TERMS OF REFERENCE

ANTI-VIRUS FOR SERVERS

1. SCOPE OF THE PROJECT

The scope of the project shall include the supply, delivery and installation of antivirus intended for servers which include licenses, subscription, warranty and support for one (1) year for the Clark International Airport Corporation.

2. TECHNICAL SPECIFICATIONS

a. **General Requirements**

i. The solution should offer a holistic approach in security with purpose-built extended detection and response (XDR), Attack Surface Risk Management, and Zero Trust capabilities.
ii. The solution must have participated with strong performance and impressive results in MITRE Engenuity ATT&CK® Evaluations
iii. The solution must be named a Leader in the latest Gartner® Magic Quadrant for Endpoint Protection Platforms, Q4 2023
iv. The solution must be named a Leader the latest Forrester Wave™: Endpoint Security, Q4 2023
v. The solution must be named a Leader in the latest Forrester Wave™: Endpoint Detection and Response (EDR), Q2 2022
vi. The solution must be named a Leader in the latest Forrester New Wave™: Extended Detection and Response (XDR), Q4 2021

b. **Prevention Requirements**

i. The solution should offer comprehensive protection against known and unknown threats.
ii. The proposed solution should have but not limited to the following prevention capabilities:
iii. Antimalware with signature/Pattern based detection
    1. Ransomware protection
    2. Machine learning - pre-execution and runtime
    3. Browser exploit protection
    4. Behavior monitoring
    5. Injection protection
    6. Script protection
    7. Anti-exploit
    8. C&C communication prevention
    9. Application control

10. File less malware prevention
11. File/web reputation

iv. The solution should offer a combination of signature-based malware protection, behavioral analysis, and AI/machine-learning based analysis.

v. Machine learning must have Pre-execution intelligence of extracting file features and run-time analysis of file/process behavior to identify threats.

vi. The solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems or on installed software's to provide additional threat protection from programs that exhibit malicious behavior.

vii. The solution must have Anti-exploit module to terminate the program exhibiting abnormal behavior associated with exploit attacks. Solution must be able to detect multiple exploit techniques like memory corruption, logic flaw, malicious code injection/execution.

viii. The solution must provide a protection mechanism against ransomware in the event of a machine becoming compromised and should have feature with documents to be protected from unauthorized encryption or modification.

ix. The solution must be able to create copies of files being encrypted by a ransomware on the endpoint and it must be able to restore the affected files back to their original state.

x. The solution must be able to identify communication over HTTP/HTTPS protocols and commonly used HTTP ports, it must be able to detect/prevent communications to Global C&C's and Allow administrators to create user defined list also.

xi. The solution should have a virtual patching capability and be able to deliver the most-timely vulnerability protection in the industry across a variety of endpoints.

xii. The solution must support host-based firewall with stateful inspection, option to create rules on the basis of Source/Destination/Port/Protocol/Application to provide stateful inspection and high-performance network virus scanning

xiii. "The solution must have an integrated Application Control module to enhance defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing

xiv. on corporate endpoints with a combination of flexible, dynamic policies, whitelisting (default-deny) and lockdown capabilities."

xv. The solution integrated Application Control should provide global and local real-time threat intelligence based on good file reputation data correlated across a global network.

xvi. "The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and

Deny Access. The Devices that are able to be restricted must include but not limited to the following:

1. USB Storage Drives (Also able to disable autorun)
2. CD-ROM
3. Floppy Disk
4. Network Drives

xvii. The solution Device Control capability must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, Com/LPT, Imaging Devices, Wireless Nic, Infrared devices

xviii. The solution must have an integrated Data Loss Prevention capability to provide data leakage prevention.

xix. The solution must have damage cleanup services to provide automated cleanup of the changes made by the malware including network and file-based malicious applications, and virus and worm remnants (Trojans, registry entries, and viral files).

c. **Detection and Correlation Requirements**

i. Should be able to collect and correlate XDR activity data for one or more vectors including but not limited to — endpoints, email, servers, cloud workloads, and networks.

ii. Should include predefined detection models which combine multiple rules, and filters using techniques such as machine learning and data stacking. Should be regularly updated to improve threat detection capabilities and reduce false positive alerts.

iii. Should have the ability to enable or disable detection models and add/configure detection model exceptions based on the organization requirements.

iv. Should allow the creation of custom detection models and custom event filters that define the events the model uses to trigger alerts.

v. The solution should be able to analyze and determine if certain indicators signal an ongoing attack, enabling SOC team to take timely prevention, investigation, and mitigation actions against targeted attack campaigns.

vi. The solution should have the capability to provide recommended actions to harden your environment against future potential attacks.

vii. Should list all the events that are mapped into the MITRE ATT&CK framework, the SOC Analyst can use these events as starting point to do further investigations.

viii. Should provide more context with mapping to the MITRE ATT&CK TTPs for faster detection and higher fidelity alerts.

ix. Should have the capability to write custom search queries, add the saved queries to the watchlist, and automatically execute them against the latest telemetry data on an interval basis.

d. **Investigation and Incident Management Requirements**

i. Should be able to provide consolidated investigation and response capabilities across endpoint, servers, emails, cloud workloads, and networks.
ii. The solution should have an AI-powered chatbot (AI Companion) to guide with the investigations and automatically provide answer to any questions related to cybersecurity.
iii. Generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.
iv. The solution should provide a platform for easier investigation like visual graphical view and timeline of the attack.
v. The solution should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.
vi. The console should provide different search methods, filters, and an easy-to-use Kibana-like query language to identify, categorize, and retrieve search results.

e. **Response Requirements**

i. Add or Remove indicators of compromise to block list including but not limited to File hash, URL, IP address, and Domains.
ii. Automatic and manual collection of forensic evidence from specified endpoints and upload the forensic package back to the management console for further investigation.
iii. Automatic and manual collection of files and objects from specified endpoints.
iv. Remotely connect to an endpoint and dump process memory.
v. Remote isolation of an endpoint but still maintain communication with the management server to continue with investigation.
vi. Ability to remotely connect and execute custom PowerShell or Bash scripts.
vii. Ability to execute custom YARA rules on the specified endpoints.
viii. Ability to execute SQL queries using osquery to obtain system information on the specified endpoints.
ix. Remote shell session capability and be able to execute remote commands.
x. Submit selected file or object for automated analysis in a sandbox, a secure virtual environment.
xi. Ability to view and terminate active processes on a specific endpoint or multiple endpoints.
xii. The solution should provide a unified platform that enables security teams to take immediate response and track actions for both email and endpoints.

f. **Threat Intelligence Requirements**

i. The solution must collect, organize, and provide an up-to-date information resource for active Threat Campaigns and Threat Actors.
ii. Threat Campaign must include information such as Threat Actor profile, Infection Chain, MITRE ATT&CK mapping, Intelligence Data, and Impact Scope.
iii. Campaign Intelligence Data must include - Intelligence Reports, TTPs, Tools, Malicious Software Used, Associated CVEs, and Indicators.
iv. The solution must support automatic and manual sweeping based on vendor curated and third-party custom intelligence to search your environment for indicators of compromise.
v. The solution should allow you to perform sweeps identifying indicators of compromise (IoC) and indicators of attack (IoA).
vi. The solution should allow a SOC analyst to manually add IoCs such as File Hashes, IP Addresses, Domains, and URL's as part of the custom intelligence.
vii. Shall be able to view information about suspicious objects that has been obtained by analyzing the suspicious file in a sandbox, a secure virtual environment.
viii. The solution should allow a SOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds using standards such as STIX and TAXII.

g. **Deployment, Management, and Operations**
i. The solution must support Windows endpoints, including Windows Servers.
ii. The solution must support macOS endpoints.
iii. The solution must support Linux endpoints.
iv. The solution must support for persistent and non-persistent VDI environments.
v. The solution must support multi-session VDI solutions without changing or limiting the functionality of your virtual desktop operating systems
vi. The solution deployment model must support to air-gapped, on- premises, and hybrid deployments.
vii. The solution must support legacy and rare operating systems including but not limited to Windows XP, Windows 7, Red Hat, Solaris, AIX, and others.
viii. The solution should have the capability to automate a variety of actions using Security Playbooks to help reduce workload and speed up security tasks and investigations.
ix. The solution needs to include an ability to build security playbooks against threats and risks, such a blocking the activity of a file, shutting down an endpoint, disconnecting an endpoint from the internet, entering files into quarantine, deleting malicious files and etc.

x. The solution should have the capability to create playbooks from scratch or use built-in templates to suit the organization specific needs.
xi. Security playbook template types should include but not limited to the following XDR threat investigation actions.
    1. Automated Response Playbook
    2. Endpoint Response Actions
    3. Incident Response Evidence Collection
xii. Solution should be capable of integrating with a cybersecurity platform that is capable of managing the organization's Endpoint, Email, Cloud, Network, OT Security, XDR and Zero Trust solution in a single console.
xiii. Provides insights into the organization's security posture using an Executive level dashboard. Must be able show the company's overall risk score, individual asset risks, a view of ongoing attacks and its contributing risk factors.
xiv. Highly customizable dashboard that provides widgets displaying statistics from Attack Surface, Email, Endpoint, Network, SecOps, XDR and Cloud
xv. Solution should be able to display MITRE ATT&CK Mapping for tactics and techniques detected in the organization for the following MITRE ATT&CK matrices.
    1. Enterprise
    2. Mobile
    3. ICS
xvi. The solution should be able to produce manual and scheduled reports that can be customized to display company information and logo. Generated reports should at least support PDF/PPT format and can be sent to specified email recipients.

h. **Infrastructure Requirements**
    i. The solution should provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets.
    ii. The solution should provide 30 days included standard of data retention period
    iii. The solution should provide an option to extend the retention of data for up to 365 days.
    iv. The solution should be cloud-delivered service with an option to deploy and manage within a private cloud.
    v. The solution should offer a credit-based licensing model for flexibility and freedom to deploy additional modules/services without the hassle of individual licenses.
    vi. The solution should be certified with the following international compliance standards:
        1. ISO 27001

2. ISO 27014
3. ISO 27034-1
4. ISO 27017
5. SOC 2/3

i. **API and Third-party Integration Requirements**
   i. The solution must be able to integrate with common SIEM and SOAR products.
   ii. The solution should provide connectors ready to integrate with supported third-party security solutions.
   iii. The solution should also have the capability to integrate with other third-party solutions via API
   iv. The solution should be able to generate API keys utilizing role- based access control for more granular permissions. API keys should have the option to expire and disabled from the management console.
   v. The solution should be able to integrate with 3rd party identity Provider (IdP) solutions for single sign on.
   vi. Solution should be able to integrate with at least one 3rd party solution in the following category.
   vii. Breach Assessment and Simulation
      1. Cloud Services
      2. Firewall and Network
      3. ITSM
      4. SIEM
      5. SOAR
      6. Threat Intel
      7. UEM
      8. Vulnerability Management

j. **Managed Services**
   i. Asset tagging on Helpdesk Monitoring & Ticketing system.
   ii. Unlimited email, phone support for 1 Year/s for any security issues related to the deployed security software / appliance / equipment.
   iii. 4-incident onsite support per year with next business day dispatch of Engineer if problem can't be resolved remotely.
   iv. Scheduled Annual Health Maintenance per Year, log capturing, device physical checking, cleaning and configuration backup whenever is applicable.
   v. Advisory and application of security patches, firmware and any software update release by the Vendor to fix certain bug/s and vulnerabilities.
   vi. 24x7 support coverage with 4- hours remote or phone response time."

k. **Implementation**
   i. Account Creation.
   ii. Management Configuration
   iii. Security Policy Configuration
   iv. AD Integration
   v. Live Testing

3. Supplier Qualification

a. Interested bidder/supplier must be an authorized reseller of the product
b. Interested bidder/supplier must be ISO/IEC 27001:2013 Certified and must provide certificate as proof for passing the Information Security Management System: ISO/IEC 27001:2013.
c. Interested bidder/supplier must be National Privacy Commission (NPC) Registered in compliance with the Data Privacy Act of 2012.

4. Delivery and Installation

After the Notice to Proceed (NTP) is accepted, the service provider will deliver the necessary components, including installation and testing within thirty (30) Calendar Days. The supplier guarantees that the system will function and be available for usage upon completion and testing.

5. Technical Support

a. Monday-Friday, 9:00 am to 5:00 pm email and remote support
b. 8 x 5 technical support service via onsite
c. Security updates and software upgrades within the subscription period.
d. Quarterly visit and system maintenance check-up
e. Technical training on the proper management and best practices on the use of the product/system.

6. Terms of Payment

The service provider shall submit an invoice and be paid in full, subject to deduction of applicable taxes and liquidation damages, with a corresponding issuance of Certificate of Acceptance and Inspection from the MIS / GIS Department.