REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF BUDGET AND MANAGEMENT
GENERAL SOLANO STREET, SAN MIGUEL, MANILA

BIDS AND AWARDS COMMITTEE

Resolution No. 2021-42

WHEREAS, the Department of Budget and Management-Bids and Awards Committee (DBM-BAC) conducted a Public Bidding for the Project, "Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution," with an Approved Budget for the Contract of P5,300,000.00 through the authorized appropriations under the FY 2021 General Appropriations Act, as reflected in the CY 2021 Annual Procurement Plan;

WHEREAS, on June 15, 2021, the Invitation to Bid for the Project was posted on the Philippine Government Electronic Procurement System (PhilGEPS) website, the DBM website, and all DBM bulletin boards;

WHEREAS, two (2) prospective bidders, namely: (i) Accent Micro Technologies, Inc. (AMTI); and (ii) Pronet Systems Integrated Network Solution, Inc., responded to the said Invitation and attended the Pre-bid Conference via videoconferencing on June 22, 2021;

WHEREAS, during the submission and opening of bids on July 6, 2021, only one (1) bidder, AMTI, submitted a bid;

WHEREAS, after preliminary examination of the bid, the DBM-BAC, using non-discretionary "pass/fail" criteria, determined the submission of AMTI as "passed" for complying with all the eligibility and technical requirements as stated in the Bidding Documents;

WHEREAS, after evaluation of the financial component of the bid, the DBM-BAC declared the submission of AMTI as the Single Calculated Bid in the amount of P5,250,000.00;

WHEREAS, after verification, validation, and ascertainment of all statements made and documents submitted by AMTI, using non-discretionary criteria, as stated in the Bidding Documents, it was determined that the submission of AMTI passed all the criteria for post-qualification.

NOW, THEREFORE, for and in consideration of the foregoing premises, the DBM-BAC **RESOLVED**, as it is hereby **RESOLVED**, the following:

1. To declare the bid of Accent Micro Technologies, Inc. for the Project, "Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution," in the amount of P5,250,000.00 as the Single Calculated and Responsive Bid, in accordance with Section 34.4 in relation to Section 36 of the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184; and

2. To recommend to the DBM Secretary, as the Head of the Procuring Entity, that the contract for the Project be awarded to Accent Micro Technologies, Inc. in the above-mentioned amount, in accordance with Section 37.1.1 of the 2016 Revised IRR of RA No. 9184.

ADOPTED, this 13th day of July 2021 at the Department of Budget and Management, General Solano St., San Miguel, Manila.

Digitally signed by Luis S. Indefenso

LUIS S. INDEFONSO
End-user Representative

Digitally signed by Virgilio A. Umpacan, Jr.

VIRGILIO A. UMPACAN JR.
B.U.D.G.E.T. Representative

Digitally signed by Dante B. De Chavez

DANTE B. DE CHAVEZ
Member

Digitally signed by Rowel D. Escalante

ROWEL D. ESCALANTE
Member

Digitally signed by Ryan S. Lita

RYAN S. LITA
Member

Digitally signed by Andrea Celene M. Magtalas

ANDREA CELENE M. MAGTALAS
Vice Chairperson

Digitally signed by Janet B. Abuel

JANET B. ABUEL
Chairperson

[✓] Approved

[ ] Disapproved

WENDEL E. AVISADO
Secretary

Date: 14 July 2021

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF BUDGET AND MANAGEMENT
GENERAL SOLANO STREET, SAN MIGUEL, MANILA

NOTICE OF AWARD

JUL 21 2021

MR. CHRISTOPHER B. GARCIA
Accent Micro Technologies, Inc.
8/F East Tower
Philippine Stock Exchange Center
Exchange Road, Ortigas Center
Pasig City

Dear **Mr. Garcia**:

We are pleased to inform you that the contract for the Project, "Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution," is hereby awarded to Accent Micro Technologies, Inc. in the amount of P5,250,000.00.

In this regard, you are hereby required to post a performance security, which shall remain valid until the issuance of the Certificate of Final Acceptance by the Department of Budget and Management (DBM), in the amount and form prescribed in Section 39 of the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act No. 9184 (the Government Procurement Reform Act).

Pursuant to Section 37.2.1 of the same IRR, you have ten (10) calendar days from receipt of this Notice to post the said performance security and enter into a contract with the DBM.

Thank you and God Bless.

Very truly yours,

WENDEL E. AVISADO
Secretary

21-02275

Received by:

July 22, 2021

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF BUDGET AND MANAGEMENT
GENERAL SOLANO STREET, SAN MIGUEL, MANILA

NOTICE TO PROCEED

10 AUG 2021

MR. CHRISTOPHER B. GARCIA
Accent Micro Technologies, Inc.
8/F East Tower
Philippine Stock Exchange Center
Exchange Road, Ortigas Center
Pasig City

Dear **Mr. Garcia**:

This is to inform your company that performance of the obligations specified in the attached Contract for the Project, "Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution," shall commence upon receipt of this Notice to Proceed in accordance with Section 37.4 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184 (The Government Procurement Reform Act).

Thank you and God Bless.

Very truly yours,

WENDEL E. AVISADO
Secretary

21-02801

I acknowledge receipt and acceptance of this Notice on AUG 13, 2021

Name of Authorized Representative: Christopher Garcia

Signature: _____

CONTRACT No. 2021-25
RENEWAL OF LICENSES FOR THE SUBSCRIPTION TO ADVANCED ENDPOINT SECURITY SOLUTION

This CONTRACT made and entered into by and between the following:

DEPARTMENT OF BUDGET AND MANAGEMENT, a government agency created by virtue of the laws of the Republic of the Philippines, with principal office address at General Solano St., San Miguel, Manila, represented herein by its **SECRETARY, WENDEL E. AVISADO**[1], hereinafter called the **"DBM"**;

- and –

ACCENT MICRO TECHNOLOGIES, INC., a corporation duly organized and existing under the laws of the Republic of the Philippines, with office address at 8/F East Tower, Philippine Stock Exchange Center, Exchange Road, Ortigas Center, Pasig City, represented by its **AUTHORIZED REPRESENTATIVE, CHRISTOPHER B. GARCIA**, hereinafter referred to as the **"SUPPLIER"**;

Collectively, the **"PARTIES"**;

WITNESSETH:

WHEREAS, the DBM conducted a public bidding for the Project, "Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution," and the bid of the Supplier was declared as the Single Calculated and Responsive Bid in the amount of Five Million Two Hundred Fifty Thousand Pesos (P5,250,000.00), hereinafter called the "Contract Price";

WHEREAS, pursuant to Sections 37 and 39 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184, the Notice of Award was issued to the Supplier last July 22, 2021, and the Supplier posted its performance security in the form of a Irrevocable Domestic Standby Letter of Credit on July 29, 2021, in the amount of Two Hundred Sixty Two Thousand Five Hundred only (P 262,500.00);

NOW, THEREFORE, for and in consideration of the foregoing premises, the parties hereby mutually stipulate and agree as follows:

1. In this Contract, words and expressions shall have the same meanings as are respectively assigned to them in the General and Special Conditions of Contract referred to in Annex D and E, respectively.

2. The following documents shall form and be read and construed as part of this Contract:

Annex	A	-	Bid Form
	B	-	Schedule of Requirements
	C	-	Technical Specifications
	D	-	General Conditions of Contract
	E	-	Special Conditions of Contract
	F	-	Notice of Award
	G	-	Performance Security

[1]Per DBM Office Order No. 366 dated July 30, 2021, Undersecretary Tina Rose Marie L. Canda was designated as Officer-in-Charge from August 2-13, 2021, which includes the authority to undertake duties and responsibilities as Head of the Procuring Entity in accordance with the provisions of Republic Act No. 9184.

3. In consideration of the payments to be made by the DBM to the Supplier, the Supplier hereby covenants with the DBM to provide the Goods and Services, which is the Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution, and to remedy defects therein in conformity with the provisions of the Contract.

4. The DBM hereby covenants to pay the Supplier, in consideration of the provision of the Goods and Services, which is the Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution, and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the time and in the manner prescribed by the Contract.

5. The period for the performance of the obligations under this Contract shall not go beyond the validity of the appropriation for this Project.

6. Entire Agreement. All parties agree that this Contract, including the attached Annexes, contains their full agreement and supersedes all previous agreements, either written or oral, if there are any. No agreements, understandings, commitments, discussions, warranty, representations or other covenants, whether oral or written, between the parties are included in this Contract, including the attached Annexes, except as set forth herein.

IN WITNESS WHEREOF, the parties hereto have signed this Contract on this ___ day of _____, 2021 at General Solano St., San Miguel, Manila, Philippines.

DEPARTMENT OF BUDGET AND MANAGEMENT	**ACCENT MICRO TECHNOLOGIES, INC.**
by:	by:
WENDEL E. AVISADO[2] *Secretary* **TINA ROSE MARIE L. CANDA** **Undersecretary**	**CHRISTOPHER B. GARCIA** *Authorized Representative*

SIGNED IN THE PRESENCE OF

ANDREA CELENE M. MAGTALAS *Director IV* Information and Communications Technology Systems Service	CHERRY ANN MACASPAC SERVICES - ACCOUNT MANAGER

[2] Id.

ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)
C I T Y O F M A N I L A) *S.S.*

BEFORE ME, a Notary Public for and in the City of MANILA, Philippines on this AUG 11 2021 day of _____, 2021 personally appeared the following:

NAME	VALID ID	VALID UNTIL
WENDEL E. AVISADO[3]	DBM ID No. 4601	
TINA ROSE MARIE L. CANDA	DBM ID NO. 0290	
Undersecretary **CHRISTOPHER B. GARCIA**	Passport # P4477365B	20 JAN 2030

known to me to be the same persons who executed the foregoing Contract and who acknowledged to me that the same is their free and voluntary act and deed and of the entities they respectively represent.

This CONTRACT for the Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution was signed by the parties, and their material witnesses on each and every page thereof.

WITNESS MY HAND AND SEAL this ____ day of AUG 11 2021, 2021.

ATTY. GARY CAMITAN AURE
NOTARY PUBLIC, ROLL NO. 60777
PTR No. 5826455 Issued on Jan. 4, 2021 until Dec. 31, 2021 Manila
IBP Lifetime No. 014599 Issued on Feb. 2, 2016
Commission No. 2020-021 Issued on Jan. 31, 2020 Until Dec. 31, 2021 Manila
MCLE No. VI-0006705 Issued on Feb. 20, 2018 at Pasig City Valid Until April 14, 2022
Office Address: GF YMCA Building, 350 Antonio Villegas Street, Ermita, Manila

Doc. No 154;
Page No 31;
Book No L0;
Series of 2021.

[3] Id.

Bid Form for the Procurement of Goods

[shall be submitted with the Bid]

BID FORM

Date: **June 28, 2021**
Project Identification No: **DBM-2021-35**

To: DEPARTMENT OF BUDGET AND MANAGEMENT
DBM Bldg. III, General Solano St.
San Miguel, Manila

Having examined the Philippine Bidding Documents (PBDs) including the Supplemental or Bid Bulletin Numbers (None), the receipt of which is hereby duly acknowledged, we, the undersigned, offer **Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution** in conformity with the said PBDs for the sum of **Five Million Two Hundred Fifty Thousand pesos only (Php 5,250,000.00)** or the total calculated bid price, as evaluated and corrected for computational errors, and other bid modifications in accordance with the details provided herein and made part of this Bid. The total bid price includes the cost of all taxes, which are itemized herein.

Particulars	Units	Unit Cost	Total Price (inclusive of VAT)
Licenses for the Subscription to Advanced Endpoint Security Solution and its components	1,500 licenses	Php 3,500.00 / license cost	Php 5,250,000.00

If our Bid is accepted, we undertake:

a. to deliver the goods in accordance with the delivery schedule specified in the Schedule of Requirements of the Philippine Bidding Documents (PBDs);

b. to provide a performance security in the form, amounts, and within the times prescribed in the PBDs;

c. to abide by the Bid Validity Period specified in the PBDs and it shall remain binding upon us at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your Notice of Award, shall be binding upon us.

We understand that you are not bound to accept the Lowest Calculated Bid or any Bid you may receive.

We certify/confirm that we comply with the eligibility requirements pursuant to the PBDs.

The undersigned is authorized to submit the bid on behalf of Accent Micro Technologies, Inc. as evidenced by the attached Duly Notarized Secretary's Certificate. We acknowledge that failure to sign each and every page of this Bid Form, shall be a ground for the rejection of our bid.

Name: **CHRISTOPHER B. GARCIA**
Legal Capacity: **AVP – PSG Head**

Signature: _____
Duly authorized to sign the Bid for and behalf of: **Accent Micro Technologies, Inc.**
Date: **June 28, 2021**

Section VI. Schedule of Requirements

The delivery schedule stipulates hereafter the date of delivery to the project site.

Item	Description	Quantity	Schedule
1	Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution and its components in accordance with Annex "A" (Detailed Technical Specifications)	1,500 licenses	The subscription period shall be from September 25, 2021 to September 24, 2022.

* The performance of the obligations under the Contract shall not go beyond the validity of the appropriation for the Project.

I hereby certify to comply and deliver all the above requirements.

Accent Micro Technologies, Inc. — Christopher B. Garcia — June 28, 2021

Name of Company/Bidder **Signature Over Printed Name of Representative** **Date**

Section VII. Technical Specifications

Bidders must state here either "Comply" or any equivalent term in the column "Bidder's Statement of Compliance" against each of the individual parameters of each "Specification."

	Specifications	Bidder's Statement of Compliance
I.	**Objective** *(see attached Annex "A" Detailed Technical Specifications, item 2.0)*	Comply
II.	**Subscription Period** *(see attached Annex "A" Detailed Technical Specifications, item 3.0)*	Comply
III.	**Specifications** *(see attached Annex "A" Detailed Technical Specifications, item 4.0)*	Comply
IV.	**Scope of Work and Services** *(see attached Annex "A" Detailed Technical Specifications, item 5.0)*	Comply
V.	**Service Level Agreement** *(see attached Annex "A" Detailed Technical Specifications, item 6.0)*	Comply
VI.	**Warranties of the Contractor** *(see attached Annex "A" Detailed Technical Specifications, item 7.0)*	Comply
VII.	**Confidentiality of Data** *(see attached Annex "A" Detailed Technical Specifications, item 8.0)*	Comply
VIII.	**Terms of Payment** *(see attached Annex "A" Detailed Technical Specifications, item 9.0)*	Comply
IX.	**Pre-Termination of Contract** *(see attached Annex "A" Detailed Technical Specifications, item 10.0)*.	Comply

I hereby certify to comply with all the above Technical Specifications.

Accent Micro Technologies Inc.	Christopher B. Garcia	June 28, 2021
Name of Company/Bidder	**Signature Over Printed Name of Representative**	**Date**

DETAILED TECHNICAL SPECIFICATIONS

1.0 PROJECT TITLE

Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution

2.0 OBJECTIVE

To continue the comprehensive and advanced endpoint security platform based on next generation cybersecurity technologies, endpoint detection and response, unknown malware analysis and managed protection for the DBM users' end devices and application servers.

3.0 SUBSCRIPTION PERIOD

The subscription period for the Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution shall be for twelve (12) months (i.e., September 25, 2021 - September 24, 2022).

4.0 SPECIFICATIONS

4.1 The CONTRACTOR shall provide licenses and support services for the following Advanced Endpoint Security Solution features:

- 4.1.1 Endpoint
  - 4.1.1.1 Able to support a wide range of Windows operating systems including Windows Servers 2016.
  - 4.1.1.2 Able to support Mac OS and Linux including Linux Containers.
  - 4.1.1.3 Able to support both Workstations, Servers and Android with single license.
  - 4.1.1.4 Signature-less solution.
  - 4.1.1.5 Microsoft Windows Security Center Certified or recognized.
  - 4.1.1.6 Able to protect proprietary applications such as in-house applications.
- 4.1.2 Management
  - 4.1.2.1 Cloud based management
  - 4.1.2.2 Capability to report all security incidents back to management immediately as long as the endpoint is connected to the management.
  - 4.1.2.3 Web-based Graphical User Interface (GUI).
  - 4.1.2.4 Able to manage policy for mobile (e.g., Android) in one single console.
  - 4.1.2.5 Allow user to upgrade endpoint without third party software or tool.
  - 4.1.2.6 Malware file report view online or download as PDF.
  - 4.1.2.7 Capability for administrator to create exception directly from security event.
  - 4.1.2.8 2FA capability without need of customer integration.
  - 4.1.2.9 Grouping capability as following but not limited to:
    - 4.1.2.9.1 Static – select from existing connected endpoints
    - 4.1.2.9.2 Dynamic – by defined condition based on Endpoint name, Domain, IP Addresses, VDI, agent version, and the Operating System on Endpoints.
- 4.1.3 Exploit Prevention
  - 4.1.3.1 Prevention against exploit kit that do fingerprinting through browser (e.g., Internet Explorer and Edge).

4.1.3.2 Prevention against exploit that attack the operating system kernel through kernel privilege escalation.
4.1.3.3 Prevent attacks which change the execution order of a process by redirecting an asynchronous procedure call (APC) to point to the attacker's malicious shellcode.
4.1.3.4 Real-time prevention against exploits of application vulnerabilities by blocking through core exploit techniques not limited to Software Logic Flaws, Memory Corruptions, code execution, DLL Hijacking, etc.
4.1.3.5 Protect the systems without knowing the CVE numbers
4.1.3.6 Prevent zero-day or undiscovered exploits of any application vulnerabilities by blocking through core exploits techniques.
4.1.3.7 Capability to perform exploit monitoring and prevention based on core exploit techniques without connection to the Management Server and/or Cloud Service or without relying on signatures.
4.1.3.8 Collect forensic data like process name, file source and path, time stamp, memory dump, operating system version, user ID, vulnerable application version while terminate the particular process that under attack.
4.1.3.9 Utilize core exploit technique to prevent or block. It shall not be based on signatures or reputation of the file.
4.1.3.10 The exploit technique modules shall be able to apply to known and popular applications as well as authorized unknown or in-house developed applications.
4.1.3.11 Provide protection against exploit including Mac OS, Windows, Linux and processes running in Linux Containers.
4.1.3.12 Provide automated forensic memory dump analysis to allow administrators to quickly understand exploit events.
4.1.3.13 Provide Behavior Analytics capability to prevent or block suspicious activities which may or may not relate to exploit.

4.1.4 Malware Prevention
4.1.4.1 Provide protection against malicious DLL files.
4.1.4.2 Provide anti-ransom ware capability through creation of decoy file and not using customer live file.
4.1.4.3 Support protection against the execution of malicious executable.
4.1.4.4 Capability to restrict files and applications execution on or from local folder, network folder, external media (e.g., USB Drive and Optical Media).
4.1.4.5 Capability to restrict files and applications from loading another process that is unknown or in the background (a.k.a. child processes).
4.1.4.6 Signature-less type of technology to prevent malware.
4.1.4.7 Dynamic analysis technology (e.g., Sandbox) to identify unknown malicious executable including DLL.
4.1.4.8 Machine Learning technology to prevent malware on Windows, Mac OS, Linux, Linux Containerized processes, and Android.
4.1.4.9 Multi-layer prevention technology that includes, but not limited to, sandbox, machine learning and restriction.

4.1.5 Unknown Malware Analysis
4.1.5.1 Cloud sandbox with NO additional cost.
4.1.5.2 Capability to prevent unknown or zero-day malware when the endpoint is in offline stage (no internet or management connection).
4.1.5.3 Capability to prevent unknown file or application through restriction policy.

4.1.5.4 Capability to prevent unknown file from executing until the file has been verified.
4.1.5.5 Capability to prevent executable file by customer provided hashes.
4.1.5.6 Capability to identify and prevent greyware.
4.1.5.7 Automatically submit unknown file to sandbox without the need of administrator intervention.
4.1.5.8 Capability to quarantine unknown and zero malware.
4.1.5.9 Identify and prevent sophisticated attacks that utilize legitimate processes and actions for malicious activity based on run-time behavior.

4.1.6 Detection and Response
4.1.6.1 Allow security administrator to hunt using Indicator of Compromise or Combine of multiple behavior of the Indicator.
4.1.6.2 Capability to display the attack timeline.
4.1.6.3 Capability to show the suspicious file was loaded or launch by which parent processes.
4.1.6.4 Shall not limit to only endpoint but also able to show and correlate network data from firewall.
4.1.6.5 Provide the behavior recording capability like network and user behavior analysis through solution provided sensors and not through Netflow data.
4.1.6.6 Endpoint Detection and Response, network user behavior analysis and Prevention should be single endpoint agent.
4.1.6.7 Capability to isolate the endpoint.
4.1.6.8 Capability to blacklist suspicious file from the investigation console.
4.1.6.9 Profile the environment for behavior detection based on but not limited to peer, time and entity.
4.1.6.10 Able to detect behavior as following but not limited to:
4.1.6.10.1 Command and Control
4.1.6.10.2 Reconnaissance
4.1.6.10.3 Lateral Movement
4.1.6.10.4 Data Exfiltration
4.1.6.11 Network and User behavior analysis shall not be based on Net Flow. It shall base on AI or Machine Learning technology with combine of Endpoint, Logs and Networks.
4.1.6.12 Able to detect file-less attack and script based attack.
4.1.6.13 Query builder for threats hunting based on the following but not limited to:
4.1.6.13.1 Process
4.1.6.13.2 File
4.1.6.13.3 Hash (MD5 and SHA256)
4.1.6.13.4 Network (IP addresses, port, protocol, country)
4.1.6.13.5 Registry
4.1.6.13.6 Signer
4.1.6.14 Provide the visualization flow of the chain of events. It must include processes in the chain that happen before the malicious process.
4.1.6.15 Able to create behavior indicators to identify malicious intent.
4.1.6.16 Able to detect threats on unmanaged device or network anomalies based on peer behavior.
4.1.6.17 Capability to chain detection from network, endpoint and cloud.
4.1.6.18 Allow administrator to create custom detection rules to adapt based on environment.
4.1.6.19 Live remote and remote isolation as response.
4.1.6.20 Process termination capability.

4.1.6.21 Capability to assign and mark the stage of investigation of specific incident.

4.1.7 Reporting

4.1.7.1 Natively built-in dashboard to monitor the following:

4.1.7.1.1 Unresolved Security Events in the defined timeframe with different severities.

4.1.7.1.2 The OS platform and the number of managed agents.

4.1.7.1.3 The endpoint license consumption status and its expiry date.

4.1.7.2 Monitor the health of the individual endpoints including but not limited to:

4.1.7.2.1 Endpoint Hostname

4.1.7.2.2 User

4.1.7.2.3 Status

4.1.7.2.4 Underlying OS

4.1.7.2.5 Agent Version

4.1.7.2.6 Last Seen Time

4.1.7.3 High-level summary of the security and deployment status of endpoints. The report can be scheduled to run on a recurring basis and on-demand. The report shall be able to optionally send to one or more e-mail addresses.

4.1.8 Forensics

4.1.8.1 Support the collection of forensic data captured by the advanced endpoint solution to a centralized location.

4.1.8.2 Automatic collection of the following forensic information for further investigation purposes:

4.1.8.2.1 Memory Dump

4.1.8.2.2 Accessed Files

4.1.8.2.3 Loaded Modules

4.1.8.2.4 Accessed URI

4.1.8.2.5 Ancestor Processes

4.1.8.3 Capability to view high level system information about the endpoint after the threat has been detected and also provide the capability to retrieve the prevention data for further analysis and investigation.

5.0 SCOPE OF WORK AND SERVICES

5.1 The CONTRACTOR shall conduct pre-implementation meeting with DBM representatives prior to the renewal of the licenses.

5.2 The CONTRACTOR shall renew the **1,500 licenses** of Advanced Endpoint Security Solution and its components on **September 25, 2021.**

5.3 Technical Support

5.3.1 The CONTRACTOR must be able to provide a 3-tier support:

5.3.1.1 Local reseller as the first-level of support

5.3.1.2 Distributor as the second-level of support

5.3.1.3 Principal as the third-level of support

5.3.2 The CONTRACTOR shall provide/render twenty-four hours a day, seven days a week (24x7) technical support services. Technical support can be delivered in a form of telephone call, electronic mail, online and/or on-site support.

The CONTRACTOR shall resolve every problem within six (6) hours after it was reported by DBM. It shall refer to a condition wherein the reported problem is resolved by the CONTRACTOR to the satisfaction of the DBM. Problem and resolution shall be logged in the DBM Help Desk Facility.

5.4 A Certificate of Acceptance shall be issued by the Director of Information and Communication Technology Systems Service (ICTSS).

6.0 SERVICE LEVEL AGREEMENT

6.1 DBM shall maintain a Service Level Agreement (SLA) with the CONTRACTOR, with provisions for liquidated damages for their non-compliance.

Component	Description	Liquidated Damages
6.1.1 Renewal	The CONTRACTOR shall renew the **1,500 licenses** of Advanced Endpoint Security Solution and its components on September 25, 2021.	One (1) % of the total contract price shall be imposed for everyday of delay.
6.1.2 Technical Support	The CONTRACTOR shall provide/render twenty-four hours a day, seven days a week (24x7) technical support services. Technical support can be delivered in a form of telephone call, electronic mail, online and/or on-site support. The CONTRACTOR shall resolve every problem within six (6) hours after it was reported by DBM. It shall refer to a condition wherein the reported problem is resolved by the CONTRACTOR to the satisfaction of the DBM. Problem and resolution shall be logged in the DBM Help Desk Facility.	$1/10^{th}$ of 1% of the total contract price shall be imposed for every hour of delay.

7.0 WARRANTIES OF THE CONTRACTOR

7.1 The CONTRACTOR warrants that it shall conform strictly to the terms and conditions of this technical specification.

7.2 The CONTRACTOR in the performance of its services shall secure, maintain at its own expense all registration, licenses, or permits required by National or Local Laws and shall comply with the rules, regulations, and directives of Regulatory Authorities and Commissions. The CONTRACTOR undertakes to pay all fees or charges payable to any instrumentality of government or to any other duly constituted authorities relating to the use or operation of the installation.

7.3 The CONTRACTOR shall neither assign, transfer, pledge, nor subcontract any part or interest to the contract being bidded out.

7.4 The CONTRACTOR shall identify the certified technical support personnel that will be given authority to access the advanced endpoint security solution management console and will perform technical support services.

7.5 The CONTRACTOR shall provide services which shall include technical support and technical trainings which shall be covered by a special bank guarantee equivalent to 5% of the total contract price. The said amount shall be released after the lapse of the subscription period. Provided that all conditions imposed under the contract have been fully met.

8.0 CONFIDENTIALITY OF DATA

8.1 All project personnel of CONTRACTOR shall be required to sign a Non-Disclosure Agreement (NDA).

8.2 The DBM Enterprise Network System, its component, parts and all products, product samples and specifications, data, ideas, technology, and technical/non-technical materials, all or any which may be derived from any of the foregoing are confidential.

8.3 The CONTRACTOR agrees to hold the Proprietary Information in strict confidence. The CONTRACTOR furthermore agrees not to reproduce, translate or disclose the Proprietary Information to third parties without prior written approval of the DBM.

9.0 TERMS OF PAYMENT

9.1 The CONTRACTOR shall be paid upon provision of licenses and support services of this Project subject to the required Final Withholding VAT (Services) of five percent (5%) and Expanded Withholding Tax of two percent (2%).

9.2 Payment shall be made within a reasonable time from the submission of the documentary requirements such as but not limited to the following, based on existing accounting and auditing laws, rules and regulations:

9.2.1 Sales Invoice/Billings
9.2.2 Certificate of Acceptance issued by ICTSS Director
9.2.3 Non-Disclosure Agreement

No advance payment shall be made as provided for in Section 88 of Presidential Decree No. 1445 (Government Auditing Code of the Philippines).

10.0 PRE-TERMINATION OF CONTRACT

The contract for the Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution may be pre-terminated by the DBM for any violation of the terms thereof. In case of pre- termination, the CONTRACTOR shall be notified by the DBM thirty (30) days prior to actual pre- termination.

paloalto NETWORKS | CORTEX

Business Benefits

- **Detect advanced attacks with analytics:** Uncover threats with AI, behavioral analytics, and custom detection rules.
- **Reduce alerts by 98%:** Avoid alert fatigue with a game-changing unified incident engine that intelligently groups related alerts.
- **Investigate eight times faster:** Verify threats quickly by getting a complete picture of attacks with root cause analysis.
- **Stop attacks without degrading performance:** Obtain the most effective endpoint protection available with a lightweight agent.
- **Maximize ROI:** Use existing infrastructure for data collection and control to lower costs by 44%.

Cortex XDR

Safeguard Your Entire Organization with the Industry's First Extended Detection and Response Platform

Security teams are inundated with inaccurate, incomplete alerts. Today's siloed security tools force analysts to pivot from console to console to piece together investigative clues, resulting in painfully slow investigations and missed attacks. Even though they've deployed countless tools, teams still lack the enterprise-wide visibility and deep analytics needed to find threats. Faced with a shortage of security professionals, teams must simplify operations.

Prevent, Detect, Investigate, and Respond to All Threats

Cortex® XDR™ is the world's first extended detection and response platform that integrates endpoint, network, and cloud data to stop sophisticated attacks. It unifies prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency. Combined with our Managed Threat Hunting service, Cortex XDR gives you round-the-clock protection and industry-leading coverage of MITRE ATT&CK techniques.

Block the Most Endpoint Attacks with Best-in-Class Prevention

The Cortex XDR agent safeguards endpoints from malware, exploits, and fileless attacks with industry-best, AI-driven local analysis and behavior-based protection. Organizations can stop never-before-seen threats with a single cloud-delivered agent for endpoint protection, detection, and response. The agent shares protections across network and cloud security offerings from Palo Alto Networks to provide ironclad, consistent security across the entire enterprise.

Detect Stealthy Threats with Machine Learning and Analytics

Cortex XDR identifies evasive threats with unmatched accuracy by continuously profiling user and endpoint behavior with analytics. Machine learning models analyze data from Palo Alto Networks and third-party sources to uncover stealthy attacks targeting managed and unmanaged devices.

Investigate and Respond at Lightning Speed

Cortex XDR accelerates investigations by providing a complete picture of every threat and automatically revealing the root cause. Intelligent alert grouping and alert deduplication simplify triage and reduce the experience required at every stage of security operations. Tight integration with enforcement points lets analysts respond to threats quickly.

Key Capabilities

Safeguard Your Assets with Industry-Best Endpoint Protection

Prevent threats and collect data for detection and response with a single, cloud native agent. The Cortex XDR agent offers a complete prevention stack with cutting-edge protection for exploits, malware, ransomware, and fileless attacks. It includes the broadest set of exploit protection modules available to block the exploits that lead to malware infections. Every file is examined by an adaptive AI-driven local analysis engine that's always learning to counter new attack techniques. A Behavioral Threat Protection engine examines the behavior of multiple, related processes to uncover attacks as they occur. Integration with the Palo Alto Networks WildFire® malware prevention service boosts security accuracy and coverage. Visit us online to read more about endpoint protection.

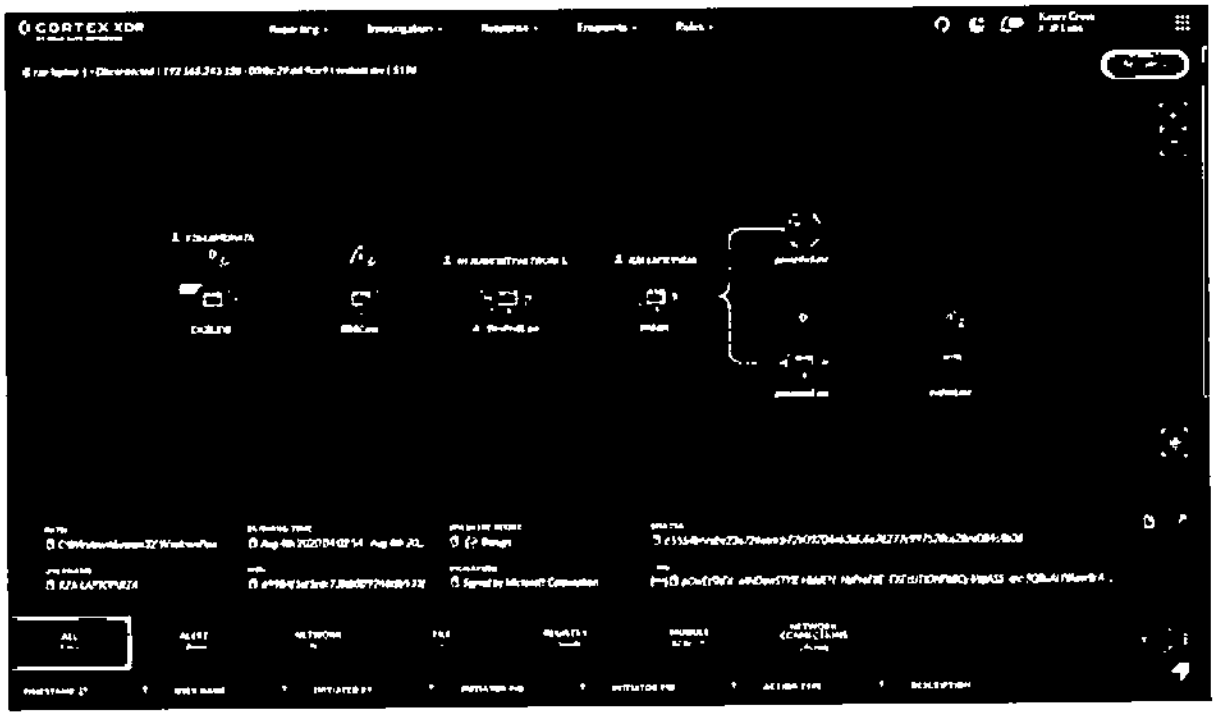

Figure 1: Cortex XDR triage and investigation view

Securely Manage USB Devices

Protect your endpoints from malware and data loss with Device Control. The Cortex XDR agent allows you to monitor and secure USB access without needing to install another agent on your hosts. You can restrict usage by vendor, type, endpoint, and Active Directory® group or user. Granular policies allow you to assign write or read-only permissions per USB device.

Protect Endpoint Data with Host Firewall and Disk Encryption

Reduce the attack surface of your endpoints. With host firewall and disk encryption capabilities, you can lower your security risks as well as address regulatory requirements. The Cortex XDR host firewall enables you to control inbound and outbound communications on your Windows® and macOS® endpoints. Additionally, you can apply BitLocker® or FileVault® encryption on your endpoints by creating disk encryption rules and policies. Cortex XDR provides full visibility into endpoints that were encrypted and lists all encrypted drives. Host firewall and disk encryption capabilities let you centrally configure your endpoint security policies from the Cortex XDR management console.

Get Full Visibility with Comprehensive Data

Break security silos by integrating all data. Cortex XDR automatically stitches together endpoint, network, and cloud data to accurately detect attacks and simplify investigations. It collects data from Palo Alto Networks products as well as third-party logs and alerts, enabling you to broaden the scope of intelligent decisions across all network segments. Third-party alerts are dynamically integrated with endpoint data to reveal root cause and save hours of analysts' time. Cortex XDR examines logs collected from third-party firewalls with behavioral analytics, enabling you to find critical threats and eliminate any visibility blind spots.

Discover Threats with Continuous ML-Based Threat Detection

Find stealthy threats with analytics and out-of-the-box rules that deliver unmatched MITRE ATT&CK coverage. Cortex XDR automatically detects active attacks, allowing your team to triage and contain threats before the damage is done. Using machine learning, Cortex XDR continuously profiles user and endpoint behavior to detect anomalous activity indicative of attacks. By applying analytics to an integrated set of data, including security alerts and rich network, endpoint, and cloud logs, Cortex XDR meets and exceeds the detection capabilities of siloed network traffic analysis (NTA), endpoint detection and response (EDR), and user behavior analytics (UBA) tools. Automated detection works all day, every day, providing you peace of mind.

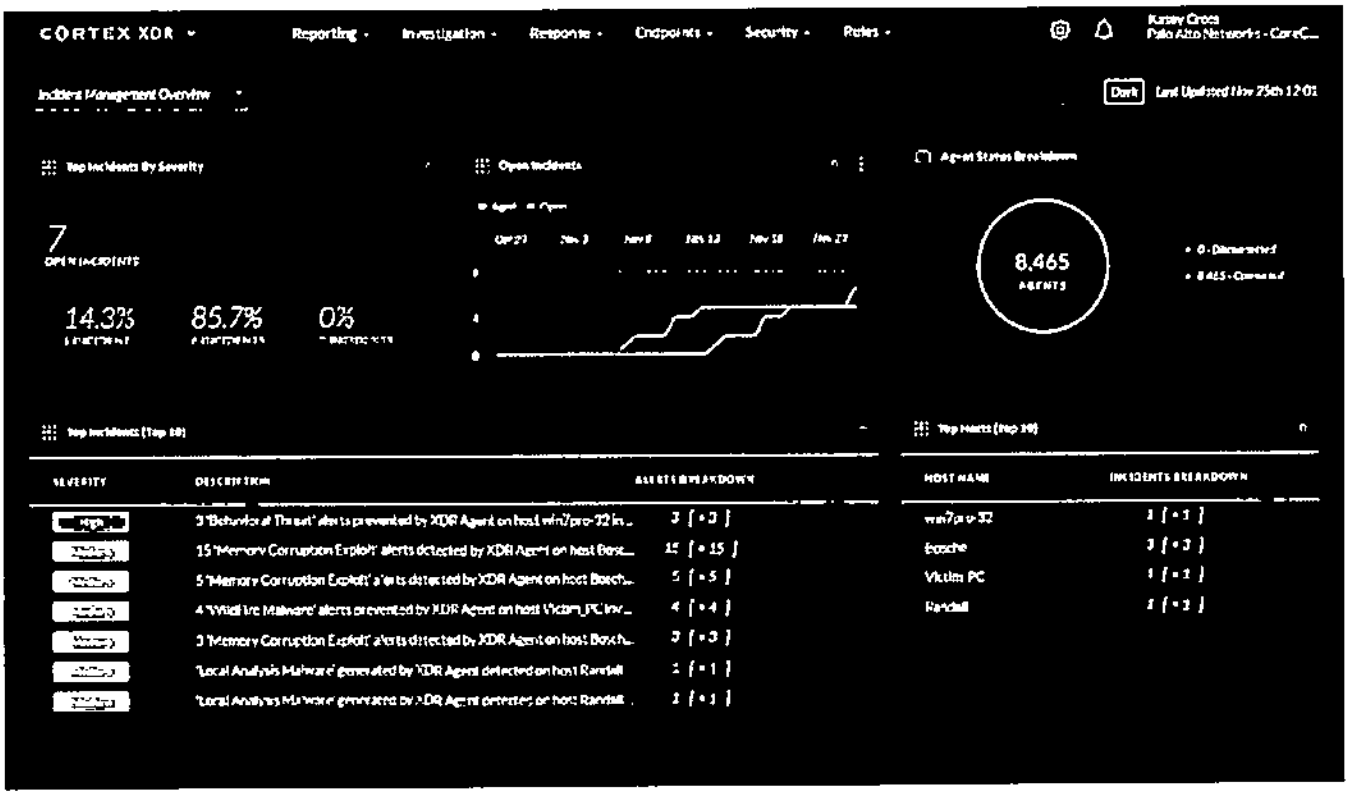

Figure 2: Customizable dashboard

Investigate Eight Times Faster

Automatically reveal the root cause of every alert. With Cortex XDR, your analysts can examine alerts from any source—including third-party tools—with a single click, streamlining investigations. Cortex XDR automatically reveals the root cause, reputation, and sequence of events associated with each alert, lowering the experience level needed to verify an attack. By consolidating alerts into incidents, Cortex XDR slashes the number of individual alerts to review and alleviates alert fatigue. Each incident provides a complete picture of an attack, with key artifacts and integrated threat intelligence details, accelerating investigations.

Hunt for Threats with Powerful Search Tools

Uncover hidden malware, targeted attacks, and insider threats. Your security team can search, schedule, and save queries to identify hard-to-find threats. Flexible searching capabilities let your analysts unearth threats using an intuitive Query Builder as well as construct advanced queries and visualize results with XQL Search. By integrating threat intelligence with an extensive set of security data, your team can catch malware, external threats, and malicious insiders. An Asset Management feature streamlines network management and reveals potential threats by showing you all the devices in your environment, including managed and unmanaged devices.

Coordinate Response Across Endpoint, Network, and Cloud Enforcement Points

Stop threats with fast and accurate remediation. Cortex XDR lets your security team instantly contain endpoint, network, and cloud threats from one console. Your analysts can quickly stop the spread of malware, restrict network activity to and from devices, and update prevention lists like bad domains through tight integration with enforcement points. The powerful Live Terminal feature lets Tier 1 analysts swiftly investigate and shut down attacks without disrupting end users by directly accessing endpoints; running Python®, PowerShell®, or system commands and scripts; and managing files and processes from graphical file and task managers.

Get Unprecedented Visibility and Swift Response with Host Insights

Understand your risks and contain threats quickly before they can spread. Host Insights, an add-on module for Cortex XDR, combines vulnerability assessment, application and system visibility, and a powerful Search and Destroy feature to help you identify and contain threats. Vulnerability Assessment provides you real-time visibility into vulnerability exposure and current patch levels across your endpoints. Host Inventory presents detailed information about your host applications and settings while Search and Destroy lets you swiftly find and eradicate threats across all endpoints. Host Insights offers a holistic approach to endpoint visibility and attack containment, helping reduce your exposure to threats so you can avoid future breaches.

24/7 Threat Hunting Powered by Cortex XDR and Unit 42 Experts

Augment your team with the industry's first threat hunting service operating across endpoint, network, and cloud data. Cortex XDR Managed Threat Hunting offers round-the-clock monitoring from world-class threat hunters to discover attacks anywhere in your environment. Our Unit 42 experts work on your behalf to discover advanced threats, such as state-sponsored attackers, cybercriminals, malicious insiders, and malware. To detect adversaries hiding in your organization, our hunters comb through comprehensive data from Palo Networks and third-party security solutions. Detailed Threat Reports reveal the tools, steps, and scope of attacks so you can root out adversaries quickly, while Impact Reports help you stay ahead of emerging threats.

Natively Integrate with Cortex XSOAR for Security Orchestration and Automation

Standardize and automate response processes across your security product stack. Cortex XDR integrates with Cortex XSOAR, our security orchestration, automation, and response platform, enabling your teams to feed incident data into Cortex XSOAR for automated, playbook-driven response that spans more than 450 product integrations and promotes cross-team collaboration. Cortex XSOAR playbooks can automatically ingest Cortex XDR incidents, retrieve related alerts, and update incident fields in Cortex XDR as playbook tasks.

Unify Management, Reporting, Triage, and Response in One Intuitive Console

Maximize productivity with a seamless platform experience. The management console offers end-to-end support for all Cortex XDR capabilities, including endpoint policy management, detection, investigation, and response. You can quickly assess the security status of your organization's or individual endpoints with customizable dashboards as well as summarize incidents and security trends with graphical reports that can be scheduled or generated on demand. Public APIs extend management to third-party tools, enabling you to retrieve and update incidents, collect agent information, and contain endpoint threats from the management platform of your choice.

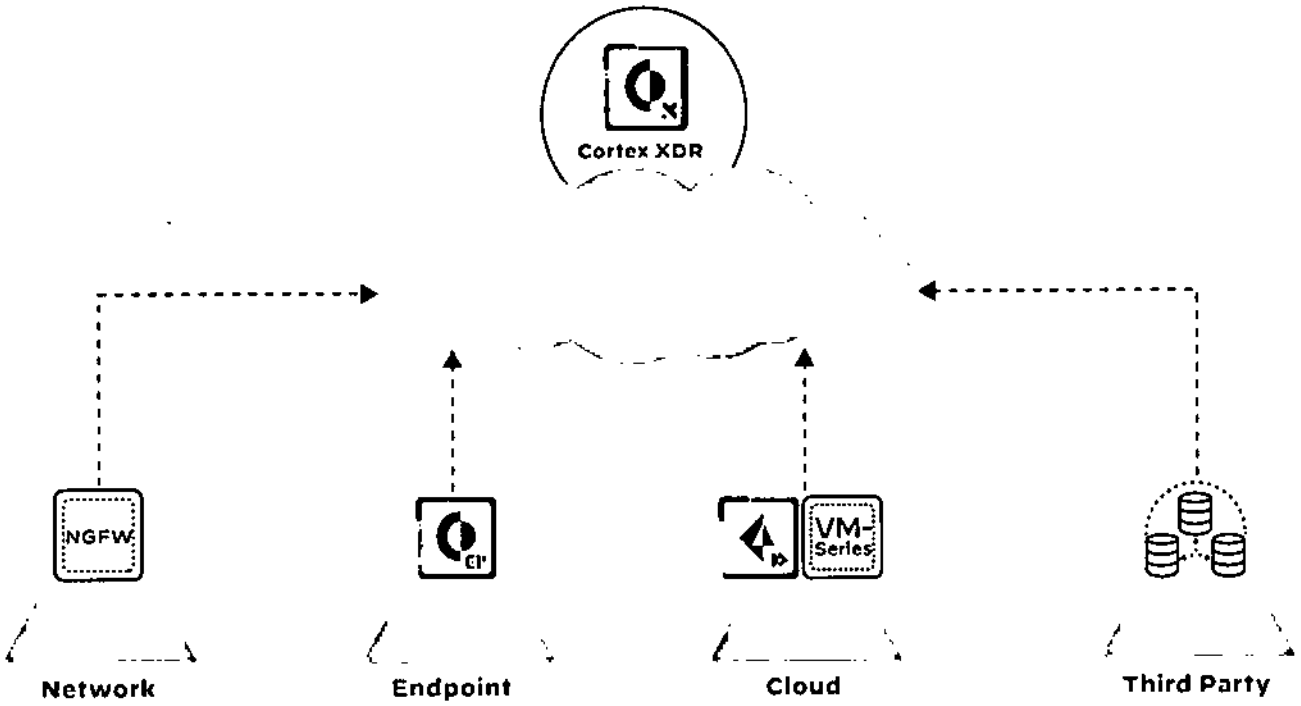

Figure 3: Analysis of data from any source for detection and response

Operational Benefits

Block known and unknown attacks with powerful endpoint protection: Leverage AI-based local analysis and Behavioral Threat Protection to stop the most malware, exploits, and fileless attacks in the industry.

Gain visibility across network, endpoint, and cloud data: Collect and correlate data from Palo Alto Networks and third-party tools to detect, triage, investigate, hunt, and respond to threats.

Automatically detect sophisticated attacks 24/7: Use always-on AI-based analytics and custom rules to detect advanced persistent threats and other covert attacks.

Avoid alert fatigue and personnel turnover: Simplify investigations with automated root cause analysis and a unified incident engine, resulting in a 98% reduction in alerts and lowering the skill required to triage alerts.

Increase SOC productivity: Consolidate endpoint security policy management and monitoring, investigation, and response across your network, endpoint, and cloud environments in one console, increasing SOC efficiency.

Eradicate threats without business disruption: Shut down attacks with surgical precision while avoiding user or system downtime with Live Terminal.

Eliminate advanced threats: Protect your network against malicious insiders, policy violations, external threats, ransomware, fileless and memory-only attacks, and advanced zero-day malware.

Supercharge your security team: Disrupt every stage of an attack by detecting indicators of compromise (IOCs) and anomalous behavior as well as prioritizing analysis with incident scoring.

Restore hosts to a clean state: Rapidly recover from an attack by removing malicious files and registry keys, as well as restoring damaged files and registry keys using remediation suggestions.

Extend detection, investigation, and response to third-party data sources: Enable behavioral analytics on logs collected from third-party firewalls while integrating third-party alerts into a unified incident view and root cause analysis for faster, more effective investigations.

Ease Deployment with Cloud Delivery

Get started in minutes. The cloud native Cortex XDR platform offers streamlined deployment, eliminating the need to deploy new on-premises network sensors or log collectors. You can use your Palo Alto Networks products or third-party firewalls to collect data, reducing the number of products you need to manage. You only need one source of data, such as Next-Generation Firewalls or Cortex XDR agents, to detect and stop threats, but additional sources can eliminate blind spots. Easily store data in Cortex Data Lake, a scalable and efficient cloud-based data repository. By integrating data from multiple sources together, automating tasks, and simplifying management, Cortex XDR delivers a 44% cost savings compared to siloed security tools.

Table 1: Cortex XDR Features and Specifications

Detection and Investigation Features and Capabilities	
Automated stitching of network, endpoint, and cloud data from Palo Alto Networks and third-party sources	Machine learning-based behavioral analytics
Third-party alert and ingestion from any source with required network information	Custom rules to detect tactics, techniques, and procedures
Third-party data from Check Point, Fortinet, Cisco ASA, Okta, PingOne, PingFederate, Azure Active Directory, Google Cloud, Google Kubernetes, AWS, and Windows Event Collector	Root cause analysis of alerts
Host Insights add-on module, providing Vulnerability Assessment, Search and Destroy, and Host Inventory	Asset management
Cortex XDR Managed Threat Hunting service	Timeline analysis of alerts
Detection of malware, fileless attacks, targeted attacks, malicious insiders, and risky user behavior	Post-incident impact analysis
Network detection and response (NDR) and user behavior analytics (UBA)	Dashboards and reporting
Endpoint detection and response (EDR)	Threat intelligence integration
Native integration with Cortex XSOAR for orchestration, automation, and response	Threat hunting
Incident management and incident scoring	Incident response and recovery
Endpoint Protection Capabilities	
Malware, ransomware, and fileless attack prevention	Customizable prevention rules (available with Cortex XDR Pro)
Behavioral Threat Protection	Endpoint script execution (available with Cortex XDR Pro)
AI-based local analysis engine	Network isolation, quarantine, process termination, file deletion, file block list
Cloud-based malware prevention with WildFire	Live Terminal for direct endpoint access
Child process protection	Remediation suggestions for host restore (available with Cortex XDR Pro)
Exploit prevention by exploit technique	Public APIs for response and data collection
Device control for USB device management	Credential theft protection
Host firewall	Scheduled and on-demand malware scanning
Disk encryption with BitLocker and FileVault	Optional automatic agent upgrades
Partner-Delivered MDR Service Benefits	
24/7 year-round monitoring and alert management	Reduction of MTTD and MTTR
Investigation of every alert and incident generated by Cortex XDR	Custom tuning of Cortex XDR for enhanced prevention, visibility, and detection
Guided or full threat remediation actions	Direct access to partners' analysts and forensic experts

CORTEX
BY PALO ALTO NETWORKS

Table 1: Cortex XDR Features and Specifications (continued)

Specification	Cortex XDR
Delivery model	Cloud-delivered application
Data retention	30-day to unlimited data storage
Cortex XDR Prevent subscription	Endpoint protection with Cortex XDR agents
Cortex XDR Pro per endpoint subscription	• Detection, investigation, and response across endpoint data sources • Endpoint protection with Cortex XDR agents
Cortex XDR Pro per TB subscription	Detection, investigation, and response across network and cloud data sources, including third-party data
Cortex XDR Managed Threat Hunting subscription	24/7 threat hunting powered by Cortex XDR and Unit 42 experts
Cortex XDR Pathfinder endpoint analysis service	Collects process information from endpoints that do not have Cortex XDR agents; included with all Cortex XDR subscriptions

Reinvent Security Operations with Cortex

Cortex XDR is part of Cortex®, the industry's most comprehensive product suite for security operations, empowering enterprises with best-in-class detection, investigation, automation, and response capabilities. The suite is built on the tightly integrated offerings of Cortex XDR and Cortex XSOAR, enabling you to transform your SOC operations from a manual, reactive model that required endless resources to a lean, proactive, and automated team that reduces both MTTD and MTTR for every security use case.

Operating System Support

The Cortex XDR agent supports multiple endpoints across Windows, macOS, Linux, Chrome® OS, and Android® operating systems. For a complete list of system requirements and supported operating systems, please visit the Palo Alto Networks Compatibility Matrix. Cortex XDR Pathfinder minimum requirements: 2 CPU cores, 8 GB RAM, 128 GB thin-provisioned storage, VMware ESXi™ V5.1 or higher, or Microsoft Hyper-V® 6.3.96 or higher hypervisor.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

paloalto NETWORKS

Certificate of Completion

This is to certify that

Bradley Jan Pucan

has successfully completed

Palo Alto Networks Accredited Systems Engineer (PSE): Cortex Associate Accreditation Exam

Date: *6/5/2020*

Section IV. General Conditions of Contract

1. Scope of Contract

This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. All the provisions of RA No. 9184 and its 2016 Revised IRR, including the Generic Procurement Manual, and associated issuances, constitute the primary source for the terms and conditions of the Contract, and thus, applicable in contract implementation. Herein clauses shall serve as the secondary source for the terms and conditions of the Contract.

This is without prejudice to Sections 74.1 and 74.2 of the 2016 Revised IRR of RA No. 9184 allowing the GPPB to amend the IRR, which shall be applied to all procurement activities, the advertisement, posting, or invitation of which were issued after the effectivity of the said amendment.

Additional requirements for the completion of this Contract shall be provided in the **Special Conditions of Contract (SCC).**

2. Advance Payment and Terms of Payment

2.1. Advance payment of the contract amount is provided under Annex "D" of the 2016 Revised IRR of RA No. 9184.

2.2. The Procuring Entity is allowed to determine the terms of payment on the partial or staggered delivery of the Goods procured, provided such partial payment shall correspond to the value of the goods delivered and accepted in accordance with prevailing accounting and auditing rules and regulations. The terms of payment are indicated in the **SCC**.

3. Performance Security

Within ten (10) calendar days from receipt of the Notice of Award by the Bidder from the Procuring Entity but in no case later than prior to the signing of the Contract by both parties, the successful Bidder shall furnish the performance security in any of the forms prescribed in Section 39 of the 2016 Revised IRR of RA No. 9184.

4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Project specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the **SCC**, **Section IV (Technical Specifications)** shall specify what inspections and/or tests the Procuring Entity requires, and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

All reasonable facilities and assistance for the inspection and testing of Goods, including access to drawings and production data, shall be provided by the Supplier to the authorized inspectors at no charge to the Procuring Entity.

5. Warranty

5.1 In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier as provided under Section 62.1 of the 2016 Revised IRR of RA No. 9184.

5.2 The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, repair or replace the defective Goods or parts thereof without cost to the Procuring Entity, pursuant to the Generic Procurement Manual.

6. Liability of the Supplier

The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines.

If the Supplier is a joint venture, all partners to the joint venture shall be jointly and severally liable to the Procuring Entity.

Section V. Special Conditions of Contract

Special Conditions of Contract

GCC Clause	
1	**Delivery and Documents** For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows: "The delivery terms applicable to the Contract are DDP delivered Manila. In accordance with INCOTERMS." "The delivery terms applicable to this Contract are to be delivered in Manila. Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination." Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements). For purposes of this Clause the Procuring Entity's Representative at the Project Site is Director Andrea Celene M. Magtalas, Information and Communications Technology Systems Service. **Incidental Services** The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements: a. performance or supervision of on-site assembly and/or start-up of the supplied Goods; b. furnishing of tools required for assembly and/or maintenance of the supplied Goods; c. furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods; and d. performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not relieve the Supplier of any warranty obligations under this Contract. The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services.

	Packaging The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the Goods' final destination and the absence of heavy handling facilities at all points in transit. The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity. The outer packaging must be clearly marked on at least four (4) sides as follows: Name of the Procuring Entity Name of the Supplier Contract Description Final Destination Gross weight Any special lifting instructions Any special handling instructions Any relevant HAZCHEM classifications A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging. **Transportation** Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price. Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the contract price.

	Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered force majeure. The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination. **Intellectual Property Rights** The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.
2.2	Payment schedule shall be in accordance with item 9.0 of Annex "A" Detailed Technical Specifications. In order to proceed with the payment process, the bidder must submit the following documents in case they were not submitted during the deadline for the submission of bidding documents/post-qualification stage/contract signing stage, as applicable: a. Renewed Mayor's/Business Permit in lieu of the submitted expired permit; b. Notarized Omnibus Sworn Statement in lieu of the submitted unnotarized Omnibus Sworn Statement; and c. Notarized Performance Securing Declaration (PSD) or any form of Performance Security, as stated in Section 39 of the 2016 Revised IRR of RA No. 9184, in lieu of the unnotarized PSD.
3	In accordance with item 6.4 of GPPB Resolution No. 09-2020, a Performance Securing Declaration (PSD) shall be accepted in lieu of a performance security to guarantee the winning bidder's faithful performance of obligations under the contract, subject to the following: a. Similar to the PSD used in Framework Agreement, such declaration shall state, among others, that the winning bidder shall be blacklisted from being qualified to participate in any government procurement activity for

	one (1) year, in case of first offense or two (2) years, if with prior similar offense, in the event it violates any of the conditions stated in the contract; b. An unnotarized PSD may be accepted, subject to submission of a notarized PSD before payment, unless the same is replaced with a performance security in the prescribed form, as stated below; and c. The end-user may require the winning bidder to replace the submitted PSD with a performance security in any of the prescribed forms under Section 39.2 of the 2016 Revised IRR of RA No. 9184 upon lifting of the State of the Calamity, or community quarantine or similar restriction, as the case may be.
4	The inspection and approval as to the acceptability of the Goods vis-à-vis its compliance with the technical specifications will be done with prior notice, written or verbal, to the authorized representative of the Supplier. The inspection will push through as scheduled even in the absence of the Supplier's representative, if the latter was duly notified. In which case the result of the inspection conducted by the Procuring Entity shall be final and binding upon the Supplier.

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF BUDGET AND MANAGEMENT
GENERAL SOLANO STREET, SAN MIGUEL, MANILA

NOTICE OF AWARD

JUL 21 2021

MR. CHRISTOPHER B. GARCIA
Accent Micro Technologies, Inc.
8/F East Tower
Philippine Stock Exchange Center
Exchange Road, Ortigas Center
Pasig City

Dear **Mr. Garcia**:

We are pleased to inform you that the contract for the Project, "Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution," is hereby awarded to Accent Micro Technologies, Inc. in the amount of P5,250,000.00.

In this regard, you are hereby required to post a performance security, which shall remain valid until the issuance of the Certificate of Final Acceptance by the Department of Budget and Management (DBM), in the amount and form prescribed in Section 39 of the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act No. 9184 (the Government Procurement Reform Act).

Pursuant to Section 37.2.1 of the same IRR, you have ten (10) calendar days from receipt of this Notice to post the said performance security and enter into a contract with the DBM.

Thank you and God Bless.

Very truly yours,

WENDEL E. AVISADO
Secretary

21-02275

Received by:

July 22, 2021

SECURITY BANK

July 27, 2021

DEPARTMENT OF BUDGET AND MANAGEMENT
General Solano Street, San Miguel, Manila

Gentlemen:

We hereby issue this Irrevocable Domestic Standby Letter of Credit No. **ISB-130021001271** in your favor (hereinafter referred to as **"BENEFICIARY"**) for the account of **ACCENT MICRO TECHNOLOGIES, INC.** (hereinafter referred to as **"APPLICANT")** with office address at 8th Floor East Tower, Philippine Stock Exchange Center, Exchange Road, Ortigas Center, Pasig City, available by your drafts at sight in duplicate up to the aggregate amount of **Philippine Pesos: Two Hundred Sixty Two Thousand Five Hundred Only (Php262,500.00).**

This Standby LC guarantees the performance obligation of the **APPLICANT** for the Renewal of Licenses for the Subscription to Advanced Endpoint Security Solution covered under Notice of Award.

Drawings under this Credit shall be made against presentation of the following:

1. The original of this Credit and amendment/s, if any.
2. Your sight drafts in duplicate drawn on Security Bank Corporation and marked "Drawn under Security Bank Corporation's Irrevocable Domestic Standby Letter of Credit No. **ISB-130021001271** dated July 27, 2021".
3. Certification duly signed by your authorized signatory(ies) stating that the Applicant has been declared in default of its obligation.

This Credit will expire on **July 22, 2022** at the counters of Security Bank Corporation, International Banking Services Division 3rd Floor, 6776 Ayala Avenue, Makati City.

We hereby engage with you that drafts drawn under and in compliance with the terms and conditions of this Credit, together with the specified documents stated herein, shall be duly honored upon presentation to us on or before **July 22, 2022.** This Credit shall cease to have any force or effect upon its expiration, whether or not the original credit is returned by the Beneficiary (any policy, rule, regulation of the Beneficiary to the contrary notwithstanding).

Furthermore, it is expressly agreed and understood that the Applicant shall, upon demand, have the sole and absolute liability to reimburse us for any drawings made under this Standby Letter of Credit.

Unless otherwise stated herein, this Credit is subject to the Uniform Customs and Practice for Documentary Credits (2007 revision) International Chamber of Commerce Publication No. 600.

Very Truly Yours,

SECURITY BANK CORPORATION
International Banking Services Division
By:

GHIA E. CLEOFE
Assistant Manager

SANTA M. DOMINGO
Manager

For inquiries and comments, please call our 24-Hour Customer Service hotline at (632) 888-791-88 or email us at customercare@securitybank.com.ph. Security Bank Corporation is supervised by Bangko Sentral ng Pilipinas with telephone number (632) 8708-7087 and email address consumeraffairs@bsp.gov.ph

ABEGAIL D. IGNA
Procurement Management Division
JUL 29 2021