Α/Α	ΠΕΡΙΓΡΑΦΗ ΠΡΟΔΙΑΓΡΑΦΗΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ
	Γενικά		
	Λογισμικό Προστασίας από ιούς (Antivirus) με κεντρική κονσόλα διαχείρισης και 1100 άδειες χρήσης με χρονική διάρκεια 3 χρόνια	ΝΑΙ	
	Υποστηριζόμενα λειτουργικά - πλατφόρμες		
1	Το λογισμικό θα πρέπει να παρέχει προστασία για α) Σταθμούς εργασίας με λειτουργικό Windows ενδεικτικά : • Windows 11 October 2024 Update (24H2) • Windows 11 October 2023 Update (23h2) • Windows 10 November 2022 Update (22H2) • Windows 11 September 2022 Update (22h2) • Windows 11 (initial release) • Windows 10 November 2021 Update (21H2) • Windows 10 May 2021 Update (21H1) • Windows 10 October 2020 Update (20H2) • Windows 10 May 2020 Update (20H1) • Windows 10 May 2019 Update (19H1) • Windows 10 October 2018 Update (Redstone 5) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 Creators Update (Redstone 2) • Windows 10 Anniversary Update (Redstone 1) • Windows 10 November Update (Threshold 2) • Windows 10 (initial release) • Windows 8.1 • Windows 8 • Windows 7* SP1 Windows Server • Windows Server 2025 64x • Windows Server 2022 Core • Windows Server 2022 • Windows Server 2019 Core • Windows Server 2019 • Windows Server 2016 • Windows Server 2016 Core • Windows Server 2012 R2(**) • Windows Server 2012(**) • Windows Small Business Server (SBS) 2011 • Windows Server 2008 R2(*) (**)	ΝΑΙ	

	β)) Σταθμούς εργασίας με λειτουργικό Linux : • Ubuntu 16.04 (ή νεότερο) • Red Hat Enterprise Linux / CentOS 6.0 or higher • SUSE Linux Enterprise Server 11 SP4 (ή νεότερο) • openSUSE Leap 15.4-15.5 • Fedora 37 - 40 • Debian 9 (ή νεότερο) • Oracle Linux 7.χ (ή νεότερο) • Amazon Linux v2 β)) Σταθμούς εργασίας με λειτουργικό Mac : • macOS Sequoia (15.x) • macOS Sonoma (14.x) • macOS Ventura (13.x) • macOS Monterey (12.x) • macOS Big Sur (11.x)		
2	Η κονσόλα διαχείρισης να μπορεί να εγκατασταθεί σε VMware, Citrix, Hyper-V, Nutanix Prism, Red Hat Enterprise virtualization, Oracle VM	ΝΑΙ	
3	Να είναι εφικτή η ενσωμάτωση του Active Directory στην κονσόλα διαχείρισης	ΝΑΙ	
4	Να είναι εφικτή η ενσωμάτωση των Microsoft Azure, Amazon EC2, VMware NSX-V, VMware NSX-T & Nutanix Prism στην κονσόλα διαχείρισης	ΝΑΙ	
	Περιβάλλον διαχείρισης		
5	Όλες οι απαιτούμενες δυνατότητες να προσφέρονται από τον ίδιο κατασκευαστή.	ΝΑΙ	
6	Να υποστηρίζονται όλες οι λειτουργίες μέσω μίας κεντρικοποιημένης κονσόλας στο Cloud ή On Premise και χωρίς να απαιτείται η εγκατάσταση κάποιου επιπλέον client.	ΝΑΙ	
7	Να υποστηρίζει κεντρική διαχείριση μέσω κονσόλας με τις παρακάτω δυνατότητες: • Να διαθέτει σύστημα κεντρικής διαχείρισης (Remote installation, monitoring, updates κλπ.) για όλα τα απαιτούμενα εργαλεία προστασίας • Να υπάρχει δυνατότητα απομακρυσμένης εγκατάστασης / απεγκατάστασης	ΝΑΙ	
8	Να υποστηρίζει τη δυνατότητα κεντρικής σάρωσης	ΝΑΙ	

	των virtual μηχανών για την εξοικονόμηση των πόρων του Host		
9	Να παρέχει δυνατότητα σε κάθε client να μπορεί να γίνει update server για τους υπόλοιπους υπολογιστές του δικτύου	ΝΑΙ	
10	Να έχει δυνατότητα αυτόματης ανίχνευσης & καθαρισμού απειλών σε πραγματικό χρόνο	ΝΑΙ	
11	Να έχει δυνατότητα ανίχνευσης απειλών τόσο σε πραγματικό χρόνο και μετά από απαίτηση του χρήστη (on demand)	ΝΑΙ	
12	Ανίχνευση & καθαρισμός του δικτύου από malware μετά από απαίτηση	ΝΑΙ	
13	Να αναζητά ενημερώσεις μέσω δικτύου τουλάχιστον ανά μία ώρα ενώ η διαδικασία ενημέρωσης να μην απαιτεί την παρέμβαση του χρήστη	ΝΑΙ	
14	Να υποστηρίζει τη δυνατότητα προγραμματισμού της της πρόσβασης σε κατηγορίες ιστοτόπων τόσο για έναν υπολογιστή όσο και για ολόκληρες ομάδες	ΝΑΙ	
15	Επικοινωνία του Software μόνο με IP δηλαδή να δουλέψει σε περιπτώσεις όπου δεν υπάρχουν υπηρεσίες ονοματοδοσίας (DNS)	ΝΑΙ	
16	Να μπορεί να γίνει αυτόματη ανίχνευση των υπολογιστών που βρίσκονται στο τοπικό δίκτυο, ακόμα και αν αυτά δεν ανήκουν σε Active Directory	ΝΑΙ	
17	Παραγωγή αναφορών & στατιστικών σε διάφορες μορφές (txt, csv, charts) για ανάγνωση τόσο με on-demand όσο και προγραμματισμένη εκτέλεση	ΝΑΙ	
18	Να παρέχεται η δυνατότητα αποστολής ειδοποιήσεων μέσω email	ΝΑΙ	
19	Να παρέχεται η δυνατότητα εξαγωγής των ειδοποιήσεων σε syslog servers ή SIEM συστήματα (**συμβατότητα με Wazuh Server v4.11.2**)	ΝΑΙ	
20	Υποστήριξη διαφορετικών ομάδων & υποομάδων χρηστών με δυνατότητα εφαρμογής διαφορετικών ρυθμίσεων για κάθε μια	ΝΑΙ	
21	Δυνατότητα αυτόματης αλλαγής των ρυθμίσεων ασφαλείας (πολιτικών) βάσει δικτυακών κανόνων ή βάσει συγκεκριμένων χρηστών	ΝΑΙ	
22	Μεταφορά άδειας σε νέο υπολογιστή (ανεξαρτήτως λειτουργικού συστήματος) απλά διακόπτοντας τη χρήση του παλαιού	ΝΑΙ	
23	Να υπάρχει η δυνατότητα αναβάθμισης σε EDR τεχνολογία μέσα από την ίδια κονσόλα διαχείρισης χωρίς να απαιτείται επιπλέον client	ΝΑΙ	
24	Να υποστηρίζει την προσθήκη δυνατότητας εγκατάστασης και διαχείρισης patching μέσα από το ίδιο περιβάλλον διαχείρισης ασφαλείας, χωρίς να απαιτείται κάποιος επιπλέον client	ΝΑΙ	
25	Στην patch management λειτουργία, να υποστηρίζεται patching και για 3rd party windows εφαρμογές όπως	ΝΑΙ	

	και Linux και Mac λειτουργικών		
26	Να υποστηρίζει τη προσθήκη δυνατότητας εγκατάστασης και διαχείρισης της κρυπτογράφησης δίσκου μέσα από το ίδιο περιβάλλον διαχείρισης ασφαλείας, χωρίς να απαιτείται κάποιος επιπλέον client	ΝΑΙ	
27	Στην encryption λειτουργία να υποστηρίζεται full disk encryption για Windows και Mac λειτουργικά	ΝΑΙ	
28	Στην encryption λειτουργία τα κλειδιά κρυπτογράφησης να είναι αποθηκευμένα στην κονσόλα διαχείρισης ώστε να είναι εφικτή η ανάκτησή τους	ΝΑΙ	
29	Μέσα από το περιβάλλον διαχείρισης και χωρίς την εγκατάσταση επιπλέον client, να υποστηρίζει τη λειτουργία ελέγχου των λειτουργικών, των εφαρμογών καθώς και ευπαθειών που προέρχονται από τον ανθρώπινο παράγοντα με σκοπό την ελαχιστοποίηση του κινδύνου επίθεσης (Risk Management) από λανθασμένες ρυθμίσεις, ευπάθειες εφαρμογών ή ενέργειες χρηστών. Επίσης να παρέχονται περισσότερες πληροφορίες για το κάθε θέμα μαζί με την αλλαγή που συνιστάται στην εκάστοτε ρύθμιση. Επιπλέον, μέσα από το ίδιο περιβάλλον να παρέχεται και η δυνατότητα εφαρμογής των διορθωτικών ενεργειών.	ΝΑΙ	
30	Να παρέχεται διαχείριση Firewall για Windows Servers	ΝΑΙ	
	Προστασία υπολογιστών		
31	Να παρέχεται cloud reputation database για αμεσότερη προστασία από νέες απειλές.	ΝΑΙ	
32	Θα πρέπει να ενσωματώνει τεχνολογίες που του επιτρέπουν να δρα προληπτικά κατά των απειλών και να αποκλείει τις επιθέσεις, ανεξάρτητα από το μέσο εξάπλωσής τους, USB stick, δίκτυο, κλπ.	ΝΑΙ	
33	Να παρέχει δυνατότητα ανίχνευσης και καθαρισμού όλων των τύπων απειλών (viruses, Trojans, dialers, spyware, jokes, hoaxes , ransomware κλπ.)	ΝΑΙ	
34	Να υποστηρίζει τη δυνατότητα ανίχνευσης απειλών σε πραγματικό χρόνο σε Linux λειτουργικά	ΝΑΙ	
35	Να υποστηρίζει τεχνολογίες ανίχνευσης απειλών όπως signature-based, machine learning, heuristic-based και anti-stealth (rootkit detection), καθώς και file-less επιθέσεων και για την ανίχνευση αγνώστων απειλών	ΝΑΙ	
36	Να προσφέρει προστασία απέναντι σε εξελιγμένες απειλές με πολλαπλούς μηχανισμούς. Να υπάρχει η δυνατότητα επαναφοράς των αρχείων που δέχτηκαν επίθεση ransomware ώστε τα αρχεία να παραμένουν διαρκώς ασφαλή.	ΝΑΙ	
37	Να προσφέρει σάρωση σε pre-execution στάδιο με	ΝΑΙ	

	machine learning μηχανισμούς για την ανίχνευση εξελιγμένων επιθέσεων		
38	Να υποστηρίζει τη δυνατότητα ανίχνευσης exploits καθώς και αποκλεισμού τους.	ΝΑΙ	
39	Να υποστηρίζει sandboxing τεχνολογία μέσα από την ίδια κονσόλα διαχείρισης χωρίς να απαιτείται καμία επιπλέον εγκατάσταση client	ΝΑΙ	
40	Να παρέχεται forensic ανάλυση των επιθέσεων που ανιχνεύονται και αντιμετωπίζονται αυτόματα. Επίσης να υπάρχει η δυνατότητα ενεργειών έρευνας αλλά και αποκατάστασης μέσα από το ίδιο περιβάλλον.	ΝΑΙ	
41	Να παρέχει προστασία από απειλές οι οποίες εκμεταλλεύονται δικτυακές ευπάθειες όπως brute force επιθέσεις ή password stealers. Επίσης να προστατεύει από port scanning επιθέσεις.	ΝΑΙ	
42	Να παρέχει τη δυνατότητα ελέγχου αποστολής δεδομένων μέσω email ή web traffic	ΝΑΙ	
43	Να παρέχει τη δυνατότητα αποκλεισμού εκτέλεσης εγκατεστημένων εφαρμογών (blacklisting) μέσω κανόνων	ΝΑΙ	
44	Να παρέχει λίστα των εφαρμογών που χρησιμοποιούνται καθώς και να προσφέρεται η δυνατότητα εκτέλεσης μόνο συγκεκριμένων εφαρμογών (whitelisting)	ΝΑΙ	
45	Να υποστηρίζει τον έλεγχο των εφαρμογών που συνδέονται στο internet καθώς και να είναι εφικτή η δημιουργία firewall κανόνων βάσει σύνδεσης, δικτύων ή εφαρμογών	ΝΑΙ	
46	Να υποστηρίζει τον έλεγχο των συνδεδεμένων συσκευών (device control) και να παρέχει επίσης τη δυνατότητα εξαίρεσης από τον κανόνα συγκεκριμένων συσκευών	ΝΑΙ	
47	Να παρέχει την προσθήκη της δυνατότητας Integrity Monitoring η οποία ελέγχει και επικυρώνει τις αλλαγές που πραγματοποιούνται σε Windows και Linux τερματικά. Η διαχείριση του Integrity Monitoring θα γίνει μέσα από την ίδια κονσόλα χωρίς την εγκατάσταση επιπλέον client.	ΝΑΙ	
48	Να παρέχεται η προσθήκη δυνατότητας προστασίας storages	ΝΑΙ	
50	Να υπάρχει έλεγχος Κατά της Παραβίασης (Anti tampering) ο οποίος επιτρέπει να βλέπετε πότε ανιχνεύονται ευάλωτοι οδηγοί στα τελικά σημεία και πότε γίνονται προχωρημένες προσπάθειες επίθεσης.	ΝΑΙ	
51	Να παρέχεται η προσθήκη δυνατότητας δημιουργίας report που να δείχνει κατά πόσο ο οργανισμός είναι συμβατός με κανονισμούς όπως το NIS2, ISO , SOC2,		

	DORA κτλ		
	Email προστασία για Microsoft Exchange on-premise		
52	Έλεγχος και προστασία εισερχόμενου και εξερχομένου ηλεκτρονικού ταχυδρομείου όλων των χρηστών	ΝΑΙ	
53	Να παρέχεται antispam προστασία για την εισερχόμενη αλληλογραφία σε με σάρωση που ελέγχει για κυριλλικούς/ασιατικούς χαρακτήρες, URLs, σεξουαλικό περιεχόμενο καθώς και να γίνεται έλεγχος βάσει RBL servers και heuristic μηχανισμών	ΝΑΙ	
54	Να υπάρχει η δυνατότητα δημιουργίας κανόνων βάσει keywords ή ολόκληρων φράσεων στο subject ή στο κύριο μέρος των μηνυμάτων	ΝΑΙ	
55	Να υποστηρίζει τη δυνατότητα attachment filtering όπου ο έλεγχος των αρχείων να γίνεται βάσει των headers του αρχείου για την ορθότερη ανίχνευση των τύπων των αρχείων	ΝΑΙ	
	Διακρίσεις		
56	Να έχει διακρίσεις σε συγκριτικά τεστ από αξιόπιστους διεθνείς οργανισμούς (π.χ. Virus Bulletin, AV-comparatives, MITRE att&ck) από το 2011 και μετά.	ΝΑΙ	
57	Να έχει διακριθεί και από τους τρεις φορείς Forrester, Gartner και MITRE ATT&CK®	ΝΑΙ	