Trellix

DATA SHEET

Trellix Email Security – Server

Adaptive, intelligent, scalable protection from email threats

Highlights

- Offers comprehensive email security against malicious attachments, credential-phishing URLs, spoofing, and zero-day and multistage attacks
- 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
- Acquires real-time threat intelligence from Trellix Dynamic Threat Intelligence (DTI) Cloud
- Prioritizes and contains threats by providing contextual insights for alerts
- Deploys on premises with integrated or distributed MVX service

Overview

Email is a key communication channel—and securing yours is a critical part of building a thriving business. But email is also the most vulnerable vector for cyberattacks because it's highly targetable and customizable.

To stay safe from advanced email threats, like URLs linked to credential phishing sites and weaponized file attachments, your organization needs proactive protection that's always adapting

With Trellix Email Security – Server, your organization can minimize the risk of costly breaches caused by advanced email attacks. This on-premises solution empowers you to identify, isolate, and immediately stop URL and attachment-based attacks before they enter your environment. It allows you to:

- Combine intelligence-led context and detection plug-ins to identify malicious and benign phishing URLs
- Identify threats with minimal noise and nearly nonexistent false positives
- Use the signatureless Multi-Vector Virtual Execution (MVX) engine to analyze attachments and URLs against a cross-matrix of operating systems, applications, and web browsers

Trellix collects extensive threat intelligence through firsthand breach investigations and millions of sensors. And Email Security – Server uses this data, concrete evidence, and contextual intelligence to help you prioritize alerts and block threats in real time.

By integrating with additional Trellix extended detection and response (XDR) products, you can get broader visibility into multivector blended attacks and coordinate real-time protection.

Stay safe from email threats

Email Security – Server provides real-time detection and prevention against social engineering, including credential harvesting, impersonation, and spear-phishing attacks that typically evade traditional defenses. It 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 typosquatting URLs
- Unknown Microsoft Windows and Apple macOS X operating system images, browser, and application vulnerabilities
- Malicious code embedded in spear-phishing emails

It also identifies and stops hard-to-detect multistage ransomware attacks, which start with an email but also require a call back to a command-and-control server to encrypt the data.

Superior threat detection

Email Security – Server helps mitigate the risk of costly breaches by identifying and isolating advanced, targeted, and other evasive attacks and analyzing them for faster identification in the future.

Advanced URL Defense, MalwareGuard, and the MVX engine in Trellix Email Security – Server use machine learning and analytics to identify attacks that evade traditional signature and policy-based defenses.

The many features of Advanced URL Defense can help your organization achieve unparalleled defense against credential harvesting and spear-phishing attacks.

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.

The MVX engine detects zero-day, multiflow, and other evasive attacks by using dynamic, signatureless analysis in a safe, virtual environment. It identifies never-before-seen exploits and malware to stop infection and compromise.

Advanced URL Defense includes:

- An image classification engine that uses deep learning to compile and compare screenshots of trusted and commonly targeted brands against web pages referenced by URLs in an email
- A phishing detection plug-in that applies domain and page content analytics to augment machine learning
- A fully automated malware intelligence gathering system that collects social media accounts, blogs, forums, and threat feeds to discover false negatives
- Numerous other AI and machine learning based detection engines

Evasion mitigation

Email Security – Server supports a controlled live mode feature to protect against attacks that evade requests for remote objects. The MVX engine detects malware requiring multiple downloads and returns the remote objects requested by the sample binary. Controlled live mode reduces false negatives for multistage downloads, advanced spear-phishing attacks, and advanced ransomware intrusions.

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.

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.

Integration to improve alert handling efficiency

Adaptive, intelligent, scalable 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.

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
- Determine the probable identity and motives of an attacker and track their activities within your organization
- 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

Response workflow integration

Email Security – Server works seamlessly with Trellix Helix and Central Management System.

Helix, a component of Email Security – Server, provides visibility across the entire infrastructure. It augments email and third-party alerts with intelligence, correlation to the endpoint, automation, and investigative tips, surfacing unseen threats and empowering expert decisions.

Trellix Central Management System correlates alerts from both Email Security – Server and Trellix Network Security to get a broader view of an attack and set blocking rules to prevent the attack from spreading. It also supports role-based tagging to identify who is being targeted and alert response and remediation based on role-based criteria.

Additional capabilities

YARA-based rules enable customization

Email Security – Server enables analysts to specify and test custom rules to analyze email attachments for threats targeting your organization.

Executive impersonation protection

Email Security – Server can block business email compromises (BECs) to protect high-level employees from being spoofed. It creates a policy that compares inbound email display names to an approved list that matches approved envelope senders.

Message queue, alert, and quarantine management

Email Security – Server provides a high degree of control over the emails it scans. For active protection-mode deployments, messages can be tracked and managed as they move through the MTA queue. It uses email attributes to search and verify that messages were received, analyzed, and delivered to the next hop, and it monitors trends over time through an intuitive dashboard. It offers explicit allow and block lists for custom control over email processing, allows common alert attributes to be searched and selected, and performs bulk operations on alerts and quarantined messages.

Active-protection or monitor-only mode

Email Security – Server can analyze emails with potentially malicious links or attachments and quarantine threats for active protection. For monitor-only deployments, organizations can set up a transparent BCC rule to send copies of emails to Trellix for analysis.

Get flexible deployment options

Email Security – Server offers various deployment options to match your needs and budget.

Integrated email security

Standalone, all-in-one hardware appliance with integrated MVX service to secure an email ingress point at a single site.
Email Security – Server is an easy-to-manage solution that deploys in under 60 minutes and doesn't require rules, policies, or tuning.

Distributed email security

Extensible appliances with centrally shared MVX service to secure email ingress points.

Email Smart Node

Virtual sensors analyze email traffic to detect and block malicious messages and submit suspicious activity over an encrypted connection to the MVX service for definitive verdict analysis.

MVX Smart Grid

On-premises, centrally located, elastic MVX service that offers transparent scalability, built-in N+1 fault tolerance, and automated load balancing. Bursting from an integrated hardware appliance to an MVX Smart Grid provides added capacity for detecting and analyzing email threats during peak message throughput periods.

Trellix Cloud MVX

MVX service subscription that ensures privacy by analyzing traffic on the Email Smart Node. Only suspicious objects are sent over an encrypted connection to the MVX service, which discards objects revealed to be benign.

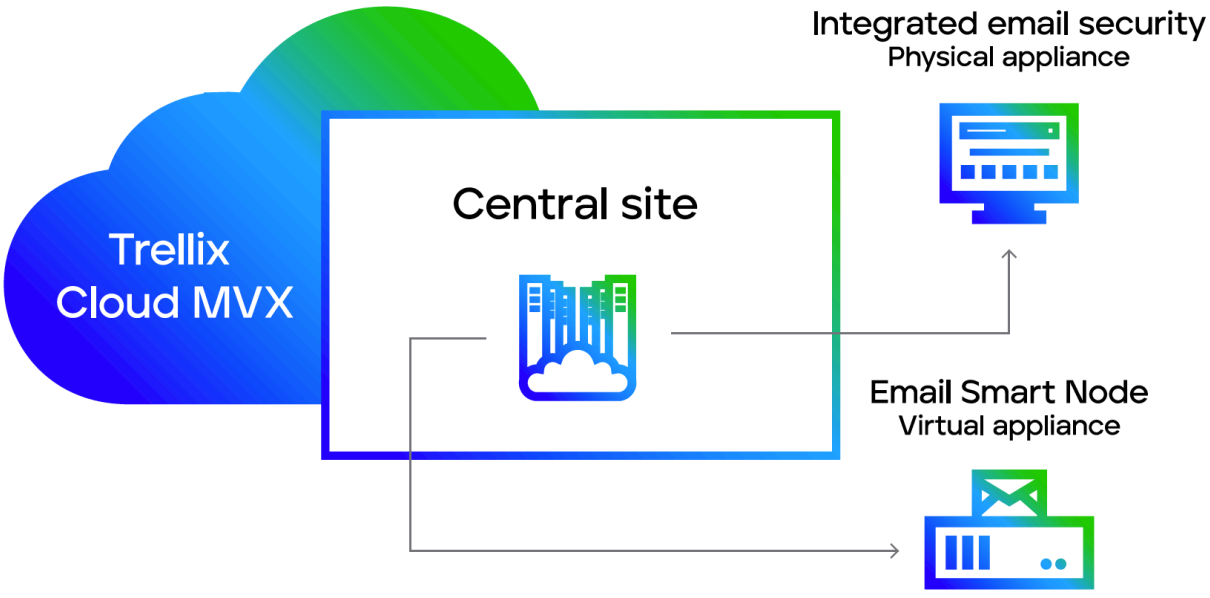

Table 1. Technical specifications

	EX 3500	EX 5500	EX 8500
Performance*	Up to 700 unique attachments per hour	Up to 1,800 unique attachments per hour	Up to 2,650 unique attachments per hour
Network interface ports	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+ (supporting 10GigE Fiber, 10GigE Copper, 1GigE Copper), 2x 1GigE BaseT
Management ports	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI monitoring	Included	Included	Included
VGA port (rear panel)	Included	Included	Included
USB ports (rear panel)	4x USB Type A Rear	2x USB Type A Front, 2x USB Type A Rear	2x USB Type A Front, 2x USB Type A Rear
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
Storage capacity	4x 2TB, RAID 10, HDD 3.5 inch, FRU	4x 2TB, RAID 10, HDD 3.5 inch, FRU	4x 2TB, 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 25.6" x 1.7" (437 x 650 x 43.2 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)
AC power supply	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 - 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC, 9 - 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC, 9 - 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU
DC power supply	Not Available	Not Available	Not Available
Thermal maximum power	245 watts (836 BTU per hour)	456 watts (1,556 BTU per hour)	530 watts (1,808 BTU per hour)
MTBF (h)	54,200 hours	57,401 hours	53,742 hours
Appliance alone/As shipped weight	30.0 lbs (13.6 kg) / 41.0 lbs (18.6 kg)	44.1 lbs (20.0 kg) / 65.3 lbs (29.6 kg)	44.4 lbs (20.2 Kg) / 65.6 lbs (29.8 kg)
Compliance safety	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
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 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
Security certifications	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
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 Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU
Operating temperature	0 ~ 35° C (32 ~ 95° F)	0 ~ 35° C (32 ~ 95° F)	0 ~ 35° C (32 ~ 95° F)
Operating relative humidity	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing
Operating altitude	3,000 m / 9,842 ft	3,000 m / 9,842 ft	

*All performance values vary depending on the system configuration and email traffic profile being processed. Size appliance(s) based on unique attachments per hour.

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
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)

Table 2. Trellix Virtual Execution smart grid specifications

Non-operating temperature	-30–70°C (-22–158°F)	-30–70°C (-22–158°F)	-40–70°C (-40–158°F)
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.

To learn more about Trellix, visit trellix.com.

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