Threat Detection & Response

Καλοχριστιανάκης Αντώνης
Διευθυντής Πωλήσεων Digital SIMA

SMART SECURITY

Βασικά Χαρακτηριστικά WatchGuard

- Κατασκευαστής μόνο UTM Firewalls

Firebox Cloud

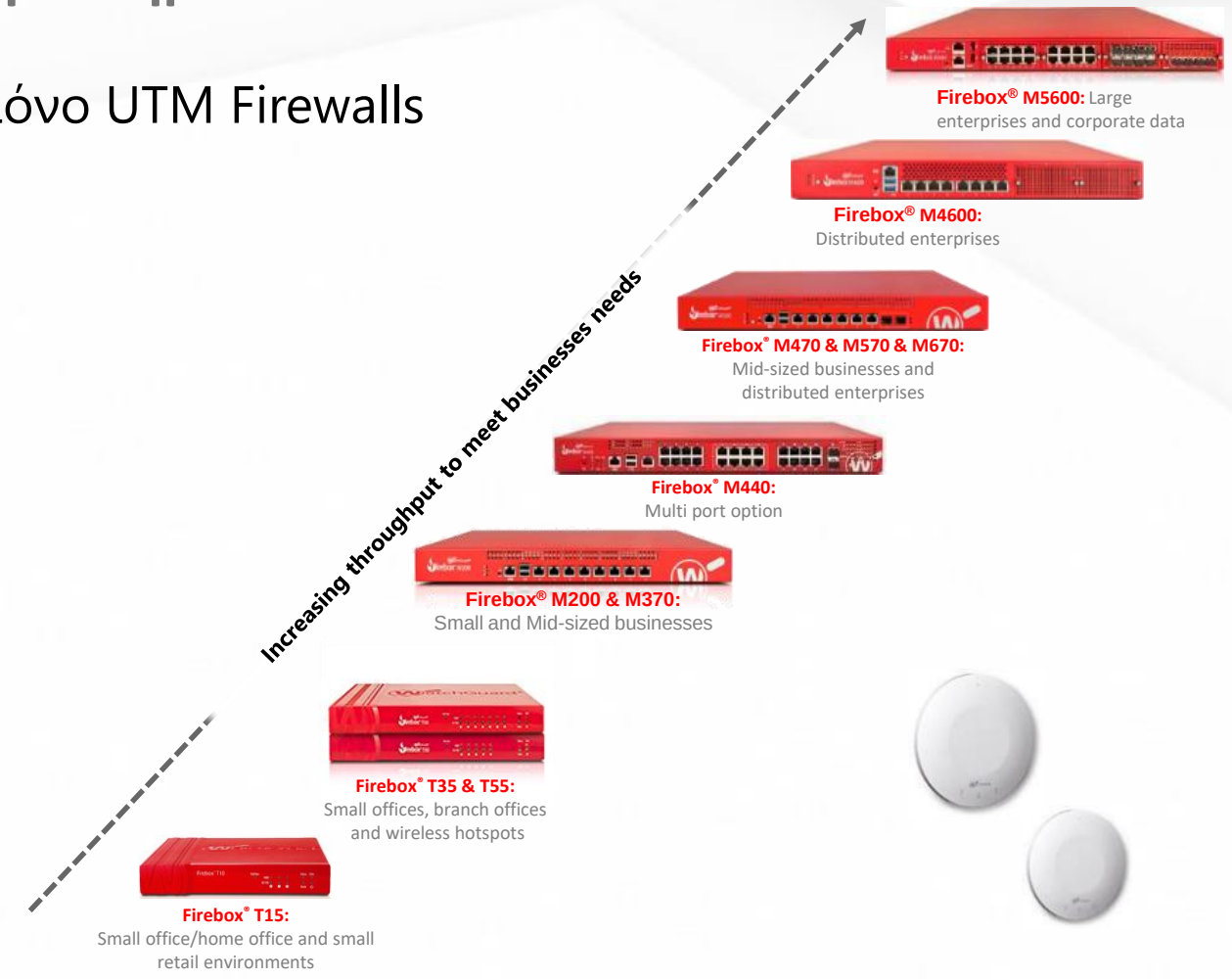
amazon web services

Microsoft Azure

Firebox V

vmware

Microsoft Hyper-V



DIGITAL SIMA

Βασικά Χαρακτηριστικά WatchGuard

- Κατασκευαστής μόνο UTM Firewalls
- Επιλογή κορυφαίων υπηρεσιών UTM

IPS . . . . . TREND MICRO

Antivirus . . . . . Bitdefender

App. Control . . . TREND MICRO

Cont. Filtering . . websense

DLP . . . . . SOPHOS

Antispam . . . . CYREN

Reputation . . . KASPERSKY lab

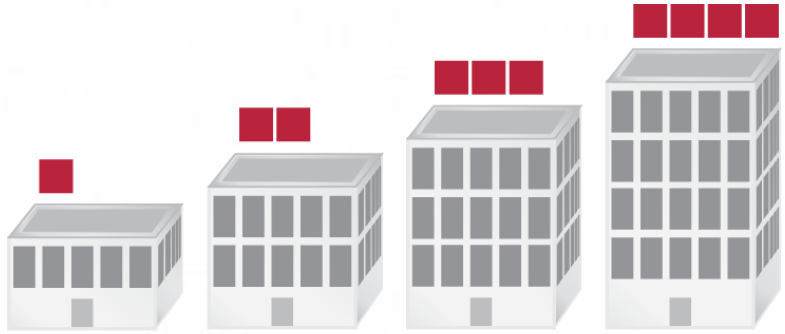
TDR . . . . . HawkEye G
Integrated Detection. Automated Response.

ATP Defence . . lastline

DIGITAL SIMA

Βασικά Χαρακτηριστικά WatchGuard

- Κατασκευαστής μόνο UTM Firewalls
- Επιλογή κορυφαίων υπηρεσιών UTM
- Απευθύνεται στη μικρομεσαία – μεγαλομεσαία αγορά



Βασικά Χαρακτηριστικά WatchGuard

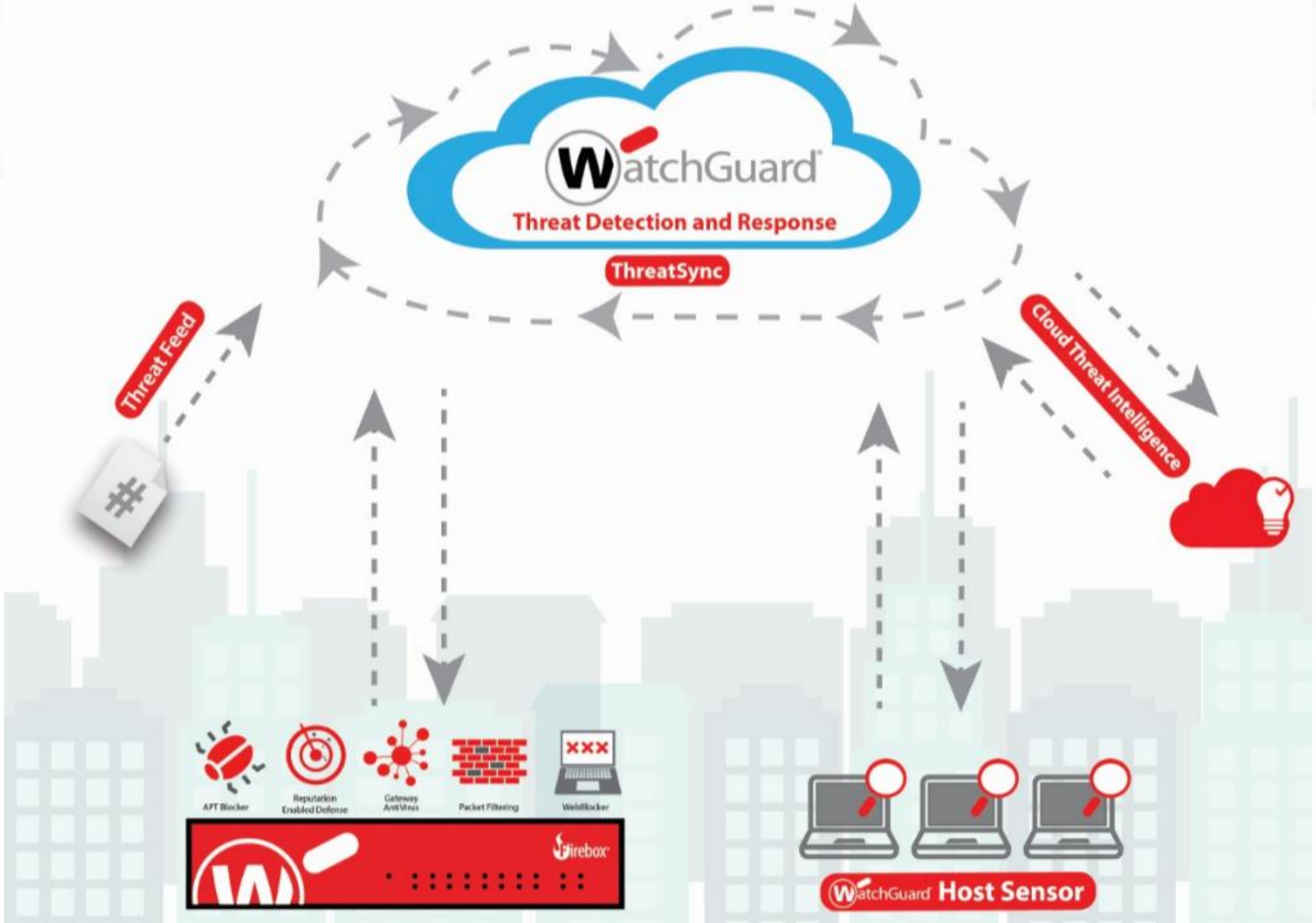
- Κατασκευαστής μόνο UTM Firewalls
- Επιλογή κορυφαίων υπηρεσιών UTM
- Απευθύνεται στη μικρομεσαία – μεγαλομεσαία αγορά
- Ικανοποιημένοι Πελάτες

+26

Customer Net Promoter Score*

*Πηγή : Deep-Insight, Οκτώβριος 2015 σε δείγμα 1.700

Threat Detection and Response



Host Sensor — Λειτουργία

- Οι Host Sensors εγκαθίστανται στα hosts
  - Δεν υπάρχει UI στο Host
  - Όλοι οι Host Sensors ελέγχονται από το λογαριασμό TDR
- Από default, ο Host Sensor:
  - Τρέχει ένα βασικό scan κάθε φορά που ξεκινά.
  - Ελέγχει αλλαγές σε αρχεία, processes, registry, δικτυακή συμπεριφορά.
  - Αναφέρει ύποπτα συμβάντα στο TDR για βαθμολογία.

Host Sensor— Ενέργειες

- Βασικές αυτοματοποιημένες δράσεις του Host Sensor:
  - Quarantine files
  - Kill processes
  - Delete a registry value
- Το Host Ransomware Prevention (HRP) είναι ενεργοποιημένο από default
  - Το Host Sensor προστατεύει από ransomware ακόμα και offline
- Μπορούν να ρυθμιστούν πολιτικές του TDR για αυτόματες δράσεις έναντι άλλων απειλών βασισμένες στη βαθμολογία συμβάντων.

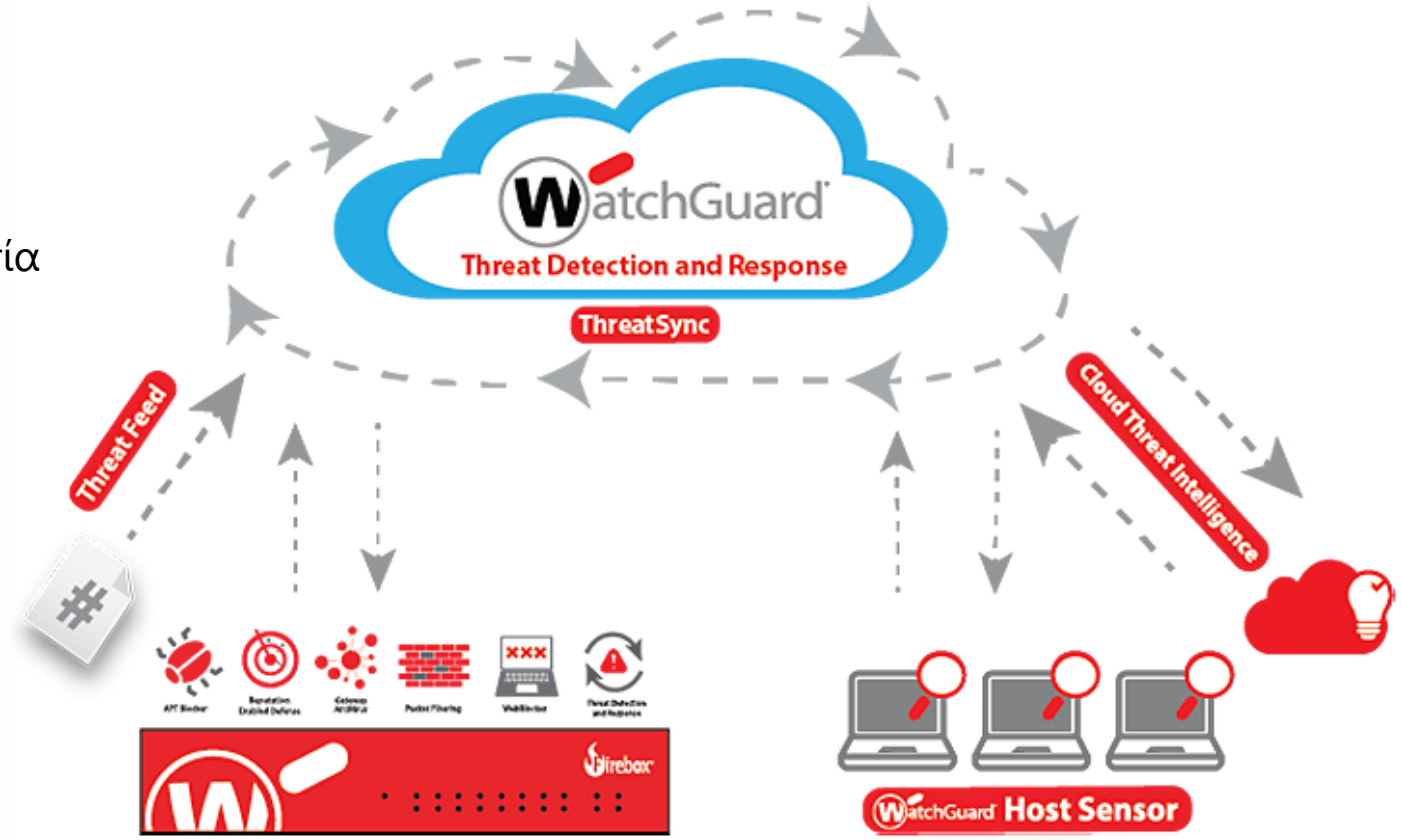
Threat Detection And Response

Οι απειλές που ανιχνεύονται από το F/W ή από το Host Sensor στέλνονται στο σύννεφο όπου αναλύονται και κατηγοριοποιούνται ανάλογα με τη σοβαρότητα.

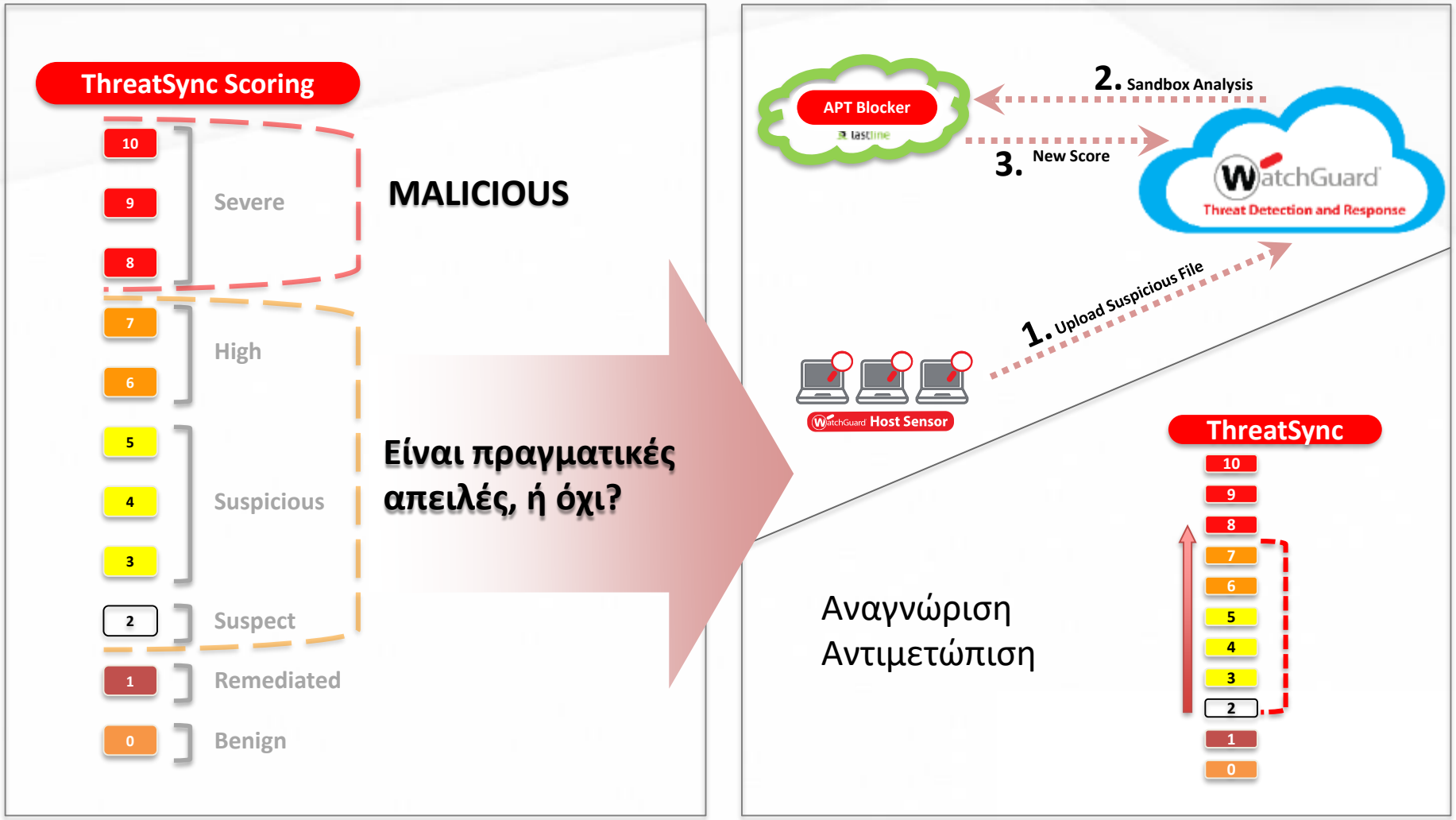
Οι απειλές ανιχνεύονται

Host Sensors
- Threat Feed: Database απειλών
- Malware Verification Service, υπηρεσία (τρίτου) που προσφέρει Threat Intelligence
- Heuristic / behavior analysis

Firebox
- UTM, APT Blocker, GAV, Botnet Detection, WebBlocker
- Blocked Sites list
- DNS Proxy denied query names



Deep TDR & APT Blocker Integration



“Τα συστήματα ασφάλειας πρέπει να νικούν κάθε φορά, ενώ ο επιτιθέμενος αρκεί να κερδίσει μόνο μία.”

Thank You