Request for Quotations

	Tender	Description	Qty	Sample/Specs
1	325-21	For the supply and delivery of Enterprise End Point Protection	1600	Attached AMENDED Specs below the table
2	328-21	For the provision of Server Patch Management and advanced server Security	135 servers	Attached AMENDED Specs below the table
3	355-21	For the supply and delivery of cellphones 1. iPhone 11 128GB 2. Samsung Galaxy A71 3. Samsung Galaxy A72 4. Samsung Galaxy Note 9 5. Samsung Galaxy S9 plus MUST BE AVAILABLE IN STOCK	 1 1 1 1 1	

Please note that **only** bidders registered with **Procurement Regulatory Authority of Zimbabwe (PRAZ) shall** be considered.

(Please attach Proof of PRAZ registration in the specified category)

Closing date for ALL Tenders: On or before 1100hrs; Wednesday 14 April 2021

Your Tender should state the price(Please state your VAT status), a firm delivery date and be placed in the tender box on the 8th Floor, South Wing, Runhare House , 107 Kwame Nkrumah Avenue, Harare; OR Emailed to procurement@telone.co.zw

Tel; 264 4 798111; 2902168; Fax 264 4 795499 Runhare House, 107 Kwame Nkrumah Avenue, Harare,

Voice | Broadband | Satellite

TelOne

AMENDED SPECIFICATIONS FOR RFQ 325-21

Endpoint Protection Specifications

Required is a light 1600-user endpoint security solution. The Endpoint Protection MUST provide centralized and uninterrupted protection for all of our Windows, Mac and Linux workstations, including laptops and servers, in addition to the leading virtualization systems and Android devices.

The Endpoint Protection, must have the protection managed conveniently and easily from a single Web console, permitting centralized administration. The system must provide:

Multi-layered defense:

- Detect malware pre-execution, during execution and post-execution.
- Zero-day threats - heuristics and machine learning as part of multi-layered approach to prevent and protect against never before-seen malware
- Respond quickly to malware upon its first incidence anywhere across the globe
- Cloud malware protection - system automatically protects against new threats without the need to wait for the next detection update

Endpoint Protection:

- Endpoint protection to prevent cyber-attacks, detect malicious activity, and provide instant remediation capabilities;
- Antivirus and Antispyware - provide proactive protection against online and offline threats and prevent malware spreading to other users
- Anti-Phishing - prevent attempts to acquire sensitive information such as usernames, passwords or banking and credit card details by fake websites
- Ransomware protection - block malware that tries to lock you out of your own data
- Advanced Machine Learning - detect never seen before malware
- Script-Based Attack Protection - detect malicious Windows PowerShell scripts and JavaScripts attacks via web browser
- UEFI Scanner - protects from threats that attack computer on a deeper level, even before the start of Windows
- Exploit Blocker - blocks attacks specifically designed to evade antivirus detection

	Features	Description	Compliance
1	Boot-Time Scan		
2	Firewall		
3	IDS/HIPS		
4	Zero-day threats	heuristics and machine learning as part of multi-layered approach to prevent and protect against never before-seen malware	
5	Centralized console		
6	Antimalware		
7	Antispyware		
8	Antiphishing		
9	Supported	Cross-platform for Linux, Windows, MacOS,	

	Features	**Description**	**Compliance**
	Platforms	Android, virtual environment	
10	Ransomware Protection	Analyzes behaviors and hacking techniques to detect and block both known and unknown malware, as well as ransomware, trojans and phishing	
11	Web filtering		
12	Virus and content filtering		
13	Centralized device control		
14	Advanced disinfection and remediation tools		
15	Email protection		
16	Light weight agent	lightweight on the PC systems resources that leaves more power to programs used daily and extend the life of computer hardware	
17	Automatic discovery Unprotected endpoint & remote installation		
18	Web protection		
19	URL filtering		
20	Centralized quarantine		
21	Non-disruptive and direct remote access		
22	Antispam protection for Exchange servers		

AMENDED SPECIFICATIONS FOR RFQ 328-21

Server Patch Management and Advanced Security Solution Specifications

Required is a solution that provides all necessary tools to manage, from a single console: 135 servers (bare metal +virtual) (Linux and Windows) server security, updates and patches both for operating systems and third-party applications. The solution must strengthen threat prevention, containment and remediation capabilities, reducing the attack surface on servers

Dashboard Features

a) Single panel view with real-time information of all vulnerable computers, pending patches and unsupported (EOL) software, with their remediation status.

b) Detailed information about patches and pending updates, details of the relevant security bulletin, as well as computer and computer group information, and more. Available actions:

c) Filter and search for patches based on criticality, computer, group, application, patch, common vulnerability and exposure (CVE) ID and status.

d) Ability to take actions directly on computers: restart, install now or schedule.

e) Unattended scanning for pending updates, in real time or at periodic intervals (3, 6, 12 or 24 hours).

f) In exploit detections, notification of pending patches.

g) Ability to launch installations immediately or scheduled from the console, isolating the computer if required.

Technical Specifications

Item	Feature Descriptions	Compliance
1	Patch Management – Windows and 3rd party apps	
2	Patches service Packs, updates and EOL apps	
3	Narrow detection, isolation and patching integration	
4	Patching roll back. Rollback to uninstall a patch that may cause an unexpected conflict with an existing configuration.	
5	Centralised console	
6	Antimalware, antispyware and anti-phishing	
7	Protection against zero-day exploits	
8	Protection against unknown malware an targeted attacks	
9	100% process attestation	
10	Antitamper	
11	Email protection	
12	Exchange antispam protection	
13	Exchange content-based email filtering	
14	Firewall	
15	IDS/HIPS	
16	Device control	
17	Web protection	
18	URL filtering by category	
19	Web browsing monitoring	

20	Advanced remediation and monitoring tools	
21	Centralized quarantine	
22	Software and device inventory and audits	
23	Non-disruptive and direct remote access	
24	Device isolation	
25	Realtime Policy enforcement and updates	
26	Unmanaged device discovery	
27	Realtime reporting and alerting	
28	Execution graphs for forensic analysis	
29	Managed threat hunting service	
30	Windows, Linux, Mac OS X, Android, Exchange and virtual systems compatible	