DATA SHEET

Trellix® Email Security Server

Comprehensive email threat defense

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. As companies extend collaborative platforms and enterprise applications to transform partner relationships, threat actors are exploiting this largely unprotected attack vector.

Solution Overview

Trellix provides the industry's most comprehensive enterprise communication and collaboration security solution. Deployed on-premises or on AWS behind the primary secure email gateway in-line or in bcc mode, 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 identifies, isolates, and blocks the latest URL attacks and provides contextual insights to prioritize and accelerate response.

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.

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

Key Capabilities

Superior threat detection

Attackers use multi-stage campaigns designed to evade email infrastructure providers. For example, in multi-staged phishing campaigns, attackers first steal credentials, then use them to log in 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 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 continually evolves and enhances evasion mitigations for phishing sites to keep your organization safe from attackers trying to evade technology that detects suspicious URLs.

Advanced Malware Protection

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

Malware detection engines analyze and quarantine email 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 macOS X operating system images, browser, and application vulnerabilities
- Malicious code embedded in spear-phishing emails
- QR Codes

Trellix Intelligent Virtual Execution (IVX) helps further defend your organization from phishing and ransomware by detonating email attachments and URLs to determine if previously legitimate files have been weaponized. Trellix 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. A Guest Image can be customized to mimic a “used” endpoint when a potentially malicious object is executed.

Trellix Dynamic Threat Intelligence

- Delivers timely and broad threat visibility
- Identifies specific capabilities and features of detected malware and malicious attachments
- Provides contextual insights to help you prioritize and accelerate response to an attacker and track their activities within your organization
- Rewrites URLs embedded within an email to protect your users from malicious links
- Retroactively identifies spear-phishing attacks and prevents access to phishing sites by highlighting malicious URLs

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.

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. Trellix 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 customers, technology partners, 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 provides integrated investigation and response to align with your larger security operations program. Analysts 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, simplifying and accelerating incident response. Elite threat intelligence 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 attacks using Trellix XDR or other third-party SIEM/XDR providers to correlate email alerts with rich metadata signals from the endpoint, network, and other security controls.

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 10GigE Fiber, 10GigE Copper, 1GigE Copper), 2x 1GigE BaseT
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 (rear panel)	DB9 (115,200 bps, No Parity, 8 Bits, 1 Stop Bit)	DB9 (115,200 bps, No Parity, 8 Bits, 1 Stop Bit)	DB9 (115,200 bps, No Parity, 8 Bits, 1 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
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 12600
OS support	Linux macOS X Microsoft Windows
Performance	5100 attachments per hour
High availability	N+1
Management ports (rear panel)	1x 1G/10G Base-T
Cluster Ports (rear panel)	1x 1G/10G Base-T 4x 1G/10G SFP+
IPMI Port (rear panel)	Included
Front LCD & keypad	No LCD
VGA ports	Included
USB ports (rear panel)	2x USB 3.1 ports
Serial port (rear panel)	115,200 bps, no parity, 8 bits, 1 stop bit
Drive capacity	4x 4TB 3.5” SAS3 HDD, RAID10, hot swappable, FRU
Enclosure	2RU, fits 19 inch rack
Chassis dimension WxDxH	19in x 26 x 3.5 in (482.6 x 660.4 x 89 mm)
DC power supply	Not available
AC power supply	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)	948 watts
Thermal dissipation maximum (BTU/h)	3232 BTU/h
MTBF (h)	Coming soon
Appliance alone / as shipped weight lb. (kg)	44 lbs (20 kg) / 70 lbs (31.8 kg)
Security certification	FIPS 140-2 Level 1, CC NDcPP v2.2e (pending)
Regulatory compliance safety	CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368, EN 62368 BS EN 62368
Regulatory compliance EMC	FCC Part 15 Class-A, CE (Class-A) CNS 13438 CISPR 32 VCCI-CISPR32
Operating altitude	0 to 5000ft
Enviornmental compliance	RoHS REACH
Operating temperature	0-35°C (50-95°F)

Table 2. Trellix Virtual Execution smart grid specifications

	VX 12600
Non-operating temperature	-40°C-70°C (-40-158°F)
Operating relative humidity	8%-90% non-condensing
Non-operating relative humidity	5%-95% non-condensing
Operating altitude	1,524 m (5,000 ft)

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

	EX 5500V	EX Int 2500V
OS support	Microsoft Windows, Apple macOS X	Microsoft Windows, Apple macOS X
Performance*	Up to 1,250 unique attachments per hour	Up to 350 unique attachments per hour
Network monitoring ports	2	1
Network management ports	2	1
CPU cores	8	8
Memory	16 GB	16 GB
Drive capacity	384 GB	384 GB
Network adapters	VMXNet 3, vNIC	VMXNet 3, vNIC
Hypervisor support	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

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

To learn more about Trellix Email Security Server, visit trellix.com.