भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Registered Office - 1001A, B Wing, 10th Floor, 'The Capital', Bandra Kurla Complex, Bandra (E),
Mumbai - 400 051

Corrigendum-2

This is with reference to NPCI's RFP No RFP no. NPCI/RFP/2021-22/IT/18 dated 04.03.2022. RFP for procurement of Network APT solution. The prospective bidders may please note the following changes:

Sr. No.	Document Reference	Description	Existing RFP Clause	Amended clause vide this note
1	Section 8 - Terms & Conditions, Clause No 8.10 Page No 25	Delivery schedule	Delivery, Installation & commissioning of the solution should be completed within 12 weeks from the date of receipt of purchase order. • Delivery of hardware, software, and license should be within 6 weeks. • Installation & commissioning should be completed in next 6 weeks.	Delivery of hardware, software, and license should be within 6-8 weeks. Installation & commissioning should be completed in next 6 weeks.
2	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Ability to automatically intercept all SSL/TLS based flows, also on other ports and protocols (not only HTTPS)	Clause stands deleted.
3	Section 9 - Technical Specifications	Section 9 - Technical Specifications	Ability to configure encryption/decryption policy (incl. block/passthrough) based on CA status	Clause stands deleted.
4	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on Cipher Suite and Key Strength	Clause stands deleted.
5	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on host/URL categorization	Clause stands deleted.
6	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on source/destination ip/port	Clause stands deleted.

7	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on Subject / Domain Name	Clause stands deleted.
8	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on threat intelligence	Clause stands deleted.
9	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Automatic detection and response against an ever-growing variety of threats, including fileless and ransomware	Automatic detection and prevent against an ever-growing variety of threats, including file and fileless attacks.
10	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Hardware should have minimum capacity of 1 TB	Hardware should have minimum capacity of 4 TB.
11	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Must have the ability to correlate the monitored attacks to the APT filters number and recommended action	Clause stands deleted.
12	Section 9 - Technical Specifications	Annexure J - Technical Compliance	NG APT engine must be a smart enough to inspect the traffic based on condition, If the traffic is suspicious then it goes for the deep packet inspection	Solution should be able to detect and prevent threats based on intelligence/signatures, and should have dynamic analysis engine with signature less detection capability & create signature in real time to block the threats inline.
13	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Sandbox appliance should have redundant power supply, 2 TB or more storage capacity with dedicated management port	Hardware should have minimum capacity of 4 TB.
14	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Sandbox must have the ability to simulate the entire threat behavior.	Clause stands deleted.
15	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Security Vendor must have a Research/Labs organization and this organization must contribute and report on finding new Zero-Day vulnerabilities being exploited in the wild.	Security Vendor must have a Research/Labs organization and provide intelligence to the solution about the zero day exploits detected in the wild and proposed solution should be able to detect and prevent the zero day exploits.
16	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Solution should inspect https traffic (Full Deep Packet / SSL Traffic) and must provide decryption of unverified encrypted traffic for scanning	"The proposed solution should detect & prevent suspicious Webshell files uploaded to web servers through HTTP POST and FTP protocols and also provide mapping of methodology & alert

			and then re encrypt it before sending	techniques to MITRE ATT&CK framework. It should also detect attempted data exfiltration & SSL/TLS handshake fingerprinting at the minimum"
17	Section 9 - Technical Specifications	Annexure J - Technical Compliance	SSL Capabilities	Built in SSL capabilities.
18	Section 9 - Technical Specifications	Annexure J - Technical Compliance	SSL functionality should be available on the proposed inline APT appliance	Built in SSL capabilities.
19	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?	Clause stands deleted.
20	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?	Clause stands deleted.
21	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Support for Fail-to-wire/fail-to-open hardware, traffic bypass filters (in the event of in-line security device failure) and configurable link state monitoring/mirroring?	Good to have
22	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Support for Fail-to-wire/fail-to-open hardware, traffic bypass filters (in the event of in-line security device failure) and configurable link state monitoring/mirroring?	Good to have
23	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Support MDS, SHA-1, and SHA-256 hash algorithms?	Support SHA-1, and SHA-256, SHA-3 hash algorithms.
24	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Support multiple active-inline devices simultaneously	Clause stands deleted.
25	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Support RSA, DHE, and ECDHE public key algorithms?	Clause stands deleted.
26	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3, SSL3, and SSL2 encryption protocols?	Solution should Support TLS 1.2 , TLS 1.3 encryption protocols
27	Section 3 – Scope of Work	Section 3.1: Scope of Work	Technical Training should be arranged by OEM directly.	Technical Training should be arranged by OEM/ OEM Authorized Partners

28	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed management system support 3rd party VA scanners(Qualys, Foundstone, Nexus) to fine tune the APT policy	Clause stands deleted.
29	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed APT should support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods	Clause stands deleted.
30	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed APT solution must support Layer 2 Fallback option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption , memory errors	Clause stands deleted.
31	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The APT filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace(Packet Capture), Rate Limit and Quarantine	Clause stands deleted.
32	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The APT filters must be categories into the following categories for easy management: Exploits, Identity Theft/Phishing, Reconnaissance, Security Policy, Spyware, virus, Vulnerabilities, Traffic Normalization,P2P, IM, Streaming Media	Clause stands deleted.
33	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The industry's most timely virtual patching: Vulnerability Protection virtually patches known and unknown vulnerabilities, giving you instant protection, before a patch is available or deployable.	Clause stands deleted.
34	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The management server must provide rich reporting capabilities include report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic	The management server must provide rich reporting capabilities include report for all attacks, Specific & Top N attack, Source, Destination, Device Traffic Statistics and Advanced threats detected.

			Statistics and Advance DDoS report	
35	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed APT must able to operate in Asymmetric traffic environment with Vulnerability / Exploit filters for protection	Clause stands deleted.
36	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed APT must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score	Clause stands deleted.
37	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed APT must be able to use Reputation Service such as IP address or DNS to block traffic from or to 'known bad host' such as spyware, phishing or Botnet C&C	Clause stands deleted.
38	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed APT must provide bandwidth rate limit to control the unwanted/nuisance traffic such as P2P, Online Game, etc.,	Clause stands deleted.
39	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed APT should support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods	Clause stands deleted.
40	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed APT solution must support Adaptive Filter Configuration(AFC) which will alert or disable ineffective filter in case of noisy filters	Clause stands deleted.
41	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed APT solution must support signatures, vulnerabilities and traffic filtering methods to detect attacks and malicious traffic	Clause stands deleted.
42	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed management system must be able to support the syslog CEF format that SIEM can support	The proposed management system must be able to support Common Event Format (CEF), Log Event Enhanced Format (LEEF), Comma-Separated Values (CSV), XML, JSON, or Text format that SIEM and other tools like automation and orchestration can support.
43	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed management system shall have a big data engine that allows customers to	The Management system should support file formats which can be ingested in Big Data Analytics

			provide faster security analytics and faster report generation	Solution for faster report generation.
44	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The Proposed Sandboxing solution must support of analysis of Windows & Linux Operating System files	Clause stands deleted.
45	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution must be available as on premise physical appliances with sandboxing capability	"The proposed solution must be available as on premise physical appliances with sandboxing capability and must be able to detect and report malware by using multiple client environments (operating systems with multiple service pack levels) supporting both x64 and x86 architectures including Windows, Mac, CentOS based on premise Virtual Execution Environment, no object/file should send to the cloud for analysis "The proposed solution must be available as on premise physical appliances with sandboxing capability and must be able to detect and report malware by using multiple client environments (operating systems with multiple service pack levels) supporting both x64 and x86 architectures including Windows, Mac, Unix, CentOs, RHEL, Ubuntu based on premise Virtual Execution Environment without any additional requirement of licenses form OS's and Applications from NPCI."
46	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution must be capable of analysis of different file types, including portable executables (PEs), web content, Web objects, images, Java, network flows, Microsoft and Adobe applications, PHP, WAR, JSP, ASP, and ASPX, archive files and multimedia etc. including all such file types which have shown presence in historic advance attackers profile, as a delivery channel, for initial compromise or backdoor or malicious dropper delivery.	"Solution should provide comprehensive support for user interaction framework for web shells, support for shell scripts (e.g.; python, Perl, and Ruby etc.), support for ELF binaries, Server-side attack detection, complete user mode and kernel mode monitoring from within and outside the Guest Images, Web shell detection support for JSP, PHP, and WAR (Web archive) file types etc."

47	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The Proposed solution should allow Admin be able to inquire how many detections come from malicious password-protected files	"Solution should provide comprehensive support for user interaction framework for web shells, support for shell scripts (e.g.; python, Perl, and Ruby etc.), support for ELF binaries, Server-side attack detection, complete user mode and kernel mode monitoring from within and outside the Guest Images, Web shell detection support for JSP, PHP, and WAR (Web archive) file types etc."
48	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects.	"The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm to prevent advanced Malware and Zero-day attacks."
49	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution should be able to detect any suspicious communication within and outside of Customer's network	"The proposed network Anti-APT solution should also be able to detect malicious post-exploitation activities such as attacker lateral movements between user workstation & Servers. Indicating source & destination IP addresses, files transferred over SMB, commands executed, with detailed execution and report of payload."
50	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The Proposed solution should be able to detect communications to known command and control centers.	"The Proposed solution should be able to detect communications to known & unknown command and control center initiated by internal infected clients."
51	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The Proposed Solution should be able to detect known bad URL before sandboxing	The Proposed Solution should be able to detect known and un-known URLs for any malicious communication.

52	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution should be able to detect reputation of URL being accessed	Clause stands deleted.
53	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and Exfiltration	Proposed Internal Network APT should detects the following types of malicious post-infection activities: a) Internal Reconnaissance b) Privilege Escalation c) Credentials Dumping d) Lateral Movement of Malware e) Remote Task Execution f) Data Exfiltration Detection g) Callback activities h) Bot-tracker features like File inspection, Packet flows, Signature matching and statistics i) Supports extensive metadata protocols including the following protocols: FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS.
54	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution should be able to run at least 50 parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis	The proposed solution should be able to run at least 50 parallel sandboxes/vms for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis
55	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution should be dedicated appliance and should not be enabled as additional licensed solution with proposed perimeter gateway devices such as firewall, APT etc.	Clause stands deleted.
56	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution should detect file-less malware tools used for extracting plain text passwords, hash, PIN codes and Kerberos tickets.	"The proposed solution should detect file-less malwares tools used for extracting encoded/XOR'ed as well as plain text passwords, hash, PIN codes."
57	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis	Clause stands deleted.
58	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution should have an built-in document vulnerabilities detection engine	Clause stands deleted.

			to assure analysis precision and analysis efficiency	
59	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution should support at least 100+ protocols for inspection	"The proposed solution for Network Ani-APT should prevent any C&C communications detected over North-South, East-west traffic regardless of ports and protocols"
60	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution should support Multiple protocols for inspection. Example HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction: SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device	The proposed solution should support Multiple protocols for inspection as following but not limited to HTTP, HTTPS, SFTP, SMB, FTP and P2P protocols on a single device. Identify object types transffered/extracted as mentioned in example but not limited to (Example- .exe, .dll, .com, .ps1, and bat) from traffic and submitted for analysis."
61	Section 9 - Technical Specifications	Annexure J - Technical Compliance	The proposed solution should support to monitor traffic from multiple segments simultaneously on single appliance (East-West, North-South).	NPCI ask is to have built in capabilities to monitor north-south, as well as east-west traffic in this same solution.
62	Section 8 - Terms & Conditions, Clause No 8.14, Page No 26	Support	The successful bidder shall provide comprehensive on-site maintenance (AMC) of the solution for a period of 3 years with back to back support with the OEM, including warranty period of 1 year and 2 years support post expiry of the warranty period of 1 year.	The successful bidder shall provide comprehensive on-site/Remote maintenance (AMC) of the solution for a period of 3 years with back to back support with the OEM, including warranty period of 1 year and 2 years support post expiry of the warranty period of 1 year.
63	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Total Packet processing capacity of single device should be 1 Gbps	Clause stands deleted.
64	Section 9 - Technical Specifications	Annexure J - Technical Compliance	Vulnerability based filter are known for most effectively for Zero Day Attack Protection and proposed solution must support vulnerability based filter	Clause stands deleted.