Τεχνικές Προδιαγραφές

Οι Τεχνικές Προδιαγραφές του αιτούμενου εξοπλισμού παρατίθενται κατωτέρω

Λογισμικό Antivirus, XDR, E-mail Protection, VA&PM,

Α/Α	Προδιαγραφή	Απαίτηση
1.2	Το λογισμικό προστασίας να υποστηρίζει τα εξής λειτουργικά συστήματα: MS Windows 10, 11 MS Windows Server 2012, 2012r2, 2016,2019,2022,2025 Linux (Ubuntu Desktop Ubuntu Desktop 20.04 LTS, Ubuntu Desktop 22.04 LTS, Ubuntu Desktop 24.04 LTS , Red Hat Enterprise Linux 8, 9, 10 with supported desktop environment installed, Linux Mint 21, 22) MacOS 11 and later MacOS Server 11 and later	ΝΑΙ
1.3	Οι ελάχιστες απαιτήσεις συστήματος να είναι 0.3 GB ελεύθερη διαθέσιμη μνήμη (RAM) και 1 GB ελεύθερος χώρος στον σκληρό δίσκο.	ΝΑΙ
1.4	Το σύστημα προστασίας θα πρέπει να έχει πιστοποίηση του ανεξάρτητου οργανισμού AV-Comparatives “Business Security Approved” και “Real World Protection Advanced” κατ’ ελάχιστον, για τα τελευταία 2 έτη τουλάχιστον.	ΝΑΙ
1.5	Το σύστημα θα πρέπει να έχει πιστοποίηση του ανεξάρτητου ινστιτούτου AV-TEST GmbH, “Approved Corporate Endpoint Protection - TOP Product” κατ’ ελάχιστον τα τελευταία 2 έτη	ΝΑΙ
1.6	Προϋπόθεση αξιολόγησης, επί ποινή αποκλεισμού, αποτελεί η συμπλήρωση του φύλλου συμμόρφωσης με παραπομπή σε φυλλάδια του κατασκευαστικού οίκου προς απόδειξη ζητουμένων στοιχείων και με σαφή αναφορά στην σελίδα και παράγραφο του φυλλαδίου, όπου εμπεριέχονται τα στοιχεία αυτά.	ΝΑΙ
2	**Αντιική Προστασία**	
2.1	Η κεντρική βάση ανίχνευσης κακόβουλου λογισμικού και οι σχετικοί μηχανισμοί ενημέρωσης, ανάλυσης και συσχέτισης απειλών θα πρέπει να παρέχονται μέσω ασφαλούς υποδομής cloud του κατασκευαστή.	ΝΑΙ
2.2	Να υποστηρίζεται ανίχνευση και καθαρισμός όλων των τύπων απειλών malware: viruses, malware, trojans, dialers, spyware, jokes, hoaxes,ransomware.	ΝΑΙ
2.3	Να υποστηρίζεται αυτόματη ανίχνευση και καθαρισμός των προαναφερθέντων απειλών σε πραγματικό χρόνο.	ΝΑΙ
2.4	Να υποστηρίζεται ανίχνευση και καθαρισμός των προαναφερθέντων απειλών.	ΝΑΙ
2.5	Να υποστηρίζεται IPS (intrusion prevention system).	ΝΑΙ
2.6	Να υποστηρίζονται τεχνολογίες advanced heuristics (ενδεικτικά: DNA, smart signatures, Behavioral Analysis) για δυνατότητα ανίχνευσης άγνωστου malware.	ΝΑΙ
2.7	Προστασία για SSL/TLS filtering στα πρωτόκολλα HTTPS, IMAPS, POP3S.	ΝΑΙ

2.8	Δυνατότητα αποτροπής γνωστών exploits	ΝΑΙ
2.9	Δυνατότητα μπλοκαρίσματος όλων των σελίδων του Internet σε ένα client καθώς και διαχείριση των σελίδων που μπορούν να είναι	ΝΑΙ

	διαθέσιμες στο χρήστη ανά κατηγορία, π.χ. αποτροπή επίσκεψης σε σελίδες social media, streaming videos.	
2.10	Δυνατότητα προστασίας σε δικτυακό επίπεδο με client based Firewall, με δυνατότητα φιλτραρίσματος σε επίπεδο θυρών και εφαρμογών σε εισερχόμενες και εξερχόμενες συνδέσεις.	ΝΑΙ
2.11	Δυνατότητα προστασίας από δικτυακές απειλές και botnets	ΝΑΙ
2.12	Δυνατότητα ενιαίας καραντίνας αρχείων που ανιχνεύθηκαν για όλο το δίκτυο, με δυνατότητες προβολής clients ανά απειλή, εξαγωγή και εξαίρεση	ΝΑΙ
2.13	Να παρέχεται από το πρόγραμμα ασφαλής περιηγητής (browser) για την προστασία ευαίσθητων δεδομένων κατά την περιήγηση στο διαδίκτυο.	ΝΑΙ
2.14	Να παρέχεται η δυνατότητα ρύθμισης προκαθορισμένων site με σκοπό την αυτόματη ανακατεύθυνση τους στον προστατευμένο περιηγητή που παρέχεται από το πρόγραμμα.	ΝΑΙ
2.15	Να παρέχεται η δυνατότητα του προγράμματος σε λειτουργικό windows server να ελέγχει τους φακέλους και τα αρχεία στο Microsoft OneDrive for Business για κακόβουλο λογισμικό.	ΝΑΙ
2.16	Να παρέχεται η δυνατότητα του προγράμματος σε λειτουργικά windows server να λειτουργούν μεταξύ τους ως cluster με σκοπό τον συγχρονισμό των δεδομένων , των ρυθμίσεων και ειδοποιήσεων .(πχ. Ανταλλαγή των προαναφερόμενων δεδομένων και ρυθμίσεων του antivirus program σε windows failover cluster nodes,network load balancing nodes, οπού και είναι απαραίτητο το πρόγραμμα να έχει το ίδιο configuration σε όλα τα nodes).	ΝΑΙ
2.17	Να παρέχεται η δυνατότητα του προγράμματος τοπικά σε λειτουργικά windows server όπου έχουν τον ρόλο του hypervisor, να πραγματοποιεί scan στους εικονικούς δίσκους (Basic) των hyperv virtual machines σε on line state αλλα και σε offline state των εν λόγω VM.	ΝΑΙ
2.18	Δυνατότητα προστασίας απο Brute Force Attack	ΝΑΙ
2.19	Ενσωματωμένη λειτουργία Sandbox καθών και πρόσθετη στο cloud.	ΝΑΙ
2.20	Application control για android συσκευές.	ΝΑΙ
2.21	Διαχείριση συσκευών (Device Control).	ΝΑΙ
2.22	Να υποστηρίζεται Η δυνατότητα επαναφοράς αρχείων από επιθέσεις ransomware.	
3	**Κεντρική διαχείριση**	
3.1	Να υποστηρίζεται η κεντρική διαχείριση όλων των λογισμικών προστασίας των σταθμών εργασίας / servers (antivirus client) μέσω κεντρικής cloud κονσόλας και με τη δυνατότητα εγκατάστασης τοπικά.	ΝΑΙ
3.2	Να υποστηρίζεται η δημιουργία πολλαπλών ομάδων με δυνατότητα εφαρμογής διαφορετικών πολιτικών / ρυθμίσεων για κάθε ομάδα.	ΝΑΙ
3.3	Λειτουργία προσωρινής απενεργοποίησης πολιτικής ανά client	ΝΑΙ

3.4	Να υποστηρίζεται η διαχείριση των ιστοσελίδων (επιτρεπόμενες, μη επιτρεπόμενες) σε ένα σταθμό εργασίας / server όπου είναι εγκατεστημένος ο antivirus client.	ΝΑΙ
3.5	Να υποστηρίζεται η αυτόματη ανίχνευση των σταθμών εργασίας που βρίσκονται στο τοπικό δίκτυο δεδομένων ακόμα κι αν αυτά δεν ανήκουν σε υπηρεσία ενεργού καταλόγου.	ΝΑΙ
3.6	Να υποστηρίζεται η εγκατάσταση και απεγκατάσταση του λογισμικού προστασίας (antivirus client) μέσω της κεντρικής κονσόλας.	ΝΑΙ

3.7	Να υποστηρίζεται ενεργοποίηση άδειας antivirus client σε σταθμό εργασίας ή server χωρίς σύνδεση στο διαδίκτυο internet (offline activation).	ΝΑΙ
3.8	Να υπάρχει η δυνατότητα εξαγωγής πακέτου με το πρόγραμμα προστασίας, διαχείρισης, τις αντίστοιχες πολιτικές - ρυθμίσεις τους και την άδεια ενεργοποίησης για τοπικές εγκαταστάσεις.	ΝΑΙ
3.9	Να μπορεί να γίνει εισαγωγή λίστας των υπολογιστών του δικτύου με τη χρήση ενδεικτικά CSV αρχείου ή text file ή Active Directory Scan ή Active Directory import ή Network Pool ή IP range κτλ.	ΝΑΙ
3.10	Να υποστηρίζεται έλεγχος και ειδοποίηση στην κεντρική κονσόλα για το αν υπάρχουν ενημερώσεις για λειτουργικά συστήματα Windows των σταθμών εργασίας / server όπου είναι εγκατεστημένος ο antivirus client.	ΝΑΙ
3.11	Να υποστηρίζεται η παρακολούθηση όλων των antivirus client και η παραγωγή αναφορών και στατιστικών σε μορφές (ενδεικτικά) PDF, PS, CSV, Charts καθώς και η αποστολή αυτοματοποιημένων emails των προαναφερόμενων αναφορών/στατιστικών.	ΝΑΙ
3.12	Να υπάρχει η δυνατότητα αυτόματων αναβαθμίσεων του προϊόντος.	ΝΑΙ
3.13	Επισκόπηση σε πραγματικό χρόνο για όλα τα τερματικά: υπολογιστές, διακομιστές, εικονικές μηχανές, διαχειριζόμενες κινητές συσκευές	ΝΑΙ
3.14	Επισκόπηση σε πραγματικό χρόνο για όλα τα τερματικά: υπολογιστές, διακομιστές, εικονικές μηχανές, διαχειριζόμενες κινητές συσκευές	ΝΑΙ
3.15	Ασφάλεια πρόσβασης RBAC Να διαθέτει σύστημα διαχείρισης προσβάσεων Role-Based Access Control για λεπτομερή εκχώρηση δικαιωμάτων διαχειριστή και χρήση κονσόλας σε συγκεκριμένες ομάδες δικτύου, ομάδες αντικειμένων.	ΝΑΙ
3.16	Πρόσβαση κονσόλας με έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA)	ΝΑΙ
3.17	Διαχείριση κινητών συσκευών (MDM -Mobile Device Management) που να καλύπτει συσκευές Android και Apple.	ΝΑΙ
3.18	Αποθετήριο Υλικού/Λογισμικού (Hardware/Software Inventory) Εντοπισμός και προβολή πληροφοριών για όλες τις εγκατεστημένες εφαρμογές λογισμικού στον οργανισμό, αλλά και για το εγκατεστημένο hardware.	ΝΑΙ
3.19	Να υποστηρίζει τα εργαλεία SIEM και να μπορεί να εξάγει όλες τις πληροφορίες καταγραφής στην ευρέως αποδεκτή μορφή JSON ή LEEF/CEF, επιτρέποντας την ενσωμάτωση με τα Κέντρα Επιχειρήσεων Ασφαλείας.	ΝΑΙ
4	**Ενημερώσεις**	

4.1	Οι ενημερώσεις από το διαδίκτυο για της κεντρικής βάσης malware θα γίνονται αυτόματα σε κεντρικό σημείο (server διαχείρισης) από το οποίο στην συνέχεια θα ενημερώνονται όλοι οι σταθμοί εργασίας και οι servers. Σε περίπτωση που δεν είναι διαθέσιμος ο server διαχείρισης, να υποστηρίζεται αυτόματη παράκαμψη του.	ΝΑΙ
4.2	Οι προαναφερόμενες ενημερώσεις θα προσφέρονται έως τη λήξη της περιόδου εγγυημένης λειτουργίας προμήθειας.	ΝΑΙ
4.3	Rollback σε προηγούμενη έκδοση του Signature File με ταυτόχρονη παύση των ενημερώσεων, επιλέγοντας το κεντρικά ή απευθείας από τον client.	ΝΑΙ
4.4	Να υπάρχει η δυνατότητα αυτόματων αναβαθμίσεων του προϊόντος.	ΝΑΙ
5	**Πρόσθετη cloud ασφάλεια για νέες απειλές**	

5.1	Να παρέχεται cloud reputation database για αμεσότερη προστασία από νέες απειλές.	ΝΑΙ
5.2	Να υπάρχει δυνατότητα ώστε τα ύποπτα δείγματα που δεν έχουν ακόμη επιβεβαιωθεί ως κακόβουλα και ενδέχεται να μεταφέρουν κακόβουλο λογισμικό να υποβάλλονται αυτόματα η και χειροκίνητα σε απομονωμένο cloud περιβάλλον του κατασκευαστή ώστε να εκτελεστούν και να αξιολογηθούν σε περιβάλλον προστατευμένης εκτέλεσης από τους Προηγμένους μηχανισμούς ανίχνευσης κακόβουλου λογισμικού του κατασκευαστή.	ΝΑΙ
5.3	Να ενημερώνεται αυτόματα η κονσόλα διαχειρίσεις για τα αποτελέσματα των υποβληθέντων αρχείων στο cloud.	ΝΑΙ
5.4	Η λύση του κατασκευαστή για τα υποβληθέντα αρχεία στο cloud να μπορεί να χρησιμοποιήσει διακομιστή μεσολάβησης για την προώθηση της σύνδεσης με τους διακομιστές του και για προσωρινή αποθήκευση των μεταφερόμενων δεδομένων.	ΝΑΙ
5.5	Να υπάρχει δυνατότητα εξαίρεσης ενός αρχείου που έχει ανιχνευθεί και υποβληθεί στο cloud του κατασκευαστή σε όλους τους υπολογιστές του δικτύου η και σε μερικούς εξ αυτόν.	ΝΑΙ
5.6	Να επιτρέπεται η ρύθμιση μέσω της κεντρικής κονσόλας διαχείρισης μέσω της οποίας θα ορίζονται οι προϋποθέσεις για τα αρχεία που θα υποβάλλονται στο cloud (π.χ. ενέργειες που θα πραγματοποιηθούν μετα την ανάλυση του αρχείου, υποβολή συγκεκριμένων file types, εξαίρεση υποβολής αρχείων με συγκεκριμένο extension, μέγιστο μέγεθος ενός υποβληθέντος αρχείου (MB)).	ΝΑΙ
6	**Ασφάλεια αρχείων**	
6.1	Δυνατότητα διαχείρισης της πλήρους κρυπτογράφησης δίσκου των διαχειριζόμενων σταθμών εργασίας Windows με πρόσθετο επίπεδο ασφάλειας πριν την εκκίνηση του υπολογιστή (pre-boot login), μέσω της κεντρικής κονσόλας.	ΝΑΙ
6.2	Να παρέχεται η επιλογή κρυπτογράφησης όλων των δίσκων η μόνο του δίσκου εκκίνησης του υπολογιστη η των υπολογιστων στο δικτυο μέσω της κεντρικής διαχείρισης.	ΝΑΙ
6.3	Να υπάρχει η δυνατότητα επιλογής χρησιμοποίησης υποστήριξης λειτουργικής μονάδας αξιόπιστης πλατφόρμας (TPM) ή Υποστήριξη μονάδας δίσκου αυτόματης κρυπτογράφησης Opal (OPAL) για την κρυπτογράφησή, με βάση το υλικό που είναι διαθέσιμο στους διαχειριζόμενους σταθμούς εργασίας.	ΝΑΙ

6.4	Να υπάρχει δυνατότητα να παραχθεί ένα μοναδικό αρχείου για κάθε υπολογιστή του δικτύου με σκοπό την αποκρυπτογράφηση του δίσκου μέσω αφαιρούμενου μέσου (usb,cd) και το οποίο θα δημιουργείται από την κεντρική κονσόλα διαχειρίσεις.	ΝΑΙ
6.5	Να υπάρχει δυνατότητα αποκρυπτογράφησης του δίσκου η των δίσκων του υπολογιστή η των υπολογιστών του δικτύου απευθείας μέσω πολιτικής από την κονσόλα κεντρικής διαχείρισης.	ΝΑΙ
6.6	Να υπάρχει η δυνατότητα επαναφοράς κωδικού χρήστη όσον αφορά την πιστοποίηση του πριν την εκκίνηση των windows σε κρυπτογραφημένους δίσκους (pre-boot login) από την κεντρική κονσόλα διαχείρισης.	ΝΑΙ
6.7	Να παρέχεται η δυνατότητα απενεργοποίησης της πιστοποίησης του χρήστη (pre-boot login) πριν την εκκίνηση του λειτουργικού συστήματος, σε κρυπτογραφημένο δίσκο συστήματος για καθορισμένο αριθμό επανεκκινήσεων του υπολογιστή.	ΝΑΙ
7	**On boot scan**	
7.1	Να υποστηρίζεται σάρωση και καθαρισμός κατά την εκκίνηση του σταθμού εργασίας / server (on-boot scan) χωρίς να χρειάζεται να ξεκινήσει το λειτουργικό σύστημα.	ΝΑΙ
8	**Ειδικές απαιτήσεις**	
8.1	Να υποστηρίζεται η εξαγωγή των ρυθμίσεων ενός antivirus client σε αρχείο και εισαγωγής των ρυθμίσεων σε άλλον από το ίδιο αρχείο.	ΝΑΙ
8.2	Να περιέχεται εφαρμογή που να καταγράφει την κατάσταση των agents / antivirus clients (εφαρμογές, processes, services κ.α) σε μία χρονική στιγμή (snapshot) και προαιρετικά να μπορεί να γίνει σύγκριση με προηγούμενη κατάσταση.	ΝΑΙ
8.3	Το μενού της κονσόλας διαχείρισης και των antivirus clients για τους σταθμούς εργασίας να διατίθεται και στην ελληνική γλώσσα.	ΝΑΙ
9	**Extended Detection and Response XDR-EDR**	
9.1	Να παρέχεται η δυνατότητα εισαγωγής κανόνων για τον εντοπισμό εφαρμογών κατά την εκτέλεση από προσωρινούς φακέλους, εντοπισμό αρχείων του Office με ενσωματωμένα scripts ή εκτελέσιμα.	ΝΑΙ
9.2	Να υπάρχει άμεση ειδοποίηση κατά την εμφάνιση γνωστού ransomware extension σε μια συσκευή και προβολή του συνολου των ενημερώσεων ransomware shield στην ίδια κονσόλα.	ΝΑΙ
9.3	Να υπάρχει δυνατότητα εντοπισμού αδύναμων στοιχείων με ταξινόμηση των υπολογιστών κατά αριθμό μοναδικών συναγερμών, προβληματικών συσκευών/χρηστών και δυνατότητα ανάλυσης root cause για γρήγορο εντοπισμό της πηγής μόλυνσης.	ΝΑΙ
9.4	Τα υπάρχει η δυνατότητα ταξινόμησης με βάση τη δημοτικότητα ή τη φήμη του αρχείου, την ψηφιακή υπογραφή, τη συμπεριφορά και τις πληροφορίες metadata και παραπομπή των στοιχείων με την πλατφόρμα MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™).	ΝΑΙ
9.5	Να παρέχεται η δυνατότητα αναζήτησης σε όλους τους υπολογιστές για την ύπαρξη της νέας απειλής και για ενδείξεις παραβίασης ότι η απειλή υπήρχε απο πριν και δυνατότητα αποκλεισμού περαιτέρω διείσδυσης στο δίκτυο.	ΝΑΙ

9.6	Να υποστηρίζεται προσαρμογή κανόνων ανίχνευσης που περιγράφουν τεχνικές επίθεσης στο συγκεκριμένο περιβάλλον του οργανισμού.	ΝΑΙ
9.7	Να υπάρχει δυνατότητα προβολής, φιλτραρίσματος, αποκλεισμού, καθαρισμού και ειδοποίησης των χρηστών για όλες τις εγκατεστημένες εφαρμογές και αρχεία αυτοματοποίησης(scripts).	ΝΑΙ
9.8	Να υποστηρίζει διερεύνηση και αποκατάσταση με κατανόηση περιέχομενου (Context aware) όπως και να υπάρχει δυνατότητα προσδιορισμού και ταξινόμησης των υπολογιστών αυτόματα ή χειροκίνητα ή με χρήση Active Directory.	ΝΑΙ
9.9	Να υποστηρίζει έλεγχο (Allow or Block) εφαρμογών ή αρχείων αυτοματοποίησης(scripts) βάση ομαδοποίησης υπολογιστών ή χρήστη και δυνατότητα ειδοποίησης μόνο για συγκεκριμένες ομάδες.	ΝΑΙ
9.10	Να διαθέτει πάνω από 800 προρυθμισμένους κανόνες με δυνατότητα επεξεργασίας με γλώσσα XML για εύκολη ρύθμιση ή δημιουργία νέων.	ΝΑΙ
9.11	Να υποστηρίζει λειτουργία εύκολης όπως και άμεσης απόκλισης	ΝΑΙ
9.12	Να επιτρέπει τον αποκλεισμό αρχείων βάση hash, να έχει την ικανότητα τερματισμού διαδικασιών, εισαγωγής σε καραντίνα και	ΝΑΙ

	απομόνωσης ή απενεργοποίησης μηχανημάτων εξ αποστάσεως με ένα κλίκ καθώς και να παρέχει πρότασεις για αποκατάσταση.	
9.13	Λεπτομερής ανάλυση Root Cause με αποτύπωση της αλυσίδας γεγονότων.	ΝΑΙ
9.14	Διαχείριση εφαρμογών με δυνατότητα αποκλεισμού με HASH.	ΝΑΙ
10	**Λογισμικό Mail Security**	
10.1	Προστασία emails από malware, spam και phishing web pages	ΝΑΙ
10.2	Δυνατότητα αποστολής αναφορών σε επιλεγμένους χρήστες και διαχειριστές για τα emails που βρίσκονται στην καραντίνα. Όπως και δυνατότητα διαγραφής ή απελευθέρωσης ενός email άμεσα.	ΝΑΙ
10.3	Δυνατότητα τοπικής καραντίνας με λειτουργία απελευθέρωσης email όπως και εξαίρεση συγκεκριμένων διεργασιών ή εφαρμογών από την Anti-malware σάρωση.	ΝΑΙ
10.4	Δυνατότητα αποθήκευσης και διαχείρισης μηνυμάτων καραντίνας από ένα σημείο μέσω του Quarantine mailbox ή MS Exchange quarantine.	ΝΑΙ
10.5	Δυνατότητα διαχείρισης της καραντίνας μέσω web browser με πρόσβαση είτε από το διαχειριστή συνολικά, είτε από κάθε χρήστη προσωποποιημένα.	ΝΑΙ
10.6	Δυνατότητα ελέγχου ύποπτων δειγμάτων που δεν έχουν ακόμη επιβεβαιωθεί ως κακόβουλα και ενδέχεται να μεταφέρουν κακόβουλο λογισμικό να υποβάλλονται αυτόματα η και χειροκίνητα σε απομονωμένο cloud περιβάλλον του κατασκευαστή ώστε να εκτελεστούν και να αξιολογηθούν από προηγμένους μηχανισμούς ανίχνευσης κακόβουλου λογισμικού.	ΝΑΙ
10.7	Δυνατότητα cluster σε λειτουργικά συστήματα windows server (συγχρονισμός των δεδομένων , των ρυθμίσεων και ειδοποιήσεων).	ΝΑΙ

10.8	Δυνατότητα καταγραφής σημαντικών συμβάντων του προγράμματος, καθώς και πλήρης καταγραφή αποτελεσμάτων σαρώσεων, ανιχνεύσεων/απειλών (logs).	ΝΑΙ
10.9	Υποστήριξη Remote monitoring and management (RMM).	ΝΑΙ
10.10	Πραγματοποίηση ελέγχων SPF, DKIM, DMARC.	ΝΑΙ
10.11	Λειτουργία σάρωσης βάσης on-demand.	ΝΑΙ
10.12	Υποστήριξη κανόνων φιλτραρίσματος με βάση τις ιδιότητες των emails (π.χ. τύπος επισυναπτόμενου) και αντιστοίχιση ενεργειών.	ΝΑΙ
10.13	Υποστήριξη λιστών εγκεκριμένων/μη αποδεκτών IPs, domains, αποστολέων.	ΝΑΙ
10.14	Υποστήριξη επιπλέον υπηρεσιών RBL/DNSBL.	ΝΑΙ
10.15	Δυνατότητα λειτουργίας Greylisting.	ΝΑΙ
10.16	Δυνατότητα σάρωσης Office 365 mailbox scan για περιβάλλοντα Exchange Hybrid.	ΝΑΙ
10.17	Δυνατότητα Backscatter protection.	ΝΑΙ
10.18	Δυνατότητα διαχείρισης και μέσω περιβάλλοντος γραμμής εντολών.	ΝΑΙ
10.19	Δυνατότητα διαχείρισης του προϊόντος από κεντρική κονσόλα διαχείρισης.	ΝΑΙ

11	**Λογισμικό Cloud Office security για Microsoft 365 και Google Workspace**	
11.1	Δυνατότητα προστασίας των cloud Microsoft 365, Exchange Online όπως και Microsoft OneDrive(να συμπεριλαμβάνονται τα Microsoft 365 plans: enterprise, business, education.)	ΝΑΙ
11.2	Δυνατότητα προστασίας Google Workspace, Gmail και Google Drive.	
11.3	Δυνατότητα προστασίας Microsoft Teams και Sites.	ΝΑΙ
11.4	Να υπάρχει δυνατότητα multi-tenant προστασίας.	ΝΑΙ
11.5	Να υποστηρίζεται προστασία: Antispam, Anti-Phishing, AntiMalware.	ΝΑΙ
11.6	Να υπάρχει δυνατότητα διαχείριση καραντίνας με εναλλαγές ανάμεσα σε καρτέλες Exchange Online, OneDrive, Team groups και SharePoint sites.	ΝΑΙ
11.7	Να υποστηρίζετε δημιουργία και κατανομή πολιτικών ανά γκρούπ ή ανά χρήστη.	ΝΑΙ
11.8	Να υπάρχει η δυνατότητα προστασίας ανά γραμματοκιβώτιο όπως και κοινών γραμματοκιβωτίων(Shared Mailboxes).	ΝΑΙ

11.9	Να υπάρχει η δυνατότητα δημιουργίας αναφορών με επιλεγμένα κριτήρια καθώς και προγραμματισμό παραγωγής αναφορών(Scheduled reports).	ΝΑΙ
11.10	Να υπάρχει η δυνατότητα αποστολής αναφορών σε πολλαπλούς αποδέκτες.	ΝΑΙ
11.11	Να υπάρχει δυνατότητα αυτόματου καθαρισμού παλαιότερων αρχείων αναφοράς(Log files rotation).	ΝΑΙ
11.13	Δυνατότητα ανίχνευσης potentially unwanted, suspicious, unsafe applications.	ΝΑΙ
11.13	Δυνατότητα προστασίας σε πραγματικό χρόνο (Real-time).	ΝΑΙ
11.14	Δυνατότητα προστασίας με υποβοήθηση μάθησης μηχανής (Machine learning).	ΝΑΙ
11.15	Δυνατότητα αλλαγής προφίλ ανίχνευσης(Aggressive, Balanced, Cautious, Off).	ΝΑΙ
11.16	Δυνατότητα αναφοράς ψευδώς θετικών(False positive) και ψευδώς αρνητικών(False negative) δειγμάτων	ΝΑΙ
11.17	Προβολή στατιστικών σε μια σελίδα με ανανέωση ανά 10 λεπτά(Dashboard).	ΝΑΙ
11.18	Να ενσωματόνεται σαν υπηρεσία (SaaS)	ΝΑΙ
12	**Ενημερώσεις ασφαλείας και ευπαθειών για λειτουργικά συστήματα και εφαρμογές Windows**	
12.1	Διαχείριση ενημερώσεων ασφαλείας και ευπαθειών για λειτουργικά συστήματα και εφαρμογές Windows και Linux (Patch Management/Vulnerability).	ΝΑΙ
12.2	Αυτοματοποιημένη σάρωση εφαρμογών (Automated scanning).	ΝΑΙ
12.3	Καθορισμός προτεραιότητας με βάση τη σοβαρότητα (Severity-based prioritization), πλήρης ορατότητα διαθέσιμων αναβαθμίσεων απο κεντρικό σημείο.	ΝΑΙ
12.4	Αυτοματοποιημένη ή κατ' απαίτηση αναβάθμιση εφαρμογών μέσω πολιτικής (Automatic and manual patching)	ΝΑΙ
13	**Επαλήθευση ταυτότητας πολλαπλών παραγόντων (Multifactor authentication)**	
13.1	Αποτροπή παραβιάσεων σε κρίσιμες υποδομές.	ΝΑΙ
13.2	Πολλαπλοί τρόποι για αυθεντικοποίηση.	ΝΑΙ
13.3	Να υπάρχει η δυνατότητα χρήσης MFA σε υποδομές, εικονικών ιδιωτικών δικτύων (VPN), remote desktop (RDP), διαδικτυακής πρόσβασης στο Outlook (OWA),VMware Horizon View και υπηρεσιών RADIUS-based.	ΝΑΙ

13.4	Δυνατότητα αποστολής κωδικού (OTP) ή single tap το οποίο να λειτουργεί σε συσκευές Android και IOS.	ΝΑΙ
13.5	Δυνατότητα integration τοσο σε cloud όσο και σε on-premise εφαρμογές.	ΝΑΙ
13.6	Δυνατότητα integration με Active Directory περιβάλλοντα.	ΝΑΙ
13.7	Να μπορεί να πραγματοποιηθεί απομακρυσμένη διαχείριση από κονσόλα Cloud ή on-premise.	ΝΑΙ
13.8	Να υπάρχει η δυνατότητα extension του MFA σε προσαρμοσμένες εφαρμογές με API και SDK integration.	ΝΑΙ
13.9	Η λύση θα πρέπει είναι συμβατή με OATH tokens και με Active Directory, Entra ID, Okta, LDAP	ΝΑΙ
13.10	Η λύση πρέπει να διαθέτει IP address whitelisting, ώστε ο διαχειριστής να μπορεί να ορίζει εγκεκριμένες IP διευθύνσεις ή εύρη IP από τα οποία δεν θα ζητείται 2FA/OTP, όπου αυτό υποστηρίζεται από το εκάστοτε προστατευόμενο σενάριο πρόσβασης.	ΝΑΙ
13.11	Η λύση πρέπει να υποστηρίζει χρήση third-party TOTP authenticator applications, όπως Google Authenticator, Microsoft Authenticator και λοιπές εφαρμογές που υποστηρίζουν OATH/TOTP, χωρίς υποχρεωτικό κλείδωμα του φορέα σε αποκλειστική εφαρμογή του κατασκευαστή.	ΝΑΙ

Πρότυπα διασφάλισης ποιότητας και πρότυπα περιβαλλοντικής διαχείρισης

Ο ανάδοχος να διαθέτει τα παρακάτω πιστοποιητικά, τα οποία θα πρέπει να προσκομίσει μαζί με την προσφορά:

- **ISO 9001: 2015** ή ισοδύναμο ή μεταγενέστερης έκδοσής του στα πεδία εφαρμογής του σχεδιασμού, ανάπτυξης, εγκατάστασης υποστήριξης και συντήρησης πληροφοριακών συστημάτων
- **ISO 27001: 2013** ή ισοδύναμο ή μεταγενέστερης έκδοσής του στο πεδίο εφαρμογής της Ασφάλειας Πληροφοριών
- **ISO 14001: 2015** ή ισοδύναμο ή μεταγενέστερης έκδοσής του στο πεδίο εφαρμογής διαχείριση του περιβάλλοντος που καλύπτει τον εντοπισμό περιβαλλοντικών επιπτώσεων (ρύποι, απόβλητα, κατανάλωση ενέργειας κ.λπ.)

Η αναθέτουσα αρχή αναγνωρίζει ισοδύναμα πιστοποιητικά που έχουν εκδοθεί από φορείς διαπιστευμένους από ισοδύναμους Οργανισμούς διαπίστευσης, εδρεύοντες και σε άλλα κράτη - μέλη. Επίσης, κάνει δεκτά άλλα αποδεικτικά στοιχεία για ισοδύναμα μέτρα διασφάλισης ποιότητας, εφόσον ο ενδιαφερόμενος οικονομικός φορέας δεν είχε τη δυνατότητα να αποκτήσει τα εν λόγω πιστοποιητικά εντός των σχετικών προθεσμιών για λόγους για τους οποίους δεν ευθύνεται ο ίδιος,
υπό την προϋπόθεση ότι ο οικονομικός φορέας αποδεικνύει ότι τα προτεινόμενα μέτρα διασφάλισης ποιότητας πληρούν τα απαιτούμενα πρότυπα διασφάλισης ποιότητας.

ΠΑΡΑΡΤΗΜΑ ΙΙ – ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ ΠΙΝΑΚΑΣ 1 : Τεχνικές Προδιαγραφές				
Α/Α	**Προδιαγραφή**	**ΑΠΑΙΤΗΣΗ**	**ΑΠΑΝΤΗΣΗ**	**ΠΑΡΑΤΗΡΗΣΕΙΣ**
1.	Γενικές απαιτήσεις			
1.1.	Ο ανάδοχος να διαθέτει τα παρακάτω πιστοποιητικά, τα οποία θα πρέπει να προσκομίσει μαζί με την προσφορά: • **ISO 9001: 2015** ή ισοδύναμο ή μεταγενέστερης έκδοσής του στα πεδία εφαρμογής του σχεδιασμού, ανάπτυξης, εγκατάστασης υποστήριξης και συντήρησης πληροφοριακών συστημάτων • **ISO 27001: 2013** ή ισοδύναμο ή μεταγενέστερης έκδοσής του στο πεδίο εφαρμογής της Ασφάλειας Πληροφοριών • **ISO 14001: 2015** ή ισοδύναμο ή μεταγενέστερης έκδοσής του στο πεδίο εφαρμογής διαχείριση του περιβάλλοντος που καλύπτει τον εντοπισμό περιβαλλοντικών επιπτώσεων (ρύποι, απόβλητα, κατανάλωση ενέργειας κ.λπ.) •	ΝΑΙ		

Επίσης, Ο υποψήφιος Ανάδοχος θα πρέπει να διαθέτει τουλάχιστον έναν (1), τουλάχιστον, εξειδικευμένοπιστοποιημένο τεχνικό, για την υλοποίηση του έργου.

Υποβάλλεται το παρόν πρακτικό, με τις προδιαγραφές προς διαβούλευση, προκειμένου να προκηρυχθεί ο σχετικός διαγωνισμός και να εξεταστεί η προκήρυξη του διαγωνισμού με σύντμηση προθεσμιών λόγω του επείγοντος.