ΤΜΗΜΑ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

ΠΡΟΜΗΘΕΙΑ
ΕΦΑΡΜΟΓΩΝ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΔΗΜΟΤΙΚΗ
ΕΠΙΧΕΙΡΗΣΗ
ΥΔΡΕΥΣΗΣ
ΑΠΟΧΕΤΕΥΣΗΣ
Π Α Τ Ρ Α Σ

CPV: 48732000-8

Κ.Α.Ε.: 16.17.005.531

1. **Τεχνικές Προδιαγραφές**
2. **Προϋπολογισμός**
3. **Έντυπο προσφοράς τεχνικών προδιαγραφών**
4. **Προϋπολογισμός Προσφοράς**

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

ΔΕΥΑΠ

ΤΜΗΜΑ
ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

Οι προδιαγραφές αφορούν εφαρμογές ασφάλειας δεδομένων που είναι αναγκαίο να εγκατασταθούν στον μηχανογραφικό εξοπλισμό της ΔΕΥΑΠ ώστε να επιτευχθεί κατάλληλο επίπεδο ασφάλειας για την συμμόρφωση προς τον Γενικό Κανονισμό Προστασίας Δεδομένων.

Α. ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΦΑΡΜΟΓΗΣ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ – ESET Antivirus	
1.1	Για την προστασία από κακόβουλο λογισμικό στα τερματικά και τους εξυπηρετητές του έργου θα προσφερθούν άδειες ESET Endpoint antivirus
1.2	ESET Endpoint antivirus
1.3	Υποστήριξη για τις εξής πλατφόρμες λειτουργικών συστημάτων: - Microsoft Windows XP, Vista, 7, 8, 10 - Microsoft Windows Server 2003(R2), 2008(R2), 2012(R2),2016 - Linux με kernel 2.6.x και νεότερα - Mac OS X - Android 4 ή νεότερο
2	**Εξειδίκευση των απαιτήσεων προστασίας**
2.1	Δυνατότητα ανίχνευσης και καθαρισμού όλων των τύπων απειλών: viruses, trojans, dialers, spyware, jokes, hoaxes
2.2	Δυνατότητα αυτόματης ανίχνευσης & καθαρισμού των προαναφερθέντων απειλών σε πραγματικό χρόνο
2.3	Δυνατότητα επιλογής ανίχνευσης malware σε δικτυακές τοποθεσίες, on-demand και σε πραγματικό χρόνο
2.4	Να παρέχεται cloud reputation database για αμεσότερη προστασία από νέες απειλές
2.5	Υποστήριξη τεχνολογίων Advanced heuristics/DNA/Smart Signatures για δυνατότητα ανίχνευσης άγνωστων ιών
2.6	Δυνατότητα για host intrusion prevention system
2.7	Η ανανέωση των signature files να είναι incremental
2.8	Δυνατότητα Rollback των Signature Files σε προηγούμενη έκδοση του με ταυτόχρονη παύση των ενημερώσεων, επιλέγοντας το κεντρικά ή απευθείας από το client
2.9	Δυνατότητα κατεβάσματος ενημερώσεων με νεότερες engines που βρίσκονται σε δοκιμαστικό στάδιο, επιλέγοντας το κεντρικά ή απευθείας από το client
2.10	Δυνατότητα να μπορεί να γίνει ένα client update server για τα υπόλοιπα clients του δικτύου χωρίς την εγκατάσταση τμήματος της κονσόλας διαχείρισης ή άλλου εξωτερικού software
2.11	Δυνατότητα για SSL/TLS filtering στα πρωτόκολλα HTTPS, IMAPS, POP3S
2.12	Δυνατότητα μπλοκαρίσματος όλων των σελίδων του Internet σε ένα client
2.13	Δυνατότητα εξαγωγής των ρυθμίσεων ενός client σε αρχείο και εισαγωγής των ρυθμίσεων σε άλλο client από το ίδιο αρχείο.
2.14	Να υπάρχει ενσωματωμένη εφαρμογή που να καταγράφει την κατάσταση του

ΤΜΗΜΑ
ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

	συστήματος (εφαρμογές, processes, services κ.α) – κατόπιν εντολής τοπικά ή από την κονσόλα - σε μία χρονική στιγμή (snapshot) και να αποθηκεύει τα αποτελέσματα για σύγκριση τους με την κατάσταση του συστήματος από διαφορετική χρονική στιγμή.
2.15	Παροχή Bootable Media που να περιέχει το antivirus ώστε να δίνει τη δυνατότητα για καθαρισμό του συστήματος χωρίς να χρειάζεται να ξεκινήσει το λειτουργικό σύστημα
3	**Απαιτήσεις απομακρυσμένης και κεντρικής διαχείρισης**
3.1	Κεντρική διαχείριση όλων των clients των τερματικών και servers
3.2	Υποστήριξη πολλαπλών ομάδων και υπο-ομάδων με δυνατότητα εφαρμογής διαφορετικών πολιτικών για κάθε περίπτωση
3.3	Λειτουργία προσωρινής απενεργοποίησης πολιτικής ανά client
3.4	Δυνατότητα για ομάδες διαχείρισης με βάση ιδιότητες υπολογιστών, π.χ. αυτόματη ομαδοποίηση υπολογιστών με Windows 10
3.5	Εγκατάσταση & απεγκατάσταση της προστασίας μέσω κεντρικής κονσόλας (Remote deployment)
3.6	Να υπάρχει η δυνατότητα εξαγωγής ενιαίου πακέτου με το πρόγραμμα προστασίας, σύνδεση διαχείρισης, πολιτικές και την άδεια ενεργοποίησης
3.7	Να παρέχεται ξεχωριστό εργαλείο ανίχνευσης τερματικών και push εγκατάστασης του παραπάνω ενιαίου πακέτου
3.8	Επικοινωνία του client μόνο με IP, δηλαδή να δουλέψει σε περιπτώσεις όπου δεν υπάρχουν υπηρεσίες ονοματοδοσίας (DNS servers)
3.9	Να μπορεί να γίνει αυτόματη ανίχνευση των τερματικών που βρίσκονται στο τοπικό δίκτυο, ακόμα κι αν αυτά δεν ανήκουν σε Active Directory
3.10	Να μπορεί να γίνει εισαγωγή λίστας των τερματικών του δικτύου με τη χρήση CSV αρχείου
3.11	Η επικοινωνία των servers και των clients να διασφαλίζεται μέσω certificate
3.12	Να μπορεί να γίνει ενεργοποίηση σε δίκτυο χωρίς σύνδεση στο internet (offline activation)
3.13	Να γίνεται ενημέρωση από το Internet από κεντρικό σημείο, από το οποίο στην συνέχεια θα ενημερωθούν όλοι οι clients του δικτύου
3.14	Τα antivirus να μπορούν να λάβουν signature files μέσω HTTP proxy cache, με αυτόματη παράκαμψή του σε περίπτωση που δεν είναι διαθέσιμος ο proxy server
3.15	Να περιλαμβάνεται έλεγχος και ειδοποίηση για το αν υπάρχουν ενημερώσεις για το λειτουργικό σύστημα, καθώς και η δυνατότητα να δοθεί εντολή ενημέρωσης λειτουργικού συστήματος
3.16	Παρακολούθηση όλων των clients και παραγωγή reports και στατιστικών σε πολλές μορφές (Προγραμματισμένα emails, PDF, PS, CSV, Charts)
3.17	Δυνατότητα ενιαίας καραντίνας αρχείων που ανιχνεύθηκαν για όλο το δίκτυο, με δυνατότητες προβολής clients ανά απειλή, εξαγωγή και εξαίρεση
3.18	Ο server διαχείρισης να μπορεί να γίνει εγκατάσταση με τις παρακάτω μεθόδους. α) Αυτοματοποιημένα με τη μορφή Wizard β) Χειροκίνητα, εκτελώντας ανεξάρτητα τα τμήματα της εγκατάστασης γ) Ως προεγκατεστημένο Virtual Appliance με Linux OS
3.19	Η εγκατάσταση της βάσης δεδομένων της κονσόλας θα πρέπει απαραίτητα να γίνεται σε ένα υπολογιστή οπουδήποτε στο εσωτερικό δίκτυο της εταιρίας και όχι σε εξωτερικό δίκτυο π.χ. Cloud.
3.20	Να παρέχεται εργαλείο ελέγχου κατάστασης αδειών και αριθμού ενεργοποιήσεων,

ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΥΔΡΕΥΣΗΣ ΑΠΟΧΕΤΕΥΣΗΣ ΠΑΤΡΑΣ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

ΔΕΥΑΠ

ΤΜΗΜΑ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

ΔΗΜΟΤΙΚΗ
ΕΠΙΧΕΙΡΗΣΗ
ΥΔΡΕΥΣΗΣ
ΑΠΟΧΕΤΕΥΣΗΣ
ΠΑΤΡΑΣ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

	ακόμα κι αν αυτές έχουν γίνει εκτός της κεντρικής κονσόλας (stand alone εγκαταστάσεις)
3.21	Να παρέχεται η δυνατότητα διαχείρισης Android και iOS συσκευών μέσω της ίδιας κονσόλας (MDM)
3.22	Να παρέχεται η δυνατότητα agentless προστασίας μηχανημάτων σε περιβάλλον VMWare χωρίς εγκατάσταση λογισμικού antivirus στο λειτουργικό σύστημα του εικονικού μηχανήματος
3.23	Η είσοδος στην κονσόλα διαχείρισης να μπορεί να κλειδωθεί με πιστοποίηση διπλού παράγοντα (2-factor authentication)
3.24	Δυνατότητα εξαγωγής των logs και events σε εξωτερικό σύστημα Syslog/SIEM με την υποστήριξη του IBM QRadar
3.25	Το μενού της κονσόλας διαχείρισης και του antivirus για τα workstations να διατίθεται και στην Ελληνική γλώσσα
Β. ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΦΑΡΜΟΓΗΣ ΑΠΟΤΡΟΠΗΣ ΑΠΩΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ – Safetica DLP	
1.1	Για την αποφυγή λανθασμένων ή προσχεδιασμένων διαρροών δεδομένων, προσφέρεται λογισμικό εφαρμογής πολιτικών ασφάλειας στα τερματικά των χρηστών (Data Leak Prevention)
1.2	Safetica DLP
1.3	Υποστήριξη για τις εξής πλατφόρμες: - Υποστήριξη Windows 7, 8.1 και 10 - Microsoft Windows Server 2008R2, 2012(R2), 2016 - Υποστήριξη MS SQL 2016 database server και νεότερο
1.4	Integration με Microsoft Active Directory
1.5	Να μην απαιτείται αγορά λογισμικού τρίτου κατασκευαστή για τη λειτουργία του, π.χ. για βάσεις δεδομένων κλπ.
2	**Εξειδικευμένες Απαιτήσεις**
2.1	Υποστήριξη Microsoft terminal server
2.2	Προσαρμόσιμη κεντρική κονσόλα διαχείρισης
2.3	Προσαρμόσιμα δικαιώματα πρόσβασης σε αναφορές, ρυθμίσεις και διαχείριση δικαιωμάτων των διαχειριστών
2.4	Δυνατότητα απόκρυψης εγκατάστασης και διεργασιών από χρήστες και διαχειριστές
2.5	Προστασία τερματισμού διεργασίας του λογισμικού προστασίας από χρήστες ή διαχειριστές
2.6	Προστασίας ανεπιθύμητης απεγκατάστασης του λογισμικού προστασίας
2.7	Δυνατότητα αποτροπής έναρξης του συστήματος σε ασφαλή λειτουργία
2.8	Η προστασία να ισχύει ακόμα κι όταν το τερματικό είναι offline, ή συνδεδεμένο σε άλλο δίκτυο
2.9	Η σουίτα να διαθέτει ενσωματωμένη δυνατότητα backup στοιχείων εφαρμογής, καταγραφών και των πολιτικών
2.10	Ειδοποίηση με email σε περίπτωση συμβάντων, με δυνατότητα ρύθμισης επιπέδου ευαισθησίας και ιδιοτήτων συμβάντων
2.11	Αποστολή αναφορών με email με τη δυνατότητα παραμετροποίησης σε πλήρες βαθμό (ποσότητα πληροφοριών, χρήστες, συχνότητα αποστολής, παραλήπτες)
2.12	Δυνατότητα αποστολής καταγραφών σε συστήματα SIEM
2.13	Να παρέχει εργαλείο πληροφόρησης (κονσόλα) για παρακολούθηση αναφορών

ΤΜΗΜΑ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

	από χρήστες χωρίς δικαιώματα διαχειριστή
3	**Απαιτήσεις Ελέγχου Ασφάλειας - Πληροφόρησης**
3.1	Λεπτομερής πληροφόρηση για τον χρόνο εκκίνησης εφαρμογών, καθώς και τον ενεργό χρόνο χρήσης τους. Οι εφαρμογές να κατηγοριοποιούνται ανάλογα τον τύπο τους για ταχύτερη αξιολόγηση
3.2	Πληροφόρηση σχετικά με τον ενεργό χρόνο χρήσης ιστοσελίδων, με λεπτομερή πληροφόρηση σχετικά με το URL, πρωτόκολλο και τίτλο ιστοσελίδας, ανεξάρτητα από τον τύπο φυλλομετρητή που χρησιμοποιείται. Οι ιστοσελίδες να παρουσιάζονται κατηγοριοποιημένες ανάλογα με τον τύπο τους
3.3	Δυνατότητα εξαγωγής αναφορών σε XLS, PDF
3.4	Δυνατότητα καταγραφής αποστολής αρχείων μέσω πάσης φύσεως λογισμικών email client και instant messaging
3.5	Λεπτομερής πληροφόρηση για την χρήση αρχείων, π.χ. ποιος χρήστης άνοιξε, αντέγραψε, διέγραψε το αρχείο και από που
3.6	Καταγραφή αρχείων που εκτυπώθηκαν
3.7	Υποστήριξη POP3, IMAP, MAPI / Exchange protocol καθώς και SSL encrypting
3.8	Η σουίτα να παρακολουθεί κάθε είδους email client, π.χ. MS Outlook, Thunderbird, κλπ
3.9	Καταγραφή κινήσεων HTTP και HTTPS με κάθε είδους φυλλομετρητή
3.10	Δραστηριότητα τερματικών: - Καταγραφή εκκίνησης/τερματισμού υπολογιστή - Καταγραφή εισόδου/εξόδου λογαριασμών υπολογιστή - Καταγραφή λειτουργίας sleep/wake up
3.11	Δραστηριότητα δικτύου: - Καταγραφή όγκου απεσταλμένων/ληφθέντων δεδομένων
3.12	Δυνατότητα παρακολούθησης αρχείων στην υπηρεσία Office 365
4	**Δυνατότητες κατηγοριοποίησης / ευρετηρίασης**
4.1	Κατηγοριοποίηση αρχείων με βάση την τοποθεσία τους, είτε είναι τοπική ή δικτυακή
4.2	Κατηγοριοποίηση αρχείων που εξάγονται από web εφαρμογές, π.χ. Intranet site
4.3	Κατηγοριοποίηση αρχείων που εξάγονται από Windows εφαρμογές, π.χ. σουΐτα ERP
4.4	Ανίχνευση αρχείων που περιέχουν ευαίσθητες πληροφορίες, όπως αριθμούς πιστωτικών καρτών, IBAN, αριθμό ΑΜΚΑ κλπ
4.5	Δυνατότητα ορισμού keywords ή regular expressions για την κατηγοριοποίηση αρχείων
5	**Δυνατότητες προστασίας**
5.1	Μετά την κατηγοριοποίηση ευαίσθητων δεδομένων να μπορεί να περιοριστεί η μετακίνηση και η επεξεργασία αυτών. Π.χ. επιτρεπόμενα μέσα για μεταφορές, επιτρεπόμενες ιστοσελίδες για μεταφόρτωση, επιτρεπόμενοι παραλήπτες email, επιτρεπόμενα λογισμικά επεξεργασίας
5.2	Δυνατότητα ορισμού πολιτικών για συγκεκριμένες εφαρμογές ή πηγές, π.χ. συγκεκριμένα δεδομένα, πρόσβαση σε εξωτερικές συσκευές, δίκτυο
5.3	Δυνατότητες εφαρμογής κανόνων σε λειτουργία δοκιμής, ενημέρωσης ή αποτροπής
5.4	Αποτροπή ενεργειών σε αρχεία, όπως αντιγραφή, μετακίνηση, μεταφόρτωση στο Web, σε FTP, σε εξωτερική συσκευή, με αναφορά πηγής και προορισμού, τη

ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΥΔΡΕΥΣΗΣ ΑΠΟΧΕΤΕΥΣΗΣ ΠΑΤΡΑΣ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

ΤΜΗΜΑ
ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

	διαδρομή, τύπο συσκευών
5.5	Αποτροπή αντιγραφής μέσω clipboard και screen capture
5.6	Κρυπτογράφηση: - Δυνατότητα Full Disk Encryption μέσω BitLocker service, όπου αυτό είναι διαθέσιμο - Κρυπτογράφηση δίσκων USB Flash μέσω BitLocker
5.7	Device Control: - Ολικός περιορισμός σε συσκευές USB, firewire, κάρτες μνήμης, LPT, COM, Bluetooth, CD, DVD, Blue-ray - Δυνατότητα read-only λειτουργίας συσκευών - Καταγραφή συνδέσεων εξωτερικών συσκευών
5.8	Δυνατότητα application control για την αποτροπή εκτέλεσης ορισμένων κατηγοριών λογισμικών
5.9	Δυνατότητα web control για την αποτροπή επίσκεψης σε ορισμένες κατηγορίες ιστοσελίδων
5.10	Δυνατότητα print control για προσαρμογή ορίων εκτύπωσης σε χρήστες
C. ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΡΥΘΜΙΣΗ ΕΦΑΡΜΟΓΩΝ	
1.	**Εγκατάσταση και ρύθμιση εφαρμογής κακόβουλου λογισμικού** Προβλέπεται η εγκατάσταση και ρύθμιση της εφαρμογής ESET Remote Administrator Console και η εγκατάσταση και ρύθμιση 10 αντιπροσωπευτικών τερματικών για σκοπούς εκπαίδευσης του προσωπικού που θα χειρίζεται την εφαρμογή του server. Οι παραπάνω εργασίες θα ολοκληρωθούν εντός δύο εργάσιμων ημερών με επιτόπια επίσκεψη τεχνικού.
2.	**Εγκατάσταση και ρύθμιση εφαρμογής και αποτροπής απώλειας δεδομένων** Προβλέπεται η εγκατάσταση και ρύθμιση της εφαρμογής Safetica Remote Administrator Console και η εγκατάσταση και ρύθμιση 10 αντιπροσωπευτικών τερματικών για σκοπούς εκπαίδευσης του προσωπικού που θα χειρίζεται την εφαρμογή του server. Οι παραπάνω εργασίες θα ολοκληρωθούν εντός δύο εργάσιμων ημερών με επιτόπια επίσκεψη τεχνικού.
D. ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΦΑΡΜΟΓΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ESET Endpoint Encryption Pro Edition	
1.	Εφαρμογή κρυπτογράφησης που παρέχει πλήρη απομακρυσμένο έλεγχο των κλειδιών κρυπτογράφησης των endpoints και της πολιτικής ασφαλείας για αρχεία σε σκληρούς δίσκους, φορητές συσκευές και μηνύματα ηλεκτρονικού ταχυδρομείου που εξασφαλίζει: • Μηδενικές παραβιάσεις δεδομένων • Συμμόρφωση με τις απαιτήσεις • Αδιάλειπτη κρυπτογράφηση
2.	Το ESET Endpoint Encryption μπορεί να διαχειρίζεται συσκευές οπουδήποτε στον κόσμο χωρίς να απαιτεί VPN ή εξαιρέσεις στο firewall. Η διαχείριση πραγματοποιείται χρησιμοποιώντας σύνδεση HTTPS, καθιστώντας εξαιρετικά εύκολη την εγκατάσταση και τη ρύθμιση σε επιχειρήσεων οποιουδήποτε μεγέθους. Επιπλέον Η εφαρμογή της κρυπτογράφησης είναι απολύτως διαφανής για τους χρήστες και δεν απαιτεί καμία ενέργεια εκ μέρους τους. Επιπλέον, δεν υπάρχει επιπλέον κόστος για τα τμήματα IT, καθώς και καμία ανάγκη εκπαίδευσης των χρηστών.

ΔΗΜΟΤΙΚΗ
ΕΠΙΧΕΙΡΗΣΗ
ΥΔΡΕΥΣΗΣ
ΑΠΟΧΕΤΕΥΣΗΣ
ΠΑΤΡΑΣ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

ΔΕΥΑΠ
ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΥΔΡΕΥΣΗΣ ΑΠΟΧΕΤΕΥΣΗΣ ΠΑΤΡΑΣ

ΤΜΗΜΑ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.g
george.papadimitropoulos@deyap.

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

3.	Το ESET Endpoint Encryption είναι πιστοποιημένο κατά FIPS 140-2 με κρυπτογράφηση 256 bit AES. Η κρυπτογράφηση υποστηρίζεται σε Windows 10, 8, 8.1, 7, Vista, XP, και Server 2003 – Server 2016 και iOS.
Ε. ΠΡΟΔΙΑΓΡΑΦΕΣ ΥΠΗΡΕΣΙΑΣ ΕΛΑΧΙΣΤΟΠΟΙΗΣΗΣ ΝΕΩΝ ΑΠΕΙΛΩΝ ESET Dynamic Threat Defense	
1.	Υπηρεσία επί πληρωμή που παρέχεται από την ESET. Σκοπός της είναι να προσθέσει ένα επίπεδο προστασίας που έχει σχεδιαστεί ειδικά για την ελαχιστοποίηση των νέων απειλών που κυκλοφορούν. Τα ύποπτα αρχεία υποβάλλονται αυτόματα στο cloud της ESET. Στο cloud αναλύονται από τους προηγμένους μηχανισμούς ανίχνευσης κακόβουλου λογισμικού. Ο χρήστης που παρείχε το δείγμα θα λάβει μια αναφορά συμπεριφοράς, η οποία προσφέρει μια περίληψη της συμπεριφοράς που παρατηρήθηκε στο δείγμα.
2.	Τα αρχεία μπορούν να υποβληθούν μη αυτόματα ή αυτόματα με βάση τη διαμόρφωση πολιτικής. Η μη αυτόματη υποβολή αρχείου εκτελείται από την κονσόλα διαδικτύου ESMC ή από τους υπολογιστές πελάτες με ενεργό προϊόν ασφάλειας ESET και την υπηρεσία ESET Dynamic Threat Defense.
F. ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΦΑΡΜΟΓΗΣ ΠΡΟΣΤΑΣΙΑΣ ΓΙΑ ENDPOINTS ΚΑΙ FILE SERVERS ESET Secure Business	
1.	Πλήρης συνδυαστική λύση προστασίας για endpoints και file servers. Οι απειλές που μεταδίδονται μέσω ηλεκτρονικού ταχυδρομείου μπλοκάρονται στο επίπεδο του server. Προσφέρει τα παρακάτω: • Προστασία ενάντια σε στοχευμένες απειλές • Προστασία από το ransomware • Πρόληψη επιθέσεων που δεν χρησιμοποιούν αρχεία • Προστασία email gateway • Απομακρυσμένη διαχείριση
2.	Οι λύσεις προστασίας endpoint της ESET αξιοποιούν πολυεπίπεδες τεχνολογίες σε μια δυναμική ισορροπία. Οι on-premise και off-premise λύσεις μας εξισορροπούν συνεχώς την απόδοση, την ανίχνευση με ελάχιστα σφάλματα.
3.	Παρέχει προηγμένη προστασία σε όλους τους δικτυακούς αποθηκευτικούς χώρους, γενικούς διακομιστές και διακομιστές πολλαπλών χρήσεων. Εξασφαλίζει τη σταθερή λειτουργία των servers χωρίς συγκρούσεις. Ελαχιστοποιεί τις επανεκκινήσεις και την εμφάνιση παραθύρων συντήρησης εξασφαλίζοντας την απρόσκοπτη λειτουργία της επιχείρησης.
4.	Το ESET Mail Security φιλτράρει όλα τα ανεπιθύμητα και τα κακόβουλα προγράμματα προτού φτάσουν στα γραμματοκιβώτια των χρηστών. Βασισμένο στην αποδεδειγμένη τεχνολογία NOD32, το ESET Mail Security είναι μια πρώτη γραμμή άμυνας που συμπληρώνει την ασφάλεια του δικτύου σας.
ΕΙΔΙΚΟΙ ΟΡΟΙ	
1. Η προμηθεύτρια θα πρέπει να προσκομίσει βεβαίωση – υπεύθυνη δήλωση του άρθρου 8 του ν.1599/1986 ότι διαθέτει εκπαιδευμένους τεχνικούς.	
2. Η προμηθεύτρια θα πρέπει να υποβάλει εταιρική παρουσίαση όπου θα περιγράφεται ο τρόπος οργάνωσης και λειτουργίας της.	
3. Η προμηθεύτρια θα πρέπει να διαθέτει τις παρακάτω πιστοποιήσεις ISO:	

ΤΜΗΜΑ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

a. ISO 9001:2015
b. ISO 14001:2015
c. ISO 27001:2013
d. ISO 22301:2012

4. Η προμηθεύτρια θα πρέπει να παρέχει υπηρεσίες Συμμόρφωσης με τον κανονισμό προστασίας προσωπικών δεδομένων (GDPR) και να προσκομίσει τουλάχιστον πέντε (5) βεβαιώσεις ή συμβάσεις αντίστοιχων έργων σε Οργανισμούς και τουλάχιστον δύο (2) να αφορούν ΔΕΥΑ.
5. Η προμηθεύτρια θα πρέπει παρέχει υπηρεσίες εγκατάστασης ISO 27001 για τουλάχιστον δέκα (10) έτη και να προσκομίσει τουλάχιστον τρεις (3) βεβαιώσεις αντίστοιχων έργων.
6. Προσκόμιση Υπεύθυνης δήλωσης του συμμετέχοντα φορέα ότι δεν εμπίπτει στις περιπτώσεις του άρθρου 73 παρ.1 και 2 του Ν.4412/2016 και **ότι σε περίπτωση που αναδειχθεί ανάδοχος και πριν την υπογραφή της σύμβασης θα προσκομίσει:**
α) απόσπασμα ποινικού μητρώου,
β) πιστοποιητικό φορολογικής ενημερότητας και
γ) πιστοποιητικό ασφαλιστικής ενημερότητας
7. ΠΡΟΣΟΧΗ: Ο προσφέρον είναι υποχρεωτικό να δώσει συνολική προσφορά

ΠΡΟΣΟΧΗ:

- Η προσφορά αφορά το **σύνολο** των ζητούμενων ειδών.
- Μαζί με την τεχνική προσφορά να κατατεθεί φύλλο συμμόρφωσης προς όλες τις παραγράφους των τεχνικών προδιαγραφών με ίδια σειρά και αρίθμηση και με αντίστοιχες παραπομπές στα prospectus των **οποίων η κατάθεση είναι υποχρεωτική.** Αν το είδος εκτρέπεται τότε πρέπει να περιγράφονται αναλυτικά η εκτροπή ή η ασυμφωνία για να σχηματίζεται με σαφήνεια η γνώμη για την περαιτέρω εκτίμηση. Η μη κατάθεση του φύλλου συμμόρφωσης συνεπάγεται τον αποκλεισμό του διαγωνιζόμενου. Όλες οι τεχνικές προδιαγραφές είναι απαιτητές και επί ποινής αποκλεισμού.

Πάτρα **8/11/2019**

Ο Προϊστάμενος
Τμήματος Μηχανοργάνωσης

Γεώργιος Παπαδημητρόπουλος

ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΥΔΡΕΥΣΗΣ ΑΠΟΧΕΤΕΥΣΗΣ ΠΑΤΡΑΣ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

ΔΕΥΑΠ

ΤΜΗΜΑ
ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ

Κ.Α.Ε. 2019: ***16.17.005.531***

	ΠΕΡΙΓΡΑΦΗ	ΤΕΜΑΧΙΑ	ΤΙΜΗ ΑΝΑ ΤΕΜΑΧΙΟ	ΣΥΝΟΛΙΚΗ ΤΙΜΗ	Φ.Π.Α.	ΤΕΛΙΚΗ ΤΙΜΗ ΜΕ Φ.Π.Α.
A	ΕΦΑΡΜΟΓΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ – ESET Antivirus	160	19,00 €	3.040,00 €	729,60 €	3.769,60 €
B	ΕΦΑΡΜΟΓΗ ΑΠΟΤΡΟΠΗΣ ΑΠΩΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ – Safetica DLP	160	43,00 €	6.880,00 €	1.651,20 €	8.531,20 €
C	ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΡΥΘΜΙΣΗ ΕΦΑΡΜΟΓΩΝ ESET Endpoint	1	1.280,00 €	1.280,00 €	307,20 €	1.587,20 €
C	ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΡΥΘΜΙΣΗ ΕΦΑΡΜΟΓΩΝ ESET SAFETICA DLP	1	1.920,00 €	1.920,00 €	460,80 €	2.380,80 €
D	ΕΦΑΡΜΟΓΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ESET Endpoint Encryption Pro Edition	5	36,25 €	181,25 €	43,50 €	224,75 €
E	ΥΠΗΡΕΣΙΑ ΕΛΑΧΙΣΤΟΠΟΗΣΗΣ ΝΕΩΝ ΑΠΕΙΛΩΝ ESET Dynamic Threat Defense	250	5,76 €	1.440,00 €	345,60 €	1.785,60 €
F	ΕΦΑΡΜΟΓΗ ΠΡΟΣΤΑΣΙΑΣ ΓΙΑ ENDPOINTS ΚΑΙ FILE SERVERS ESET Secure Business	250	19,20 €	4.800,00 €	1.152,00 €	5.952,00 €
				19.541,25 €	**4.689,90 €**	**24.231,15 €**

ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΥΔΡΕΥΣΗΣ ΑΠΟΧΕΤΕΥΣΗΣ Π Α Τ Ρ Α Σ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

Πάτρα **8/11/2019**

Ο Προϊστάμενος
Τμήματος Μηχανοργάνωσης

Γεώργιος Παπαδημητρόπουλος

ΔΕΥΑΠ

ΤΜΗΜΑ
ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.g
george.papadimitropoulos@deyap.

ΕΝΤΥΠΟ ΠΡΟΣΦΟΡΑΣ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ

Α. ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΦΑΡΜΟΓΗΣ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ – ESET Antivirus		**ΑΠΑΝΤΗΣΗ ΝΑΙ/ΟΧΙ**
1.1	Για την προστασία από κακόβουλο λογισμικό στα τερματικά και τους εξυπηρετητές του έργου θα προσφερθούν άδειες ESET Endpoint antivirus	
1.2	ESET Endpoint antivirus	
1.3	Υποστήριξη για τις εξής πλατφόρμες λειτουργικών συστημάτων: - Microsoft Windows XP, Vista, 7, 8, 10 - Microsoft Windows Server 2003(R2), 2008(R2), 2012(R2),2016 - Linux με kernel 2.6.x και νεότερα - Mac OS X - Android 4 ή νεότερο	
2	**Εξειδίκευση των απαιτήσεων προστασίας**	
2.1	Δυνατότητα ανίχνευσης και καθαρισμού όλων των τύπων απειλών: viruses, trojans, dialers, spyware, jokes, hoaxes	
2.2	Δυνατότητα αυτόματης ανίχνευσης & καθαρισμού των προαναφερθέντων απειλών σε πραγματικό χρόνο	
2.3	Δυνατότητα επιλογής ανίχνευσης malware σε δικτυακές τοποθεσίες, on-demand και σε πραγματικό χρόνο	
2.4	Να παρέχεται cloud reputation database για αμεσότερη προστασία από νέες απειλές	
2.5	Υποστήριξη τεχνολογίων Advanced heuristics/DNA/Smart Signatures για δυνατότητα ανίχνευσης άγνωστων ιών	
2.6	Δυνατότητα για host intrusion prevention system	
2.7	Η ανανέωση των signature files να είναι incremental	
2.8	Δυνατότητα Rollback των Signature Files σε προηγούμενη έκδοση του με ταυτόχρονη παύση των ενημερώσεων, επιλέγοντας το κεντρικά ή απευθείας από το client	
2.9	Δυνατότητα κατεβάσματος ενημερώσεων με νεότερες engines που βρίσκονται σε δοκιμαστικό στάδιο, επιλέγοντας το κεντρικά ή απευθείας από το client	
2.10	Δυνατότητα να μπορεί να γίνει ένα client update server για τα υπόλοιπα clients του δικτύου χωρίς την εγκατάσταση τμήματος της κονσόλας διαχείρισης ή άλλου εξωτερικού software	
2.11	Δυνατότητα για SSL/TLS filtering στα πρωτόκολλα HTTPS, IMAPS, POP3S	
2.12	Δυνατότητα μπλοκαρίσματος όλων των σελίδων του Internet σε ένα client	
2.13	Δυνατότητα εξαγωγής των ρυθμίσεων ενός client σε αρχείο και εισαγωγής των ρυθμίσεων σε άλλο client από το ίδιο αρχείο.	
2.14	Να υπάρχει ενσωματωμένη εφαρμογή που να καταγράφει την κατάσταση του συστήματος (εφαρμογές, processes, services κ.α) – κατόπιν εντολής τοπικά ή από την κονσόλα - σε μία χρονική στιγμή (snapshot) και να αποθηκεύει τα αποτελέσματα για σύγκριση τους με	

ΔΕΥΑΠ
ΤΜΗΜΑ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΥΔΡΕΥΣΗΣ ΑΠΟΧΕΤΕΥΣΗΣ ΠΑΤΡΑΣ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

	την κατάσταση του συστήματος από διαφορετική χρονική στιγμή.	
2.15	Παροχή Bootable Media που να περιέχει το antivirus ώστε να δίνει τη δυνατότητα για καθαρισμό του συστήματος χωρίς να χρειάζεται να ξεκινήσει το λειτουργικό σύστημα	
3	**Απαιτήσεις απομακρυσμένης και κεντρικής διαχείρισης**	
3.1	Κεντρική διαχείριση όλων των clients των τερματικών και servers	
3.2	Υποστήριξη πολλαπλών ομάδων και υπο-ομάδων με δυνατότητα εφαρμογής διαφορετικών πολιτικών για κάθε περίπτωση	
3.3	Λειτουργία προσωρινής απενεργοποίησης πολιτικής ανά client	
3.4	Δυνατότητα για ομάδες διαχείρισης με βάση ιδιότητες υπολογιστών, π.χ. αυτόματη ομαδοποίηση υπολογιστών με Windows 10	
3.5	Εγκατάσταση & απεγκατάσταση της προστασίας μέσω κεντρικής κονσόλας (Remote deployment)	
3.6	Να υπάρχει η δυνατότητα εξαγωγής ενιαίου πακέτου με το πρόγραμμα προστασίας, σύνδεση διαχείρισης, πολιτικές και την άδεια ενεργοποίησης	
3.7	Να παρέχεται ξεχωριστό εργαλείο ανίχνευσης τερματικών και push εγκατάστασης του παραπάνω ενιαίου πακέτου	
3.8	Επικοινωνία του client μόνο με IP, δηλαδή να δουλέψει σε περιπτώσεις όπου δεν υπάρχουν υπηρεσίες ονοματοδοσίας (DNS servers)	
3.9	Να μπορεί να γίνει αυτόματη ανίχνευση των τερματικών που βρίσκονται στο τοπικό δίκτυο, ακόμα κι αν αυτά δεν ανήκουν σε Active Directory	
3.10	Να μπορεί να γίνει εισαγωγή λίστας των τερματικών του δικτύου με τη χρήση CSV αρχείου	
3.11	Η επικοινωνία των servers και των clients να διασφαλίζεται μέσω certificate	
3.12	Να μπορεί να γίνει ενεργοποίηση σε δίκτυο χωρίς σύνδεση στο internet (offline activation)	
3.13	Να γίνεται ενημέρωση από το Internet από κεντρικό σημείο, από το οποίο στην συνέχεια θα ενημερωθούν όλοι οι clients του δικτύου	
3.14	Τα antivirus να μπορούν να λάβουν signature files μέσω HTTP proxy cache, με αυτόματη παράκαμψή του σε περίπτωση που δεν είναι διαθέσιμος ο proxy server	
3.15	Να περιλαμβάνεται έλεγχος και ειδοποίηση για το αν υπάρχουν ενημερώσεις για το λειτουργικό σύστημα, καθώς και η δυνατότητα να δοθεί εντολή ενημέρωσης λειτουργικού συστήματος	
3.16	Παρακολούθηση όλων των clients και παραγωγή reports και στατιστικών σε πολλές μορφές (Προγραμματισμένα emails, PDF, PS, CSV, Charts)	
3.17	Δυνατότητα ενιαίας καραντίνας αρχείων που ανιχνεύθηκαν για όλο το δίκτυο, με δυνατότητες προβολής clients ανά απειλή, εξαγωγή και εξαίρεση	
3.18	Ο server διαχείρισης να μπορεί να γίνει εγκατάσταση με τις παρακάτω μεθόδους. α) Αυτοματοποιημένα με τη μορφή Wizard β) Χειροκίνητα, εκτελώντας ανεξάρτητα τα τμήματα της	

ΤΜΗΜΑ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

	εγκατάστασης γ) Ως προεγκατεστημένο Virtual Appliance με Linux OS	
3.19	Η εγκατάσταση της βάσης δεδομένων της κονσόλας θα πρέπει απαραίτητα να γίνεται σε ένα υπολογιστή οπουδήποτε στο εσωτερικό δίκτυο της εταιρίας και όχι σε εξωτερικό δίκτυο π.χ. Cloud.	
3.20	Να παρέχεται εργαλείο ελέγχου κατάστασης αδειών και αριθμού ενεργοποιήσεων, ακόμα κι αν αυτές έχουν γίνει εκτός της κεντρικής κονσόλας (stand alone εγκαταστάσεις)	
3.21	Να παρέχεται η δυνατότητα διαχείρισης Android και iOS συσκευών μέσω της ίδιας κονσόλας (MDM)	
3.22	Να παρέχεται η δυνατότητα agentless προστασίας μηχανημάτων σε περιβάλλον VMWare χωρίς εγκατάσταση λογισμικού antivirus στο λειτουργικό σύστημα του εικονικού μηχανήματος	
3.23	Η είσοδος στην κονσόλα διαχείρισης να μπορεί να κλειδωθεί με πιστοποίηση διπλού παράγοντα (2-factor authentication)	
3.24	Δυνατότητα εξαγωγής των logs και events σε εξωτερικό σύστημα Syslog/SIEM με την υποστήριξη του IBM QRadar	
3.25	Το μενού της κονσόλας διαχείρισης και του antivirus για τα workstations να διατίθεται και στην Ελληνική γλώσσα	
Β. ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΦΑΡΜΟΓΗΣ ΑΠΟΤΡΟΠΗΣ ΑΠΩΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ – Safetica DLP		**ΑΠΑΝΤΗΣΗ ΝΑΙ/ΟΧΙ**
1.1	Για την αποφυγή λανθασμένων ή προσχεδιασμένων διαρροών δεδομένων, προσφέρεται λογισμικό εφαρμογής πολιτικών ασφάλειας στα τερματικά των χρηστών (Data Leak Prevention)	
1.2	Safetica DLP	
1.3	Υποστήριξη για τις εξής πλατφόρμες: - Υποστήριξη Windows 7, 8.1 και 10 - Microsoft Windows Server 2008R2, 2012(R2), 2016 - Υποστήριξη MS SQL 2016 database server και νεότερο	
1.4	Integration με Microsoft Active Directory	
1.5	Να μην απαιτείται αγορά λογισμικού τρίτου κατασκευαστή για τη λειτουργία του, π.χ. για βάσεις δεδομένων κλπ.	
2	**Εξειδικευμένες Απαιτήσεις**	
2.1	Υποστήριξη Microsoft terminal server	
2.2	Προσαρμόσιμη κεντρική κονσόλα διαχείρισης	
2.3	Προσαρμόσιμα δικαιώματα πρόσβασης σε αναφορές, ρυθμίσεις και διαχείριση δικαιωμάτων των διαχειριστών	
2.4	Δυνατότητα απόκρυψης εγκατάστασης και διεργασιών από χρήστες και διαχειριστές	
2.5	Προστασία τερματισμού διεργασίας του λογισμικού προστασίας από χρήστες ή διαχειριστές	
2.6	Προστασίας ανεπιθύμητης απεγκατάστασης του λογισμικού προστασίας	
2.7	Δυνατότητα αποτροπής έναρξης του συστήματος σε ασφαλή λειτουργία	
2.8	Η προστασία να ισχύει ακόμα κι όταν το τερματικό είναι offline, ή συνδεδεμένο σε άλλο δίκτυο	

ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΥΔΡΕΥΣΗΣ ΑΠΟΧΕΤΕΥΣΗΣ ΠΑΤΡΑΣ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

ΔΕΥΑΠ

ΤΜΗΜΑ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΥΔΡΕΥΣΗΣ ΑΠΟΧΕΤΕΥΣΗΣ ΠΑΤΡΑΣ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

2.9	Η σουίτα να διαθέτει ενσωματωμένη δυνατότητα backup στοιχείων εφαρμογής, καταγραφών και των πολιτικών	
2.10	Ειδοποίηση με email σε περίπτωση συμβάντων, με δυνατότητα ρύθμισης επιπέδου ευαισθησίας και ιδιοτήτων συμβάντων	
2.11	Αποστολή αναφορών με email με τη δυνατότητα παραμετροποίησης σε πλήρες βαθμό (ποσότητα πληροφοριών, χρήστες, συχνότητα αποστολής, παραλήπτες)	
2.12	Δυνατότητα αποστολής καταγραφών σε συστήματα SIEM	
2.13	Να παρέχει εργαλείο πληροφόρησης (κονσόλα) για παρακολούθηση αναφορών από χρήστες χωρίς δικαιώματα διαχειριστή	
3	**Απαιτήσεις Ελέγχου Ασφάλειας - Πληροφόρησης**	
3.1	Λεπτομερής πληροφόρηση για τον χρόνο εκκίνησης εφαρμογών, καθώς και τον ενεργό χρόνο χρήσης τους. Οι εφαρμογές να κατηγοριοποιούνται ανάλογα τον τύπο τους για ταχύτερη αξιολόγηση	
3.2	Πληροφόρηση σχετικά με τον ενεργό χρόνο χρήσης ιστοσελίδων, με λεπτομερή πληροφόρηση σχετικά με το URL, πρωτόκολλο και τίτλο ιστοσελίδας, ανεξάρτητα από τον τύπο φυλλομετρητή που χρησιμοποιείται. Οι ιστοσελίδες να παρουσιάζονται κατηγοριοποιημένες ανάλογα με τον τύπο τους	
3.3	Δυνατότητα εξαγωγής αναφορών σε XLS, PDF	
3.4	Δυνατότητα καταγραφής αποστολής αρχείων μέσω πάσης φύσεως λογισμικών email client και instant messaging	
3.5	Λεπτομερής πληροφόρηση για την χρήση αρχείων, π.χ. ποιος χρήστης άνοιξε, αντέγραψε, διέγραψε το αρχείο και από που	
3.6	Καταγραφή αρχείων που εκτυπώθηκαν	
3.7	Υποστήριξη POP3, IMAP, MAPI / Exchange protocol καθώς και SSL encrypting	
3.8	Η σουίτα να παρακολουθεί κάθε είδους email client, π.χ. MS Outlook, Thunderbird, κλπ	
3.9	Καταγραφή κινήσεων HTTP και HTTPS με κάθε είδους φυλλομετρητή	
3.10	Δραστηριότητα τερματικών: - Καταγραφή εκκίνησης/τερματισμού υπολογιστή - Καταγραφή εισόδου/εξόδου λογαριασμών υπολογιστή - Καταγραφή λειτουργίας sleep/wake up	
3.11	Δραστηριότητα δικτύου: - Καταγραφή όγκου απεσταλμένων/ληφθέντων δεδομένων	
3.12	Δυνατότητα παρακολούθησης αρχείων στην υπηρεσία Office 365	
4	**Δυνατότητες κατηγοριοποίησης / ευρετηρίασης**	
4.1	Κατηγοριοποίηση αρχείων με βάση την τοποθεσία τους, είτε είναι τοπική ή δικτυακή	
4.2	Κατηγοριοποίηση αρχείων που εξάγονται από web εφαρμογές, π.χ. Intranet site	
4.3	Κατηγοριοποίηση αρχείων που εξάγονται από Windows εφαρμογές, π.χ. σουίτα ERP	
4.4	Ανίχνευση αρχείων που περιέχουν ευαίσθητες πληροφορίες, όπως αριθμούς πιστωτικών καρτών, IBAN, αριθμό ΑΜΚΑ κλπ	

ΔΕΥΑΠ
ΤΜΗΜΑ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

ΔΗΜΟΤΙΚΗ
ΕΠΙΧΕΙΡΗΣΗ
ΥΔΡΕΥΣΗΣ
ΑΠΟΧΕΤΕΥΣΗΣ
Π Α Τ Ρ Α Σ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

4.5	Δυνατότητα ορισμού keywords ή regular expressions για την κατηγοριοποίηση αρχείων	
5	**Δυνατότητες προστασίας**	
5.1	Μετά την κατηγοριοποίηση ευαίσθητων δεδομένων να μπορεί να περιοριστεί η μετακίνηση και η επεξεργασία αυτών. Π.χ. επιτρεπόμενα μέσα για μεταφορές, επιτρεπόμενες ιστοσελίδες για μεταφόρτωση, επιτρεπόμενοι παραλήπτες email, επιτρεπόμενα λογισμικά επεξεργασίας	
5.2	Δυνατότητα ορισμού πολιτικών για συγκεκριμένες εφαρμογές ή πηγές, π.χ. συγκεκριμένα δεδομένα, πρόσβαση σε εξωτερικές συσκευές, δίκτυο	
5.3	Δυνατότητες εφαρμογής κανόνων σε λειτουργία δοκιμής, ενημέρωσης ή αποτροπής	
5.4	Αποτροπή ενεργειών σε αρχεία, όπως αντιγραφή, μετακίνηση, μεταφόρτωση στο Web, σε FTP, σε εξωτερική συσκευή, με αναφορά πηγής και προορισμού, τη διαδρομή, τύπο συσκευών	
5.5	Αποτροπή αντιγραφής μέσω clipboard και screen capture	
5.6	Κρυπτογράφηση: - Δυνατότητα Full Disk Encryption μέσω BitLocker service, όπου αυτό είναι διαθέσιμο - Κρυπτογράφηση δίσκων USB Flash μέσω BitLocker	
5.7	Device Control: - Ολικός περιορισμός σε συσκευές USB, firewire, κάρτες μνήμης, LPT, COM, Bluetooth, CD, DVD, Blue-ray - Δυνατότητα read-only λειτουργίας συσκευών - Καταγραφή συνδέσεων εξωτερικών συσκευών	
5.8	Δυνατότητα application control για την αποτροπή εκτέλεσης ορισμένων κατηγοριών λογισμικών	
5.9	Δυνατότητα web control για την αποτροπή επίσκεψης σε ορισμένες κατηγορίες ιστοσελίδων	
5.10	Δυνατότητα print control για προσαρμογή ορίων εκτύπωσης σε χρήστες	
C. ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΡΥΘΜΙΣΗ ΕΦΑΡΜΟΓΩΝ		**ΑΠΑΝΤΗΣΗ ΝΑΙ/ΟΧΙ**
1.	**<u>Εγκατάσταση και ρύθμιση εφαρμογής κακόβουλου λογισμικού</u>** Προβλέπεται η εγκατάσταση και ρύθμιση της εφαρμογής ESET Remote Administrator Console και η εγκατάσταση και ρύθμιση 10 αντιπροσωπευτικών τερματικών για σκοπούς εκπαίδευσης του προσωπικού που θα χειρίζεται την εφαρμογή του server. Οι παραπάνω εργασίες θα ολοκληρωθούν εντός δύο εργάσιμων ημερών με επιτόπια επίσκεψη τεχνικού.	
2.	**<u>Εγκατάσταση και ρύθμιση εφαρμογής και αποτροπής απώλειας δεδομένων</u>** Προβλέπεται η εγκατάσταση και ρύθμιση της εφαρμογής Safetica Remote Administrator Console και η εγκατάσταση και ρύθμιση 10 αντιπροσωπευτικών τερματικών για σκοπούς εκπαίδευσης του προσωπικού που θα χειρίζεται την εφαρμογή του server. Οι παραπάνω εργασίες θα ολοκληρωθούν εντός δύο εργάσιμων ημερών με επιτόπια επίσκεψη τεχνικού.	

ΤΜΗΜΑ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

D. ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΦΑΡΜΟΓΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ESET Endpoint Encryption Pro Edition		**ΑΠΑΝΤΗΣΗ ΝΑΙ/ΟΧΙ**
1.	Εφαρμογή κρυπτογράφησης που παρέχει πλήρη απομακρυσμένο έλεγχο των κλειδιών κρυπτογράφησης των endpoints και της πολιτικής ασφαλείας για αρχεία σε σκληρούς δίσκους, φορητές συσκευές και μηνύματα ηλεκτρονικού ταχυδρομείου που εξασφαλίζει: • Μηδενικές παραβιάσεις δεδομένων • Συμμόρφωση με τις απαιτήσεις • Αδιάλειπτη κρυπτογράφηση	
2.	Το ESET Endpoint Encryption μπορεί να διαχειρίζεται συσκευές οπουδήποτε στον κόσμο χωρίς να απαιτεί VPN ή εξαιρέσεις στο firewall. Η διαχείριση πραγματοποιείται χρησιμοποιώντας σύνδεση HTTPS, καθιστώντας εξαιρετικά εύκολη την εγκατάσταση και τη ρύθμιση σε επιχειρήσεων οποιουδήποτε μεγέθους. Επιπλέον Η εφαρμογή της κρυπτογράφησης είναι απολύτως διαφανής για τους χρήστες και δεν απαιτεί καμία ενέργεια εκ μέρους τους. Επιπλέον, δεν υπάρχει επιπλέον κόστος για τα τμήματα IT, καθώς και καμία ανάγκη εκπαίδευσης των χρηστών.	
3.	Το ESET Endpoint Encryption είναι πιστοποιημένο κατά FIPS 140-2 με κρυπτογράφηση 256 bit AES. Η κρυπτογράφηση υποστηρίζεται σε Windows 10, 8, 8.1, 7, Vista, XP, και Server 2003 – Server 2016 και iOS.	
E. ΠΡΟΔΙΑΓΡΑΦΕΣ ΥΠΗΡΕΣΙΑΣ ΕΛΑΧΙΣΤΟΠΟΙΗΣΗΣ ΝΕΩΝ ΑΠΕΙΛΩΝ ESET Dynamic Threat Defense		**ΑΠΑΝΤΗΣΗ ΝΑΙ/ΟΧΙ**
1.	Υπηρεσία επί πληρωμή που παρέχεται από την ESET. Σκοπός της είναι να προσθέσει ένα επίπεδο προστασίας που έχει σχεδιαστεί ειδικά για την ελαχιστοποίηση των νέων απειλών που κυκλοφορούν. Τα ύποπτα αρχεία υποβάλλονται αυτόματα στο cloud της ESET. Στο cloud αναλύονται από τους προηγμένους μηχανισμούς ανίχνευσης κακόβουλου λογισμικού. Ο χρήστης που παρείχε το δείγμα θα λάβει μια αναφορά συμπεριφοράς, η οποία προσφέρει μια περίληψη της συμπεριφοράς που παρατηρήθηκε στο δείγμα.	
2.	Τα αρχεία μπορούν να υποβληθούν μη αυτόματα ή αυτόματα με βάση τη διαμόρφωση πολιτικής. Η μη αυτόματη υποβολή αρχείου εκτελείται από την κονσόλα διαδικτύου ESMC ή από τους υπολογιστές πελάτες με ενεργό προϊόν ασφάλειας ESET και την υπηρεσία ESET Dynamic Threat Defense.	
F. ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΦΑΡΜΟΓΗΣ ΠΡΟΣΤΑΣΙΑΣ ΓΙΑ ENDPOINTS ΚΑΙ FILE SERVERS ESET Secure Business		**ΑΠΑΝΤΗΣΗ ΝΑΙ/ΟΧΙ**
1.	Πλήρης συνδυαστική λύση προστασίας για endpoints και file servers. Οι απειλές που μεταδίδονται μέσω ηλεκτρονικού	

ΤΜΗΜΑ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

	ταχυδρομείου μπλοκάρονται στο επίπεδο του server. Προσφέρει τα παρακάτω: • Προστασία ενάντια σε στοχευμένες απειλές • Προστασία από το ransomware • Πρόληψη επιθέσεων που δεν χρησιμοποιούν αρχεία • Προστασία email gateway • Απομακρυσμένη διαχείριση	
2.	Οι λύσεις προστασίας endpoint της ESET αξιοποιούν πολυεπίπεδες τεχνολογίες σε μια δυναμική ισορροπία. Οι on-premise και off-premise λύσεις μας εξισορροπούν συνεχώς την απόδοση, την ανίχνευση με ελάχιστα σφάλματα.	
3.	Παρέχει προηγμένη προστασία σε όλους τους δικτυακούς αποθηκευτικούς χώρους, γενικούς διακομιστές και διακομιστές πολλαπλών χρήσεων. Εξασφαλίζει τη σταθερή λειτουργία των servers χωρίς συγκρούσεις. Ελαχιστοποιεί τις επανεκκινήσεις και την εμφάνιση παραθύρων συντήρησης εξασφαλίζοντας την απρόσκοπτη λειτουργία της επιχείρησης.	
4.	Το ESET Mail Security φιλτράρει όλα τα ανεπιθύμητα και τα κακόβουλα προγράμματα προτού φτάσουν στα γραμματοκιβώτια των χρηστών. Βασισμένο στην αποδεδειγμένη τεχνολογία NOD32, το ESET Mail Security είναι μια πρώτη γραμμή άμυνας που συμπληρώνει την ασφάλεια του δικτύου σας.	
	ΕΙΔΙΚΟΙ ΟΡΟΙ	**ΑΠΑΝΤΗΣΗ ΝΑΙ/ΟΧΙ**
1.	Η προμηθεύτρια θα πρέπει να προσκομίσει βεβαίωση – υπεύθυνη δήλωση του άρθρου 8 του ν.1599/1986 ότι διαθέτει εκπαιδευμένους τεχνικούς.	
2.	Η προμηθεύτρια θα πρέπει να υποβάλει εταιρική παρουσίαση όπου θα περιγράφεται ο τρόπος οργάνωσης και λειτουργίας της.	
3.	Η προμηθεύτρια θα πρέπει να διαθέτει τις παρακάτω πιστοποιήσεις ISO: a. ISO 9001:2015 b. ISO 14001:2015 c. ISO 27001:2013 d. ISO 22301:2012	
4.	Η προμηθεύτρια θα πρέπει να παρέχει υπηρεσίες Συμμόρφωσης με τον κανονισμό προστασίας προσωπικών δεδομένων (GDPR) και να προσκομίσει τουλάχιστον πέντε (5) βεβαιώσεις ή συμβάσεις αντίστοιχων έργων σε Οργανισμούς και τουλάχιστον δύο (2) να αφορούν ΔΕΥΑ.	
5.	Η προμηθεύτρια θα πρέπει παρέχει υπηρεσίες εγκατάστασης ISO 27001 για τουλάχιστον δέκα (10) έτη και να προσκομίσει τουλάχιστον τρεις (3) βεβαιώσεις αντίστοιχων έργων.	
6.	Προσκόμιση Υπεύθυνης δήλωσης του συμμετέχοντα φορέα ότι δεν εμπίπτει στις περιπτώσεις του άρθρου 73 παρ.1 και 2 του Ν.4412/2016 και **ότι σε περίπτωση που αναδειχθεί ανάδοχος**	

ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΥΔΡΕΥΣΗΣ ΑΠΟΧΕΤΕΥΣΗΣ ΠΑΤΡΑΣ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

ΤΜΗΜΑ
ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

και πριν την υπογραφή της σύμβασης θα προσκομίσει: **α) απόσπασμα ποινικού μητρώου,** **β) πιστοποιητικό φορολογικής ενημερότητας και** **γ) πιστοποιητικό ασφαλιστικής ενημερότητας**	
7. ΠΡΟΣΟΧΗ: Ο προσφέρον είναι υποχρεωτικό να δώσει συνολική προσφορά	

ΠΡΟΣΟΧΗ:

- Η προσφορά αφορά το **σύνολο** των ζητούμενων ειδών.
- Μαζί με την τεχνική προσφορά να κατατεθεί φύλλο συμμόρφωσης προς όλες τις παραγράφους των τεχνικών προδιαγραφών με ίδια σειρά και αρίθμηση και με αντίστοιχες παραπομπές στα prospectus των **οποίων η κατάθεση είναι υποχρεωτική.** Αν το είδος εκτρέπεται τότε πρέπει να περιγράφονται αναλυτικά η εκτροπή ή η ασυμφωνία για να σχηματίζεται με σαφήνεια η γνώμη για την περαιτέρω εκτίμηση. Η μη κατάθεση του φύλλου συμμόρφωσης συνεπάγεται τον αποκλεισμό του διαγωνιζόμενου. Όλες οι τεχνικές προδιαγραφές είναι απαιτητές και επί ποινής αποκλεισμού.

ΔΗΜΟΤΙΚΗ
ΕΠΙΧΕΙΡΗΣΗ
ΥΔΡΕΥΣΗΣ
ΑΠΟΧΕΤΕΥΣΗΣ
Π Α Τ Ρ Α Σ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

ΔΕΥΑΠ

ΤΜΗΜΑ
ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

ΠΡΟΥΠΟΛΟΓΙΣΜΟΣ ΠΡΟΣΦΟΡΑΣ

	ΠΕΡΙΓΡΑΦΗ	ΤΕΜΑΧΙΑ	ΤΙΜΗ ΑΝΑ ΤΕΜΑΧΙΟ	ΣΥΝΟΛΙΚΗ ΤΙΜΗ	Φ.Π.Α.	ΤΕΛΙΚΗ ΤΙΜΗ ΜΕ Φ.Π.Α.
A	ΕΦΑΡΜΟΓΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ – ESET Antivirus	160		- €	- €	- €
B	ΕΦΑΡΜΟΓΗ ΑΠΟΤΡΟΠΗΣ ΑΠΩΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ – Safetica DLP	160		- €	- €	- €
C	ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΡΥΘΜΙΣΗ ΕΦΑΡΜΟΓΩΝ ESET Endpoint	1		- €	- €	- €
	ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΡΥΘΜΙΣΗ ΕΦΑΡΜΟΓΩΝ ESET SAFETICA DLP	1		- €	- €	- €
D	ΕΦΑΡΜΟΓΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ESET Endpoint Encryption Pro Edition	5		- €	- €	- €
E	ΥΠΗΡΕΣΙΑ ΕΛΑΧΙΣΤΟΠΟΙΗΣΗΣ ΝΕΩΝ ΑΠΕΙΛΩΝ ESET Dynamic Threat Defense	250		- €	- €	- €
F	ΕΦΑΡΜΟΓΗ ΠΡΟΣΤΑΣΙΑΣ ΓΙΑ ENDPOINTS ΚΑΙ FILE SERVERS ESET Secure Business	250		- €	- €	- €
				- €	**- €**	**- €**

ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΥΔΡΕΥΣΗΣ ΑΠΟΧΕΤΕΥΣΗΣ Π Α Τ Ρ Α Σ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr

ΔΕΥΑΠ

ΤΜΗΜΑ
ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ

ΠΡΟΪΣΤΑΜΕΝΟΣ
Γεώργιος Παπαδημητρόπουλος
Τηλ.: 2610.366.120
Email: computerisation@deyap.gr
george.papadimitropoulos@deyap.gr

ΠΙΝΑΚΑΣ ΤΙΜΩΝ ΟΛΟΓΡΑΦΩΣ

	ΠΕΡΙΓΡΑΦΗ	ΤΕΜΑΧΙΑ	ΤΙΜΗ ΑΝΑ ΤΕΜΑΧΙΟ	ΣΥΝΟΛΙΚΗ ΤΙΜΗ	Φ.Π.Α.	ΤΕΛΙΚΗ ΤΙΜΗ ΜΕ Φ.Π.Α.
A	ΕΦΑΡΜΟΓΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ – ESET Antivirus	160				
B	ΕΦΑΡΜΟΓΗ ΑΠΟΤΡΟΠΗΣ ΑΠΩΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ – Safetica DLP	160				
C	ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΡΥΘΜΙΣΗ ΕΦΑΡΜΟΓΩΝ ESET Endpoint	1				
	ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΡΥΘΜΙΣΗ ΕΦΑΡΜΟΓΩΝ ESET SAFETICA DLP	1				
D	ΕΦΑΡΜΟΓΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ESET Endpoint Encryption Pro Edition	5				
E	ΥΠΗΡΕΣΙΑ ΕΛΑΧΙΣΤΟΠΟΙΗΣΗΣ ΝΕΩΝ ΑΠΕΙΛΩΝ ESET Dynamic Threat Defense	250				
F	ΕΦΑΡΜΟΓΗ ΠΡΟΣΤΑΣΙΑΣ ΓΙΑ ENDPOINTS ΚΑΙ FILE SERVERS ESET Secure Business	250				
	ΣΥΝΟΛΑ					

ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΥΔΡΕΥΣΗΣ ΑΠΟΧΕΤΕΥΣΗΣ ΠΑΤΡΑΣ

Ακτή Δυμαίων 48
263 33 Πάτρα
Τηλ.:2610.366.100
Fax:2610.325.780
Email: info@deyap.gr