Η αρχιτεκτονική του Empisto: ιδιωτικό AI στη δική σας υποδομή, φτιαγμένο να αντέχει στον χρόνο

Πώς είναι φτιαγμένο το Empisto, πώς κρατά τα δεδομένα σας μέσα στην επιχείρηση και γιατί ο αρθρωτός σχεδιασμός του σας επιτρέπει να υιοθετείτε νέο AI χωρίς να ξεκινάτε από την αρχή. Για στελέχη IT, ασφάλειας και διοίκησης που αξιολογούν λύσεις ιδιωτικού AI.

10 Νοεμβρίου 2026

empisto.ai · τοπικό · ιδιωτικό · αξιόπιστο

Περιεχόμενα

01 Σύνοψη

02 Γιατί η αρχιτεκτονική έχει σημασία στο AI

03 Αρχές σχεδιασμού

04 Η πλατφόρμα με μια ματιά

05 Αρθρωτό και έτοιμο για το μέλλον

06 Ταυτότητα και πρόσβαση

07 Τα έγγραφά σας

08 Από την ερώτηση στην απάντηση

09 Μοντέλα AI

10 Εφαρμογές και εργαλεία

11 Ασφάλεια και προστασία δεδομένων

12 Εγκατάσταση και λειτουργία

13 Κατανομή ευθυνών

14 Διαβάστε επίσης

01 Σύνοψη

Το Empisto είναι μια πλατφόρμα ιδιωτικού AI που η επιχείρηση λειτουργεί στους δικούς της διακομιστές. Οι εργαζόμενοι ρωτούν σε απλή γλώσσα και παίρνουν απαντήσεις από τα έγγραφα της ίδιας της εταιρείας, και κάθε απάντηση συνοδεύεται από τις πηγές της. Στον ίδιο βοηθό λειτουργούν επίσης εφαρμογές για έργα, γραφήματα, ανάλυση δεδομένων και επιχειρησιακά συστήματα.

Τρεις ιδέες διατρέχουν όλη την αρχιτεκτονική. Πρώτον, τα δεδομένα σας μένουν σε υποδομή που ελέγχετε εσείς, και τίποτα δεν χρειάζεται το διαδίκτυο για να λειτουργήσει. Δεύτερον, η πρόσβαση κρίνεται με τους δικούς σας κανόνες πριν γίνει αναζήτηση σε οποιοδήποτε έγγραφο, και καθετί σημαντικό καταγράφεται. Τρίτον, κάθε κομμάτι είναι αρθρωτό, ώστε η πλατφόρμα να ενσωματώνει νέα μοντέλα AI, εργαλεία και πηγές καθώς κυκλοφορούν, χωρίς να χρειαστεί έργο μετάπτωσης.

Το κείμενο αυτό εξηγεί πώς επιτυγχάνονται όλα αυτά, στο βάθος που χρειάζεται ένα στέλεχος IT, ασφάλειας ή διοίκησης για να σχηματίσει άποψη. Εξετάζει τα δομικά στοιχεία της πλατφόρμας, τη σύνδεση και την πρόσβαση, τον τρόπο που αξιοποιούνται τα έγγραφα, τι γίνεται όταν κάποιος κάνει μια ερώτηση, τα μοντέλα AI, τις εφαρμογές και τα εργαλεία, την ασφάλεια και την προστασία δεδομένων, και τέλος πώς στήνεται και λειτουργεί μια εγκατάσταση.

ΠΟΥ ΤΡΕΧΕΙ

Στους δικούς σας διακομιστές, στις εγκαταστάσεις σας ή στο ιδιωτικό σας κέντρο δεδομένων.

ΤΑ ΔΕΔΟΜΕΝΑ ΣΑΣ

Έγγραφα, συνομιλίες και καταγραφές παραμένουν στη δική σας υποδομή.

ΜΟΝΤΕΛΑ AI

Ανοιχτά μοντέλα στον δικό σας διακομιστή GPU, που επιλέγονται ανά ομάδα.

ΣΥΝΔΕΣΗ

Με τους εταιρικούς λογαριασμούς που έχουν ήδη οι εργαζόμενοί σας, μέσω του παρόχου ταυτότητάς σας.

ΔΙΑΔΙΚΤΥΟ

Δεν χρειάζεται για τη λειτουργία. Κάθε εξωτερική σύνδεση είναι προαιρετική και την ενεργοποιείτε εσείς.

ΤΗΛΕΜΕΤΡΙΑ

Καμία. Δεν στέλνεται τίποτα πίσω στο Empisto.

02 Γιατί η αρχιτεκτονική έχει σημασία στο AI

Οι περισσότερες υπηρεσίες AI ζητούν από την εταιρεία να στέλνει τα έγγραφα και τις ερωτήσεις της σε διακομιστές τρίτων. Όταν πρόκειται για συμβάσεις, φακέλους ασθενών, οικονομικά στοιχεία ή οτιδήποτε καλύπτεται από συμφωνία εμπιστευτικότητας, εκεί συχνά τελειώνει η συζήτηση. Η

χρέωση ανά χρήση φέρνει κι ένα δεύτερο πρόβλημα: όσο περισσότεροι χρησιμοποιούν το εργαλείο, τόσο λιγότερο προβλέψιμος γίνεται ο λογαριασμός.

Υπάρχει και τρίτος κίνδυνος, που εύκολα περνά απαρατήρητος. Το AI εξελίσσεται ταχύτερα από κάθε άλλο κομμάτι της πληροφορικής. Το καλύτερο μοντέλο της φετινής χρονιάς δεν θα είναι το καλύτερο της επόμενης, και τα εργαλεία που θέλουν οι χρήστες να συνδέσουν μαζί του αλλάζουν συνεχώς. Μια πλατφόρμα χτισμένη γύρω από ένα μοντέλο, έναν προμηθευτή ή έναν μόνο τρόπο δουλειάς θα χρειαστεί αντικατάσταση ακριβώς τη στιγμή που αρχίζει να αποδίδει.

Η αρχιτεκτονική του Empisto απαντά και στα τρία. Η πλατφόρμα τρέχει μέσα στην επιχείρησή σας, με σταθερή άδεια χρήσης αντί για μετρητή, και αποτελείται από αντικαταστάσιμα κομμάτια που συνδέονται μεταξύ τους με ανοιχτά πρότυπα.

03 Αρχές σχεδιασμού

Μία περίμετρος. Όλα τα κομμάτια του Empisto τρέχουν μέσα στο δικό σας περιβάλλον. Η πλατφόρμα δεν χρειάζεται σύνδεση με το διαδίκτυο ή με το Empisto για να λειτουργήσει, και κάθε προαιρετική εξωτερική σύνδεση την ενεργοποιεί συνειδητά ένας διαχειριστής.

Πρώτα η πρόσβαση, μετά η απάντηση. Πριν ψάξει οτιδήποτε, το Empisto ξεκαθαρίζει ποια έγγραφα επιτρέπεται να χρησιμοποιήσει ο χρήστης. Μια απάντηση δεν μπορεί ποτέ να βασιστεί σε υλικό που ο χρήστης δεν είχε δικαίωμα να δει.

Κάθε κομμάτι αντικαθίσταται. Κάθε δομικό στοιχείο κάνει μία δουλειά, πίσω από μια σαφώς ορισμένη διεπαφή. Ένα καλύτερο μοντέλο ή ένα νέο εργαλείο ανάγνωσης εγγράφων παίρνει τη θέση του παλιού χωρίς να θιγούν τα υπόλοιπα.

Επέκταση, όχι ανακατασκευή. Οι νέες δυνατότητες προστίθενται ως εφαρμογές στην ίδια πλατφόρμα. Κάθε μία κληρονομεί την ίδια σύνδεση, τους ίδιους κανόνες πρόσβασης και το ίδιο αρχείο καταγραφής.

Καταγραφές που μπορείτε να ελέγξετε. Οι απαντήσεις δείχνουν τις πηγές τους. Οι σημαντικές ενέργειες γράφονται σε αρχείο καταγραφής που δεν μπορεί να αλλοιωθεί. Το περιεχόμενο που παράγει το AI φέρει σχετική σήμανση.

04 Η πλατφόρμα με μια ματιά

Το Σχήμα 1 δίνει τη συνολική εικόνα του Empisto. Οι χρήστες το χρησιμοποιούν μέσα από τον browser. Το μόνο κομμάτι που είναι προσβάσιμο από το δίκτυό σας είναι μια ασφαλής πύλη σύνδεσης. Πίσω της, τέσσερα επίπεδα κάνουν τη δουλειά, και τα συστήματα που ήδη έχετε συνδέονται σε αυτά χωρίς να μετακινηθούν.

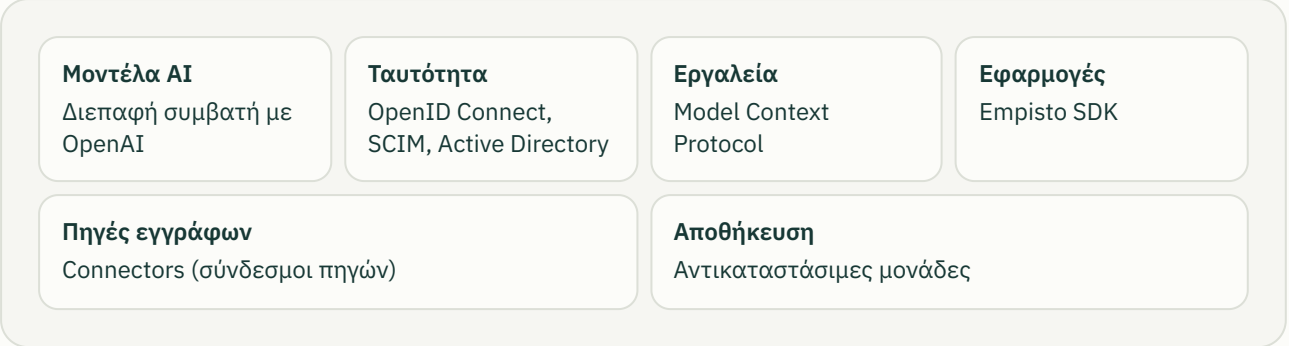


Σχήμα 1. Το Empisto στους διακομιστές σας. Τα συστήματά σας συνδέονται από κάτω. Το AI στο cloud μένει απέξω, πίσω από μια πύλη που από προεπιλογή είναι κλειστή.

Οι **Εφαρμογές** είναι ό,τι χρησιμοποιούν οι εργαζόμενοι στη δουλειά τους: ο βοηθός AI, η βιβλιοθήκη εγγράφων και εφαρμογές όπως τα Έργα, τα Γραφήματα και ο Αναλυτής δεδομένων. Ο **Έλεγχος** αποφασίζει ποιος βλέπει και κάνει τι, και κρατά το ιστορικό όσων έγιναν. Η **Γνώση** μετατρέπει τα έγγραφά σας σε υλικό που ο βοηθός μπορεί να αναζητήσει και να παραθέσει ως πηγή. Τα **Μοντέλα AI** κάνουν την ανάγνωση και τη γραφή, σε εξοπλισμό που σας ανήκει.

05 Αρθρωτό και έτοιμο για το μέλλον

Μια πλατφόρμα AI πρέπει να μπορεί να ενσωματώνει μοντέλα, εργαλεία και πηγές που δεν υπάρχουν ακόμη. Το Empisto είναι φτιαγμένο ακριβώς γι' αυτό. Κάθε κομμάτι συνδέεται μέσω μιας σαφώς ορισμένης διεπαφής, και όπου υπάρχει ανοιχτό πρότυπο του κλάδου, το Empisto το χρησιμοποιεί. Το Σχήμα 2 δείχνει τα σημεία όπου συνδέονται τα νέα κομμάτια.



Σχήμα 2. Τα σημεία όπου συνδέονται νέα κομμάτια. Καθένα μπορεί να προστεθεί ή να αντικατασταθεί χωρίς να αλλάξει τίποτα άλλο.

Κομμάτι	Πώς συνδέεται	Τι σημαίνει για εσάς
Μοντέλα AI	Η διεπαφή συμβατή με OpenAI, την οποία υποστηρίζουν οι περισσότεροι διακομιστές μοντέλων	Τρέχετε πολλά μοντέλα παράλληλα, επιλέγετε ποιο θα χρησιμοποιεί κάθε ομάδα και περνάτε στην επόμενη γενιά απλώς προσθέτοντάς την, χωρίς μετάπτωση
Ταυτότητα	OpenID Connect, SCIM και Active Directory	Κρατάτε τον πάροχο ταυτότητας και τον κατάλογο που ήδη έχετε. Το Empisto συγχρονίζεται μαζί τους
Εργαλεία	Το Model Context Protocol, το ανοιχτό πρότυπο για τη σύνδεση του AI με άλλα συστήματα	Συνδέετε επιχειρησιακά συστήματα ως εργαλεία, το καθένα με έγκριση διαχειριστή
Εφαρμογές	Το Empisto SDK	Οι νέες δυνατότητες προστίθενται ως εφαρμογές στην ίδια βάση, με τους ίδιους κανόνες
Πηγές εγγράφων	Σύνδεσμοι (connectors) για διακομιστές αρχείων, συσκευές NAS, SharePoint και OneDrive	Κάθε νέα πηγή προστίθεται με τον δικό της σύνδεσμο και διαβάζεται εκεί όπου βρίσκεται, όπως και οι προηγούμενες
Αποθήκευση	Μία αντικαταστάσιμη μονάδα για κάθε λειτουργία	Η βάση δεδομένων, το ευρετήριο αναζήτησης, ο χώρος φύλαξης κωδικών και το εργαλείο ανάγνωσης εγγράφων αντικαθίστανται το καθένα ανεξάρτητα

Τα κομμάτια αυτά είναι δοκιμασμένα στοιχεία ανοιχτού κώδικα. Αυτό σημαίνει επίσης ότι η ομάδα σας ή ένας ανεξάρτητος ελεγκτής μπορεί να εξετάσει πώς λειτουργούν. Αν αργότερα προτιμήσετε κάποιο άλλο, αλλάζετε μία μονάδα, όχι πλατφόρμα. Τα έγγραφα, οι χώροι εργασίας, τα δικαιώματα και οι εφαρμογές σας μένουν εκεί που είναι.

06 Ταυτότητα και πρόσβαση

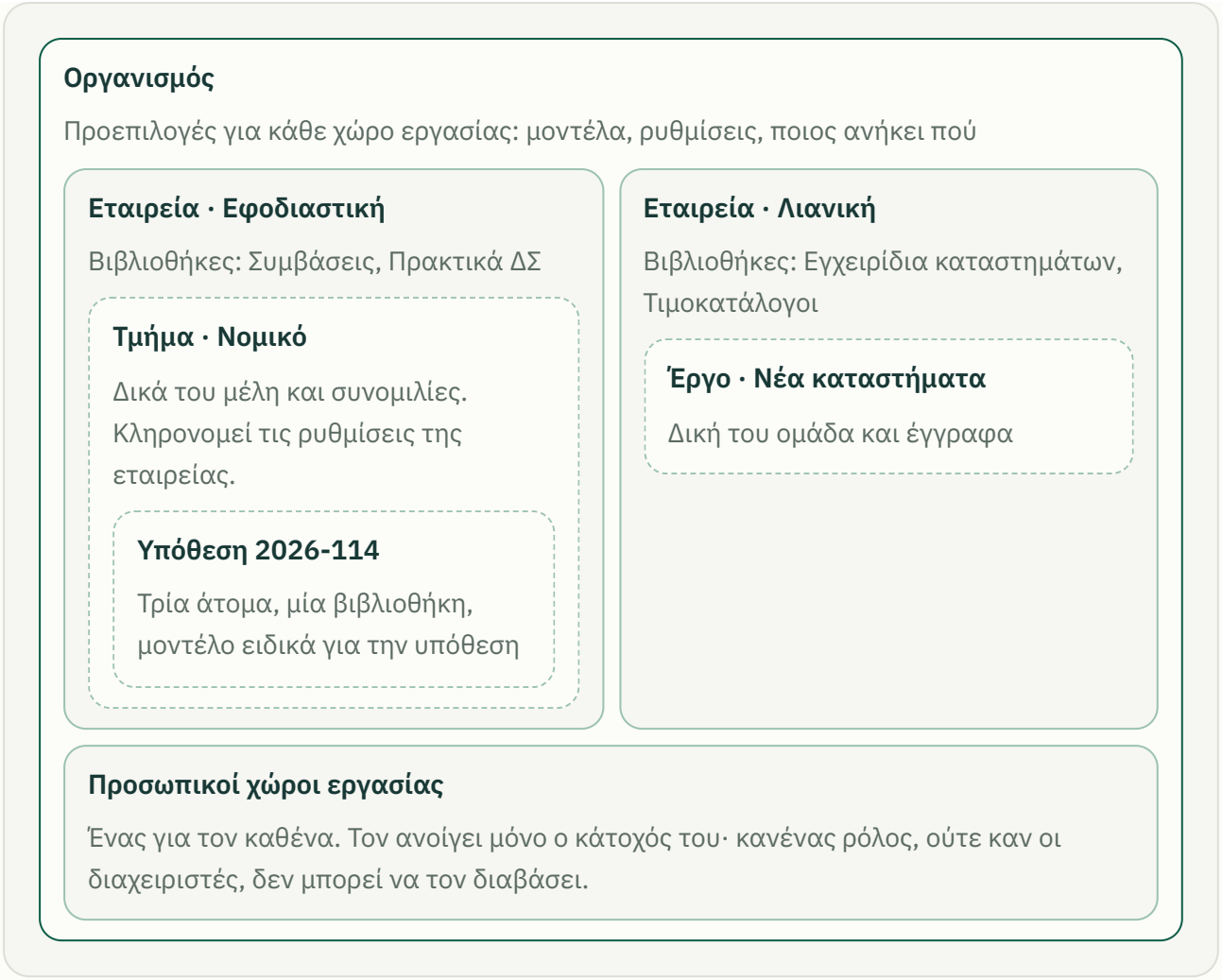
Σύνδεση με τους λογαριασμούς που ήδη έχετε

Οι χρήστες συνδέονται μέσω του παρόχου ταυτότητάς σας, για παράδειγμα του Microsoft Entra ID ή οποιουδήποτε παρόχου υποστηρίζει OpenID Connect. Το Empisto μπορεί επίσης να συγχρονίζει χρήστες και ομάδες με τον εταιρικό σας κατάλογο, μέσω SCIM ή Active Directory. Όταν το τμήμα IT αφαιρεί κάποιον, χάνεται μαζί και η πρόσβασή του στο Empisto. Δεν χρειάζεται να διαχειρίζεστε ξεχωριστούς κωδικούς.

Οι ομάδες του καταλόγου μετατρέπονται σε δικαιώματα. Ένας διαχειριστής ορίζει ποια ομάδα παίρνει ποιον ρόλο, είτε σε όλη την πλατφόρμα είτε σε έναν μόνο χώρο εργασίας, και οι αλλαγές στον κατάλογο εφαρμόζονται χωρίς να χρειαστεί κανείς να πειράξει το Empisto.

Χώροι εργασίας στα μέτρα του οργανισμού σας

Ο χώρος εργασίας είναι ένα ξεχωριστό περιβάλλον για μια ομάδα, μια εταιρεία, ένα έργο ή μια υπόθεση. Έχει τα δικά του μέλη, συνομιλίες και ρυθμίσεις, και αποκτά πρόσβαση στις βιβλιοθήκες εγγράφων που του χρειάζονται. Οι χώροι εργασίας μπορούν να μπαίνουν ο ένας μέσα στον άλλο, ώστε να αντιστοιχούν στη δομή του οργανισμού, και οι ρυθμίσεις περνούν από τα πάνω επίπεδα στα κάτω. Έτσι ένα τμήμα μπορεί να έχει δικό του μοντέλο ή δικούς του κανόνες χωρίς να επαναλαμβάνει όλη τη διαμόρφωση.



Σχήμα 3. Χώροι εργασίας ο ένας μέσα στον άλλο, όπως η δομή ενός οργανισμού. Οι ρυθμίσεις περνούν από πάνω προς τα κάτω. Οι προσωπικοί χώροι εργασίας μένουν χωριστά.

Κάθε χρήστης έχει επίσης τον δικό του προσωπικό χώρο εργασίας, που ανήκει αποκλειστικά σε εκείνον. Κανένας διαχειριστής δεν μπορεί να τον διαβάσει. Σε έναν κοινόχρηστο χώρο εργασίας, οι συνομιλίες είναι από προεπιλογή ορατές στην ομάδα, αλλά μια συνομιλία μπορεί να μείνει ιδιωτική για όποιον την ξεκίνησε.

Βιβλιοθήκες και ρόλοι

Τα έγγραφα οργανώνονται σε βιβλιοθήκες, και κάθε βιβλιοθήκη παραχωρείται στους χώρους εργασίας που επιτρέπεται να τη χρησιμοποιούν. Οι ρόλοι καθορίζουν τι μπορεί να κάνει ο καθένας: οι διαχειριστές έχουν την ευθύνη της πλατφόρμας ή ενός μεμονωμένου χώρου εργασίας, οι επιμελητές γνώσης φροντίζουν τις βιβλιοθήκες και τα έγγραφα, και τα μέλη διαβάζουν και κάνουν ερωτήσεις. Κάθε εφαρμογή προσθέτει επιπλέον τα δικά της δικαιώματα.

Το Empisto δεν αντιγράφει τα δικαιώματα των διακομιστών αρχείων σας. Το ποιος μπορεί να δει ένα έγγραφο εξαρτάται από τη βιβλιοθήκη στην οποία ανήκει και από τους ρόλους που αναθέτετε. Έτσι η πρόσβαση ορίζεται σε ένα μόνο σημείο και ελέγχεται εύκολα.

07 Τα έγγραφά σας

Τα έγγραφα φτάνουν στο Empisto με δύο τρόπους. Είτε οι χρήστες τα ανεβάζουν από τον browser, είτε ένας διαχειριστής συνδέει έναν διακομιστή αρχείων ή ένα NAS, οπότε το Empisto διαβάζει τα έγγραφα εκεί όπου βρίσκονται, με δικαίωμα μόνο ανάγνωσης. Οι συνδεδεμένες πηγές ελέγχονται σε διαστήματα που ορίζετε εσείς: τα νέα και τα τροποποιημένα αρχεία ενσωματώνονται και τα διαγραμμένα αφαιρούνται. Τίποτα δεν χρειάζεται να μετακινηθεί ή να μεταφερθεί αλλού.

Το Empisto διαβάζει τις μορφές αρχείων που χρησιμοποιούν στην πράξη οι επιχειρήσεις: PDF (και με σαρωμένες σελίδες), Word, PowerPoint, Excel και CSV, ιστοσελίδες και αρχεία κειμένου, εικόνες, καθώς και συνήθεις μορφές δεδομένων και σχεδίων. Το κείμενο σε σαρωμένα έγγραφα και εικόνες αναγνωρίζεται στα αγγλικά, στα ελληνικά και στα πολωνικά. Οι επικεφαλίδες, οι πίνακες και οι αριθμοί σελίδων διατηρούνται, ώστε μια απάντηση να μπορεί να παραπέμψει στη συγκεκριμένη σελίδα και ενότητα από την οποία προέρχεται.

Η επεξεργασία κάθε εγγράφου γίνεται στους δικούς σας διακομιστές, από τα δικά σας μοντέλα. Τίποτα δεν στέλνεται έξω για ανάγνωση, μετάφραση ή ευρετηρίαση.

08 Από την ερώτηση στην απάντηση

Το Σχήμα 4 ακολουθεί μια ερώτηση από τη στιγμή που υποβάλλεται μέχρι να εμφανιστεί η απάντηση στην οθόνη. Όλα διαρκούν λίγα δευτερόλεπτα, και κάθε βήμα γίνεται στους διακομιστές σας.

1	ΣΥΝΔΕΣΗ	Ο χρήστης αναγνωρίζεται μέσω του παρόχου ταυτότητάς σας, χωρίς νέο κωδικό.
2	ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ	Πριν από κάθε αναζήτηση, το Empisto ορίζει ποιες βιβλιοθήκες μπορεί να χρησιμοποιήσει ο χρήστης σε αυτόν τον χώρο εργασίας.
3	ΕΥΡΕΣΗ ΑΠΟΣΠΑΣΜΑΤΩΝ	Η αναζήτηση γίνεται μόνο σε αυτές τις βιβλιοθήκες και βρίσκει τα αποσπάσματα που απαντούν στην ερώτηση.
4	ΣΥΝΤΑΞΗ ΑΠΑΝΤΗΣΗΣ	Ένα γλωσσικό μοντέλο στους δικούς σας διακομιστές διαβάζει τα αποσπάσματα και γράφει την απάντηση.
5	ΠΗΓΕΣ ΚΑΙ ΚΑΤΑΓΡΑΦΗ	Η απάντηση εμφανίζεται με αριθμημένες πηγές και η αναζήτηση γράφεται στο αρχείο καταγραφής.

Σχήμα 4. Η διαδρομή μιας ερώτησης. Η πρόσβαση κρίνεται πριν από την αναζήτηση, δεν φιλτράρεται εκ των υστέρων.

Για μια ομάδα ασφαλείας, δύο σημεία εδώ μετρούν περισσότερο από όλα. Επειδή η πρόσβαση κρίνεται πριν από την αναζήτηση, ένα απόσπασμα από βιβλιοθήκη που ο χρήστης δεν έχει δικαίωμα

να διαβάσει δεν ανακτάται καν. Και επειδή κάθε απάντηση παραθέτει τις πηγές της, οι χρήστες μπορούν να ελέγξουν όσα τους λέγονται.

Αν κάποιος χρησιμοποιήσει ένα εργαλείο μέσα σε μια συνομιλία, για παράδειγμα για να δημιουργήσει μια εργασία στα Έργα, κάθε ενέργεια που αλλάζει κάτι ζητά πρώτα τη δική του επιβεβαίωση.

09 Μοντέλα AI

Το Empisto δουλεύει με ανοιχτά μοντέλα AI που τρέχουν στον δικό σας διακομιστή GPU, μέσω της διεπαφής που χρησιμοποιούν οι περισσότεροι διακομιστές μοντέλων. Δεν είναι δεμένο με κανένα συγκεκριμένο μοντέλο ή προμηθευτή. Τα μοντέλα τα επιλέγετε εσείς: ένα γλωσσικό μοντέλο για τις απαντήσεις, ένα μοντέλο αναζήτησης για την εύρεση αποσπασμάτων και, αν το θέλετε, μοντέλα για εικόνα και ομιλία.

Τα μοντέλα επιλέγονται ανά χώρο εργασίας. Το νομικό τμήμα μπορεί να δουλεύει με ένα μοντέλο και η υπόλοιπη εταιρεία με άλλο, ενώ ένα νέο μοντέλο μπορεί να δοκιμαστεί πρώτα σε μία ομάδα πριν δοθεί σε όλους. Όταν κυκλοφορήσει ένα καλύτερο ανοιχτό μοντέλο, η υιοθέτησή του είναι θέμα ρύθμισης, όχι ολόκληρο έργο.

Εξοπλισμός. Τα μοντέλα τρέχουν σε GPU της NVIDIA ή της AMD. Το κατάλληλο μέγεθος εξαρτάται από τα μοντέλα που επιλέγετε και από το πόσοι τα χρησιμοποιούν ταυτόχρονα, και είναι μέρος κάθε εκτίμησης που ετοιμάζουμε.

Μοντέλα στο cloud. Το Empisto παραδίδεται χωρίς κανένα ρυθμισμένο AI στο cloud, και στην κανονική λειτουργία τίποτα δεν βγαίνει από το δίκτυό σας. Για τις ομάδες που θέλουν ένα μοντέλο στο cloud για μέρος της δουλειάς τους, το Empisto προσφέρει αυτή τη δυνατότητα με τους δικούς της ελέγχους: είναι ανενεργή από προεπιλογή, επιτρέπεται ή απαγορεύεται ανά χώρο εργασίας, τα ευαίσθητα έγγραφα μένουν μέσα, τα προσωπικά στοιχεία αφαιρούνται πριν από την αποστολή και κάθε αίτημα καταγράφεται.

Το παραγόμενο περιεχόμενο επισημαίνεται. Οι απαντήσεις, τα έγγραφα που εξάγονται και ο ήχος που παράγεται φέρουν σήμανση ότι δημιουργήθηκαν από AI. Έτσι υποστηρίζονται οι υποχρεώσεις διαφάνειας που θέτει ο Κανονισμός για την ΤΝ (AI Act).

10 Εφαρμογές και εργαλεία

Εφαρμογές

Οι εφαρμογές προσθέτουν δυνατότητες στον βοηθό χωρίς να βγαίνουν από τους κανόνες της πλατφόρμας. Κάθε μία χρησιμοποιεί την ίδια σύνδεση, τηρεί τους ίδιους κανόνες πρόσβασης και γράφει στο ίδιο αρχείο καταγραφής. Αναπτύσσονται με το Empisto SDK, και κάθε εγκατεστημένη εφαρμογή είναι επαληθευμένη έκδοση.

Εφαρμογή	Τι κάνει
Έργα	Πίνακες, εργασίες και ροές εργασιών, που ο βοηθός μπορεί να δημιουργεί και να ενημερώνει μέσα από μια συνομιλία
Γραφήματα	Μετατρέπει απαντήσεις και πίνακες σε γραφήματα
Αναλυτής δεδομένων	Απαντά σε ερωτήσεις για υπολογιστικά φύλλα εκτελώντας την ανάλυση σε απομονωμένο περιβάλλον, χωρίς πρόσβαση στο δίκτυο και με δεδομένα μόνο για ανάγνωση
Σύνδεση ERP	Ερωτήσεις για παραγγελίες, αποθέματα και τιμολόγια, με πρόσβαση μόνο για ανάγνωση

Εργαλεία

Τα εργαλεία επιτρέπουν στον βοηθό να συνεργάζεται με άλλα συστήματα. Συνδέονται μέσω του Model Context Protocol, ενός ανοιχτού προτύπου, οπότε η ίδια προσέγγιση ισχύει και για τα σημερινά συστήματα και για όσα έρθουν αύριο. Όλα τα εργαλεία περνούν από τους ίδιους ελέγχους:

1. **Έγκριση.** Ένας διαχειριστής εγκρίνει κάθε εργαλείο πριν το χρησιμοποιήσει οποιοσδήποτε, και το εγκρίνει ξανά αν αλλάξει.
2. **Ανά χώρο εργασίας.** Κάθε χώρος εργασίας έχει μόνο τα εργαλεία που του έχουν δοθεί.
3. **Επιβεβαίωση.** Ένα εργαλείο που πρόκειται να αλλάξει κάτι ζητά πρώτα επιβεβαίωση από τον χρήστη.
4. **Καταγραφή.** Κάθε χρήση εργαλείου γράφεται στο αρχείο καταγραφής.

11 Ασφάλεια και προστασία δεδομένων

Η περίμετρος του δικτύου

Οι χρήστες φτάνουν στο Empisto μόνο μέσω της ασφαλούς πύλης σύνδεσης, με κρυπτογραφημένη επικοινωνία. Τα υπόλοιπα κομμάτια δεν είναι εκτεθειμένα στους χρήστες: λειτουργούν μέσα στους διακομιστές και στο εσωτερικό δίκτυό σας. Το Empisto δεν χρειάζεται τίποτα από το διαδίκτυο για να λειτουργήσει, και δεν έχει τηλεμετρία, αναφορές χρήσης, έλεγχο για ενημερώσεις ή διακομιστή αδειών. Δεν μας στέλνεται τίποτα.

Οι λίγες εξωτερικές συνδέσεις που μπορεί να υπάρξουν είναι όλες προαιρετικές και υπό τον έλεγχό σας.

Σύνδεση	Πότε χρησιμοποιείται	Ποιος αποφασίζει
Ο πάροχος ταυτότητάς σας	Κατά τη σύνδεση των χρηστών, αν ο πάροχός σας είναι υπηρεσία cloud, όπως το Microsoft Entra ID	Η δική σας επιλογή παρόχου ταυτότητας
Εξωτερικά εργαλεία	Μόνο αν ένας διαχειριστής προσθέσει εργαλείο εκτός του δικτύου σας	Έγκριση διαχειριστή, ανά χώρο εργασίας
Ιστοσελίδες σε συνομιλία	Ανενεργές από προεπιλογή. Αν ενεργοποιηθούν, μόνο οι ιστότοποι που περιλαμβάνονται σε λίστα	Διαχειριστής

Σύνδεση	Πότε χρησιμοποιείται	Ποιος αποφασίζει
Διακομιστές μοντέλων AI	Μόνο οι διακομιστές που δηλώνουν οι διαχειριστές σας	Διαχειριστής

Μια εγκατάσταση μπορεί επίσης να λειτουργεί σε πλήρη απομόνωση (air-gapped), οπότε τα εξωτερικά εργαλεία και οι ιστοσελίδες απενεργοποιούνται εντελώς.

Τα δεδομένα σας

Τα έγγραφα, οι συνομιλίες, το ευρετήριο αναζήτησης και το αρχείο καταγραφής αποθηκεύονται όλα στους δικούς σας διακομιστές. Οι κωδικοί και τα κλειδιά που χρειάζεται το Empisto φυλάσσονται σε ειδικό χώρο φύλαξης κωδικών, ποτέ σε αρχεία ρυθμίσεων. Την κρυπτογράφηση των αποθηκευμένων δεδομένων την παρέχει η υποδομή σας, μέσω κρυπτογράφησης δίσκων ή τόμων αποθήκευσης στους διακομιστές.

Το αρχείο καταγραφής

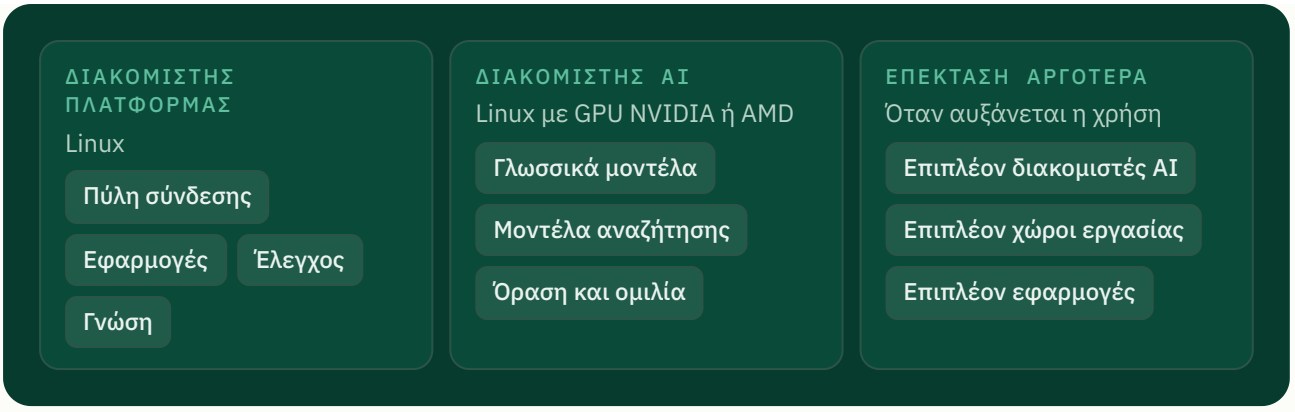
Καταγράφονται οι σημαντικές ενέργειες: αλλαγές σε χώρους εργασίας, μέλη και ρόλους, σε βιβλιοθήκες και έγγραφα, σε μοντέλα και ρυθμίσεις, κάθε αναζήτηση και απάντηση, και κάθε χρήση εργαλείου. Κανείς δεν μπορεί να αλλάξει ή να διαγράψει μια εγγραφή μέσα από το Empisto, ούτε καν οι διαχειριστές. Το αρχείο δείχνει ποιος έκανε τι και πότε, όχι το περιεχόμενο των ερωτήσεων. Οι εξουσιοδοτημένοι διαχειριστές μπορούν να το εξετάσουν και να το εξαγάγουν.

Διατήρηση και διαγραφή δεδομένων

Οι χρήστες μπορούν να εξαγάγουν τις συνομιλίες τους σε Word, PDF ή Markdown. Για κάθε είδος δεδομένων μπορεί να οριστεί η δική του περίοδος διατήρησης, και τα δεδομένα ενός προσώπου μπορούν να εξαχθούν ή να διαγραφούν κατόπιν αιτήματος, ενώ το αρχείο καταγραφής διατηρεί το ιστορικό των ενεργειών.

12 Εγκατάσταση και λειτουργία

Το Empisto τρέχει ως σύνολο από containers σε διακομιστές Linux. Οι περισσότερες εταιρείες ξεκινούν με δύο διακομιστές, έναν για την πλατφόρμα και έναν για τα μοντέλα AI. Με κατάλληλη GPU, τα δύο μπορούν να συνυπάρχουν σε ένα μηχάνημα.



Σχήμα 5. Μια τυπική εγκατάσταση και πώς επεκτείνεται. Οι δύο ρόλοι, πλατφόρμα και AI, μπορούν επίσης να συνυπάρχουν σε έναν διακομιστή με αρκετή μνήμη GPU.

Εγκατάσταση και ενημερώσεις. Μηχανικοί του Empisto εγκαθιστούν και ενημερώνουν την πλατφόρμα μαζί με την ομάδα IT σας, όποτε επιλέξετε εσείς, από ψηφιακά υπογεγραμμένες και αριθμημένες εκδόσεις. Για δίκτυα χωρίς πρόσβαση στο διαδίκτυο υπάρχει πακέτο εγκατάστασης εκτός σύνδεσης.

Παρακολούθηση. Κάθε υπηρεσία αναφέρει την κατάστασή της, και οι καταγραφές λειτουργίας στέλνονται σε όποια εργαλεία παρακολούθησης ήδη χρησιμοποιείτε.

Αντίγραφα ασφαλείας. Ένα πλήρες αντίγραφο ασφαλείας καλύπτει τις βάσεις δεδομένων, το ευρετήριο αναζήτησης και τον χώρο αποθήκευσης εγγράφων. Μπορούμε να σας παρέχουμε μια κρυπτογραφημένη, προγραμματισμένη διαδικασία λήψης αντιγράφων που καλύπτει και τα τρία.

13 Κατανομή ευθυνών

Όταν το AI τρέχει στη δική σας υποδομή, η δουλειά μοιράζεται με τρόπο που καλό είναι να συμφωνηθεί από νωρίς.

Τομέας	Empisto	Εσείς
Εξοπλισμός και λειτουργικό σύστημα	Συμβουλές για το μέγεθος του εξοπλισμού και μια διαμόρφωση αναφοράς	Οι διακομιστές, το λειτουργικό σύστημα και οι ενημερώσεις του
Δίκτυο	Η λίστα με τις συνδέσεις που χρειάζεται το Empisto	Τείχη προστασίας, τμήματα δικτύου και το πιστοποιητικό ασφαλείας
Ταυτότητα	Η σύνδεση του Empisto με τον πάροχο ταυτότητας και τον κατάλογό σας	Ο πάροχος ταυτότητας, οι ομάδες του και ποιοι ανήκουν σε αυτές
Προστασία δεδομένων	Πρόσβαση ανά βιβλιοθήκη και ρόλο, το αρχείο καταγραφής	Η κρυπτογράφηση δίσκων στους διακομιστές και το ποιος μπορεί να συνδεθεί σε αυτούς
Αντίγραφα ασφαλείας	Η διαδικασία λήψης αντιγράφων	Η λήψη των αντιγράφων και οι δοκιμές επαναφοράς

Τομέας	Empisto	Εσείς
Μοντέλα AI	Προτάσεις και ρύθμιση	Η επιλογή των μοντέλων και οι όροι άδειας χρήσης τους
Ενημερώσεις	Οι νέες εκδόσεις και ο τρόπος εφαρμογής τους	Τα παράθυρα συντήρησης και η έγκριση

14 Διαβάστε επίσης

Η σελίδα «Αρχιτεκτονική» δείχνει την ίδια πλατφόρμα με απλά λόγια, μαζί με μια διαδραστική παρουσίαση της διαδρομής μιας ερώτησης. Η σελίδα «Ασφάλεια» απαντά στις έξι ερωτήσεις που θέτουν πρώτα απ' όλα οι ομάδες ασφαλείας, και η σελίδα «Αρθρωτός σχεδιασμός» δείχνει πώς μπορεί να αντικατασταθεί κάθε κομμάτι. Για μια τεχνική συνάντηση με τους ανθρώπους που έφτιαξαν το Empisto ή για μια εκτίμηση για το δικό σας περιβάλλον, ξεκινήστε εδώ.