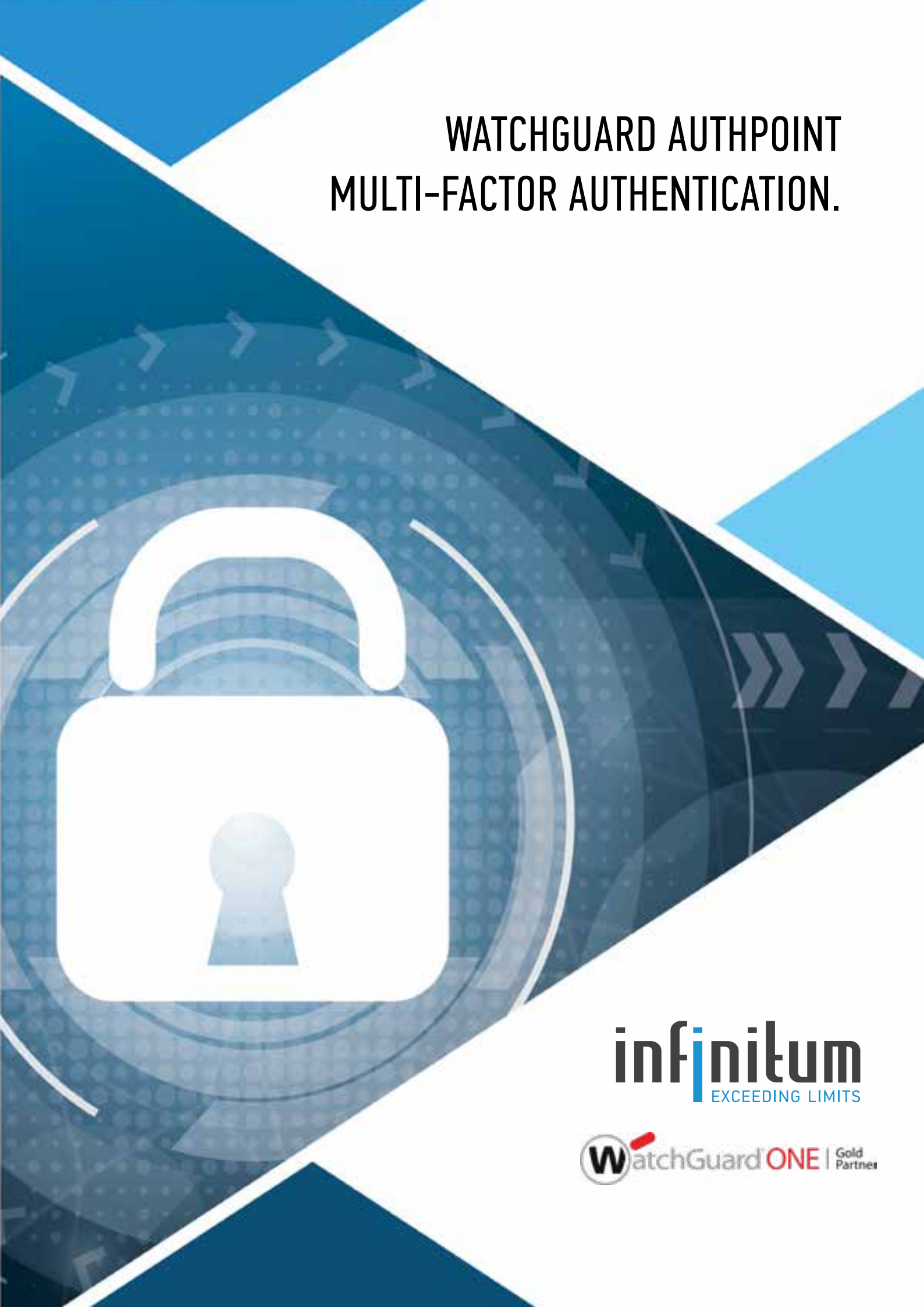
WATCHGUARD AUTHPOINT MULTI-FACTOR AUTHENTICATION.



infinitum
EXCEEDING LIMITS

WatchGuard ONE | Gold Partner

Τι είναι ο Έλεγχος Ταυτότητας Πολλαπλών Παραγόντων (MFA).

Η διαδικασία ελέγχου ταυτότητας (Authentication) είναι, πλέον, γνωστή στους χρήστες εταιρικών δικτύων αλλά και του διαδικτύου και μια -σχεδόν- καθημερινή διαδικασία για όλους.

Στην απλούστερη μορφή του, περιλαμβάνει την εισαγωγή ενός ονόματος χρήστη και ενός κωδικού που γνωρίζει μόνον ο χρήστης αυτός, ώστε να επιβεβαιώνεται ότι η προσπάθεια πρόσβασης γίνεται από ένα συγκεκριμένο πρόσωπο.
Η διαδικασία αυτή, προϋποθέτει ότι τον κωδικό τον γνωρίζει μόνον ένα πρόσωπο (ο χρήστης). Απώλεια ή η με κάποιον έμμεσο τρόπο διαρροή του κωδικού, παρακάμπτει το φράγμα ασφαλείας και θέτει σε κίνδυνο τα δεδομένα του δικτύου.

Ο Έλεγχος Ταυτότητας Πολλαπλών Παραγόντων (Multi-Factor Authentication, MFA), είναι μια μέθοδος ελέγχου ταυτότητας η οποία προσφέρει ασύγκριτα υψηλότερη ασφάλεια. Η διαδικασία περιλαμβάνει την εισαγωγή του ονόματος χρήστη και δύο, ή περισσότερα στοιχεία (ή παράγοντες) που επιβεβαιώνουν την ταυτότητά του.

AuthPoint: Cloud-based υπηρεσία MFA.

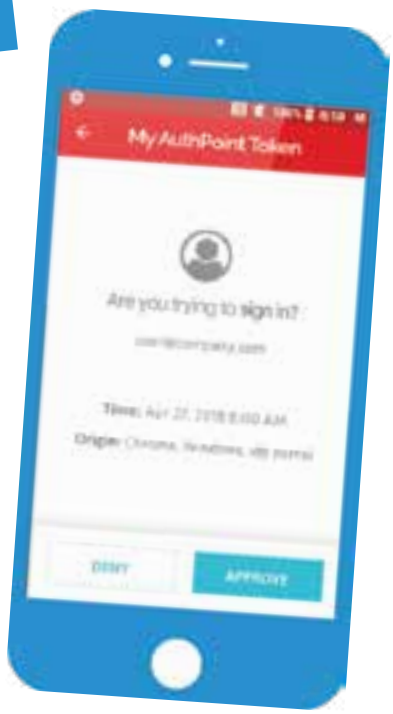
Το AuthPoint είναι η Cloud-based υπηρεσία MFA (Multi-Factor Authentication) της WatchGuard. Με το AuthPoint, οι χρήστες πρέπει να πιστοποιήσουν την ταυτότητά τους μέσω μιας κινητής συσκευής, προκειμένου να συνδεθούν σε προστατευόμενους πόρους τις εταιρείας όπως είναι οι υπολογιστές, οι εφαρμογές μέσω VPN αλλά και άλλες υπηρεσίες οι οποίες παρέχονται μέσω του Cloud.

Το AuthPoint χρησιμοποιεί τις πιο πρόσφατες μεθόδους MFA για την προστασία των πολύτιμων πόρων του οργανισμού σας από μη εξουσιοδοτημένη πρόσβαση. Οι χρήστες εγκαθιστούν την εφαρμογή AuthPoint για κινητές (mobile) συσκευές στο τηλέφωνό τους. Στη συνέχεια, όταν απαιτηθεί να συνδεθούν απομακρυσμένα σε οποιαδήποτε πόρο είτε αυτός βρίσκεται τοπικά σε κάποιο data center της εταιρείας, είτε στο Cloud, πρέπει να πιστοποιήσουν την ταυτότητά τους με μία από τις μεθόδους που υποστηρίζονται, ενώ ο διαχειριστής του συστήματος μπορεί να επιλέξει διαφορετικές μεθόδους ελέγχου ταυτότητας για συγκεκριμένες ομάδες χρηστών και εφαρμογές.

Μέθοδοι πιστοποίησης χρηστών.

Το AuthPoint υποστηρίζει μια σειρά από διαφορετικές μεθόδους πιστοποίησης της ταυτότητας ενός χρήστη, έτσι ώστε να μπορεί να προσαρμοστεί στις ανάγκες κάθε οργανισμού.

Push Notification: Όταν ο χρήστης κάνει αίτηση σύνδεσης, το AuthPoint στέλνει (push) μια ειδοποίηση στην κινητή του συσκευή, την λήψη της οποίας μπορεί είτε να εγκρίνει, προκειμένου να πιστοποιήσει ότι η προσπάθεια σύνδεσης γίνεται από τον ίδιο και να συνεχίσει τη διαδικασία ασφαλούς σύνδεσης, είτε να απορρίψει, προκειμένου να αποτρέψει μια προσπάθεια πρόσβασης που δεν έγινε από αυτόν.



One-Time Password (OTP): Ένας Κωδικός Μίας Χρήσης είναι ένας μοναδικός, προσωρινός κωδικός πρόσβασης στην εφαρμογή AuthPoint, ο οποίος χρησιμοποιείται για τον έλεγχο ταυτότητας και ισχύει για συγκεκριμένο, μικρό, χρονικό διάστημα.

Κωδικός QR: Όταν ο χρήστης κάνει αίτηση σύνδεσης, πρέπει να σαρώσει έναν κωδικό QR (ένα είδος ραβδωτού κώδικα δύο διαστάσεων) με την εφαρμογή AuthPoint για κινητά και να χρησιμοποιήσει τον κωδικό επαλήθευσης που θα του αποσταλεί, ώστε να συμπληρωθεί ο έλεγχος ταυτότητας. Το AuthPoint χρησιμοποιεί ασφαλείς κωδικούς QR που μπορούν να αποκρυπτογραφηθούν μόνο από την εφαρμογή AuthPoint για κινητά.

Τα μέρη του AuthPoint.

Management Graphical User Interface

Το γραφικό περιβάλλον διαχείρισης του AuthPoint βρίσκεται στο WatchGuard Cloud και είναι το σημείο όπου ο διαχειριστής δημιουργεί και διαχειρίζεται τους χρήστες, τις ομάδες χρηστών, τους πόρους, τις εξωτερικές ταυτότητες καθώς και το AuthPoint Gateway.
Ως "Πόροι" χαρακτηρίζονται οι εφαρμογές για τις οποίες ορίζεται μια διαδικασία MFA. Οι εξωτερικές ταυτότητες χρησιμοποιούνται για την σύνδεση με μια βάση δεδομένων χρηστών έτσι ώστε να μπορέσει το AuthPoint να έχει πρόσβαση στο profile του χρήστη και να τον συσχετίσει με τις αποφασισμένες από τον διαχειριστή μεθόδους ελέγχου πρόσβασης στους πόρους της εταιρείας.

AuthPoint Gateway

Το AuthPoint Gateway είναι μια ελαφριά εφαρμογή που πρέπει να εγκατασταθεί στο δίκτυό του οργανισμού, έτσι ώστε το AuthPoint να μπορεί να επικοινωνεί με τα πρωτόκολλα RADIUS (Remote Authentication Dial-In User Service) και LDAP (Lightweight Directory Access Protocol) μέσω Security Assertion Markup Language (SAML).

AuthPoint mobile app

Για την πιστοποίηση ταυτότητας του χρήστη, απαιτείται η εφαρμογή AuthPoint για κινητά. Μέσω της εφαρμογής αυτής, ο χρήστης μπορεί να δει και να διαχειριστεί τα tokens του, να εγκρίνει ειδοποιήσεις push, να λάβει OTPs και να σαρώσει τους κωδικούς QR, ανάλογα με την μέθοδο πιστοποίησης ταυτότητας που χρησιμοποιείται.

Logon App

Μέσω της εφαρμογής Logon App απαιτείται από τους χρήστες να πιστοποιήσουν τα στοιχεία τους όταν πρόκειται να συνδεθούν σε υπολογιστή ή σε server ακόμα και όταν βρίσκονται εντός της εταιρείας και όχι μόνο όταν επιχειρούν μια απομακρυσμένη σύνδεση.
Το Logon App αποτελείται από 2 μέρη, Την εφαρμογή η οποία εγκαθίσταται στον υπολογιστή ή τον server του οποίου απαιτείται η προστασία και τον πόρο (resource) για τον οποίο θα ισχύει η άδεια πρόσβασης που θα δοθεί μέσω του AuthPoint.

Λίγα λόγια για την Infinitum

Η Infinitum έχει συμπληρώσει πάνω από 25 χρόνια τεχνογνωσίας στον τομέα των υπηρεσιών IT, προσφέροντας κορυφαίες λύσεις και υπηρεσίες υποδομών, δικτύωσης και λογισμικού. Σταθερός στόχος μας είναι η δημιουργία ενός απροβλημάτιστου περιβάλλοντος με προηγμένη, data-driven τεχνολογία για κάθε επιχείρηση, ώστε οι άνθρωποί της να μπορούν να επικεντρώνονται σε ό,τι έχει πραγματική σημασία. Διαθέτουμε την ευελιξία να προσαρμοζόμαστε στις νέες τεχνολογίες, υλοποιώντας τις πραγματικά πιο ωφέλιμες λύσεις έτσι ώστε οι επιχειρήσεις να συμβαδίζουν με τους διαρκώς εξελισσόμενους ρυθμούς της αγοράς.

Επικοινωνήστε μαζί μας σήμερα ώστε να συζητήσουμε από κοντά τις λύσεις που καλύπτουν τις απαιτήσεις της δικής σας επιχείρησης.

Email: info@infinitum.gr

infinitum
EXCEEDING LIMITS

Μ. Κωνσταντίνου 20-22, Νέο Ηράκλειο 14 122 - Αθήνα
T. (+30) 213 01 80 000 F. (+30) 213 01 80 080
Email. info@infinitum.gr

www.infinitum.gr