Northern Maine Community College
Data Loss Prevention Software
Request for Proposals
April 2021

Northern Maine Community College (NMCC) is seeking proposals for data loss prevention software that will detect PII, PCI, HIPPA, and GDPR restricted information located in various file types on local and network storage locations.

Project Information:

The objective of this project is to define and implement a Data Loss Prevention Platform that:

- Will provide extensive visibility on where sensitive/protected data is located at rest and residing on NMCC systems.
- Will provide custom reports of what protected data was discovered, where that data is located, and what security policy it violates.
- Will have built in security policies including but not limited to HIPAA, PCI, GDPR, as well as the ability to be able to create custom security policies.
    - These custom policies should include the ability to do pattern matching.
- Will have the ability to automatically execute scans on specified intervals.
- Will be able to perform more than one scan at a time.
- Should also contain mechanisms to throttle or limit based on size, time window, and/or row count.
- Will be able to remediate violations of data at rest policies by encrypting or erasing restricted data once it has been identified.

Requirements:

The solution must:

- Provide the ability to scan unstructured data at rest that resides on Microsoft shares, as well as, to find and report any protected information defined by specified security policies.
- Provide an easy-to-use GUI interface that enables proficiency without extensive training.
- Provide the ability to limit the bandwidth a scan can use during certain times.
- Provide the ability to set scheduling for the automatic execution of scan times.
- Provide detailed, exportable, custom reports that displays the location of where the sensitive protected data is within the data at rest, as well as what security policy that data violates.
- Provide built in security policies such as HIPAA, PCI, GDPR, and others, as well as allow for custom security policies to be created by the user.
- Possess capability to be scalable to scan data volumes of 110 terabytes and higher without crashing.
- Possess capability to scan images, using Optical Character Recognition (OCR).
    - Should at a minimum include TIFF, PDF, BLOB, JPEG, GIF, PNG.

- Should have the ability to scan and process unstructured data files.
    - Should understand common MIME types including but not limited to:
        - Microsoft office, Office Open Document Format (general), Adobe Creative Suite created documents, image and video files.
- Provide the ability to scan data at rest in a Microsoft distributed file server (DFS) environment.
- Provide the ability to scan data sources that reside on both physical and virtual server machine environments.
- Employ security measures to limit visibility of reported data content found during the scans to only authorized users.
- Scan rest data for 150 Faculty and Staff on approximately 300 devices.
- Be scalable to address 20,000 student and staff/faculty/service Microsoft Active Directory accounts or more, if the DLP software requires it to operate.
- Be easy, cost-effective, and scalable.
- Be supported with implementation, training, and help desk services.
- Be supported with documentation.
- Provide a detailed line item quote for both 1-year, and a 3-year purchase of product license(s) as well as support for those years.
- Support running on Nutanix AHV if virtual servers are required.

RFP Estimated Timeline:

4/2/2021 – Request for Proposals will be distributed.
~~4/9/2021 – Due date for any clarification questions.~~
~~4/13/2021 – NMCC will respond to requests for clarification.~~
~~4/16/2021 – Final date for proposal submittal.~~
~~4/23/2021 – Selected vendor(s) will be notified if demonstration will be required.~~
~~4/30/2021 – Estimated date of vendor award.~~

Data Loss Prevention Software RFP Estimated Timeline – updated 4/8/2021:

4/13/2021 – Due date for any clarification questions.
4/15/2021 – NMCC will respond to requests for clarification.
4/20/2021 – Final date for proposal submittal.
4/26/2021 – Selected vendor(s) will be notified if demonstration will be required.
4/30/2021 – Estimated date of vendor award.

RFP responses must include the following:

Vendor Information:

1. A brief organizational history, including the amount of time spent supporting Higher Education organizations.
2. Please provide a description of your company's size (# of employees) and organizational structure.

3. Provide an approximation of the proportion of the organization that is solely focused on your Data Loss Prevention solution.
4. Have all components of your solution been designed and developed in house? If not, please indicate which components have been externally developed and provide a detailed description of how they integrate with your core product.
5. Please provide details as to any industry awards held by your organization, relevant to Data Loss Prevention.
6. Please provide customer references of three existing customers. NMCC prefers that those references be from similar sized colleges.

Scanning of Data:

1. Please provide a list of operating systems your product can connect to and scan.
2. Please provide a list of operating systems your scanning server product can operate on.
3. Please provide a list of virtual environments that your product can operate on.
4. Please provide a list of recommended processor, memory, and storage requirements a single scanning server would need to perform a scan on a volume size of 75 terabytes.
5. Please list the available installation method for your proposed solution (cloud or hybrid).
6. What is the expected impact on server performance while your product is scanning?
7. Does your solution require an agent for any collection methods or are all collection methods supported without an agent? If so, how do agents communicate with your product: Is it a two-way communication, what ACLs/network ports need to be open to enable communication?
8. Is the agent self-healing and updating after initial install? Please provide detail.
9. Describe the process of resuming a scan in the event the scan in disrupted because the client went offline. Does the scan have to start at the beginning again?
10. Does your solution provide the ability to perform full, differential, and/or incremental scans of data at rest?
11. Describe what type of connection protocols are needed between the scanning server and the target server in order for a scan to take place.
12. Explain how your solution would be implemented in order to scan and be ready to remediate in a Microsoft Distributed File System (DFS) environment.
13. Does your solution have the ability to do form recognition?
14. Does your solution utilize machine learning technologies?
15. Does your solution provide the ability to scan image files to discover images of protected data?
16. If your solution does provide image scanning, what image files can be read by the solution?
17. If your solution provides file fingerprinting, please describe how the solution utilizes this feature.
18. What features or methods does your solution employ to aid in minimizing false positives?
19. Does your solution provide information on what users have access to a file or folder that has been found to contain sensitive protected data?
20. Does your solution allow multiple scans to occur simultaneously on the same scanning server?
21. Does your solution scan unprotected compressed files and volumes?
22. Does your solution report what files could not be scanned because of encryptions or incompatible formats?
23. Does your solution have a file size limit in which it scans?

Remediation:

1. Does your solution provide automated remediation? Please describe the capabilities, including those provided out-of-the-box if applicable.
2. Does your solution require a software agent to be installed in order to perform remediation actions on a target server?
3. Please list what scripting languages could be automatically triggered by your software when an information match is found during a scan.
4. What are the capabilities for customers to add their own automated remediation?

Security:

1. How does your solution authenticate users to prevent unauthorized access to the system? Describe the security applied to the database to prevent unauthorized access to data.
2. What type of security is applied to internal communications between client and server machines? What method of encryption does your solution use to encrypt messages and transactions?
3. How does your solution store usernames and passwords?
4. Does your solution provide a way to self-audit and record user activities within the solution itself? What external, third-party security standards is your solution validated to or certified by?
5. Does your solution support two factor authentication?

Support:

1. What support options are available?
2. Please describe your SLA's for support.
3. Are support representatives responsible for more than one product? Please list all products supported by your support representatives.
4. How often do you release updates or upgrades to your platform?
5. How are customers notified about these upgrades?
6. How do we receive updates to your platform when there are changes in compliance regulations or new products on the market which may be utilized within our organization?
7. On average, how many levels of support does an end user need to navigate through before reaching someone directly familiar with your product?
8. Are your product specific support teams located in the countries or regions where your customers are located? Please describe the locations of these product specific support personnel.
9. Are any of your support personnel located in the same facilities as your product specific engineering personnel? If not, please explain the process by which your support personnel have access to engineering resources for advanced problem/issue resolution.
10. What method do you employ to collect customer feedback and incorporate it into future releases?

Training:

1. Do you offer training courses specifically for the product(s) included in the proposal? If so, please list the courses available.

2. Is training delivered by the vendor or by third party?
3. Are there online and classroom training options?

Documentation:

Is your solution supplied with any documentation? If so, please list how it is provided (e.g. electronic, hard copy, etc.).

Pricing:

1. How is your product licensed (e.g. per user, per site, per reporting device)?
2. If your pricing is based on user license count, please provide the user count you are basing it on.
3. Please provide the solution price breakdown by line item.
4. What is the cost of maintenance plans?
5. Please provide a price breakdown for licensing for 1-year and 3-year.
6. How are additional not out-of-the-box log sources handled (e.g. no additional cost, professional services)?
7. Would the purchased license entitle NMCC to any newer versions of the software (beyond updates) during the licensing period?

Evaluation:

Proposals will be reviewed and selection of one vendor will be based on the following criteria:

Factor	Weight
Total Proposed Price	35%
Response to RFP Questions	25%
Technical Support Availability (long term)	15%
Overall Suitability to NMCC's needs	15%
Proposal Quality, Detail, and Organization	10%

All questions and bids related to this request for proposals should be directed by email to jeclark@nmcc.edu and nccyr@nmcc.edu. The subject of the e-mail should clearly state "Questions: Data Loss Prevention Software." Deadline for questions is 4:00 pm April ~~9~~ 13, 2021. Questions and responses will be posted on our website: http://www.nmcc.edu/about-nmcc/news-info/rfps/. It is the College's intent to respond to all questions by April ~~13~~ 15, 2021. It will be the vendors' responsibility to check this site for updates.

The terms and conditions, including pricing, of the final agreement resulting from this RFP process shall be available to any MCCS entity for the procurement of goods and services from the selected vendor(s).

The college reserves the right to reject any or all bids.
This RFP shall be referenced in, and considered part of, any final contract.
See attached Notice to Bidders.

NOTICE TO VENDORS AND BIDDERS:
STANDARD TERMS AND CONDITIONS APPLICABLE TO ALL MCCS CONTRACTS

The following standard contracting terms and conditions are incorporated and shall become a part of any final contract that will be awarded by any college or other operating unit of the Maine Community College System (collectively "MCCS"). These terms and conditions derive from the public nature and limited resources of the MCCS. **MCCS DOES NOT AGREE TO:**

1. Provide any defense, hold harmless or indemnity;
2. Waive any statutory or constitutional immunity;
3. Apply the law of a state other than Maine;
4. Procure types or amounts of insurance beyond those MCCS already maintains or waive any rights of subrogation;
5. Add any entity as an additional insured to MCCS policies of insurance;
6. Pay attorneys' fees; costs, including collection costs; expenses or liquidated damages;
7. Promise confidentiality in a manner contrary to Maine's Freedom of Access Act;
8. Permit an entity to change unilaterally any term or condition once the contract is signed;
9. Automatic renewals for term(s) greater than month-to-month;
10. Limitations on MCCS' recovery of lawful damages incurred as a result of breach of the contract;
11. Limitation of the time period under which claims can be made or actions brought arising from the contract;
12. Vendor's terms prevailing over MCCS' standard terms and conditions, including addenda; and
13. Unilateral modifications to the contract by the vendor.

BY SUBMITTING A RESPONSE TO A REQUEST FOR PROPOSAL, BID OR OTHER OFFER TO DO BUSINESS WITH MCCS, YOUR ENTITY UNDERSTANDS AND AGREES THAT:

1. The above standard terms and conditions are thereby incorporated into any agreement entered into between MCCS and your entity; that such terms and condition shall control in the event of any conflict with such agreement; and that your entity will not propose or demand any contrary terms;

2. The above standard terms and conditions will govern the interpretation of such agreement notwithstanding the expression of any other term and/or condition to the contrary;

3. Your entity will not propose to any college or other operating unit of the MCCS any contractual documents of any kind that are not in at least 11-point black font on a white background and completely contained in one Word or PDF document, and that any references to terms and conditions, privacy policies or any other conditions referenced outside of the contract will not apply; and

4. Your entity will identify at the time of submission which, if any, portion or your submitted materials are entitled to "trade secret" exemption from disclosure under Maine's Freedom of Access Act; that failure to so identify will authorize MCCS to conclude that no portions are so exempt; and that your entity will defend, indemnify and hold harmless MCCS in any and all legal actions that seek to compel MCCS to disclose under Maine's Freedom of Access Act some or all of your submitted materials and/or contract, if any, executed between MCCS and your entity.