GTB Technologies
Data Security that Works™

Όταν τα Ιατρικά Δεδομένα Ξεφεύγουν από τον Έλεγχο: Το DLP στην Πρώτη Γραμμή Άμυνας

Προστατεύοντας τις πληροφορίες των ασθενών σε μια εποχή εξελιγμένων κυβερνοαπειλών και πολύπλοκων οικοσυστημάτων υγειονομικής περίθαλψης

Λάμπρος Κατσώνης
Διευθυντής τεχνολογικών λύσεων,
Guardbyte

GTB Technologies
Data Security that Works™

Το Σημερινό Τοπίο Δεδομένων Υγειονομικής Περίθαλψης

Ψηφιακός Μετασχηματισμός

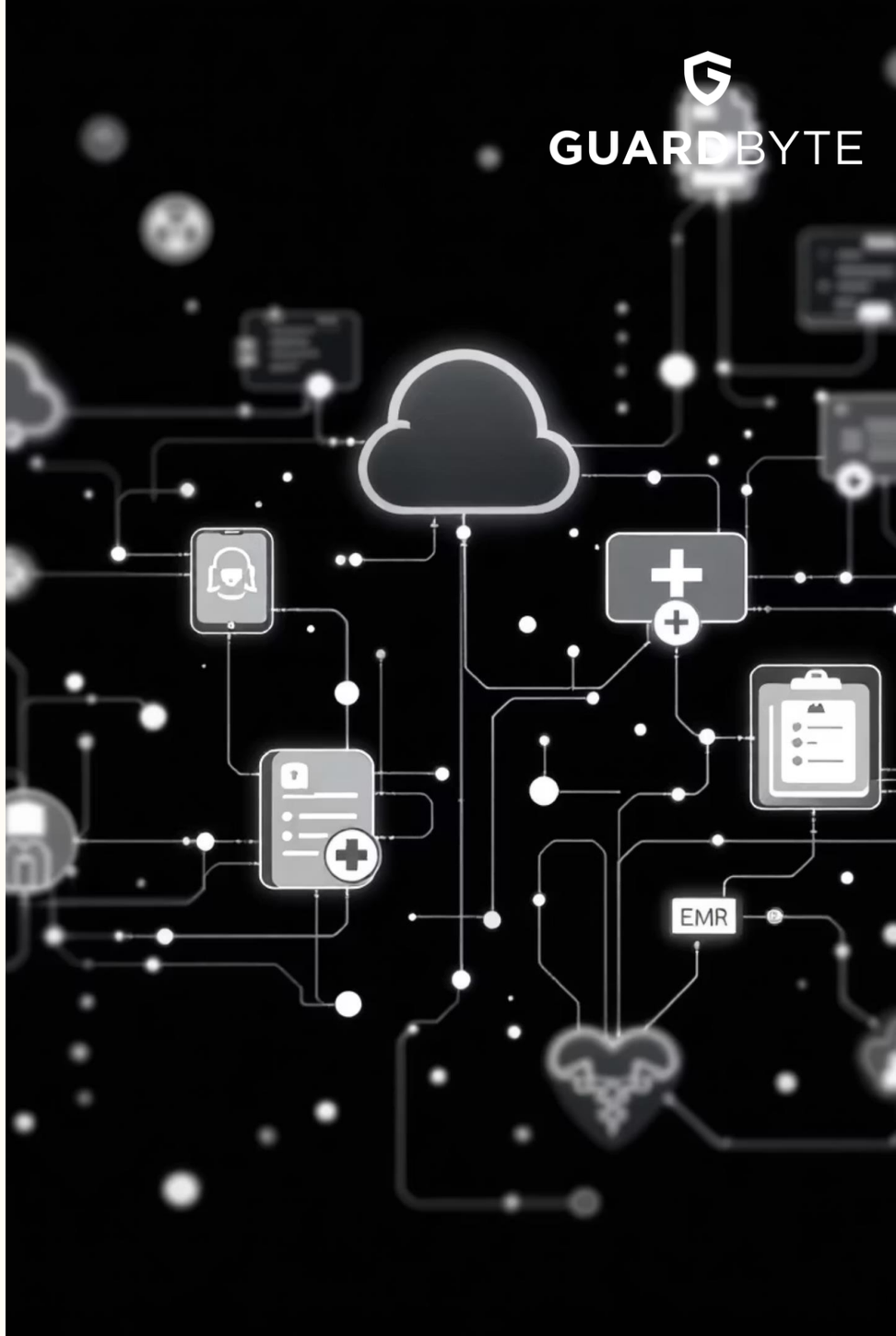
Οι οργανισμοί υγειονομικής περίθαλψης επεξεργάζονται καθημερινά εκατομμύρια ευαίσθητα ιατρικά αρχεία ασθενών μέσω ηλεκτρονικών συστημάτων υγείας, πλατφορμών cloud και κινητών συσκευών.

Αυτή η ψηφιακή μετάβαση βελτιώνει την παροχή φροντίδας, αλλά δημιουργεί νέες ευπάθειες για την έκθεση δεδομένων.

Ρυθμιστική Πίεση

Ο GDPR, ο HIPAA και οι εθνικοί κανονισμοί υγειονομικής περίθαλψης επιβάλλουν αυστηρή προστασία των προσωπικών πληροφοριών υγείας.

Η μη συμμόρφωση συνεπάγεται σοβαρές οικονομικές κυρώσεις και ανεπανόρθωτη ζημιά στην φήμη του ιδρύματος.



Κρίσιμες Ευπάθειες στην Υγειονομική Περίθαλψη

Μη κρυπτογραφημένες επικοινωνίες

Το ιατρικό προσωπικό συχνά μοιράζεται δεδομένα ασθενών μέσω email και εφαρμογών ανταλλαγής μηνυμάτων χωρίς κατάλληλη κρυπτογράφηση ή πρωτόκολλα ασφαλείας.

Κίνδυνοι από φορητές συσκευές

Οι μονάδες USB και οι εξωτερικές συσκευές αποθήκευσης μπορούν εύκολα να αντιγράψουν και να αφαιρέσουν ευαίσθητες πληροφορίες από ασφαλή περιβάλλοντα.

Ανθρώπινο Λάθος

Η τυχαία αποκάλυψη δεδομένων μέσω λανθασμένων email, λανθασμένων συνημμένων ή λανθασμένων ρυθμίσεων κοινής χρήσης παραμένει η κύρια αιτία παραβιάσεων.

Σκιώδης Πληροφορική (Shadow IT)

Οι μη εξουσιοδοτημένες υπηρεσίες cloud και οι προσωπικές εφαρμογές παρακάμπτουν τους θεσμικούς ελέγχους ασφαλείας, δημιουργώντας διαδρομές διαρροής δεδομένων.

GUARDBYTE

Το Κόστος της Απώλειας Δεδομένων

€4.5M

Μέσο Κόστος Παραβίασης

Οι παραβιάσεις δεδομένων στον τομέα της υγείας κοστίζουν κατά μέσο όρο €4,5 εκατομμύρια ανά περιστατικό στους οργανισμούς στην Ευρώπη.

280

Ημέρες για Εντοπισμό

Ο μέσος χρόνος για τον εντοπισμό και τον περιορισμό μιας παραβίασης δεδομένων υγείας υπερβαίνει τις 280 ημέρες.

67%

Επαναλαμβανόμενοι Στόχοι

Οργανισμοί που έχουν υποστεί μία παραβίαση έχουν 67% περισσότερες πιθανότητες να στοχευθούν ξανά.

Πέρα από τις οικονομικές απώλειες, οι παραβιάσεις δεδομένων καταστρέφουν την εμπιστοσύνη των ασθενών, διαταράσσουν τις κλινικές λειτουργίες και εκθέτουν τους οργανισμούς σε νομικές ευθύνες και ρυθμιστικές κυρώσεις.

GTB Technologies
Data Security that Works™

GUARDBYTE

Πραγματικά Σενάρια Απειλών

Ο Τυχαίος Εσωτερικός Παράγοντας

Μια νοσοκόμα αποστέλλει κατά λάθος αποτελέσματα εξετάσεων ασθενών στον λάθος παραλήπτη, εκθέτοντας εμπιστευτικές ιατρικές πληροφορίες σε μη εξουσιοδοτημένα άτομα.

Ο Κακόβουλος Δράστης

Ένας δυσαρεστημένος υπάλληλος κατεβάζει βάσεις δεδομένων ασθενών σε ένα USB stick πριν αποχωρήσει από τον οργανισμό, σκοπεύοντας να πουλήσει τα αρχεία στο dark web.

Το Θύμα Ηλεκτρονικού Ψαρέματος (Phishing)

Μέλος ιατρικού προσωπικού κάνει κλικ σε ένα εξελιγμένο email ηλεκτρονικού ψαρέματος (phishing), παρέχοντας στους επιτιθέμενους πρόσβαση σε διαπιστευτήρια που μπορούν να διαρρεύσουν χιλιάδες αρχεία ασθενών.

Ο Χρήστης Shadow IT

Οι γιατροί ανεβάζουν σαρώσεις ασθενών σε προσωπικό αποθηκευτικό χώρο στο cloud για ευκολία, τοποθετώντας εν αγνοία τους ευαίσθητα δεδομένα εκτός ελέγχου ασφαλείας.

GTB Technologies
Data Security that Works™

GUARDBYTE

Καθημερινά Use Cases Απώλειας Δεδομένων

Τα ιατρικά δεδομένα χάνονται συχνότερα μέσω απλών, καθημερινών ενεργειών παρά από εξελιγμένες επιθέσεις. Δείτε πώς συμβαίνουν οι πιο κοινές παραβιάσεις στην πράξη:

Μεταφορά Δεδομένων από Ιατρικές Συσκευές

Μεταφέρω δεδομένα από ένα εγκεφαλογράφο (EEG), ένα υπέρηχο, ένα καρδιογράφο σε ένα USB stick για να τα μεταφέρω σε άλλο σύστημα ή για αναφορά. Αν χαθεί το USB; Τα δεδομένα γίνονται ελεύθερα προσβάσιμα σε οποιονδήποτε.

- *Αρχεία ασθενών χωρίς κρυπτογράφηση*
- *Προσωπικά δεδομένα υγείας εκτός ελέγχου*
- *Πιθανή πώληση στο dark web*
- *Παραβίαση GDPR με πρόστιμα εκατομμυρίων*

Λανθασμένη Αποστολή Κλινικών Αποτελεσμάτων

Στέλνω τα αποτελέσματα μιας κλινικής εξέτασης ή μιας απεικόνισης σε λάθος email - πληκτρολογώ λάθος διεύθυνση ή επιλέγω λάθος επαφή από το address book.

- *Διαγνωστικές εικόνες σε άγνωστο*
- *Εργαστηριακά αποτελέσματα παραλήπτη*
- *Ιστορικό ασθενή εκτεθειμένο*
- *Μη αναστρέψιμη κατάσταση*

Σύμφωνα με τα στοιχεία, πάνω από το 55% όλων των παραβιάσεων ασφαλείας στον ιατρικό κλάδο προέρχονται από εσωτερικούς παράγοντες, συχνά μέσω αυτών των απλών καθημερινών ενεργειών.

Πραγματικές Συνέπειες των Use Cases

Σενάριο USB με Ιατρικές Συσκευές

01

Η Συλλογή

Τεχνικός μεταφέρει δεδομένα από υπέρηχο σε USB για ανάλυση σε άλλο σύστημα

02

Η Απώλεια

USB χάνεται στο πάρκινγκ ή κλέβεται από το γραφείο

03

Η Εκμετάλλευση

Δεδομένα 200+ ασθενών πωλούνται στο dark web για €50,000

04

Οι Συνέπειες

€2M πρόστιμο GDPR + αγωγές ασθενών + καταστροφή φήμης

Σενάριο Λάθος Email

01

Η Αποστολή

Γιατρός στέλνει CT scan και διάγνωση καρκίνου σε λάθος email

02

Η Αντίληψη

Παραλήπτης βλέπει προσωπικά δεδομένα άγνωστου ασθενή

03

Η Αναφορά

Περιστατικό αναφέρεται στην Αρχή Προστασίας Δεδομένων

04

Η Κύρωση

€500,000 πρόστιμο για παραβίαση προσωπικών δεδομένων υγείας

Πραγματικό Παράδειγμα: *Το 2024, μια υπόθεση στον τομέα της υγειονομικής περίθαλψης είχε ως αποτέλεσμα πρόστιμο €3.8 εκατομμυρίων αφού κλάπη ένας μη κρυπτογραφημένος εξωτερικός δίσκος που περιείχε αρχεία ασθενών.*

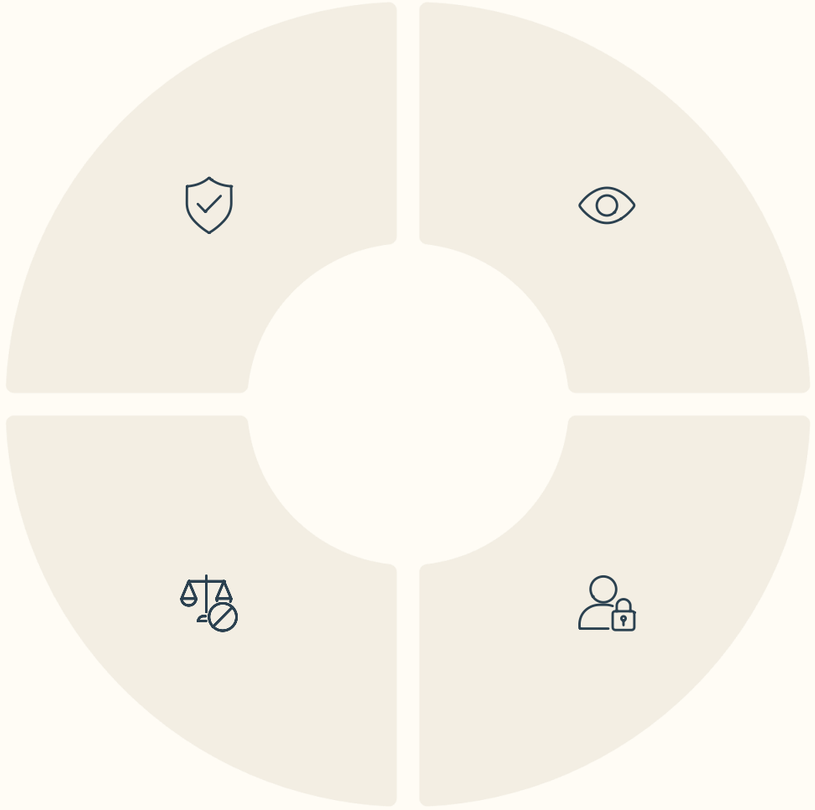
Πρόληψη Απώλειας Δεδομένων: Βασικές Αρχές

Ανακάλυψη

Προσδιορίστε πού βρίσκονται τα ευαίσθητα ιατρικά δεδομένα σε όλα τα συστήματα, τα τελικά σημεία και τις υπηρεσίες cloud

Παρακολούθηση

Παρακολουθήστε συνεχώς την κίνηση των δεδομένων και τα πρότυπα πρόσβασης σε πραγματικό χρόνο σε ολόκληρο τον οργανισμό



Πρόληψη

Αποκλείστε μη εξουσιοδοτημένες μεταφορές δεδομένων και επιβάλλετε πολιτικές στο σημείο πιθανής απώλειας δεδομένων

Προστασία

Εφαρμόστε αυτόματη κρυπτογράφηση και ελέγχους πρόσβασης βάσει ταξινόμησης δεδομένων και δικαιωμάτων χρήστη

GTB Technologies
Data Security that Works™

GUARDBYTE

Δημιουργία Ολοκληρωμένης Άμυνας DLP

01

Ταξινόμηση Δεδομένων

Κατηγοριοποιήστε τις ιατρικές πληροφορίες με βάση το επίπεδο ευαισθησίας – αναγνωριστικά ασθενών, διαγνώσεις, σχέδια θεραπείας και οικονομικά δεδομένα

02

Δημιουργία Πολιτικών

Θεσπίστε σαφείς κανόνες που διέπουν τον τρόπο πρόσβασης, κοινής χρήσης και μετάδοσης διαφορετικών τύπων δεδομένων

03

Ανάπτυξη Τεχνολογίας

Εφαρμόστε λύσεις DLP σε τελικά σημεία, δίκτυα, συστήματα ηλεκτρονικού ταχυδρομείου και πλατφόρμες cloud

04

Συνεχής Παρακολούθηση

Παρακολουθήστε τις ροές δεδομένων και αναλύστε τα μοτίβα για τον εντοπισμό ανωμαλιών και πιθανών περιστατικών ασφάλειας

05

Πρωτόκολλα Απόκρισης

Αναπτύξτε διαδικασίες για τη διερεύνηση ειδοποιήσεων και την αντιμετώπιση επιβεβαιωμένων συμβάντων απώλειας δεδομένων

GTB Technologies
Data Security that Works™

GUARDBYTE

Τεχνολογικές Δυνατότητες που Προστατεύουν

Επιθεώρηση Περιεχομένου

Η προηγμένη αναγνώριση προτύπων εντοπίζει ευαίσθητα ιατρικά δεδομένα σε αρχεία, email και μεταδόσεις, ανεξάρτητα από τη μορφή ή την τοποθεσία.

Περιβαλλοντική Ανάλυση

Η ανάλυση συμπεριφοράς αξιολογεί τις ενέργειες των χρηστών, την ευαισθησία των δεδομένων και τον προορισμό για να εκτιμήσει τα επίπεδα κινδύνου σε πραγματικό χρόνο.

Αυτόματη Κρυπτογράφηση

Τα ευαίσθητα δεδομένα κρυπτογραφούνται αυτόματα κατά τη μετάδοση και αποθήκευση, διατηρώντας την ασφάλεια χωρίς να διακόπτεται η ροή εργασιών.

Αντιμετώπιση Περιστατικών

Οι αυτοματοποιημένες ειδοποιήσεις ενημερώνουν τις ομάδες ασφαλείας για παραβιάσεις πολιτικής, επιτρέποντας τη γρήγορη διερεύνηση και αποκατάσταση πιθανών παραβιάσεων.

Αρχεία Ελέγχου

Η ολοκληρωμένη καταγραφή δημιουργεί αποδεικτικά στοιχεία για ελέγχους συμμόρφωσης και διερευνήσεις περιστατικών ασφαλείας.

Ενοποίηση Συστημάτων

Οι λύσεις DLP ενσωματώνονται με την υπάρχουσα υποδομή ασφαλείας, τις πλατφόρμες SIEM και τα συστήματα διαχείρισης ταυτότητας για ενοποιημένη προστασία.

GTB Technologies
Data Security that Works™

GUARDBYTE

Βέλτιστες Πρακτικές Εφαρμογής

1

Ξεκινήστε με την Ανακάλυψη

Ξεκινήστε χαρτογραφώντας πού υπάρχουν ευαίσθητα δεδομένα πριν αναπτύξετε ελέγχους πρόληψης

2

Προτεραιοποιήστε Περιοχές Υψηλού Κινδύνου

Επικεντρώστε τις αρχικές προσπάθειες σε email, αφαιρούμενα μέσα και εφαρμογές cloud όπου συνήθως συμβαίνουν παραβιάσεις

3

Συνεχής Εκπαίδευση του Προσωπικού

Η τακτική εκπαίδευση βοηθά τους επαγγελματίες υγείας να κατανοήσουν τις πολιτικές ασφάλειας δεδομένων και τον κρίσιμο ρόλο τους στην προστασία

4

Ισορροπία Ασφάλειας και Ευχρηστίας

Σχεδιάστε πολιτικές που προστατεύουν τα δεδομένα χωρίς να δημιουργούν τριβή που οδηγεί τους χρήστες να παρακάμπτουν τους ελέγχους

5

Παρακολούθηση και Βελτίωση

Ελέγχετε τακτικά την αποτελεσματικότητα του DLP και προσαρμόζετε τις πολιτικές βάσει των εξελισσόμενων απειλών και των λειτουργικών αναγκών

GUARDBYTE

Η προστασία της εμπιστοσύνης των ασθενών ξεκινά με τον έλεγχο των δεδομένων

Το ερώτημα δεν είναι αν θα εφαρμόσετε DLP, αλλά πόσο γρήγορα μπορείτε να το αναπτύξετε.

TQRCG

Λάμπρος Κατσώνης