(Cybercrime*Cryptolocker + Spie*APT)/ Datacenter * Hybrid cloud = AIUTOOOOO!

Alessio L.R. Pennasilico - apennasilico@clusit.it
Maurizio Martinozzi - maurizio_martinozzi@trendmicro.it

Security Summit
Milano - Marzo 2015

$whois -=mayhem=-

Security Evangelist @ 

Committed:

AIP Associazione Informatici Professionisti

CLUSIT, Associazione Italiana per la Sicurezza Informatica

IISFA, Italian Linux Society, Metro Olografix

Sikurezza.org, Spippolatori

....

Maurizio Martinozzi

Sales Engineering Manager @ 

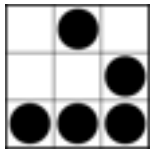
La vera sfida

Governare la complessità

nello scenario attuale


Rapporto
Clusit
2015
sulla sicurezza ICT
in Italia

#iosonopreoccupato



TREND MICRO

Buzzword

Clusit

Clusit Education

Cybercrime

Cryptolocker

Cyber Espionage

Hacktivism

“new” Vulnerabilities

APT

Big Data

Web / APP / ?

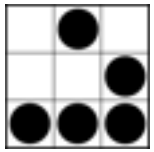
Ma come ci bucano davvero?

#iosonopreoccupato

#1bitcoin

Chi si potrà ancora permettere

di usare Internet?



Scenario

Perimetro?

Device?

Infrastruttura?

Dato!

Persone!

Cosa fare?

Strategia

è la descrizione di un piano d'azione di lungo termine

usato per impostare e successivamente coordinare le azioni

tese a raggiungere uno scopo predeterminato

http://it.wikipedia.org/wiki/Strategia

Strategia

si applica a tutti i campi in cui per raggiungere l'obiettivo

sono necessarie una serie di operazioni separate

la cui scelta non è unica e/o il cui esito è incerto

http://it.wikipedia.org/wiki/Strategia

Tattica

ha invece lo scopo di pianificare al meglio la singola azione

e deve tener conto di tutti i vincoli pratici e contingenti di essa

http://it.wikipedia.org/wiki/Strategia

Tattica vs Strategia

Cambiare tattica nel corso delle operazioni è normalmente possibile

senza grossi problemi, e anzi è spesso vantaggioso

per adattarsi a situazioni nuove o per ottenere la sorpresa sul nemico

http://it.wikipedia.org/wiki/Strategia

Sun Tzu

"Conosci il nemico,

conosci te stesso,

mai sarà in dubbio il risultato di 100 battaglie"

GRCI


Governance
Incident Management
Risk Management
Compliance

A world **safe** for exchanging digital information

CEO	Eva Chen
Founded	1988, United States
Headquarters	Tokyo, Japan
Employees	5,137
Offices	36
2012 Sales	$1.2B USD

New malware every ½ second

Global Threat Intelligence
- 1,200+ experts worldwide

96% of the top 50 global corporations.

100% of the top 10 automotive companies.

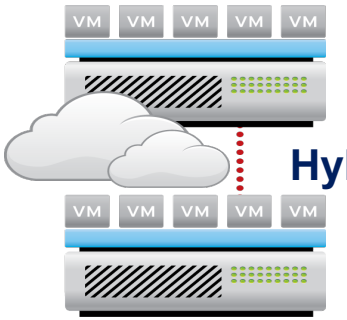
100% of the top 10 telecom companies.

80% of the top 10 banks.

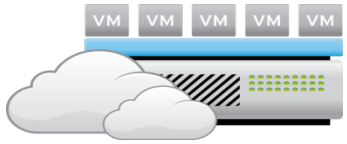
90% of the top 10 oil companies.

Sicurezza “Dato-centrica”

Big Data, dove?

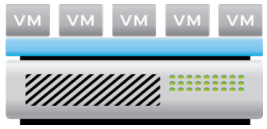


Hybrid Cloud



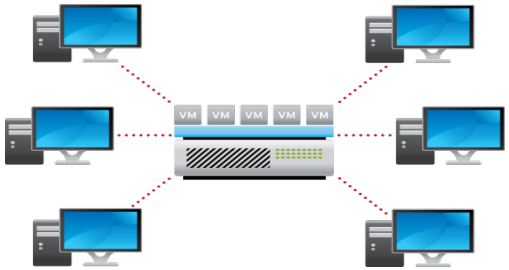
Public Cloud

BYOPC



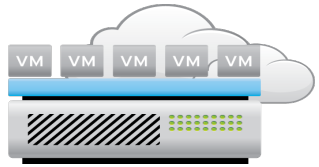
Server Virtualization

Physical Desktops & Servers



Desktop Virtualization

BYOD



Private Cloud

Cloud Computing

Virtualisation

Dynamic Data Center with
Shared System, Share Storage

Endpoint
Revolution

Highly Mobile Devices

Ubiquitous, Borderless
Data Access, Data Everywhere

Cloud Infrastructure

Cloud Application

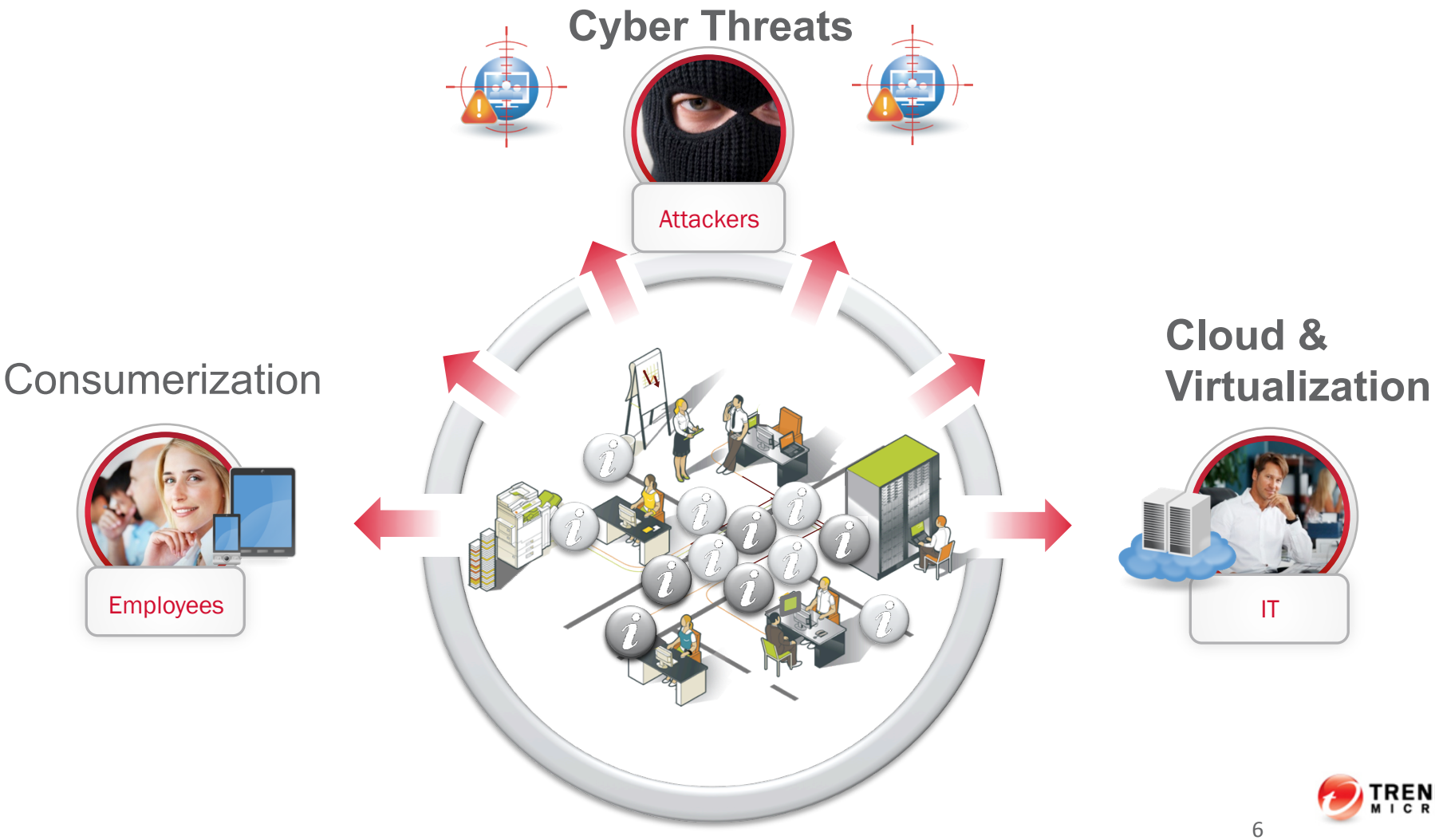
Shared Data Storage

Ownership of Data vs. Computing
Confidentiality & Access Control

Cloud Data

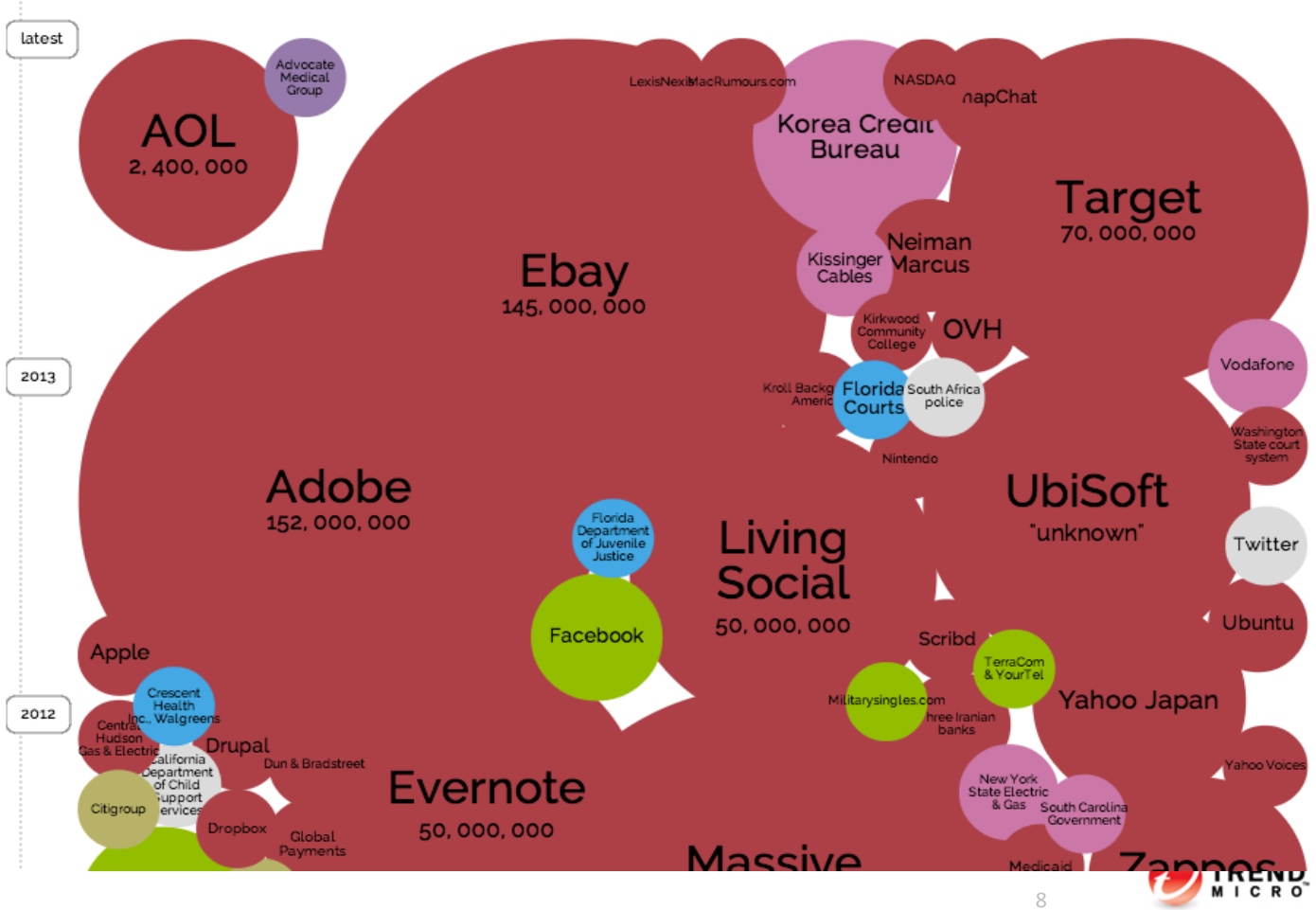
Application Platform

New Platform for New Apps.
Example,
Web Defacing, SQL Injection


Cyber Threats
Attackers
Consumerization
Employees
Cloud &
Virtualization
IT

Che sta succedendo ?

World's Biggest Data Breaches: Most are Hacks



Source:
www.informationisbeautiful.net

Minacce sofisticate

Web Apps obiettivo primario del cybercrime

Web Applications are a favorite target for attackers[1]

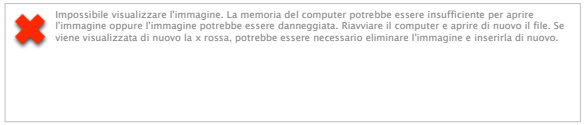
1. Easy to develop exploits
2. High potential value of data

600k+ web servers affected by the Heartbleed vulnerability

SANS

Top 20 Critical Controls
Application Software Security
(known initial entry point for attacks)

Top 10 Web App Security Risks



TREND MICRO

11

- il 60% di attacchi informatici è cybercrime

Hacktivism il 27%, l'espionage l'8% e la cyber warfare il 5%

- Colpiti i siti GOV, News, Banche
- Health e Pharma, incremento del 190% rispetto al 2013
- Attacchi Ransomware in aumento

Fonte: Rapporto Clusit 2015

POLIZIA DI STATO
UNITÀ DI ANALISI SUL CRIMINE INFORMATICO

È STATA RIVELATA UN'ATTIVITÀ ILLEGALE. IL SISTEMA OPERATIVO È STATA BLOCCATA PER UNA VIOLENZA DELLE LEGGI DELLA REPUBBLICA ITALIANA!
È STATA FISSATA UNA SEGUENTE VIOLAZIONE: DAL TUO INDIRIZZO IP "93.32.168.148" ERA ESEGUITO UN ACCESSO ALLE WEB-PAGINE CONTENENTI LA PORNOGRAFIA, LA PORNOGRAFIA MINORILE, ZOOFILIA, NONCHÉ LA VIOLENZA DEI BAMBINI.

L'ANNO	GIORNO	MESE	ALLE ORE	REATO / CRIMINE
2012	31	05	19.44	CRIMINE INFORMATICO

INDIRIZZO IP	LOCALIZZAZIONE	DEL BROWSER
[illegible]	MILAN	IE9

LE VIOLAZIONI DELLE NORME INTERNAZIONALI DI FUNZIONAMENTO DI INTERNET
ITC-BZXCCDD/FF

Nel tuo computer sono stati trovati video-file contenenti la pornografia, elementi di violenza e la pornografia minorile.
Dalla posta elettronica era effettuato anche la distribuzione dello spam con un senso recondito terroristico.
Il bloccaggio di computer serve per troncare l'attività illegale dalla parte tua.

Per togliere il bloccaggio devi pagare una multa di 100 euro.
Hai due seguenti varianti di pagamento:
1) Effettuare il pagamento tramite l'Ukash.
Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché premi "Pagare una multa" (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi "Pagare una multa")

Ukash or paysafecard

Puoi richiedere e ottenere Ukash presso migliaia di punti vendita, edicole, stazioni di servizio, bar e tabacchi e negozi di telefonia mobile dotati di terminale Epay, Epipoli.
Paysafecard è disponibile in tutta sicurezza vicino a te in Italia, ad esempio presso numerose edicole, bar, tabaccai anche nei negozi Sisal e Penny.

epay PayMat Bitcard EPIPOLI

MICRO

Come operare “in Sicurezza”

Le criticità

TREND MICRO | Securing Your Web World

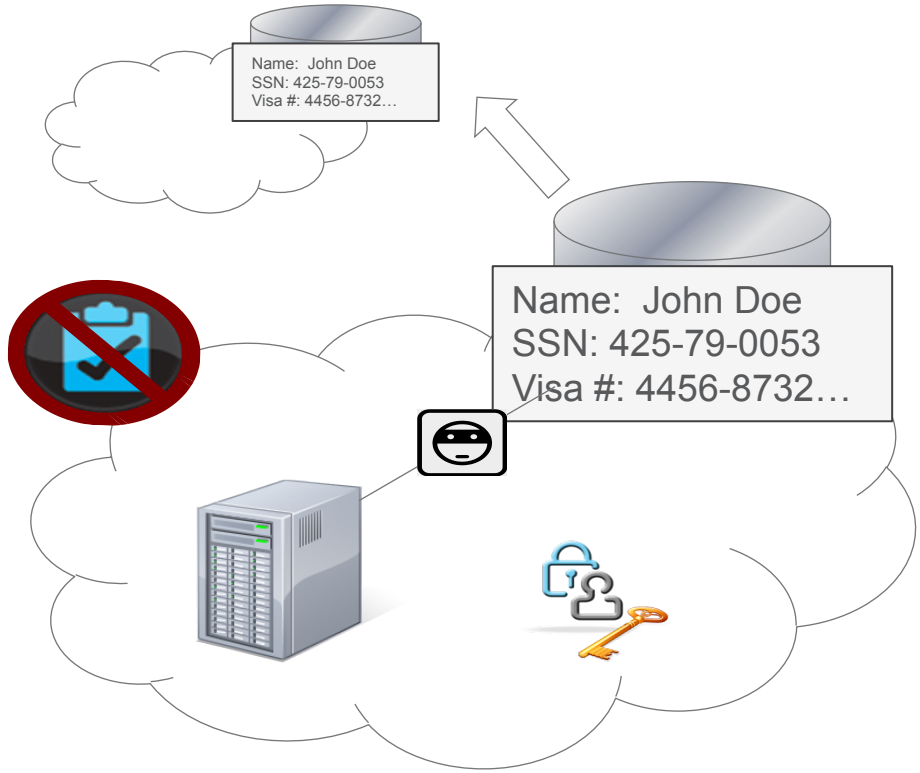
Cosa chiedo all'ISP?
- offerta
- definizione e mantenimento degli SLA
- privacy

Sicurezza dei dati contro:
- Vulnerabilità, perdita, danneggiamento e sono I tuoi dati? Sono stati rimossi?
- Acquisizione/fusione provider??

La Crittografia è usata raramente:
- Chi può vedere le tue informazioni?

- Server possono accedere ai dati:
- Chi si sta connettendo al tuo storage?

Necessità di una sicurezza esclusiva in infrastrutture condivise



15

TREND MICRO

Le criticità

- Le nuove tecnologie/piattaforme moltiplicano le vulnerabilità e le opportunità di successo per il cybercrime

- L'elemento umano è fondamentale: un utente può essere usato come testa di ponte e fornire accesso involontario per un attacco

- La protezione perimetrale non è più idonea a garantire un adeguato livello di protezione. L'approccio "datocentrico"' è la chiave per una maggior sicurezza.

Quindi?

E’ necessario aumentare Il livello di sicurezza

- Intensificare il controllo relativo al patching
- Educare gli utenti con campagne di formazione – insegnare le vulnerabilità ----
- Verificare i processi di sicurezza
- Aggiornare sistematicamente le tecnologie di sicurezza

http://us.trendmicro.com/us/trendwatch/vision/index.html

Il “cuore” dell’attività:
il SDDC (Software Defined Datacenter)

Standard Defenses are Insufficient

- Advanced reconnaissance
- Spear-phishing emails
- Embedded payloads
- Unknown malware & exploits
- Dynamic command and control (C&C) servers
- BYOD and remote employees create a broad attack surface

Next-gen Firewall

Intrusion Detection (IDS)

Intrusion Prevention (IPS)

Traditional AV

Email /Web Gateways

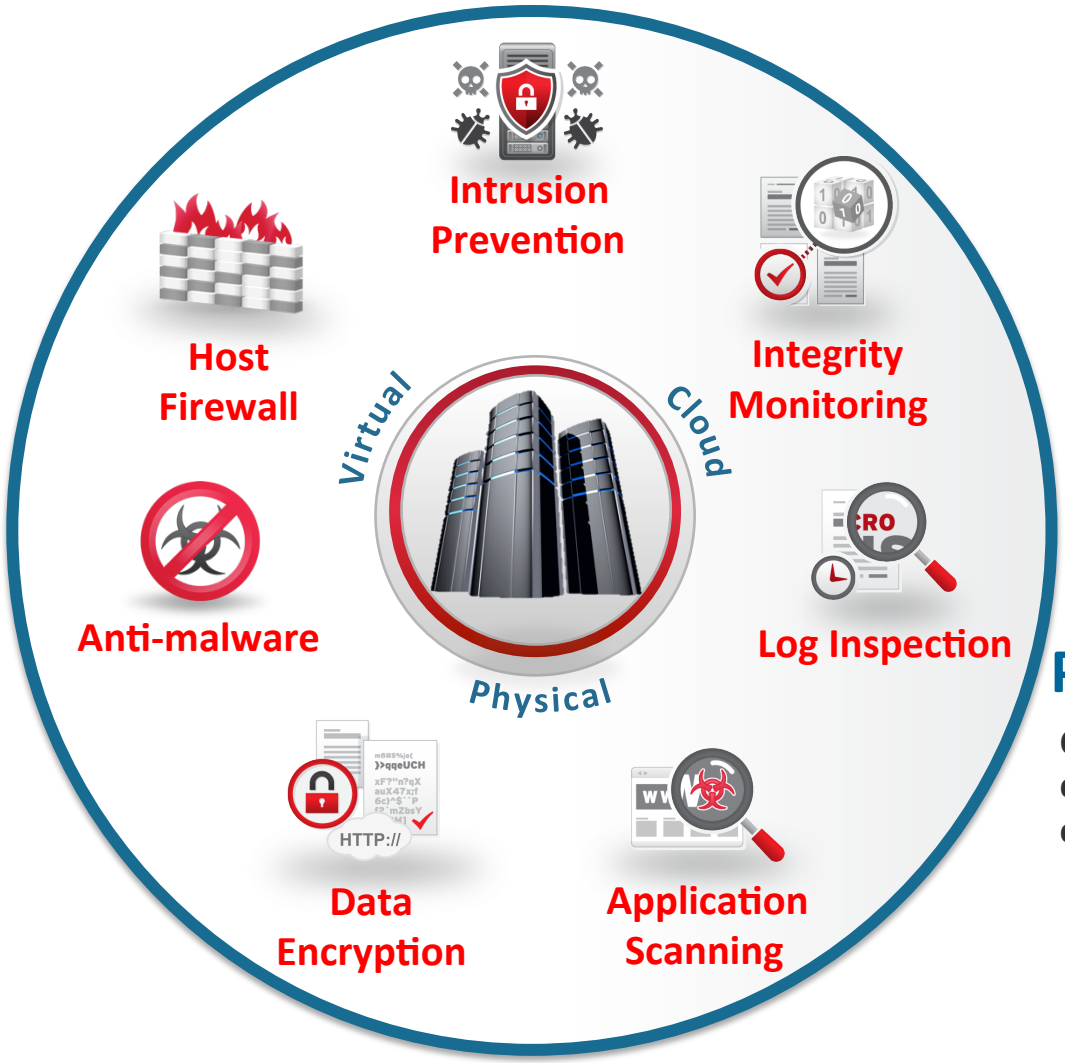
TREND MICRO

ADAPTIVE

Intelligent, dynamic provisioning & policy enforcement

CONTEXT

Workload & application-aware



SOFTWARE

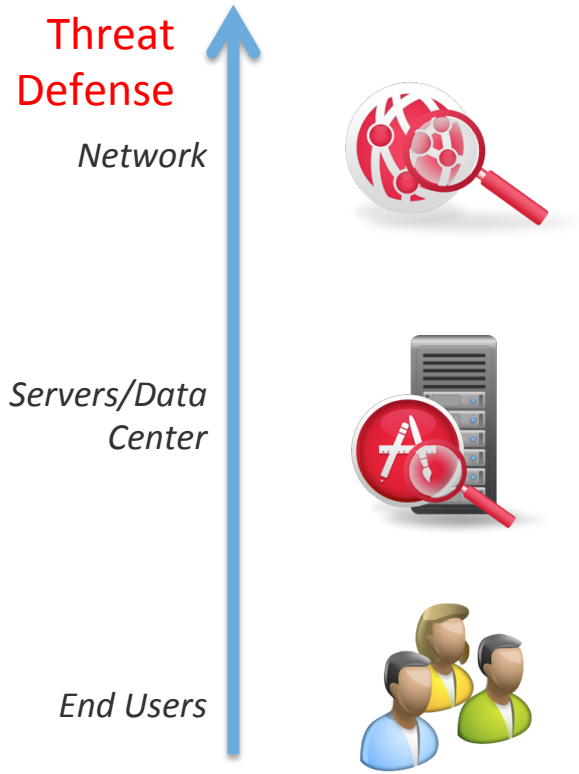
Optimized for virtualization & cloud infrastructure

PLATFORM

Comprehensive capabilities across data center & cloud

TREND MICRO

Next Generation Threat Defense
…Across Every Layer

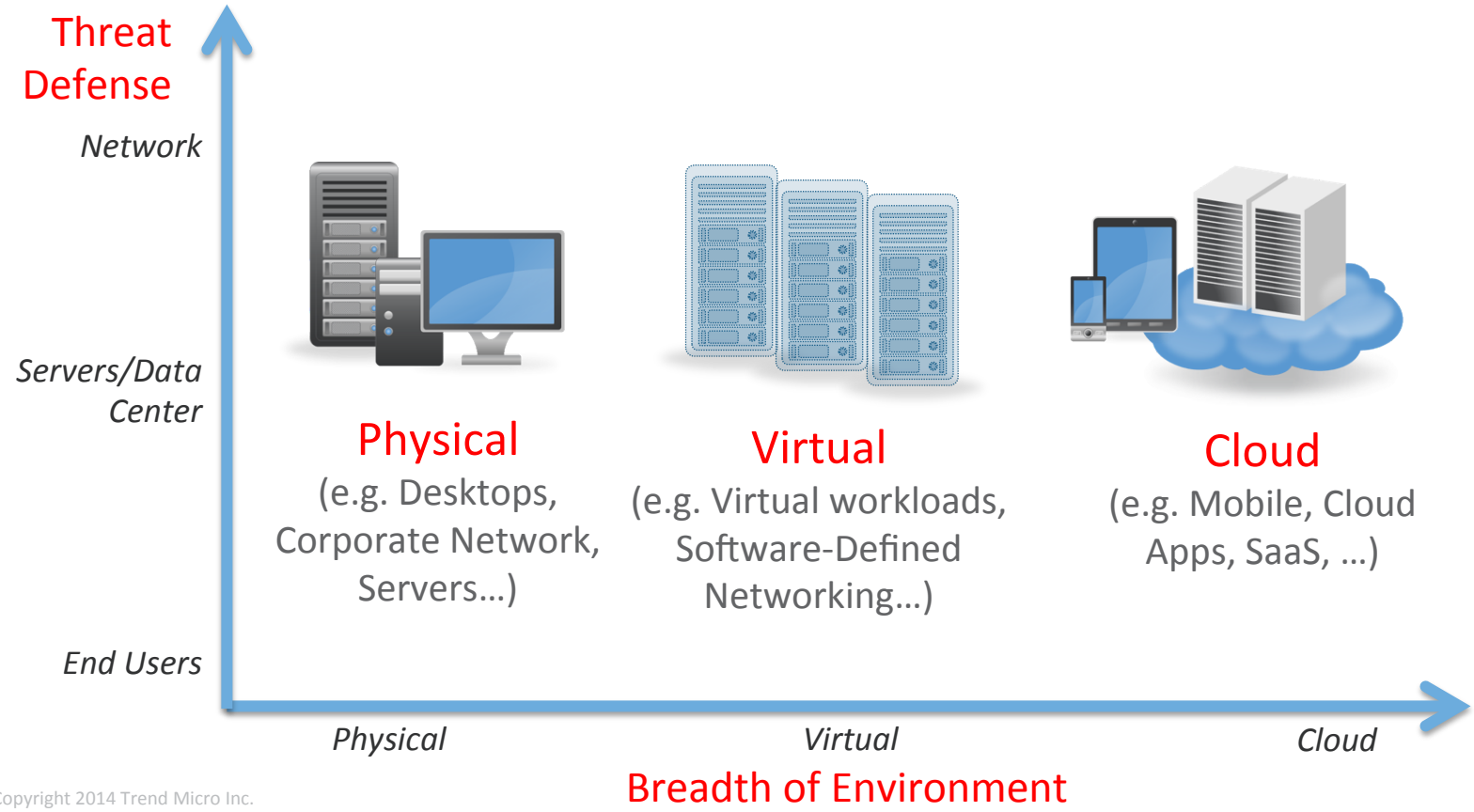


Network Threat Defense
Sandboxes
Lateral movement detection of threats
User-awareness

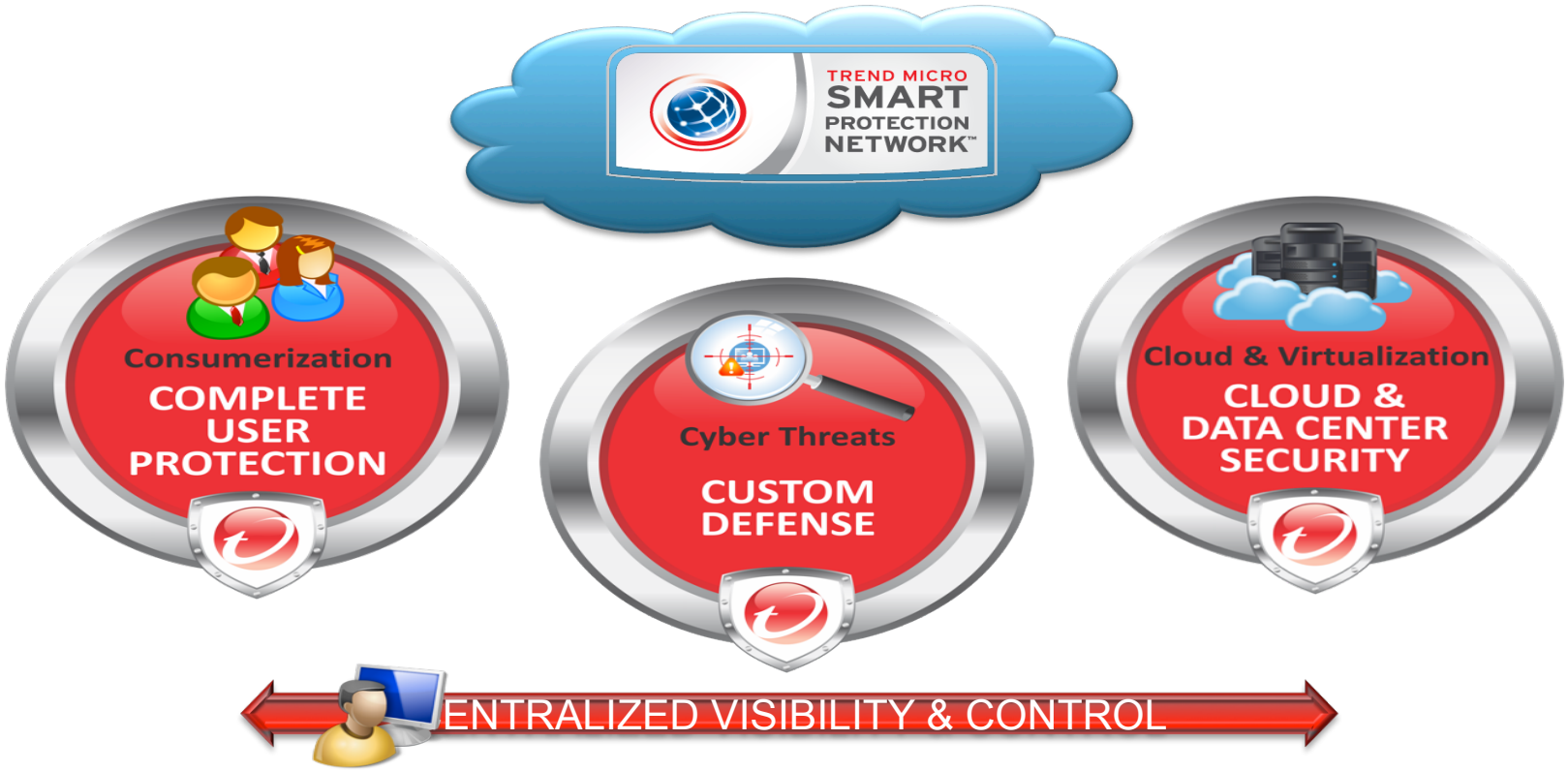
Server and Data Center Defense
Application-specific protection
Virtual/cloud awareness and optimization
Data access control (identity-based encryption)

End User Defense
Indicators of Compromise (IOC)
Contextual awareness
Big data analysis for correlation

Next Generation Threat Defense
…Across the Breadth of Environments



Detect , Analyze, Adapt, Respond



Conclusioni

#iosonopreoccupato

Dato!

Persone!

Tattica!

Strategia!

GRCI


Governance
Incident Management
Risk Management
Compliance

Grazie dell'attenzione!

Domande?

Alessio L.R. Pennasilico - apennasilico@clusit.it
facebook:alessio.pennasilico - twitter:mayhemspp - linkedin:alessio.pennasilico

Maurizio Martinozzi - maurizio_martinozzi@trendmicro.it