A logo of a university of patras

AI-generated content may be incorrect.

Πολυτεχνική Σχολή

Τμήμα Μηχανικών Η/Υ & Πληροφορικής

Εφαρμοσμένα Πληροφοριακά Συστήματα ΙΙ

**Zero Trust Security και Προστασία Επιχειρησιακών Πληροφοριακών Συστημάτων**

Ναταλία-Μαρία Ηλία

Α.Μ. 1093367

Νικόλαος Χριστοδούλου

Α.Μ. 1093514

Πάτρα, 2025

Περιεχόμενα

[1) Εισαγωγή 3](#_Toc199785450)

[1.1     Σημασία του Προβλήματος 3](#_Toc199785451)

[1.2       Συνεισφορά 3](#_Toc199785452)

[1.3       Διάρθρωση 4](#_Toc199785453)

[2)  State-of-the-Art 4](#_Toc199785454)

[2.1       Επισκόπηση 4](#_Toc199785455)

[2.2   Μελέτες και τρέχουσες λύσεις 4](#_Toc199785456)

[2.3       Πρακτικές 6](#_Toc199785457)

[3 Παρουσίαση 7](#_Toc199785458)

[3.1   Παρουσίαση 7](#_Toc199785459)

[3.2 Αξιολόγηση 9](#_Toc199785460)

[4) Μελέτη Περίπτωσης 14](#_Toc199785461)

[Εισαγωγή 14](#_Toc199785462)

[4.1 Μελέτη Περίπτωσης – Προστασία Εσωτερικού Δικτύου σε Νοσοκομεία 14](#_Toc199785463)

[4.2 Μελέτη Περίπτωσης – Υποδομή DevOps Πλατφόρμας SaaS 15](#_Toc199785464)

[4.3 Μελέτη Περίπτωσης – Προστασία Τηλεργασίας σε Πολυεθνική Επιχείρηση Τραπεζικών Υπηρεσιών 16](#_Toc199785465)

[5) Μελλοντικές Προτάσεις 17](#_Toc199785466)

[6) Συμπεράσματα 18](#_Toc199785467)

[Βιβλιογραφία- Αναφορές 19](#_Toc199785468)

# 1) Εισαγωγή

## 1.1     Σημασία του Προβλήματος

Η συνεχώς αυξανόμενη πολυπλοκότητα των εταιρικών δικτύων, λόγω της ενσωμάτωσης τεχνολογιών όπως το cloud computing, οι φορητές συσκευές και η απομακρυσμένη εργασία, έχει δημιουργήσει νέες προκλήσεις στον τομέα της κυβερνοασφάλειας. Οι παραδοσιακές αρχιτεκτονικές ασφάλειας, οι οποίες βασίζονται σε  perimeter-based μοντέλα προστασίας, αποτυγχάνουν να ανταποκριθούν στις σύγχρονες απειλές. Τα μοντέλα αυτά βασίζονται στην υπόθεση ότι τα πάντα εντός του δικτύου είναι αξιόπιστα, γεγονός που καθιστά το εσωτερικό των συστημάτων ιδιαίτερα ευάλωτο στις πλευρικές κινήσεις των επιτιθέμενων και στις εσωτερικές απειλές [1][2]. Σύμφωνα με την έκθεση της IBM για το 2023, το 25% των παραβιάσεων δεδομένων οφείλονται σε εξουσιοδοτημένους χρήστες που καταχράστηκαν τα δικαιώματά τους [3]. Επιπλέον, όπως αναφέρει η Cisco (2024), οργανισμοί που δεν υιοθέτησαν σύγχρονα μοντέλα ασφάλειας, όπως η Zero Trust Architecture (ZTA), υπέστησαν κατά 40% περισσότερες επιτυχημένες παραβιάσεις [4]. Λόγω απειλών, όπως οι επιθέσεων ransomware, οι παραβιάσεις δεδομένων, η κλοπή ταυτότητας, το phishing, τα κενά ασφαλείας στο cloud και οι εσωτερικές απειλές, η ανάγκη για ένα νέο μοντέλο ασφάλειας είναι πλέον επιτακτική [2].

Η βασική αρχή της «μηδενικής εμπιστοσύνης » (Zero Trust), που συνοψίζεται στη φράση «ποτέ μην εμπιστεύεσαι, πάντα να επαληθεύεις», αντιμετωπίζει αυτά τα προβλήματα μέσω της συνεχούς επαλήθευσης της ταυτότητας των χρηστών και των συσκευών που επιχειρούν να έχουν πρόσβαση στους πόρους του οργανισμού. Ταυτόχρονα, το πρότυπο της μηδενικής εμπιστοσύνης  στηρίζεται στην ιδέα ότι θα παρέχονται μόνο τα ελάχιστα δικαιώματα στους εξουσιοδοτημένους χρήστες, δηλαδή αυτά που είναι αναγκαία για την εκτέλεση των καθηκόντων τους [7]. Επιπλέον, το μοντέλο δημιουργεί μικρές ασφαλείς ζώνες εντός του δικτύου, δηλαδή αξιοποιεί τεχνικές μικρο-κατακερματισμού (micro-segmentation), με σκοπό να μειώσει την εξάπλωση των εξωτερικών και εσωτερικών απειλών, με τις δεύτερες να είναι σήμερα πιο σημαντικές και κυρίαρχες [8][2]. Τέλος, πρόκειται για μία τεχνική, η οποία συμμορφώνεται με τους νομικούς κανονισμούς, οι οποίοι δεσμεύουν τους οργανισμούς να προστατεύουν δεδομένα και συστήματα με συγκεκριμένους τρόπους. Χαρακτηριστικά, το 2021, ο πρόεδρος των Ηνωμένων Πολιτειών καθιέρωσε την χρήση της τεχνικής της μηδενικής εμπιστοσύνης  σε όλες τις ομοσπονδιακές υπηρεσίες [9].

## 1.2       Συνεισφορά

  Το παρόν έγγραφο παρουσιάζει τις προκλήσεις που κατέστησαν αναγκαία τη στροφή προς την αρχιτεκτονική μηδενικής εμπιστοσύνης (Zero Trust Architecture - ZTA), δηλαδή την αυξανόμενη πολυπλοκότητα των εταιρικών δικτύων και τους περιορισμούς των παραδοσιακών περιμετρικών μοντέλων ασφάλειας. Δείχνει την εξέλιξή της από τα πρώτα μοντέλα ασφάλειας και επισημαίνει τα βασικά ορόσημα στην ανάπτυξή της από ερευνητές και ιδρύματα. Συζητά τα κενά ασφάλειας που εντοπίζονται στα σύγχρονα περιβάλλοντα δικτύων, όπως το cloud, τα δίκτυα επικοινωνίας και το IoT, και εξηγεί πώς οι αρχές της μηδενικής εμπιστοσύνης μετριάζουν τις εσωτερικές και εξωτερικές απειλές μέσω της συνεχούς επαλήθευσης και της μικρο-τμηματοποίησης. Περιγράφει τους βασικούς πυλώνες και τους θεμελιώδεις μηχανισμούς ενός συστήματος μηδενικής εμπιστοσύνης, τα απαιτούμενα τεχνολογικά στοιχεία και γίνεται σύγκριση με τα συμβατικά μοντέλα ασφάλειας όσον αφορά την αποτελεσματικότητα και την ανθεκτικότητα. Παρουσιάζει τα στρατηγικά στάδια και τις προκλήσεις που εμπλέκονται στην εφαρμογή ενός μοντέλου μηδενικής εμπιστοσύνης. Επιπλέον, προσφέρει μια λεπτομερή ανάλυση περιπτώσεων εφαρμογών zero trust σε εσωτερικά δίκτυα νοσοκομείων, στην υποδομή DevOps πλατφορμών SaaS και σε πολυεθνικές επιχειρήσεις τραπεζών. Τέλος, διερευνά τις τρέχουσες ερευνητικές τάσεις και τις μελλοντικές προοπτικές, δίνοντας έμφαση στην ενσωμάτωση της τεχνητής νοημοσύνης, της μηχανικής μάθησης, του blockchain και της ασφάλειας IoT για την ενίσχυση και επέκταση του Zero Trust.

## 1.3       Διάρθρωση

  Η εργασία περιλαμβάνει έξι ενότητες. Η τρέχουσα αποτελεί μία γενική εισαγωγή του μοντέλου της μηδενικής εμπιστοσύνης, καθώς και των αναγκών που οδήγησαν στη δημιουργία του. Στην δεύτερη πραγματοποιείται μία επισκόπηση των τεχνικών που έχουν προταθεί για την υλοποίηση του. Η τρίτη ενότητα περιλαμβάνει την αναλυτική παρουσίαση της αρχιτεκτονικής, των προτερημάτων και των μειονεκτημάτων της.  Η τέταρτη ενότητα επικεντρώνεται στους τομείς στους οποίους εφαρμόζεται. Στην πέμπτη ενότητα, γίνονται προτάσεις για μελλοντικές βελτιώσεις και στην έκτη παρουσιάζονται τα συνολικά συμπεράσματά μας.

# 2)  State-of-the-Art

## 2.1       Επισκόπηση

Η αρχιτεκτονική μηδενικής εμπιστοσύνης (ΖΤΑ) διατυπώθηκε για πρώτη φορά το 2010 από τον John Kindervag, ο οποίος πρότεινε ένα μοντέλο ασφάλειας που αμφισβητούσε ριζικά τη συμβατική προσέγγιση «trust but verify». Τα παραδοσιακά μοντέλα ασφάλειας λειτουργούσαν με την υπόθεση ότι οι οντότητες εντός της περιμέτρου ενός δικτύου μπορούσαν να είναι εξ’ ορισμού αξιόπιστες, δημιουργώντας μια δυαδική διάκριση μεταξύ «αξιόπιστων» εσωτερικών δικτύων και «μη αξιόπιστων» εξωτερικών δικτύων. Η επαναστατική προσέγγιση του Kindervag εξάλειψε αυτή την έμμεση εμπιστοσύνη, απαιτώντας αντίθετα, την αυθεντικοποίηση και εξουσιοδότηση όλων των χρηστών, των συσκευών και των ροών δικτύου, ανεξάρτητα από τη θέση τους στο δίκτυο [18].

Η βασική αρχή της μηδενικής εμπιστοσύνης μπορεί να συνοψιστεί ως εξής: καμία οντότητα (χρήστης, συσκευή, εφαρμογή ή δίκτυο) δεν πρέπει να είναι εγγενώς έμπιστη με βάση αποκλειστικά τη φυσική ή δικτυακή της θέση. Η προσέγγιση αυτή αντιμετωπίζει την αυξανόμενη ανεπάρκεια της ασφάλειας που βασίζεται στην περίμετρο σε σύγχρονα υπολογιστικά περιβάλλοντα.

## 2.2   Μελέτες και τρέχουσες λύσεις

Η αρχιτεκτονική μηδενικής εμπιστοσύνης (ΖΤΑ) έχει υποστεί σημαντική εξέλιξη από την αρχική της διατύπωση, με πολλούς ερευνητές και οργανισμούς να επεκτείνουν τα θεμέλια του Kindervag. Η παρούσα ενότητα παρακολουθεί τη χρονολογική εξέλιξη των προσεγγίσεων μηδενικής εμπιστοσύνης και συγκρίνει τις ιδιαίτερες αρχιτεκτονικές υλοποιήσεις τους.

Αρχικά, το μοντέλο μηδενικής εμπιστοσύνης του Kindervag που προτάθηκε το 2010 εισήγαγε την προσέγγιση «Data Acquisition Network» (DAN). Αυτή η πρωτοποριακή εφαρμογή εξήγαγε δεδομένα δικτύου σε ένα κεντρικό κέντρο διαχείρισης, για επιθεώρηση και ανάλυση σε πραγματικό χρόνο. Αν και πρωτοποριακό στην ιδέα του, στην πράξη, αυτό το πρώιμο μοντέλο αντιμετώπισε προκλήσεις, όπως η αυξημένη πολυπλοκότητα του δικτύου και οι καθυστερήσεις στην επικοινωνία των χρηστών [18].

Ύστερα, οι DeCusatis et al. προχώρησαν σε αυτόν τον τομέα το 2016 αναπτύσσοντας μια μέθοδο μηδενικής εμπιστοσύνης που βασίζεται στον έλεγχο πρόσβασης στις μεταφορές. Αυτή η υλοποίηση χρησιμοποίησε τεχνικές στεγανογραφίας και αντικατάστασης, ενσωματώνοντας σημεία ελέγχου ταυτότητας μέσα σε πακέτα αίτησης TCP και σε πακέτα πρώτου ελέγχου ταυτότητας. Αυτή η προσέγγιση ενίσχυσε την ασφάλεια των επιχειρηματικών πόρων σε περιβάλλοντα cloud computing και απέτρεψε την ανεπιθύμητη αναγνώριση των προστατευμένων πόρων, μέσω τεχνικών αναγνώρισης δακτυλικών αποτυπωμάτων. Παρόλα αυτά, αυτή η προστασία περιοριζόταν στα επίπεδα 3/4 του μοντέλου OSI, αφήνοντας το επίπεδο 7, που αφορά τις εφαρμογές, ευάλωτο σε επιθέσεις [19].

Το 2020, οι Rose et al. συνέβαλαν σημαντικά με τη σύνοψη των υφιστάμενων συστημάτων μηδενικής εμπιστοσύνης και την πρόταση τυποποιημένων βασικών λογικών στοιχείων για την αρχιτεκτονική. Επικεντρώθηκαν στην πρακτική εφαρμογή, αναγνωρίζοντας ότι η υιοθέτηση της ZTA θα πρέπει να είναι μια σταδιακή διαδικασία και όχι να απαιτεί πλήρη αντικατάσταση της υποδομής. Αυτή η προσέγγιση παρείχε στους οργανισμούς μια σαφή πορεία για τη μετάβαση από την αρχιτεκτονική που βασίζεται στην περίμετρο, στη μηδενική εμπιστοσύνη [20].  
 Την περίοδο από το 2020 και μετά παρατηρήθηκε ταχεία επέκταση της μηδενικής εμπιστοσύνης σε εξειδικευμένους τομείς, όπως ιατρικά συστήματα και συστήματα που χρησιμοποιούν containers. Συγκεκριμένα, οι Sultana et al. (2020) ανέπτυξαν ένα ασφαλές σύστημα ανταλλαγής ιατρικών εικόνων που συνδυάζει τις αρχές της μηδενικής εμπιστοσύνης με την τεχνολογία blockchain, ενισχύοντας την προστασία των ευαίσθητων ιατρικών πληροφοριών [21]. Επίσης, οι Weever et al. (2020) αντιμετώπισαν την πρόκληση της εφαρμογής της μηδενικής εμπιστοσύνης για την επικοινωνία και τη διακίνηση δεδομένων στο εσωτερικό ενός δικτύου, μεταξύ μικροϋπηρεσιών σε περιβάλλοντα κοντέινερ, αξιοποιώντας τις τεχνολογίες Kubernetes και το service mesh Istio [22].

Σημαντική πρόοδος σημειώθηκε το 2021, όταν οι Ramezanpour και Jagannath πρότειναν μια αρχιτεκτονική μηδενικής εμπιστοσύνης βασισμένη στην τεχνητή νοημοσύνη (i-ZTA). Αυτή η προσέγγιση αξιοποίησε την τεχνητή νοημοσύνη για έξυπνη ανίχνευση, αξιολόγηση και λήψη αποφάσεων, βελτιώνοντας σημαντικά την αποτελεσματικότητα των στοιχείων ZTA στην επεξεργασία μεγάλων δεδομένων. Η αρχιτεκτονική ενσωμάτωσε την τεχνητή νοημοσύνη με τα σημεία επιβολής πολιτικής (Policy Enforcement Points - PEP) και τα σημεία λήψης αποφάσεων πολιτικής (Policy Decision Points - PDP), χρησιμοποιώντας την ενισχυτική μάθηση για τη μεγιστοποίηση των αποτελεσμάτων ασφαλείας και την από κοινού μάθηση για την παροχή αξιολόγησης με επίγνωση του πλαισίου [23].

Την ίδια χρονιά, οι Tian και Song επικεντρώθηκαν στην ανάπτυξη ενός ολοκληρωμένου μοντέλου εμπιστοσύνης βασισμένου στα μοντέλα BLP και BIBA. Το σύστημά τους αξιολόγησε τα σκορ εμπιστοσύνης για διάφορους πόρους του συστήματος, όπως χρήστες, τερματικά, αρχεία και εφαρμογές, εφαρμόζοντας διαφορετικά βάρη για την ενίσχυση της προστασίας της εμπιστευτικότητας και της ακεραιότητας. Ωστόσο, υπήρχαν αναπάντητα ερωτήματα σχετικά με τον τρόπο καθορισμού των αρχικών τιμών εμπιστοσύνης, καθώς και με την πληρότητα και ακρίβεια του τρόπου που είχαν οριστεί τα βάρη για την αξιολόγηση των διαφόρων συστατικών του συστήματος [24].

Το 2021, οι Ghate et al. πρότειναν μια προηγμένη αρχιτεκτονική που αξιοποιεί την εξαγωγή γενικευμένων σχέσεων χαρακτηριστικών για την αυτοματοποίηση του ελέγχου πρόσβασης με λεπτομερή κλίμακα. Αυτή η καινοτομία υποσχόταν χαμηλό κόστος για τον λεπτομερή έλεγχο, βελτιωμένη απόδοση, επεκτασιμότητα και ενισχυμένη ασφάλεια για τα επιχειρηματικά δίκτυα [25].

Το 2024, οι Gambo και Almulhem παρουσίασαν μια εκτενή βιβλιογραφική ανασκόπηση για μια δεκαετία έρευνας πάνω στη ZTA. Η εργασία αυτή πρότεινε ένα λεπτομερές ταξινομικό πλαίσιο για τις εφαρμογές και τις τεχνολογίες της ZTA, παρέχοντας σαφείς κατευθύνσεις για τη μελλοντική της χρήση, τόσο σε ερευνητικό όσο και σε πρακτικό επίπεδο. Η ανασκόπηση κατέδειξε την αυξανόμενη εφαρμογή της ZTA σε δυναμικά περιβάλλοντα, όπου απαιτείται προσαρμοστική ασφάλεια [26].

Το 2025, οι Nasiruzzaman et al. δημοσίευσαν μια ερευνητική εργασία που ανέλυσε την εξέλιξη της ZTA από θεωρία σε πράξη. Η μελέτη αυτή εστίασε στην τρέχουσα κατάσταση υλοποίησης της ZTA, τονίζοντας τη σημασία βασικών τεχνολογιών, όπως η πολυπαραγοντική αυθεντικοποίηση (multi-factor authentication), η δυναμική πολιτική πρόσβασης και η χρήση μηχανικής μάθησης για την αυτοματοποίηση της ανίχνευσης απειλών και της εφαρμογής πολιτικών ασφάλειας [27].

## 2.3       Πρακτικές

Η υιοθέτηση της αρχιτεκτονικής μηδενικής εμπιστοσύνης (ZTA) σε οργανισμούς και κυβερνήσεις αποκτά αυξανόμενη σημασία, ιδιαίτερα υπό το φως κυβερνοαπειλών που καθιστούν ανεπαρκείς τις παραδοσιακές μεθόδους ασφαλείας. Στις Ηνωμένες Πολιτείες, η Εκτελεστική Εντολή 14028 (2021) [29] καθόρισε την υποχρεωτική μετάβαση όλων των ομοσπονδιακών οργανισμών σε πρότυπα ZTA, οδηγώντας στην έκδοση στρατηγικής από το OMB και πρακτικών οδηγιών από το CISA. Οι οδηγίες αυτές προτείνουν ένα μοντέλο ωρίμανσης με έμφαση στην ταυτότητα, τις συσκευές, το δίκτυο, τις εφαρμογές και τα δεδομένα [30]. Παράλληλα, κορυφαίοι τεχνολογικοί οργανισμοί, όπως η Google με το BeyondCorp, η Microsoft μέσω της πλατφόρμας Azure, και η IBM με λύσεις ZTA-as-a-Service, πρωτοστατούν στην εφαρμογή των σχετικών τεχνολογιών. Η μετάβαση, συνήθως, δεν απαιτεί πλήρη αναδιάρθρωση των υπαρχουσών υποδομών, καθώς εφαρμόζονται υβριδικά μοντέλα που ενσωματώνουν τεχνικές όπως η αρχή της ελάχιστης προνομιακής πρόσβασης, η πολυπαραγοντική αυθεντικοποίηση και η τμηματοποίηση του δικτύου. Σημαντικές είναι επίσης οι εφαρμογές της ZTA σε κρίσιμους τομείς, όπως η υγειονομική περίθαλψη, η άμυνα και η ενέργεια, όπου απαιτείται υψηλή προστασία δεδομένων και συστημάτων. Τέλος, και στην Ευρωπαϊκή Ένωση παρατηρείται αυξημένη εστίαση στην υιοθέτηση ZTA, τόσο για τη διασφάλιση της ψηφιακής κυριαρχίας όσο και για τη συμμόρφωση με κανονισμούς όπως ο GDPR, μέσω εθνικών πολιτικών και ερευνητικών πρωτοβουλιών στο πλαίσιο του Horizon Europe.

# 3 Παρουσίαση

## 3.1   Παρουσίαση

Η τεχνική της μηδενικής εμπιστοσύνης (Zero Trust) αποτελεί ένα σύγχρονο framework κυβερνοασφάλειας που στηρίζεται στην φράση “ποτέ μην εμπιστεύεσαι, πάντα να επαληθεύεις”. Σύμφωνα με τη θεμελιώδη αυτή αρχή κανένας χρήστης ή συσκευή, ανεξαρτήτως τοποθεσίας ή προηγούμενης ταυτοποίησης, δεν μπορεί να θεωρηθεί ασφαλής για ένα πληροφοριακό σύστημα. Επομένως, απαιτείται διαρκής επαλήθευση ταυτότητας και αυστηρός έλεγχος πρόσβασης σε κάθε στάδιο αλληλεπίδρασης με τα συστήματα του οργανισμού. Πιο συγκεκριμένα, ακόμη και οι επιβεβαιωμένοι χρήστες καλούνται να επιβεβαιώνουν ξανά ανά τακτά χρονικά διαστήματα την ταυτότητά τους, καθώς βασική αρχή του μοντέλου της μηδενικής εμπιστοσύνης είναι ότι απειλές μπορούν να αποτελέσουν και οι επιβεβαιωμένοι χρήστες. Αυτή μάλιστα είναι και η βασική διαφορά του μοντέλου με τα παραδοσιακά μοντέλα ασφαλείας, τα οποία θεωρούσαν ότι υπήρχε μια περίμετρος προστασίας και οποιοσδήποτε χρήστης εντός της περιμέτρου θεωρείται ασφαλείς [7]. Ωστόσο, οι απειλές για έναν οργανισμό τείνουν να είναι πλέον ως επί το πλείστον προερχόμενες από το εσωτερικό του οργανισμού, οπότε η λογική της περιμέτρου προστασίας καταρρίπτεται. Αυτό άλλωστε είναι λογικό γιατί όσο περισσότερο οι χρήστες χρησιμοποιούν ένα σύστημα, τόσο καλύτερα μαθαίνουν τις αδυναμίες του. Επομένως, οι κακόβουλες βλέψεις των εσωτερικών χρηστών του συστήματος αποτελούν τον μεγαλύτερο κίνδυνο [6]. Το μοντέλο της μηδενικής εμπιστοσύνης  δημιουργήθηκε προκειμένου να μπορέσουν να αντιμετωπιστούν τέτοιου είδους προκλήσεις, όπως είναι οι πλευρικές επιθέσεις (lateral attacks) και επιπλέον να συμβάλλει στην αντιμετώπιση των παραβιάσεων δεδομένων (data breaches). Άλλωστε οι παραβιάσεις δεδομένων ολοένα και αυξάνονται, λόγω των συνθηκών της εποχής και πιο συγκεκριμένα της κυριαρχίας του cloud, το οποίο τις κάνει πιο εύκολες [5], [8].

A table of security codes

AI-generated content may be incorrect.

***Εικόνα 1****. Παραδοσιακό vs Zero Trust Μοντέλο Ασφάλειας*

Η τεχνική της μηδενικής εμπιστοσύνης  έχει ως σκοπό να παρέχει προστασία στους πέντε βασικούς πυλώνες ενός πληροφοριακού συστήματος, δηλαδή τους χρήστες (identity), τις συσκευές (devices), τα δίκτυα (networks), τα δεδομένα (data) και τις εφαρμογές και εργασίες (applications and workloads). Οι πέντε αυτοί άξονες συνιστούν τα θεμελιώδη σημεία ελέγχου και προστασίας, στα οποία πρέπει να εφαρμόζονται πολιτικές ασφάλειας, ώστε να διασφαλιστεί η ακεραιότητα και η ανθεκτικότητα του συστήματος. Επιπροσθέτως, όπως έχει προταθεί από τον Εθνικό Οργανισμό Προτύπων και Τεχνολογίας των Ηνωμένων Πολιτειών (NIST), το μοντέλο της μηδενικής εμπιστοσύνης  στηρίζεται σε ορισμένες βασικές αρχές: την επαλήθευση ταυτότητας (identity verification) και την συνεχής επιβεβαίωση και επιτήρηση (continuous verification and monitoring), το ελάχιστο απαραίτητο προνόμιο (least privilege access) και την μικρο-τμηματοποίηση του δικτύου (micro-segmentation), τον έλεγχος με βάση το περιβάλλον (context-aware policies) και την υπόθεση παραβίασης (assume breach) [9], [6], [12].

A diagram of a company

AI-generated content may be incorrect.

***Εικόνα 2:*** *Η διαδικασία ταυτοποίησης και επιβεβαίωσης των χρηστών*

Όσον αφορά την επαλήθευση ταυτότητας αυτή γίνεται όταν κάποιος χρήστης ή συσκευή ζητάει πρόσβαση στους πόρους ενός οργανισμού. Ωστόσο, αυτή είναι μια διαδικασία που δεν περιορίζεται μόνο στην αρχή, συνεχίζεται και κατά τη διάρκεια της χρήσης των πόρων του συστήματος. Αρχικά, γίνεται η αξιολόγηση του αιτήματος πρόσβασης και κρίνεται πόσο επικίνδυνη θεωρείται η παροχή της σε έναν χρήστη ή συσκευή. Εάν κριθεί ότι αυτός πληρεί τα προκαθορισμένα κριτήρια, το αίτημά του ικανοποιείται και του δίνεται πρόσβαση στο δίκτυο του οργανισμού [7]. Αυτή είναι μία διαδικασία για την οποία χρησιμοποιούνται τεχνικές όπως multi-factor authentication (MFA), Security Information and Event Management (SIEM) συστήματα και Endpoint Detection and Response (EDR) [8]. Ωστόσο, από τη στιγμή που δίνεται πρόσβαση σε έναν χρήστη ή μία συσκευή αυτός δεν θεωρείται άξιος εμπιστοσύνης για όσο συνεχίζει να χρησιμοποιεί τους πόρους του δικτύου. Αντιθέτως, εφαρμόζεται μία συνεχής επιβεβαίωση της ταυτότητας του προκειμένου να διασφαλιστεί ότι δεν πρόκειται για κάποιον που μπορεί να αποτελέσει απειλή για το πληροφοριακό σύστημα. Πιο συγκεκριμένα, μόλις παρέλθει ένα εξ’ αρχής ορισμένο χρονικό διάστημα ή παρατηρηθεί κάποια ασυνήθιστη ή περίεργη συμπεριφορά η διαδικασία επαλήθευσης επαναλαμβάνεται, προσπαθώντας βέβαια πάντα να μην επηρεαστεί η απρόσκοπτη χρήση του δικτύου από τον χρήστη [5].

Η τεχνική της μικροτμηματοποίησης περιλαμβάνει την διάσπαση του δικτύου σε μικρότερα τμήματα καθένα από τα οποία έχει τις δικές του πολιτικές προστασίας. Ο σκοπός αυτής της ιδέας και η χρήση της στο ZTA είναι να προσφέρει τον περιορισμό μίας πιθανής επίθεσης στο συγκεκριμένο υποτμήμα του δικτύου, με αποτέλεσμα να μην απειληθεί ολόκληρος ο οργανισμός. Κομβικό σημείο για την ενίσχυση αυτής της ιδέας είναι ότι οι χρήστες και οι συσκευές επιλέγεται να έχουν πρόσβαση μόνο στο τμήμα που τους είναι αναγκαίο για την εκτέλεση των καθηκόντων τους, δηλαδή στους ελάχιστους δυνατούς πόρους. Βέβαια όταν κριθεί αναγκαίο ή ζητηθεί από τους χρήστες αύξηση της περιμέτρου πρόσβασης γίνονται εκ νέου οι απαραίτητοι έλεγχοι, για να επιτραπεί η περιπλάνηση ενός χρήστη μέσα στους κόμβους του δικτύου. Με αυτόν τον τρόπο επιβεβαιώνεται εάν πρέπει να γίνει η παροχή πρόσβασης σε περισσότερους πόρους λόγω αλλαγής των καθηκόντων του και εάν πληρούνται τα προκαθορισμένα κριτήρια ασφαλείας. Όταν επιβεβαιωθούν αυτές οι προϋποθέσεις γίνεται η έγκριση του αιτήματος επέκτασης της ακτίνας πρόσβασης [7], [6], [8].

Μέσα σε ένα δίκτυο κάθε οντότητα είναι δυνητικός κίνδυνος και επομένως, κρίνεται απαραίτητη η συνεχής συλλογή δεδομένων από τα τερματικά σημεία (endpoints) του δικτύου για να διασφαλιστεί η ασφάλεια του πληροφοριακού συστήματος. Αυτή η διαδικασία περιλαμβάνει αρχικά την αξιοποίηση των μηχανισμών ασφαλείας που αναφέρθηκαν, δηλαδή την επαλήθευση ταυτότητας, τη παροχή των ελαχίστων πόρων και επιπλέον την ανάλυση της συμπεριφοράς των χρηστών. Πιο συγκεκριμένα, γίνεται προσπάθεια εύρεσης ανωμαλιών και περίεργης δραστηριότητας, χρησιμοποιώντας αλγόριθμους τεχνητής νοημοσύνης, όπως μοντέλα μηχανικής μάθησης (machine learning models) που εκπαιδεύονται σε φυσιολογική συμπεριφορά χρηστών, το ZTA μπορεί να εντοπίσει περίεργα λογικά μοτίβα στους χρήστες, τα οποία θα μπορούσαν να κριθούν επικύνδυνα [8]. Επιπλέον, στο πλαίσιο της πεποίθησης ότι κάθε χρήστης ή συσκευή θα μπορούσε να είναι εν δυνάμει επικίνδυνος, το μοντέλο ενσωματώνει μηχανισμούς προσαρμοστικότητας και ευελιξίας. Με αυτή την προσθήκη η τεχνική της μηδενικής εμπιστοσύνης  έχει τη δυνατότητα να προσαρμόζεται γρήγορα σε αλλαγές που μπορεί να συμβαίνουν, ανιχνεύοντας απειλές σε πραγματικό χρόνο, ακόμη και εάν αυτές προέρχονται από επιβεβαιωμένους χρήστες του δικτύου. Αυτό συμβαίνει γιατί έχει την δυνατότητα να προσαρμόζεται στις αλλαγές τοποθεσίας, δεδομένων και εργασιών [7].

## 3.2 Αξιολόγηση

Το μοντέλο της μηδενικής εμπιστοσύνης  έχει σαφή πλεονεκτήματα και υπερτερεί έναντι των παραδοσιακών μοντέλων από την άποψη της ασφάλειας που προσφέρει στα πληροφοριακά συστήματα. Πρόκειται για ένα μοντέλο το οποίο μπορεί να σταθεί αντάξιο στις απαιτήσεις ασφαλείας της εποχής, όπου τα δίκτυα είναι αποκεντρωποιημένα και οι χρήστες τους έχουν πρόσβαση σε αυτά από διάφορες περιοχές και συσκευές. Συχνά οι χρήστες βρίσκονται εκτός της περιμέτρου του δικτύου και αυτό δείχνει την υπεροχή του ZTA έναντι στα παραδοσιακά μοντέλα που βασίζονται στην ιδέα της ασφάλειας μέσα στην περίμετρο του δικτύου του οργανισμού. Άλλωστε σήμερα οι εργαζόμενοι δουλεύουν εξ’ αποστάσεως, στα δίκτυα της επιχείρησης χρησιμοποιούνται συσκευές IoT και η χρήση του cloud κυριαρχεί. Όλα αυτά δημιουργούν μια πραγματικότητα που απέχει πολύ από την έννοια της περιμέτρου.

Η μηδενική εμπιστοσύνη στηρίζεται στον διαχωρισμό του δικτύου σε μικρότερα τμήματα και αυτό συμβάλλει σημαντικά στην μείωση των επιθέσεων πλευρικής κίνησης (lateral attacks). Αυτό προσφέρει στο μοντέλο ένα σημαντικό πλεονέκτημα, καθώς περιορίζει τους εισβολείς σε ένα μικρό τμήμα του δικτύου, μειώνοντας σημαντικά τον κίνδυνο των παραβιάσεων ευρείας κλίμακας. Το παρακάτω γράφημα παρουσιάζει τη βελτίωση της ασφάλειας σε διάφορους τομείς, σε σύγκριση με προηγούμενα μοντέλα ασφαλείας  [8].

A graph of blue and green bars

AI-generated content may be incorrect.

***Εικόνα 3:*** *Μείωση περιστατικών ασφαλείας ανά τομέα μετά την εφαρμογή ZTA*

Το νέο αυτό μοντέλο προσφέρει και άλλα ουσιώδη πλεονεκτήματα στην ενίσχυση της ασφάλειας. Οι τεχνικές που χρησιμοποιούνται για την ταυτοποίηση των χρηστών και η συνεχής επιβεβαίωση αυτής της διαδικασίας έχει καταφέρει να συμβάλλει καθοριστικά στη μείωση των επιθέσεων που βασίζονται σε υποκλοπή ή κατάχρηση διαπιστευτηρίων (credential-based attacks) σε ένα μεγάλο ποσοστό που αγγίζει το 40%. Επιπλέον, στο ίδιο πλαίσιο της συνεχής επαλήθευσης και του ελέγχου, καταγράφεται επίσης αξιοσημείωτη μείωση και στις επιθέσεις που προέρχονται από τους χρήστες του δικτύου (insider threats), σε ποσοστό περίπου 30%. Πρόκειται για μία σημαντική επιτυχία του ZTA, καθώς οι εσωτερικές επιθέσεις κλωνίζουν τα πληροφοριακά συστήματα, των οποίων οι χρήστες διαχειρίζονται ευαίσθητα προσωπικά δεδομένα [8]. Στη συνέχεια, παρουσιάζεται μία εικόνα που δείχνει με σαφήνεια τον τρόπο με τον οποίο το μοντέλο ZTA περιορίζει δραστικά τη δυνατότητα ενός εισβολέα να διεισδύσει στο δίκτυο και να περιπλανηθεί ανεμπόδιστα μέσα σε αυτό.

A diagram of a computer system

AI-generated content may be incorrect.

***Εικόνα 4****: Σύγκριση παραδοσιακής ασφάλειας και Zero Trust Architecture*

Πρόκειται για ένα χαρακτηριστικό σενάριο επίθεσης κατά το οποίο ένας κακόβουλος χρήστης  εγκαταθιστά λογισμικό κακόβουλης λειτουργίας (malware) μέσω ενός μηνύματος ηλεκτρονικού ψαρέματος (phishing email) στον υπολογιστή ενός εργαζομένου, ο οποίος εργάζεται εξ’ αποστάσεως. Στα παραδοσιακά μη ασφαλή πλέον μοντέλα αυτό εξαπλώνεται εύκολα σε ολόκληρο το δίκτυο του οργανισμού. Ωστόσο, στο μοντέλο του ZTA, όπου εφαρμόζονται πολυεπίπεδοι μηχανισμοί ασφαλείας, τέτοιου είδους επιθέσεις μπορούν να αποτραπούν αποτελεσματικά και το δίκτυο να συνεχίσει να είναι ασφαλές, παρά την προσπάθεια επίθεσης [13]. Πιο συγκεκριμένα, προσφέρεται προστασία σε κάθε τμήμα και κόμβο του δικτύου, εφαρμόζοντας επιθεώρηση στο έβδομο επίπεδο του προτύπου OSI (Layer 7 inspection). Αυτό σημαίνει ότι γίνεται μία σε βάθος ανάλυση της εισερχόμενης δικτυακής κίνησης με επίκεντρο το περιεχόμενο, εξετάζοντας το είδος των δεδομένων που ανταλλάσσονται, τον σκοπό της επικοινωνίας και τον τρόπο με τον οποίο γίνεται η χρήση των εφαρμογών. Πρόκειται για την επίτευξη εντοπισμού περίπλοκων και πιθανώς δύσκολων στην εύρεση απειλών του επιπέδου εφαρμογής, οι οποίες δεν θα μπορούσαν να βρεθούν με τα παραδοσιακά μοντέλα. Αυτή η αντίθεση προκύπτει από το γεγονός ότι στο παρελθόν οι έλεγχοι εστίαζαν στα χαμηλότερα επίπεδα του μοντέλου OSI και έδιναν έμφαση στην ταυτοποίηση των συμμετεχόντων στην επικοινωνία, όπως για παράδειγμα στις IP διευθύνσεις ή στους αριθμούς των θυρών [14].

Η αρχιτεκτονική της μηδενικής εμπιστοσύνης  προσφέρει τη δυνατότητα παρακολούθησης του δικτύου του οργανισμού με μεγάλη ακρίβεια, μέσω των συνεχών ελέγχων όλων των ενεργειών που πραγματοποιούνται. Αυτό έχει σαν αποτέλεσμα να γνωρίζει ο  οργανισμός ανά πάσα στιγμή ποιος συνδέεται, από ποια τοποθεσία, με ποια συσκευή, τι ενέργειες προσπαθεί να εκτελέσει και ποια δεδομένα προσπελαύνει. Ως αποτέλεσμα μπορεί να εντοπιστεί γρήγορα και αποτελεσματικά πιθανή κακόβουλη συμπεριφορά [13]. Η ενισχυμένη ορατότητα που προσφέρει το ZTA περιλαμβάνει πληροφορίες όχι μόνο σχετικά με απειλές που αφορούν την κίνηση μέσα στο δίκτυο, αλλά και στα ίδια τα δεδομένα και στους τύπους τους. Αυτό αποτελεί ένα πολύ σημαντικό πλεονέκτημα του μοντέλου για τις ομάδες ασφαλείας, καθώς όσο πιο ξεκάθαρη είναι η εικόνα που έχουν για το τι συμβαίνει συνεχώς μέσα στο δίκτυο, τόσο πιο εύκολη και ολοκληρωμένη γίνεται η παροχή ασφάλειας στους χρήστες. Είναι γεγονός ότι τα πληροφοριακά συστήματα πάσχιζαν για αυτήν την παροχή, καθώς η αύξηση των παραβιάσεων των δεδομένων δεν ήταν το μόνο πρόβλημα που έπρεπε να αντιμετωπίσουν, αλλά και η αδυναμία των εταιρειών να τις αντιληφθούν. Αξιοσημείωτη είναι η χρονική διάρκεια των εβδομήντα οκτώ ημερών που χρειάζεται ένας οργανισμός για να αντιληφθεί την παραβίαση, σύμφωνα με σχετικές έρευνες [14].

Ένα επιπλέον σημαντικό πλεονέκτημα της μηδενικής εμπιστοσύνης  είναι τα μειωμένα κόστη που προσφέρει η τεχνική αυτή όταν εφαρμοστεί. Τα παλιά μοντέλα ασφαλείας έχουν κριθεί πλέον μη ασφαλή και αναξιόπιστα και οι επιχειρήσεις καταβάλλουν προσπάθειες για να προστατευθούν. Σε αυτό το πλαίσιο άρχισαν να προσθέτουν δαπανηρούς επιπλέον ελέγχους προκειμένου να καλύψουν τα κενά ασφαλείας, χωρίς ωστόσο να εφαρμόζουν κάποια συγκεκριμένη, ξεκάθαρη και ολοκληρωμένη τακτική. Τα αποτελέσματα αυτού ήταν απογοητευτικά, τα προβλήματα δεν μπόρεσαν να διορθωθούν και οι εταιρείες κατέληξαν να ξοδεύουν υπέρογκα ποσά. Η μηδενική εμπιστοσύνη αντιμετωπίζει αυτό το πρόβλημα του κόστους. Μέσω της τεχνικής της μικρο-τμηματοποίησης που περιλαμβάνει, δίνει τη δυνατότητα εφαρμογής των ελέγχων ασφαλείας σε μία ενιαία συσκευή, αξιοποιώντας πλατφόρμες όπως ένα nGFW (Next-Generation Firewall). Επιπλέον, με αυτόν τον τρόπο μπορεί να επιτευχθεί μία κεντρικοποιημένη διοίκηση, γεγονός που συνεπάγεται μείωση του υλικού εξοπλισμού (hardware) και των υποδομών που απαιτούνται και άρα την μείωση των εξόδων. Κατά συνέπεια, εξοικονομείται χρόνος για τις ομάδες ασφαλείας, αφού η συγχώνευση μειώνει την πολυπλοκότητα και καθιστά τη διαχείριση του δικτύου πιο εύκολη, δίνοντας τους τη δυνατότητα να επικεντρωθούν σε πιο σύνθετες και στρατηγικής σημασίας εργασίες [14].

Η μηδενική εμπιστοσύνη έχει ανταγωνιστικό πλεονέκτημα όσον αφορά τις απαιτήσεις συμμόρφωσης στους νόμους. Η τεχνική της μικρο-τμηματοποίησης του δικτύου είναι η πηγή αυτού. Επειδή το δίκτυο χωρίζεται σε μικρότερα τμήματα καθένα από αυτά θα πρέπει να υπακούει στους ανάλογους νόμους και αυτό κάνει το δίκτυο πιο διαχειρίσιμο, λιγότερο περίπλοκο και άρα θα μπορέσει να συμμορφωθεί πιο εύκολα στην εκάστοτε κανονιστική απαίτηση [14]. Άλλωστε, οι αλλαγές στους νόμους που έχουν γίνει τα τελευταία χρόνια δείχνουν ότι η αρχιτεκτονική zero trust είναι μονόδρομος [9].

Η εφαρμογή του μοντέλου μηδενικής εμπιστοσύνης (Zero Trust) συμβάλλει όχι μόνο στην ενίσχυση της ασφάλειας ενός πληροφοριακού συστήματος, αλλά και στη βελτίωση της συνεργασίας μεταξύ των ομάδων που το υποστηρίζουν. Η ασφάλεια αντιμετωπίζεται με ενιαίο τρόπο, απαιτώντας μία ενοποιημένη και διαρκή εφαρμογή των πολιτικών ασφαλείας σε όλα τα επίπεδα του συστήματος, από το επίπεδο δικτύου εώς το επίπεδο εφαρμογών. Επομένως όλες οι ομάδες ενός οργανισμού πρέπει να συνεργαστούν στενά για να επιτευχθεί ο κοινός στόχος της ασφάλειας. Επιπλέον, η αυξημένη ορατότητα που προσφέρει το μοντέλο μειώνει τις συγκρούσεις ανάμεσα στους εργαζομένους που προκύπτουν λόγω του καταμερισμού των ευθυνών. Αυτό οφείλεται στο γεγονός ότι όλες οι ενέργειες εντός του δικτύου είναι πλέον φανερές και η πηγή του εκάστοτε προβλήματος μπορεί να βρεθεί πιο εύκολα [9].

Το μοντέλο της μηδενικής εμπιστοσύνης υπερτερεί σε θέματα ασφάλειας, συμμόρφωσης στους κανονισμούς και διασφαλίζει έναν διαφανή και υγιή συντονισμό του ανθρώπινου δυναμικού. Ωστόσο, παρά την πληθώρα των πλεονεκτημάτων του, η εφαρμογή του συνεπάγεται ορισμένες προκλήσεις. Το βασικότερο πρόβλημα που αντιμετωπίζει το μοντέλο είναι ότι τα συστήματα των οργανισμών χρησιμοποιούσαν μέχρι τώρα τα παραδοσιακά μοντέλα ασφαλείας και η μετάβαση στην ZTA είναι μία διαδικασία περίπλοκη και κοστοβόρα [10]. Οι επιχειρήσεις πρέπει να ακολουθήσουν μια σειρά οργανωμένων και στρατηγικά καθορισμένων βημάτων, με σκοπό να μπορέσουν να εφαρμόσουν την τεχνική αυτή. Πρόκειται για μία διαδικασία τριών σταδίων, η οποία περιλαμβάνει την καταγραφή των πόρων της εταιρίας, την αξιολόγηση του κινδύνου και την τελική εφαρμογή του μοντέλου.

A diagram of a triangle

AI-generated content may be incorrect.

***Εικόνα 5****: Διαδικασία Εφαρμογής του Μοντέλου ZTA*

Το πρώτο στάδιο περιλαμβάνει την λεπτομερή καταγραφή των δομικών στοιχείων της επιχείρησης, στα οποία ανήκουν το ανθρώπινο δυναμικό, ο υλικός εξοπλισμός και το λογισμικό. Σημαντική προσθήκη για την αρχιτεκτονική είναι η προστασία που προσφέρει όταν στο δίκτυο συνδέονται και απομακρυσμένες συσκευές που δεν ανήκουν στην εταιρεία. Ταυτόχρονα, αυτό αποτελεί και μία πρόκληση, καθώς χρειάζεται ένας προσεκτικός χειρισμός προκειμένου να αποφευχθούν προβλήματα ιδιωτικότητας. Η πλήρης κατανόηση των υπάρχοντων πόρων καθιστά δυνατή την ομαλή εφαρμογή της μηδενικής εμπιστοσύνης , αφού τότε θα ξέρει τους τομείς που χρήζουν αυξημένης προστασίας και περαιτέρω ενίσχυσης. Όπως είναι αναμενόμενο, τα κριτήρια πρόσβασης σε κάθε πληροφοριακό πόρο διαφοροποιούνται ανάλογα με τη σημασία και την ευαισθησία του. Ο καθορισμός τους και η επιλογή της ελαστικότητας ή αυστηρότητάς τους, αποτελεί μία αρκετά δύσκολη και δεσμευτική διαδικασία. Πιθανά λάθη σε αυτή θα μπορούσαν να αποβούν μοιραία, όπως είναι η παραχώρηση πρόσβασης σε εν τέλη επικίνδυνους χρήστες, λόγω ελαστικών κριτηρίων ή ο περιορισμός αξιόπιστων χρηστών λόγω πολύ αυστηρών κριτηρίων. Αυτοί οι λόγοι υποδεικνύουν τη σημαντικότητα του πρώτου βήματος. Στο δεύτερο στάδιο της εφαρμογής θα πρέπει να γίνει η αξιολόγηση κινδύνου και ρίσκου. Μία καλή στρατηγική είναι η σταδιακή εφαρμογή της αρχιτεκτονικής σε περιοχές με χαμηλό επίπεδο κινδύνου, γεγονός που μειώνει τις πιθανότητες αποτυχίας και επιτρέπει την ομαλότερη προσαρμογή. Το τρίτο στάδιο είναι η εφαρμογή του μοντέλου, αφού έχει δημιουργηθεί η στρατηγική που θα ακολουθηθεί. Η εταιρεία πρέπει να εφαρμόσει συνεχείς ελέγχους για να διαβεβαιώσει ότι όλα γίνονται σωστά και άρα να ανταπεξέλθει σε τυχόν προβλήματα που μπορεί να δημιουργηθούν [16]. Επομένως, πρόκειται για μία διαδικασία χρονοβόρα και δύσκολη, με αποτέλεσμα οι υπάλληλοι των εταιρειών συχνά να είναι αντίθετοι με την υιοθέτησή της, αφού είναι πιθανό να μην θέλουν να αντιμετωπίσουν τις προκλήσεις που ελλοχεύουν και να μην είναι εξοικειωμένοι με τα τεχνικά χαρακτηριστικά του μοντέλου [8].

Ακόμη και με την εφαρμογή της κατάλληλης στρατηγικής, η εφαρμογή του μοντέλου είναι μία δύσκολη διαδικασία. Αυτό οφείλεται στο γεγονός ότι πρόκειται για μία σχετικά νέα και εξελισσόμενη τεχνολογία, η οποία δεν διατίθεται ακόμη ως πλήρης και ολοκληρωμένη λύση από κάποιον ενιαίο προμηθευτή. Η χρήση διαφορετικών προμηθευτών οδηγεί σε πιθανά προβλήματα στη συμβατότητα ανάμεσά τους, γεγονός που καθιστά την τεχνική δύσχρηστη. Επιπλέον, ενέχει τον κίνδυνο, η διαδικασία αλλαγής παρόχου να είναι σύνθετη και χρονοβόρα σε περίπτωση δυσαρέσκειας ή μεταβαλλόμενων επιχειρησιακών αναγκών [16].

Όσον αφορά την εμπειρία των τελικών χρηστών, η υιοθέτηση του μοντέλου μηδενικής εμπιστοσύνης ενδέχεται να προκαλέσει ορισμένες καθυστερήσεις στη λειτουργία των συστημάτων. Η αρχιτεκτονική απαιτεί συνεχή επαλήθευση της ταυτότητας των χρηστών, αλλά και ανάλυση της δραστηριότητας εντός του δικτύου. Αυτή η διαδικασία της αδιάκοπης παρακολούθησης και καταγραφής (logging) των όσων συμβαίνουν, αναμένεται να προκαλέσει ορισμένες καθυστερήσεις στην απόκριση του συστήματος, οι οποίες μπορούν να γίνουν αντιληπτές από τους χρήστες κατά τη χρήση των πόρων του οργανισμού [15]. Επιπλέον, η συνεχής καταγραφή εκτός από το αντίκτυπο στον χρόνο, ενέχει και κινδύνους σχετικά με την διασφάλιση των προσωπικών δεδομένων των χρηστών. Από την μία πλευρά ο συνεχής έλεγχος  ενισχύει σημαντικά την ασφάλεια εντός του δικτύου, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση και τις επιθέσεις. Από την άλλη πλευρά ο όγκος αυτών των δεδομένων που παράγεται και παρακολουθείται, περιέχει προσωπικά δεδομένα. Επομένως, υπάρχει περίπτωση αυτά να χρησιμοποιηθούν με κακόβουλες προθέσεις, απαιτώντας επίλυση των ζητημάτων ιδιωτικότητας και ασφάλειας που προκύπτουν, μέσω ισχυρών μηχανισμών ασφαλείας [17].

# 4) Μελέτη Περίπτωσης

## Εισαγωγή

Οποιοδήποτε επιχειρησιακό περιβάλλον μπορεί να σχεδιαστεί με γνώμονα τις αρχές της μηδενικής εμπιστοσύνης. Η ιδέα του Zero Trust δεν είναι πολύ καινούρια, ωστόσο η εφαρμογή της σε τεχνολογικό επίπεδο βρίσκεται ακόμη σε πολύ αρχικό στάδιο. Δεν είναι ιδιαίτερα πολλές οι περιπτώσεις χρήσης, αλλά ορισμένες ενδεικτικές αναφέρονται στη βιβλιογραφία και αφορούν:

* Προστασία Εσωτερικού Δικτύου σε Νοσοκομεία
* Υποδομή DevOps Πλατφόρμας SaaS
* Προστασία Τηλεργασίας σε Πολυεθνική Επιχείριση Τραπεζικών Υπηρεσιών

## 4.1 Μελέτη Περίπτωσης – Προστασία Εσωτερικού Δικτύου σε Νοσοκομεία

Τα νοσοκομειακά πληροφοριακά συστήματα στα οποία υπάρχουν γνωστές εφαρμογές του zero trust αφορούν:

* Ηλεκτρονικό Φάκελο Ασθενών (EHR)
* PACS (Απεικονιστικά Συστήματα/ Ακτινολογικά Δεδεομένα)
* ERP/ HRM/ Σύστημα Προμηθειών
* Εσωτερικό δίκτυο με VLANs, servers on-prem & private cloud

Υπάρχει ένα πλήθος χαρακτηριστικών επιθέσεων που έδειξαν ότι είναι επιτακτική ανάγκη η εφαρμογή του μοντέλου ZTA στα νοκομεία. Αρχικά, η επίθεση ransomware Conti στο Health Service Executive (HSE) της Ιρλανδίας το 2021, η οποία οδήγησε στην κρυπτογράφηση περίπου του 80% των δεδομένων του οργανισμού και στην αναστολή κρίσιμων υπηρεσιών [33]. Αντίστοιχα, περιστατικά είναι η διαρροή δεδομένων τριών εκατομμυρίων ατόμων μέσω της παραβίασης της NationsBenefits το 2023 [34], καθώς και το περιστατικό της Medibank στην Αυστραλία το 2022 [35]. Ένα ακόμη παράδειγμα, αποτελεί μεγάλο πανεπιστημιακό νοσοκομείο στην Ευρώπη, το οποίο υπέστη απόπειρα ransomware επίθεσης, μέσω phishing email που απέκτησε πρόσβαση σε ένα endpoint υπολογιστή νοσηλευτή, το 2022. Οι χρήστες πατώντας σύνδεσμο στο email τους, εκτέλεσαν κακόβουλο λογισμικό (dropper). Ο επιτιθέμενος απόκτησε πρόσβαση στο domain account (με δικαιώματα shared folder στο EHR) και στη συνέχεια υπήρξε σωρεία παραβιάσεων στα παραπάνω συστήματα [56].

Η εφαρμογή του Zero Trust αναφέρεται σε:

i. Micro-segmentation, όπου το δίκτυο χωρίζεται σε μικρότερα τμήματα (π.χ.εργαστηριακό, φαρμακευτικό, διοικητικό) και η πρόσβαση από κάθε endpoint περιορίστηκε με firewall policies μεταξύ VLANs [36].

ii. Identity-Aware Access Control, όλοι οι υπάλληλοι υποχρεώνονται να κάνουν login μέσω SSO με MFA (Multi-Factor Authentication) χρησιμοποιώντας το Microsoft Azure AD. Εφαρμόζοντας Conditional Access Policy, που ανάλογα με το ρίσκο, τη συσκευή και γεωγραφική θέση, η πρόσβαση επιτρέπεται ή απορρίπτεται [37].

iii. Endpoint Detection & Response (EDR), με την εγκατάσταση του CrowdStrike Falcon σε κάθε endpoint με real-time detection και απομόνωση compromised endpoints [38].

Περιπτώσεις νοσοκομείων που έχει εφαρμοστεί Zero Trust προσέγγιση είναι τα:

* Dayton Children’s Hospital (ΗΠΑ), το νοσοκομείο αυτό εφάρμοσε αρχιτεκτονική Zero Trust χρησιμοποιώντας λύσεις της Cisco και της Ordr για την προστασία της υποδομής του. Μέσω της μικρο-τμηματοποίησης (microsegmentation), κατάφερε να απομονώσει κρίσιμα συστήματα και να αποτρέψει μη εξουσιοδοτημένη πρόσβαση, ενισχύοντας την ασφάλεια των δεδομένων των ασθενών [39].
* Ανώτατο Πανεπιστημιακό Νοσοκομείο στις Ηνωμένες Πολιτείες, ένα από τα κορυφαία 10 νοσοκομεία στις ΗΠΑ συνεργάστηκε με την Lookout για την εφαρμογή λύσεων Zero Trust, διασφαλίζοντας την προστασία ευαίσθητων δεδομένων στο cloud και τη συμμόρφωση με κανονισμούς [40].
* Μεγάλο Παιδιατρικό Νοσοκομείο στις ΗΠΑ, συνεργάστηκε με την ColorTokens για την εφαρμογή της πλατφόρμας Xtended Zero Trust. Μέσα σε τέσσερις εβδομάδες, κατάφερε να εντοπίσει μη εξουσιοδοτημένη κίνηση, να αυτοματοποιήσει την ταξινόμηση περιουσιακών στοιχείων και να εφαρμόσει πολιτικές ασφαλείας με ελάχιστη επίδραση στην απόδοση των εφαρμογών [41].

## 4.2 Μελέτη Περίπτωσης – Υποδομή DevOps Πλατφόρμας SaaS

Μια startup SaaS που προσφέρει B2B λύσεις φιλοξενίας API υπέστη παραβίαση λόγω ανεπαρκών ελέγχων πρόσβασης στους cloud-based CI/CD pipelines. Η εφαρμογή της Zero Trust περιλαμβάνει:

* IAM Policies στον Cloud Provider (π.χ. AWS), όπου όλοι οι πόροι (Lambda, S3, EC2) ρυθμίζονται με least privilege IAM roles. Δυνατή, επίσης, είναι η εφαρμόγη του Zero Trust network access (ZTNA) με χρήση AWS PrivateLink και Identity Center [42].
* Zero Trust στα CI/CD Pipelines (GitLab), με pipelines να εκτελούνται σε self-hosted runners σε isolated subnets, όπου απαιτείται certificate-based mutual TLS. Τα secrets και credentials αποθηκεύονται σε HashiCorp Vault με ροή access μέσω dynamic tokens [43].
* Just-In-Time Access, οι διαχειριστές DevOps λαμβάνουν περιορισμένη, προσωρινή πρόσβαση μέσω Access Management Portal (π.χ. Teleport) με πλήρες audit logging [44].

Επιτυγχάνεται δραστική μείωση επιφανείας επίθεσης στον CI/CD κύκλο, απόκρυψη εσωτερικών APIs από το δημόσιο διαδίκτυο και κεντρικός έλεγχος και logging προσβάσεων.

Περιπτώσεις εφαρμογής είναι:

* Η GitLab έχει ενσωματώσει αρχές Zero Trust στο DevOps pipeline της, εφαρμόζοντας αυστηρή ταυτοποίηση, έλεγχο πρόσβασης και συνεχή παρακολούθηση για την προστασία των πόρων της [45].
* Η Microsoft που παρέχει οδηγίες για την εφαρμογή του Zero Trust σε περιβάλλοντα DevOps, εστιάζοντας στην αρχή της ελάχιστης προνομιακής πρόσβασης και στην ασφάλεια των πλατφορμών ανάπτυξης [46].
* Η Akamai εφάρμοσε ένα μοντέλο Zero Trust χωρίς τη χρήση VPN, προστατεύοντας τις εφαρμογές και τα δεδομένα της, μέσω ταυτοποίησης και εξουσιοδότησης σε επίπεδο εφαρμογής [47].
* Η FinTech, μια κορυφαία εταιρεία χρηματο-οικονομικής τεχνολογίας υιοθέτησε μοντέλο Zero Trust στο DevSecOps pipeline της, ενσωματώνοντας MFA, υπογεγραμμένα commits και συνεχή παρακολούθηση για την ενίσχυση της ασφάλειας [48].
* Η Accenture εφάρμοσε στρατηγική Zero Trust στο cloud, επικεντρώνοντας την ασφάλεια στην ταυτότητα και την πρόσβαση, ενσωματώνοντας πολιτικές και τεχνολογίες για την προστασία των υπηρεσιών και των δεδομένων της [49].

## 4.3 Μελέτη Περίπτωσης – Προστασία Τηλεργασίας σε Πολυεθνική Επιχείρηση Τραπεζικών Υπηρεσιών

Μετά την περίοδο του COVID-19, που οδήγησε στην ραγδαία αύξηση της τηλεργασίας, πολλές - κυρίως πολυεθνικές- τράπεζες έπρεπε να επιτρέψουν την απομακρυσμένη πρόσβαση του προσωπικού και των υπαλλήλων με ασφάλεια και συμμόρφωση (PCI DSS, GDPR).

Εφάρμοσαν Zero Trust προσέγγιση με χρήση:

* ZTNA αντί για VPN, καταργώντας την παραδοσιακή VPN πρόσβαση. Η λύση ZTNA (π.χ. Zscaler Private Access - ZPA) συνδέει τους χρήστες μόνο με συγκεκριμένες εφαρμογές και όχι με το δίκτυο [50].
* Ενσωμάτωση User and Entity Behavior Analytics (Behavioral Analytics με UEBA) που παρακολουθεί πρότυπα συμπεριφοράς (π.χ. ξαφνική πρόσβαση από νέα χώρα, αύξηση αριθμού queries σε DBs) χρησιμοποιώντας alerting και auto-block μέσω AI-based ανάλυσης συμπεριφοράς [51].
* Device Posture Checks, όπου πριν την πρόσβαση σε κρίσιμες εφαρμογές, κάθε endpoint ελέγχεται για ενεργοποιημένο antivirus, ενημερωμένο λειτουργικό, κρυπτογράφηση δίσκου (BitLocker), κ.α. [52]

Επιτυγχάνουν συνεχής αξιολόγηση κινδύνου με μηδενική εμπιστοσύνη, δυνατότητα καταγραφής και forensic ανάλυσης ύποπτων ενεργειών και πλήρης συμβατότητα με ρυθμιστικά πρότυπα (SOX, PCI, ISO 27001).

Παραδείγματα Τραπεζών με Εφαρμογή Zero Trust στην Τηλεργασία είναι:

* Η DZ BANK που υιοθέτησε στρατηγική Zero Trust με επίκεντρο τη Διαχείριση Προνομιακής Πρόσβασης (Privileged Access Management) μέσω της πλατφόρμας Identity Security της CyberArk. Αυτό επέτρεψε την ασφαλή απομακρυσμένη πρόσβαση, τη συμμόρφωση με κανονισμούς και τη μείωση των κυβερνοκινδύνων [53].
* Η D Commerce Bank, η οποία υλοποίησε αρχιτεκτονική Zero Trust χρησιμοποιώντας τα ML-Powered Next-Generation Firewalls της Palo Alto Networks. Αυτό επέτρεψε την πλήρη ορατότητα και προστασία του εταιρικού δικτύου, με μείωση των ειδοποιήσεων ασφαλείας κατά 50% και συνεχή επιθεώρηση της κίνησης δικτύου [54].
* Η African Bank εφαρμόζοντας στρατηγική Zero Trust Access με ενσωματωμένη αρχιτεκτονική SD-WAN μέσω της Fortinet. Αυτό επέτρεψε την ασφαλή απομακρυσμένη πρόσβαση, την προστασία των υποκαταστημάτων και τη συμμόρφωση με απαιτήσεις, όπως το SWIFT Customer Security Programme [55].

# 5) Μελλοντικές Προτάσεις

Το μοντέλο της αρχιτεκτονικής μηδενικής εμπιστοσύνης υπερτερεί σημαντικά έναντι στα παραδοσιακά μοντέλα, ωστόσο δεν παύει να είναι μία νέα τεχνική που χρήζει βελτιώσεις. Το κρίσιμο ζήτημα, με το οποίο θα πρέπει να ασχοληθούμε είναι ότι για να συνεχίσει το μοντέλο να είναι ανταγωνιστικό απέναντι σε διαρκώς αυξανόμενες και πολύπλοκες απειλές, κρίνεται αναγκαία η ενσωμάτωση τεχνολογιών που θα αναβαθμίσουν τις δυνατότητές του, στον εντοπισμό των κινδύνων και στην συνεχή και σε πραγματικό χρόνο επαλήθευση ταυτότητας [8]. Επομένως, το επόμενο βήμα είναι η εφαρμογή των ιδεών της τεχνικής αυτής σε σύγχρονους και ταχέως αναπτυσσόμενους τομείς ενδιαφέροντος, όπως είναι η τεχνητή νοημοσύνη και η μηχανική μάθηση. Αυτές οι τεχνολογίες μπορούν να αξιοποιηθούν για να ενισχύσουν το Zero Trust και ταυτόχρονα η ενσωμάτωση της αρχιτεκτονικής στις τεχνολογίες αυτές είναι εξίσου αναγκαία, ώστε να διασφαλίζεται η ασφάλεια και η αξιοπιστία τους [5]. Στη συνέχεια παρουσιάζονται αναλυτικά οι τομείς στους οποίους θα πρέπει να εφαρμοστεί η μηδενική εμπιστοσύνη:

* **Τεχνητή Νοημοσύνη και Μηχανική Μάθηση:** Οι τεχνικές αυτές αναμένεται να επηρεάσουν σημαντικά το μοντέλο της μηδενικής εμπιστοσύνης, ενισχύοντας την ασφάλεια, καθώς προσφέρουν αυτοματοποίηση στον τρόπο υλοποίησης των ιδεών της ZTA. Ιδιαίτερα στο πεδίο των συστημάτων SIEM (Security Information and Event Management), η ενσωμάτωση τεχνικών AI, μπορεί να εντοπίσει τις λεπτές αποκλίσεις ανάμεσα σε μία φυσιολογική συμπεριφορά χρήστη και σε μία περίεργη συμπεριφορά. Οι διαφορές αυτές ενδέχεται να αποτελούν πρώιμες ενδείξεις κακόβουλης δραστηριότητας, που συχνά δεν είναι ανιχνεύσιμες από τις παραδοσιακές μεθόδους ή την ανθρώπινη παρατήρηση. Η μηχανική μάθηση χρησιμοποιείται στην εκπαίδευση των συστημάτων για την ανίχνευση αυτών των αποκλίσεων προσφέροντας τη δυνατότητα πρόβλεψης και έγκαιρης απόκρισης σε εν δυνάμει απειλές. Η μελλοντική έρευνα πρέπει να εστιάσει στη βελτιστοποίηση των αλγορίθμων που χρησιμοποιούνται, στοχεύοντας στην ελαχιστοποίηση των πιθανοτήτων σφάλματός και αυξάνοντας την ακρίβεια. Επίσης, στο πεδίο της Διαχείρισης Ταυτότητας και Πρόσβασης (Identity and Access Management - IAM), η τεχνητή νοημοσύνη μπορεί να βελτιώσει τους συνεχείς ελέγχους του μοντέλου, εκτελώντας δυναμική αξιολόγηση του κινδύνου σε πραγματικό χρόνο, με βάση τα χαρακτηριστικά του κάθε χρήστη που προσπαθεί να αποκτήσει πρόσβαση στους πόρους του οργανισμού. Πιο συγκεκριμένα, βασίζεται σε παράγοντες όπως είναι η τοποθεσία, το είδος της συσκευή, το ιστορικό χρήστη κοκ. Μία επιπλέον ιδέα στην οποία θα μπορούσαν να αξιοποιηθούν οι μηχανισμοί αυτοί είναι για την προστασία των IoT συσκευών και του δικτύου του οργανισμού, εκπαιδεύοντας τα μοντέλα μηχανικής μάθησης στην φυσιολογική συμπεριφορά των IoT συσκευών [8].
* **Blockchain and Internet of Things (IoT):** Η τεχνολογία blockchain μπορεί να αξιοποιηθεί συμπληρωματικά προς την αρχιτεκτονική μηδενικής εμπιστοσύνης, με σκοπό την ενίσχυση της προστασίας σε κάθε συναλλαγή και κόμβο του συστήματος [5]. Άλλωστε, η  φύση του ταιριάζει απόλυτα στο zero trust, καθώς το blockchain είναι αποκεντροποιημένο  και περιλαμβάνει την λογική της συνεχής καταγραφής (logging) των όσων συμβαίνουν. Επομένως, μπορεί να ενσωματωθεί μέσα στο μοντέλο υλοποιώντας την διαφανή καταγραφή κάθε ενέργειας και πρόσβασης. Η μελλοντική έρευνα πρέπει να εστιάσει στην εφαρμογή του συνδυασμού των δύο σε τομείς διαχείρισης ευαίσθητων δεδομένων. Ωστόσο, η πρακτική εφαρμογή του συνδυασμού τους στον τομέα των επιχειρήσεων αντιμετωπίζει προκλήσεις, λόγω της αυξημένης κατανάλωσης ενέργειας και των καθυστερήσεων που επιφέρει η επεξεργασία των συναλλαγών στο blockchain. Είναι σημαντικό η μελλοντική δουλειά να στοχεύσει στην εύρεση βιώσιμων και αποδοτικών λύσεων στην εφαρμογή του συνδυασμού τους σε αυτόν τον τομέα [8]. Επιπλέον, έχουν προταθεί ιδέες που υιοθετούν την ενσωμάτωση του blockchain και του zero trust στη διαδικασία αυθεντικοποίησης των συσκευών Internet of Things (IoT), με χαρακτηριστικό παράδειγμα την πρόταση BasIoT [15]. Αλλά το πεδίο παραμένει ανοιχτό για μελλοντικές βελτιώσεις και έρευνα που προσφέρουν προστασία στις συσκευές IoT που άλλοτε ήταν ανασφαλείς, λόγω των ελλειπών μέτρων ασφαλείας τους. Το ZTA μπορεί να εξαλείψει τις απειλές που δημιουργεί η χρήση τους στα πληροφοριακά συστήματα, ιδίως με την εφαρμογή της τεχνικής της μικρο-τμηματοποίησης, καθώς με αυτή καταφέρνει να τις περιορίσει προστατεύοντας το υπόλοιπο δίκτυο. Μία σημαντική κατεύθυνση για μελλοντική έρευνα, θα ήταν η όλη διαδικασία να γίνει δυναμική [8].
* **Containers και μικρο-υπηρεσίες (microservices):** Οι μικρο-υπηρεσίες πρέπει να αρχίσουν να χρησιμοποιούν το ZTA, καθώς στο πλαίσιο λειτουργίας του, όπως αυτό έχει διαμορφωθεί μέχρι σήμερα, εξαρτώνται σε μεγάλο βαθμό από πόρους ή συναρτήσεις από άλλες υπηρεσίες. Επομένως, η βελτίωση της λειτουργίας τους αποτελεί ανοιχτό πεδίο έρευνας, δεδομένου ότι το ZTA θα μπορούσε να προσφέρει λύση στα προβλήματα αποδοτικότητας που αντιμετωπίζουν, εφαρμόζοντας  δυναμική αξιολόγηση πρόσβασης, δίνοντας σε κάθε υπηρεσία ακριβώς τα δικαιώματα που χρειάζεται, τη στιγμή που τα χρειάζεται [5].
* **Βιώσιμα Συστήματα Νεφών (Cloud):** Το μοντέλο ZTA παρέχει πρόσβαση μόνο στους απαραίτητους πόρους, με αποτέλεσμα να μειώνεται η άσκοπη χρήση υπολογιστικής ισχύος και bandwidth. Επομένως, το μοντέλο πετυχαίνει μειωμένη ενεργειακή κατανάλωση, παρέχοντας ταυτόχρονα τη μέγιστη ασφάλεια. Αυτό θα μπορούσε να αποτελέσει τη βάση για τη σχεδίαση των μελλοντικών βιώσιμων δικτύων, αφού οι πυλώνες αυτών, είναι η υψηλή ασφάλεια και η αποδοτική χρήση πόρων, όπως η ηλεκτρική ενέργεια [5].

# 6) Συμπεράσματα

 Η παρούσα εργασία  εξετάζει τη λειτουργία της αρχιτεκτονικής μηδενικής εμπιστοσύνης (zero trust architecture) και τις διάφορες τεχνολογικές προσεγγίσεις που έχουν προταθεί. Παρουσιάζεται μία εις βάθος ανάλυση του μοντέλου, των πλεονεκτημάτων που προσφέρει  έναντι των παραδοσιακών τεχνικών, αλλά και των δυσκολιών που δημιουργούνται κατά την εφαρμογή του. Βέβαια, παρά τις προκλήσεις που ανακύπτουν, κρίνουμε ότι αποτελεί μία προσέγγιση που αρμόζει στα σύγχρονα συστήματα και δίκτυα. Η εκτίμησή μας βασίστηκε, αφενός στην επιτυχία του μοντέλου να εξαλείψει τους κινδύνους που τα παραδοσιακά μοντέλα δεν μπόρεσαν να αντιμετωπίσουν, και αφετέρου στην πεποίθηση ότι με την περαιτέρω ωρίμανση της ιδέας θα γίνουν οι απαραίτητες βελτιώσεις και το μοντέλο θα είναι πλέον πιο ολοκληρωμένο και εύκολο στην εφαρμογή. Συνοψίζοντας, και με βάση την ανάλυση που πραγματοποιήθηκε, καταλήγουμε στο συμπέρασμα ότι πρόκειται για μία ιδέα που παρότι βρίσκεται ακόμη σε φάση εξέλιξης και αναβάθμισης, αναμένεται να κυριαρχήσει στον χώρο της ασφάλειας των πληροφοριακών συστημάτων, καθώς αντιμετωπίζει με επιτυχία τα προβλήματα που πλήττουν τις εταιρείες.

# Βιβλιογραφία- Αναφορές

[1] “zero\_trust\_maturity\_model\_v2\_508.” Accessed: May 04, 2025. [Online]. Available: <https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf>

[2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” National Institute of Standards and Technology, Aug. 2020. doi: [10.6028/NIST.SP.800-207](https://doi.org/10.6028/NIST.SP.800-207).

[3] “Cost of a data breach 2024 | IBM.” Accessed: May 04, 2025. [Online]. Available: <https://www.ibm.com/reports/data-breach>

[4] newsroom, “2024 Cisco Cybersecurity Readiness Index.” Accessed: May 04, 2025. [Online]. Available: <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m03/cybersecurity-readiness-index-2024.html>

[5] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, “Security of Zero Trust Networks in Cloud Computing: A Comparative Review,” *Sustainability*, vol. 14, no. 18, Art. no. 18, Jan. 2022, doi: [10.3390/su141811213](https://doi.org/10.3390/su141811213).

[6] “Zero Trust Architecture: Trend and Impact on Information Security,” ResearchGate. Accessed: May 04, 2025. [Online]. Available: <https://www.researchgate.net/publication/361758378_Zero_Trust_Architecture_Trend_and_Impact_on_Information_Security>

[7] “What is Zero Trust? - Guide to Zero Trust Security | CrowdStrike,” CrowdStrike.com. Accessed: May 04, 2025. [Online]. Available: <https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/>

[8] M. Hasan, “Enhancing Enterprise Security with Zero Trust Architecture,” Oct. 23, 2024, *arXiv*: arXiv:2410.18291. doi: [10.48550/arXiv.2410.18291](https://doi.org/10.48550/arXiv.2410.18291).

[9] “What Is Zero Trust? | IBM.” Accessed: May 04, 2025. [Online]. Available: <https://www.ibm.com/think/topics/zero-trust>

[10] “A Survey on Zero Trust Architecture: Challenges and Future Trends,” ResearchGate. Accessed: May 04, 2025. [Online]. Available: <https://www.researchgate.net/publication/361335518_A_Survey_on_Zero_Trust_Architecture_Challenges_and_Future_Trends>

[11] “Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities,” ResearchGate. Accessed: May 04, 2025. [Online]. Available: <https://www.researchgate.net/publication/378177918_Zero_Trust_Architecture_in_Cloud_Networks_Application_Challenges_and_Future_Opportunities>

[12] “A Survey on Zero Trust Architecture: Challenges and Future Trends,” ResearchGate. Accessed: May 04, 2025. [Online]. Available: <https://www.researchgate.net/publication/361335518_A_Survey_on_Zero_Trust_Architecture_Challenges_and_Future_Trends>

[13] “An analysis of zero-trust architecture and its cost-effectiveness for organizational security,” ResearchGate. Accessed: May 04, 2025. [Online]. Available: <https://www.researchgate.net/publication/363374198_An_analysis_of_zero-trust_architecture_and_its_cost-effectiveness_for_organizational_security>

[14] C. Cunningham, D. Holmes, and J. Pollard, “The Eight Business And Security Benefits Of Zero Trust,” 2019.

[15] S. Li, M. Iqbal, and N. Saxena, “Future Industry Internet of Things with Zero-trust Security,” *Information Systems Frontiers*, vol. 26, no. 5, pp. 1653–1666, Mar. 2022, doi: [10.1007/s10796-021-10199-5](https://doi.org/10.1007/s10796-021-10199-5).

[16] S. Teerakanok, T. Uehara, and A. Inomata, “Migrating to Zero Trust Architecture: Reviews and Challenges,” *Security and Communication Networks*, vol. 2021, no. 1, p. 9947347, 2021, doi: [10.1155/2021/9947347](https://doi.org/10.1155/2021/9947347).

[17] “Zero Trust: Applications, Challenges, and Opportunities,” ResearchGate. Accessed: May 04, 2025. [Online]. Available: <https://www.researchgate.net/publication/373753509_Zero_Trust_Applications_Challenges_and_Opportunities>

[18] J. Kindervag, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture,” 2010.

[19] “Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication,” ResearchGate. Accessed: May 04, 2025. [Online]. Available: <https://www.researchgate.net/publication/311920171_Implementing_Zero_Trust_Cloud_Networks_with_Transport_Access_Control_and_First_Packet_Authentication>

[20] “Zero Trust Architecture,” ResearchGate. Accessed: May 04, 2025. [Online]. Available: <https://www.researchgate.net/publication/339242127_Zero_Trust_Architecture>

[21] M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, “Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology,” *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, p. 256, Oct. 2020, doi: [10.1186/s12911-020-01275-y](https://doi.org/10.1186/s12911-020-01275-y).

[22] C. de Weever and M. Andreou, “Zero Trust Network Security Model in containerized environments,” 2020. Accessed: May 04, 2025. [Online]. Available: <https://www.semanticscholar.org/paper/Zero-Trust-Network-Security-Model-in-containerized-Weever-Andreou/5d2b02e5d079886c44d624752accc20b064e5a15>

[23] “Intelligent Zero Trust Architecture for 5G/6G Tactical Networks: Principles, Challenges, and the Role of Machine Learning,” ResearchGate. Accessed: May 04, 2025. [Online]. Available: <https://www.researchgate.net/publication/351342318_Intelligent_Zero_Trust_Architecture_for_5G6G_Tactical_Networks_Principles_Challenges_and_the_Role_of_Machine_Learning>

[24] “A zero trust method based on BLP and BIBA model,” ResearchGate. Accessed: May 04, 2025. [Online]. Available: <https://www.researchgate.net/publication/357976953_A_zero_trust_method_based_on_BLP_and_BIBA_model>

[25] Ghate N., Mitani S., Singh T., and Ueda H., “Advanced Zero Trust Architecture for automating fine-grained access control with generalized attribute relation extraction,” *IEICE Proceedings Series*, vol. 68, no. C1-5, Dec. 2021, Accessed: May 04, 2025. [Online]. Available: <https://www.ieice.org/publications/proceedings/summary.php?iconf=ICETC&session_num=C1&number=C1-5&year=2021>

[26] M. L. Gambo and A. Almulhem, “Zero Trust Architecture: A Systematic Literature Review,” Mar. 21, 2025, *arXiv*: arXiv:2503.11659. doi: [10.48550/arXiv.2503.11659](https://doi.org/10.48550/arXiv.2503.11659).

[27] M. Nasiruzzaman, M. Ali, I. Salam, and M. H. Miraz, “The Evolution of Zero Trust Architecture (ZTA) from Concept to Implementation,” in *2025 29th International Conference on Information Technology (IT)*, Feb. 2025, pp. 1–8. doi: [10.1109/IT64745.2025.10930254](https://doi.org/10.1109/IT64745.2025.10930254).

[28] T. W. House, “Executive Order on Improving the Nation’s Cybersecurity,” The White House. Accessed: May 04, 2025. [Online]. Available: <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

[29] “Zero Trust Maturity Model | CISA.” Accessed: May 04, 2025. [Online]. Available: <https://www.cisa.gov/zero-trust-maturity-model>

[30] “BeyondCorp Zero Trust Enterprise Security,” Google Cloud. Accessed: May 04, 2025. [Online]. Available: <https://cloud.google.com/beyondcorp>

[31] msmbaldwin, “Zero Trust security in Azure.” Accessed: May 04, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/azure/security/fundamentals/zero-trust>

[32] “Zero Trust Security Solutions | IBM.” Accessed: May 04, 2025. [Online]. Available: <https://www.ibm.com/zero-trust>

[33] S. Alder, “HC3: Lessons Learned from the Ransomware Attack on Ireland’s Health Service Executive,” The HIPAA Journal. Accessed: May 04, 2025. [Online]. Available: <https://www.hipaajournal.com/hc3-lessons-learned-from-the-ransomware-attack-on-irelands-health-service-executive/>

[34] S. Alder, “NationsBenefits Holdings Confirms 3 Million Record Data Breach,” The HIPAA Journal. Accessed: May 04, 2025. [Online]. Available: <https://www.hipaajournal.com/nationsbenefits-holdings-confirms-3-million-record-data-breach/>

[35] B. Tosif, “Medibank’s Cyber Incident: One of Australia’s most invasive data breach,” Medium. Accessed: May 04, 2025. [Online]. Available: <https://medium.com/@BilalTosif/medibanks-cyber-incident-one-of-australia-s-most-invasive-data-breach-a75c3bd54c2c>

[36] [Verify Zero Trust Security Whitepaper - Cisco](https://www.cisco.com/c/en/us/support/docs/security-vpn/security-vpn/218443-verify-zero-trust-security-whitepaper.html)

[37] “What is Conditional Access in Microsoft Entra ID? - Microsoft Entra ID.” Accessed: May 31, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview>

[38] “Secure the Endpoint, Stop the Breach | CrowdStrike Endpoint Security,” CrowdStrike.com. Accessed: May 27, 2025. [Online]. Available: <https://www.crowdstrike.com/en-us/platform/endpoint-security/>

[39] “Dayton Children’s Reduced the Risk of Cyberattacks,” Cisco. Accessed: May 27, 2025. [Online]. Available: <https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/dayton-childrens.html>

[40] “How Lookout Enforces Consistent Policies Across a Hybrid Cloud and Keeps Patient Data Secure.” Accessed: May 27, 2025. [Online]. Available: <https://www.lookout.com/blog/hospital-secures-patient-data-with-lookout>

[41] “ColorTokens-Childrens-Hospital-casestudy.” Accessed: May 27, 2025. [Online]. Available: <https://colortokens.com/wp-content/uploads/ColorTokens-Childrens-Hospital-casestudy.pdf>

[42] “Implementing OTP Verification and Zero Trust Security for Role-Based Access Control in Medical Records | Request PDF,” in *ResearchGate*, doi: [10.1109/ICSTSN61422.2024.10671108](https://doi.org/10.1109/ICSTSN61422.2024.10671108).

[43] “Pipeline security | GitLab Docs.” Accessed: May 27, 2025. [Online]. Available: <https://docs.gitlab.com/ci/pipelines/pipeline_security/>

[44] “Understand just-in-time virtual machine access - Microsoft Defender for Cloud.” Accessed: May 27, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-overview>

[45] “Why DevOps and zero trust go together.” Accessed: May 27, 2025. [Online]. Available: <https://about.gitlab.com/blog/2022/08/17/why-devops-and-zero-trust-go-together/>

[46] “Secure DevOps environments for Zero Trust.” Accessed: May 27, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/security/zero-trust/develop/secure-devops-environments-zero-trust>

[47] “How Akamai implemented a zero-trust model | CSO Online.” Accessed: May 27, 2025. [Online]. Available: <https://www.csoonline.com/article/567209/how-akamai-implemented-a-zero-trust-model.html>

[48] USA and P. Nutalapati, “Zero Trust Architecture in Cloud-Based Fintech Applications,” *J Arti Inte & Cloud Comp*, vol. 2, no. 1, pp. 1–8, Mar. 2023, doi: [10.47363/JAICC/2023(2)E152](https://doi.org/10.47363/JAICC/2023(2)E152).

[49] “Cloud Security Case Study: Zero Trust Strategy | Accenture.” Accessed: May 27, 2025. [Online]. Available: <https://www.accenture.com/us-en/case-studies/about/cloud-security>

[50] “Transforming secure access with Zscaler Private Access (ZPA).” Accessed: May 27, 2025. [Online]. Available: <https://www.zscaler.com/products-and-solutions/zscaler-private-access>

[51] “The role of User Entity Behavior Analytics to detect network attacks in real time,” ResearchGate. Accessed: May 27, 2025. [Online]. Available: <https://www.researchgate.net/publication/336259455_The_role_of_User_Entity_Behavior_Analytics_to_detect_network_attacks_in_real_time>

[52] “device-posture.” Accessed: May 27, 2025. [Online]. Available: <https://docs.citrix.com/en-us/device-posture/device-posture.pdf>

[53] “DZ BANK Builds Zero Trust Security Strategy With CyberArk,” CyberArk. Accessed: May 27, 2025. [Online]. Available: <https://www.cyberark.com/customer-stories/dz-bank/>

[54] “D Commerce Bank drives digital transformation with Zero Trust, AI-driven network security,” Palo Alto Networks. Accessed: May 27, 2025. [Online]. Available: <https://www.paloaltonetworks.com/customers/d-commerce-bank-drives-digital-transformation-with-zero-trust-ai-driven-network-security>

[55] “African Bank Adopts Zero Trust Access Strategy with New Integrated SD-WAN Security Architecture,” Convergia. Accessed: May 27, 2025. [Online]. Available: <https://convergia.io/en/case-studies/connectivity/african-bank-sd-wan-fortinet-solutions/>

[56] “Phishing Attacks, Email Security Incidents Hit 3 Healthcare Orgs | TechTarget,” Healthtech Security. Accessed: May 27, 2025. [Online]. Available: <https://www.techtarget.com/healthtechsecurity/news/366594859/Phishing-Attacks-Email-Security-Incidents-Hit-3-Healthcare-Orgs>