PUBLIC TENDER No. 03/IAVE/2022

TENDER SPECIFICATIONS

Acquisition of Endpoints, Displays and Security Software Package

CPV Classification: 30213300-6 Laptop Computers
30231310-3 - Flat screen displays
48730000-4 – Security software package

PART I - Legal Clauses

Article 1
Object

1. The object of these specifications is the acquisition of:

Type	Description	Quantity
Endpoint Type 1	Basic Endpoint	200
Endpoint Type 2	Advanced Endpoint	150
Display	Monitor 23.8”	200
Device Security	Device Security	300

for Instituto de Avaliação Educativa, I.P. (hereinafter referred to as IAVE, I.P.);

2. The execution of all services inherent to after-sales services are considered to be covered by the object of this procedure, in accordance with the specifications described in Article 23 of these Tender Specifications.

Article 2
Form and contract documents

1. The contract to be signed also includes the following elements:
   a) Correction of errors and omissions in the Specifications identified by the invited entities, provided that these errors and omissions have been expressly accepted by the competent body for the decision to contract;
   b) Clarifications and corrections relating to the Tender Specifications;
   c) These Tender Specifications;
   d) The awarded tender;
   e) Clarifications on the awarded tender provided by the contractor.

2. In case of discrepancy between the documents referred to in the previous number, the respective prevalence is determined by the order provided therein.

3. In case of divergence between the documents referred to in number 2 and the articles of the contract and its annexes, the former prevail, except for the proposed adjustments, in accordance with Article 99 of the Public Contracts Code (hereinafter referred to as PCC) and accepted by the contractor, pursuant to Article 101 of the same law.

4. In addition to the documents referred to in number 2, the contractor is also obliged to respect, when applicable, the European and Portuguese norms, specifications and homologations by official bodies and manufacturers or entities holding patents.

Article 3

Good faith

The parties oblige themselves to act in good faith in the performance of the contract and not to exercise the rights provided therein, or by law, in an abusive manner.

Article 4

Place, form and duration of the contract

1. The contract that is celebrated will be in force until the day of delivery of the goods.

2. The goods must be made available at the IAVE, at the premises of Instituto de Avaliação Educativa, I.P., located at Travessa Terras de Sant'Ana, 15,1250-269 Lisbon, within 120 days of the award.

3. The additional obligations that, under legal or contractual terms, must subsist beyond the termination of the contract, are excluded from the period established in the previous number of this article.

Article 5

Base price

The base price, for the purposes of this procedure, corresponds to €840,153 (eight hundred and forty thousand, one hundred and fifty-three euros), price to which VAT is added at the legal rate in force.

Article 6

Payment conditions

1. The amounts owed by IAVE under the contract will be paid under the terms set forth in the following numbers.

2. Payments will be made within a maximum period of 60 (sixty) days after receipt of the respective invoices, which can only be issued after the due date of the respective obligation based on worksheets signed by both parties, which contain the goods.

3. Under no circumstances are advance payments granted.

4. In case of disagreement on the part of IAVE, I.P., regarding the values indicated in the invoices, the respective grounds must be communicated in writing to the contractor, who is obliged to provide the necessary clarifications or issue a new corrected invoice.

5. Invoices must contain the commitment number generated by the contracting authority, under the terms of the law, as well as a description of the goods.

6. Provided they are regularly issued, and in compliance with the provisions of the preceding numbers, invoices are paid by bank transfer, to the IBAN indicated by the contractor upon completion of the supplier form.

Article 7

Contractor's obligations

1. The contractor's obligations, in addition to others arising from what is established in the parts of this procedure and in the applicable legislation, are those that are set forth below and that must be subject to specific clauses to be included in the contract to be signed:

a. Ensure the provision of the goods, as defined in these Specifications and its annexes, as well as in other contractual documents;
b. Communicate, in advance, to IAVE, I.P. any fact that makes it totally or partially impossible to provide any of the goods object of this procedure, or that implies the breach of any other of its obligations;
c. No alteration of the underlying conditions for the provision of the services agreed between the parties, through the signing of a written contract between them, without prior authorization from the contracting authority;
d. Ensure all human and material resources that prove necessary and indispensable for the performance of the contract;
e. Ensure, in a correct and reliable manner, the information regarding the conditions under which the goods will be provided, giving all the clarifications that are justified and within the period indicated by IAVE, I.P.;
f. Non-cession of the contractual position, without prejudice to the provisions of Article 13 of these Specifications;
g. Communicate any fact that, occurring during the performance of the contract, proves to be relevant for the normal provision of the goods and for the contractual performance, namely, the change of the corporate name or of its legal representatives.

Article 8

Patents, licenses and trademarks

1. The contractor is responsible for any charges resulting from the use of registered trademarks, registered patents, licenses or other similar rights.

Article 9

Use of distinctive signs

Neither party may use the name, brands, trade names, logos and other distinctive trade signs belonging to the other without its prior written consent.

Article 10

Confidentiality

1. The contractor will guarantee confidentiality regarding any information that they may become aware of regarding the activity of IAVE, I.P., due to the acquisition of the goods, object of this contract.

2. It is excluded from the duty of confidentiality referred to in the previous number, the information and documentation that are proven to be in the public domain on the date of the respective acquisition by the provider of goods, or that the latter is obliged to reveal, by force of law, in a judicial proceeding or at the request of regulatory authorities or other competent administrative entities.

Article 11

Data Protection Regulation

1. The contractor is obliged to comply with all applicable legal provisions regarding the processing of personal data, in the sense given by Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27th, 2016, on the protection of the natural persons with regard to the processing of personal data and the free circulation of such data ("General Regulation on Data Protection") and other applicable community and national legislation, in relation to all personal data accessed within or for the purpose of providing the goods, namely, personal data of customers, employees, collaborators and suppliers of goods of IAVE, I.P.

2. The parties acknowledge and accept that, with regard to all personal data to which the contractor has access or is transmitted by IAVE, I.P. for the purposes of providing the goods:

a. IAVE, I.P. will act as data controller (as defined in the General Regulation on Data Protection), determining the purposes and forms of data processing by the contractor;

b. The contractor will act as a subcontracting entity (as defined in the General Regulation on Data Protection), processing personal data in strict compliance with the instructions of the data controller;

c. For this purpose, the processing of personal data is understood to be the operations, with or without recourse to automated means, carried out on the personal data of IAVE, I.P. employees, including the collection, registration, organization, storage, adaptation or modification, retrieval, consultation, use, disclosure, transfer and/or making available to third parties, aligning, combining, blocking, erasing and destroying the aforementioned data.

3. The contractor is obliged not to copy, reproduce, adapt, modify, change, delete, destroy, disseminate, transmit, disclose or, by any other person, make available to third parties the personal data to which they have access or have been transmitted by the data controller under this Agreement, without having been expressly instructed, in writing, by the data controller or by the data subjects in the exercise of their respective rights.

4. Without prejudice to the other obligations provided for in this Contract, the contractor is obliged to strictly comply with the provisions of the applicable legislation regarding the processing of personal data, and in particular to:

a. Treat it only in accordance with the instructions of IAVE, I.P., solely and exclusively, for the purposes of this provision of goods, complying with the statutory obligations on data protection;

b. Provide all the collaboration needed to clarify any issue related to the processing of personal data carried out under this Agreement and keep IAVE, I.P. informed concerning the processing of personal data;

c. Provide assistance to IAVE, I.P. , taking into account the nature of the treatment and the information at its disposal, in order to ensure the obligations regarding the notification of violations of personal data, namely through communication, whenever possible up to 72 hours after the knowledge (of the occurrence) of any violation of personal data that occurs, also collaborating with IAVE, I.P. in the adoption of measures to respond to the incident, in the investigation and in the elaboration of the notifications that are necessary under the terms of the law;

d. Collaborate with IAVE, I.P. taking into account the nature of the treatment, and, as far as possible, adopting the technical and organizational measures referred to in this Article, which include encryption or pseudonymization of personal data, in order to reduce the risks for the data holders in question, not excluding other possible data protection measures, so as to fulfil the obligation to respond to requests from data subjects, with the purpose of allowing them to exercise their rights under the terms of the law;

e. Not to communicate personal data to third parties and providers of goods not authorized or indicated by IAVE, I.P.;

f. Depending on the choice of IAVE, I.P. or of the data subjects to delete or return the personal data at the time of cession of the contract, deleting any existing copies, except if the conservation or transmission of the data is required by law;

g. Keep records of data processing activities carried out on behalf of IAVE, I.P. under this agreement, in accordance with the requirements provided for by law;

H. Comply with all other legal provisions regarding the registration, transmission or any other processing operation of personal data provided for by law;

i. Not to transfer personal data outside the European Economic Area, without the prior written consent of the data controller;

j. Provide the data controller with all the information necessary to show compliance with the obligations provided for by law in the respective scope and facilitate and contribute to audits, including inspections conducted by the data controller or by another auditor mandated by the controller;

k. Ensure that the personnel authorized to process personal data assume a commitment to confidentiality and that they are aware of and commit themselves to fulfil all obligations set forth herein.

5. The contractor is obliged to implement the technical and organizational measures necessary for the protection of personal data processed on behalf of IAVE, I.P. against their accidental or unlawful destruction, accidental loss, alteration, unauthorized dissemination or access, as well as against any other illicit form of processing of that personal data.

6. The measures referred to in the previous number must ensure an adequate level of security in relation to the risks that the processing of data presents, the nature of the data to be protected and the risks, of varying probability and severity, for the rights and freedoms of the natural persons.

7. The contractor agrees that access to personal data processed under this Contract will be strictly limited to personnel who need to have access to it for the purposes of fulfilling the obligations assumed herein by the contractor.

8. The contractor is obliged to notify the data controller of any situation that may affect the processing of personal data or in any way give rise to non-compliance with the legal provisions on data protection, and must also take all necessary measures in its power to stop it immediately.

9. The contractor will be responsible for any damage IAVE, I.P. may incur as a result of the processing of personal data or in violation of applicable legal rules and the provisions of this Contract, when such violation is attributable to the contractor, together with its staff, within the scope of the service provided, when the violation is attributable to the action of the latter.

10. The contractor is authorized to resort to subcontracting a third party to collaborate in the provision of the goods, ensuring, however, that it will comply with the provisions of the applicable legislation. Such obligation must be included in a written contract that the contractor celebrates with the third party, thus ensuring compliance with the obligations arising from Regulation (EU) 2016/679 and other applicable legislation regarding personal data, binding the actions to the essence, nature and purposes of this contract, in strict compliance with the duty of confidentiality.

11. Whenever IAVE, I.P. receives a request for access or rectification of personal data or an opposition to its processing by its data holders, the contractor must assist the data controller through appropriate technical and organizational measures, to allow it to fulfil its obligation to respond to requests from holders, while allowing them to exercise their legal rights.

Article 12
Amendments to the contract

1. Any amendment to the contract must be in a written document signed by both parties and it will take effect from the date of the respective signature.

2. The party interested in the amendment must communicate this intention in writing to the other party, at least 60 (sixty) days in advance of the date on which it intends to see the amendment introduced;

3. The contract can be amended by:
   a) Agreement between the parties, which cannot be less solemn than that of the contract;
   b) Judicial or arbitral decision, except in cases where the amendment interferes with the result of the exercise of the margin of free administrative decision underlying it, or it implies the expression of valuations specific to the exercise of the administrative function;
   c) Administrative act of the public contracting party, in cases where:

i. Contract clauses that clearly, accurately and unequivocally indicate the scope and nature of any amendments, as well as the conditions under which they may be applied;
ii. Abnormal and unforeseeable alteration of the circumstances on which the parties have based their decision to contract, provided that the requirement of the obligations assumed by them seriously affects the principles of good faith, and it is not covered by the risks inherent to the contract;
iii. Reasons of public interest arising from new needs or a new understanding of existing circumstances.

Article 13
Cession of contractual position

1. The contractor may not cede the contractual position or any of the rights and obligations arising from the contract, without prior authorization from IAVE, I.P.

2. For the purposes of the authorization referred to in the previous number, it is required, without prejudice to what is also legally due:
a) that the cessionary will present all the documentation required of the contractor in the present procedure;
b) that IAVE, I.P. will assess whether the cessionary is not in any of the situations provided for in Article 55 of the CCP.

3. The possibility of cession of the contractual position is foreseeable, in accordance with the provisions of Article 318 of the CCP (it only applies to contracting procedures with two or more competitors).

Article 14
Contract termination

1. Failure by one of the parties to fulfil the obligations resulting from the contract grants to the other party, under the terms provided for in the applicable legal regime, the right to terminate the contract, without prejudice to the corresponding legal indemnities and other general grounds for legally terminating the contract.

2. For the purpose of the provisions of the previous number, a definitive default is considered to exist when there is a delay in the provision for a period exceeding 10 working days.

3. The resolution will be carried out upon prior notice, by registered letter with acknowledgment of receipt, sent at least 10 working days in advance.

4. Termination of the contract does not affect the application of any pecuniary sanctions, under the terms of the following Article.

Article 15

Penalties

1. In the event of non-compliance with contractual obligations, the contracting authority may apply the following pecuniary contractual sanctions to the contractor, depending on the seriousness or repetition of the infringement:

a) For non-compliance with obligations relating to the duty of confidentiality, up to €1000.00 (one thousand euros), per breach;

b) Failure to comply with obligations relating to intellectual property and personal data, up to €1000.00 (one thousand euros), per breach;

c) Failure to comply with the information duties, up to €250.00 (two hundred and fifty euros), per breach;

d) For non-compliance with the determination that is addressed to the contractor under the terms of these Specifications, which include the obligations provided for in Article 1, up to €250.00 (two hundred and fifty euros), per breach;

e) For non-compliance with the obligations listed above, the said penalties may be applied, not exceeding 20% or 30% of the total amount awarded, depending on the case, and in accordance with the provisions of Article 329 of the PCC.

2. Payment of any penalties incurred by the contractor will be deducted from the net value of the second party's billing.

3. The penalties applied do not prevent the contracting authority from demanding compensation for excess damage.

4. The application of the penalties provided for in this article will be subject to a prior hearing, under the terms provided for in paragraph 2 of Article 308 of the PCC.

5. The contractor will be notified, in writing, so that within a period of 5 (five) business days they can pronounce themselves. If the contractor does not respond within the allotted period, the contracting authority applies the penalty in accordance with number 2 of this Article.

Article 16

Entitlement to interest on late payment

1. Delay in the payment of any regularly issued invoices does not authorize the contractor to invoke the exception of non-compliance with any of the obligations in the contract, except in the cases provided for in Article 327 of the PCC.

2. The delay in any payment does not determine the maturity of the remaining payment obligations.

2. In case of delay, payments due by the contracting authority bear interest, at the legal rate, from the date on which they became due and until full payment, under the terms of Article 326 of the PCC.

3. In case of disagreement on the amount due, the public contracting party must make the payment on the amount with which the co-contracting party agrees.

5. The amounts contested by the contracting authority, and which are subject to correction do not earn default interest in case of non-payment.

Article 17

Acts of God or "Force Majeure"

1. Neither party shall incur liability if, due to acts of God or "Force Majeure", it is prevented from fulfilling the obligations assumed in the contract, being understood as such the circumstances that make it impossible to carry out the activity, beyond the will of the affected party, which it could not have known about or foreseen on the date of conclusion of the contract, and whose effects it was not reasonably required to circumvent or avoid.

2. They may constitute "force majeure", if the requirements of the previous number are verified, namely, earthquakes, floods, fires, epidemics, sabotage, strikes, international embargoes or blockades, acts of war or terrorism, riots and injunctive governmental or administrative determinations.

3. The following do not constitute "force majeure", namely:

a) Strikes or labour disputes limited to the companies of the second party or to groups of companies of which it is a part, as well as to companies or groups of companies of its subcontractors;

b) Circumstances that do not constitute "force majeure" for the subcontractors of the second party, in the part in which they intervene;

c) Governmental, administrative, or judicial determinations of a sanctioning nature or otherwise resulting from the non-compliance by the second party with the duties or obligations that fall upon it;

d) Demonstrations resulting from the non-compliance, by the second party, with legal norms;

e) Fires or floods originating in the premises of the second party, whose cause, propagation or proportions are due to its fault or negligence or to non-compliance with safety standards;

f) Malfunctions in the computer or mechanical systems of the second party not due to sabotage;

g) Events that are or should be covered by insurance.

3. The party that invokes acts of God or "force majeure" must immediately communicate and justify such situations to the other party, by any written means, as well as inform the foreseeable period for re-establishing the situation.

5. "Force majeure" determines the extension of the deadlines for the fulfilment of contractual obligations affected by the period of time, demonstrably corresponding to the impediment resulting from "force majeure".

Article 18.

Counting of deadlines in the performance phase of the contract

When calculating deadlines in the performance phase of the contract following this procedure, the subsequent rules apply:

a) The deadlines are continuous, not suspended on Saturdays, Sundays and holidays;

b) The deadline that falls on a Saturday, Sunday, holiday or on a day when the facility, before which the act must be carried out, is not open to the public, or does not operate during the normal period, is transferred to the first next working day.

Article 19

Celebration of the written contract

In accordance with Article 94(1) of the PCC, the contract will be in writing.

Article 20

Communications and Notifications

1. All notifications and communications between the contracting authority and the contractor must be made in writing, by mail, email or fax, to the home address or registered office of each one, identified in the contract, with sufficient clarity, so that the recipient is aware of its nature and content.

2. Any changes to the contact information contained in the contract, even if occasional or temporary, must be communicated immediately and in writing to the other party.

Article 21

Grounds for the decision of the procedure

1. This public tender procedure is adopted under the terms of paragraph b) of Article 20 and Article 130 and following of the CCP and the decision to contract was taken by the IAVE President of the Board of Directors, Luís Santos.

Article 22

Competent court

1. In everything that is omitted in these Specifications, the provisions of the CCP and other applicable legislation and regulations will be observed.

2. The district court of Lisbon is competent for the communication of any disputes arising from the contract, namely relating to the respective interpretation, execution, non-compliance, invalidity, resolution or reduction.

Part II

Technical specifications

Article 23
Equipment technical specifications

1. The technical specifications of the equipment are categorized according to the following specifications. All equipment must be of the same brand, except for security software:

- **Basic Endpoint**

REQ	Requirement
Processor	
1	Intel vPro Essentials with Intel Core i7-1255U (10 Core) 1.70 GHz to 4.70 GHz
Operating System	
2	Windows 10 Pro (Includes Windows 11 Pro License) English, Spanish, Italian, French, Portuguese
Screen	
3	14.0" FHD (1920x1080) Anti Glare, SLP, Non-Touch, ComfortView+, WVA, 400 nits, FHD IR Camera+Intelligent Privacy
Memory	
4	16GB, 2x8GB, DDR4 Non-ECC
Disk	
5	M.2 256GB PCIe NVMe Class 40 Opal 2.0 Self Encrypting Solid State Drive
Various	
6	Palmrest, Touch Fingerprint Reader (in Power Button), Contacted Smart Card, Contactless Smart Card NFC and Control Vault 3.0 Advanced Authentication with FIPS 140-2 Level 3 Certification
7	Face IR camera (Windows Hello compliant) with ExpressSign-in (Camera Sensing), Intelligent Privacy (onlooker detection with screen texturizing and adaptive dimming), Camera Shutter, SafeScreen, Mic
8	3 Cell 41 Whr Express Charge Capable Battery
9	Intel AX211 WiFi 6e 2x2 AC+ BT 5.2 vPro
10	Single Point keyboard Portuguese with backlit
Docking station with the following Interfaces	
12	USB-C 3.1 Gen 2 | 2. USB-A 3.1 Gen 1 with PowerShare
13	2x DisplayPort 1.4
14	1x HDMI
15	USB-C Multifunction DisplayPort
16	Dual USB-A 3.1 Gen 1
17	Gigabit Ethernet RJ45
18	Power AC 180W
19	Thunderbolt 3
Guarantee	
20	The guarantee is for a period of five years

Advanced Endpoint

REQ	Requirement
Processor	
1	12th Generation Intel vPro Enterprise with Intel Core i7-1265U (10 Core, 12 MB Cache, 12 Threads, up to 4.80 GHz)
Operating System	
2	Windows 10 Pro (Windows 11 Pro license included), English, French, Italian, Portuguese, Spanish
Screen	
3	Laptop 13.3" FHD (1920x1080) AG, Touch, WVA, 300 nits, FHD IR Camera + Intelligent Privacy
Memory	
4	16GB 3200MHz DDR4, Non-ECC, Integrated
Disk	
5	M.2 512GB PCIe NVMe Class 40 Opal 2.0 Self Encrypting Solid State Drive
Various	
6	Palmrest, Touch Fingerprint Reader (in Power Button), Contacted Smart Card, Contactless Smart Card NFC and Control Vault 3.0 Advanced Authentication with FIPS 140-2 Level 3 Certification
7	FHD/IR Camera with ExpressSign-In + Intelligent Privacy, Temporal Noise Reduction, Camera Shutter, Mic
8	58WHR, 4 Cell Battery Express Charge Capable
9	Intel(R) Wi-Fi 6E AX211 2x2 802.11ax 160MHz + Bluetooth 5.2 Wireless Card
10	Single Pointing Backlit Portuguese Keyboard
Guarantee	
11	The guarantee is for a period of five years

Display

Below are described the characteristics of the displays to be acquired. They must be from the same manufacturer as the endpoints.

REQ	Requirement
Characteristics	
1	LED-backlit LCD monitor / TFT active matrix
2	USB Power Delivery - 65W
3	Diagonal Size – 23.8”
4	Interfaces – USB 3.2 Gen 1 / USB-C hub
5	Aspect Ratio – 16:9
6	Resolution - Full HD (1080p) 1920 x 1080 at 60 Hz
7	Contrast Ratio – 1000:1
8	WLED
9	DisplayPort (DisplayPort 1.2 mode, HDCP 1.4)
10	DisplayPort output (MST)
11	HDMI (HDCP 1.4)
12	USB-C 3.1 Gen 1 upstream/DisplayPort 1.2 with Power Delivery (power up to 65W)
13	4 x USB 3.2 Gen 1 downstream
14	Network (RJ-45)
Guarantee	
15	The guarantee is for a period of five years

Device security

The goal is to acquire a tool for monitoring and detecting threats, vulnerabilities and malware to be used in our infrastructure for a total of 300 endpoints and/or servers.

Below are described the characteristics of the tool to be acquired, which must include all the necessary licenses for the intended functionalities during the term of the contract.

REQ	Requirement
1	The proposed solution must continuously analyze and monitor the activity of files, processes and communications on servers and endpoints in order to find any suspicious activity.
2	This solution must be based on a global intelligence network that has information about the latest attacks and malware.
3	It must also offer full visibility and control to quickly detect, contain and remediate threats/malware that may exist on the network and have not been detected by currently existing solutions. In these cases, it must be possible to identify:
4	How the malware got in
5	Which systems were affected
6	What the malware did and what it is doing
7	The problem and its origin
Functionalities	
8	The solution must also offer the following functionalities:
9	File reputation
10	The solution should use traditional mechanisms to verify the file reputation, such as 1to1 signatures. It must also use mechanisms based on artificial intelligence and be able to identify malware that uses polymorphism.
11	Antivirus engine
12	The solution must contain an Antivirus engine in order to have a single agent for Antivirus and advanced functionalities for detection, protection, and forensic investigation.
13	Outbreak Control
14	The solution should allow the definition of lists for:
15	Applications blockage
16	It should be possible, in addition to quarantining an application, to simply block it to prevent its execution.
17	It should be possible to define applications to be blocked for Android environments
18	Applications Whitelist
19	Customized signatures
20	IPs Blacklist/Whitelist
21	Customized signatures
22	The solution should allow the administrator to create signatures for file detection. Supported formats should be:
23	MD5 signatures
24	MD5, PE section-based signatures
25	File body-based signatures
26	Extended signature format (offsets, wildcards, regular expressions)

27	Logical signatures
28	Icon signatures
29	Static and dynamic analysis of files
30	The solution should allow static and dynamic analysis of the files using a sandbox platform. In these cases, a report must be generated containing generic and detailed information on the activity of the analyzed file. It should also be possible to visualize the behaviour of the file on the sandboxing platform through a video.
31	Retrospective detection
32	It should be possible to receive alerts when the verdict of a file changes (from clean or unknown to malicious). It is essential that the solution offers visibility into malware that evades the first lines of defence or malware, which is not detected during the first file analysis.
33	The solution should periodically check whether a clean or unknown file still has the same verdict or whether that verdict has changed.
34	External links
35	The solution should detect connections to the outside that represent danger (for example, Command and Control Networks)
36	Trajectory of files on the network
37	The solution must monitor the activity of files within the network, namely the way in which they spread within the network. In the event that a file is classified as malware after it has entered the network, the solution should make it possible to understand how the file entered the network, how it spread and which systems it infected from a single dashboard. It should also be possible to block and quarantine this type of files with just a few clicks, regardless of the number of infected endpoints.
38	Trajectory of files and processes within the device
39	The solution should monitor all the activity of files, applications and processes in the endpoints, in order to identify the source of potential malware. There must be a temporal graphic where it is possible to verify how the different processes in the endpoints interact with each other.
40	Root Cause
41	The solution should make it possible to identify not only malicious files, but also be able to identify the source of the problem. Example: If Adobe Reader is compromised and executes malicious code, the proposed solution should allow to identify this behaviour and block or quarantine only the Adobe version that is compromised on any endpoint with the agent installed.
42	Research
43	It should be possible to search for a file/SHA or an IP in order to understand which systems have that file or which systems have opened a connection to the searched IP.
44	Automatic file submission to sandbox
45	The system must track files executed in the organization and automatically submit files that are uncommon in the organization to be analyzed in a sandboxing environment. It should also be possible to manually upload files to the sandboxing platform.

46	The sandboxing solution, through additional licensing, must allow the administrator to interact directly with the files while they are being analyzed. It should also provide access to a portal with the history of samples analyzed by the organization.
47	The sandboxing report should generate a report with the following sections:
48	Metadata
49	File behaviour
50	HTTP traffic
51	DNS traffic
52	TCP/IP streams
53	Executed processes
54	Observed artifacts
55	Registry activity
56	FileSystem activity
57	It should be possible to download the analyzed sample, visualize a video that shows the behaviour of the analyzed file during its execution and download the PCAP and the artifacts observed during file execution.
58	Customizing compromise indications
59	The system must support the creation and customization of compromise indications in the endpoints, through the OpenIoC framework.
60	Vulnerabilities
61	The solution must identify software present on endpoints that have known vulnerabilities (CVEs - Common Vulnerabilities and Exposures).
62	API
63	The solution must have a bi-directional API that allows integration with third-party systems
64	Visibility on arguments passed by command line
65	The system must ensure visibility into which arguments are passed through the command line to launch executables. It should be possible to see if legitimate applications are being used maliciously.
66	Integration with proxies
67	The solution must be able to be integrated with different proxy manufacturers in order to be able to detect compromised machines, even if they do not have an agent installed.
68	Integration with NGFW and NGIPS
69	The solution must at least be able to be integrated with the manufacturer's own NGFW and NGIPS solutions, so that it is possible to automatically correlate information and obtain information about compromised machines in a single centralized dashboard.
70	Architecture
71	The endpoint solution must be able to be integrated into a complete architecture that includes: endpoint, proxy, network and email solutions.
72	Reports
73	The solution should automatically generate weekly reports with the following information:
74	Active connectors

75	Potentially infected computers
76	Malicious files detected
77	Computers that attempted to connect to malicious IPs outside the organization
78	Quarantined files
79	Blocked apps
80	Retrospective Events – False Positives
81	Indications of Compromise
82	Heat Map
83	It should be possible to group endpoints and visualize on a heat map which groups contain infected endpoints.
84	It should be possible to integrate with a central management console that will allow integration with: firewalls, email and web security, endpoint security, network analytics, strong authentication, network access control solution and application security. It should also allow:
85	Orchestration and automation: it must integrate with the various solutions mentioned and simplify security operations by allowing the creation and management of incident response workflows
86	Incident investigation and response: addressing indicators of compromise (IoC) and carrying out security investigations, providing information from intelligence sources, analyzing the risk and impact of these IoCs in the context of the endpoints and with other indicators. Once the investigation materializes in a security incident, it should be possible to develop automatic workflows and remediation processes, such as: blocking malicious IPs, domains, URLs and files.
87	It provides dashboards of the tools with which it integrates
88	It provides single sign-on