



Trellix Central Management System

Centralize device and intelligence management to correlate data across attack vectors

Overview

Key Benefits

- Offers integrated controls for multiple platform deployments
- Enables blended threat prevention through multivector correlation
- Provides a purpose-built platform that can be deployed quickly without requiring rules, policies, or tuning
- Displays an at-a-glance security dashboard that provides advanced targeted attack protection status
- Speeds reports and audits through a consolidated security event storehouse
- Streamlines management of multiple Trellix solutions and reduces time spent managing configurations, threat updates, and software upgrades

Trellix Central Management System consolidates the administration, reporting, and data sharing of Trellix products in one easy-to-deploy, network-based solution. Central Management enables real-time sharing of auto-generated threat intelligence to identify and block advanced attacks targeting your organization. It also provides centralized configuration, management, and reporting for several Trellix solutions.

Real-time sharing of local threat intelligence

Trellix solutions generate real-time threat intelligence using the Trellix Multi-Vector Virtual Execution (MVX) engine. Central Management distributes that threat intelligence to multiple Trellix deployments, ensuring that each solution has the same dynamic protections against advanced attacks. Subscribers to the Trellix Dynamic Threat Intelligence (DTI) Cloud can use Central Management to centralize the sending and receiving of anonymized threat intelligence across Trellix solutions deployed at customers, technology partners, and service providers around the world.

At-a-glance security dashboard, plus drilldowns

Central Management consolidates activities and improves situational awareness with a unified security dashboard. The dashboard gives administrators a real-time view of the number of infected systems and lets them drill directly down to infection details to determine next steps.

Unified analysis of advanced targeted attacks

The analysis of blended threats, such as pinpointing a spear-phishing email used to distribute malicious URLs and correlating a perimeter alert to the endpoint, becomes possible. Security analysts can connect the dots of a blended attack to get the actionable intelligence they need to protect their organization against advanced targeted attacks.



Enterprise-class console and alerting

Central Management provides a web-based GUI console where administrators can view, search, and filter events and send real-time alert notifications via SMTP, SNMP, syslog, or HTTP POST. Administrators can filter by events, dates, or IP ranges and results are displayed to only show data based on the administrator's IT operational role. Notifications can also be sent to third-party SIEM tools. Administrators can click on an event link and connect seamlessly to specific Trellix solutions to view the network segment being protected.

Central configuration and platform upgrades

For efficient enterprise deployments, Central Management features dynamic configurations that can be determined centrally and then distributed across an organization accordingly. Administrators can remotely configure and view settings for one or more Trellix security solutions. Plus, all upgrades can be simultaneously deployed to all managed solutions, ensuring that they have the latest security capabilities.

Consolidated storehouse and detailed reporting

Larger and regulated organizations can use Central Management for efficient, consolidated reporting of security data. You can collect and store audit-relevant security events to meet long-term data retention requirements.

Trellix Central Management System offers convenient ways to search for and report on threats by name or type. Organizations can also view summaries such as the top infected hosts and malware and callback events, including geolocation details. Trending views can help show progress toward reducing the number of compromised systems.

DATASHEET

Table 1. Next generation appliances

	CM 9600	CM 7600
Network interface ports	(1) 10/100/1000BASE-T Port	(1) 10/100/1000BASE-T Port
HA link/HA backup link/ Management Interfaces	(3) 10/100/1000BASE-T Port	(3) 10/100/1000BASE-T Port
IPMI port (rear panel)	1 X IPMI 1GbaseT RJ45	1 X IPMI 1GbaseT RJ45
PS/2 keyboard and mouse, DB15 VGA ports (rear panel)	1X VGA port	1X VGA port
USB ports (rear panel)	2x USB3.2, 2xUSB2	2x USB3.2, 2xUSB2
Serial port (rear panel)	1 X serial DB9	1 X serial DB9
Storage capacity	(4) 10 TB HDD, RAID 10, 3.5 inch, FRU	(4) 4TB HDD, RAID 10, 3.5 inch, FRU
Enclosure	2 RU, fits 19-inch Rack	2 RU, fits 19-inch Rack
Chassis dimensions (WxDxH)	19"x26"x3.5"	19"x26"x3.5"
AC power supply	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
Power consumption maximum (watts)	427	500
Thermal dissipation maximum (BTU/h)	1457	1705
MTBF (h)	Coming soon	Coming soon
Appliance alone/As shipped weight lb. (kg)	40 lbs/ 66 lbs	41 lbs/ 67 lbs
Safety certifications	"CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368, EN 62368 BS EN 62368"	"CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368, EN 62368 BS EN 62368"
EMC/EMI certifications	"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"	"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 REACH"	"RoHS REACH"
Operating temperature	5°C - 35°C (41°F - 95°F))	5°C - 35°C (41°F - 95°F))
Operating relative humidity	8% - 90% (non-condensing)	8% - 90% (non-condensing)
Operating altitude	0 to 5000ft	0 to 5000ft

DATA SHEET

Table 2. Appliance specifications

	CM 4500	CM 7500	CM 9500
Network interface ports	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
Management ports (rear panel)	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI port (rear panel)	Included	Included	Included
Front panel LCD and keypad	Included	Included	Included
PS/2 keyboard and mouse, DB15 VGA ports (rear panel)	Included	Included	Included
USB ports (rear panel)	2x Type A USB ports	2x Type A USB ports	2x Type A USB 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
Storage capacity	4 x 4 TB HDD, RAID 10 usable; 8 TB	4 x 4 TB HDD, RAID 10 usable; 8 TB	4 x 4 TB HDD, RAID 10 usable; 8 TB
Enclosure	1 RU, Fits 19-inch rack	2 RU, fits 19-inch rack	2 RU, 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 W AC PSUs	Redundant (1+1) 800 W AC PSUs	Redundant (1+1) 800 W AC PSUs
Power consumption maximum (watts)	245 watts	456 watts	612 watts
Thermal dissipation maximum (BTU/h)	836 BTU/h	1556 BTU/h	2088 BTU/h
MTBF (h)	35,200 h	60,700 h	60,700 h
Appliance alone/As shipped weight lb. (kg)	30.0 lbs (13.6 kg)/41.0 (18.6 kg)	44.1 lbs (20.0 kg)/65.3 lbs (29.6 kg)	50.4 lbs (22.9 kg)/71.6 lbs (32.5 kg)
Safety certifications	IEC 60950, EN 60950, CSA 60950-00, CE Marking	IEC 60950, EN 60950, CSA 60950-00, CE Marking	IEC 60950, EN 60950, CSA 60950-00, CE Marking
EMC/EMI certifications	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A
Regulatory compliance	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE
Operating temperature	0 ~ 35° C	0 ~ 35° C	0 ~ 35° C
Operating relative humidity	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing
Operating altitude	5,000 ft.	5,000 ft.	5,000 ft.

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

DATA SHEET

Table 3. Virtual appliance specifications

Model	CPU cores	RAM	Virtual NICS	Hard disk space
CM2500V	4	32 GB	4 (total): 1 (management) 1-3 (for future use)	512 GB
CM4500V	8	64 GB	4 (total): 1 (management) 1-3 (for future use)	1,200 GB
CM7500V	16	128 GB	4 (total): 1 (management) 1-3 (for future use)	1,200 GB
CM9500V	32	256 GB	4 (total): 1 (management) 1-3 (for future use)	1,200 GB

Note: Each virtual appliance must meet the following specifications.

Table 4. AWS specifications

Model	vCPU	Memory	AWS instance type
CM1500V	2	8	m5.large
	4	16	m5.xlarge
	2	4	c5.large
	4	8	c5.xlarge
	8	16	c5.2xlarge
	2	16	r5.large
	4	32	r5.xlarge
CM2500V	8	32	m5.2xlarge
	16	32	c5.4xlarge
	8	64	r5.2xlarge
CM4500V	16	64	m5.4xlarge
	36	72	c5.9xlarge
	48	96	c5.12xlarge
	16	128	r5.4xlarge
CM7500V	32	128	m5.8xlarge
	48	192	m5.12xlarge
	72	144	c5.18xlarge
	96	192	c5.24xlarge
	32	256	r5.8xlarge
	48	384	r5.12ixlarge
CM9500V	64	256	m5.16xlarge
	96	384	m5.24xlarge
	64	512	r5.16xlarge
	96	768	r5.24xlarge

DATA SHEET

Table 5. Azure specifications

Model	vCPU	Memory	AWS instance type
CM1500V	1	3.5	Standard_D1_v2
	2	7	Standard_D2_v2
	4	14	Standard_D3_v2
	8	28	Standard_D4_v2
	1	3.5	Standard_D1s_v2
	2	7	Standard_D2s_v2
	4	14	Standard_D3s_v2
	8	28	Standard_D4s_v2
	2	8	Standard_D2s_v3
	4	16	Standard_D4s_v3
CM2500V	8	32	Standard_D8s_v3
	16	56	Standard_D5_v2
	16	56	Standard_D5s_v2
CM4500V	16	64	Standard_D16_v3
	16	64	Standard_D16s_v3
CM7500V	32	128	Standard_D32_v3
	48	192	Standard_D48_v3
	32	128	Standard_D32s_v3
	48	192	Standard_D48s_v3
CM9500V	64	256	Standard_D64_v3
	64	256	Standard_D64s_v3

For more information, visit trellix.com.

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



About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.

