SHARED SERVICES CANADA

Request for Information
for the Procurement Process for
Advanced Endpoint Security and Software License Management Consultation

Request for Information No.	15-35615	Date	February 24, 2016
Issuing Office	Shared Services Canada 180 Kent Street, 13th Floor, 13-125 Ottawa, Ontario K1P 0B6		
Contracting Authority (The Contracting Authority is SSC's representative for all questions and comments about this document.)	Name	Betty-Jane Horton	
	Telephone No.	613-301-5643	
	Email Address	betty-jane.horton@canada.ca	
	Postal Address	Shared Services Canada 180 Kent Street, 13th Floor, 13-102 Ottawa, Ontario K1P 0B6	
Closing Date and Time	March 10, 2016, 2:00 p.m.		
Time Zone	Eastern Standard Time (EST)		
Destination of Goods/Services	Not applicable – Request for Information Only		
Email Address for Submitting your Response by the Closing Date	betty-jane.horton@canada.ca		

Contents

SHARED SERVICES CANADA

Request for Information
for the Procurement Process for
Advanced Endpoint Security and Software License Management Consultation

1. General Information

1.1 Introduction

1) **Phase 1 of Procurement Process**: This Request for Information (RFI) is the first phase of a procurement process by Shared Services Canada (SSC) for Advanced Endpoint Security and Software License Management Consultation (the "**Project**"). Suppliers are invited to submit responses to assist Canada in refining its requirements for the Project. Suppliers are not required to submit a response to this RFI in order to participate in any later phases of the procurement process for the Project.

2) **RFI Phase is not a Bid Solicitation**: This RFI is not a solicitation of bids or tenders. No contract will be awarded as a result of the activities undertaken during this RFI. Canada reserves the right to cancel any of the preliminary requirements described as part of the Project at any time during the RFI or any other phase of the procurement process. Given that the RFI process and any related procurement activity may be partially or completely cancelled by Canada, it may not result in any subsequent procurement processes.

3) **Response Costs**: SSC will not reimburse any supplier or any of its representatives for any overhead or expenses incurred in participating in or responding to any part of the RFI phase. Suppliers are also responsible for carrying out their own independent research, due diligence and investigations (including seeking independent advice) that they consider necessary or advisable in connection with their participation in the RFI process and any future procurement process.

1.2 Overview of the Project

1) **Overview of Project**:

The Center for Internet Security (CIS), a non-profit organization focused on enhancing the cybersecurity readiness and response of public and private sector, in partnership with the SANS Institute, one of the most trusted providers of information security training in the world, has recently published the latest version of the top 20 critical security controls (CSCs)[1]. The Communication Security Establishment (CSE) recognizes these CSCs as being an "excellent considerations for generic networks" [2]. The following controls are at the very top of that list:

a) Inventory of authorized and unauthorized devices (CSC 1) ;
b) Inventory of authorized and unauthorized software (CSC 2);
c) Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers (CSC 3); and
d) Continuous vulnerability assessment and remediation (CSC 4).

[1] https://www.sans.org/critical-security-controls
[2] https://www.cse-cst.gc.ca/en/node/1297/html/25231

Shared Services Canada (SSC) and the Department of National Defence (DND) have investigated how these controls have been implemented within the departments. Although several initiatives and projects are underway to improve SSC and DND/CAF network security, the CSCs listed previously are currently only partially implemented across the enterprise.

a. Objective for the Project

Through this RFI, SSC and DND are looking at gathering information on advanced endpoint security and system management solutions that could potentially help in meeting those CSCs and fill the gaps that currently exist. The proposed solutions should also address the secure configuration of network devices CSC (CSC 11), endpoint threat detection and remediation and remote forensics analysis of devices.

Finally, the Departments are also trying to improve the efficiency of license management related activities. To that end, SSC and DND are seeking solutions that could automate the management of licenses across the enterprise and gather statistic on software usage.

b. Purpose of this Request for Information

The purpose of this RFI is to receive feedback, ideas and suggestions from suppliers on advanced endpoint security and license management solutions. The main objectives of this RFI are to:

a) Confirm availability of and gather information on advanced endpoint security and system management solutions;
b) Confirm availability of and gather information on license management solutions;
c) Identify important technical aspects that must be considered; and
d) Estimate the level of effort and the development time frame required to implement proposed solutions.

Given the scope of this RFI, there is a strong possibility that a single solution will not be able to meet all these requirements. Therefore, suppliers are encouraged to submit their proposal even if their solution can only meet some of the requirements.

Suppliers are asked to specify which of the following functionalities they would like to submit information on:

a) IT Asset Management/Configuration Management;
b) Software License Management;
c) Software and Patch Management;
d) Detection/Incident Response; and
e) Remote Device Forensics.

Note: In Section 4 of this document, all suppliers should answer the *General Questions* section. Suppliers should also answer *Functionality Specific Questions* related to the categories selected above.

This document remains a work in progress and respondents should not assume that new clauses or requirements will not be added to any bid solicitation that is ultimately published by DND, SSC or other Government of Canada departments/agencies. Nor should respondents assume that none of the clauses or requirements will be deleted or revised. Comments regarding any aspect of the draft document are welcome. If respondents feel a question or key area has been missed, we welcome comments or information to this fact in their response.

2) **Scope of Anticipated Procurement:**

a. **Potential Client Users**: This RFI is being issued by SSC. It is intended that the contract resulting from any subsequent solicitation would be used by SSC to provide shared services to one or more of its clients. SSC's clients include SSC itself, those government institutions for which SSC's services are mandatory at any point during the life of any resulting instrument(s), and those other organizations for which SSC's services are optional at any point during the life of any resulting instrument(s) and that choose to use those services from time to time. Any subsequent procurement process will not preclude SSC from using another method of supply for any of its clients with the same or similar needs, unless a subsequent solicitation for this Project expressly indicates otherwise.

b. **Number of Contracts**: Canada is currently contemplating the award more than one contract.

c. **Term of any Resulting Contract**: Canada has not yet determined the contract period of whether it will include option years.

3) **National Security Exception**: Canada has invoked the National Security Exception in respect of this requirement and, as a result, none of the trade agreements apply to this requirement.

1.3 Submitting Questions

1) Questions about this RFI can be submitted to the Contracting Authority at the email address identified on the cover page. These questions should be submitted within the following question period. Questions received after this period may not be answered.

Question Period: Questions should be submitted no later March 10, 2:00 p.m.

2) Respondents should reference as accurately as possible the numbered item of the RFI to which the question relates. Care should be taken by Respondents to explain each question in sufficient detail in order to allow Canada to provide an accurate answer.

3) To ensure the consistency and quality of information provided to suppliers, significant questions received and the answers will be posted on the Government Electronic Tendering Service (GETS) as an amendment to this RFI.

2. Supplier Responses

2.1 Submitting a Response

1) **Time and Place for Submission of Responses**: Suppliers interested in providing a response should submit it by email to the Contracting Authority at the email address for submitting a response identified on the cover page by the closing date and time identified on the cover page of this document.

2) **Responsibility for Timely Delivery**: Each supplier is solely responsible for ensuring its response is delivered on time to the correct email address.

3) **Identification of Response**: Each supplier should ensure that its name and address, the solicitation number, and the closing date are included in the response in a prominent location. The supplier should also identify a representative whom Canada may contact about the response, including the person's name, title, address, telephone number and email address.

4) **Nature and Format of Responses Requested:** Respondents are requested to provide their comments, suggestions, concerns and, where applicable, alternative recommendations regarding how the requirements or objectives described in this RFI could be satisfied. Respondents should explain any assumptions they make in their responses.

a. **Cover page**: If the response includes multiple volumes, respondents are requested to indicate on the front cover page of each volume the title of the response, the solicitation number, the volume number and the full legal name of the respondent.

b. **Title page**: The first page of each volume of the response, after the cover page, should be the title page, which should contain:

a) The title of the respondent's response and the volume number;
b) The name and address of the respondent;
c) The name, address and telephone number of the respondent's contact;
d) The date; and
e) The RFI number.

c. **Numbering system:** Respondents are requested to prepare their response using a numbering system corresponding to the one in this RFI. All references to descriptive material, technical manuals and brochures included as part of the response should be referenced accordingly.

d. **Number of copies**: DND and SSC requests that respondents submit electronically by email 1 copy of their responses to each organization.

If a supplier considers any portion of its response to be proprietary or confidential, the supplier should clearly mark those portions of the response as proprietary or confidential. Canada will treat the responses in accordance with the *Access to Information Act* and any other laws that apply.

3. Canada's Review of Responses

3.1 Review of Responses

Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify its procurement strategy. Canada will review all responses received by the RFI closing date and time. Canada may, in its discretion, review responses received after the RFI closing date and time.

3.2 Review Team

A review team composed of representatives of Canada will review and consider the responses. Canada may hire any independent consultant(s), or use any Government resource(s), to review any response. Not all members of the review team will necessarily participate in all aspects of the review process.

3.3 Follow-up Activity

Canada may, in its discretion, contact any suppliers to follow up with additional questions or for clarification of any aspect of a response. Canada's follow-up may involve a request for a further written response or for a meeting with representatives of Canada.

3.4 One-on-One Meetings

DND, SSC and other Government of Canada departments/agencies may, in their sole discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a response during one-on-one meetings.

4. Information Requested by Canada

4.1 Questions for Industry

4.1.1 SSC Environment

SSC is responsible for networks spanning 43 Departments. While they currently remain separate, SSC is working on consolidating these network environments. When providing their answers, suppliers are asked to consider how their solution would integrate into an environment with the following characteristics/requirements:

1) Many complex network infrastructures with various enclaves and IT security zones requiring the use of zone interface points and information exchange gateways needing to provide command and control both to the local network support team and to a central system.

2) Multiple tenants/networks that require easy identification of assets by tenant/network (which may have overlapping IP addresses) and provide access control separation between tenants (e.g. Execute a command only on particular tenants rather than the enterprise.

3) Separate networks that are consolidating to one network.

4) Large network infrastructures (over 450,000 clients).

5) Both virtualized and non-virtualized environment.

6) High latency and low bandwidth WAN connections between specific sites.

7) Periodic direct connections to GC intranet (e.g. Reporting may need to be stored until next time the end device is connected directly to GC network - including a VPN or collected though Internet rather than GC network).

8) Use of commercial grade and limited military grade cryptographic devices at the network layer.

9) Various operating systems (servers and clients) including MS Windows for desktops, mobile and servers, Mac OS for desktops and Linux for desktops and servers.

10) Various forms of network (layer 2) port control which include, but not limited to, 802.1x and MAC filtering.

4.1.2 DND Environment

When providing their answers, suppliers are asked to consider how their solution would integrate into an environment with the following characteristics:

1) Complex network infrastructures with various enclaves and IT security zones requiring the use of several zone interface points and information exchange gateways.

2) Large network infrastructures (over 100,000 clients on the main unclassified network and over 8,000 clients on the main classified network).

3) Both virtualized and non-virtualized environment.

4) High latency and low bandwidth WAN connections between specific sites (episodic networks deployed across the globe).

5) Extensive use of commercial grade and military grade cryptographic devices at the network layer.

6) Various operating systems (servers and clients) including MS Windows for desktops, mobile and servers and Linux for desktops and servers.

7) Various forms of network (layer 2) port control which include, but not limited to, 802.1x and MAC filtering.

8) Shared responsibility for the IT environment between SSC (e.g. network and server infrastructure) and DND (e.g. applications and endpoints).

Note: All suppliers should answer the *General Questions* section. Suppliers should then only answer *Functionality Specific Questions* related to the categories they would like to submit information on.

4.2 General Questions

4.2.1 Architecture/Infrastructure Questions

1) Does your solution provide agentless and/or agent-based solution alternatives?

2) If your solution is agent-based, is the computation of tasks (e.g. queries, VA, etc.) performed on the host or does the data need to be pulled centrally for computation?

3) Does your solution support other agents (e.g. Mandiant Intelligence Response, GRR Rapid Response, etc.)?

4) What are the hardware requirements to integrate your solution to an existing network (provide basic system architecture overview including required servers, networks and storage)?

5) What are the software/technical requirements to integrate your solution to an existing network?

6) Does your solution integrate with LDAP (e.g. Active Directory) for authentication?

7) Does your solution provide distributed management and hierarchical monitoring capabilities (e.g. different departments can manage their own resources but monitoring can be done centrally)?

8) Does your solution support a multi-tenant/multi-network environment where searches and actions taken need to respect identification of and separation between tenants (e.g. actions cause change on 3 specific tenants or action causes change on all except 3 specific tenants, reports per tenant, etc.)?

9) Can your solution be deployed on networks with different IT security zones and caveats (explain how – e.g. is a server required in each zone)?

10) How does your solution address scalability issues in large deployment (over 500,000 clients) to reduce the impact on the network (e.g. bandwidth, availability)? What is the estimated network capacity requirement on a per end-point basis?

11) Does your solution support out of band (i.e. no available ip network path) functionalities (e.g. scans or patch deployment)?

12) Does your solution enable out of band extraction and exploitation of information (e.g. logs, security metrics)?

13) How does your solution maintain currency of the information gathered from the systems and how current is it (e.g. daily, on demand, etc.)?

14) Does your software provide a feature rich API that allows integration with other third-party systems: Security Incident and Event Management (SIEM)?

    a. Log analytic tools?
    b. Help desk ticketing systems?
    c. Asset management tool?
    d. Configuration management tool?
    e. Incident management tool?
    f. Vulnerability scanning tool?
    g. Others (specify)?

4.2.2 Security/Certification and Accreditation Questions

15) Has your solution been certified/accredited by NATO members, trusted governmental organizations or large private corporations (banks or others)? If so, which certifications/accreditations have been achieved?

16) What credentials are required to perform actions/scans on an entire network, what mechanisms are in place to transfer those credentials across the network and how are those credentials protected?

17) How are communications between the central authority and the devices protected? Does your solution support CSE approve key management technologies and processes?

18) If encryption keys are employed, how are the keys safeguarded on the hosts?

19) Does your solution provide granular role-based access control and regulate permissions based on the user's responsibility?

20) Does your solution provide auditing and logging features? Where are the logs stored (locally, centrally, both)?

21) Does your solution include any additional security features (list them)?

4.2.3 Customization Questions

22) What report generation capabilities does your solution provide? What format(s) are supported for these reports (e.g. PDF, RTF, MS Word, etc.)? Can these reports be customized?

23) What dashboard capabilities does your solution provide? How customizable is the dashboard? Can the dashboard include input from other solutions from other manufacturers?

24) Does your solution allow users to build custom queries and search for specific information? What are the languages and the mechanisms used (e.g. internet search engine format, regular expressions, etc.)?

25) Can your solution make use of custom scripts to automate some of the solution functionalities? What language does it use or support?

26) Does your solution include analytics and trending analysis capabilities (provide details)?

27) What languages/regional support does your solution provide (e.g. FR-CA, EN-CA, etc.)?

4.2.4 Vendor support Questions

28) How frequent are solution updates or new capabilities released and how long is support maintained for previous versions?

29) How frequently are patches and/or service packs for your solution released and what mechanism is used for patching/updates?

30) What is the process for updating/patching installations with no direct Internet connectivity?

31) Will the vendor of your solution authorize configuration testing in a GC-hosted lab environment?

32) What is the licensing model for your solution (e.g. subscription based, perpetual with yearly fees, etc.)?

33) What is the solution support model (e.g. direct to the OEM or through a third party)?

4.3 Functionality Specific Questions

4.3.1 IT Asset Management/Configuration Management Questions

34) Can your solution perform asset discovery of the following devices on a network?
    a. Network equipment (e.g. routers, switches, firewalls, VPN gateways etc.)?
    b. Computer hosts and servers?
    c. Printers/multi-function devices?
    d. Wireless Access Points (WAP)?
    e. Video Teleconferencing (VTC)?
    f. Desktops and thin clients (including directly connected devices like printers, USB storage devices, wireless card/sticks, etc.)?
    g. Hypervisors (e.g. VMware, IBM pSeries – specify which ones)?
    h. Virtual machines (e.g. Windows or Linux virtual guest)?
    i. Voice Over IP (VOIP) devices?
    j. Mobile devices? Which ones (e.g. Android, Apple, BlackBerry, Windows, etc.)?
    k. Others (specify)?

35) Can your solution perform asset discovery of the above devices without the use of installed agents using protocols such as ICMP, SNMPv3 and port scans?

36) Does your solution allow for dynamic groupings of discovered assets based on their configuration with the goal of applying specific actions to those assets (e.g. condition-based software installation or condition-based configuration gathering)?

37) Does your solution offer the ability to send alerts when specific events are triggered (e.g. new asset discovered, asset becomes unavailable, network link saturation threshold, etc.)?

38) Does your solution offer the ability to discover connections between network devices?

39) Does your solution offer the ability to graphically/visually display the network topology?

40) Can your solution monitor network device status?

41) Can your solution provide historical data and statistics on hardware usage (e.g. CPU/Memory utilization, disk usage, etc.)? What type of data/statistics can it provide?

42) Can your solution monitor network link utilization on switches, routers, firewalls, etc.?

43) Can your solution monitor configuration information on the following devices:

    a. Network equipment (e.g. routers, switches, firewalls, VPN gateways etc.)?
    b. Computer hosts and servers?
    c. Printers/multi-function devices?
    d. Wireless Access Points (WAP)?
    e. Video Teleconferencing (VTC)?
    f. Desktops and thin clients (including directly connected devices like printers, USB storage devices, wireless card/sticks, etc.)?
    g. Hypervisors (e.g. VMware, IBM pSeries) – specify which ones?
    h. Virtual machines (e.g. Windows or Linux virtual guest)?
    i. Voice Over IP (VOIP) devices?
    j. Mobile devices? Which ones (e.g. Android, Apple, BlackBerry, Windows, etc.)?
    k. Others (specify)?

44) What type of configuration information can be collected for each of the device types identified at the previous question (e.g. for computer host: OS version, patch level, registry settings, etc.; for routers: software version, active interfaces, etc.)?

45) Can custom scripts be deployed with your solution to gather additional configuration information? What language does it use or support?

46) Can your solution integrate and run Security Content Automation Protocol (SCAP) configuration compliance tests?

47) Does your solution provide an API that allows to export and import SCAP queries and results to and from third-party tools?

48) Can you solution provide alerts and remediate configuration deltas discovered on network devices (thus ensuring compliance to a specified configuration baseline)?

49) Can your solution integrate with Open Vulnerability and Assessment Language (OVAL)?

50) Does your solution allow for direct connection to open sources vulnerability and configuration management databases, such as National Vulnerability Database (NVD), Configuration Management Database (CMDB)?

51) Can your solution integrate with systems using Structured Threat Information eXpression (STIX), Trusted Automated Exchange of Indicator Information (TAXII) and Cyber Observable Expression (CybOX) in order to consume and provide cyber threat information (e.g. indicators of compromise)?

52) Does your solution support any existing industry partnerships or alliances that provide added value through integration with other solutions? If so, which partnerships/alliances/ solutions/API?

53) Can your solution integrate with LDAP (e.g. Active Directory) for retrieving additional asset information (e.g. Physical location, assigned user, purpose, etc.).

54) Does your solution include a functionality to integrate data from multiple scans (e.g. comparison across multiple timestamps as well as multiple LANs of the same WAN)?

55) Can scanning rights and permissions be granted based on granular role-based access control?

56) Does your solution offer the ability to export asset information as XML or CSV format?

4.3.2 Software License Management Questions

57) Can your solution provide the following application/software management related information?

    a. List of applications installed on a host/server and workstations including:
        a) Version?
        b) Release?
        c) License keys and IDs used?
        d) Manufacturer/Publisher?

    b. Historical data and statistics on usage (software metering) including:

        a) Install base (number of software instance)?
        b) Installation date?
        c) Last usage date?
        d) Usage within a fixed period of time?

58) Can your tool perform searches and gather information about software using normalized format (e.g. a search for Adobe should also provide results for Adobe Systems, Adobe systems Inc., Adobe Inc., etc.)?

59) Does your solution provide a license management module and automated mechanisms to verify compliance including:

    a. License quantities as contracted?
    b. Overprovisioned (unused) licenses?
    c. Concurrent use of licenses?
    d. Ability to track and manage various complex licensing models (Oracle, IBM, VMware, Microsoft, etc.)?

60) Does your solution support remote license reclamation (the process of reclaiming unused software solution licenses from current license users and reassigning them to others)?

61) Can your solution perform the above license management activities on:

a. Mobile devices? Which ones (e.g. Android, Apple, BlackBerry, Windows, etc.)?
b. Virtual machines?
c. Desktops and thin clients?
d. Servers and hosts?

4.3.3 Software and Patch Management and Deployment Questions

62) Can your solution perform patch and software deployment and installation across a network (explain how patches and software are deployed)?

63) Does your solution allow whitelisting and blacklisting of applications/software on the network?

64) Can your solution perform dynamically-triggered and manually-triggered rollback of previously installed software?

65) Does your solution offer the ability to perform pre- or post-actions to deployment package(s) (e.g. tasks that are part of the software packaging process such as stopping and starting services, copying files to specific locations, notifying users etc.)?

66) Does your solution offer the ability to customize the patching process by defined rules and exceptions and predefined schedules?

67) Does your solution offer patch management and software deployment performance metrics such as number of patches released per month, patch success and failure ratio (per patch), agent health (e.g. 95% healthy – daily measurement), etc.?

68) Does your solution have the capacity to report on relationships/dependencies between applications? What type of relationships (i.e. one-to-one, one-to-many)?

69) Does your solution ensure that date stamps are tied to the time/date the information was scanned/verified and not to the time/date the report was produced?

70) Does your solution offer the ability to deploy desktop or server operating systems to endpoint devices over the network including:

a. Advanced features such as pre-deployment checks of endpoint device requirements and an ability to apply advanced OS deployment logic (e.g. condition-based software installation as part of OS deployment)?

b. Does your solution offer the ability to install basic hardware drivers (e.g. .inf) on desktop and server operating system?

c. Does your solution offer the ability to deploy desktop or server Operating Systems to disconnected endpoint devices via offline media (e.g. USB storage media);

d. Does your solution offer the ability to deploy desktop or server Operating Systems to UEFI systems?

e. Does your solution offer integration to hardware driver management utilities, such as Deploy Expert, ENGL Driver Manager and Big Bang LLC Universal Imaging Utility?

f. Does your solution offer the ability to deploy and manage virtualized software, specifically Microsoft App-V and VMware ThinApp software packages?

71) Can your solution perform the above software and patch management activities on:

a. Mobile devices? Which ones (e.g. Android, Apple, BlackBerry, Windows, etc.)?
b. Virtual machines?
c. Desktops and thin clients?
d. Servers and hosts?

4.3.4 Detection/Incident Response Questions

72) Can your solution provide the following up-to-date inventory information about hosts?

a. Running processes/scripts?
b. Files currently opened by users?
c. Listening network data ports?
d. Established network connections?
e. Registry settings?
f. User account in use?
g. Directly connected devices (e.g. USB)?
h. Event logs information?
i. Others (specify)?

73) Can your solution identify unauthorized and/or previously unknown devices on a network?

74) Can your solution monitor file integrity and provide automated real time alerts when changes to critical executable files occur? Can your solution prevent changes to critical executable files?

75) Can your solution detect and evaluate potential compromise based on indicators such as filenames, file paths, registry settings, IP addresses, network traffic, file hashes or observable suspicious behaviours?

76) Can your solution ingest threat stream data from open-source services (e.g. Virus Total, ThreatStream, McAfee TIE, Yara, OpenIOC, etc.) and automatically check in the infrastructure for presence of those indicators?

77) What remote incident response management functionalities does your solution provide? (e.g. remotely kill processes, shut down services or ports, change registry settings, etc.)?

78) Can your solution send notifications to users on endpoint devices? Is the language of these notifications selectable? Can the notifications be customized?

79) What correlation capabilities does your solution have for detecting threats and incidents?

80) What coordination capabilities does your solution have for responding to threats (e.g. once a malicious file is found on one system, can it quickly deal with it on all systems in the enterprise, including blocking further copies of the file from being saved and/or executed)?

81) What methods does your solution have to prioritize and bring potential threats to the attention of security staff?

82) Does your solution have any form of case management where records can be retained about incidents and resolutions (e.g. include a report from an analyst as to why they took certain response actions to address an incident)?

4.3.5 Remote Device Forensics Questions

83) Can your solution record and provide historical data on the following endpoint activities and for what time period?

a. Files accessed?
b. Files created?
c. Network connections established?
d. Processes/scripts ran?
e. Applications installed?
f. Applications/commands/scripts used?
g. User accounts used?
h. Event logs?
i. Internet browser usage?
j. Others (specify)?

84) Does your solution allow remote, live acquisition of memory?

85) Does your solution allow remote, live acquisition of forensics artifacts (e.g. retrieving suspicious files for inspection)?

86) How is the integrity of these artifacts preserved during acquisition and/or file transfer?

87) How does your solution allow for offline and real-time analysis of this artifact? Must it be done from a central location or can this be performed through some remote interface?