NCIA/ACQ/2016/1459

05 August 2016

Market Survey Request for Information

Enhanced Endpoint Protection Solution

NCI Agency Ref: MS-CO-14325-CS

NCI Agency is seeking information from Nations and their Industry regarding the availability of Commercial-Off-The-Shelf (COTS) products to meet the requirements of an enhanced endpoint protection solution containing anti-malware, intrusion detection and prevention, application control, device control, data loss prevention, file and disk encryption and mobile devices management capabilities

NCI Agency Senior Contracting Officer: Mr Peter Kowalski

E-mail: peter.kowalski@ncia.nato.int

To: See Distribution List

Subject: **NCI Agency Market Survey Request**

Endpoint Protection Solutions

1. NCI Agency requests the assistance of the Nations and their Industry to identify potential COTS products available to meet the requirement for an enhanced endpoint protection solution. This Market Survey is being issued to identify potential solutions and possible suppliers.

2. In addition to the firms noted in Annex C of this letter, the broadest possible dissemination by Nations of this Market Survey Request to their qualified and interested industrial base above and beyond the Annex C list of firms is requested.

3. A summary of this emerging requirement is set forth in the Annex A attached hereto. Respondents are requested to reply via the questionnaire at Annex B. Other supporting information and documentation (technical data sheets, marketing

brochures, catalogue price lists, descriptions of existing installations, etc.) are also desired.

4. The NCI Agency reference for this Market Survey Request is NCIA/ACQ/2016/1459, and all correspondence and submissions concerning this matter should reference this number.

5. Responses may be issued to NCI Agency directly from Nations or from their Industry. Respondents are invited to carefully review the requirements in Annex A.

6. Responses shall in all cases include the name of the firm, telephone number, e-mail address, designated Point of Contact, and a NATO UNCLASSIFIED description of the capability available and its functionalities. This shall include any restrictions (e.g. export controls) for direct procurement of the various capabilities by NCI Agency. Non-binding product pricing information is also requested as called out in Annex B.

7. Responses are due back to NCI Agency no later than **close of business 3 October 2016**.

8. Please send all responses either via post/courier or email to the following NCI Agency contact:

For Attention Of:	Mr. Peter Kowalski Senior Contracting Officer – DACQ/ASG Email: Peter.Kowalski@ncia.nato.int
Postal address:	NATO Communications and Information Agency Boulevard Leopold III 1110 Brussels Belgium
Courier delivery address (e.g. DHL or FEDEX):	NATO Communications and Information Agency Bourgetlaan 140 1140 Evere Belgium

9. Product demonstrations or face-to-face briefings/meetings with industry are not foreseen during this initial stage. Respondents are requested to await further

instructions after their submissions and are requested not to contact any NCI Agency staff directly other than the POC identified above in Para 8.

10. Any response to this request shall be provided on a voluntary basis. Negative responses shall not prejudice or cause the exclusion of companies from any future procurement that may arise from this Market Survey. Responses to this request, and any information provided within the context of this survey, including but not limited to pricing, quantities, capabilities, functionalities and requirements will be considered as indicative and informational only and will not be construed as binding on NATO for any future acquisition.

11. The NCI Agency is not liable for any expenses incurred by firms in conjunction with their responses to this Market Survey and this Survey shall not be regarded as a commitment of any kind concerning future procurement of the items described.

12. Your assistance in this Market Survey request is greatly appreciated.

FOR THE GENERAL MANAGER:

L. T. Herway
Chief of Contracts

Attachment(s):

- Annex A – Market Survey Requirements
- Annex B – Market Survey Questionnaire
- Annex C – Market Survey Industrial Recipients

Distribution List for Market Survey Request for Information – Enhanced Endpoint Protection Solution

Potential Industrial Suppliers	1

NATO Delegations (Attn: Infrastructure Adviser):

Albania	1
Belgium	1
Bulgaria	1
Canada	1
Croatia	1
Czech Republic	1
Denmark	1
Estonia	1
France	1
Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
The Netherlands	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Turkey	1
United Kingdom	1
United States	1

Belgian Ministry of Economic Affairs	1

Embassies in Brussels (Attn: Commercial Attaché):

Albania	1
Bulgaria	1
Canada	1
Croatia	1
Czech Republic	1
Denmark	1

Estonia	1
France	1
Germany	1
Greece	1
Hungary	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
The Netherlands	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Turkey	1
United Kingdom	1
United States (electronic copy to brussels.office.box@mail.doc.gov)	1

Distribution for information

NATO HQ

NATO Office of Resources
Management and Implementation Branch – Attn: Deputy Branch Chief 1

NATO Office of Security
Policy Oversight Branch/CIS Security Section Head (Mr. F.A. Micevski Scharf) 1

NATO HQ C3 Staff
Attn: Mr. Omer Hasret 1

Strategic Commands

HQ SACT Attn: R&D Contracting Office	1
SHAPE J2X CIS Security Section Head (LTC. Stefan Weiss)	1

NCI Agency –Internal Distribution

ACQ Director of Acquisition – Mr P Scaruppe	1
ACQ Deputy Director of Acquisition – Ms A Szydelko	1
ACQ Contract Award Board Administrator – Ms M-L Le Bourlot	1
ACQ Chief of Contracts – Mr L.T. Herway	1
ACQ Principal Contracting Officer - Ms T Pezzi	1
ACQ Senior Contracting Officer Mr P Kowalski	1
Cyber Security/Chief - Mr. I West	1

Cyber Security/Capability Development Branch Head (Mr. Frederic Jordan)	1
Cyber Security/Compliance and Audit Branch Head (Cdr. Askin Ercetin)	1
Cyber Security/Operations Branch Head (Col. Orhan Akdogan)	1
Cyber Security/Project Support Branch Head	1
Core Enterprise Services/ Chief (Mr. Pierre Pradier)	1
Core Enterprise Services/ ITM Program Manager (Mr. Frank Mikla)	1
Registry (for distribution)	1

NCI Agency NATEX

Belgium	1
Denmark	1
France	1
Germany	1
Greece	1
Italy	1
Netherlands	1
Norway	1
Poland	1
Spain	1
Turkey	1
United Kingdom	1
United States	1

NCIA/ACQ/2016/1459
Annex A

Request for Information
"Enhanced Endpoint Protection Solution"
Market Survey

Annex A – Requirements

NCI Agency conducts this survey in order to identify available endpoint protection solutions on the market that fulfil the requirements presented below.

The objective of this effort is to enhance the security of NATO networks by improving/replacing the products, technologies and mechanisms used today for securing NATO servers, workstations, laptops and mobile equipment.

NCI Agency foresees the Enhanced Endpoint Protection Solution (EEPS) to fulfil most of the following requirements:

Functional Requirements

1. Anti-malware features
    - 1.1. Provides protection against malicious software (malware), viruses, 1rojans, worms, spyware, ransomware, adware, unwanted programs, spam, and rootkits;
    - 1.2. Ensures high malware detection effectiveness
    - 1.3. Has a minimum system impact
    - 1.4. Allows the customer to define malware signatures, IOCs, potentially unwanted programs (PUP) and policies
    - 1.5. Allows the usage of regular expressions in signatures and policies definitions
    - 1.6. Uses file reputation databases (both local and cloud-based)
    - 1.7. Performs analysis based on files' real content (not only by extension)
    - 1.8. Uses application containment (sandboxing) for host protection
    - 1.9. Performs on-access, on-demand and scheduled scans
    - 1.10. Allows configuration of local or centralized quarantine, for malware containment
    - 1.11. Uses signature-based malware detection
    - 1.12. Uses heuristic (behavioural) malware detection
    - 1.13. Uses algorithmic techniques (e.g. machine learning) and computational methods to detect unknown malware
    - 1.14. Maximizes heuristic engine effectiveness (reduces both the false negatives and false positives)

1.15. Provides configurable automated remediation: kill processes, quarantine threats, malware removal, roll back changes done by malware (based on recorded behaviour)

1.16. Protects against unknown (“zero-day”) attacks that attempt to exploit undiscovered and unpatched holes (or vulnerabilities) in the applications or in the operating systems

1.17. Uses honeypots to provide early warnings of lateral attacks

1.18. Facilitates enterprise-wide malware hunt (in memory and on disk) based on suspicious objects, OpenIOC or Yara rules

1.19. Provides visibility for incident and forensic investigations to determine when, where and how the initial infection occurred, what happened after the infection started and what other systems were infected (records endpoint activity)

1.20. Provides APIs to import and export IOCs using common, documented formats

1.21. Protects against web browser exploits for IE, Firefox, Chrome, Safari

1.22. Protects against attacks against email clients (Outlook), webmail and instant messaging (Skype)

1.23. Enforces web browsing policies by authorizing or blocking website access

1.24. Provides intuitive security ratings and warnings for the web users, to stay safe as they search, browse and perform online transactions

1.25. Checks URL links embedded in e-mail and instant messages and warns users before they click on the links about the web sites reputation

1.26. Scans inbound and outbound emails for infected attachments, malicious content and URLs

1.27. Provides reputation and antispam protection using both predefined and customised web sites categories

1.28. Uses sandboxes for automated/manual malware inspection

1.29. Allows automated sandbox analysis for the email attachments and the files (local or downloaded/uploaded from/to internet), based on multiple, configurable criteria (file type, sender/destination, etc.)

1.30. Prevents antimalware protection for being disabled/uninstalled (tamper protection)

2. Host Intrusion Detection/Prevention (HIPS) features

2.1. Filters inbound and outbound access, dynamically by applications, IP addresses, ports, protocols (TCP,UDP) and states (statefull firewall)

2.2. Uses malware signatures to detect/prevent against intrusions

2.3. Uses heuristic (behavioural) methods to detect/prevent against intrusions

2.4. Uses algorithmic techniques (e.g. machine learning) and computational methods to detect/prevent intrusions

2.5. Provides vulnerability shielding anti-exploit protection against common attacked software (Windows, Java, Acrobat Reader, Flash, Internet Explorer etc.)

2.6. Works in blocking mode (IPS) or in detection and logging mode (IDS)

2.7. Monitors in memory processes' integrity

2.8. Monitors files and registry integrity and detects unauthorized changes

2.9. Detects OS and applications vulnerabilities and missing patches

2.10. Conducts compliancy assessments with the ability to isolate a managed system that does not meet predefined requirements

2.11. Prevents security protection from being disabled (tamper protection)

2.12. Provides start-up protection by blocking communication during host start-up until the security policy is fully enforced

3. Application control

3.1. Restricts execution to known good applications (white listing)

3.2. Restricts execution of known bad applications (black listing)

3.3. Allows default-deny application control policy

3.4. Provides full application attestation, i.e. classifies the entire application and process inventory into bad, good and unknown; accelerates the classification of the unknown objects into good or bad

3.5. Blocks unauthorized executables using multiple, flexible criteria: file hash, signer certificate (Authenticode) fields, path, regular expressions

3.6. Supports trusted sources of change

3.7. Uses behavioural monitoring of application code

3.8. Uses online and offline application reputation database

3.9. Prevents application control from being disabled (tamper protection)

4. Port and device control

4.1. Prevents loss of sensitive data by restricting the use of removable media

4.2. Blocks or allows (in read-only and read-write mode) the following types of storage devices:

- removable storage devices (for example, USB flash drives, PC Card readers, and external hard disk drives)
- optical media drives (CD-ROM/DVD/Blu-ray drives)
- floppy disk drives

- secure removable storage devices (for example, hardware-encrypted USB flash drives)

4.3. Blocks or allows the following types of network devices:

- modems (fixed phone lines, GSM, GPRS, 3G)
- wireless (Wi-Fi interfaces, 802.11 standard)

4.4. Allows disabling wireless or modem network adapters when the computer is connected to a physical network (typically through an Ethernet connection) and automatically enabling the wireless or modem network adapters when computer is disconnected from the physical network

4.5. Blocks or allows the short range communication devices having the following interfaces:

- Bluetooth interfaces
- infrared (IrDA infrared interfaces)

4.6. Blocks or allows (in read-only and read-write mode) the media devices (MTP, PTP); this includes mobile phones, tablets, digital cameras, media players and other devices that connect to a computer using Media Transfer Protocol (MTP) or Picture Transfer Protocol (PTP)

4.7. Allows USB power charge only, blocking data access (read and write)

4.8. Enforces device control policies based on user roles and computer groups, in sync with LDAP (AD)

4.9. Allows customer defined policies

4.10. Prevents port and device control being disabled (tamper protection)

5. Data Loss Prevention (DLP)

5.1. Prevents data leakage when data is modified, copied, pasted, printed, saved to external devices or transmitted from the endpoint using file, email, webmail, IM, web (HTTP and HTTPS) and FTP, according to customer defined policies

5.2. Allows custom remediation actions in case of non-compliance with defined rules, including encrypting, redirecting, quarantining, blocking

5.3. Generates comprehensive leakage related information, in real time (e.g. sender, recipient, timestamp, action, content) for proper analysis, investigation and audit, remediation, and risk assessment

5.4. Allows discovery and categorization of data at rest on local hard drives and network shares

5.5. Provides high degree of flexibility in definition of the rules (e.g. the administrator can create a list of URLs that are excluded from web protection rules)

5.6. Allows customer defined policies and classification rules

5.7. Uses regular expression for rules' definition

5.8. Works with text and binary file types, including Microsoft Office (Word, Excel, PowerPoint) and Adobe Acrobat files

5.9. Uses optical character recognition (OCR) for analysing the content of the image files

5.10. Allows write-only, permanent tagging/marking of the files (classification marking cannot be removed by regular users, once applied)

5.11. Allows multiple tags/labels for files, using configurable criteria

5.12. Allows classification marking overwriting by designated users with administrative privileges

5.13. Integrates with device control and media encryption components

5.14. Prevents data loss prevention being disabled (tamper protection)

6. Enterprise mobility management (EMM)

6.1. Provides anti-theft, management, monitoring and reporting, VPN, browsing protection, and AV

6.2. Uses on-premise-based (not cloud-based) management console, preferably integrated with the EP management console

7. Disk and File Encryption

7.1. Provides full hard-disk encryption, files and folders (local or on network shares) encryption and removable media encryption with enterprise restoration capability

7.2. Implements manual and automated encryption based on policy

7.3. Provides key management that lets authorized users share data securely and easily

7.4. Stops unauthorized users from reading lost or stolen media

7.5. Allows authorized users to recover forgotten passwords

7.6. Encrypts data in the background, so that protection doesn't impact the users

7.7. Uses processor level encryption features to reduce encrypted machines performance impact

7.8. Manages third-party security applications such as Windows BitLocker and Mac FileVault 2 drive encryption

7.9. Uses internationally recognized standards for encryption of hard-disks, files, folders and media

8. Rogue systems detection

8.1. Detects rogue systems connected on the network using passive and active network discovery techniques

8.2. Allows administrators to create and apply rules, ignore known managed systems and filter unmanaged devices that are of no threat by adding them to exceptions lists

8.3. Execute different actions on the list of rogue devices: track, alert, remediate

9. Sandbox system for malware inspection

9.1. Integrates with the antimalware component and allows automatic sandbox analysis of the scanned files, based on configurable criteria

9.2. Allows manual file submission

9.3. Uses a documented API for automated file submission for analysis and results collection and allows integration with 3rd party systems

9.4. Allows the usage of customer-provided VM templates (gold images)

9.5. Uses both virtualization technologies and bare-metal hardware, for virtualization-aware malware analysis

10. Protected endpoint platforms supported

10.1. Windows Client (x32, x64): 7, 8.1, 10, Windows To Go

10.2. Windows Server (x32, x64): 2003R2, 2008, 2008R2, 2012, 2012R2, 2016

10.3. Linux: RHEL6, RHEL7, Ubuntu LTS 14.04, 15.04,16.04

10.4. Mac OSX

10.5. Hypervisors: VMWare, Microsoft, Citrix

10.6. Microsoft Exchange Server: 2007, 2010, 2013, 2016

10.7. Microsoft Sharepoint Server: 2010, 2013, 2016

10.8. Mobile: iOS 9, Windows Mobile 8, 10, Blackberry, Android

10.9. SAN, NAS (integrated at SAN/NAS management console level)

11. Optimizations for virtualized environments

11.1. Supports integration with Vmware NSX, vShield APIs

11.2. Facilitates higher virtual machine (VM) density, reducing I/O and CPU usage

11.3. Uses virtualized environment optimization techniques, e.g. agentless, coordinated sharing of caches between VMs, etc.

11.4. Whitelists files from virtual machine template images to optimize scanning

11.5. Detects threats in offline VM images

11.6. Randomizes scan and update schedules to prevent resource utilization spikes

11.7. Scans files once, shares the results between clients, and de-duplicates file scanning to reduce bandwidth and latency

11.8. Detects automatically the clients running in a virtual environment and facilitates the setup of different policies for virtual machines

11.9. Detects I/O and CPU load levels and reduces scan speed to prevent utilization spikes

12. Management

12.1. Manages policies, deployment, compliance, and reporting from a single, centralized console

12.2. Shares policies and event data in real time between the managed endpoint protection components

12.3. Integrates with external threat intelligence feeds (e.g. IOCs, customer specific vulnerabilities, geo-location info) using open standards/formats

12.4. Integrates with network security solutions using open standards/formats

12.5. Imports/exports policies and signatures in common/standard/full documented formats (e.g. STIX, OpenIOC, Yara)

12.6. Allows complete/partial configuration import and export

12.7. Allows policies export in human and machine readable format (e.g. XML)

12.8. Allows automated configuration checks using full documented API

12.9. Allows deployment in a hierarchical architecture, containing one ore multiple management nodes, in master-slave, multiple levels, configuration

12.10. Has a lightweight, unique agent that integrates all client components, with minimal performance impact

12.11. Allows automated and manual deployment of the agent on the endpoints, in AD-based and non-AD environments

12.12. Performs automated agent deployment/redeployment/update on selected endpoints

12.13. The agent and all endpoint protection components are compatible with Microsoft operating systems protection mechanisms (e.g. EMET, Applocker, Firewall) and other customer specific endpoint agents (Online Computer Forensics, e.g. Encase Enterprise, Access Data Enterprise, Fidelis Cybersecurity)

12.14. Allows configuration of endpoints' hardware resources maximum load limits

12.15. Has centralized log collection capabilities for all its components

12.16. Has configurable reporting capabilities, including multiple report formats (e.g. PDF, XML) and distribution methods (e.g. email, web portal, RSS)

12.17. Allows manual and automatic exports of the event-related information to external systems (i.e. Information Sharing: MISP, SIEM: HP Arcsight, Ticketing systems) using common/standard/full documented APIs

12.18. Has configurable alerting capabilities, including Syslog, Windows Event, email, SNMP

12.19. Provides insights to the state of systems, users, applications, threats, generating configurable (role and user specific) dashboards with consolidated security health status, with drill down capability, in order to find specific details

12.20. Allows manual and automated updates of the software components and signatures definition

12.21. Works both in environments connected to internet and in environments without internet connectivity

12.22. Allows online and offline, configurable update sources

12.23. Has the ability to upgrade the endpoint components

12.24. Performs automatic and manual discovery of the endpoints

12.25. User interface to the management console is web based, using HTML 5 technology (not using Flash/Activex/Java components on the client side)

12.26. Uses role based access control (RBAC) to the console, providing granular read/write user roles

12.27. Allows both local definition of users and roles and LDAP(AD) integration

12.28. Allows multitenant mode of operation, limiting multiple entities' users access to their own endpoints, policies, events, alerts and logs

Non-Functional Requirements:

13. Support

13.1. Offers multiple support channels (phone/email/web portal/chat)

13.2. Uses qualified, dedicated support staff

13.3. Done within specified response and resolution timeframes

13.4. Provides customized protection policies and malware signatures/IOCs

14. Training

14.1. Provide Train-the-Trainer courses for NCIA personnel (a total maximum of 20 pupils to allow future in-house training of all roles without external contractor support)

Glossary of Terms and Definitions

TERM	DESCRIPTION
CLS	*Contractor Logistics Support*
COTS	*Commercial-Off-the-Shelf*
EPS	*Endpoint Protection Solution*
HIPS	*Host IPS*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
NCI AGENCY	*NATO Communications and Information Agency*

Annex B – Market Survey Questionnaire

Industrial Organisation name: _____

Name & full contact details of POC within Industrial Organisation: _____

Notes

- Please **DO NOT** change the formatting. If you need additional space to complete your response then expand the response boxes provided by adding more text lines.
- Please feel free to make assumptions *HOWEVER* you must list your assumptions in the spaces provided.
- Please **DO NOT** include any company marketing or sales material as part of your answers to the questions below. Please submit such material as enclosures with the appropriate references within your replies. If you need additional space, please use the continuation sheet at the end of this Annex.
- Please **DO** try and answer the relevant questions as comprehensively as possible.
- All questions within this document should be answered in conjunction with the requirements in Annex A

A. COTS Solution

1. Please indicate the requirements from Annex A that your proposed system/technology is compliant with (entirely or partially). For each of these, provide details how the requirement is fulfilled. Add as many lines as needed to the table below:

Req. no	Compliant (Partial/Full)	Details/Observations

2. Is your proposed system/technology currently in active service as a COTS solution? If so, where and what types of support (software and signatures updates, spares, malware analysis and training) does your organisation currently provide for such a capability?

3. Please provide us with estimated license fees for your current COTS solution calculated for a number of 5000/35000 endpoints. Are estimated fees recurring or non-recurring, and does these estimated fees cover all maintenance and support costs?

4. Please provide the following information regarding current and previous uses of your available COTS solution:
   a. Names of customers/users and contact details of their POC's.
   b. UNCLASSIFIED details on the specific program your COTS solution supported.
   c. Overview of any modifications to the COTS solution necessary to support these customers and the licensing terms applicable to modifications of the COTS product, stating also whether those will be assigned to the NCI Agency (Foreground/Background IPR).
   d. Estimated cost to the purchaser for modifications.

5. Please provide us with any additional capabilities of your COTS solution that go above and beyond those included in Annex A. Also, include the following:
   - A Rough Order of Magnitude (ROM) Procurement & Life Cycle costs including all assumptions the estimate is based upon,
   - Advantages & disadvantages of your product/solution/organisation,
   - Any other supporting information you may deem necessary including any assumptions relied upon.

B. <u>Previous NATO or Equivalent National Defence Experience</u>

1. Does your company have experience in achieving Security Certification and Accreditation through the NATO or equivalent national defence process? Please list applicable past projects where such certifications were achieved.

2. Does your company have experience in achieving approval through the NATO Request for Change (RFC) or an equivalent national defence process? Please list applicable past projects.

Continuation Sheet Please feel free to add any information you may think that may be of value to NCI Agency in the space provided below. Should you need additional space, please copy this page and continue with the appropriate page numbers.	Page __ of __

ANNEX C – INITIAL INDUSTRIAL DISTRIBUTION

Company	Point Of Contact
Intel Security	Mr. Sven Haegeman **Intel Corporation NV** Veldkant 31 2550 Kontich Belgium Mobile: +32 493 096064 Email: sven.haegeman@intel.com
Trend Micro	Mr. Steven Heyde **Trend Micro Benelux** Campus Mechelen – Building H, Schaliënhoevedreef 20 2800 Mechelen, Belgium Office: +32 (0)15 281480 steven_heyde@trendmicro-europe.com
Symantec	**Symantec B.V.B.A.** Regus Brussels Airport Pegasuslaan 5 1831 Diegem Belgium Téléphone :+32 (2) 709 20 00 Fax: +32 2 531 1141 brussels_reception@symantec.com
Sophos	**Sophos B.V.** Hoevestein 11B 4903 SE Oosterhout NB Netherlands Tel: +32 (0) 16 44 01 35 salesbenelux@sophos.com