Trellix

DATASHEET

Trellix Email Security - Server

Comprehensive enterprise communication and collaboration security

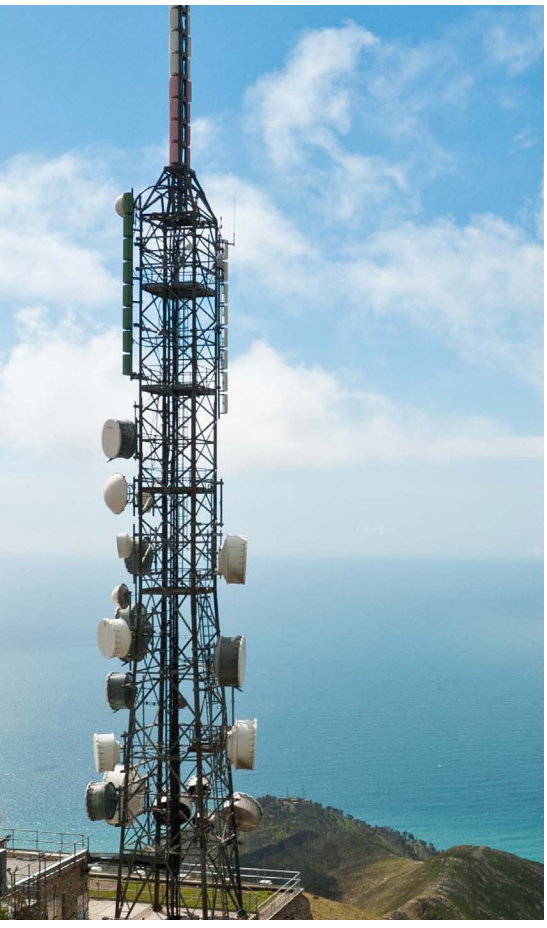
Email connects customers, suppliers, partners, and coworkers—and continues to be the most successful attack vector. Over 90 % of cyberattacks begin with phishing. Cybercriminals use targeted social engineering to trick users into clicking malicious URLs and opening compromised attachments. And as companies extend collaborative platforms and enterprise applications to transform partner relationship, threat actors are already exploiting this largely unprotected attack vector.

Solution Overview

Trellix provides the industry's most comprehensive enterprise communication and collaboration security solution. Deployed on premise behind the primary secure email gateway as in-line or bcc mode, Trellix

Highlights

- Supports analysis against Microsoft Windows and Apple macOS x operating system images
- Examines email for threats hidden in password-protected files, encrypted attachments, and URLs.
- Deploys on premises with integrated or distributed IVX service
- Metadata streaming to third party SIEM solutions
- Supports custom YARA rules to enhance threat detection efficacy



Email Security-Server also supports AWS bare metal form factor and minimizing the risk of costly breaches.

Trellix Email Security – Server offers superior detection that leads the industry in identifying, isolating, and immediately stopping ransomware, business email compromise, spear phishing, credential harvesting, and attachment-based attacks before they enter your environment. Trellix Email Security-Server solution identifies, isolates and blocks the latest URL attacks and provides contextual insights to prioritize and accelerate response.

Integrated investigation and response ensure alignment with your overall security operations program.

By integrating with additional Trellix extended detection and response (XDR) products Trellix Email Security-Server provides broader visibility into multi-vector blended attacks for coordinated real-time protection.

Use the Trellix Central Management System to view real-time alerts, create smart custom rules and generate reports.

Trellix Email Security, paired with Trellix Intelligent Virtual Execution (IVX) provides a comprehensive enterprise communication and collaboration security solution, spanning email infrastructure, enterprise applications, and collaboration platforms, ensuring people can work together securely across the extended enterprise.

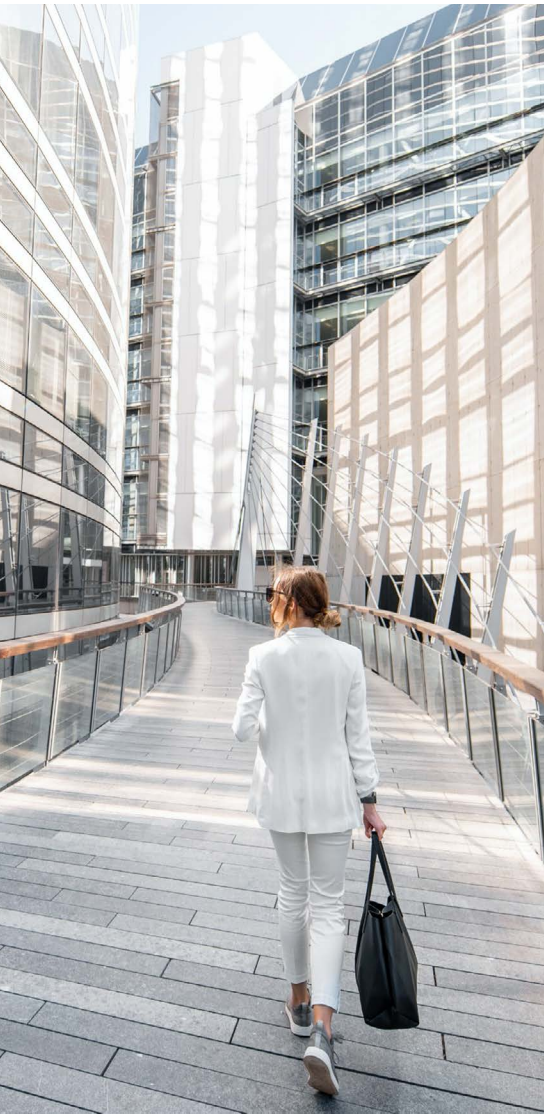
Providing a critical second layer of protection to secure email infrastructure, Email Security –Server is an integral part of the Trellix learning and adaptive ecosystem. Trellix continuously monitors the threat landscape, correlating threat data gathered from more than 40k enterprise customers, technology partners, and service provider networks around the world, ensuring you stay ahead of known and emerging threats.

Key capabilities

Superior threat detection

Attakers use multi-stage campaigns, designed to evade email infrastructure providers. For example, in multi-staged phishing campaigns, attackers first steal credentials then use the stolen credentials login to the mail server and distribute phishing emails throughout the organization. Phishing is popular among attackers because cybercriminals can use targeted social engineering to trick

almost any user into clicking a URL. While ransomware attacks start with an email, a callback to a command-and-control server is required to encrypt the data.



Advanced URL Defense

Email Security – Server offers multiple advanced URL defense techniques to identify malicious URLs, protecting your organization from credential harvesting and spear-phishing attacks.

Advanced URL Defense, MalwareGuard, and the IVX engine in the solution analyzes and quarantines blocked emails if it finds unknown or advanced threats found hidden in:

- Attachment types including EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4, and ZIP/RAR/TNEF archives
- Password-protected and encrypted attachments
- Password-protected attachments with password sent via image
- URLs embedded in emails, Microsoft 365 documents, PDFs, archive files (ZIP, ALZip, JAR), and other file types (unencoded, HTML)
- Files downloaded through URLs including FTP links
- Obfuscated, spoofed, shortened, and dynamically redirected URLs
- Credential-phishing and typo-squatting URLs
- Unknown Microsoft Windows and Apple mac OS X operating system images, browser, and application vulnerabilities
- Malicious code embedded in spear-phishing emails

The many features of Advanced URL Defense can help your organization achieve unparalleled defense against credential harvesting and spear-phishing attacks. Advanced URL Defense continually evolves and enhances evasion mitigations for phishing sites to keep your organization safe from attackers trying to evade technology that detects suspicious URLs.

Malware protection

MalwareGuard is a machine learning utility that takes binary files as input and outputs a suspiciousness score. It examines every Portable Executable (PE) file on the wire, makes a decision based on the score, and assigns a name to detections.

Trellix Intelligent Virtual Execution (IVX) helps further defend your organization from phishing and ransomware by detonating all email attachments and URLs to determine if previously legitimate files have been weaponized.

IVX is a signature-less, dynamic intelligence-driven analysis engine that inspects suspicious objects using real-time multi-flow, multi-vector analysis to identify and block targeted, evasive and emerging threats.

Guest Image, another evasion mitigation, can be customized to mimic a "used" endpoint when a potentially malicious object is executed. By ensuring Guest Image reproduces an endpoint domain, domain user, Outlook data, and browser history, you can prevent many evasion techniques.

Rapid adaptation to the evolving threat landscape

Trellix Email Security – Server helps your organization continually adapt your proactive protection from email threats via real-time threat intelligence from the Trellix Dynamic Threat Intelligence (DTI) Cloud. It combines deep adversarial, machine, and victim intelligence to:

- Deliver timely and broad threat visibility
- Identify specific capabilities and features of detected malware and malicious attachments
- Provide contextual insights to help you prioritize and accelerate response an attacker and track their activities within your organization
- Determine the probable identity and motives of
- Rewrite all URLs embedded within an email to protect your users from malicious links
- Retroactively identify spear-phishing attacks and prevent access to phishing sites by highlighting malicious URLs

Integrated Detection, Investigation, and Response

Security threats are more dynamic and sophisticated than ever. Static, siloed solutions are simply not enough to protect your businesses. Email Security – Server is an integral part of the Trellix learning and adaptive ecosystem. The Trellix ecosystem continuously monitors the threat landscape, correlating threat data gathered from customer, technology partner, and service provider networks around the world.

Our artificial intelligence algorithms, machine learning models, and security analytics use this threat intelligence to strengthen threat prevention and detection at the speed of the adversary, so you stay ahead of known and emerging email-borne threats.

Trellix Email Security – Server enables integrated investigation and response to align with your larger security operations program. Analyst can perform retrospective analysis by searching for newly identified IOCs in previously received emails to quickly identify the source of a compromise. Analysts can also claw back emails weaponized post-delivery, simplify and accelerating incident response.

Elite intel analysts from Trellix's Advanced Research Center actively track vulnerabilities and malware campaigns—and the nation-states and malicious actors behind them—providing rich contextual intelligence to inform and accelerate response.

Gain real-time protection from multi-vector, multi-staged attack using Trellix XDR, or other third party SIEM/XDR providers, to correlate email alerts with rich metadata with signals from endpoint, network and other security controls.

Comprehensive and resilient, protection from email threats

Email Security – Server analyzes every email attachment and URL to accurately identify today's advanced attacks. Real-time updates from the entire Trellix security ecosystem, combined with alert attribution to known threat actors, provide context for prioritizing and acting on critical alerts and blocking advanced email attacks.

The tool identifies known, unknown, and non-malware-based threats with minimal noise and false positives so you can focus resources on real attacks, helping reduce operational expenses. And riskware categorization separates genuine breach attempts from undesirable, but less malicious activity (such as adware and spyware) to prioritize alert response. Trellix Email Security- Server integrates with other security solutions to detect threats across different technologies and products.

Table 1. Technical specifications

	EX 3600	EX 5600	EX 8600
Performance	Up to 875 unique attachments per hour	Up to 2,200 unique attachments per hour	Up to 3,300 unique attachments per hour
Network interface ports	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 1GbaseSX, 10GbaseSR, 1 GbaseLX, 10GbaseLR, 10GbaseCU, 1GbaseT)
Management ports	1 X 10/100/1000BASE-T port	2x 1GigE BaseT	2x 1GigE BaseT
IPMI monitoring	Included	Included	Included
VGA port (rear panel)	Included	Included	Included
USB ports (rear panel)	USB2.0, USB3.2	2x USB3.1 Type A	2x USB3.1 Type A
Serial port (real panel)	DB9 (115,200 bps, No Parity, 8 Bits, 1 Stop Bit)	DB9 (115,200 bps, No Parity, 8 Bits, 1 Stop Bit)	DB9 (115 8 Bits, 1,200 bps, No Parity, Stop Bit)
Storage capacity	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
Enclosure	1RU, fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack
Chassis dimensions (WxDxH)	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 power supply	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 power supply	Not Available	Not Available	Not Available
Thermal maximum power	1024 BTU/hr	480 watts (1,637 BTU per hour)	580 watts (1,978 BTU per hour)
Appliance alone/As shipped weight	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)
Compliance safety	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
Compliance EMC	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
Environmental compliance	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
Operating temperature	5° to 35° C (41°F - 95°F)	5°C - 35°C (41°F - 95°F)	5°C - 35°C (41°F - 95°F)
Operating relative humidity	8%-90%(non-condensing)	5% - 95% (non-condensing)	5% - 95% (non-condensing)
Operating altitude	0 to 5000ft	0 to 5000ft	0 to 5000ft

Table 2. Trellix Virtual Execution smart grid specifications

	VX 5500	VX 12550	VX 12600
OS support	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Performance	600 unique attachments per hour	5100 unique attachments per hour	5100 unique attachments per hour
High availability	N+1	N+1	N+1
Management ports (rear panel)	1x 10/100/1000 Mbps BASE-T	1x 10/100/1000 Mbps BASE-T	1x 1G/10G Base-T
Cluster Ports (rear panel)	3x 10/100/1000 Mbps BASE-T	1x 10/100/1000 Mbps BASE-T, 2x 10 Gbps BASE-T, 4x 10 GigE SFP+ ports	1x 1G/10G Base-T 4x 1G/10G SFP+
IPMI Port (rear panel)	Included	Included	Included
Front LCD & keypad	Not available	No LCD	No LCD
VGA ports	Included	Included	Included
USB ports (rear panel)	4x Type A USB ports	2x Type A USB Ports	2x USB 3.1 ports
Serial port (rear panel)	115,200 bps, no parity, 8 bits, 1 stop bit	115,200 bps, no parity, 8 bits, 1 stop bit	115,200 bps, no parity, 8 bits, 1 stop bit

	VX 5500	VX 12550	VX 12600
Drive capacity	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
Enclosure	1RU, fits 19 inch rack	2RU, fits 19 inch rack	2RU, fits 19 inch rack
Chassis dimension WxDxH	17. 2 x 25.6 x 1.7 In (437 x 650 x 43.2 mm)	17.2 x 31 x 3.5 in (437 x 787 x 89 mm)	19in x 26 x 3.5 in (482.6 x 660.4 x 89 mm)
DC power supply	Not available	Not available	Not available
AC power supply	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
Power consumption maximum (watts)	285 watts	660 watts	948 watts
Thermal dissipation maximum (BTU/h)	972 BTU/h	2594 BTU/h	3232 BTU/h
MTBF (h)	54,200 h	54,041 h	Coming soon
Appliance alone / as shipped weight lb. (kg)	27.0 lbs (12.2 kg) / 38.0 lbs (17.2 kg)	44 lbs (20 kg) / 71 lbs (32.2 kg)	44 lbs (20 kg) / 70 lbs (31.8 kg)
Security certification	FIPS 140-2 Level 1, CC NDcPP v2.2e	FIPS 140-2 Level 1, CC NDcPP v2.2e	FIPS 140-2 Level 1, CC NDcPP v2.2e (pending)
Regulatory compliance safety	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
Regulatory compliance EMC	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
Environmental compliance	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS REACH
Operating temperature	0-40°C (32-104°F)	0-40°C (32-104°F)	10-35°C (50-95°F)
Non-operating temperature	-30-70°C (-22-158°F)	-30-70°C (-22-158°F)	-40-70°C (-40-158°F)

	VX 5500	VX 12550	VX 12600
Operating relative humidity	10%–95% at 40°C non-condensing	10%–90% at 40°C non-condensing	8%–90% non-condensing
Non-operating relative humidity	10%–95% at 60°C non-condensing	10%–95% at 55°C non-condensing	5%–95% non-condensing
Operating altitude	3,000 m (9,842 ft)	3,000 m (9,842 ft)	1,524 m (5,000 ft)

Table 3. Trellix Email Security – Server Smart Node virtual sensor specifications

	EX 5500V
OS support	Microsoft Windows Apple macOS X
Performance*	Up to 1,250 unique attachments per hour
Network monitoring ports	2
Network management ports	2
CPU cores	8
Memory	16 GB
Drive capacity	384 GB
Network adapters	VMXNet 3, vNIC
Hypervisor support	VMware ESXi 6.0 or later

*All performance values vary depending on the system configuration and traffic profile being processed.

Learn more about Trellix Email Security-Server at:
www.trellix.com/en-us/products/email-security-server.html

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com