做出决定，并为 MalwareGuard 触发的检测分配名称。

Trellix IVX 会引爆所有电子邮件附件和 URL，确定以前合规的文件是否已被武器化，进一步保护您的企业免受网络钓鱼和勒索软件的侵害。

IVX是一款无特征码、动态的智能分析引擎，通过实时多流、多向量分析来检测可疑对象，以识别和阻止针对性、逃避性和新出现的威胁。

另一种规避检测措施是 Guest Image，可以自定义，模仿“使用过的”终端执行潜在恶意软件。通过确保 Guest Image 再现终端域、域用户、Outlook数据和浏览器历史记录，可以防止许多规避技术。

快速适应不断变化的威胁形势

Trellix 电子邮件安全服务器版通过 Trellix 动态威胁情报 (Dynamic Threat Intelligence, DTI) 云服务提供的实时威胁情报，帮助您的企业不断调整主动防御措施，从而抵御电子邮件威胁。关于威胁和攻击者的深度情报，它能将入侵者、机器和受害者的情报结合起来：

- 提供及时、全面且可视化的威胁情报。
- 检测到的恶意软件和不安全的附件，识别其特定功能和特性。
- 提供上下文关联分析，以确定优先级并加速对攻击者的响应，跟踪他们在您企业内的活动。
- 确定攻击者的可能身份与动机。
- 重写电子邮件中嵌入的所有URL，保护用户免受恶意链接的侵害。
- 通过突出显示恶意URL，防止访问网络钓鱼站点，主动追溯识别鱼叉式网络钓鱼攻击。

集成检测、调查和响应

安全威胁变得越来越动态和复杂，而静态和孤立的解决方案已经不足以保护您的业务。Trellix 电子邮件安全服务器版是 Trellix 学习和自适应生态系统不可或缺的一部分。Trellix 生态系统持续监察威胁形势，关联从世界各地的客户、技术合作伙伴和服务供应商网络收集的威胁数据。

Trellix的人工智能算法、机器学习模型和安全分析运用这些威胁情报，以对手的速度加强威胁预防和检测，以便您领先于已知和新出现的电子邮件威胁。

Trellix电子邮件安全服务器版支持集成调查和响应，以配合您更大的安全运维计划。分析师可以通过在之前收到的电子邮件中搜索新识别的IOC来执行回顾性分析，以快速识别攻击源。分析师还可以收回在发送后被武器化的电子邮件，简化并加速事件响应。

Trellix高级研究中心杰出的情报分析师积极追踪漏洞、恶意软件活动以及其背后的攻击者，提供丰富的上下文情报以告知和加速响应。

使用Trellix XDR或其他第三方SIEM、XDR供应商来获得针对多向量、多阶段攻击的实时防护，将具有丰富元数据的电子邮件警报与来自终端、网络和其他安全控制的信号关联起来。

全面且有弹性的防护可抵御电子邮件威胁

Trellix 电子邮件安全服务器版分析每个电子邮件附件和 URL，准确识别当今的高级攻击。来自整个Trellix安全生态系统的实时更新，结合已知攻击者的警报归因，为确定关键警报的优先级和采取行动以及阻止高级电子邮件攻击提供了上下文信息。

该工具可以识别已知、未知和非恶意软件威胁，最大程度减少噪音和误报，这样您就可以将资源集中在真正的攻击上，从而帮助降低运维费用。风险软件分类将真正的入侵企图与不良但恶意程度较低的活动（如广告软件和间谍软件）区分开来，以优先处理警报响应。Trellix电子邮件安全服务器与其他安全解决方案集成，以检测跨不同技术和产品的威胁。

表 1. 技术规格

	EX 3600	EX 5600	EX 8600
性能	每小时最多处理875个独立附件	每小时最多处理2200个独立附件	每小时最多处理3300个独立附件
网络接口端口	1X10/100/1000BASE-T端口（实时模式分析） 2X10/100/1000BASE-T端口（SMTP 接口端口）	2x 1GigE BaseT	4x SFP+（支持 1GbaseSX、10GbaseSR、1GbaseLX、10GbaseLR、10GbaseCU、1GbaseT）
管理端口	1 X 10/100/1000BASE-T 端口	2x 1GigE BaseT	2x 1GigE BaseT
IPMI 监控	包含	包含	包含
VGA 端口（后面板）	包含	包含	包含
USB 端口（后面板）	USB2.0、USB3.2	2 个 USB3.1 A 型	2 个 USB3.1 A 型
串行端口（后面板）	DB9(115200bps、无奇偶校验、8个数据位、1 个停止位)	DB9(115200bps、无奇偶校验、8个数据位、1个停止位)	DB9(115200bps、无奇偶校验、8个数据位、1个停止位)
存储容量	4x 4TB HDD，RAID 10，3.5 英寸，FRU	4x 4TB，RAID 10，3.5 英寸 HDD，FRU	4x 4TB，RAID 10，3.5 英寸 HDD，FRU
外接盒	1 RU，适合19英寸机架	2 RU，适合19英寸机架	2 RU，适合19英寸机架
机箱尺寸 宽x长x高	17.2 英寸（437 毫米）X 19.98 英寸（507 毫米）X 1.7 英寸（43 毫米）	19 英寸（482.6 毫米）X 26 英寸（660.4 毫米）X 3.5 英寸（88.9 毫米）	19 英寸（482.6 毫米）X 26 英寸（660.4 毫米）X 3.5 英寸（88.9 毫米）
AC电源	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电源	不适用	不适用	不适用
最大热功率	1024 BTU/h	480 瓦（1637 BTU/h）	580 瓦（1978 BTU/h）
设备本身/发货重量	39.3 磅	44.1 磅（20.0 kg）/ 67 磅（30.4 kg）	44.1 磅（20.0 kg）/ 67 磅（30.4 kg）
安全合规性	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

	EX 3600	EX 5600	EX 8600
EMC 合规性	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 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
环境合规性	指令 2011/65/EU CNS 15663	RoHS 指令 2011/65/EU;REACH; WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU;REACH; WEEE 指令 2012/19/EU
运行温度	5°C - 35°C 41°F - 95°F	5°C - 35°C 41°F - 95°F	5°C - 35°C 41°F - 95°F
运行相对湿度	8% - 90% (无结露)	5% - 95% (无结露)	5% - 95% (无结露)
正常运行的海拔高度	0-5000 英尺	0-5000 英尺	0-5000 英尺

表 2. Trellix Virtual Execution 智能系统网络的规格

	VX 5500	VX 12550	VX 12600
支持的操作系统	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
性能	每小时可处理600个独立附件	每小时可处理5100个独立附件	每小时可处理5100个独立附件
高可用性	N+1	N+1	N+1
管理端口(后面板)	1x 10/100/1000 Mbps BASE-T	1x 10/100/1000 Mbps BASE-T	1x 1G/10G Base-T
集群端口(后面板)	3x 10/100/1000 Mbps BASE-T	1x 10/100/1000 Mbps BASE-T, 2x 10 Gbps BASE-T, 4x 10 GigE SFP+ 端口	1x 1G/10G Base-T 4x 1G/10G SFP+
IPMI 端口(后面板)	包含	包含	包含
前 LCD 和键盘	不适用	没有 LCD	没有 LCD
VGA 端口	包含	包含	包含
USB 端口(后面板)	4 个 A 型 USB 端口	2 个 A 型 USB 端口	2 个 USB 3.1 端口
串行端口(后面板)	115200bps、无奇偶校验、 8个数据位、1个停止位	115200bps、无奇偶校验、 8个数据位、1个停止位	115200bps、无奇偶校验、 8个数据位、1个停止位

	VX 5500	VX 12550	VX 12600
驱动器容量	2x 2TB 3.5” SAS3 HDD, RAID 1, hot-swappable, FRU	2x 4TB 3.5” SAS3 HDD, RAID 1, hot-swappable, FRU	4x 4TB 3.5” SAS3 HDD, RAID10, hot-swappable, FRU
外接盒	1 RU，适合19英寸机架	2 RU，适合19英寸机架	2 RU，适合19英寸机架
机箱尺寸 宽x长x高	17.2 英寸 (437 毫米) X 25.6 英寸 (650 毫米) X 1.7 英寸 (43.2 毫米)	17.2 英寸 (437 毫米) X 31 英寸 (787 毫米) X 3.5 英寸 (89 毫米)	19 英寸 (482.6 毫米) X 26 英寸 (660.4 毫米) X 3.5 英寸 (89 毫米)
DC电源	不适用	不适用	不适用
AC电源	Redundant (1+1) 750 watt, 100–240 VAC, 8 - 3.8 A, 50–60 Hz, IEC60320-C14, inlet, hot-swappable, FRU	Redundant (1+1) 1000 watt, 100–240 VAC 10.5–4.0A, 50–60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1),FRU,1000W/1200W with Input 100-127/200 - 240Vac, 15 12A/8.5- 7A, 50-60 Hz IEC60320-C14 inlet
最大功耗 (瓦)	285 瓦	660 瓦	948 瓦
最大散热量 (BTU/h)	972 BTU/h	2594 BTU/h	3232 BTU/h
平均无故障时间 (h)	54200 h	54041 h	即将推出
设备本身/发货重量磅 (kg)	27.0 磅 (12.2 kg) / 38.0 磅 (17.2 kg)	44 磅 (20 kg) / 71 磅 (32.2 kg)	44 磅 (20 kg) / 70 磅 (31.8 kg)
安全认证	FIPS 140-2 等级 1, CC NDcPP v2.2e	FIPS 140-2 等级 1, CC NDcPP v2.2e	FIPS 140-2 等级 1, CC NDcPP v2.2e (待定)
安全合规性	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368, EN 62368 BS EN 62368
EMC 合规性	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	FCC Part 15 Class-A, CE (Class-A) CNS 13438 CISPR 32 VCCI-CISPR32 EN 55035 EN 55032 EN 61000 ICES-003 KN 32, KN 35
环境合规性	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS REACH
运行温度	0°C - 40°C 32°F - 104°F	0°C - 40°C 32°F - 104°F	10°C - 35°C 50°F - 95°F
非运行温度	-30°C - 70°C -22°F - 158°F	-30°C - 70°C -22°F - 158°F	-40°C - 70°C -40°F - 158°F

	VX 5500	VX 12550	VX 12600
运行相对湿度	10–95% at 40°C 无结露	10–90% at 40°C 无结露	8–90% 无结露
非运行相对湿度	10–95% at 60°C 无结露	10–95% at 55°C 无结露	5–95% 无结露
正常运行的海拔高度	3000 米 (9842 英尺)	3000 米 (9842 英尺)	1524 米 (5000 英尺)

表 3. Trellix 电子邮件安全服务器版 智能节点虚拟传感器的规格

	EX 5500V
支持的操作系统	Microsoft Windows Apple macOS X
性能*	每小时最多处理1250个独立附件
网络监控端口	2
网络管理端口	2
CPU 核心	8
内存	16 GB
驱动器容量	384 GB
网络适配器	VMXNet 3, vNIC
支持的Hypervisor	VMware ESXi 6.0 或更高版本

*根据系统的配置和所处理的网络流量，所有性能值都会发生变化。

Trellix

关于 Trellix
Trellix是一家重新定义网络安全未来的全球性公司。它的开放式原生扩展检测和响应 (XDR) 平台，可帮助企业抵御当今最先进的网络威胁攻击，并保护其业务不受影响。Trellix安全团队和庞大的合作伙伴生态系统，运用人工智能、机器学习和自动化加速技术创新，为 40,000 多家企业客户提供服务。