

1. Could the University provide an extension for submitting response to the proposal?
 - Yes, we will extend the date for proposals until end of the day, January 18, 2023. The revised timeline dates have been published in Addendum #4 to the RFP.
2. Could Re-seller provide response to this RFP?
 - Yes
3. Please describe the scope for implementation services of the new EDR platform that should be included in the proposal response?
 - The scope includes planning the implementation, providing support during implementation until handoff. We have technical resources for deployment and implementation but will need vendor planning and support.
4. Please describe the scope for operating/maintaining the new EDR platform post implementation that should be included in the proposal response?
 - We have technical resources for first level user support but will require vendor support for major issues. Please describe your support options.
5. What is the current EDR solution in place? Is it a SaaS/ on-prem type of solution?
 - There isn't a current EDR platform. This is a replacement to AV
6. What is the current stack of Network and Security Device(s) client having?
 - We do not disclose this information publicly. The majority of our equipment is from well-known vendors, and we do not have any highly specialized or complicated components.
7. In scenario of implementation/migration, what is the anticipated time for completion?
 - That has not been determined. We would ask our respondents to provide estimates.
8. How many endpoints are managed in the current state and expectation of future state? (Endpoints include Servers, Workstations & Mobile devices) (Kindly share the operating systems segregation).
 - Windows Servers 319, Windows Desktops 3691, Linux Servers 71, Linux Desktops 5, Mac Desktops 517
9. In current state, how are the Agents upgrade performed? (Via existing console or external deployment software's like SCCM)
 - SCCM, Ivanti, some patching might be done via Lansweeper

10. How is the current Policy Management structured?

- Currently it is decentralized, but we will move to centralized policy management with EDR.

11. What's the frequency of scans and hosts scanned in each window of current state and expectation of future state?

- We would like our respondents to provide advice on best practices

12. Are there any Integration plans for future or during Implementations? Or are we already integrated with various platform (E.g., SIEM, ServiceNow, etc.)

- We would be interested in possible integrations with Aruba Clearpass, Fortinet Firewalls, or Fortinet VPNs. Also any SIEM integration capability.

13. What is EDR Logs retention policy defined in current state?

- We would like our respondents to provide advice on best practices

14. In scenario of Operationalizing EDR, what are the expectations from MSS vendor and activity scope?

- In the case we contract with an MSS vendor, we would minimally expect the vendor to provide alert filtering to our endpoint and security team to allow us to focus on the critical notifications.

15. How is the EDR team support structured in the current scope or expectation for future? (e.g., Support Hours, No. of Team members)

- This will be a new team

16. Is there an escalation matrix defined in the current state?

- No

17. Does the current state have playbooks/SOP's defined for operational activities?

- No

18. What is the number of Apple iOS devices (iPads, iPhones) that need to be supported?

- We do not have plans for IOS or Android devices at this time, but we are interested in the vendor's capabilities in this space.

19. Are all Windows servers supported and under warranty?

- Yes

20. What is the total number of Linux servers by Operating System? (i.e. RedHat, CentOS, Ubuntu)

- There are a total of 71 Linux servers. We do not have the breakdown by OS

21. Are all Linux servers supported and under warranty?

- Yes

22. What are you currently using to manage your endpoints? i.e. deploying updates, applications, policies, etc.

SCCM, Ivanti, some patching might be done via Lansweeper

23. Does VSC have MS licensing (i.e. In-Tune) for its endpoints?

- Yes

24. Could you please clarify the type of reference required for the RFP?

- Customer references

25. Should the references be those of the Vendor, Channel Partner or both together?

- Customer references

26. In the context of requirement 3.1.16 ("Ability to fully protect and support mobile endpoints that are disconnected from colleges' networks for an extended period."), does "mobile" mean Android/iOS mobile devices? Or is this requirement simply to address portable workstations and laptops running the desktop operating systems specified in requirement 3.1.8?

- This is to address portable workstations and laptops. We do not have plans for IOS or Android devices at this time, but we are interested in the vendor's capabilities in this space.

27. What is the number of users for Vermont State Colleges (VSC)? The RFP mentions 4,500 endpoints. Does it relate to the number of users as well?

- We estimate 3100 end users

28. Does VSC have a breakdown of endpoints by device type and operating system?

- Windows Servers 319, Windows Desktops 3691, Linux Servers 71, Linux Desktops 5, Mac Desktops 517

29. Is VSC looking to manage the solution internally or are you looking for help with managed services/professional services for 24x7x365 monitoring and alerting and response support?

- We would manage the solution internally but welcome your support options.

30. What are the security tools currently deployed at VSC?

- We cannot disclose this information. We have commonly used applications

31. Do you have a network diagram/topology that can be shared?

- We do not share this information publically

32. Number of VSC that house the endpoints that need to be protected?

- 1

33. Are all the endpoints and users located within the USA?

- Yes, but some users travel outside of the US with their laptops.

34. Is there an incumbent solution provider in place currently?

- No

35. Please list other agents installed on the endpoints to confirm compatibility with our solution options?

- We do not share this information publicly. We do not have any highly specialized or complicated agents.

36. Is there an allocated and approved budget for this project?

- Yes

37. Please describe the current solution?

- Various Antivirus solutions. We are looking to combine into a single platform.

38. Are there any critical systems that this solution will need to integrate with? i.e. a SIEM solution, PowerBI analytics platform, etc.

- We would be interested in possible integrations with Aruba Clearpass, Fortinet Firewalls, or Fortinet VPNs. Also any SIEM integration capability.

39. Will you be implementing this solution with internal resources or will you require assistance to deploy?

- We have technical resources for deployment and implementation but will need vendor support.

40. Do you need a rollback capability?

- No

41. What is your timeline for making a decision?

- The timeline has been adjusted. Please see Addendum #4 for the new timeline.

42. What is your timeline for completion of the project?

- TBD

43. Did any specific event create the need for this project?

- N/A

44. Please describe any specific use cases you require.

- N/A

45. Describe the structure/expertise/experience of your current security team?

- We do not share this information publicly

46. As part of an endpoint security solution, what feature/functions are a top priority?

- Please see the RFP

47. What is your current solution for 3rd party access control?

- We do not share this information publicly

48. What is your current visibility into east-west traffic?

- We do not share this information publicly

49. "Which legacy platforms are you still supporting? What critical applications are running on your legacy platforms?"

- We do not share this information publicly

50. Do you have a data retention requirement for event data and logs?

- We would like access to a minimum of 30 days of log history

51. Do you follow a specific security framework currently?

- We do not share this information publicly

52. Do you have any specific compliance requirements? Ex: PCI, HIPPA, FEDRAMP, CMMC, etc.

- We do not share this information publicly

53. Describe your network segmentation.

- We do not share this information publicly

54. Will your team require training for the proposed solution?

- Yes

55. Will you require a proof of concept / proof of value?

- No

56. Please describe you requirements/expectations for forensic response from the solution or provider.

- We would be interested to hear about the vendors capabilities.

57. What are the most important expectations you have for a security partner?

- N/A

58. What are your top requirements for the solution provider you choose which will set them apart from other bidders?

- N/A