Exhibit D

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L1 – Service Category 1: Endpoint-Based Asset Discovery

Respondent Name: Gamma Defense in partnership with Heimdal

Solution Name: Heimdal Advanced Vulnerability Management Solution

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 10. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 10 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 10 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-10 / 9) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1.

Prompt 1: An Endpoint-Based Asset Discovery Solution must continuously scan, detect, and inventory all endpoint devices, including, but not limited to, laptops, desktops, servers, and any other connected devices across the enterprise. The Solution must utilize lightweight agents that are deployed via endpoints, consuming minimal CPU and memory resources to avoid degrading performance or user experience.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

With Heimdal, your security is our top priority. Part of Heimdal's robust, defense-in-depth, unified security platform, Heimdal's Advanced Vulnerability Management solution provides organizations with real-time visibility and control over all managed endpoints, ensuring that devices are correctly configured, secured, and updated. Our solution, managed through Heimdal's award-winning unified dashboard, effectively manages discovered devices that access an organization's network or IT environment, including laptops, desktops, servers, and mobile devices, to maintain an up-to-date inventory of discovered hardware and software.

Configure patching or updating schedules to align perfectly with your organization's requirements. Whether it's enforcing urgent updates, prioritizing user groups, or rolling back unstable software versions, our solution offers unparalleled flexibility. For those who prefer a hands-off approach, trust in the system's intelligent automation to optimize vulnerability and software asset management decisions. Achieve unparalleled policy customization with our effortless "set-and-forget" configurations. Our solution offers hassle-free management with complete control over scheduling and deployment, including custom or hands-free setups that won't disrupt end-users.

Our solution automatically installs updates based on your configured policies without requiring manual input. As soon as new patches are released, Heimdal provides thoroughly tested, repackaged, and ad-free updates using encrypted packages inside encrypted HTTPS, and our technology silently deploys them to your endpoints without reboots or user interruption, ensuring your system's safety. This comprehensive approach improves security management and incident response and delivers comprehensive AI-powered endpoint security in a single, lightweight agent consuming minimal CPU and memory resources to avoid degrading performance or user experience.

With our solution's centralized console and comprehensive reporting, gain deep insights into vulnerabilities, sorted by severity, CVE, and type, irrespective of the OS in use. Seamlessly install, deploy, and administer both security and non-security updates across any system, ensuring compatibility and efficiency at all times and preventing configuration drift. Our solution helps ensure compliance with organizational policies and industry regulations and provides in-depth security status insights for strategic and operational planning. With complete visibility and granular control over your entire software inventory, you'll never have to worry about missing a critical patch again.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Real-Time Asset Discovery –Solution should run continuously, detecting new devices as they connect to the network. This should include remote devices.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution runs continuously, detecting new devices, including remote devices, as they connect to the network. To do this, Heimdal scans networks for "non-Heimdal" devices, illuminating endpoints or servers that do not carry the Heimdal lightweight agent and, thereby, Heimdal's cybersecurity protection.

Prompt 3: Detailed Hardware and Software Inventories – Solution should include inventory of processor types, memory, storage, installed software, patch levels, operating system versions, and device configurations.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution provides both software and hardware asset inventories of endpoint devices. Heimdal will discover all software assets on organization devices, giving a centralized view of applications, versions, and on which devices. Software Asset Management of licensed software can also be achieved. Hardware details are captured for client devices, including, but not limited to, processor types, memory, storage, and OS system information.

Prompt 4: Customizable Asset Classifications – Solution should allow administrators to tag devices by type, location, or business unit for easier management.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution's intuitive console enables administrators to group devices as requirements dictate for easier identification or management. Customizable notes can be left against device instances within the console to assist device management and collaboration within the Heimdal platform.

Prompt 5: Agent Health Monitoring – Solution should ensure that agents are functioning correctly and can be managed or repaired from a central console, if necessary. The Solution should provide alerts if an agent becomes inactive or fails to report.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution ensures that agents are functioning correctly and can be managed or repaired from a central console. Moreover, the fully self-healing Heimdal agent will automatically capture and alert all warnings with the initial timestamp and the moment of resolution.

Prompt 6: Centralized Management Console – Solution should provide a centralized management console that displays an up-to-date view of all discovered endpoints, including non-standard devices such as personal mobile devices or tablets.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution's centralized console provides real-time visibility and granular control of all agents and devices across the organization's network. It allows the Customer's team to send scripts, visualize telemetry, and, with add-on services, including Heimdal Remote Desktop, Heimdal Privileged Access Management, and Heimdal Application Control, perform remote connections, manage admin rights and elevation requests, and manage application allow/blocklisting.

Prompt 7: Compliance Enforcement – Solution should provide alerts to where endpoints that fail to meet security requirements (e.g., outdated patches or unauthorized software) can be flagged for remediation.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution utilizes a single, lightweight agent to capture data from protected endpoints silently. This includes signal and telemetry data from identities, apps, devices, and connectivity, allowing you to continuously track and update software vulnerabilities across your software inventory by severity, CVE, and type. Our solution enables you to proactively address vulnerabilities to ensure compliance with organizational policies and prevent configuration drift.

Prompt 8: Integration of CTI Data Feeds – Solution should provide real-time insights into endpoint vulnerabilities, ensuring that newly discovered devices are checked against the latest IoCs (Indicators of Compromise) and CVEs (Common Vulnerabilities and Exposures) behaviors targeting specific operating systems or device types.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution will continually check devices, including newly discovered ones, against software and OS vulnerabilities, mapping the latest CVEs against the software applications on the device. Heimdal will use eXtended Threat Protection to map TTPs to indicate instances of IoCs and IoAs within an organization ranked by severity.

Prompt 9: Patching and Deployment Capability – Solutions should provide endpoint patch and deploy services which allows managing patch and deployment of operating system and application updates on systems utilizing the agent.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution automatically installs updates based on your configured policies without requiring manual input. As soon as new patches are released, Heimdal provides thoroughly tested, repackaged, and ad-free updates using encrypted packages inside encrypted HTTPS, and our technology silently deploys them to your endpoints without reboots or user interruption, ensuring your system's safety.

Prompt 10: Metrics – Solution should provide the ability to roll-up patch and deployment level metrics across the domain.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. The Heimdal suite provides reporting capabilities for patch management activity, including patch deployment success, vulnerable applications, and device compliance to regulatory standards.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L3 – Service Category 3: Endpoint Detection and Response

Respondent Name: Gamma Defense in partnership with Heimdal

Solution Name: Heimdal Unified Endpoint Detection & Response Solution

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 9. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 9 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 9 are worth a maximum of 4 points total. An individual Evaluator's technical score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-9 / 8) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: An Endpoint Detection and Response (EDR) Solution is designed to provide continuous and comprehensive monitoring of endpoint activities to detect, investigate, and respond to threats in real-time. The Solution collects and analyzes detailed telemetry data, such as file access patterns, process execution, network connections, and registry changes, to identify malicious behavior that traditional antivirus software might miss.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Heimdal's Endpoint Detection & Response (EDR) solution is comprised of multiple security services, ensuring advanced protection at the endpoint. Incorporated into the EDR solution is Heimdal's DNS Security, Next Generation Anti-Virus (NGAV) with eXtended Threat Protection (XTP) and Ransomware Encryption Protection (REP).

Greater than 90% of all known malware leverages the DNS in its attack chain. By protecting the DNS vector on the endpoint, Heimdal is well positioned to efficiently and effectively neutralize malware exploiting the vector for initial delivery, communication to command-and-control servers, and exfiltration of data.

Heimdal's DNS Security deploys two engines: Darklayer Guard and VectorN Detection. Darklayer guard blocks malicious DNS communication, protecting the end-user device from malicious network communication to mitigate Zero Hour exploits, Ransomware C&Cs, next-gen attacks, and data leakages. Threat-to-process correlation technology in the solution will identify the processes or .exes making malicious DNS requests.

AI is incorporated into the solution to determine the reputation of "0-hour" domains (newly created domains whose reputation is not yet available in conventional intel feeds), further protecting the end-user device from unknown threats.

Heimdal's XTP engine provides organizations with granular detail and monitoring of processes running on end-user devices, with severity-based alerting against adversary tactics, techniques, and procedures mapped to the Mitre Att&ck framework. 'Living off the land' style threats and fileless malware will be detected, which typically evade traditional security technologies. The organization will be protected against malicious activities including, but not limited to, credential access, defense evasion, exploits, exfiltration, and lateral movement.

Heimdal's NGAV provides real-time malware protection, which runs at all times on the end-user device, searching for threats or infections. Next-Gen Antivirus uses traditional and advanced methods to detect and prevent malware from infecting your device. These include Signature-based detection, heuristic-based detection, and behavior-based detection.

When operating with Heimdal's Threat Hunting & Action Center, further forensic capabilities are incorporated into the EDR offering, including sandboxing capabilities. Security teams can upload and execute suspicious files for further analysis.

Heimdal's Ransomware Encryption Protection (REP) is a 100% signature-free solution that protects your devices against malicious encryption attempts initiated during ransomware attacks. REP operates on behavioral analysis (it triggers detections based on rules that mimic ransomware behavior) and processes kernel events for I/O reads, writes, directory enumeration, and file execution.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on how the Solution meets the identified technical capabilities and features.

Prompt 2: Real-Time Monitoring and Logging – Solution should provide real-time monitoring and logging of all endpoint activities, including, but not limited to, file changes, process creation and termination, registry edits, network connections, and USB device insertion.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution provides real-time monitoring and logging of all endpoint activities. Heimdal achieves this through proactive threat hunting and continuous monitoring across machine processes and network activity for known TTPs. Utilizing known/predictive intelligence, our XTP Engine and additional security modules process through more than 1500 Sigma rules, mapped to the MITRE ATT&CK framework to provide granular telemetry into IT environments, endpoints, networks, and end users.

Prompt 3: Behavioral Analytics – Solution should use an extended portfolio of security tools, like endpoint firewalls, device and application control, application inventory, signature matching, vulnerability and patch management and others, plus network-level tools such as secure email and sandboxing.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Heimdal's portfolio can provide endpoint-based firewalls, granular device and application management/control, signature detection, vulnerability discovery and patching, and network-based security with secure email capability. Heimdal has an extensive portfolio of security tools covering Cloud Security, Network Security, Vulnerability Management, Privileged Access Management, and Email Security, in addition to an EDR solution.

Prompt 4: Automated Response Mechanisms – Solution should take predefined actions when threats are detected, such as isolating the affected device from the network, terminating malicious processes, or blocking IP addresses.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution can automate actions when threats are detected. Actions include, but are not limited to are logging off the user, shutting down, isolation of the device, and cloud disconnection. IPs and processes can be blocked/quarantined for analysis by security teams. An overlay of the internal SOC at Heimdal can also respond to these items with pre-agreed responses from the MXDR Adapt service 24/7/365.

Prompt 5: Threat Hunting Tools – Solution should allow analysts to query across the entire organization's endpoints, searching for specific indications or compromise (IoCs) or patterns that may indicate the presence of advanced threats.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution can aggregate IoCs/patterns that present as advanced threats. Heimdal's TAC center is a central hub that collates all sensor telemetry and provides a stack-ranked risk score. Security analysts are then able to swiftly threat hunt across the entire estate and are provided with recommended actions depending on the alert. Depending on the configuration, this can be acted on by the internal SOC team or Heimdal's own SOC Team.

Prompt 6: Support for Remote Endpoints – Solution should ensure that devices outside of the network, such as remote or mobile works, are protected and monitored regardless of location.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Heimdal is a cloud-first endpoint protection platform. Devices will be protected and monitored, regardless of location.

Prompt 7: Remediation Playbooks – Solution should provide detailed guidance for resolving detected incidents, including step-by-step instructions for isolating infected devices, rolling back malicious changes, and restoring systems to a known good state.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Heimdal's SOC engineers have stress-tested playbooks and strategies to provide comprehensive prevention, detection, containment, and remediation of security incidents. Playbooks can be enacted alongside Heimdal SOC engineers/analysts as part of the MXDR service or can be provided to be executed internally with Heimdal's customer success function.

Prompt 8: Integration of CTI Data Feeds – Solution should provide real-time updates on emerging malware strains, threat actor campaigns, and new attack vectors targeting endpoints. The EDR Solution can use CTI feeds to compare endpoint behavior when known IoCs, enhancing detection and automated response capabilities.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution natively leverages multiple real-time threat intelligence feeds and signature-based and signatureless engines to block known and unknown cyberattacks. Heimdal will work with Customers to determine if additional desired feeds can be integrated.

Prompt 9: Forensic Capabilities – Solution should allow security analysts to investigate historical endpoint activities, enabling root cause analysis and providing a detailed timeline of events leading up to a security incident.

Yes. Our forensic capabilities are reflected in the Threat-hunting and Action Center. A potent threat intel and hunting toolkit, it equips security leaders and operations teams with the ability to detect and respond to next-gen threats using a visual storyboard and sandbox across the entire IT landscape. Data captured from multiple sensors due to the breadth of the platform allows analysts to decipher and easily storyboard security events/root cause analysis.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L5 – Service Category 5: Email Security

Respondent Name: Gamma Defense in partnership with Heimdal

Solution Name: Heimdal Advanced Email Security Solution

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response Score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Email Security Solutions must protect against email-based threats such as phishing, malware, ransomware, and email compromises. The Solution should analyze both inbound and outbound email communications in real-time, using advanced detection techniques to filter malicious content without disrupting legitimate business correspondence.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Heimdal's Email Security solution is a robust tool that effectively blocks all email-based threats, including phishing, malware, ransomware, and email compromise as well as spam. It employs advanced AI-powered protection mechanisms against phishing and spam, conducts deep attachment scanning using state-of-the-art detection technologies, and adds extra layers of protection to M365 and Google environments. The Heimdal Email Fraud Prevention module uses more than 125 analysis vectors and live threat intelligence to find and stop Business Email Compromise scams, phishing, and complex malware before you're compromised.

Our advanced mail exchange gateway solution utilizes state-of-the-art technologies to process inbound and outbound emails quickly and efficiently, ensuring timely delivery. We maintain a delay of only between 5 and 15 seconds. By employing optimized algorithms, intelligent routing protocols, and parallel processing techniques, our solution streamlines the mail exchange process, minimizing latency and maximizing throughput. It leverages distributed computing, multi-threading, and performance optimization features to handle large email volumes within demanding timeframes, achieving exceptional performance and scalability. Our solution also incorporates intelligent traffic management mechanisms to prioritize critical email traffic, expediting delivery and minimizing bottlenecks. With a robust and fault-tolerant architecture, our solution ensures continuous operation even under high loads, providing a reliable platform for government email exchange needs.

The solution provides the ability to create and enforce email security policies that align with the Customer's security requirements. This shall include policies for anti-spam, anti-phishing, anti-malware, data loss prevention, encryption, and email archiving. Once email configuration is established, policy violations are impossible.

Our solution, which is managed within the same intuitive console as the rest of Heimdal's award-winning unified defense-in-depth cybersecurity solutions, offers a comprehensive suite of features. It analyzes both inbound and outbound emails to detect potential threats in real-time, incorporating many advanced inspection processes, from basic email security (DMARC, DKIM/SPF, TLS) to advanced AI-powered malware, phishing, and spam detection and filtering engines, deep content inspection, real-time reformatting of attachments, and secure detonation of executables through advanced sandboxing with deep attachment scanning. It also provides customizable threat alerts and policies, full forensics with complete data logging, and more, ensuring all your email security needs are met. With an exceptional 0.05% false-positive rate, our innovative solution is a robust shield, effectively identifying and blocking malicious emails without disrupting legitimate business correspondence.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Content Filtering – The Solution should break down files to their discrete components in real-time and reconstruct a clean version of the email, removing anything that doesn't conform with the file type specifications, a nationally recognized standard, or company policy.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution uses a real-time high-speed and high-performance sandbox for deep content inspection and deconstructs each incoming file into its discrete components. It disarms and reconstructs each file, automatically removing malware-laced attachments and extracting anything that doesn't conform to the file type specifications, a nationally recognized standard, or company policy before returning a safe, sanitized email to the recipient.

Prompt 3: Phishing Detection – Solution should analyze the email's context, structure, and metadata (e.g., header information) to detect phishing attempts, which may include spear-phishing and targeted attacks.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution includes robust inbound and outbound customer-specific AI-enabled detection for CEO fraud and protects against spear-phishing and targeted attacks within the organization. The solution learns the baseline communication patterns, methods, and over 120 other vectors to alert anomalous behavior with an industry-leading 0.05% false-positive rate, effectively fortifying end-users and organization-wide communications against phishing, malware, ransomware, and spam.

Prompt 4: Sandboxing Technology – Solution should have the capability to safely execute email attachments and embedded links in an isolated environment to determine if they are malicious before delivery to the recipient.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution enables the safe execution of various email attachments and content within the email, including embedded links, macros, scripts, and PDF attachments, through advanced sandboxing with deep attachment scanning before returning a clean email to the intended recipient.

Prompt 5: Advanced Anti Spoofing Protections – Solution should include enforcement of Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message

Authentication, Reporting, and Conformance (DMARC) protocols to prevent sender impersonation.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution enforces DMARC, DKIM/SPF, and TLS protocols to prevent sender impersonation. It provides spoofed message security using AI and ML-based fuzzy name matching to detect spoofed display names by analyzing email headers and sender names and comparing them against a predetermined list of potential targets, advanced AI-powered malware, phishing and spam filtering engines, deep content inspection, real-time reformatting of attachments, and much more to neutralize phishing attempts.

Prompt 6: Email Encryption – Solution should include encryption for sensitive communications, ensuring enforcement that messages are encrypted both in transit and at rest.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Heimdal ESEC offers different settings for TLS communication. The TLS Setting in the general configuration per domain defines how ESEC communicates with inbound servers of the organization. The other setting is handling incoming emails to ESEC. Here you can Force TLS and define how the emails will be handled (Rejected, Quarantined, Tagged). The last setting regarding TLS is used to define the communication the next Hop server (Outbound verification) here you can set "Forced TLS" as default.

Prompt 7: End-User Awareness Features – Solution should include automatic banners or warnings added to suspicious emails, helping users recognize potential threats.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution provides feature capabilities to automatically tag email correspondence from outside the organization for closer inspection by the user, helping users recognize potential threats. Fraud prevention capabilities will isolate emails into a separate folder should they trigger a certain threshold by presenting hallmarks of fraudulent activity.

Prompt 8: Quarantine and Remediation Tools – Solution should provide quarantine and remediation tools for administrators, allowing them to review flagged messages, release legitimate emails mistakenly identified as threats, and block harmful content.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution provides quarantine and remediation tools for administrators. Based on the configuration in the Heimdal Security tool, the administrator will have several options for managing the email environment further (including its content)- they can release, allowlist, blocklist, add to quarantine, or even deny a specific email.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L7 – Service Category 7: Security Operations Platform

Respondent Name: Gamma Defense in partnership with Heimdal

Solution Name: Heimdal Security Operations Platform Solution

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: The Security Operations Platform (SOP) must integrate multiple security tools and technologies into a single unified platform, providing comprehensive visibility into an organization's IT environment. The Solution should allow security teams to detect, investigate, and respond to threats in real-time, correlating data from across the infrastructure to provide a holistic view of security incidents.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

The Heimdal Security Operations Platform is built with state-of-the-art proactive & reactive security as core capabilities, layering multiple cybersecurity tools and technologies into a single unified platform, providing comprehensive visibility into an organization's IT environment. The solution allows security teams to detect, investigate, and respond to threats in real time, correlating data from across the infrastructure to provide a holistic view of security incidents and enabling Security Operators to take specific actions tailored to each detection at the click of a button.

Our solution combines Threat Prevention at the endpoint and/or network level, Patch & Asset Management, NextGen Anti-virus with Extended Threat Protection, Anti-Ransomware Protection, Application Control, Privilege Elevation & Delegation Management, and our Remote Desktop modules with our Award-winning Threat Hunting & Action Center. This unique tool combines capabilities from XDR, SIEM, and SOAR tools by leveraging all the Heimdal products in a Security Operations tool with out-of-the-box pre-defined actions for each detection, automated or manual (depending on their potential impact on the affected endpoints), which does not require any configuration time, reducing the implementation and staff training time and providing immediate value to the organization. Moreover, the manual remediation responses can be automated going forward.

Our solution automatically blocks malicious activity from both proactive and reactive perspectives (via Threat Prevention, NextGen Anti-Virus, and Ransomware Encryption Protection) or processes that were not pre-verified or flagged by the operators (via Application Control, depending on the configuration chosen by the operators); once the operator selects a change in the policies, they can immediately replicate that as an automated response going forward for all or some groups. The solution utilizes proprietary AI algorithms (Machine Learning and multiple Neural Networks) and automatically integrates multiple additional threat intelligence sources to further enrich the AI's learning capacity in real time.

Our solution enables immediate enterprise protection through a unified platform approach, ensuring consistent security across various environments. The 24x7 proactive monitoring and threat remediation capabilities help minimize enterprise-wide security risks by detecting and responding to threats in real time. By leveraging proactive and automated responses, Heimdal significantly reduces mean time to detect (MTTD) and mean time to respond (MTTR) across multiple attack vectors, including network, endpoints, emails, access, and identity. Furthermore, Heimdal addresses SecOps skills shortages by providing advanced investigations and forensics, allowing internal teams to focus on critical objectives while relying on Heimdal for comprehensive security coverage.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Log Event Aggregation and Correlation – Solution should log event aggregation and correlation from various security devices (firewalls, IDS/IPS, endpoint detection tools, network devices, and cloud services) to identify patterns and indicators of compromise.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution empowers users by providing direct access to aggregated logs from sources like Event Viewer, Sysmon, and Heimdal proprietary software. Log aggregation and correlation of events into the TAC portal is native and comes pre-configured out of the box. These can be downloaded for detailed inspection and analysis.

Prompt 3: Automated Incident Response Workflows – Solution should allow security operations teams to optionally automate common tasks such as blocking IP addresses, isolating infected devices, or generating alerts for further investigation

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution will provide security operations teams with the capabilities to automate common tasks or detections within their environment with a stock response, reducing operational overheads and time sinks. Automated isolation of devices can be configured, reducing the time to respond to critical alerts.

Prompt 4: Real-Time Threat Detection – Solution should be powered by machine learning models and behavioral analytics, capable of identifying zero-day attacks, insider threats, and anomalous activities that deviate from the organization's baseline.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution is powered by machine learning models that overlay the aggregated alerts and analytics collected. This model is able to commute the risk within an environment against the baseline within an organization to highlight IoCs and IoAs.

Prompt 5: Customizable Dashboards – Solution should have dashboards displaying real-time security metrics, providing visualizations of key performance indicators (KPIs) such as the number of incidents, time-to-respond, or threat severity.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. When operating in Heimdal's Threat Hunting & Action Center, security operations teams will engage with a dashboard that displays real-time security metrics captured across the unified suite of security modules deployed within the Heimdal Endpoint Protection Platform. Alert triage is simplified as data from multiple security tools is aggregated and contextualized into actionable insights, including severity and device/user risk scores.

Prompt 6: Incident Management Capabilities – Solution should provide detailed incident tracking, ticketing integration, and root cause analysis, ensuring that all security events are fully documented and addressed.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution lets security teams track incidents/alerts in a unified view. This view consolidates incidents and analysis of events so that teams can work across departments and update investigation details in real-time.

Prompt 7: Integration with Threat Intelligence Platforms (TIPs)– Solution should enrich security alerts with contextual information about current threat actors, malware campaigns, and indicators of compromise.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution natively leverages multiple real-time threat intelligence feeds and signature-based and signatureless engines to block known and unknown cyberattacks. Heimdal will work with Customers to determine if additional desired threat intelligence and CTI data feeds can be integrated.

Prompt 8: Integration of CTI Data Feeds – Solution should Allow for real-time enrichment of alerts, correlating incidents with known global threat actor campaigns, IoCs, and TTPs (Tactics, Techniques, and Procedures), improving situational awareness and response times

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution natively leverages multiple real-time threat intelligence feeds and signature-based and signatureless engines to block known and unknown cyberattacks. Heimdal will work with Customers to determine if additional desired threat intelligence and CTI data feeds can be integrated.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L13 – Service Category 13: Vulnerability Assessment and Management

Respondent Name: Gamma Defense in partnership with Heimdal

Solution Name: Heimdal Advanced Vulnerability Management Solution

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-8 / 7) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Vulnerability Assessment and Management Solutions must enable organizations to continuously scan their IT assets for security vulnerabilities, evaluate the risks associated with these vulnerabilities, and prioritize remediation efforts. The Solution should automate both scanning and remediation workflows, providing real-time visibility into the organization's security posture.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Heimdal's Advanced Vulnerability Management Solution enables organizations to continuously scan their IT assets for security vulnerabilities, evaluate the associated risks, and prioritize remediation efforts. Our solution automates both scanning and remediation workflows, providing near real-time visibility into the organization's security posture.

Heimdal combines detailed vulnerability assessment and patch management into a single, automated solution at the software and operating system levels. Near real-time vulnerability assessment provides security teams with granular telemetry of software and OS vulnerabilities across the IT estate, regardless of a device's location. CVE and CVSS data are integrated into the Heimdal platform to inform organizations of vulnerability severity and provide actionable insights via NIST.

Heimdal provides vulnerability remediation in patch management automation for third-party applications and operating systems updates across Windows, Mac, and Linux (Ubuntu). Heimdal's third-party patch management solution natively supports the automated update of ~250 everyday critical applications, incorporating robust testing processes for newly released patches before availability for customer environments. Four hours is the typical time taken for testing to be completed before a patch is available for the Heimdal customer network. Customers can create robust patching controls and remediation workflows with simplicity at a policy level. Patching schedules or maintenance windows can be swiftly curated for client devices.

Operations teams will be further supported by granular controls such as rollback functionality, fresh application deployment, or uninstallation. Operating system updates can be automated or closely managed, providing flexibility for the administrator. Schedules for deployment and reboots can be managed to ensure the organization meets robust patching controls while managing the disruption to the user, improving engagement with reboot mechanisms.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Automated and Continuous Vulnerability Scanning – Solution should include automated and continuous scanning of network devices, servers, endpoints, and applications. The scans should identify known vulnerabilities (e.g., CVEs), misconfigurations, and missing patches.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution will continuously scan servers and endpoints for software application and OS vulnerabilities. Security teams will have a detailed understanding of known vulnerabilities across

their estate with data points enriched by CVE and CVSS data and integrated from NIST databases. Automated deployment of required patches and updates significantly reduces exposure to vulnerabilities while removing the resource overheads typically associated with robust vulnerability management.

Prompt 3: Risk-Based Vulnerability Prioritization – Solution should allow vulnerabilities to be sorted and ranked based on the criticality of the affected asset, the exploitability of the vulnerability, and the business impact. This helps organizations focus on high-priority issues that pose the most risk.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution's reporting of vulnerabilities can be swiftly ranked based on the severity of the vulnerabilities found within the organization's estate according to their CVSS scoring or severity assigned by Microsoft, etc. When using the Threat Hunting & Action Centre, software and OS vulnerabilities are key components of any risk scoring. Devices registering the highest risk based on present vulnerabilities can be easily identified and triaged.

Prompt 4: Remediation Workflows – Solution should integrate with IT service management (ITSM) systems, automatically creating tickets or work orders for IT teams to address vulnerabilities, track progress, and close issues once remediated.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution supports the use of APIs, enabling data points to be migrated into ITSM systems for ticketing or auditing purposes. Vulnerability detection and remediation of software applications and operating systems are contained within the single solution, from which reports of activities, vulnerabilities, and patching statuses can be shared directly with required stakeholders.

Prompt 5: Detailed Vulnerability Reports – Solution should include the ability to provide reports including information such as affected assets, severity ratings (e.g., CVSS scores), vulnerability descriptions, and recommended fixes.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution provides reports of vulnerabilities in the application and OS layers. Reports will include, but are not limited to, identification of vulnerable applications, affected assets, CVSS or CVE information, and patching errors.

Prompt 6: Real-Time Insights and Trend Analysis – Solution should provide insights into the overall security posture, such as the number of open vulnerabilities, time-to-remediation, and patch compliance rates.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. When using Heimdal's Threat Hunting & Action Center, a risk score is presented for each device based on threat telemetry across multiple security modules, with open application and operating system vulnerabilities contributing to the overall score. A granular understanding of the organization's patch compliance rates, open vulnerabilities, and time-stamped patching activities is also captured for security, compliance, and operations teams.

Prompt 7: Integration with Patch Management Solutions – Solution should allow organizations to deploy patches to vulnerable systems directly from the platform.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. The Heimdal platform includes the proprietary Patch & Asset Management module. The module enables IT functions to automate vulnerability scanning and patch deployment for both operating systems and third-party applications, including complete "set and forget" workflows.

Prompt 8: Integration of CTI Data Feeds – Solution should enhance vulnerability prioritization by providing real-time threat intelligence on active exploitation campaigns, emerging threats, or vulnerabilities that are being specifically targeted by threat actors.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes. Our solution natively leverages multiple real-time threat intelligence feeds and signature-based and signatureless engines to block known and unknown cyberattacks. Heimdal will work with Customers to determine if additional desired threat intelligence and CTI data feeds can be integrated.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L15 – Service Category 15: Data Security

Respondent Name: Gamma Defense in partnership with Assured Data Protection

Solution Name: Assured Rubrik Data Security Solution

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 11. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 11 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 11 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-11 / 10) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Data Security Solutions are designed to protect sensitive information from unauthorized access, loss, or exfiltration. The Solution should monitor data in use, in motion, and at rest, enforcing data protection policies, and detecting any unauthorized attempts to access or share sensitive data. The Solution must integrate with existing security frameworks and support compliance requirements to ensure organizations meet their regulatory obligations.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Assured's data security solution, powered by Rubrik, was designed to protect sensitive information from unauthorized access, loss, or exfiltration. The solution monitors data in use, in motion, and at rest, enforcing data protection policies and detecting any unauthorized attempts to access or share sensitive data. It seamlessly integrates with existing security frameworks and supports compliance requirements to ensure organizations meet their regulatory obligations.

Rubrik collapses backup software, catalog management, replication, and de-duplicated storage into a single appliance. Distributed architecture means Data Protection and management services scale in line with your production workloads to maximize efficiency and deliver near-zero recovery times at scale. Global file search capabilities within Rubrik extend the reach of an IT administrator into their backup platform to satisfy the most challenging restore and compliance requirements. Our distributed design allows for horizontal scale-out capability for thousands of nodes to support the largest backup environments.

Our solution fully supports cloud-based, on-premises, and multi-cloud deployments, providing a unified management console to protect and manage data across all environments. This approach allows users to back up, recover, and replicate data seamlessly, whether in a private data center, on a public cloud like AWS, Azure, or GCP, or across multiple clouds simultaneously, effectively managing data protection across a hybrid cloud landscape with an intuitive and easy-to-use console on a single pane of glass.

For the portions that are prompts (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features..

Prompt 2: Data Discovery and Classification – Solution should automatically identify and classify sensitive data across the organization's infrastructure, including databases, file shares, cloud storage, and endpoint devices. The classification engine should apply tags based on predefined policies for data types such as Personally Identifiable Information (PII), financial data, and intellectual property. Enable continuous data discovery to detect new or modified data that requires protection.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution automatically identifies and classifies sensitive data across an organization's infrastructure without negatively impacting production. The solution applies tags based on predefined policies and enables continuous data discovery to detect new or modified data that

requires protection, providing a reportable chronological record of all data access and manipulation within a system.

Prompt 3: Data Loss Prevention (DLP) – Solution should monitor and block unauthorized sharing of sensitive data across multiple communication channels, including email, cloud services, USB devices, and other pathways. Ensure that sensitive data is protected from being copied or moved without proper authorization, with real-time monitoring and alerting capabilities.

Please describe if and how Respondent's proposed Solution meets this prompt in the field below.

Yes. Our solution monitors and blocks unauthorized sharing of sensitive data across multiple communication channels, ensuring that sensitive data is protected from being copied or moved without proper authorization, with real-time monitoring and alerting capabilities. It also seamlessly integrates with other dedicated DLP tools to provide a comprehensive data security solution that aligns with your organization's DLP approach.

Prompt 4: Encryption – Solution should monitor and block unauthorized sharing of sensitive data across multiple communication channels, including email, cloud services, USB devices, and other pathways. Ensure that sensitive data is protected from being copied or moved without proper authorization, with real-time monitoring and alerting capabilities.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution uses the strong AES-256 encryption algorithm to ensure that sensitive data is encrypted at rest and in transit, ensuring that data accessed without proper authorization remains unreadable. Key management is done internally, providing an additional layer of security and enabling secure cluster erasure. Moreover, our solution was designed for scale, efficiently meeting the needs of high data growth in an enterprise environment.

Prompt 5: User and Entity Behavior Analytics (UEBA) – Solution should analyze how users interact with sensitive data, detecting anomalous behaviors such as copying large amounts of data, accessing restricted files, or sharing data with unauthorized third parties. The Solution should use machine learning to identify insider threats and abnormal data access patterns before breaches occur.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution can analyze how users interact with sensitive data, detecting anomalous behaviors like copying large amounts of data, accessing restricted files, or sharing data with unauthorized third parties through its User Access Analysis feature. The solution uses machine learning to identify abnormal user access patterns, allowing for monitoring and alerting on potentially suspicious data manipulation behaviors and potential data breaches.

Prompt 6: Automated Incident Response – Solution should automate response mechanisms to prevent unauthorized actions, such as blocking sensitive data transfers, issuing alerts, or requiring additional authentication when policy violations are detected. Quarantine suspicious files, block access to certain data, or alert security teams in real-time when DLP policies are breached.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution automates incident response mechanisms to prevent unauthorized actions through its reporting, alerting, and quarantine functions. The solution automatically detects and classifies sensitive data, generates alerts in real-time when potential data breaches are identified, and prevents further access or exposure by quarantining potentially compromised data.

Prompt 7: Audit Trails and Reporting – Solution should provide comprehensive audit trails of all data-related activities, including details of who accessed sensitive data, what actions were taken, and when. Generate detailed reports for compliance audits, security evaluations, and incident response investigations.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution provides comprehensive audit trails by maintaining a detailed log of all user actions and system events, including details of who accessed sensitive data, what actions were taken, and when. Our solution's intuitive reporting feature easily generates detailed reports for compliance audits, security evaluations, and incident response investigations.

Prompt 8: Compliance Management – Solution should integrate with compliance management platforms to help organizations meet regulatory requirements (e.g., GDPR, CCPA, HIPAA) and provide detailed reporting on data access and protection measures. Ensure organizations can map security controls to compliance frameworks and track any compliance gaps.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution can integrate with compliance management platforms and provides automated data discovery, classification, retention, and reporting capabilities to monitor and manage data compliance and identify any compliance gaps.

Prompt 9: Data Catalog and Metadata Management – Solution should provide comprehensive data discovery, search, and metadata management across various data sources within the organization. Metadata management should include data definitions, lineage, quality metrics, and usage patterns to ensure full context for all data assets. Provide tools for data profiling to assess data quality, identify inconsistencies, and maintain data completeness.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our solution's data discovery, search, and metadata management capabilities can be used across various data sources within the organization. It uses machine learning to automatically discover and classify sensitive data and leverages Rubrik Security Cloud to provide data protection and cyber resilience across enterprise, cloud, and SaaS applications and uses. Our solution allows users to set protocols based on their organization's data needs.

Prompt 10: Integration with Data Management Tools – Solution should provide seamless integration with ETL (Extract, Transform, Load) tools, data warehousing, and analytics platforms to streamline data processing workflows. Ensure scalability, enabling the Solution to handle large volumes of data and grow with the organization's evolving needs.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Our immutable, scalable, secure data protection solution integrates seamlessly with various tools and applications. The solution securely manages backup datasets and provides analysis of the backup data for sensitive data discovery and classification, anomaly detection and identification, alerting, and automated response to potential data breaches. Backup metadata can be extracted for analysis.

Prompt 11: Master Data Management (MDM) – Solution should provide capabilities to create and maintain a single, consistent view of master data (e.g., customer, product, or supplier data) across the organization. Ensure high data quality through robust cleansing, deduplication, and validation tools, while supporting governance frameworks for data ownership and access control.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Mostly. Our solution is a Cloud Data Management (CDM) platform focusing on data protection, backup, recovery, and archival across multiple cloud environments. It ensures high data quality through robust cleaning, deduplication, and validation tools while supporting governance frameworks for data ownership and access control. While it is not a traditional MDM solution, Rubrik seamlessly integrates with MDM solutions to provide a comprehensive, cyber-resilient data security solution.