

**State of Israel - Ministry of Finance  
 Accountant General - Government Procurement Administration**

**Central Tender 05-2022**

**Tender Number 3 for the supply of CNAPP (Cloud Native Application Protection Platform) Systems and Accompanying Services for these Systems**

**Version 1- February 2023**

Appendix C - Technical Requirements

1. Instructions for responding to the requirements of this appendix
   1. In clauses that include an explicit demand for a specific feature or capability, the bidder must specify in detail how it meets the requirement of that clause.
   2. In clauses stating that “details are required,” the bidder is expected to provide a detailed response to the requirements specified in the clause.
   3. For each feature or supported capability, a detailed response is required regarding whether this feature or capability is included in the proposed items of the reference model, or whether further procurement or licensing is required in order to implement them.
   4. To the extent that the bidder did not provide an adequate response to the clause, it shall be deemed as if the bidder accepted the requirements of the clause as provided.
   5. **It must be further emphasized that the absence of a response, a response that does not address the requirement, the lack of a response to a requirement, or an unclear or ambiguous response, may result in a low score for the bid or its disqualification, pursuant to the sole discretion of the tender administrator.**
2. Terms and Requirements pertaining to the Manufacturer and the Bidder
   1. In addition to the bidder’s operation of an active service center as stipulated in section 3.13.6.2 to the Central Tender documents, the manufacturer shall be required to provide a support center that shall address professional requests and questions, through which it will be possible to receive answers within 24 hours, via one or more of the following options: **(a)** Phone, during regular office hours, as defined in section 3.10.1 to the Central Tender documents. **(b)** A portal for opening service requests **(c)** A designated email address for this tender. The bidder shall provide details regarding the manufacturer’s Service Level Agreement (SLA), method of communication, address/telephone, and method of operating the center.
   2. The support center shall provide support in English. Details must be provided regarding Hebrew support capabilities.
   3. The bidder shall be required to provide the manufacturer’s Best Practices documents for its recommended strengthening procedures and security configurations for the CNAPP, with an emphasis on the product’s method of use in order to achieve an accepted security standard such as ISO-27002, NIST, or CIS.
   4. The bidder shall provide the manufacturer’s list of certifications, as well as local and international standards supported by the system, such as ISO27018, ISO27017, ISO27001, SOC2 Type II, and others.
   5. The bidder shall provide details of the manufacturer’s policy regarding transparency and reporting on security exposures/problems detected in its products involved in the area of the tender, or regarding any other breach or exposure of information from its systems, including the time frame for receiving such reports.
   6. Location of the product’s development:
      1. The bidder shall provide details regarding the location where the products and systems involved in the tender are manufactured. A manufacturer’s confirmation of the information must be attached accordingly.
      2. If the manufacturer is committed to establishing a development center in Israel in the field of the tender, details of this must be presented, and the manufacturer’s commitment on the matter must be attached accordingly.
   7. Details of the bidder’s experience with the proposed product:
      1. The bidder’s experience with the proposed product must be presented, including the year of commencement of the bidder’s work with the proposed manufacturer, the bidder’s level of certification on behalf of the manufacturer of the proposed system, and any other relevant information.
      2. Information regarding all the manufacturer’s certified technicians for the proposed products and services in the tender shall be included, in the following format:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Number | Employee Name | Years of Experience in The Subject of the Tender | Certification for the Proposed Products | Certification Year | | Security Clearance, if Applicable | |
| 1 |  |  |  | |  | |  |
| 2 |  |  |  | |  | |  |
| 3 |  |  |  | |  | |  |
| 4 |  |  |  | |  | |  |
| 5 |  |  |  | |  | |  |

* 1. The bidder shall provide details regarding its method of support of the following services:
     1. Provision of security consulting to the Client – specify the nature of the proposed services.
     2. Provision of support on-site to the Client’s – specify the assistance and escalation processes.
     3. Provision of professional training to the Client’s team, including formal training and certifications provided by parties certified by the manufacturer’s – specify the types of courses and certifications offered both by the bidder and by the manufacturer.

1. System/Products Requirements
   1. In the context of this tender, **Cloud Native Application Protection Platform (CNAPP)** products are the overall unified tools and technologies included in Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) and further tools under a single platform offered in a SaaS (Software as a Service) configuration, enabling protection of the organization’s applications and software development life cycle at the Client’s cloud environment and within the organization (hereinafter: “**the System”** / “**the Service”**).
   2. The proposed system and licenses within the reference model shall include all requirements specified in this appendix, without any additional payment, including interfacing capabilities to third party products required in the tender documents.
   3. The bidder’s proposal shall include all necessary components for addressing the requirements of the tender documents, specifications, and reference model. The bidder, in its tender bid, undertakes that all products and services proposed by it in the tender are routinely manufactured, and that the bidder or the manufacturer have no information or suspicion regarding the possibility of cessation of the sale, manufacture, or support of the products and services (or components or items used in them) proposed by the bidder.
   4. The bidder must verify that its bid for each of the components includes all licensing required for the system’s operation and use.
   5. A clear and comprehensible licensing specification must be provided for each proposed component in accordance with the reference model and specifying the licensing model (Perpetual, Subscription, and so on).
   6. The manufacturer’s Best Practice document regarding the management and optimization of the licenses and their operation must also be provided.
   7. Below find is a list of the required items:
      1. **Component A – Software CNAPP license for a large office:**

| **Topic** | **The bidder’s response** | **Remarks** |
| --- | --- | --- |
| Cloud-based CNAPP license (SaaS configuration) that includes all of the following components:   1. CSPM tool that includes support and management of up to 1,000 assets/resources as specified in section ‎3.2.1.2.4 below. 2. CWPP tool that includes support and management of up to 1,000 Workloads as specified in section ‎3.2.2.2.1 below. |  | Details must be provided for all items required.  Payment shall reflect the quantity of assets/resources and Workloads operating **concurrently**, with no other limitation on the type of components or their quantity. |
| A unified and central management system for all aforementioned components. |  | Details must be provided for all items required.  The management system shall support all required components with no limitation regarding the type of components or their quantity. |

* + 1. **Component B – Software CNAPP license for a medium-sized office:**

| **Topic** | **The bidder’s response** | **Remarks** |
| --- | --- | --- |
| Cloud-based CNAPP license (SaaS configuration) that includes all of the following components:   1. CSPM tool that includes support and management of up to 500 assets/resources as specified in section ‎3.2.1.2.4 below. 2. CWPP tool that includes support and management of up to 500 Workloads as specified in section ‎3.2.2.2.1 below. |  | Details must be provided for all items required.  Payment shall reflect the quantity of assets/resources and Workloadsoperating **concurrently**, with no other limitation on the type or quantity of components. |
| A unified and central management system for all aforementioned components. |  | Details must be provided for all items required.  The management system must provide support for all required components with no limitation regarding the type or quantity of components. |

* + 1. **Component C – Software CNAPP license for a small office:**

| **Topic** | **The bidder’s response** | **Remarks** |
| --- | --- | --- |
| Cloud-based CNAPP license (SaaS configuration) that includes all of the following components:   1. CSPM tool that includes support and management of up to 100 assets/resources as specified in section ‎3.2.1.2.4 below. 2. CWPP tool that includes support and management of up to 100 Workloads as specified in section‎3.2.2.2.1 below. |  | Details must be provided for all items required.  Payment shall reflect the quantity of assets/resources and Workloads operating **concurrently**, with no other limitation on the type of quantity of components. |
| A unified and central management system for all aforementioned components. |  | Details must be provided for all items required.  The management system shall support all required components with no limitation regarding the type or quantity of components. |

1. Technological requirements
   1. **General attributes**
      1. **CNAPP tool configuration**
         1. The bid must include a cloud CNAPP solution (SaaS) using a single manufacturer platform for CSPM, CWPP tools and additional integrated tools under a unified management system, in such a way that all components are required to interface with the Client’s cloud environment and be operated by the Client without depending on another manufacturer’s products.
         2. The solution must fully support a Multi Cloud environment as well as public cloud platforms, such as AWS, GCP, and others.
      2. **Additional configurations for CNAPP tools**
         1. Details must be provided regarding the support of hybrid configurations that include on-site and parallel cloud-based components.
         2. Details must be provided regarding the public cloud platforms on which the service is provided, including whether they support private clouds, the method of protecting confidentiality and information security, method of product management, and so on.
         3. Details must be provided regarding support offered for Self-hosted/On-Premise configuration by local installation at the Client’s environment (such as a private cloud); for example, Virtual Appliance.
         4. Details must be provided regarding additional configurations in which the proposed products can be purchased.
      3. **Additional Integrated BNAPP tools that are part of the solution** 
         1. Details must be provided regarding Infrastructure as Code (IaC) scanning tools offered by the proposed manufacturer.
         2. Details must be provided regarding Cloud infrastructure entitlement management (CIEM) tools offered by the proposed manufacturer.
         3. Details must be provided regarding Kubernetes Security Posture Management (KSPM) tools offered by the proposed manufacturer.
         4. Details must be provided regarding (SSPM) SaaS security posture management tools offered by the proposed manufacturer.
         5. Details must be provided regarding further tools offered by the proposed manufacturer in the CNAPP field.
      4. **Method of operation**
         1. The CNAPP platform and CWPP, CSPM tools must be installed and managed at a central location in the Client’s cloud environment and offer all requirements without the need to install agents (“Agentless”) on components or on Assets at the Client’s environment.
         2. Details must be provided regarding the need to install an Agent component as part of the proposed product solution.
         3. The CNAPP management component must be installed at the manufacturer’s cloud environment (SaaS) or on a server in the Client’s private-cloud environment (Self-hosted).
      5. **System requirements**
         1. Details must be provided regarding all requirements in terms of the technological infrastructure required for installing the proposed systems at the Client’s environment (On-Premise/Self-hosted). The details shall include the quantity and type of physical and virtual servers that are required, network components, operating systems, network security components, database types, and storage size required.
         2. Details must be provided regarding the system’s support of Multi-Tenancy architecture, in a hierarchical, transverse manner, with logical separation capabilities between the environments of a number of organizations under central management.
         3. Details must be provided regarding the system’s architecture and the type of infrastructures and operating systems on which the CNAPP platform operates.
         4. Support is required for synchronizing all system components with a reliable time source.
         5. Details must be provided regarding dependence on external components for the installation of the systems or limitations pertaining to components that are not part of the systems’ architecture.
      6. **Performance**
         1. Details must be provided regarding the performance of the detection system, with emphasis on the duration of the detection process and the addition of assets and resources to the system in a multi-asset cloud environment.
         2. Details must be provided regarding the effect of the detection process on the performance of scanned assets.
         3. The system must be able to support the ability to monitor the condition of the system and its services (Health Monitor).
      7. **Survivability, Backup, and Applicative Functional Continuity**
         1. The system must support a High Availability configuration. Details are required regarding system’s survivability method (Active-Active, Active-Standby, and so on.).
         2. Support is required for the backup and export capabilities of the system’s configuration to an external server/component and in an open/standard format, as well as for support of importing and restoring settings to the system.
         3. Support is required in a DR environment that enables restoration of all system capabilities and the tools embedded in the Client’s environment in the event of a system failure or catastrophe. Details must be provided regarding the method of implementation of the solution in such an event.
      8. **Language**
         1. The system is required to support English language.
         2. Details are needed regarding Hebrew language support in scenarios such as the following:
            1. Import/export of identifiers (IOCs), such as domain names in Hebrew (IDN).
            2. Executing queries regarding objectives in Hebrew, such as identifiers and asset names.
            3. Generating reports regarding objectives in Hebrew, such as identifiers and asset names.
         3. Details must be provided regarding additional supported languages.
      9. **System security**
         1. System access must support Single sign-on (SSO) and Multi-factor authentication (MFA) mechanisms. Details must be provided regarding mechanisms and identifier protocols that are supported in the system.
         2. The system must provide integrated support of work with SAML 2.0 and ADFS.
         3. Details must be provided regarding the ability to apply password policies to the system’s users (including local users), which shall include the definition of factors such as: length, complexity, validity, passwords history, and so on.
         4. The system must support a continuous and regulated registration and documentation process to the Log of every access made, change of definitions, users’ activity, and files in the system.
            1. The log files in the system shall be protected from unauthorized access (viewing, modifying, deleting).
            2. Details must be provided regarding the system’s ability to support saving and storing the log files and historical information of the system over time and within a specified time frame (for archiving purposes, investigating, and so on).
            3. The system must support the transfer/receipt of log files and events to automation and security monitoring systems such as SIEM and SOAR.
         5. The manufacturer must initiate applicative penetration tests (PT) and periodic Code Reviews. Details must be provided regarding the manufacturer’s policy.
         6. The manufacturer must submit an updated penetration test report and a successful code review of the system.
         7. Details must be provided regarding the implementation of Zero Trust model principles via the system.
         8. Details must be provided regarding monitoring and security mechanisms and strengthening procedures for all tools included in the system, with an emphasis on the application, databases, and secured links.
         9. Details must be provided regarding the system’s ability to cope with attacks (such as brute-force, DDoS, and so on) as well as details regarding mobilization, management and response to security events (IR).
      10. **Access authorizations**
          1. The system is required to allow the most limited access authorizations as possible (least privilege) for the performance of authorized operations for the system’s users. Details must be provided regarding the method of limiting access authorizations in the proposed solution.
          2. Details must be provided regarding the types of roles (Roles) of the system’s users and managers.
          3. Details must be provided regarding the types of structured rules (Rules) existing in the system for access control.
          4. Details must be provided regarding parameters by which an access authorizations policy can be defined for the various operations and regarding how to dynamically restrict users’ access to the system, based on, for example, user type, date, day, access time, IP address, asset, geographical location, and so on.
      11. **Encryption**
          1. The system must establish encrypted communication with all internal system components. Details must be provided regarding the nature of the solution, emphasizing “at rest” encryption and “in transit” encryption.
          2. The system must establish encrypted communication with all managed assets and resources.
          3. Support for managing secure access to the system via SSH keys is required.
          4. All verification data (passwords and SSH keys) must be at least AES-256 encrypted. Details must be provided for all encryption algorithms included in the proposed solution.
          5. Details must be provided regarding support for standard FIPS 140-2 encryption and upwards.
          6. Details must be provided regarding support for interfacing to KMS services for managing encryption keys.
      12. **Updated**
          1. The manufacturer must distribute routine periodical system updates that include, *inter alia*, system updates, information security updates, and repairs for damage/weaknesses/exposures identified. Details must be provided regarding the manufacturer’s policy.
      13. **User interface**
          1. Details must be provided regarding all types of existing user interfaces for managing the CNAPP platform, such as WEB interface and designated client.
          2. Details must be provided regarding the method of accessing management interfaces, whether it is necessary to access the portal located on the Internet or it is possible to access the management interface without an open routing to the Internet (such as VPC Peering).
   2. **Attributes of the system’s components:**
      1. **The CSPM (Cloud Security Posture Management) tool**
         1. **General description**
            1. Continuous monitoring and analysis of threats to the client’s cloud environment by identifying, warning, and reducing vulnerabilities in the cloud, lowering risk, and improving the security of the organization’s assets and components at the cloud environment.
            2. Details must be provided regarding the method of implementing the solution.
         2. **Mapping and asset identification capabilities** 
            1. Support is required for the performance of automatic and continuous scanning for the identification and classification of applications, resources, and assets. Details must be provided regarding the overall capabilities existing within the proposed product for the same detection and location operation, as well as for the addition of applications, assets, and resources to the system and how they work.
            2. Support is required for the performance of timed scanning for initiating manual location and addition of assets and resources by the system manager.
            3. The system is required to support graphic display for an updated status of the mapping of all the Client’s assets in the cloud. Details must be provided regarding all capabilities existing in the proposed product for presenting the assets mapping.
            4. The system is required to support detection, location, and additions to the system of all of the following assets and goals:

Public cloud platform assets with an emphasis on AWS and GCP.

Windows assets.

Linux\Unix assets.

Virtual assets (such as VMware ESX\ESXI).

Kubernetes assets.

WEB assets and applications.

Databases.

Network and information security components (switches, routers, FW).

Details must be provided regarding support for operating systems and additional components (such as IoT).

* + - * 1. Details must be provided regarding support of assets and further goals in the cloud, including platforms, applications, and third-party tools.
      1. **Monitoring, Identification, and Repair Capabilities**
         1. The system must support automatic and continuous real-time monitoring capabilities to ensure that the Client’s assets and components in the cloud operate according to Compliance, Benchmarks, and the organization’s policies, and that they are identified efficiently, and automatically added to the system, with minimal effort.
         2. The system is required to continuously monitor and identify in real time potential threats, malicious and anomalous activity, unauthorized access, exposure of sensitive information, and security events in the Client’s cloud environment.
         3. Support is required for identification capabilities and presentation of identified vulnerabilities, weaknesses, exposures, threats, and risks in accepted formats (such as CVE) and in further dynamic and graphic methods of presentation. Details must be provided regarding the overall capabilities existing in the proposed product.
         4. The system is required to identify and warn in real time of misconfigurations, changes, exceptions, risks, exposures, and security gaps found in the Client’s cloud environments, such as: Open ports, erroneous authorizations, accuracy of identification method (such as the use of MFA, passwords policy, use of user accounts, suitable encryption definitions, High Availability, backups, and so on, and to provide methods or action and application recommendations for Remediation.
         5. Details must be provided regarding support of Auto-remediation capabilities for security gaps and misconfigurations (such as closing of vulnerable ports or ports that are open unnecessarily).
      2. Details must be provided regarding the system’s support of defense based on AI/ML technologies (Supervised and Unsupervised), to support behavioral learning of the cloud assets, integrative identification and analysis of information sources, communication traffic, exceptional events and behavioral patterns pointing to malicious activity and a threat to the Client’s environment.
      3. **Compliance and Regulation**
         1. The system must support the ability to define policy rules, continuous and automatic inspection of compatibility, and ensuring that the cloud environment meets defined policies and security controls. Details must be provided regarding the method of defining terms and tests for implementing a different policy (for example, by asset groups, cloud environments, different groups of users, and so on).
         2. The system is required to support real-time compatibility testing of the cloud environment in compliance with international standards and information security frameworks, such as: NIST CSF, GDPR, HIPAA, PCI-DSS, CIS, SOC 2, GCP/AWS Well-Architected, NIST 800-53, NIST 800-171 ISO27002, MITRE ATT&CK, FedRamp, and so on. Details must be provided regarding all types of standards and security frameworks that are supported in the system.
         3. The system must support the creation of “standard” or personally tailored security frameworks (such as Best Practice or a governmental standard) for performing compatibility tests and security control for the Client’s cloud environments. The method of distributing standard/security frameworks to various clients (that are not in the same ORG) must be detailed, as well as the central updating capabilities (for instance: a central entity defines a governmental standard and distributes it to systems installed in all offices).
         4. Details are required regarding support of integrated rules in the system, the ability to enforce policy and define configuration, and identification and prevention of changes that deviate from them (for example, the ability to limit work to a specific Region / preventing specific Regions, and so on).
         5. Details must be provided regarding support of predefined policy rules and behavioral-based rules.
    1. **Cloud Workload Protection Platform (CWPP) tools** 
       1. **General description**
          1. Continuous monitoring of Client Workloads and infrastructures in the cloud and in the organization itself (On-Premises) by integrating the protection of information Integrity, applications control, behavioral monitoring, prevention of penetrations, and defense against malicious software during Runtime.
          2. Details must be provided regarding the method of implementing the solution.
       2. **Scanning and Detection capabilities** 
          1. The system is required to support continuous scanning and detection capabilities for workloads:

Local servers and virtual machines (VMs) including Windows\Unix\Linux.

Containers and serverless such as: GKE, EKS, ECS, Lambda, and so on.

Registries files such as GCR, ECR, JFrog, and so on.

Configuration management database (CMDB).

Images, such as: Apache, GZIP, Httpd, Java, Mongo, Mysql, Nginx Node, PHP, Postgres, Python, Redis, Ruby, SSL, SVN, and so on.

API interfaces.

Repositories such as GitHub.

CI/CD processes.

Secrets in files, configuration definition files, databases, source code, users and system passwords, digital certificates, API keys, and so on.

* + - * 1. Details must be provided regarding support of workloads and further cloud infrastructures including platforms, apps, and third-party tools.
        2. Support is required for integrative presentation capabilities of assets and resources identified while using dynamic and graphic presentation methods, such as a map of assets and links, risk level, status of policy compliance, and so on.
        3. Support is required for automatic implementation of policy for new assets added to the Client’s cloud environment.
      1. **Policy rules and enforcement**
         1. The system must support the ability to define and enforce policy rules, continuously and automatically inspect compatibility and the extent to which cloud-based assets and resources are compatible with defined policies, and security controls regarding common security frameworks (such as MITRE ATT&CK, CIS).
         2. The system must support the creation of FW rules and personally adjusted policy terms for enforcing security compatibility and control for assets and resources at the Client’s cloud environment.
         3. The system must support Application Control capabilities and real-time enforcement of runtime files and definitions in servers and machines based on a predefined Allowlist/Denylist.
         4. Details must be provided for the system’s support for the creation of a user activities profile for identifying Lateral Movement of threats and preventing Identity Based Attacks.
         5. Details are needed regarding the ability to create policy, enforcement rules, and applicable recommendations for improving the architecture based on behavioral learning of the network’s traffic operation.
      2. **Detection, Identification and Prevention**
         1. Details must be provided regarding the system’s overall capabilities for detection, identification and prevention of misconfiguration definitions, exposures and security gaps, malware and vulnerabilities in servers, containers and serverless, with an emphasis on the following capabilities:

Support for real-time scanning for detection, identification, and prevention of identifiers/signatures-based malware.

Support for real-time scanning for detection, identification, and prevention of malware with no identifiers/signatures and Fileless type malware.

Support for real-time scanning for detection, identification, and prevention of attempts to undermine information integrity and reliability – File Integrity Monitoring (FIM).

Support for Heuristic analysis for files in order to determine their purpose, aim, and use.

Support for real-time running of files in a safe and isolated environment (Sandbox) so as to identify hacking indicators – Indicators of Compromise (IOCs) – in the operation.

Support for real-time scanning for detection, identification, and prevention of the use of lenient, exposed, or vulnerable FW and routing rules, or of deviations and changes from the approved Baseline.

Support for real-time scanning for detection, identification, and prevention of use of FM and routing rules that are inactive or rules having a low usage level.

Support of real-time scanning for detection, identification, and prevention of the use of vulnerable services such as FTP, Telnet.

Support for real-time scanning for detection, identification, and prevention of lenient use of access authorizations for applications, assets, and resources in the Client’s cloud environment.

Support for real-time scanning for detection, identification, and micro segmentation performance enforcement for servers (such as Windows, Linux, K8, and so on) in the Client’s cloud environment.

Details must be provided regarding support for real-time running of a whitening process (CDR) for files.

Details must be provided regarding support for Genetic signature detection capabilities for identifying patterns of malware from the same family.

Details must be provided regarding the system’s support for real-time scanning to ensure that there is no exceptional use of communication traffic.

Support for real-time scanning for the detection, identification, and prevention of access of low reputation IP addresses and domains to and from the Client’s environment.

Details must be provided regarding the system’s support for real-time and retrospective detection, identification, and prevention of malware attempts to utilize vulnerabilities and runtime of hazardous code in software and in active objects in the cloud assets, including the system of files, volatile memory, configuration definitions, databases, and so on.

Details must be provided regarding support of real-time scanning to ensure that the PoLP (Principle of Least Privilege) principle is effectively implemented.

* + - 1. Information protection
         1. Details must be provided regarding support for real-time scanning for detection, identification, and prevention of the exposure of sensitive information stored at the Client’s cloud storage facilities (such as financial data or information enabling personal identification (PII), credit card numbers, I.D. numbers, and so on). Details must be provided regarding to the method of the response and supported storage systems and information types.
         2. Details must be provided regarding mapping and classifying capabilities for information in the Client’s cloud environment and automatic analysis and presentation of risks and security gaps that may result in exposure of sensitive information.
      2. **Code and application security**
         1. Support is required for scanning and analysis of vulnerabilities and security risks at servers, containers, and serverless environments at Runtime and at non-runtime environments.
         2. Support is required for real-time scanning and analysis of the reliability of authorized sources, including open sources, operating systems (OS), libraries (Git Repository), Images, and so on, in order to ensure that they originate from authorized and safe sources and meet the security controls in the software development lifecycle (SDLC).
         3. Details must be provided regarding support for the definition of basic configuration for a hardened image (Golden Image) for virtual machines (Vms) and real-time identification of exceptions and changes from an approved Baseline.
         4. Support is required for automatic scanning for the identification and analysis of vulnerabilities and security risks in API interfaces and Web applications while presenting the risk level and applicable recommendations for repair through acceptable security frameworks (such as OWASP API Security Top 10).
         5. Details must be provided regarding support for automatic scanning for the identification and analysis of dependencies between applications (Application Dependency) and the network traffic between them.
         6. Details must be provided regarding support for behavior analysis capabilities during Runtime for all components of the applications, including Processes, Network communication, system files (Filesystem), and so on, in order to ensure that the application is not vulnerable (exposed data, crypto mines, and so on).
         7. Details must be provided regarding the ability to identify sensitive files with hardcoded secrets, such as passwords, API keys, and Tokens in order to prevent unauthorized access from risk sources.
         8. Details must be provided regarding support for capabilities to perform static and dynamic tests (SAST/DAST) as part of the CI/CD Pipeline.
         9. Details must be provided regarding support for capabilities to perform static tests through Integrated Developer Environment (IDE).
         10. Details must be provided regarding SBOM (Software Bill of Materials) support for real-time presentation and analysis capabilities while using SPDX/SWID formats for the transparency and visibility of risks in the software’s supply chain.
         11. Details must be provided regarding support for scanning capabilities for the central management of SCM (Security Configuration Management) source code.
    1. **Central Management System for CNAPP tools**
       1. **Interface platform**
          1. The system shall be supplied with a unified platform for managing and operating the proposed products. Details must be provided regarding the type of platform, such as WEB and GUI portal, and whether there are different platforms for management of CSPM and CWPP components.
          2. Details must be provided regarding support for Multi-tenant configuration for central management of the system as a security provider (MSSP) towards multiple Clients in different clouds under a unified central management interface (dashboard).
          3. Details must be provided regarding support for the implementation of a constantly updating overall policy with definitions for copying, importing, and exporting capabilities from one Tenant to the next in order to duplicate preferences, rules, display, and system definitions.
          4. Support is required for the creation of personally adjusted display screens in the central management interface.
       2. **Assets and Resources management capabilities**
          1. A central capability is required for dynamic and continuous inventory management of cloud resources and assets in the Client’s environment (creation, change, addition, removal, deletion, and so on).
          2. Details must be provided regarding the maximal supported quantity of manageable resources and assets under the proposed system.
          3. A mechanism is required for the addition and removal of resources and assets to and from the system for monitoring and implementing secured access between the system and the Client’s cloud assets.
          4. Details must be provided regarding support for addition, removal, marking, and tagging of assets and resources while emphasizing manual addition that is not part of the automatic identification process.
          5. Details must be provided regarding the system’s ability to classify all assets and users of the system into sub-groups based on various parameters (such as IP ranges, naming conventions, operating system, domain, applications, cloud environment services, and so on.
       3. **Ability to present information and reports**
          1. The system’s management interface is required to present a central situation report for all system components and cloud assets, while focusing attention on events and indices that deviate from the norm.
          2. The system is required to provide a list of assets, services, resources, objects, users, and so on, that do not conform to the organization’s policies and applicable recommendations for rectification.
          3. Support is required for the ability to present an integrative uniform security status report of vulnerabilities, weaknesses, exposures, threats, and risks that have been identified in all the organization’s assets into a weighted Risk Score while using accepted parameters (such as CVSS).
          4. Details are required regarding further dynamic and graphic methods of presentations, such as attack path analysis, network topology, timeline, and so on.
          5. Details must be provided regarding support for the ability to examine implications of changes to configuration/authorizations/hardening definitions prior to actual implementation (What-if).
          6. The system must support its own interactive warnings indication interface within its interface.
          7. The system must support textual search capabilities, as well as filtering by fields, names, labeling, dates, types of cloud infrastructures, assets, resources, services, warnings, and so on.
          8. The system must support the production of prepared and customized reports regarding the entire system. Details must be provided regarding the types of existing reports in an integrated manner within the system, as well as for supported formats, such as PDF, HTML and CSV.
          9. The system must support the ability to create periodic and customized reports, according to relevant assets, cloud environments, fields, and Tags, and send them to a predefined target audience. Details must be provided, alongside an example of the system’s reports (such as a Compliance report, a meta-report for the Client’s environments which includes an Executive Summary and detailed findings).
          10. The system must provide warnings to the system’s managers and its users regarding exceptional events as defined in advance. Details must be provided regarding existing warning mechanisms in the proposed solution (Email, SMS, API interface, massaging system, voice warnings, built-in warnings in the system itself, and so on).
       4. **Analysis and investigation of suspicious events**
          1. The management system is required to collect logs and evidence of each individual event in the system, for later presentation and investigation. Details are needed regarding the duration of time in which information is kept historically (Retention Policy).
          2. Details must be provided regarding built-in support or analysis (Parsing) and mapping capabilities of logs, both manually and automatically.
          3. The system must identify and warn in real time of suspicious activity, provide a score/rating according to the level of suspicion, issue warnings to analysts and to the system’s managers, and provide recommendations and application methods of action for response and repair (Remediation).
          4. Details must be provided regarding the overall capabilities existing in the proposed product, including Auto-remediation and Incident Response capabilities.
          5. Support is required for communication analysis based on predefined past data as well as information accumulated over time regarding the organizational assets, resources, and objects.
          6. Support is required for the establishment of a baseline from which any deviations shall be defined as suspicious events.
          7. Details must be provided regarding support for recording sessions, their storage, analysis, and recurring presentation of the same sessions (such as summary over a timeline, textual summary, video).
          8. Details must be provided regarding which parameters can provide a baseline for defining a deviation from routine operations, such as operation time, special actions initiated, deviation from a user’s routine activities, suspicious IP address, unique commands, access from a geographic location, and so on.
          9. Support is required for dynamic and graphic presentation capabilities for the analysis of events, such as a map of graphic links that presents links between assets and suspicious threats, analysis of suspicious activity on a timeline, and so on.
          10. Support is required for real-time mapping of events for the cloud environment with information security frameworks such as MITRE ATT&CK.
          11. Support is required for simple search capabilities – textually and filtering by names, services and security weaknesses, and so on, in all cloud assets.
          12. Details must be provided regarding support of writing, timing, and search capabilities using advanced Queries for analysis and crossing of data from a number of different information sources in the system.
          13. Details are needed regarding the system’s support of the construction and application of Playbooks and simulation and automation capabilities for pre-running tests.
          14. Details must be provided regarding support for approvals processes for repair and response activities.
       5. **Cyber Threat Intelligence**
          1. Details must be provided regarding the system’s support of connecting and correlating with cyber threats intelligence sources. The system’s method of operation must be recorded, as well as the number of intelligence sources which the systems simultaneously supports.
          2. Details must be provided regarding built-in support for analysis and presentation of weaknesses and threats in real time / near real time, when addressing a number of different cyber intelligence sources.
          3. Details must be provided regarding support for manual addition of cyber intelligence feeds.
          4. Details must be provided regarding support for enriching the system with identifiers (IOCs) in a manual and mechanized manner.
       6. **Updates distribution capability**
          1. Support is needed for a centralized ability to inspect the status of software and security updates for the Client’s cloud assets while following existing trends and exceptions.
          2. Details must be provided regarding support for the system’s central ability to distribute/remove software and security updates to the Client’s cloud assets, manually/automatically, in accordance with a predefined delineation and policy.
  1. **Interfaces with third party products**
     1. General
        1. Details must be provided regarding the system’s support for integration to third-party products (such as cloud tools and AWS and GCP infrastructure, information security and communication products, productivity tools, automation tools, Ticketing tools, ITSM systems, design and Development management and follow-up tools, and so on).
        2. Details must be provided regarding the system’s support for Marketplace solutions.
        3. Details must be provided regarding support for third-party suppliers for identity and access management (IdPs).
        4. Support is required for a work interface with security automation and monitoring systems such as SIEM and SOAR. Details must be provided regarding the type of solution and supported tools and systems.
  2. **Roadmap**
     1. Details must be provided regarding the manufacturer’s roadmap for tenders, while focusing on Main Features and on schedules for the coming year.
  3. **The system’s infrastructure**
     1. The system shall be installed on the public cloud platform of one of the winners – Amazon Web Services and Google (hereinafter: “**the Cloud Providers”**) in tender 01-2020 for the Supply of Cloud Services on a Public Platform for Government Ministries and Auxiliary Units (hereinafter: “**The Nimbus Tender”**), pursuant to the following rules:
        1. The system must operate from a public cloud area created by one of the cloud providers within the geographic territory of the State of Israel and approved by the tender administrator (hereinafter: “The Israeli region”), no later than 6 months following the date of declaration of a winning candidate.
        2. To the extent that the Israeli region of the cloud provider for which the system is proposed based on its cloud platform has not been created yet, the system shall be provided, temporarily and until the Israeli region has been created, on the largest public cloud area operated by the cloud provider in which the proposed system is operated within the EU (hereinafter: “**The area abroad”**). In this case, the provider shall transfer the system, including users’ data, to the Israeli region within 6 months following the day in which the cloud provider has confirmed that the Israeli region is prepared for operating the system pursuant to the requirements from the provider. The transfer of users’ data shall be conducted in coordination with the clients and at no further cost.
        3. The system shall be required to meet all relevant standards and the SLA, within no more than six months from the day on which the system has begun to be provided at the Israel region.
     2. Details must be provided regarding the system’s configuration, including the following topics:
        1. The public cloud infrastructures on which the solution is based, among the cloud providers platforms.
        2. Is the account on which the system operates exclusive to the proposed system, or is it common to all clients?
     3. **Configuration of the proposed system**
        1. The configuration of the proposed system’s work must be detailed with reference to the following:
           1. Location of storing protected information – at the client’s “network” (such as VPC), at the provider’s, the manufacturer, or any other location. To the extent that the information is not stored by the client, the location of its storage must be provided.
           2. Location of content data processing (as defined below) – at the client’s “network” (such as VPC), at the provider’s, the manufacturer, or any other place. To the extent that the content data is not processed by the client, the location of its storage must be provided.
           3. To the extent that the material is stored and processed at the client’s premises, the provider’s or manufacturer’s ability to access or control the information or the system must be detailed, if applicable.
           4. Configuration of the system’s linkage to the client’s network must be detailed, with reference to the following:

Regarding the method of linking the client’s network in the cloud (such as VPC), details must be provided regarding whether the link is, for example, configured as VPC Endpoint, Peering, Private Link, or whether the service represented in the client’s network itself, or via a VPN link or otherwise, how the link is secured, and whether external addresses need to be opened in order to connect to the service.

Regarding the interface to the management system of the service, details must be provided regarding whether the link is, for example, configured as VPC Endpoint, Peering, Private Link, or whether the service is represented in the client’s network itself, or via a VPN link or otherwise, how is the link secured and whether external addresses need to be opened in order to connect to the service.

* + 1. **Securing the Human Capital**
       1. Describe the control, verification, and filtering processes conducted for the employees of the manufacturer and its sub-contractors and suppliers, while considering the differences in processes according to the types of employees and risk levels involved in their duties.
       2. Describe the training and refresher processes for security, safety, and cyber procedures for the employees of the manufacturer and sub-contractors.
       3. Describe the training and professional certification processes for the professional staff of the manufacturer and sub-contractors.
       4. Describe supervision mechanisms for the implementation of procedures and methods of handling violations of security procedures or other critical procedures.
       5. Provide details regarding whether tools are implemented for the identification of human risks (such as identifying behavioral anomalies, feedback from management or colleagues regarding specific problems, and so on) among sensitive position holders or those holding high access authorizations.
    2. **Securing the supply chain**
       1. Details must be provided regarding the standard according to which the supply chain is secured, such as NIST SP 800-53 Rev. 5/Nist SP 800-161 Rev. 1, ISO 28000, another international standard, or include the internal procedure, if applicable.
       2. Details must be provided describing the security measures implemented on the supply chain, including the following topics:
          1. Control processes on the inclusion of software from exterior sources and its updates, including identification of vulnerabilities, backdoors, or disposals with harmful capabilities.
          2. Control processes on the inclusion of software from an internal source and its updates, including identification of vulnerabilities, backdoors, or disposals with harmful capabilities.
          3. Details must be provided describing any additional relevant processes or controls.
       3. Details must be provided describing the process of supervision and control over external vendors, including the standards according to which such control is carried out.
    3. **The information accumulated by the manufacturer**
       1. Details must be provided regarding information accumulated by the manufacturer during the provision of the services, such as processing data (as defined below), or access data (as defined below).
       2. Details must be provided regarding the Retention policy and mechanisms used to delete information when required.
       3. To the extent that data is retained by the vendor or the manufacturer, the means of protecting the information must be detailed, as well as the tools and processes aimed at preventing unauthorized access to information.
       4. Details must be provided regarding the processes of providing access to this data and the groups of users authorized to view the information and control processes to identify misuse of these authorizations.
    4. **Configuration Security and Change Management**
       1. The manufacturer operates according to an orderly policy for managing configuration and change involving all systems taking part in the provision of the services, in accordance with accepted and required standards.
       2. Details must be provided regarding the standard according to which these processes are performed, if applicable, including a general description of configuration control and changes control systems, and approval and documentation processes.
       3. Details must be provided regarding controls for preventing unauthorized Downgrade of encryption mechanisms, key management mechanisms, defense systems, or defense services, if applicable.
       4. Details must be provided regarding the method of protecting and controlling development processes, as such secured development process (SDLC) and relevant standards, To the extent that the manufacturer complies with them.
    5. **Limiting Support Access**
       1. Details must be provided regarding the process of supporting the system, identity of supporting sources, whether they are on behalf of the vendor, the manufacturer or the cloud provider, and the process being implemented with the provider and the manufacturer in case of the need of such access, including internal authorization paths, approval processes with the Client, access security, its method of documentation (including registration of log, Session recording), and so on.
       2. Details must be provided regarding whether it is possible to implement a mechanism in which any support access to components used by the Client and which contain or enable access to processing data would be carried out only after implementing a predefined approvals process during the course of which it would be necessary to obtain the approval of the Client’s representative for the support access.
    6. **Risk management**
       1. To the extent that the manufacturer employs an Information Security Manager responsible for securing the information in the proposed services, details must be provided regarding his/her role description and whether he/she is a member of the manufacturer’s management.
       2. Details must be provided regarding the manufacturer’s risk management processes.
       3. Details must be provided regarding the parties carrying out these processes, supervision ranks, escalation ranks for handling issues, and method of handling findings that have not been addressed.
       4. Details must be provided regarding the tools, means, and their method of implementation in order to enable dynamic risk management in accordance with changes in the outline of threats and in the services provided.
    7. **Identification of the Proposed Service**
       1. The service must support standard identification protocols such as SAML, OpenID, OAuth for Single Sign On with the Client’s systems as well as supporting Multi Factor Authentication. Details must be provided regarding supporting identification protocols (such as U2F, FIDO, OTP).
       2. Details must be provided regarding interfacing capabilities with IdP/IAM tools for user management systems and for third party identity management systems.
       3. Details must be provided regarding support for granting individual access on a Role Based Access Control (RBAC) level, and on an Attribute Based Access Control (ABAC) level.
       4. The service must support the reception of users’ details from a central identification system using standard protocols.
    8. **Business Survivability and Continuity (SLA) of the proposed service**
       1. The SLA of the service to be provided from the Israeli region shall be equal to that of the service in any other region. Details must be provided regarding the uptime data to which the manufacturer is committed.
       2. Details must be provided regarding the mechanisms guaranteeing survivability of the service and information, including deployment of the system between various compounds, method of backing the information, maintaining integrity of the backup, inspecting restoration capabilities, meeting various failure scenarios, and so on.
       3. To the extent that backups are carried out outside the cloud environment, details must be provided regarding the mechanism that ensures destruction of out of service memory bases and components (such as their removal from the system, replacement, or in the event of failure).
       4. Details must be provided regarding the manufacturer’s method of controlling the quality of the service provided from the Israeli region and the levels of escalation that are defined in its procedures.
       5. It must be possible to routinely backup or export the **system data** to a base controlled by the Client. Details must be provided regarding the backup format and its compatibility with standard systems available in the market.
    9. **Protecting the Service Infrastructures** 
       1. The manufacturer operates an SOC that monitors its systems on cyber aspects 7/24 (24 hours a day, 365 days a year). Details must be provided regarding the capabilities of the SOC operated by the manufacturer, the SIEM system used, and further components and capabilities used by the SOC in its routine operations. In the event as the service is operated by a sub-contractor, its details must also be provided.
       2. Details must be provided regarding use of means of defense of end points (EPP/EDR/XDR) in the manufacturer’s environment. In the event this exists as a service operated by a sub-contractor (MSSP), its details must also be provided.
       3. Details must be provided regarding the use of automation tools for monitoring and handling events, as well as the manufacturer’s operating methodology (such as SOAR), relevant tools, and their method of implementation.
       4. The incoming and outgoing traffic for the service infrastructure shall be monitored to identify attacks or suspicious activity. Details must be provided regarding the manufacturer’s capabilities in the area and the work processes being implemented by the manufacturer for this purpose.
       5. The manufacturer implements monitoring and work processes in a Privacy by Design configuration, while ensuring minimal exposure of information to human sources. Details must be provided regarding the tools and methods used by the manufacturer in order to implement these processes.
       6. The manufacturer uses tools for continuous monitoring of an infrastructure exposure surface (Attack Surface Management). Details must be provided of all the tools and work processes used.
       7. Details must be provided regarding the means implemented in order to protect the systems used for granting the services from unauthorized changes and the monitoring means implemented by the manufacturer in order to control this.
       8. All proposed infrastructures, systems, and services are updated in all of the manufacturer’s relevant security updates. Details must be provided regarding the updating processes and the frequency of the updates.
       9. All users that are able to access Client’s information regarding those holding Privileged Access, such as: Administrators, Operators, Support, DevOps, and so on., shall be monitored and audited at a high level. Details must be provided regarding the work processes and tools implemented for the above.
       10. Details must be provided regarding the method of protecting access data of the system’s users, including their access control, encryption, and security tools protecting from unauthorized access or leaking.
       11. Details must be provided regarding the method of protecting system management interfaces, partitioning between users, and preventing access of unauthorized sources, including the employees of the provider, manufacturer, or its sub-contractors.
       12. Details must be provided regarding the method of protecting the system’s internal and external API interfaces.
    10. **Security tools used for protecting the proposed services**
        1. Details must be provided regarding advanced automatic analysis tools, including those that integrate AI capabilities, for the identification of suspicious activity in users’ services, exposure attempts, or exposure of sensitive information, and so on.
        2. Details must be provided regarding further control, monitoring, and cyber protection tools used by the manufacturer, which may serve Clients in order to improve the level of protection of their information, such as DLP capabilities, coping with malicious code, and so on.
    11. **Encryption and Management of Keys in the proposed services**
        1. Details must be provided regarding information encryption capabilities in the various service tiers.
        2. All of the system’s data shall be encrypted at rest and in transit, as a default condition. To the extent that the provider believes that this type of encryption is inapplicable, this must be fully explained, including compensating controls, if any.
        3. Details must be provided regarding encryption types and algorithms used by the manufacturer in its services, such as at rest encryption, in transit encryption, and runtime encryption, the standard on which they are based, and external references for algorithmic resilience and encryption protocols.
        4. Details must be provided regarding the method of management and storage of the keys regarding each of the service tiers and the various service types.
        5. Details must be provided regarding support for an interface with key management infrastructures with which the manufacturer interfaces (such as KMS).
        6. To the extent that the manufacturer operates an independent key management infrastructure, details must be provided regarding the proposed solution with an emphasis on fully complying with the FIPS- 140-2 level 2 standard and above.
        7. Details must be provided regarding the system’s ability to work using the Bring Your Own Key configuration, including system protection capabilities, its strengthening, and the user’s ability to control the various parameters of the encryption keys.
        8. All processes of violation, change, replacement, cancellation of keys, and so on., shall be carried out by the Client with no viewing or access ability by the provider or the manufacturer (beyond systems requiring key access for carrying out service operations), or any other party not permitted to do so by the Client.
    12. **Collecting of logs and monitoring**
        1. The Client shall able to receive all runtime and access data to its systems while supporting the transfer of data to the SIEM systems pertaining to the client, the tender administrator or a third party. Details must be provided regarding the method of transfer of logs (online interface, timely file transfer, API, and so on) to supported SIEM systems (such as Chronicle and QRadar) and the scope of support.
        2. Details must be provided regarding possible log sources (such as: infrastructure, applicable infrastructure, application, information security, and so on).
        3. Details must be provided regarding the currency of the information (time as of the occurrence of the event until the information has been transferred), scope of the information, investigation capabilities of the Client or its representative, and so on.
        4. Details must be provided regarding the time frame in which runtime data and access data are saved by the manufacturer, the manufacturer’s policy regarding the saving of such data and its method of protection.
    13. **Investigation**
        1. Details must be provided regarding the manufacturer’s capabilities, tools and work processes in the area of investigating and responding to cyber events in the manufacturer’s systems.
        2. Details must be provided regarding the process of operating Incident Response systems, if any, in the event of the need to investigate a security event, involvement of the cloud provider, response times, resources that are accessible to the Client, interface configuration, and so on.
    14. **Internal control and conformance to standards**
        1. The service must meet least to the following standards:
           1. ISO27001 or SOC 2 AICPA. Details must be provided regarding the standard to which the service conforms.
           2. Details must be provided regarding further standards to which the service conforms, such as: ISO27017, ISO27018, CSA STAR level 2, and so on, if applicable.
        2. Details must be provided regarding the work processes in the organization and systems/tools used by the manufacturer, which are aimed to ensure Compliance of the service with all rules and standards to which it is committed.
        3. Details must be provided regarding supervision ranks, escalation ranks for handling events, and method of handling findings that were not addressed.
    15. **Separation and Segmentation of Clients (Tenants)**
        1. Details must be provided regarding the manufacturer’s capabilities, if applicable, for insulation and differentiation of a specific tenant (client), with reference to the following points:
           1. Method of separation and differentiation of common services and means for preventing data leaks between different tenants, access of users of a certain tenant to the resources of another tenant, separation of management and control, and so on.
           2. Ability to prevent access of users of a specified client to the resources of another client (foreign), except if such access had been approved, even if the user has access authorizations to the foreign client’s resources. Prevention capabilities which are not based on the identification system must be detailed.
           3. Ability to prevent access of a foreign client’s users, to the client’s resources, unless such access has been approved, even if the foreign user has access authorizations to the client’s resources. Prevention capabilities that are not based on the identification system must be detailed.
           4. Ability to create a specific and private address (IP or URI) for the service, to be used by the client’s users or a group of clients, which is not to be used by other clients.

Appendix D – Reference Model

1. All prices shall include a guarantee as required in Chapter 3 to the Central Tender and as specified in the tender documents.
2. The bidder shall enter its bid, in accordance with the prices on the official price list on the Excel sheet enclosed as Addendum D1 to the tender notification.
3. The prices will be determined in the online dynamic bid, pursuant to the terms stipulated herein.

Installation, Implementation, and Maintenance Services

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Clause** | **Quantity for adjusted calculation** | **Maximum rate (including VAT)** | **Remarks** |
| A | Annual maintenance cost, calculated as a percentage of the actual product prices (as of the second year onwards). | 4 | 20% | A total of five years for adjusted calculation in the tender. |

**Remarks:**

1. If the product’s pricing model is subscription-based, the cost will be calculated based on the following model:
   1. The annual subscription price will be multiplied by 5 in accordance with the tender’s calculation horizon, as stipulated above. Therefore, the total procurement and maintenance cost will be suitable for a 5-year comparison period. For example, if the annual subscription price for a certain component is $100, the opening price of the total 5-year cost of that component will be $500, including all procurement and maintenance costs for this period.
   2. The maintenance price will be fixed at 20% of the purchase price and will not be included in the calculation of the proposal cost, nor will this component have any impact on the price or on the discount rate.
   3. The annual subscription prices to be determined at the end of the tender will be valid for each year purchased by the Client, even after the fifth year, and will include all procurement and maintenance costs, as specified in section 2.5.3.3 above.