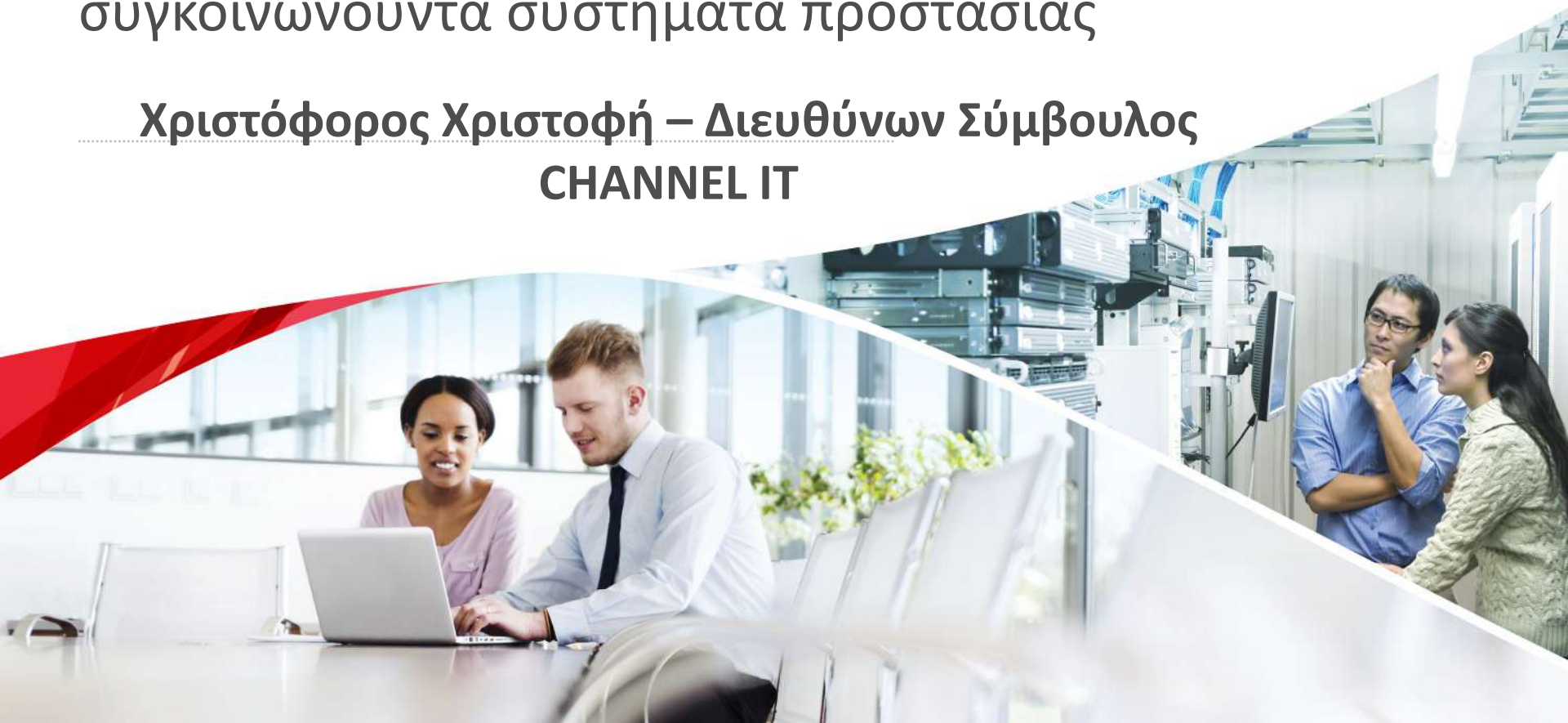
# Connected Threat Defense

## συγκοινωνούντα συστήματα προστασίας

**Χριστόφορος Χριστοφή – Διευθύνων Σύμβουλος**

**CHANNEL IT**



Πριν **πέντε** χρόνια η **ασφάλεια** των επιχειρήσεων ήταν ήδη δύσκολη υπόθεση

# Ο μοντέρνος χώρος εργασίας
# δεν έχει σύνορα

Η On-premise προστασία ή η περιμετρική προστασία

δεν αρκεί πιά

80%

ΤΟΥ ΦΟΡΤΟΥ ΒΡΙΣΚΕΤΑΙ ΣΕ ΕΙΚΟΝΙΚΕΣ ΕΦΑΡΜΟΓΕΣ

95%

85%

Χρησιμοποιούν διάφορες εφαρμογές ή υπηρεσίες INFRASTRUCTURE AS A SERVICE

Υιοθετούν στρατηγική MULTI-CLOUD

Το πεδίο απειλών
εξελίσσεται


Ransomware

Targeted
Attacks

Point of Sale
RAM Scrapers

Flash Exploits

Macro Malware

Είναι δύσκολη η **ορατότητα** σε όλα αυτά τα διαφορετικά περιβάλλοντα

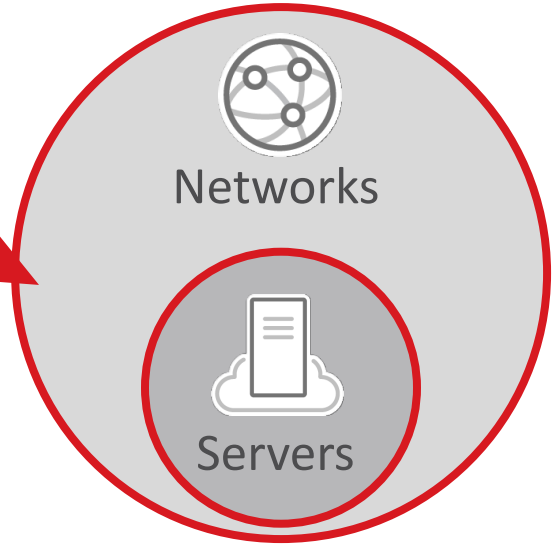
Είναι και πολλά τα σημεία εισόδου των απειλών που πρέπει να προστατέψουμε

# Η διαχείριση όλων αυτών των κινδύνων προϋποθέτει μια δομημένη, πολύ-επίπεδη μέθοδο προστασίας

Προστατεύει τους server όπου και αν βρίσκονται – physical, virtual ή cloud

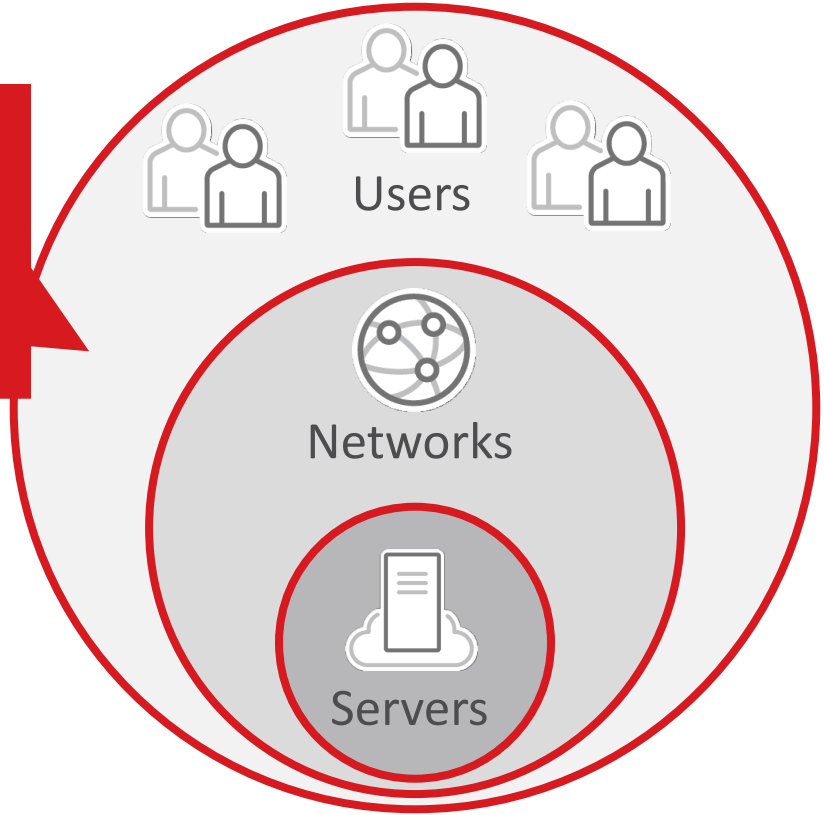
# Η διαχείριση όλων αυτών των κινδύνων προϋποθέτει μια δομημένη, πολύ-επίπεδη μέθοδο προστασίας

Να εντοπίζει και να σταματά επιθέσεις στο data center και στους χρήστες αποτελεσματικά



# Η διαχείριση όλων αυτών των κινδύνων προϋποθέτει μια δομημένη, πολύ-επίπεδη μέθοδο προστασίας

Προστατεύει τους χρήστες όπου και να βρίσκονται, σε οποιαδήποτε συσκευή

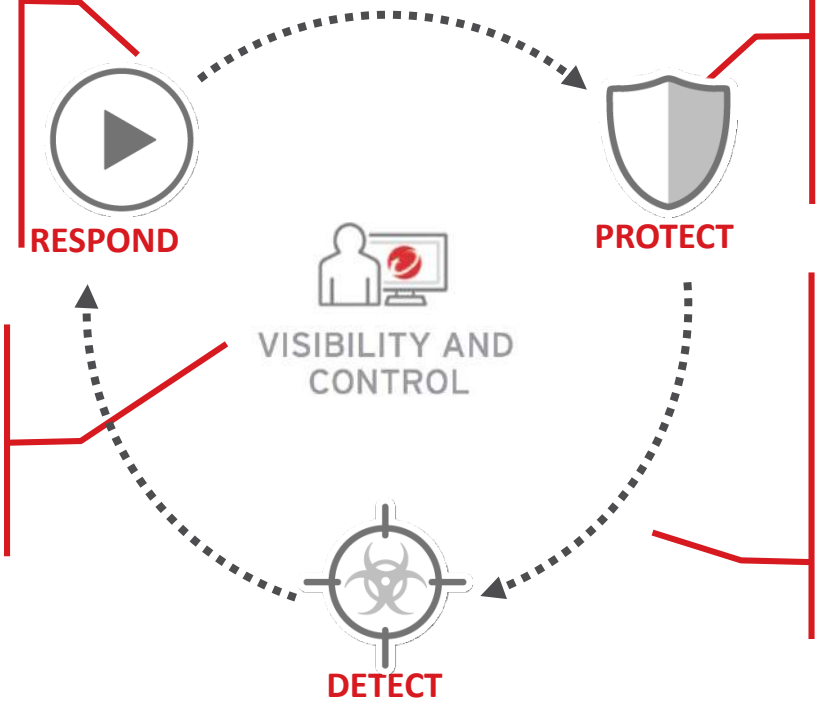



*Η ανάγκη για δομημένη προστασία και ορατότητα σε όλο το δίκτυο αυξάνεται*

# Connected Threat Defense: Αμεση και ολοκληρωμενη Προστασία

Γρήγορη αντιμετώπιση μέσω ανταλλαγής πληροφοριών για απειλές και την έγκαιρη εφαρμογή των updates σε πραγματικό χρόνο

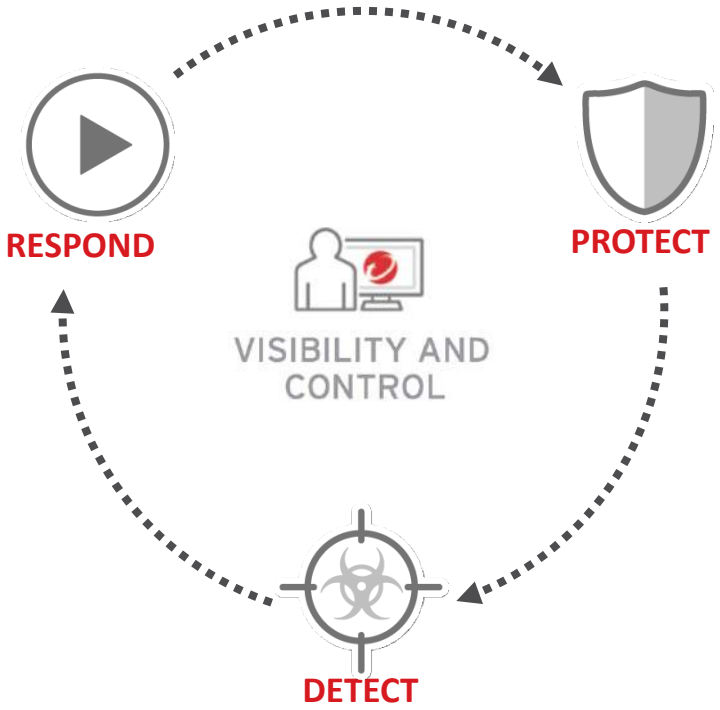
Άμεση εκτίμηση πιθανών «αδυναμιών» για έγκαιρη αντιμετώπιση και προστασία endpoints, servers και εφαρμογών




Αυξημένη Κεντρική Ορατότητα σε όλο το δίκτυο – ανάλυση και εκτίμηση επιπτώσεων

Εντοπίζει περίεργες συμπεριφορές και προηγμένα malware – αόρατα σε συνηθισμένα συστήματα προστασίας

# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία



# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

**PROTECT**

Anti-Malware and Content Filtering

App Control

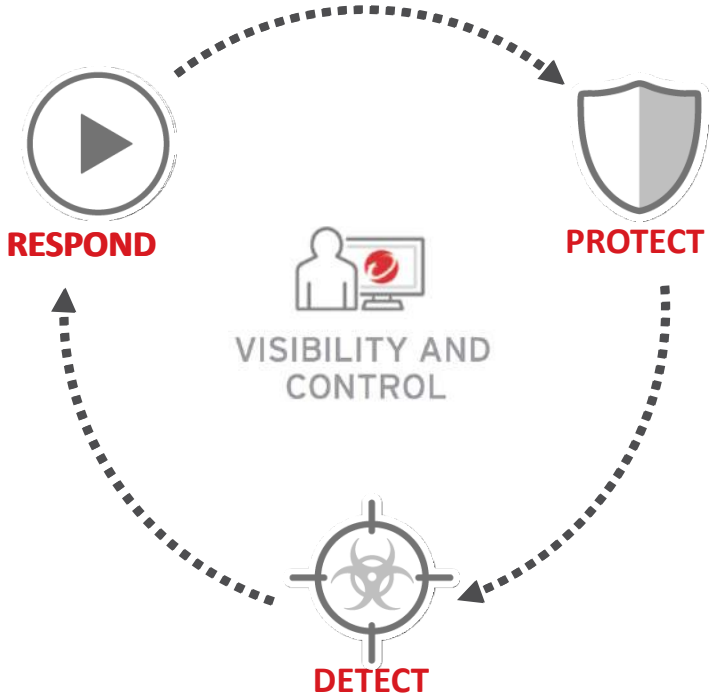
Encryption and Data Loss Prevention

Intrusion Prevention

Integrity Monitoring

# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

PROTECT



# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία


*“The traditional defense-in-depth components are still necessary, but are no longer sufficient in protecting against advanced targeted attacks and advanced malware.”*

Network Content Inspection

Custom Sandbox Analysis

Lateral Movement Detection

Machine Learning

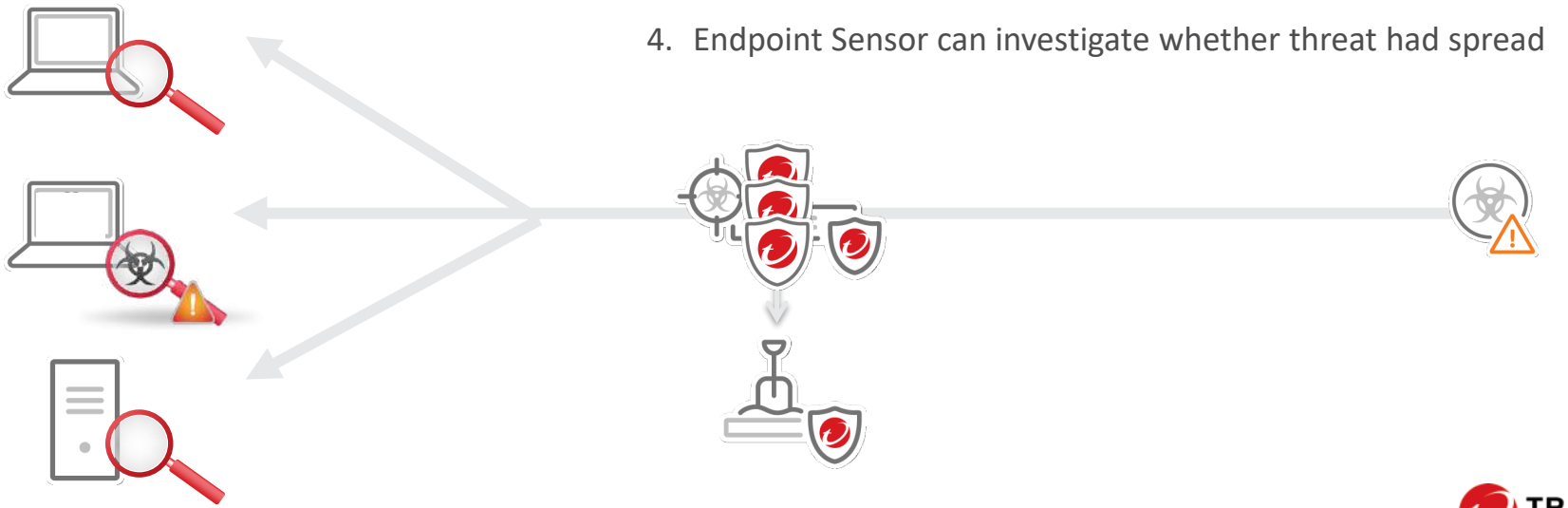
Behavioral Analysis

# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

**RESPOND**

## RAPID RESPONSE

1. Malware infects an endpoint
2. Deep Discovery detects malware
3. Real-time signature pushed to endpoints (logging or blocking)
4. Endpoint Sensor can investigate whether threat had spread

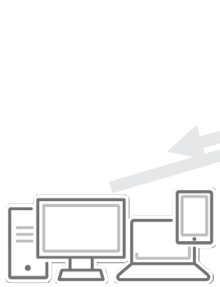


# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

**RESPOND**

CENTRALIZED THREAT SHARING AND VISIBILITY

CUSTOM SANDBOX



ENDPOINT PROTECTION

| | |
|---|---|
| Apex One | URL, File, IP |
| EDR | IOC, SHA, IP, Domain |

# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

**RESPOND**

CENTRALIZED THREAT SHARING AND VISIBILITY

CUSTOM SANDBOX

ENDPOINT PROTECTION

MAIL SECURITY

| | |
|---|---|
| ScanMail for Exchange | SHA-1 |
| InterScan Mail Security | SHA-1 |

# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

**RESPOND**

CENTRALIZED THREAT SHARING AND VISIBILITY

CUSTOM SANDBOX

ENDPOINT PROTECTION

MAIL SECURITY


WEB GATEWAY

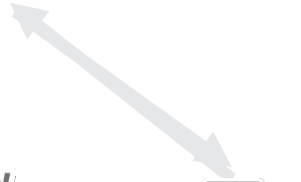
| | |
|---|---|
| Intelligence, Web Security | URL, File, IP |

# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

**RESPOND**

CENTRALIZED THREAT SHARING AND VISIBILITY

CUSTOM SANDBOX



ENDPOINT PROTECTION

MAIL SECURITY


WEB GATEWAY

HYBRID CLOUD SECURITY

| | | | |
|---|---|---|---|
| Deep Security | Action | URL, File | |




TREND MICRO

# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

**RESPOND**

CENTRALIZED THREAT SHARING AND VISIBILITY

CUSTOM SANDBOX

ENDPOINT PROTECTION

MAIL SECURITY


WEB GATEWAY

HYBRID CLOUD SECURITY


INTRUSION PREVENTION

| TippingPoint IPS | URL, File, IP, Domain |
|---|---|

# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

**RESPOND**

## CENTRALIZED THREAT SHARING AND VISIBILITY

CUSTOM SANDBOX

VISIBILITY AND CONTROL

| | |
|---|---|
| Control Manager | URL, File, IP, Domain, SHA |

ENDPOINT PROTECTION

MAIL SECURITY


WEB GATEWAY

HYBRID CLOUD SECURITY


INTRUSION PREVENTION

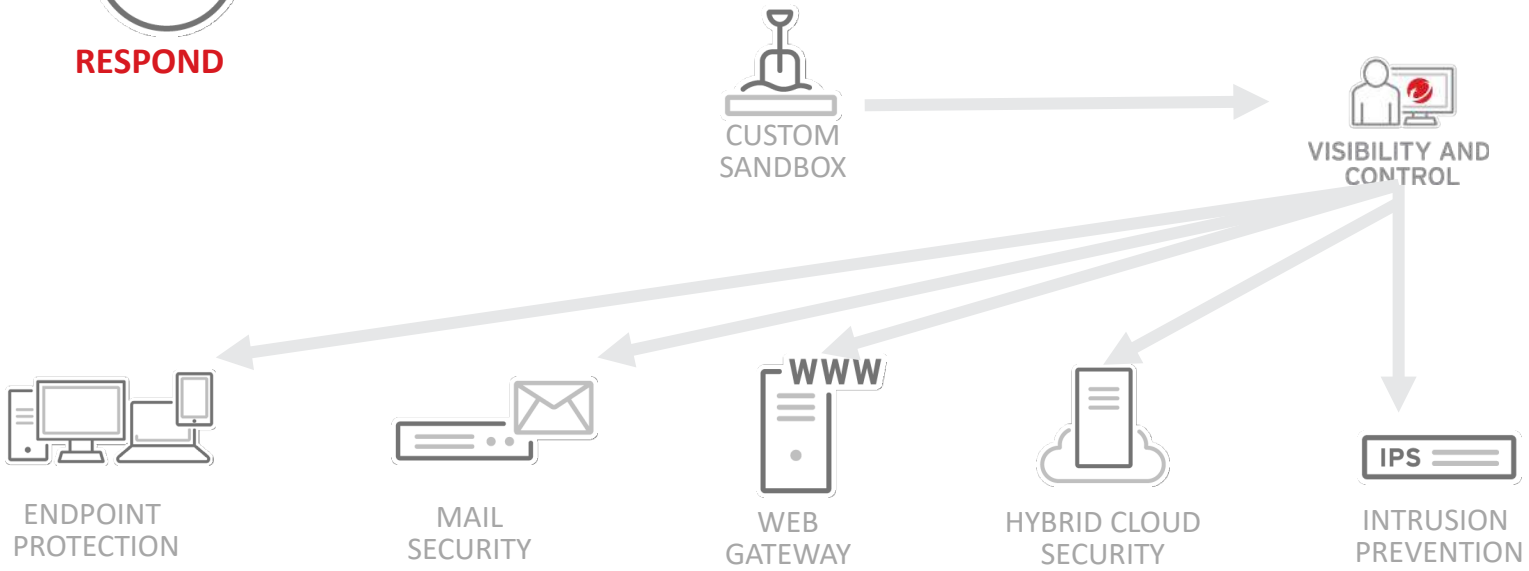



TREND MICRO

# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

**RESPOND**

## CENTRALIZED THREAT SHARING AND VISIBILITY

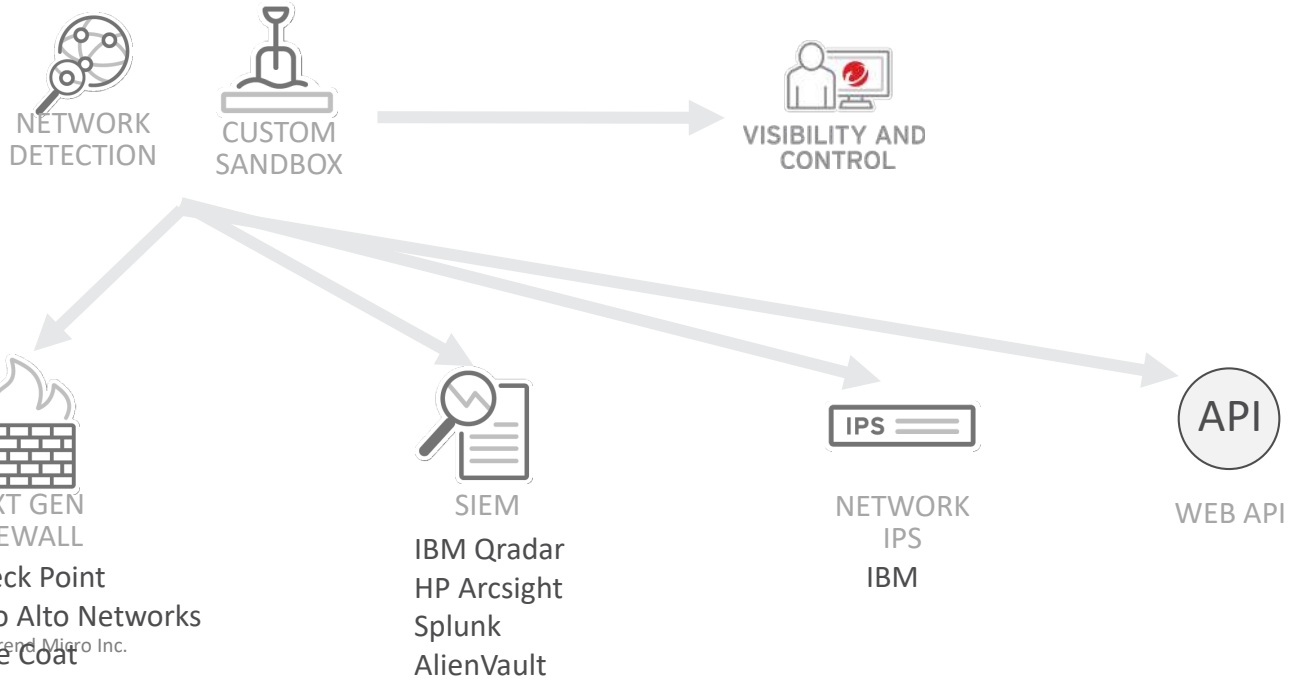


# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

**RESPOND**

## THIRD PARTY SHARING

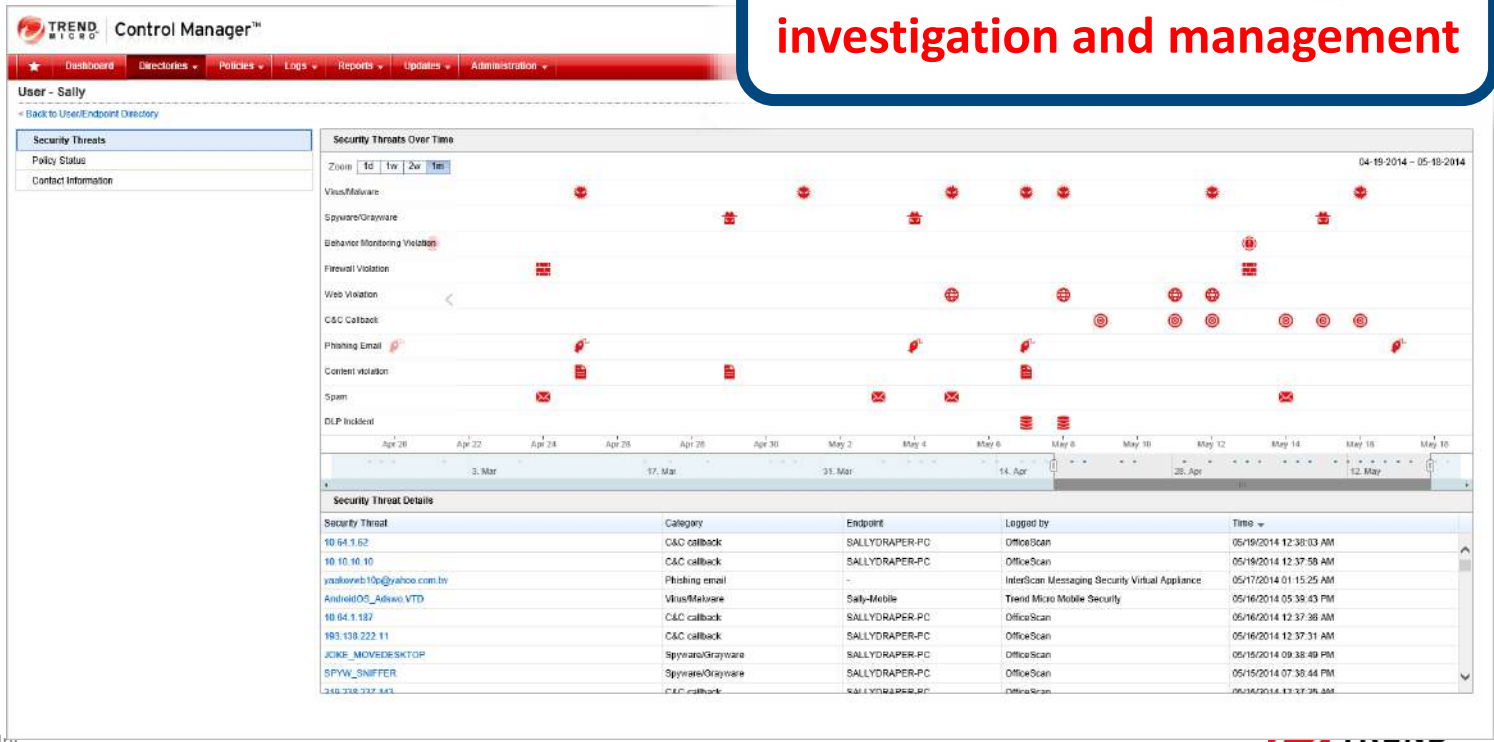
Threat Information can be shared with third party applications such as SIEMs, Firewalls, IPS and other applications via Web API

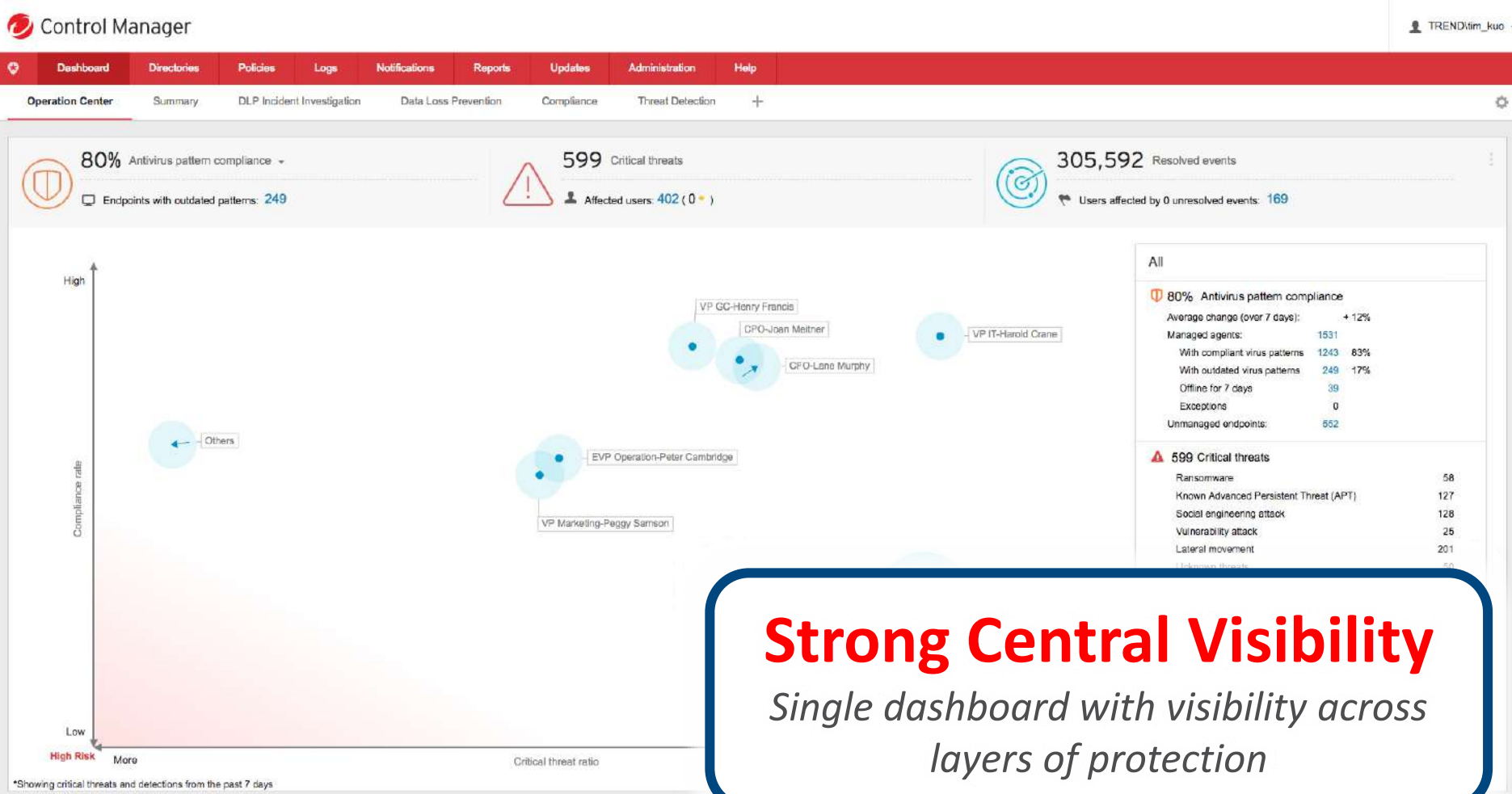


# Connected Threat Defense: Καλύτερη και Γρηγορότερη Προστασία

VISIBILITY AND CONTROL

**User-based visibility, investigation and management**






# Strong Central Visibility

*Single dashboard with visibility across layers of protection*

ManageEngine

Bringing IT together

# Seminar 2019

## Limassol

May 20, 2019

Atlantica Miramare

## Nicosia

May 21, 2019

Hilton Park Nic