



# Il Content Security dall'ambiente fisico al virtuale : come approcciare le nuove sfide ?

Alessio L.R. Pennasilico - [apennasilico@clusit.it](mailto:apennasilico@clusit.it)  
Gastone Nencini - [gastone\\_nencini@trendmicro.it](mailto:gastone_nencini@trendmicro.it)



**Security Summit**  
**10 Giugno 2010**  
**SGM Conference Center, Roma**

*Clusit*  
*Education*

# Alessio L.R. Pennasilico

Security Evangelist @  Albast

## Board of Directors:

Associazione Informatici Professionisti

Associazione Italiana Professionisti Sicurezza Informatica

CLUSIT

Italian Linux Society, LUGVR, Metro Olografix, Sikurezza.org

Hacker's Profiling Project, CrISTAL

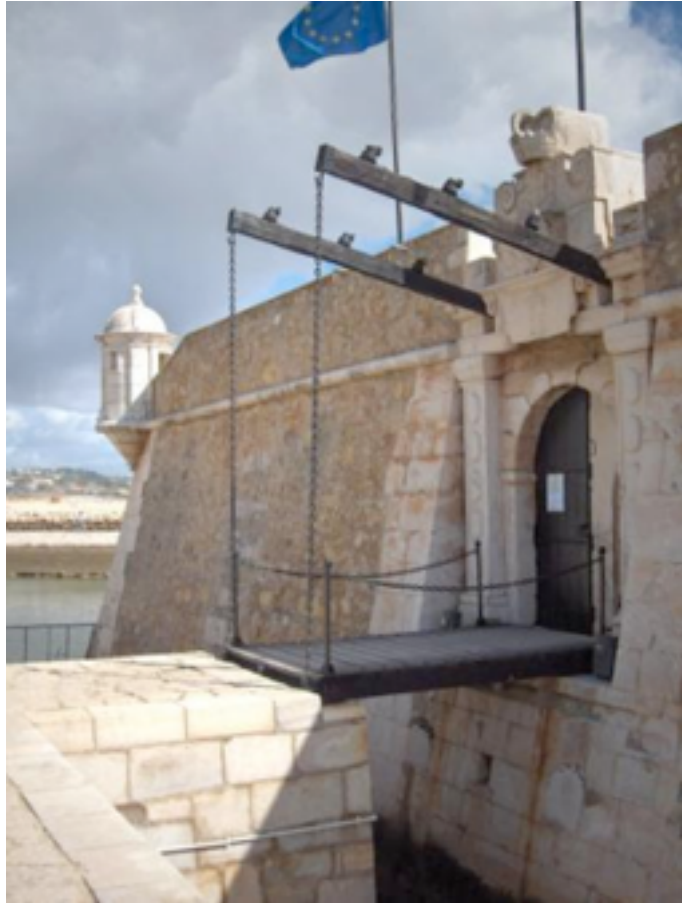
# Gastone Nencini

Senior Technical Manager  
South Europe



**TREND**  
M I C R O™

# IT Security...



Un inutile impedimento  
che rallenta le comuni operazioni  
e danneggia il business?

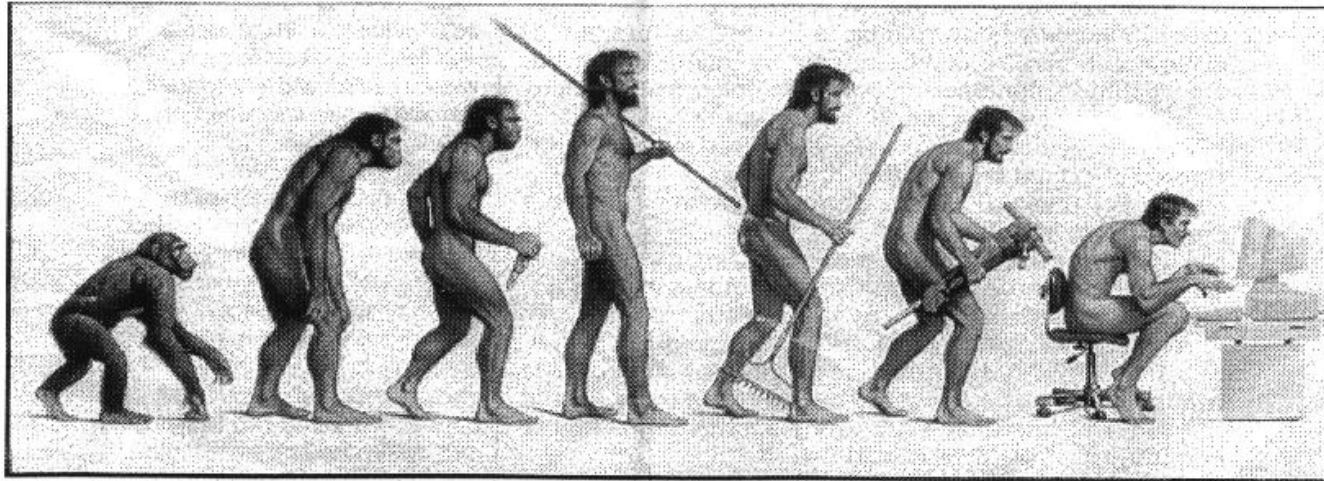
# IT Security...



○ prevenzione e risposta ad eventi che danneggerebbero il business in modo peggiore?

# Evoluzione

La tecnologia si evolve...



**Somewhere, something went terribly wrong**

... e con essa anche le minacce!

# Content Security

SPAM/SPIT  
Phishing/Vishing  
Malware  
Botnet  
WebThreats  
DDOS

# Malware

Virus  
Worm  
Keylogger  
Trojan  
Dialer?  
Spyware  
Backdoor

# Navigazione

Queste minacce possono essere inconsapevolmente scaricate in maniera attiva dagli utenti

Oppure possono essere infettati i client utilizzando vulnerabilità note

# Minacce classiche

Software Vulnerability Exploits  
Patch Management  
Web Application Threats  
Policy & Compliance  
System & Data Integrity

# Perché virtualizzare?

Administrative overhead

Risparmio sui consumi

Scalabilità

Flessibilità

Disaster recovery facilitato

# Virtualizzazione

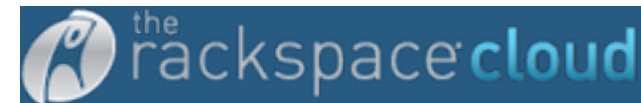
PHYSICAL SERVERS

VIRTUALIZED SERVERS

CLOUD COMPUTING



Amazon Elastic Compute Cloud



# Security

Cosa cambia?

# HyperVisor

## **Tipo 1** (bare-metal, nativo)

Eseguito direttamente sull'hardware del sistema  
es: iSeries, zSeries, VMWare ESX, XEN

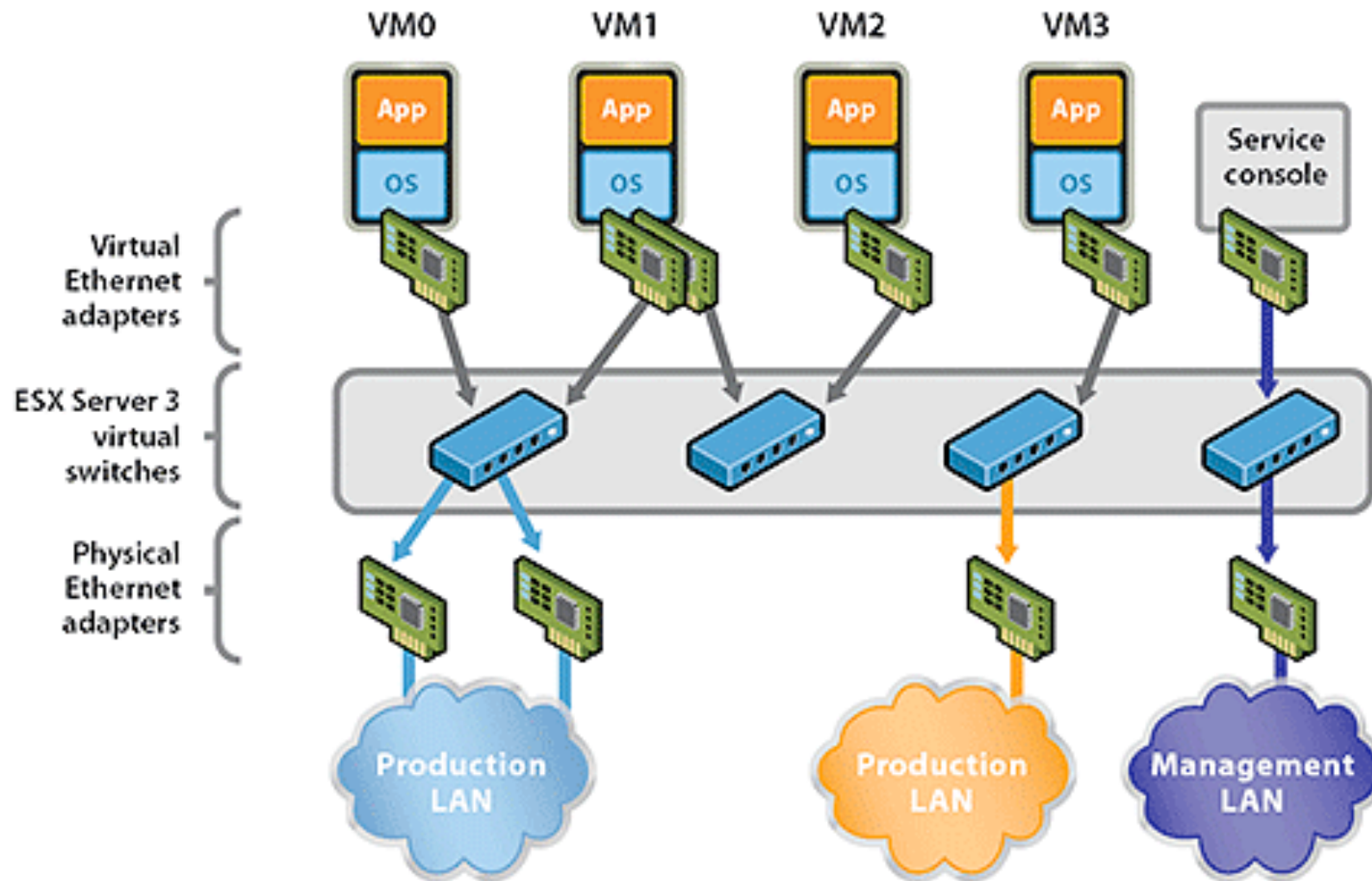
## **Tipo 2** (hosted)

Eseguito sul "normale" sistema operativo  
es: VMWare Server, Parallels Desktop

# Parent exploit

Alcune vulnerabilità di prodotti di virtualizzazione permettono di prendere possesso dell'host a partire da una VM

# Reti “Virtuali”



# Firewall

Serve

Non difende da tutto e da tutti

Quello di frontiera non deve essere virtualizzato

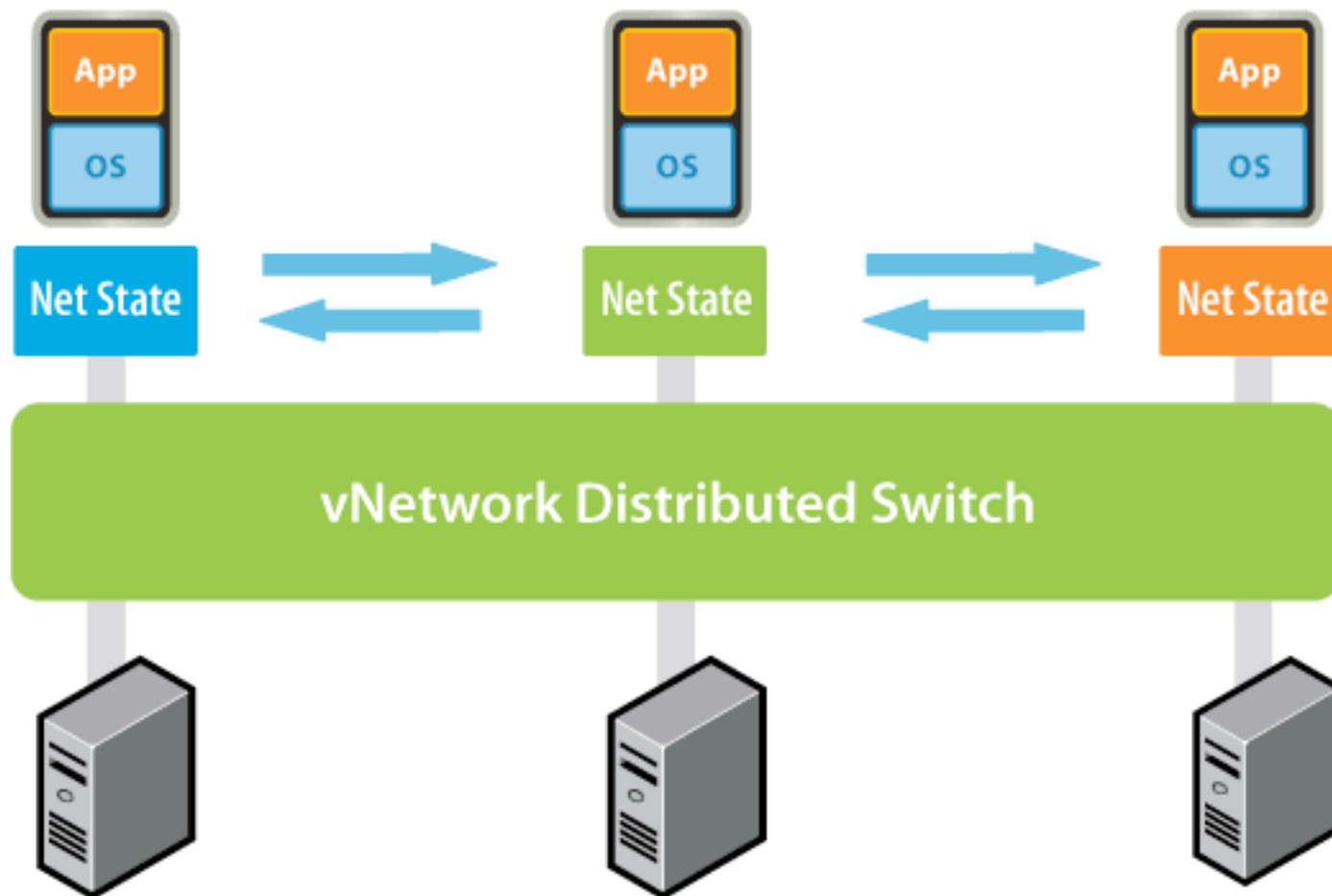
Possono esistere firewall virtuali per segmentare

# Perimetro

Quale è il perimetro dell'azienda?

WiFi - VPN - Laptop - SmartPhone

# Configurazioni comuni



# VoIP

Traffico Real Time (continuity)  
Traffico prioritizzato (QoS)

# Inter-VM traffic

Chi controlla questo traffico?

*Porte di monitor fisiche vs virtuali*

# vMotion

Alcuni PoC hanno dimostrato la possibilità di  
manipolare le VM

durante le live-migration

# VM Sprawl



Security weaknesses replicate quickly  
Security provisioning creates bottlenecks  
Lack of visibility into, or integration with, virtualisation  
console increases management complexity

# Dormant VMs

Template e Backup

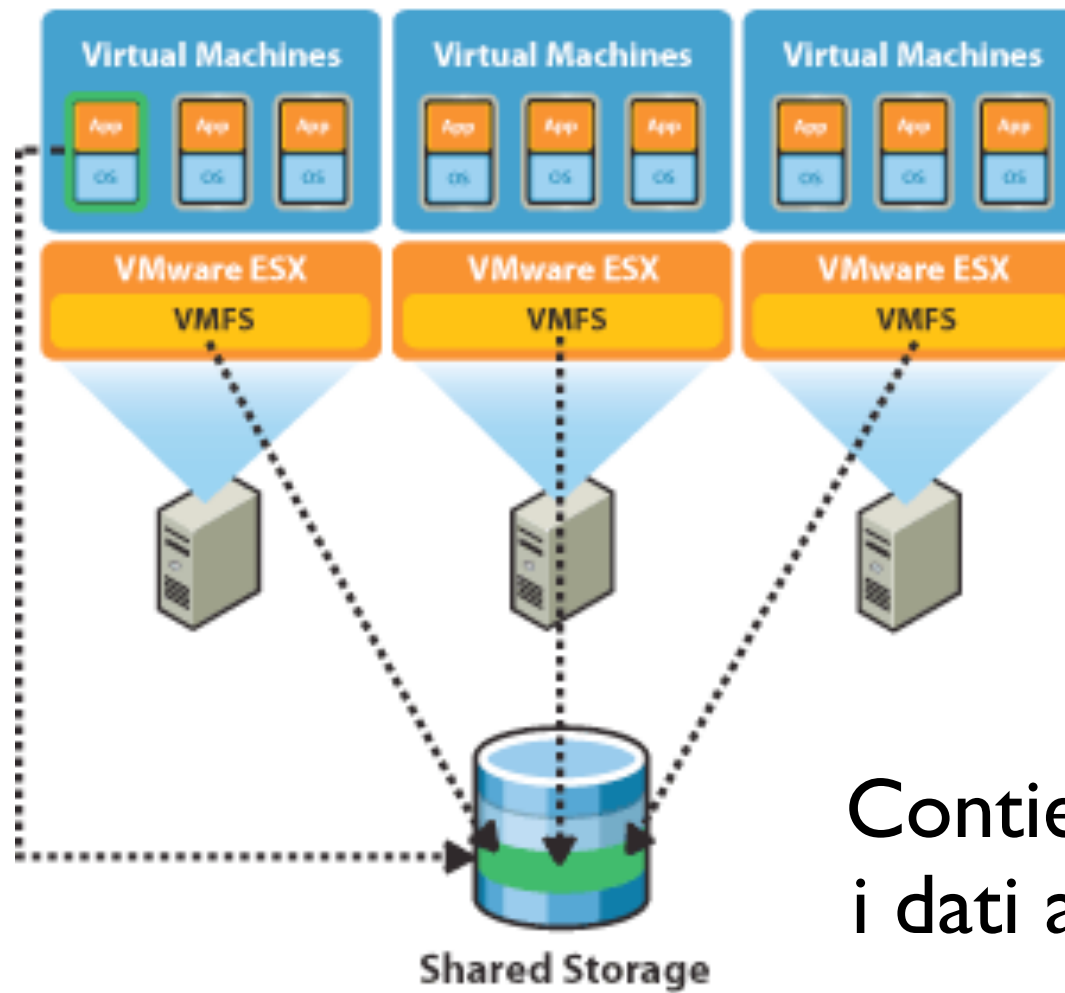
Non ci sono agent attivi / possono essere infettate

Firme di IPS/Antivirus obsolete

Malware VM-aware

Nessun isolamento tra anti-malware e minacce

# Storage



Contiene *tutti*  
i dati aziendali

# Data Loss Prevention

Perdita di dati dovuta ad infezione / intrusione accidentale o pilotata (competitor/disgruntled)

E' solo la non disponibilità il problema?

# Social Engineering

Non importa il vettore  
(mail, chat, social network)

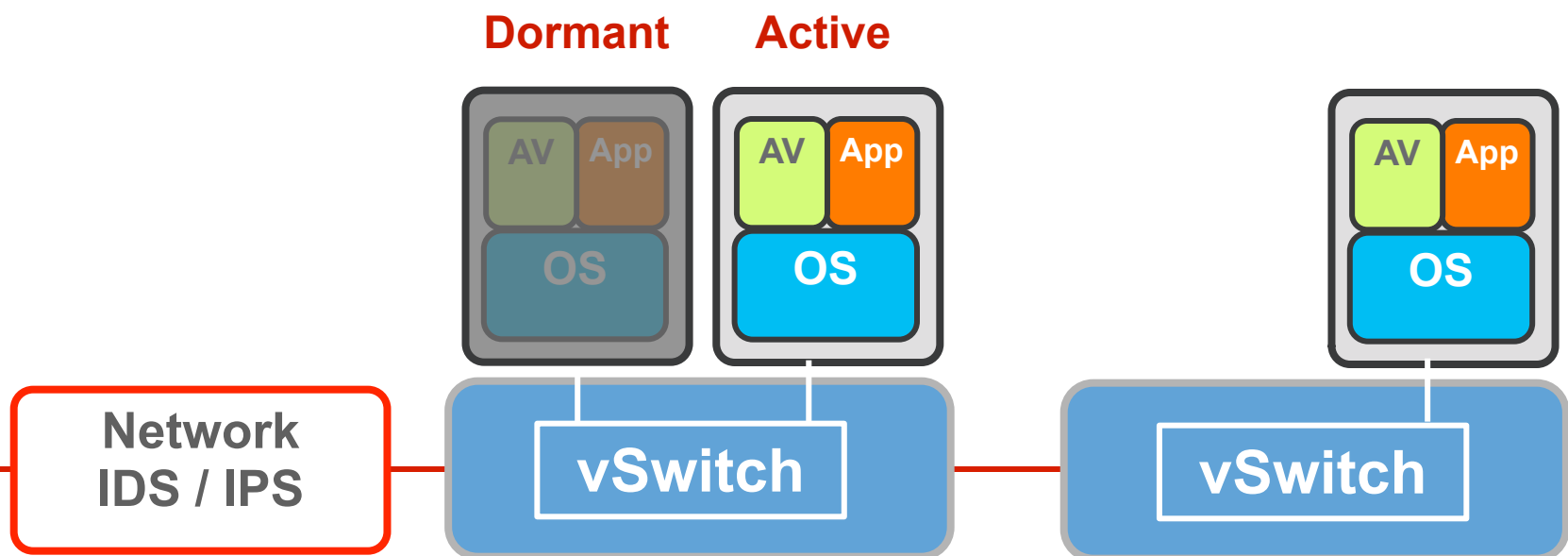
Basta convincere l'utente a rilasciare alcune  
informazioni riservate

# Resource contention

Eseguire contemporaneamente su troppe macchine operazioni onerose può causare gravi problemi di performance

Antivirus / Backup / Scan

# VM Mobility



## vMotion & vCloud:

Reconfiguration required: cumbersome  
 VMs of different sensitivities on same server  
 VMs in public clouds (IaaS) are unprotected

# Patch

Gestione puntuale  
Gestione automatica

Problemi automatici?

Virtual patching  
Host patching

# Piattaforme

Molti OS diversi tra loro

Necessità di uno strumento unificato

# Gestione integrata

Infrastrutture complesse

Gestione complessa?

# Minacce?

“34% of all data breach attacks exploited Web applications”

*Verizon*

“75% of attacks take place at the application layer”

*Gartner*

# Compliance

PCI Requirement Area		Trend Micro Enterprise Solutions				
		Endpoint Security	Web Security	Messaging Security	Threat Management Services	
Build & Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data	●	●			★
	2. Do not use vendor supplied defaults...(shared hosting providers)	●	●	●		
Protect Cardholder Data	3. Protect stored cardholder data	●		●		★
	4. Encrypt transmission of cardholder data across open, public networks	●		●		★
Maintain a Vulnerability Protection Program	5. Use and regularly update antivirus software or programs	●	●	●	●	★
	6. Develop and maintain secure systems and applications	●	●		●	★
Implement Strong Access Measures	7. Restrict access to data					
	8. Assign unique IDs					
	9. Restrict physical data access					
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	●	●			
	11. Regularly test security systems and processes	●	●		●	
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors	●	●	●		

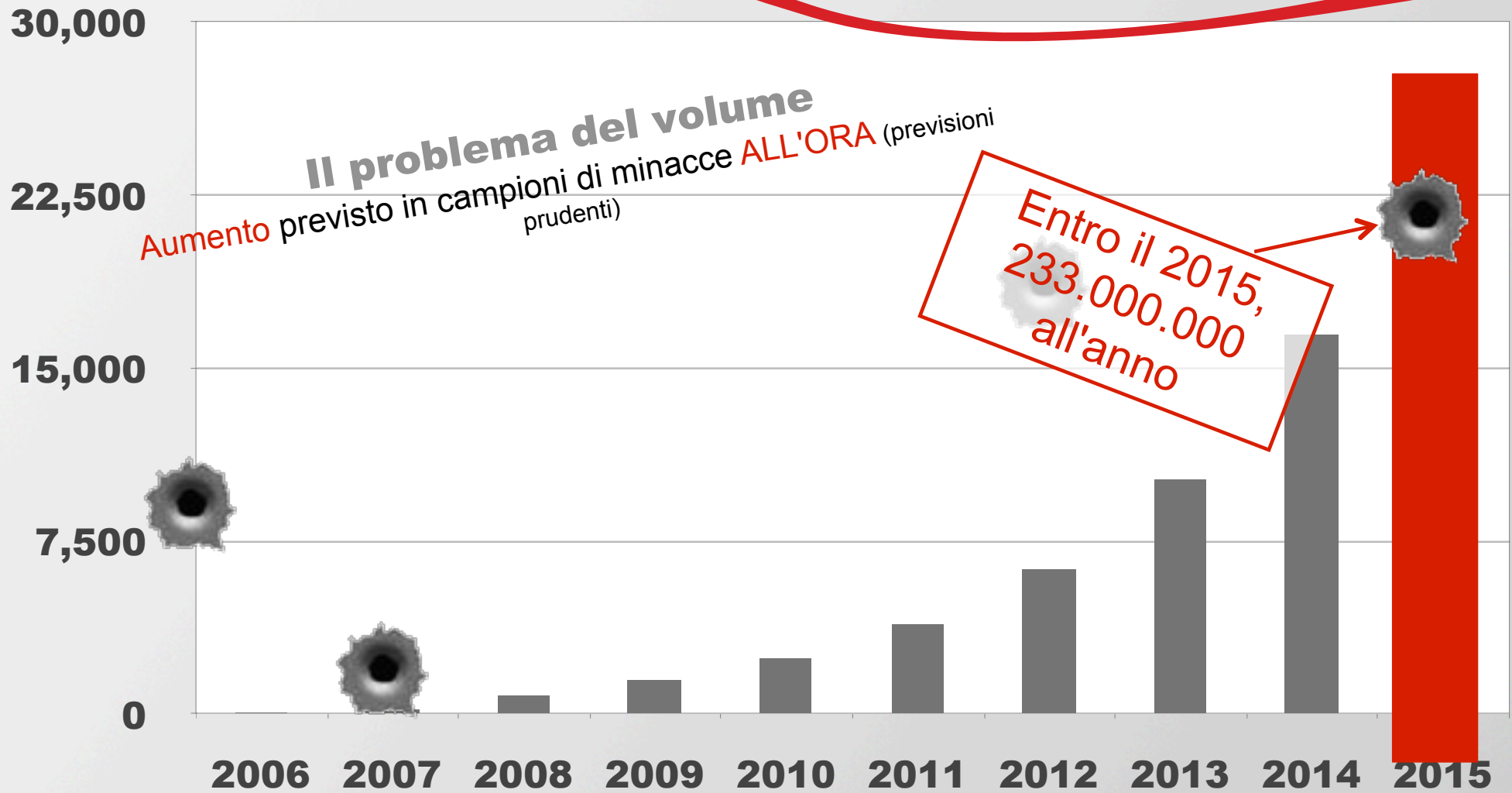
PCI/DSS

# Perché compliance?

81% delle intrusioni avvengono su reti che non soddisfano i requirement delle più diffuse norme/best practice / guidelines

*Gartner*

# Minacce previste



# Conclusioni

Le minacce da affrontare sono molte e spesso non banali da gestire

La tecnologia supporta il lavoro del CSO

Purtroppo si rende sempre necessario fare “hardening” del personale oltre che delle macchine

# Web-o-Grafia

<https://securecloud.com/>

<http://blog.trendmicro.com/>

<http://www.vmware.com/>

<http://www.eecs.umich.edu/techreports/cse/2007/CSE-TR-539-07.pdf>

<http://www.cisco.com/go/securityreport>

<http://www.alba.st/presentazioni.php>



These slides are written by Alessio L.R. Pennasilico aka mayhem. They are subjected to Creative Commons Attribution-ShareAlike-2.5 version; you can copy, modify, or sell them. "Please" cite your source and use the same licence :)



# Grazie dell'attenzione!

## Domande?

Alessio L.R. Pennasilico - [apennasilico@clusit.it](mailto:apennasilico@clusit.it)  
Gastone Nencini - [gastone\\_nencini@trendmicro.it](mailto:gastone_nencini@trendmicro.it)



**Security Summit**  
**10 Giugno 2010**  
**SGM Conference Center, Roma**

*Clusit*  
*Education*