Email Security – Email DLP			
Technical Specifications & Core Features			
Sr. No.	**Requirement**	**Compliance (Y/N)**	**Remarks**
1	Solution integrates via API with Office 365 and/or Google Workspace with no change on current architecture and MX of email service		
2	Solution relies on a cloud-based delivery model		
3	The solution must provide three modes of protection for email via API integration - Detect, Detect and Remediate, and Prevent (Inline).		
4	Solution should not disable any native security of customer Email Cloud Service Provider and will act as additional layer of security		
5	Email Security should be inline and should be invisible for any attack reconnaissance		
6	Email Security should prevent mail borne threats and should be block/prevent before it reaches user inbox		
7	Solution should have a real time threat intelligence on the cloud with real time threat prevention		
8	Email Security can integrate with email provider with reports of phishing and malware		
9	Email Security should have DLP to scan emails and prevent sensitive information		
10	Email Security should have CDR (Content Disarm & Reconstruction) to prevent Zero Day Attacks and implement Zero-Trust		
11	Email Security should have Threat Emulation (Next-Gen CPU Based Sandboxing) to complement sandboxing of files to prevent Zero Day attacks and avoid impairment of productivity of users		
12	Email Security should have utilized machine-learning that builds a profile based upon historical event information like login locations, data-transfer behaviour, top email collaborators, user profile		
13	Email Security should have the ability to rescan and reclassify emails as an automated post delivery mechanism for threats discovered after deliver either from internal metadata or from other CP customers via Threat Cloud.		
14	Solution should have a post-delivery protection, Mail Search, and Destroy or M-SOAR capabilities		
15	Email Security should support the identification of applications (Shadow IT) used by users via E-mail notifications, reminders or any application generated application		
16	Email Security should be able detect and stop impersonation and Business Email Compromise (BEC) attacks either by blocking access to the account or initiating a recent password action		
17	Solution to classify emails so that users can know what is suspicious before opening it		
18	Solution detects spoofed messages based on email headers and the sender names (Display Name Spoof Detection)		
19	Solution provides the capability to monitor all the relationships of senders' recipients (i.e. first sender to send mail to some user) and seek near-match deviations		
20	Solution flags lookalike domains (i.e. cousin domains, Fake domains)		
21	Solution detects sophisticated attack messages based on sender, recipient, envelope, content, history and any other context		
22	Spam and phishing (even with a low number of messages) is detected using non-rule-based techniques (i.e. telemetry and intelligence)		
23	Solution performs anomaly detection by analysing the metadata (reputation of the sender's address, sending domain, IP, attempts to deceive the sender's identity and authentication)		

24	Solution should also perform anomaly detection by detection leverage on historic communication, i.e. typical communication between sender, recipient and their domains		

25	For suspicious looking emails that cannot be categorize as Phishing attacks, the solution should be able to a means to educate recipients about the possible malicious nature of the email through Smart Banners		
26	Solution detects calendar invite attacks (CIAs) - calendar invite attacks are disguised as ICS files (CVE-2023-23397)		
27	Solution is able to connect to other Office 365 SaaS applications to scan for malicious files being stored		
	URL Based Threats		
28	For the time-of-delivery protection, solution is able to rewrite URLs before being delivered to the users (e.g. non-clickable URL, text replacement, etc.		
29	For the time-of-click protection, solution redirects the URL to a URL Emulation Service at the time of click by user		
30	Solution is able to examine URLs in subject lines, apart from e-mail body		
31	Solution counts with a RBI (Remote Browser Isolation) service to inspect embedded URLs		
32	The RBI counts with anti-evasion capabilities, to prevent malware to identify it is being run in a virtualized sandbox environment		
33	Solution should be able to scan and detect malicious URLs hidden in QR Codes		
34	Solution should be able to rewrite URLs hidden in QR codes and redirect users to a Real time URL Emulation service upon the time of click		
	Attachment based Threats		
35	Email solution should have protection against known and unknown malware threats		
36	Solution counts with a network sandbox to inspect attachments		
37	Solution counts with a network sandbox to inspect files (e.g. PDF and Microsoft Office) accessible through an URL included in the email body		
38	The network sandbox covers file types commonly used in attacks (e.g. , zip, wsf, js, macros, python, exe, sh, bat, ps1)		
39	Solution counts with anti-evasion capabilities, to prevent malicious email attachment to identify it is being run in a virtualized sandbox environment		
40	Solution provides CDR (Content Disarm and Reconstruction) capabilities to remove malware and exploits from attachments		
41	CDR capabilities (file breaking down and rebuilding without anything that does not conform to the file type specification) are delivered in near-real-time.		
42	Solution is able to scan and block e-mails with malicious URLs embedded within attachments		
43	Solution should be able to rewrite URLs in attachments that redirect users to a Real time URL Emulation service upon the time of click		
44	Solution utilises a service to provide scanning of password-protected (at least when password is included within the email body) and multiple-compressed files		
	Deployment		
45	Solution should be able to offer automated inline-API based enabled email security that can be integrated with existing E-mail Cloud Provider without down time		
46	The email security should rely on a cloud-based delivery mode and it should run in a monitor-only mode for any trials, as well as inline to test end-user workflows.		

47	Solution will not only protect e-mail but also Collaboration or shared storage applications used by customer		
48	Solution should secure Incoming, outgoing and Internal e-mail of customers to avoid later movements of threats		
49	Email Security should support Deployment without the need to change DNS MX records		
50	Email Security should support large scale organizations		
51	Capability to apply email protection solution gradually to specific users or Groups		
	Detection & Response Capabilities		
52	Solution provides detection and response capabilities once the email lands in a user's inbox, post-delivery protection		
53	Solution is able to remove (automatically and manually) a malicious message from users' inbox (opened already or not by the final user, in the inbox or any other folder, etc.)		
54	Solution is also able to undo a remediation action in case a mail was mistakenly identified as malicious message (false positive)		
55	Solution provides mechanisms based on DLP and AI models to detect and alert users of potential sensitive data in outbound email		
56	Solution analyses the recipients that are addressed in the To, Cc and Bcc fields and scan whether the content is relevant for the recipient by monitoring the sending and receiving patterns		
57	Solution detects whether the sender domain supports inspection of DMARC, SPF and DKIM		
58	Solution includes the ability to analyse user submitted messages to validate their malicious nature		
59	Solution is able to connect to Office 365 to provide insight into potentially compromised accounts		
	Accessibility and Management		
60	Email Security should be managed and monitored in single dashboard for both built-in Cloud Email security and the Vendor Email Security		
61	E-mail Security should be able to offer a consolidated dashboard of its Security events and the Native Cloud E-mail Solution Security		
62	E-mail Security solution events should be able to show a consolidated view of its own event analysis and the Native Cloud security solution's analysis		
63	Email Security should have audit trails for anybody performing the monitoring and investigation of attacks		
64	Email Security Should have a single Quarantine Email management section to review and restore both emails quarantined by E-mail Security Solution and the native Cloud E-mail security		
65	Solution should come with an End User Quarantine portal to let users Securely view and manage quarantined mails and provide with an E-mail body preview capability		
66	Email Security Should integrate with Cloud E-mail Native Report Phishing function without the need to install a separate outlook client add-on.		
67	Email Security Should have a separate section to view User Reported Phishing emails via Admin console		
68	Email Solution offers the capability to make exceptions per mailbox, sender, IP, etc. to allow emails without the need to go through the classification engine		
69	Email Security Should have the capability to identify and log users that clicked URL re-written links or users who proceeded to visit a website after a security reminder prompt/warning		
70	Email Security Should have the capability to send and control frequency of E-mail Security Daily Digest		

71	Email Security Should have the capability to consolidate individual User E-mail digest with the Cloud Native E-mail digest eliminating the need to configure two separate e-mail digests		
72	Email Security should be able to easily enable Allow or Block Lists of email senders by domain, IP and numerous other criteria.		
73	All users have individual User Admins accounts and only access information when required to do so to perform job functions, based on a need-to-know basis		
74	All access is controlled using Role based access Control models		
75	Risk is mitigated by the fact that all data/systems are stored on the cloud provider		
	Compliance		
76	OEM/bidder MAF is required		
	DLP		
77	Email Security should have DLP to scan emails and prevent sensitive information		
78	Email Security should have CDR (Content Disarm & Reconstruction) to prevent Zero Day Attacks and implement Zero-Trust		
79	Solution should detect sensitive data sharing via email and immediately limits data exposure		
80	Solution should be able to enforce a data leakage policy based on Bank's needs, with hundreds of predefined and custom data types.		
81	Blocking of PII data such as Credit card details, Personal information		
82	Scanning of PNG & JPG files to check for DLP violations.		
83	Policy based on Hit Count (e.g.: Keyword matches 5 times or more in a mail)		