Request for Information (RFI)

RFI-2024-005

Email Security Solution

8/6/2024

Submit Responses To: Stephanie Waits
Phone: 918.960-2221
E-mail: stephanie.waits@grda.com

NOTE: If Respondent has any questions pertaining to the enclosed RFI, direct them to the Buyer as listed above. Only answers provided by the GRDA Central Purchasing Unit will be considered official and valid by GRDA.

NOTICES/INSTRUCTIONS

1.1 INTRODUCTION

This request is for information only to assist the Grand River Dam Authority in determining the best software solution for the Authority to implement to reduce the number of spam and malicious emails that continue to be received, even with current filtering software in place.

1.2 PURPOSE

This Request for Information (RFI) is to solicit technical and performance narratives along with suggested pricing information from vendors and identify additional supply or product resources for email spam/malicious filtering software. Ideally, the software will deliver a robust platform that includes, but not limited to, the features listed in the Requirements section.

1.3 VENDOR REQUIREMENTS

The vendor must:

- Work the Value Added Reseller Fulcrum Technologies Solutions (https://www.ftsc.com/).
  - Primary points-of-contacts:
    - Josh Tatum jtatum@ftsc.com and John Barnard jbarnard@ftsc.com
- Have 24x7 global support for the product and provide substantiating documentation.
- Ensure enterprise support and provide substantiating documentation.
- Ensure product license scalability and provide substantiating documentation.
- Implement and maintain appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of the data. This includes protecting against unauthorized access, disclosure, alteration, and destruction of data in accordance with a compliance framework.

Additionally:

- All data processed, stored, or transmitted by the email security tool shall remain the exclusive property of GRDA.
- The vendor &/or solution shall not use, disclose, or share this data for any purpose other than providing the agreed-upon services under this contract.

1.4 TECHNICAL REQUIREMENTS

The Solution shall:

- Have the ability to provide role-based access control (RBAC) via a centralized management console.
- Be able to integrate with various modern authentication methods with IDP via protocols such as SAML or OIDC. Azure Conditional Access
- Have the ability to forward log data, such as audit data, from the centralized management console
- Have a built-in reporting function; whereas, pre-built or custom reports can be rendered adhoc or scheduled via GUI and/or API.

- Have the capability to store audit information for all policy and configuration changes.
- Support Microsoft 365
- Have Business Email Compromise (BEC) Detection capabilities
- Have Social Engineering Attack Detection capabilities
- Have Advanced Malware Detection capabilities
- Have URL and Link Protection capabilities
- Have Data Loss Prevention (DLP) capabilities
- Have encryption on demand capabilities
- Have Attachment Analysis (File sandboxing) capabilities
- Have the ability to report on DMARC
- Have the ability to integrate with 3rd threat intel feeds. ISAC feeds (STIX/TAXII)
- Have the ability to remediate post delivery malicious emails. Both automated and a workflow for reviewing.
- Have end-user education and awareness functionality
- Have account takeover protection and remediation capabilities
- Have regulatory compliance reporting functionality
- Have capabilities to protect against malicious QR codes
- Have capabilities for end-user reporting of malicious mail
- Have the ability to black/white listing of both domains and individual emails from an administrator perspective
- Have real-time statistics
- Provide specific details and indicators around identified malicious mail
- Provide specific reports around detailed mail volumes for domains and individuals
- Provide the ability to apply customized banners based on certain criteria
- Provide a DKIM capability for outbound mail
- Have API capability to integrate with a SOAR solution
- Be able to leverage and/or report on AIP tags for DLP
- Be able to create and enforce custom security policies
- Have the ability to protect against mail blast
- Have comprehensive reports on security incidents and trends
- Have high availability and redundancy to ensure uptime
- Have transparency and explainability of AI decisions
- Have multiple geolocations for point of presence
- Have recursive unpacking/blocking capabilities for nested attachments
- Have the ability to detect malware in password protected files
- Have the ability to use wildcards in the middle of email addresses or domains getting whitelisted/blacklisted
- Have the ability to archive and/or backup emails

- Have the ability to detect behavioral anomalies and patterns that may be malicious
- Have detailed tracking and logging of email delivery, opens, clicks, and other interactions
- Have the ability to quarantine emails and give the users a portal to review
- Have the ability to import historic emails from SourceOne and categorize them based on predefined criteria such as sender, date, subject, and content. (.EMX files)
- Have a Business Continuity web portal with the ability to send/receive emails when Microsoft is unavailable
- Have the ability to black/white listing of both domains and individual emails from an end user portal

1.5 CURRENT CIRCUMSTANCE/SITUATION

GRDA has identified a need to supplement the email security functionality that we are currently getting from Microsoft. Email filtering is allowing too much spam &/or malicious emails through to our users and it does not allow enough granularity for filtering and blocking email senders and/or domains.

1.6 RESPONSE REQUIREMENTS

Please keep your response to 10 pages or less. RFI responses should contain the following:

- Contact Information
  - Please provide the following contact information:
    - Company Name
    - Address
    - Name of the individual who will act as primary point of contact for inquiries
    - Contact Person's Telephone Number
    - Contact Person's Email Address

- Comments
  - Please provide your evaluative comments on the project description and requirements outlined in this document. Include any suggestions or advice regarding the design, implementation, management, technology, etc. of this issue. Detail what additional information or clarifications would be needed in order to prepare a comprehensive proposal in the future. Please include with your response your past work history and years of experience on projects of a similar scope.

  - Responses to the Vendor & Technical Requirements, sections 1.3 & 1.4 respectively, should be answered in the "GRDA Email Security Requirements Response Form.xlsx" file provided with this RFI.

- Approach

  - Based on the project information provided to date, briefly describe the approach you would recommend for this project and why.

- Pricing

- Indicative pricing, or a rough estimate, only is requested for budgetary purposes.

- Site Visit
  - No site visit is required at this time.

- *****PLEASE DO NOT PROVIDE A FORMAL QUOTE OR PROPOSAL FOR THIS RFI*****

1.7 SUBMISSION OF INFORMATION

Written responses must be submitted no later than August 21, 2023 at 5:00 PM CT.

Responses to this RFI must be submitted via email to the following:

Stephanie Waits
9933 E 16th St
Tulsa, OK 74128
Email: **stephanie.waits@grda.com**

Preparation and submittal of a response shall be at the expense of the vendor and at no cost to GRDA.

Any questions pertaining to this RFI must be sent in writing to Stephanie Waits at **stephanie.waits@grda.com** by no later than August 14, 2023 at 5:00 PM CT.

Only answers provided by the GRDA Central Purchasing Unit will be considered official and valid by GRDA.

1.8 OUTCOME

The Grand River Dam Authority does not guarantee any formal solicitation will be generated based on this.