PRODUCT SECURITY MATRIX

OFFICE OF MANAGEMENT AND BUDGET: KEY PRINCIPLES TO ENHANCING AND STRENGTHENING CYBER SECURITY VERTIV™ PRODUCT FEATURES	UMG	ACS	MPU	RCP1000	RCP2	DSView	*Trellis™*	SECURE SWITCH	SECURE KVM	KM
	DATA CENTER							DESKTOP		
Controlling, Containing, and Recovering from Incidents: Contain malware proliferation, privilege escalation, and lateral movement. Quickly identify and resolve events and incidents										
Private interface ports are protected from each other by Private VLAN configuration preventing lateral movement between different systems connected to the same appliance	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
KVM/vMedia as remote access technology enables network-less (out of band) forensics analysis and recovery of systems which increases efficiency and reduces downtime	✓	N/A	✓	N/A	N/A	✓*	✓**	N/A	N/A	N/A
Serial alert strings can be created to alert when certain conditions/activities take place that could indicate a problem or attack	✓	✓		N/A	N/A	✓*	N/A	N/A	N/A	N/A
Appliance can be remotely recovered in case of firmware failure, configurations can be backed up/restored	✓	✓	✓		✓	N/A	N/A	N/A	N/A	N/A
Dial-up/cellular connection failover prevents the management appliance from going offline during an outage/attack ensuring that operators maintain the ability to mitigate and recover via out-of-band access		✓	✓			✓*	N/A	N/A	N/A	N/A
Account privileges (Local/Remote) can be used to permit/deny user access in the event of an incident	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A
Appliance internally operates on a restricted/hardened OS	✓	✓	✓	✓	✓	N/A	N/A	✓	✓	✓
Network connection failover prevents the management appliance from going offline during an outage/attack ensuring that operators maintain the ability to mitigate and recover via out-of-band access	✓	✓	✓			✓*	N/A	N/A	N/A	N/A
Network isolation capability to physically separate user networks from more sensitive management/maintenance networks while maintaining the ability to grant legitimate operator access (proxy) to the management/maintenance network assets/devices	✓	N/A	N/A	N/A	N/A	✓	N/A	N/A	N/A	N/A
User Sessions and Remote Access sessions have inactivity time outs	✓	✓	✓		✓	✓	✓	N/A	N/A	N/A
FIPS 140-2 compliant ciphers & operating mode		✓	✓			✓		N/A	N/A	N/A
PCI compliant operating mode						✓		N/A	N/A	N/A
Customizable SNMP Community strings with Allowable Managers whitelist		✓	✓	✓	✓		✓*	N/A	N/A	N/A
Failed authentication lockout features prevent brute force password attacks		✓	✓			✓	✓	N/A	N/A	N/A
Local console authentication prevents unauthorized walk-up system access	✓	✓	✓	N/A	✓	N/A	N/A	N/A	N/A	N/A
LDAP/Active Directory Authentication support	✓	✓	✓		✓	✓	✓	N/A	N/A	N/A
TACACS+ Authentication Support		✓			✓	✓		N/A	N/A	N/A
RADIUS Authentication Support		✓			✓	✓		N/A	N/A	N/A
NIS Authentication Support		✓						N/A	N/A	N/A

✓* - When used with an appliance
✓** - When integrated with Avocent® DSView™

PRODUCT SECURITY MATRIX

VERTIV.

OFFICE OF MANAGEMENT AND BUDGET: KEY PRINCIPLES TO ENHANCING AND STRENGTHENING CYBER SECURITY VERTIV™ PRODUCT FEATURES	UMG	ACS	MPU	RCP1000	RCP2	DSView	*Trellis™*	SECURE SWITCH	SECURE KVM	KM
	DATA CENTER							DESKTOP		
Controlling, Containing, and Recovering from Incidents: Contain malware proliferation, privilege escalation, and lateral movement. Quickly identify and resolve events and incidents										
Kerberos Authentication Support		✓			✓			N/A	N/A	N/A
SSH Key Authentication Support		✓				✓		N/A	N/A	N/A
Serial Console output logging for forensic analysis	✓	✓			N/A	✓		N/A	N/A	N/A
Configurable appliance/system access rights		✓					✓	N/A	N/A	N/A
Configurable target device access rights	✓	✓	✓	✓	✓	✓		N/A	N/A	N/A
Redundant system capability enabling it to be Highly Available and able to withstand an outage of one or more primary/ backup systems without going completely offline						✓				
Multi-Factor Authentication Support (Currently only RSA SecurID)						✓		✓	✓	✓
Device Configuration Integrity Feature								N/A	N/A	N/A
Standardizing and Automating Processes: Decrease time needed to manage configurations and patch vulnerabilities										
Capable of pushing firmware updates into SPs in an automated fashion	✓		N/A	N/A	N/A			N/A	N/A	N/A
Automated System discovery	✓		N/A	N/A	N/A	✓	✓*	N/A	N/A	N/A
Centralized console/API that could be automated/scripted against to simplify automation	✓	✓			✓	✓	✓	N/A	N/A	N/A
NTP/Syslog format standards facility automatic event capture and categorization	✓	✓	✓		✓			N/A	N/A	N/A
Configuration backup/restore	✓	✓	✓		✓	✓	✓	N/A	N/A	N/A
Zero-Touch Provisioning feature automatically performs configuration template & firmware distribution to new Appliances connected to the network		✓						N/A	N/A	N/A
Automatic network fail-over	✓	✓	✓			✓*	N/A	N/A	N/A	N/A
Serial port speed detection	✓	✓		N/A	N/A	✓*	N/A	N/A	N/A	N/A
Serial port pinout detection	✓			N/A	N/A	✓*	N/A	N/A	N/A	N/A
Target hostname auto-detection/auto-naming	✓	✓				✓*	✓*	N/A	N/A	N/A
Automatic detection of connected KVM dongles	✓		✓	N/A	N/A	✓*	N/A	N/A	N/A	N/A
Preconfigured security profiles to auto-harden the configuration of the product		✓						✓	✓	✓
Single Sign-on authentication support		✓				✓	✓	N/A	N/A	N/A
User account auto-expiration support (specific date/predefined interval)	✓	✓				✓	✓	N/A	N/A	N/A
User account groups or roles to categorize and simplify the task of administering access rights	✓	✓	✓		✓	✓	✓	N/A	N/A	N/A
Dynamic routing protocol support	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Supports task automation and scheduling						✓	✓	N/A	N/A	N/A
Peer Integrity						N/A	N/A	N/A	N/A	N/A

✓* - When used with an appliance
✓** - When integrated with Avocent® DSView™

PRODUCT SECURITY MATRIX

VERTIV.

OFFICE OF MANAGEMENT AND BUDGET: KEY PRINCIPLES TO ENHANCING AND STRENGTHENING CYBER SECURITY VERTIV™ PRODUCT FEATURES	UMG	ACS	MPU	RCP1000	RCP2	DSView	*Trellis™*	SECURE SWITCH	SECURE KVM	KM
	DATA CENTER							DESKTOP		
Protecting Data: Better protect data at rest and in transit										
Storage encryption to prevent hackers from reading data off of the media if removed/discarded	✓	N/A	N/A	N/A	N/A			N/A	N/A	N/A
Running configuration data is protected behind user credentials and privileges	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A
Root access is not natively permitted to the OS reducing the risk of malicious modification of the applications or installation of malware	✓		✓	✓	✓	N/A	N/A	N/A	N/A	N/A
Media Retention warranty option for RMA destruction by customer	✓					N/A	N/A			
USB ports and vMedia can be disabled to prevent potential data exfiltration	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A
User permissions/rights allow/deny access of users to systems and their data	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A
Memory buffer data is erased when power is removed	✓	✓	✓	✓	✓	N/A	N/A	✓	✓	✓
KVM Session data encryptable with DES/3DES/128SSL/128AES	✓	N/A	✓	N/A	N/A	✓*	✓**	N/A	N/A	N/A
Browser sessions encrypted with SSL/TLS using 2048 bit certificates	✓	✓	✓			✓	✓	N/A	N/A	N/A
Private interface ports are protected from each other by Private VLAN configuration	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Proprietarily compressed and encrypted remote access capabilities to servers eliminates the need to expose the server/device to common attacks involving RDP/VNC	✓	N/A	✓	N/A	N/A	✓*	✓**	N/A	N/A	N/A
Encrypted remote access capabilities to servers eliminates the need to expose the server/device to common attacks involving Telnet	✓	✓	✓	N/A	N/A	✓	✓**	N/A	N/A	N/A
VPN support to mask all management traffic within an encrypted tunnel		✓				N/A	✓	N/A	N/A	N/A
Supports a configurable x.509 certificate policy and trust store						✓	✓	N/A	N/A	N/A
Improving Situational Awareness: Improve indication and warning										
The product will log all activities/changes performed by the user within the various product UI's							✓	N/A	N/A	N/A
The product provides onscreen indicators/pop-up alerts when critical activity occurs							✓	N/A	N/A	N/A
The product contains event/alert logs to inform the operator of activities that occur on/with connected/managed devices	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A
The product contains physical LEDs to indicate various port/device operating statuses	✓	✓	✓	✓	✓	N/A	N/A	✓	✓	✓
The product will scan SP event logs to identify hardware component failures that don't cause a complete system outage	✓	N/A	N/A	N/A	N/A	N/A	✓	N/A	N/A	N/A
The product can conveniently display server/SP information to indicate if a system is on/off, hot/cool, power hungry/not, in-use, has a full log, poor airflow, front panel open/closed, ID light active	✓	N/A	N/A	N/A	N/A	✓*	✓	N/A	N/A	N/A
Serial alert strings can be configured to notify of any situation/status reported by a connected device/server	✓	✓		N/A	N/A	✓*	N/A	N/A	N/A	N/A
Environmental sensors can notify an operator if a door is open/closed, if there is motion in an area and if there is a condensation/precipitation leak/pool in an area	✓			✓	✓	✓*	✓*	N/A	N/A	N/A
A siren/beacon can visually/audibly alert onsite operators of alert conditions or problems	✓					N/A	N/A	N/A	N/A	N/A
KVM dongle version information is conveniently displayed for the operator	✓	N/A	✓	N/A	N/A	✓*	N/A	N/A	N/A	N/A

✓* - When used with an appliance ✓** - When integrated with Avocent® DSView™

PRODUCT SECURITY MATRIX

OFFICE OF MANAGEMENT AND BUDGET: KEY PRINCIPLES TO ENHANCING AND STRENGTHENING CYBER SECURITY VERTIV™ PRODUCT FEATURES	UMG	ACS	MPU	RCP1000	RCP2	DSView	*Trellis™*	SECURE SWITCH	SECURE KVM	KM
	DATA CENTER							DESKTOP		
Improving Situational Awareness: Improve indication and warning										
SP firmware version information is conveniently displayed for the operator	✓	N/A	N/A	N/A	N/A	✓*	✓	N/A	N/A	N/A
Support for Rack PDU management provides operator awareness and control over hundreds of outlets in a single convenient location	✓	✓	✓	✓	✓	✓*	✓	N/A	N/A	N/A
KVM scan mode that cycles through systems to efficiently enable operators to spot problematic behavior		N/A	✓	N/A	N/A	✓*	N/A	N/A	N/A	N/A
Non-blocked KVM session capability allowing operators to perpetually observe systems to spot problematic behavior	✓	N/A		N/A	N/A	✓*	N/A	N/A	N/A	N/A
Administrator view of current sessions with disconnect ability	✓	✓	✓	N/A	N/A	✓	N/A	N/A	N/A	N/A
Web/SSH console login banner (security disclaimer) support		✓				✓		N/A	N/A	N/A
User notification when a session is being shared with others	✓	✓	✓	N/A	N/A	✓*	N/A	N/A	N/A	N/A
Support for U-Level asset location systems	✓						✓*	N/A	N/A	N/A
Support for report generation						✓	✓	N/A	N/A	N/A
Strengthening Systems Lifecycle Security: Increase inherent security of platforms by buying more secure systems and retiring legacy systems in a timely manner										
Current generation product that employs a current generation kernel, file system, encryption ciphers and open source packages	✓	✓	✓		✓	✓	✓	✓	✓	✓
Firmware/Software updates (including CVE vulnerability patches) occur 3+ times a year	✓	✓	✓		✓	✓	✓	N/A	N/A	N/A
Quality Assurance penetration tested regularly to identify and repair weaknesses/vulnerabilities	✓					✓	✓	N/A	N/A	N/A
Capability to update Appliance SSL certificate as needed/desired	✓	✓	✓		✓	✓	✓	N/A	N/A	N/A
DIACAP certified								N/A	N/A	N/A
FIPS 140-2 Compliant (Employs Certified Ciphers)		✓	✓			✓		N/A	N/A	N/A
Common Criteria/NIAP Certified								✓	✓	✓
Tempest Certification						N/A	N/A			
SNMPv3 Support	✓	✓		✓	✓	✓	✓*	N/A	N/A	N/A
TLS1.2 Support	✓	✓				✓		N/A	N/A	N/A
IPv6 Support	✓	✓	✓		✓	✓	✓	N/A	N/A	N/A
Removed support for Telnet an insecure command protocol		✓						N/A	N/A	N/A
Secure Mode capability to lock the product to a single management system	✓	✓	✓			✓*	N/A	N/A	N/A	N/A

✓* - When used with an appliance
✓** - When integrated with Avocent® DSView™

PRODUCT SECURITY MATRIX

OFFICE OF MANAGEMENT AND BUDGET: KEY PRINCIPLES TO ENHANCING AND STRENGTHENING CYBER SECURITY VERTIV™ PRODUCT FEATURES	UMG	ACS	MPU	RCP1000	RCP2	DSView	*Trellis™*	SECURE SWITCH	SECURE KVM	KM
	DATA CENTER							DESKTOP		
Reducing Attack Surfaces: Decrease complexity and number of things defenders need to protect										
Non-Networked product that is immune to remote attacks								✓	✓	✓
Aggregate product that does the same job of many different product types reducing IPs/interfaces.	✓		✓			✓*	✓	N/A	N/A	N/A
USB ports can be disabled	✓	✓		N/A		N/A	N/A	N/A	N/A	N/A
Ability to disable ICMP Ping Reply via firewall/setting configuration to minimize chance of network scanning detection	✓	✓	✓			N/A	✓	N/A	N/A	N/A
Ability to allow/reject/drop/log any source/destination IP/Port/Protocol via firewall configuration to restrict access to minimally desired criteria	✓	✓				N/A	✓	N/A	N/A	N/A
Ability to allow/dis-allow multi-session access to target consoles	✓	✓		N/A	N/A	✓*	N/A	N/A	N/A	N/A
Secure Analog Dial-in w/Call-back support		✓				✓*	N/A	N/A	N/A	N/A
Increase Awareness: improve overall risk awareness by all users										
Comprehensive event/alert logging and notification via local & email, snmp, syslog, DSView	✓	✓	✓	✓	✓	✓*	✓	N/A	N/A	N/A
Capable of notifying operators when compute systems experience hardware component failures that could lead to a system outage	✓	✓				✓*	✓	N/A	N/A	N/A
Capable of conveniently providing data about system firmware versions to assist in spotting older/at-risk versions	✓					✓*	✓	N/A	N/A	N/A
Convenient portal for providing operator access to a variety of systems for conducting audits/risk analysis	✓	✓	✓			✓	✓	N/A	N/A	N/A
Capable of discovering and identifying SPs (including rogue/ghost systems) on a network and even determining if default credentials are in use for those SPs	✓					✓*	✓*	N/A	N/A	N/A
Serial alert strings can be created to alert when certain conditions/activities take place on an attached console that could indicate a problem or attack	✓	✓				✓*	N/A	N/A	N/A	N/A
Configuration Integrity using MD5 Checksum		✓						N/A	N/A	N/A

✓* - When used with an appliance
✓** - When integrated with Avocent® DSView™

PRODUCT SECURITY MATRIX

OFFICE OF MANAGEMENT AND BUDGET: KEY PRINCIPLES TO ENHANCING AND STRENGTHENING CYBER SECURITY VERTIV™ PRODUCT FEATURES	UMG	ACS	MPU	RCP1000	RCP2	DSView	*Trellis™*	SECURE SWITCH	SECURE KVM	KM
	DATA CENTER							DESKTOP		
Increasing Cybersecurity Proficiency: Ensure a robust capacity to recruit and retain cybersecurity personnel										
Vertiv offers online/in-person training on how to use/maintain/secure our products	✓	✓	✓			✓	✓			
Centralized remote access increases operator efficiency, reduces repetitive tasks, affords operators more time to focus on cybersecurity related activities	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A
Remote Access to systems enables Cybersecurity personnel to perform Out-of-Band audits from anywhere in the world which reduces travel expenses and incentivizes the best professionals to work for your company	✓	✓	✓	✓	✓	✓	✓**	N/A	N/A	N/A
UI localization enables operators to use/understand the system in their native language (up to/including: English, Chinese, Japanese, Russian, French, Spanish, German, Portuguese)	✓	✓	✓			✓	✓	N/A	N/A	N/A

For More Information, Please Contact:

Chris Ruffing

Dell EMC Alliance Manager

512-934-8270

Chris.Ruffing@VertivCo.com

Steven Grasley

Dell EMC Alliance Manager

512-534-1693

Steven.Grasley@VertivCo.com

Team email

goDell@VertivCo.com

Visit our customer-facing site for documents, SKUs, FAQs and other information: www.DellKVM.com

GSC-DELL-001/ (R05/17)