EDR, EPDR, XDR, MDR

Μηχανισμοί και Υπηρεσίες άμεσης αντίδρασης

Αντώνης Καλοχριστιανάκης, Sales Director

WatchGuard

Digital Sima

Τεχνολογίες... DR

EDR	End Point Detection & Response
EPDR	End Point Protection & Detection & Response (AV + EDR)
XDR	eXtended Detection & Response (EDR με κάτι ακόμη επιπλέον του End Point)
MDR	Managed Detection & Response (Συνοδεύεται από Υπηρεσία)

Τι πρέπει να ξέρουμε για το XDR

- Είναι της «μόδας», γίνεται πολύς θόρυβος.
- Αναμένεται να γίνει βασικό εργαλείο ασφάλειας.
- Ο κάθε κατασκευαστής το ορίζει διαφορετικά.
- Οι πάροχοι υπηρεσιών ασφάλειας (Integrators & MSSPs) θα πρέπει να το κατανοήσουν και να επενδύσουν τεχνικά.

WatchGuard ηγείται στο EDR & XDR

Το XDR είναι καινούριος όρος . . . όχι καινούρια έννοια.

2015

Introduced the first EDR solution with a zero-trust application service

Launched by Panda Security, now offered as WatchGuard EDR and EPDR

2017

WatchGuard launches ThreatSync, the first Cloud-based XDR solution

Network to endpoint correlation built on Hexis Hawkeye-G technology

2018

First appearance of the XDR term

Extended Detection and Response (XDR), a concept where the "X" represented anything

2020

Gartner defines XDR

An Innovation Insight paper on March 19, 2020, describes three requirements for XDR products

2020 - Forever

XDR is enhanced with ThreatSync as part of our Unified Security Platform

Additional endpoint and identity events grow our XDR capabilities

Η WatchGuard είχε προβλέψει την ανάγκη, εξαγόρασε τεχνολογία και πρόσφερε προϊόν XDR πριν καν υπάρξει ο όρος.

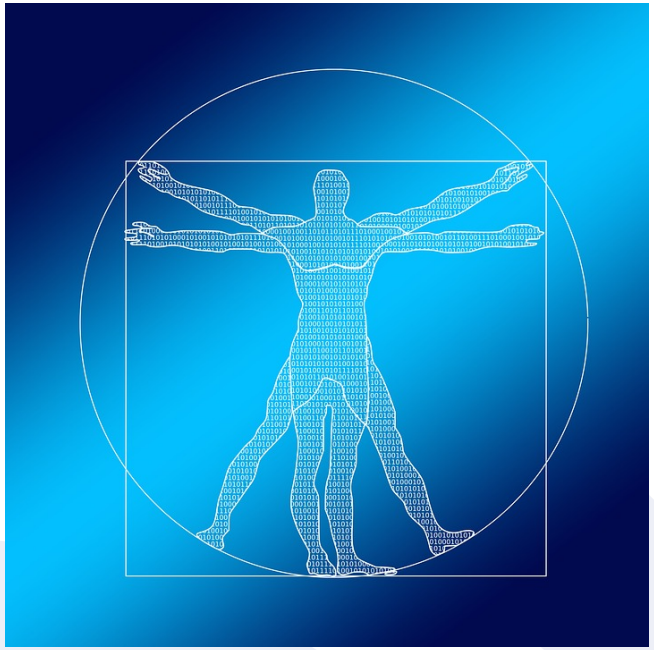
Η πρωτοπορία του ThreatSync συνεχίζει ως ουσιώδες στοιχείο της αρχιτεκτονικής Unified Security Platform περιλαμβάνοντας και ταυτοποίηση (2xFA)

Τι είναι το XDR

Ορισμός Gartner

Το Extended detection & response (XDR) είναι εργαλείο ανίχνευσης απειλών και απόκρισης, που ενσωματώνει πολλαπλά προϊόντα ασφάλειας σε ένα λειτουργικό σύστημα.

- Το XDR είναι προϊόν ή/και πλατφόρμα.
- Συμμετέχουν πολλαπλά προϊόντα ασφάλειας.
- Χρησιμοποιείται συνδυασμένη threat intelligence
- Υπηρεσία στο σύννεφο.
- Vendor-specific
  - Γιατί; Μόνο ο κατασκευαστής μπορεί να δημιουργήσει αυτόματες αντιδράσεις στα χαμηλότερα επίπεδα.
  - *Το Open XDR* είναι μία προσπάθεια τυποποίησης για να μπορούν προϊόντα διαφορετικών κατασκευαστών να συμμετέχουν στο XDR ενός κατασκευαστή



Τι είναι το XDR

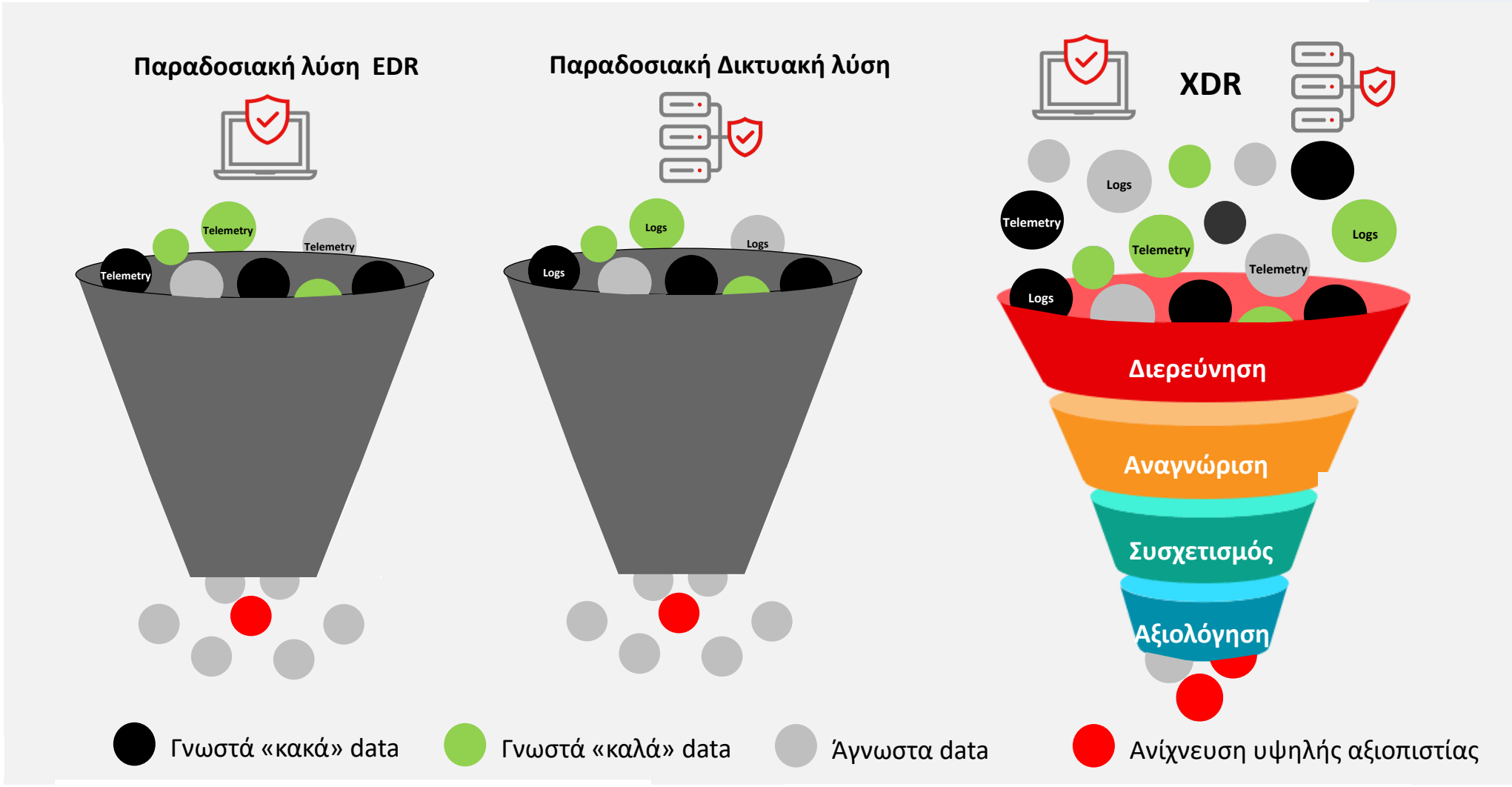
Σύμφωνα με το Forrester:

- Η τεχνολογία XDR θα αντικαταστήσει το EDR, ενώ στο μέλλον θα ανταγωνιστεί τα SIEM.
- *«Το EDR ακόμη δεν προσφέρει την πλήρη εικόνα της επίθεσης. Οι διαχειριστές συμβάντων καλούνται να αντιμετωπίσουν το πρόβλημα αναλύοντας τα alerts του EDR μέσω είτε ενός SIEM, είτε άλλων πλατφορμών ανάλυσης προσθέτοντας «χειροκίνητα» δεδομένα από άλλες πηγές.*
- *... Οι διαχειριστές συμβάντων χρειάζεται να ενσωματώσουν πηγές επιπρόσθετης τηλεμετρίας να προσφέρουν πλουσιότερα alerts και δυνατότητες πληρέστερης απόκρισης*

- Native XDR (Forrester) = XDR (Gartner)
- Hybrid XDR (Forrester) = Open XDR (Gartner)

Forrester Research: Extended Detection And Response (XDR) — A Battle Between Precedent And Innovation

Πως λειτουργεί το XDR

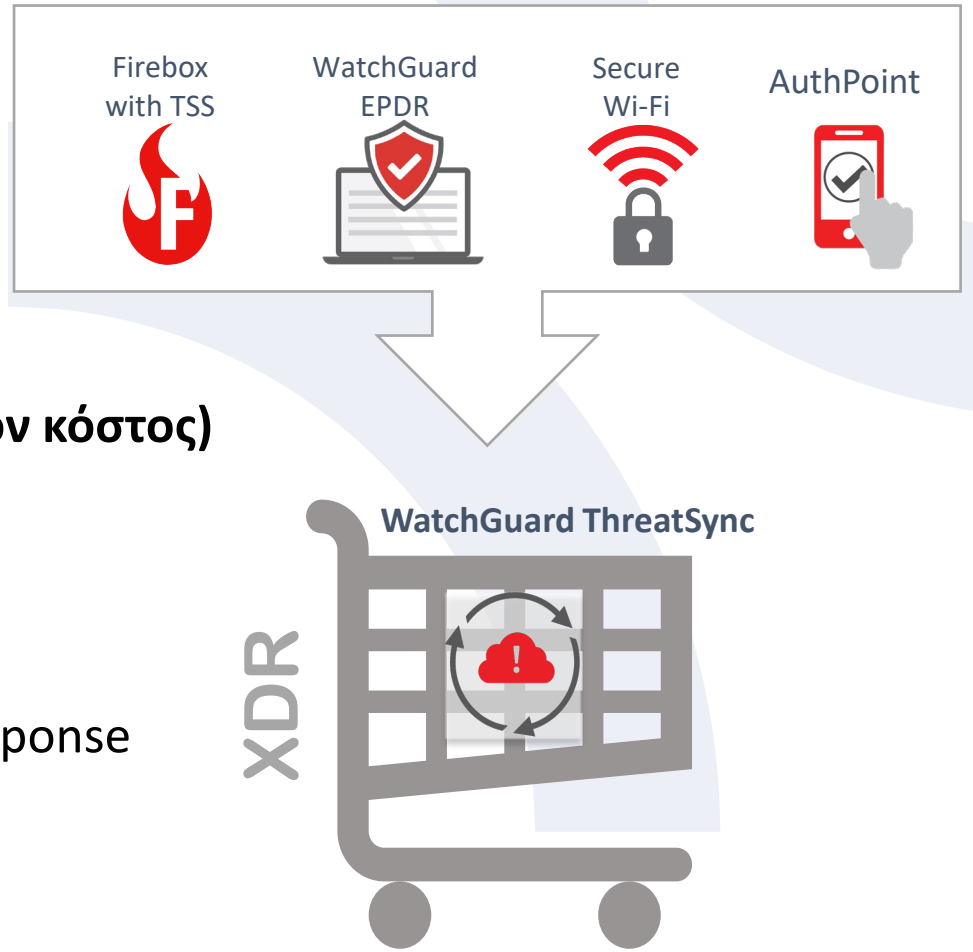


Τι προσφέρει το XDR

Ανάλυση Δεδομένων	Ανίχνευση Απειλής	Αντίδραση στην Επίθεση
Συγκέντρωση δεδομένων και συσχετισμός	Αξιολόγηση alerts και αναφορά των σημαντικών	Απομάκρυνση απειλής και εφαρμογή πολιτικών ασφάλειας

Πως προμηθεύομαι WatchGuard XDR με ThreatSync

- **Προμήθεια προϊόντων WatchGuard**
  - ✓ WatchGuard Total Security Suite από το firewall.
  - ✓ WatchGuard EDR/EPDR Endpoint Security
  - ✓ WatchGuard AuthPoint Identity Security
  - ✓ WatchGuard Secure Wi-Fi



- **Περισσότερα προϊόντα = περισσότερη αξία XDR (χωρίς επιπλέον κόστος)**

- **Χρησιμοποιείστε το ThreatSync στο WatchGuard Cloud**
  - ✓ Εξαιρετικό interface και dashboards
  - ✓ Κεντρικοποιημένο management, incident views/alerts και response actions
  - ✓ Μελλοντικές εκδόσεις ThreatSync

Experience ThreatSync in the WatchGuard Cloud Demo!

Τι αναζητούν οι επιχειρήσεις στον MSP

Εξειδίκευση 

- Οι MSPs έχουν ομάδα ειδικών στη διαχείριση και συντήρηση των XDR
- Οι πελάτες ωφελούνται από τις γνώσεις τους.

Οικονομία 

- Το outsourcing της διαχείρισης του XDR σε έναν MSP μπορεί να είναι οικονομικότερο από την διατήρηση ειδικού/κων ασφάλειας
- Τα κόστη των MSPs είναι συγκεκριμένα και προβλέψιμα

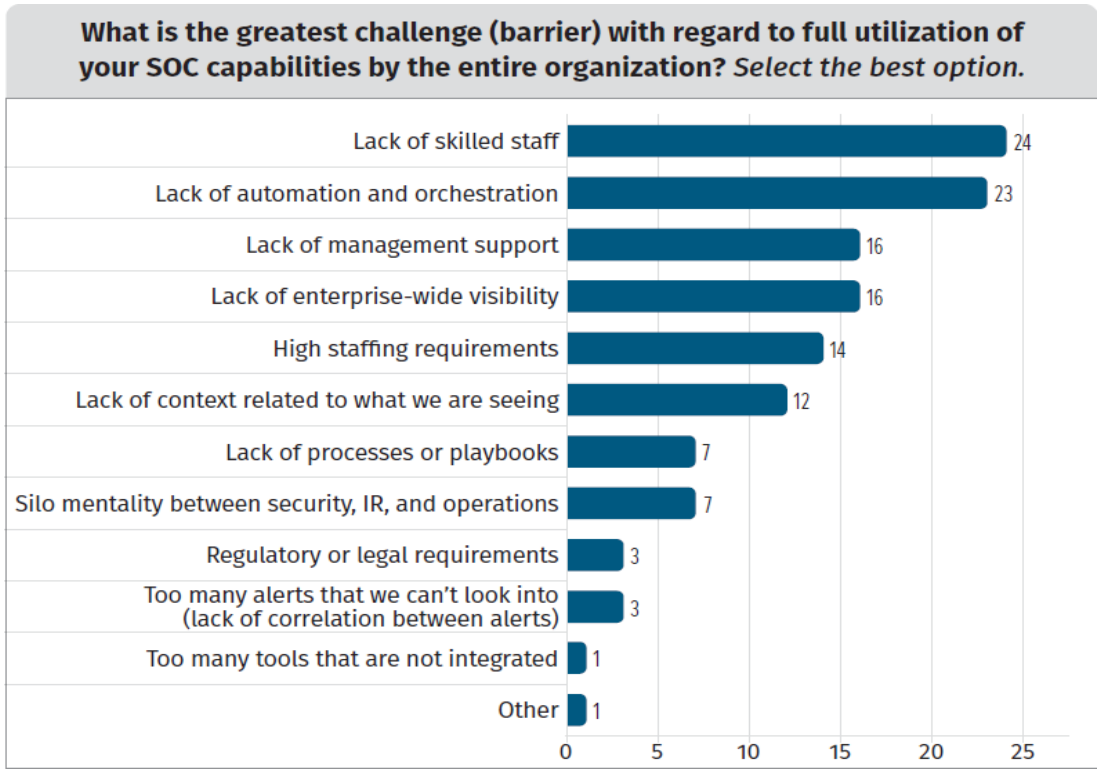
Ασφάλεια 

- Η συνεργασία με ένα MSP διασφαλίζει στην επιχείρηση ότι η λύση XDR λειτουργεί σωστά.
- Οι MSPs παραμετροποιούν τακτικά το XDR ώστε να παρέχει τη βέλτιστη δυνατή ασφάλεια

Ευελιξία 

- Οι υπηρεσίες προσαρμόζονται ανάλογα με το περιβάλλον του πελάτη.
- Το XDR προσαρμόζεται στις δικτυακές και άλλες αλλαγές.

Οι MSPs χρειάζονται το XDR για αποτελεσματική προσφορά Υπηρεσιών Ασφάλειας



SANS Institute 2021. Greatest Challenge to Full Use of Security Operations Capabilities

Έλλειψη εξειδικευμένου προσωπικού

Πληθώρα Alerts

Έλλειψη Αυτοματισμού Ασφάλειας

Έλλειψη ακρίβειας και συσχετισμού

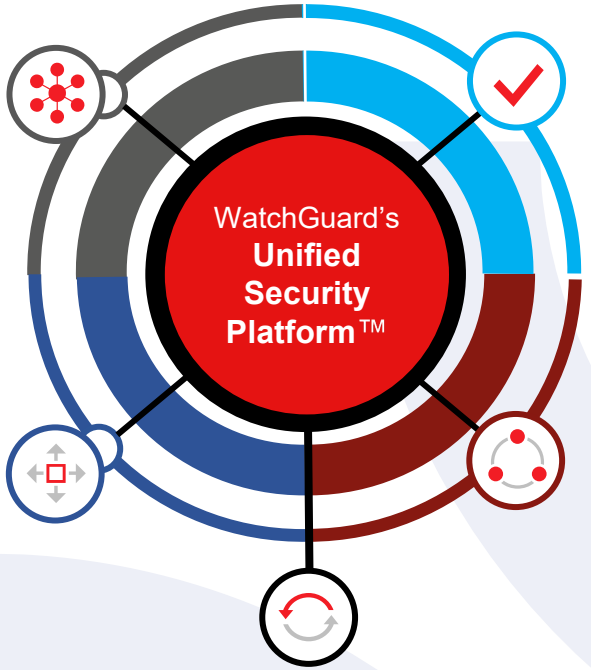
Έλλειψη ενοποιημένης συνεργασίας μεταξύ μελών SOC/IT

Έλλειψη καθορισμένων διαδικασιών και playbooks

Το XDR είναι βασικό στοιχείο της αρχιτεκτονικής WatchGuard's Unified Security Platform™.

Τι προσφέρει η WG: Πλατφόρμα φτιαγμένη και για MSPs

MSP ΠΡΟΤΕΡΑΙΟΤΗΤΕΣ	WATCHGUARD
ΕΥΡΟΣ & ΣΥΝΑΦΕΙΑ ΛΥΣΕΩΝ	Ένα πλήρες portfolio από endpoint, multi-factor authentication, και network security λύσεων για προστασία υποδομής, χρηστών και συσκευών.
ΕΥΚΟΛΙΑ ΔΙΑΧΕΙΡΙΣΗΣ	Το WatchGuard Cloud είναι κεντρική πλατφόρμα που προσφέρει ανάλυση σε βάθος, προηγμένο reporting, και πλήρη εικόνα για τον MSP
ΕΝΕΡΓΟΠΟΙΗΣΗ ΤΟΥ S ΣΤΟ MSSP	Μία πλήρως ενοποιημένη πλατφόρμα για την υλοποίηση πολιτικής μηδενικής εμπιστοσύνης μέσω του WatchGuard's Identity Framework και εφαρμογής πραγματικής XDR-based προσέγγισης για την αντιμετώπιση απειλών μέσω του ThreatSync.
ΑΥΤΟΜΑΤΕΣ ΔΙΑΔΙΚΑΣΙΕΣ	Το WatchGuard's Automation Core προσφέρει απλοποιημένη και προσαρμοσμένη απόκριση στην κάθε απειλή ανάλογα με τη βαρύτητά της.
BUSINESS MODEL FLEXIBILITY	Απλοποιημένη λειτουργία με άμεση πρόσβαση σε API, ένα πλούσιο οικοσύστημα, out-of-the-box συνεργασίες, and ευέλικτους τρόπους χρέωσης.



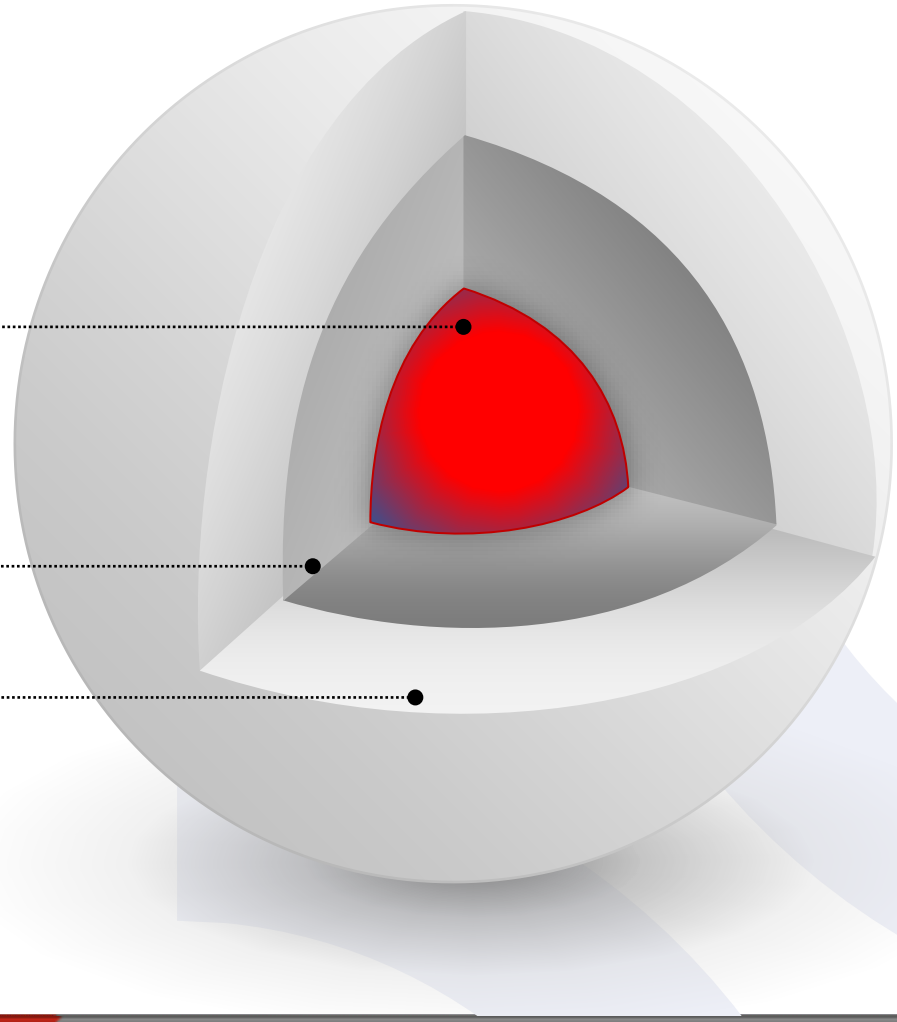
Watchguard MDR

Προστασία 24/7 χωρίς το Overhead

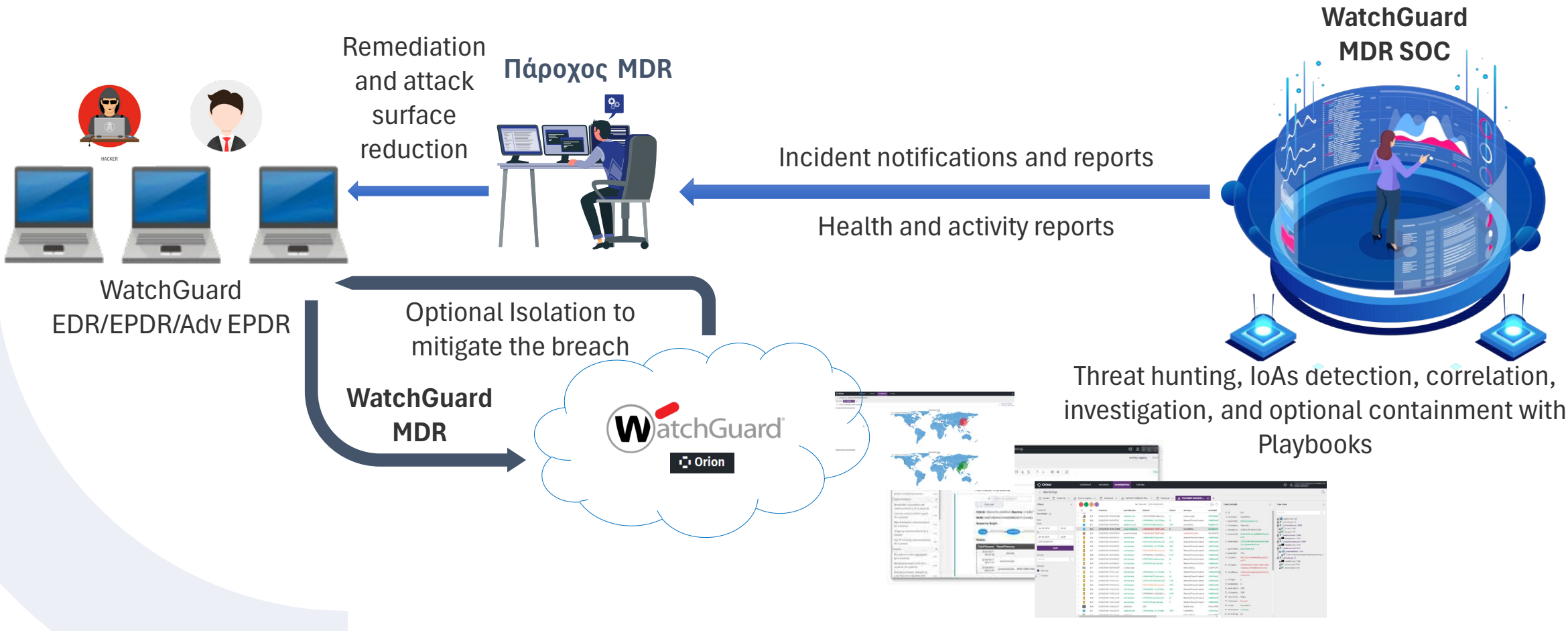
- Το **WatchGuard MDR** προσφέρει συνεχή παρακολούθηση των endpoint και του Microsoft 365, ανίχνευση απειλών και κατ' επιλογή αντιδράσεις περιορισμού των απειλών και τακτικές αξιολογήσεις της ασφάλειας, επιπλέον από αυτά που προσφέρονται από τις λύσεις **WatchGuard EDR, EPDR, ή Advanced EPDR.**

- **Στην καρδιά του WatchGuard MDR** είναι **ομάδα έμπειρων ειδικών στην κυβερνοασφάλεια προσφέροντας 24/7/365 managed detection & response** από το WatchGuard SOC.

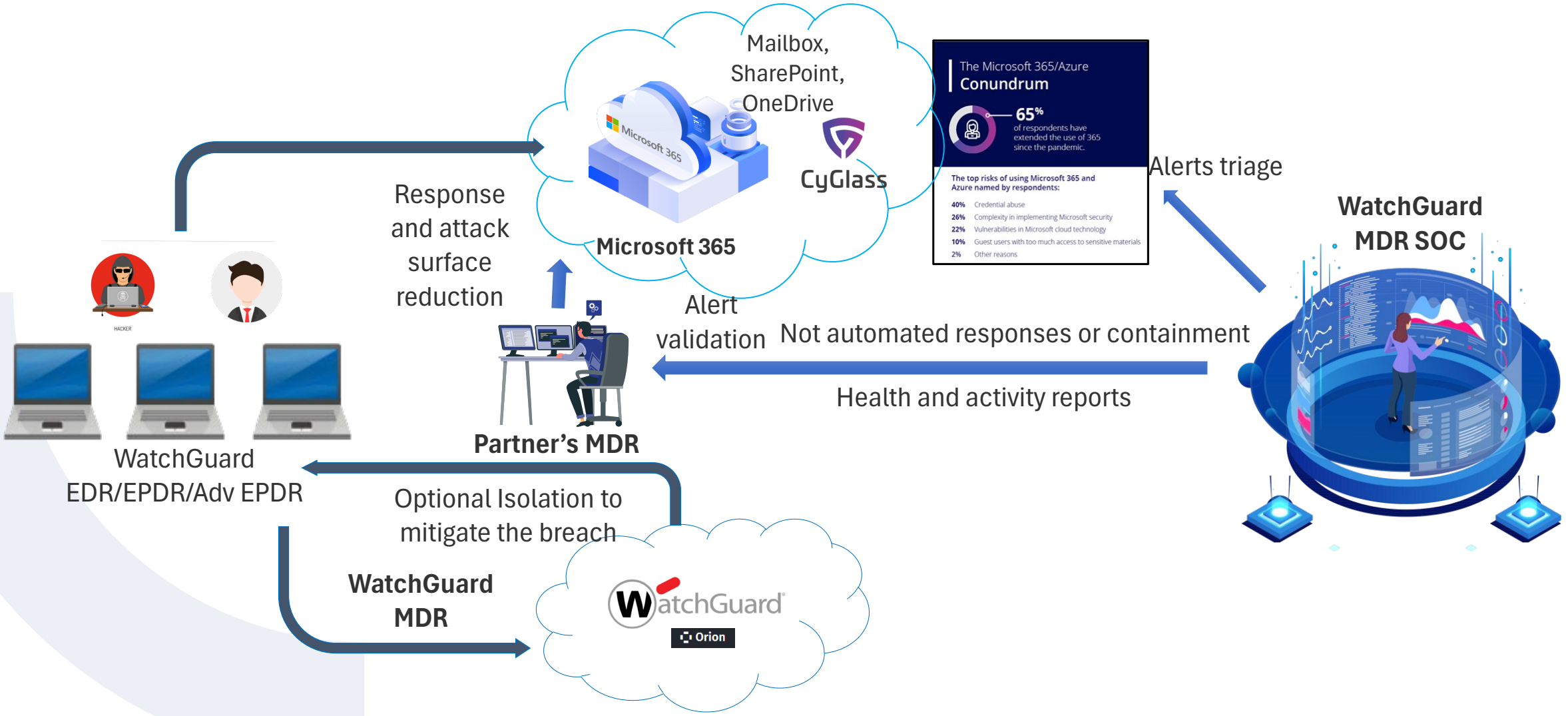
- Ο πάροχος MSP ενισχύει τις υπηρεσίες που προσφέρονται από το WatchGuard MDR προσφέροντας **on-site υποστήριξη hands-on**. Η Watchguard **περιορίζει την έκταση της επίθεσης** που δημιουργήθηκε από unpatched endpoints ή λανθασμένες ρυθμίσεις που ανίχνευσε.



Πως λειτουργεί στα endpoint



Πως λειτουργεί στο Microsoft 365



Ευχαριστούμε!

WatchGuard

Digital Sima