NATO Communications and Information Agency

Acquisition Directorate

NCIA/ACQ/2024/07540
03 December 2024

Request for Information

Distributed Denial of Service (DDOS) Protection Landscape
NCI Agency Reference: RFI-424211-DDOS

NCI Agency seeks to identify state-of-the-art DDOS Protection Landscape solutions that can be provided through Commercial of the Shelf (COTS) products, solutions and/or services that will assist NCIA and its customers at a NATO Enterprise create an accurate and current view of these solutions and decide on the next steps to set up an Invitation for Bid.

NCI Agency Point of Contact

Ms. Leonora Alushani, Contracting Officer
RFI-424211-DDOS@ncia.nato.int

To: Distribution List (Annex A)

Subject: **NCI Agency Market Survey**
Request for Information RFI-424211-DDOS

1. Through issuance of this notice, the NCI Agency seeks to identify the availability and technical capability of all qualified NATO nation businesses that can provide the services described in this announcement.

2. This is a Request for Information (RFI). It is NOT a solicitation for proposals nor a pre-solicitation notice.

3. The NCI Agency reference for this RFI is **RFI-424211-DDOS**, and all correspondence and submissions concerning this matter should reference this number.

4. The NCI Agency requests the broadest possible dissemination by the Nations of this RFI to their qualified and interested industrial base.

5. The information resulting from this effort is for assisting the NCI Agency in understanding the existing technologies, their maturity level, identifying potential NATO nation based solutions and possible suppliers and defining requirements that will become part of an IFB package to be released to industry in the near future.

6. Responses may be issued to the NCI Agency directly by eligible NATO industry to the Point of Contact indicated at Paragraph 11 below.

7. Responses shall follow the instructions for submittal at Annex B of this RFI.

8. Interested parties are responsible for adequately marking proprietary or competition sensitive information contained in their response.

9. Technical demonstrations may take place following the submission of responses, with the purpose of showcasing your solution and clarifying or further augmenting those responses where required. Product demonstrations and/or face-to-face briefings/meetings with industry may be considered with companies that have submitted a formal response to this RFI.

10. If requested, companies should be willing to provide this demo free of charge to NCI Agency.

11. The NCIA will consider and analyze all information received from this RFI and will use these findings to develop a future solicitation for a DDOS product, solution and/or services. Any future solicitation would be advertised on the Agency bulletin board for all eligible companies to respond.

12. Responses are requested to be submitted to Ms. Leonora Alushani via email at RFI-424211-DDOS@ncia.nato.int by 20 January 2025.

13. Your assistance in this RFI is greatly appreciated.

For the Chief of Acquisition:

Leonora Alushani
Contracting Officer

Enclosures:
Annex A, Distribution List
Annex B, Instructions & Questionnaire

Distribution List

NATO Delegations (Attn: Military Budget Adviser)

Albania
Belgium
Bulgaria
Canada
Croatia
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Italy
Latvia
Lithuania
Luxembourg
Montenegro
Netherlands
North Macedonia
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Turkiye
United Kingdom
United States of America

Belgian Ministry of Economic Affairs

Embassies in Brussels

(Attn: Commercial Attaché)

Albania
Belgium
Bulgaria

Canada
Croatia
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland Italy
Latvia
Lithuania
Luxembourg
Montenegro
Netherlands
North Macedonia
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Turkiye
United Kingdom
United States of America

RFI-424211-DDOS Instructions & Questionnaire

RFI RESPONSE CATEGORIES

1. **Company DDoS Protection Experience:** Company details and track record in providing solution(s) and services in for the cyber security industry. Particular interest goes out to DDoS protection solutions and your experience providing them to defense industries and international organizations such as the EU and NATO.

2. **Solution features and capabilities:** Functions and capabilities provided by the DDoS protection solution(s), detailing unique features, coverage, and DDoS detection and mitigation technologies.

3. **Solution overview and deployment model:** Overview of DDoS protection solution(s), providing details related to the architectural design, central management, and the use and deployment models.

4. **System integration:** Integration capabilities of the DDoS protection solution(s) with other (security) systems. Please detail both integration with own products and features as well as those provided by other vendors.

5. **Solution security:** Security functions and measures taken to guarantee the security of the DDoS protection solution(s) and its data.

6. **Management:** The means and mechanisms included to manage the DDoS protection solution(s), with a specific interest for large distributed implementations with a large number of stakeholders.

7. **Support, maintenance and service provisioning:** Services provided to ensure an optimal and up-to-date DDoS protection solution(s).

8. **Cost and licensing:** Breakdown of pricing and licensing of the DDoS protection solution(s), including on-demand scaling requirements.

9. **Roadmap and future development:** Planned DDoS protection solution(s) and features in the near future with associated timelines.

10. **Case studies and success stories:** Overview of recent references and success stories to highlight experience for DDoS protection. Please also indicate your ability and willingness to provide product demonstrations to showcase solution critical functionality.

RFI Response Matrix

Respondents are invited to provide very specific references in the structure depicted in the table below to clarify which file(s), page(s), section(s) or other document location identifiers are relevant for responses in each category.
If there is no information provided in the response, the box can be left empty or filled with “N/A”.
Please add to your response the table below with relevant reference information completed.

#	Response Category	File / Page / Section / Paragraph References
1	Company DDoS Protection Experience	
2	Solution features and capabilities	
3	Solution overview and deployment model	
4	System integration	
5	Solution security	
6	Management	
7	Support, maintenance and service provisioning	
8	Cost and licensing	
9	Roadmap and future development	
10	Case studies and success stories	

RFI RESPONSE CATEGORY BREAKDOWN

1. Company Overview

1.1. What is your company's history and experience in providing solutions and services for the cyber security industry?

1.2. Can you elaborate on your company's experience and track record in providing cyber security solutions and services to defense industries and international organizations such as the EU or NATO?

1.3. What is your experience in detecting and mitigating DDoS attacks?

1.4. Please provide any third-party evaluation of your solution suite, if available (e.g. MITRE, Gartner, Forrester …).

1.5. Please indicate relevant regulatory compliance standards or industry standards applicable to your solution or company.

2. Solution Overview and Deployment

2.1. Please provide an overview of your solution suite relevant to DDoS Protection functionality.

2.2. What does the system architecture of the solution look like (e.g. centralized control, other…)?

2.3. What are your solution's DDoS deployment options? (cloud only, hybrid)

2.4. Does the system architecture allow high-availability / redundancy / load-balancing scenarios within a single site or across multiple sites (e.g. two data centres)?

2.5. Does your solution rely on PKI certificates, if yes; could you provide details on where and why?

3. Solution features and capabilities

3.1. DDoS Attack Coverage

2.1.1. What is the DDoS attack coverage that your solution provides such as:

- Volumetric
- Application
- TLS based
- Low and slow DDoS attacks?

2.1.2. What is your solution's coverage scale? Is there a limit on the number of domains, IP scales of the customer for protection?

2.1.3. Does your solution protect IPv6 IP address spaces?

3.2. Detection and Mitigation Technology

3.2.1. What detection techniques do you employ to detect DDoS attacks?

3.2.2. What mitigation techniques do you employ to defend against DDoS attacks?

3.2.3. How does your solution protect the internet pipe of the organization from volumetric DDoS attacks that threaten to saturate the internet pipe?

3.2.4. How does your solution distinguish between legitimate users and attackers?

3.2.5. How do you handle false positives and false negatives in your DDoS detection?

3.2.6. How does your solution guarantee best quality of experience to legitimate users even under attack?

3.2.7. How quickly will your solution detect and mitigate an attack?

3.2.8. What is the capacity of your mitigation infrastructure?

3.2.9. Does your solution have a limit for the number of DDoS attacks that it mitigates/protects?

3.3. Alerting, Response and Reporting

3.3.1. How quickly will your solution alert the customer after detecting an attack?

3.3.2. Does your solution include a mechanism that provides real time information about an attack?

3.3.3. Does your solution have a 24x7 emergency response team to help customers under DDoS attacks?

3.3.4. What is the reporting capability of your solution? (E.g. post attack reports, other…)

4. System integration

4.1. Please explain the integration / interfacing capabilities (e.g. API, data formats) of your solution to:

4.1.1. External Identity and Access Management (IAM) (e.g. Microsoft AD)

4.1.2. External Reporting Systems / Dashboards

4.1.3. External automation / management systems

4.1.4. External complementary cyber security solutions (e.g. firewalls, forensic solutions, …)

4.2. How does your solution facilitate integration to external SIEM solutions (e.g. Splunk)?

4.3. For all questions above: which of these are supported by default and which require custom connectors?

4.4. If your solution relies on PKI certificates, does it have the capability to integrate with the customer's PKI solution and use the customer PKI certificates?

5. Solution security

5.1. What security functions and measures are included to protect the system and its data?

5.2. What security certifications do you hold? (e.g., ISO 27001, SOC 2)

5.3. What measures are taken to avoid bypassing or tampering of the system (e.g. hunting on telemetry)?

5.4. Do you have a dedicated team to assess and respond to security vulnerabilities in your solution ?

6. Management

6.1. What is the central management method for your solution(s)?

6.2. Is there a single management console controlling all your solution(s) components?

6.3. Are there functional limitations of the management console that requires use of external interfaces such as CLI?

6.4. What is the compatibility / integration for the management component for on-premises and cloud related modules?

6.5. What reporting capabilities are available in your solution for auditing, compliance, and executive reporting purposes?

7. Support, maintenance and service provisioning

7.1. How is your solution(s) ensured to be up to date with the latest developments, both functionally and to mitigate new risks?

7.2. What parts of the DDoS protection solution(s) are expected to be operated by the purchaser and which can be provided as a service?

7.3. Can you specify what service level guarantees (SLA templates) can be provided through these services?

7.4. Are you able to provide any examples of service support models for any managed services that you currently operate?

7.5. What levels and type of support do you offer for your solution(s) identified in this questionnaire (e.g. Support Portal; Help Desk 24x7 / 9x5; Technical Account Manager; Development Team access; Onsite Professional Services …)?

7.6. What system diagnostic information needs to be provided with support cases?

7.7. Are you able to provide any guaranteed response and/or resolution times for support cases raised by a customer?

7.8. What onsite consultancy services are you able to provide (e.g. deployment; integration; configuration, tuning, optimisation; policy management …)?

7.9. Where DDoS attack is unable to be detected and mitigated by your solution(s), what will your remedies be for the SLA breach? How do you coordinate and work with the customer?

7.10. Explain available training scenarios to provide training specific to your solution (e.g. Face-To-Face at purchaser / vendor site; Online or CBT; Training material …)

7.11. What are your policies and procedures regarding notification of security vulnerabilities which may be identified in your solutions (e.g. through internal release testing)?

8. Cost and licensing

8.1. Can you provide a breakdown of your pricing and licensing structure for your DDoS protection solution(s) and related support (throughput, on-demand scaling, bundles …)?

9. Roadmap and future development

9.1. Can you provide an overview of your relevant near-future DDoS protection solution/product roadmap?

10. Case studies and success stories

10.1. Do you have any recent references and/or success stories for DDoS protection that would be relevant that you can/want to share?

10.2. Can you provide a demo environment, workshop, video, or similar, to showcase solution critical functionalities?