



**LANline//Events**  
»Experten im Dialog mit Ihnen«



## **The seven sisters wearing the emperor's new clothes**

On the changing role of  
fundamental network security  
principles in the age of  
virtualization and cloud computing

*Enno Rey, [erey@ernw.de](mailto:erey@ernw.de)*

# ERNW GmbH

- **Heidelberg based security consulting and assessment company with currently 18 employees (as of Nov 2010).**

- Independent
- Deep technical knowledge
- Structured (assessment) approach
- Business reasonable recommendations
- We understand corporate



- **Blog: [www.insinuator.net](http://www.insinuator.net)**
- **Conference: [www.troopers.de](http://www.troopers.de)**



# Agenda

---

- **Bad things that can happen in virtualized environments**
- **The role of current security controls in the age of virtualization (and *the cloud*)**
- **Trust & Control – Applying a new security paradigm**



# Gartner on Security Risks in Data Center Virtualization Projects



- ***Gartner Research Report G00173434, published 01/25/2010***
  
- **Main risks as of this report**
  - Information Security Isn't Initially Involved in the Virtualization Projects
  - A Compromise of the Virtualization Layer Could Result in the Compromise of All Hosted Workloads
  - The Lack of Visibility and Controls on Internal Virtual Networks Created for VM-to-VM Communications Blinds Existing Security Policy Enforcement Mechanisms
  - Workloads of Different Trust Levels Are Consolidated Onto a Single Physical Server Without Sufficient Separation
  - Adequate Controls on Administrative Access to the Hypervisor/VMM Layer and to Administrative Tools Are Lacking
  - There Is a Potential Loss of SOD for Network and Security Controls
  
- **Full report available at Gartner, for a fee. Summary here:**  
<http://security.tekrati.com/research/10810/>



# A Compromise of the Virtualization Layer Could Result in the Compromise of All Hosted Workloads

- In quite some discussions about virtualization security, this is “the big one”.
- The *risk is not* the same for all virtualization solutions.
- At least in VMware ESX space this *has* happened in the past.



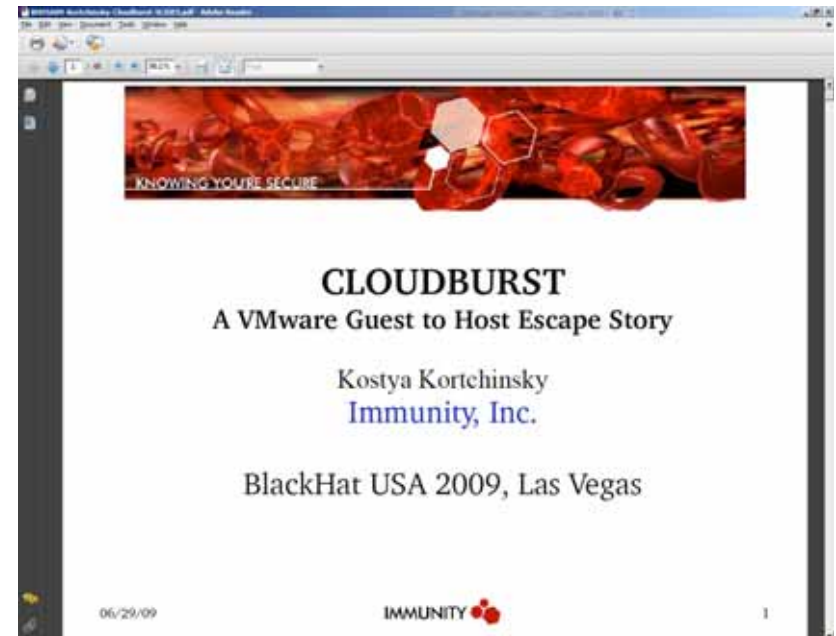
# Workloads of Different Trust Levels Are Consolidated Onto a Single Physical Server Without Sufficient Separation

- This is an interesting one... as it contains a (pre-) judgement.
- That is: “mixing security levels on one platform is a bad thing”.
- Is it?
- If so why?
- This is related to some of the others.
- Still, in the end of the day “it’s all about risk...”.



# A side note on Cloudburst

- **Full guest → host escape on VMware ESX**
  - Call it “full [ESX] host compromise by guest attacker”, for that matter.
- **Initially shown at BH US 2009**
- **Illustrates some potential (real) problems of VMware ESX.**
- <http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf>



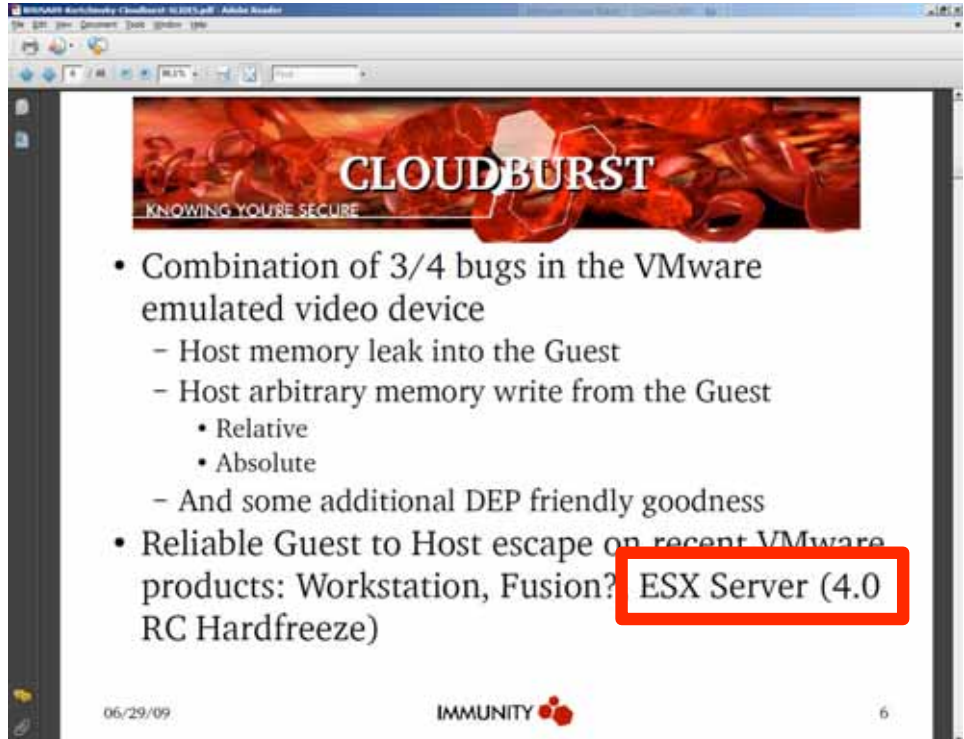
# Devices ... and their use for attacks



**Why devices?**  
KNOWING YOU'RE SECURE

- I don't have enough low-level system Moio ☹
- They are common to all VMware products
- They run on the Host
  - vmware-vmx process
- They can be accessed from the guest
  - Through Port I/O or memory-mapped I/O
- They are written in C/C++
- They sometimes parse some complex data!

06/29/09 IMMUNITY 4

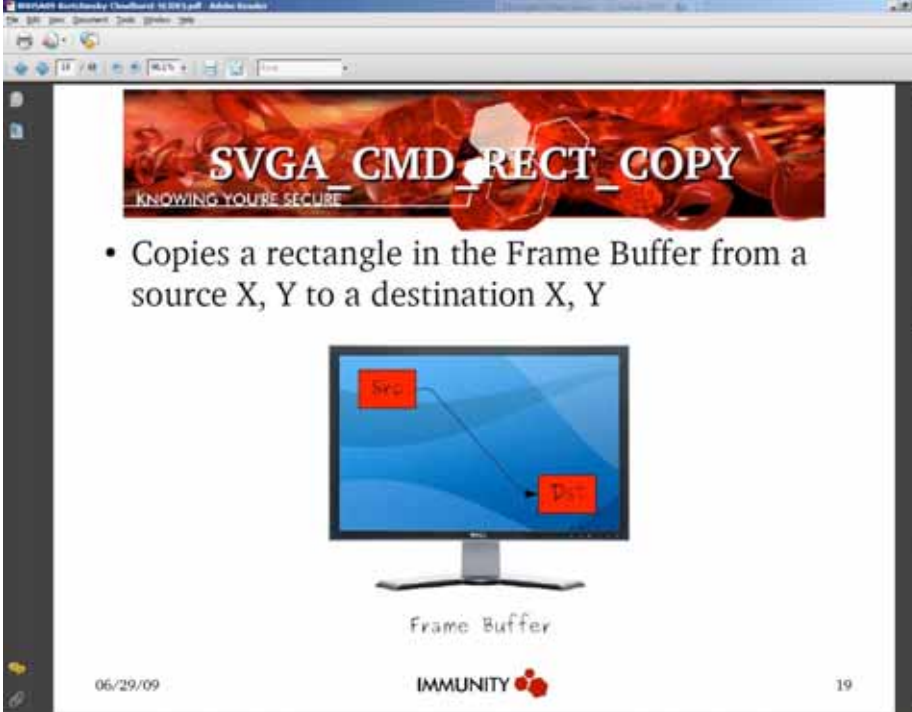


**CLOUDBURST**  
KNOWING YOU'RE SECURE

- Combination of 3/4 bugs in the VMware emulated video device
  - Host memory leak into the Guest
  - Host arbitrary memory write from the Guest
    - Relative
    - Absolute
  - And some additional DEP friendly goodness
- Reliable Guest to Host escape on recent VMware products: Workstation, Fusion? **ESX Server (4.0 RC Hardfreeze)**

06/29/09 IMMUNITY 6

# Rectangles ...




SVGA\_CMD\_RECT\_COPY  
KNOWING YOU'RE SECURE

- Copies a rectangle in the Frame Buffer from a source X, Y to a destination X, Y

Frame Buffer

06/29/09 IMMUNITY 19



SVGA\_CMD\_RECT\_COPY  
KNOWING YOU'RE SECURE

- Boundaries checks on the destination location can be bypassed (to a lower extent than source)

Frame Buffer

06/29/09 IMMUNITY 21

# ... and glyphs...



**SVGA\_CMD\_DRAW\_GLYPH**  
KNOWING YOU'RE SECURE

- Draws a glyph into the frame buffer
- Requires `svga.yesGlyphs="TRUE"`



Virtual Screen

06/29/09 IMMUNITY 23



**SVGA\_CMD\_DRAW\_GLYPH**  
KNOWING YOU'RE SECURE

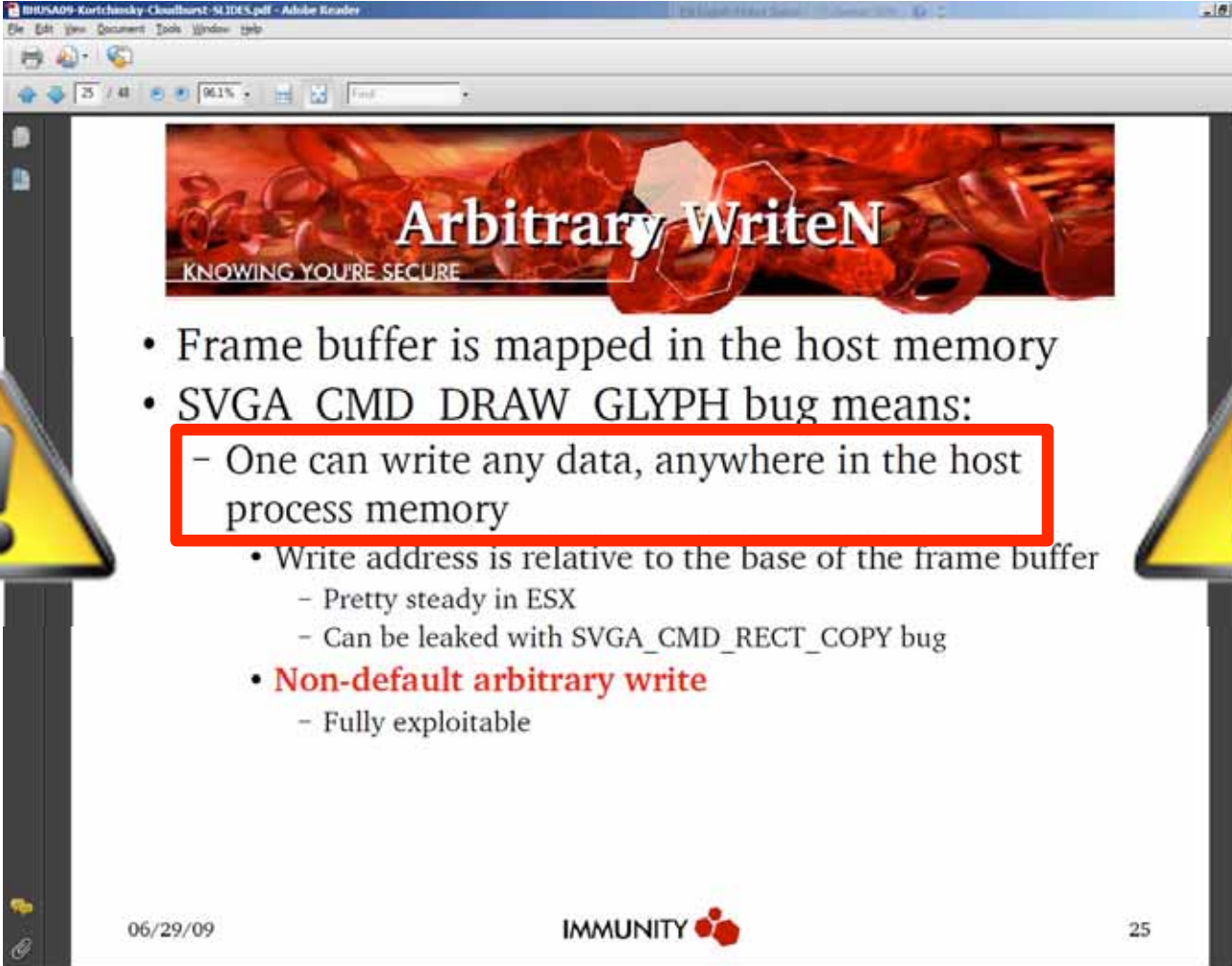
- There is no check on the X, Y where the glyph is to be copied



Virtual Screen

06/29/09 IMMUNITY 24

# The consequence

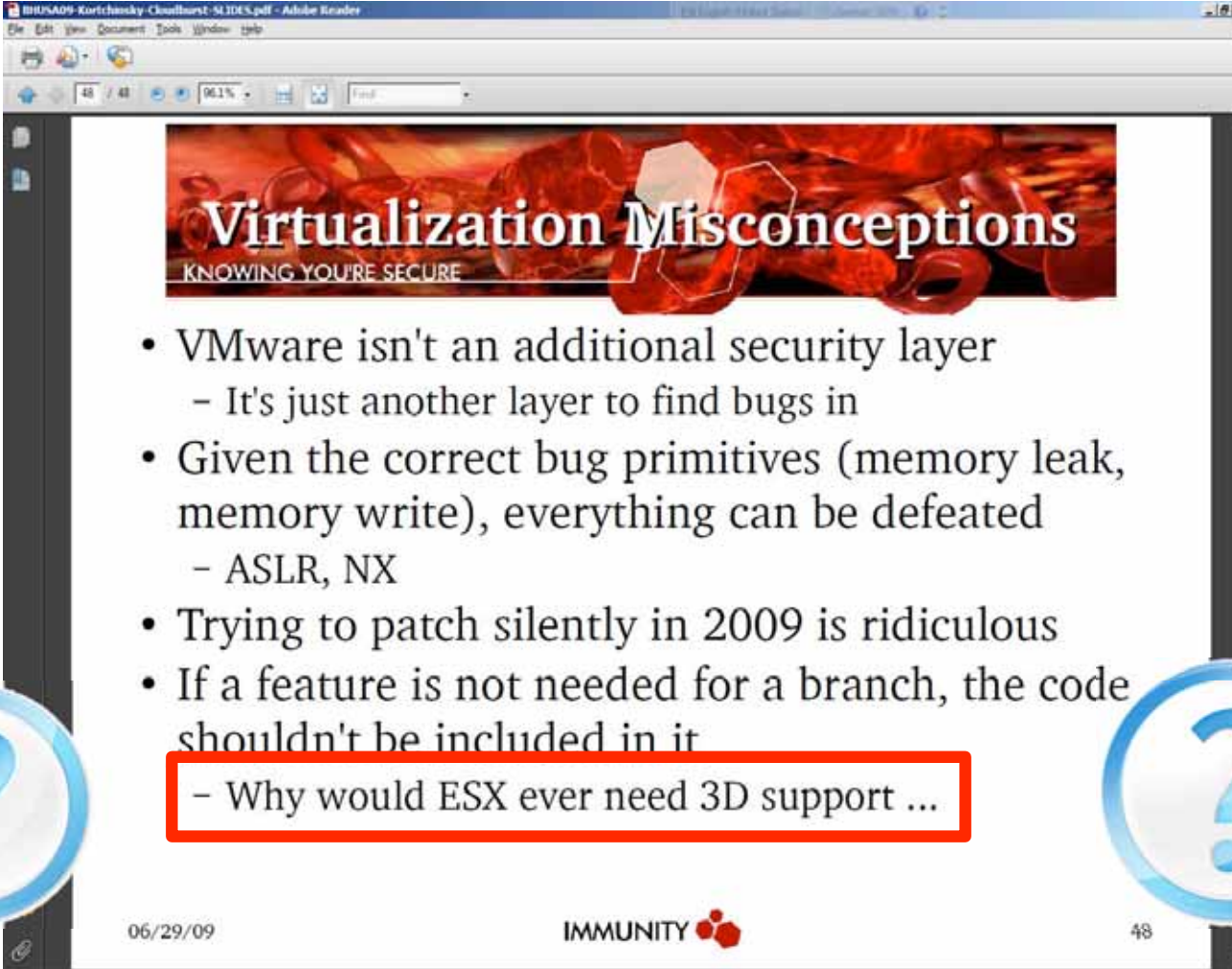


**Arbitrary WriteN**  
KNOWING YOU'RE SECURE

- Frame buffer is mapped in the host memory
- SVGA\_CMD\_DRAW\_GLYPH bug means:
  - One can write any data, anywhere in the host process memory
  - Write address is relative to the base of the frame buffer
    - Pretty steady in ESX
    - Can be leaked with SVGA\_CMD\_RECT\_COPY bug
  - **Non-default arbitrary write**
    - Fully exploitable

06/29/09 IMMUNITY 25

# Conclusions, as of Black Hat talk



Virtualization Misconceptions  
KNOWING YOU'RE SECURE

- VMware isn't an additional security layer
  - It's just another layer to find bugs in
- Given the correct bug primitives (memory leak, memory write), everything can be defeated
  - ASLR, NX
- Trying to patch silently in 2009 is ridiculous
- If a feature is not needed for a branch, the code shouldn't be included in it
  - Why would ESX ever need 3D support ...

06/29/09 IMMUNITY 48

Ok, so here's a "potential security issue"...

- ... now the main question – as always – is:

how to deal with this



- **Most common approaches**

- Ignore it
  - At times camouflaged as “the risk treatment option we chose” ;-)
  - And, of course (1): “there’s all those huge cost savings”.
  - And, of course (2): “we’ll harden the stuff later”.
    - When *Godot* shows up.
- Implement \$SOME\_SECURITY\_CONTROLS



# Implement \$SOME\_SECURITY\_CONTROLS



- **There are different flavors of this one, too.**
  - Use (architecture level) controls “that we’ve been using before”
    - “ERNW’s seven sisters” or similar stuff comes to mind.
  
  - Follow “Industry Best Practices”
    - “What’s in the standards?”
    - ISO xy, NIST SP800-125, *IT-Grundschutz-Kataloge* etc., (depending the part of the world you’re in)



# Let's have a look at the 7 sisters first

*Dei sju søstre, Norway*



# The *seven sisters* of infrastructure security



Access Control



Isolation



Restriction



Encryption



Hardening



Secure Management



Visibility



Access Control



Hardening



Isolation



Secure Management



Encryption



Restriction



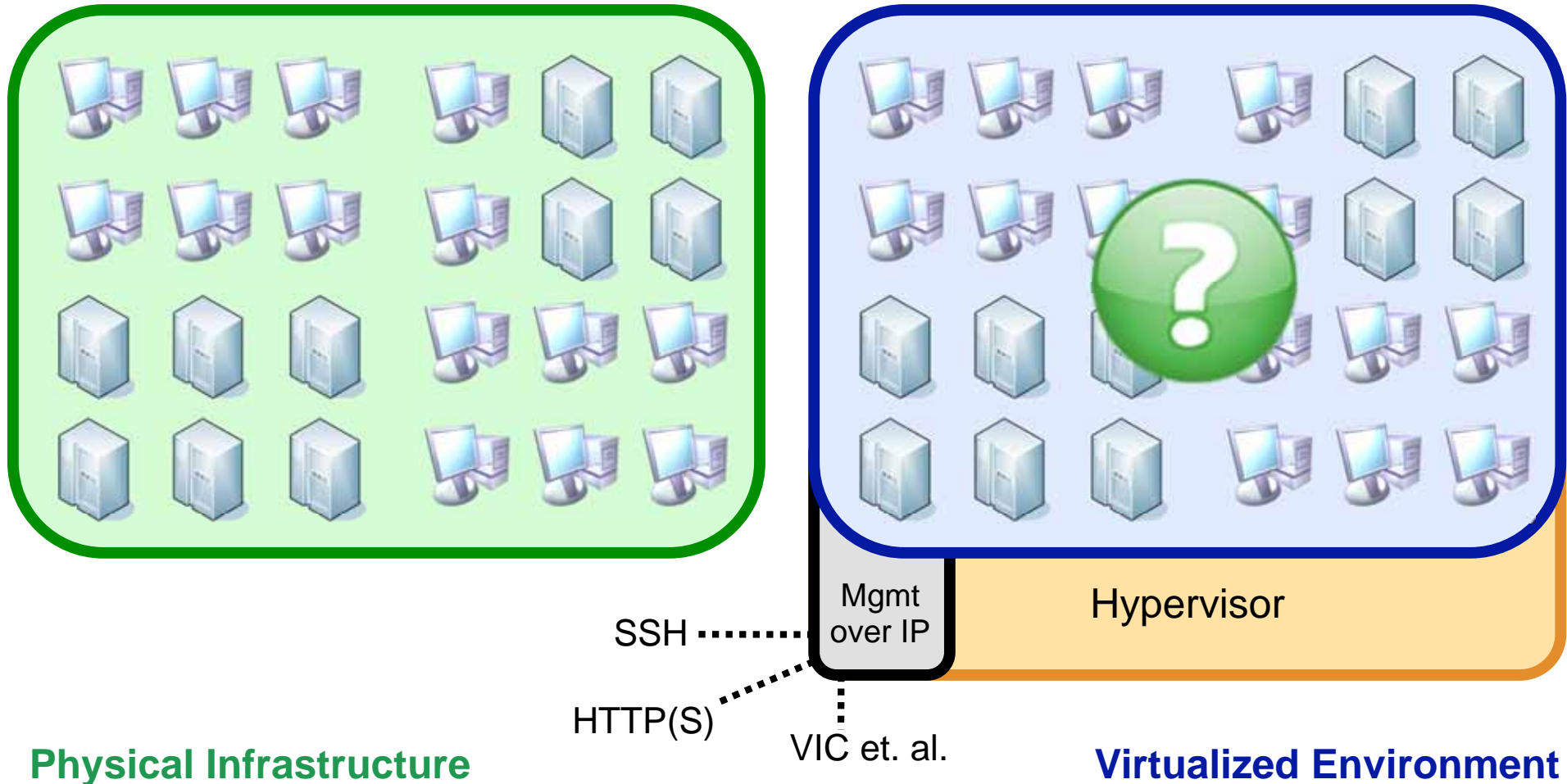
Visibility

**... and how they  
change in the  
virt\_world**



# Access control, change in virt\_world

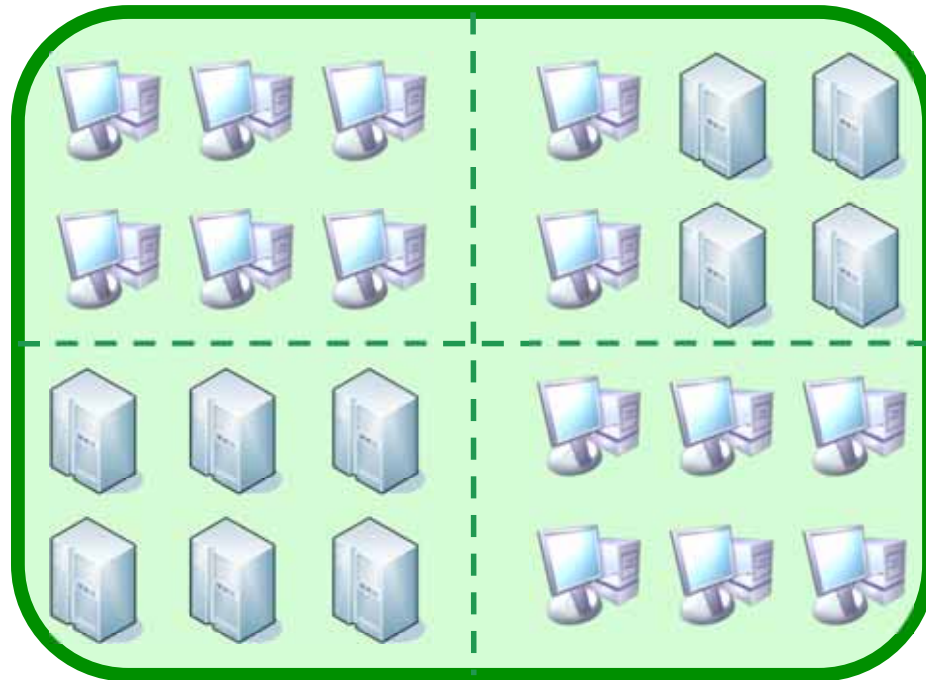
Datacenter



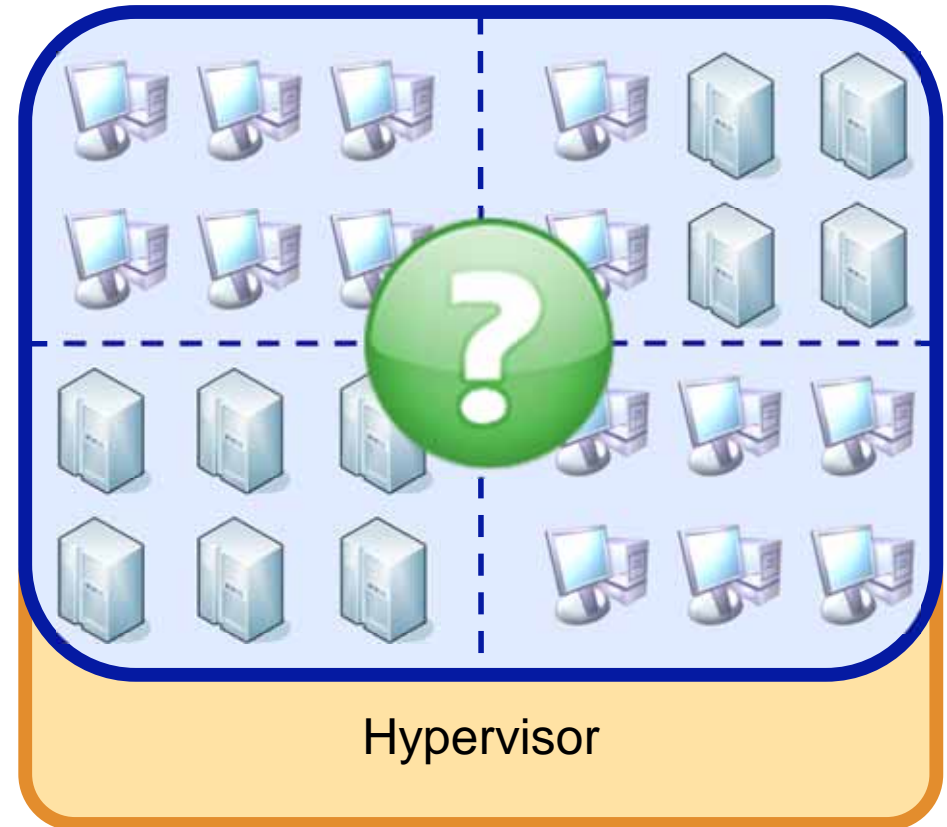
**Physical Infrastructure**

**Virtualized Environment**

# Isolation, Change in virt\_world



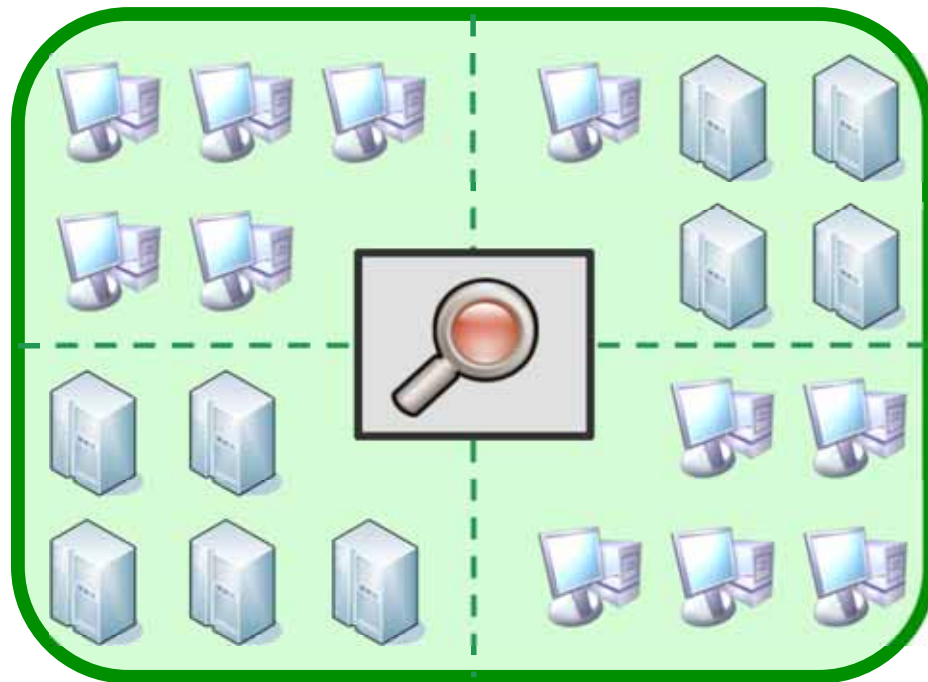
--- e.g. VLANs



**Physical Infrastructure**

**Virtualized Environment**

# Isolation + restriction, change in virt\_world

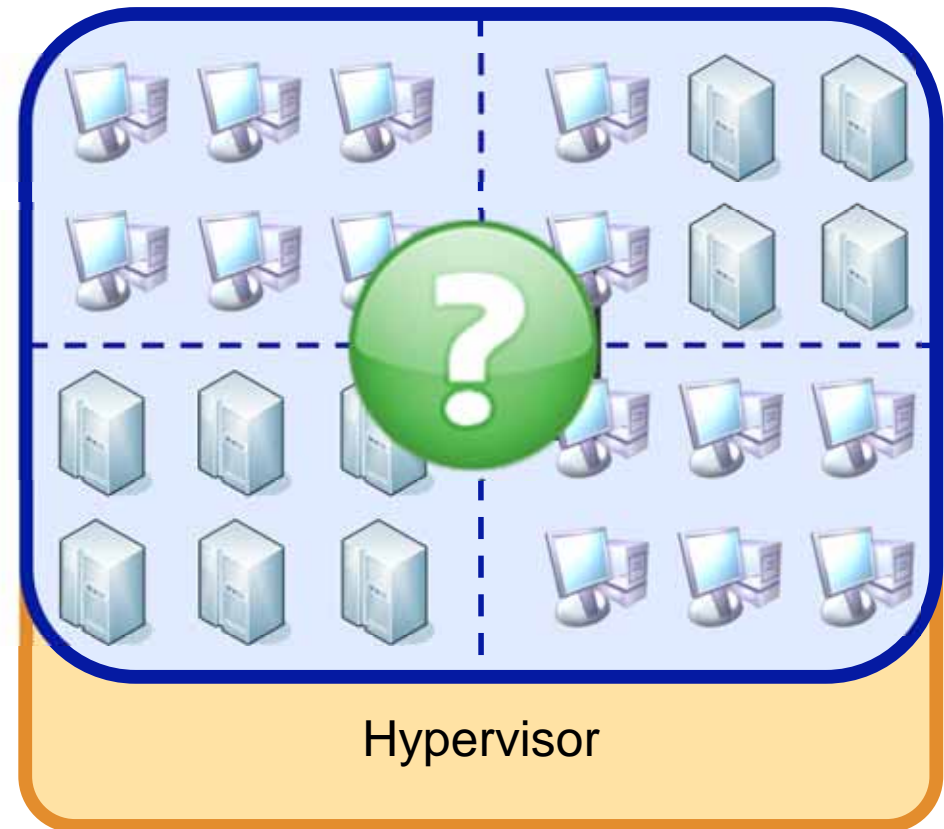


--- e.g. VLANs



Packetfilter

**Physical Infrastructure**



Hypervisor

**Virtualized Environment**

# Isolation – There's three layers

- **Computing (Memory, CPU)**



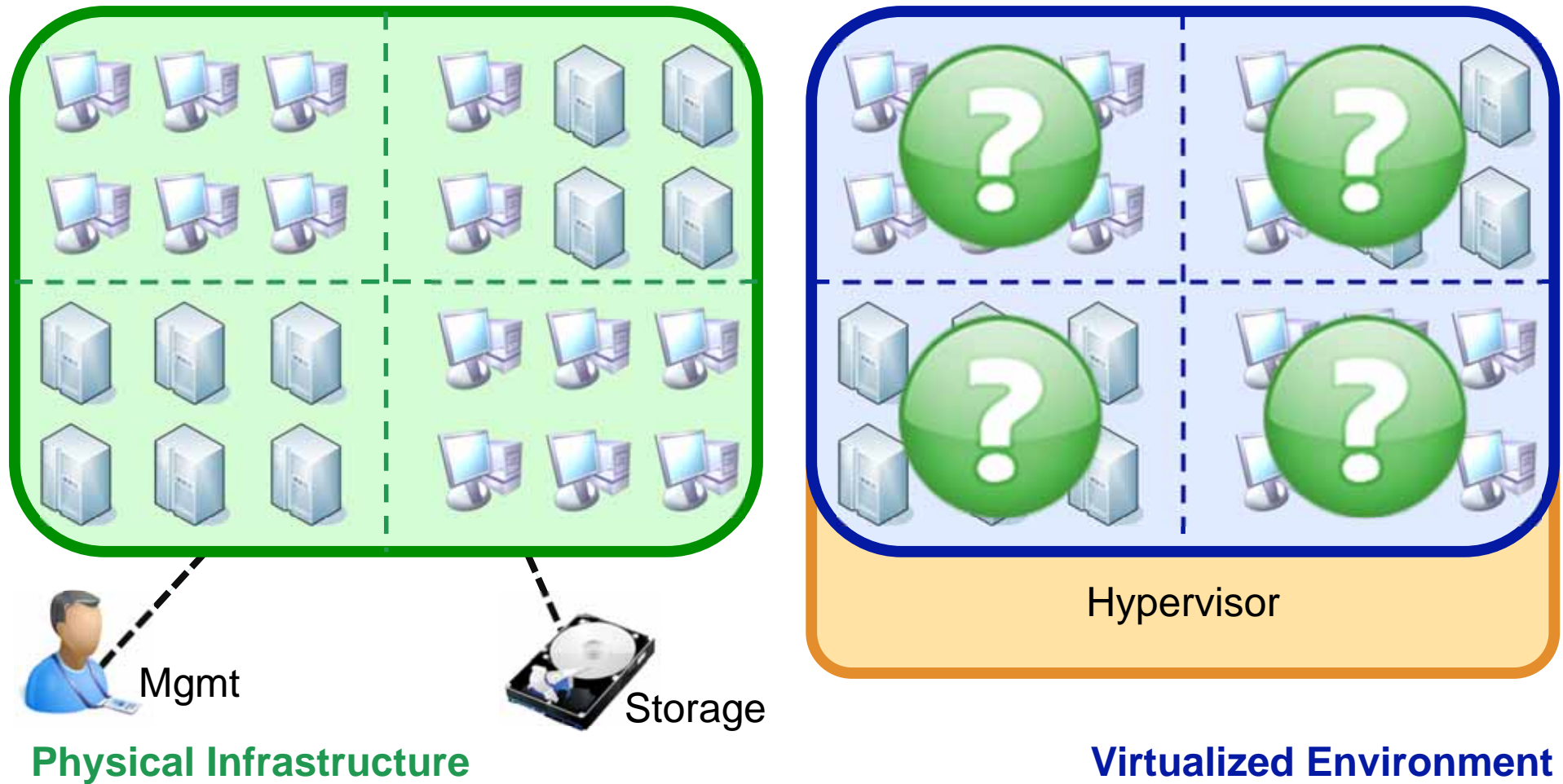
- **Network**



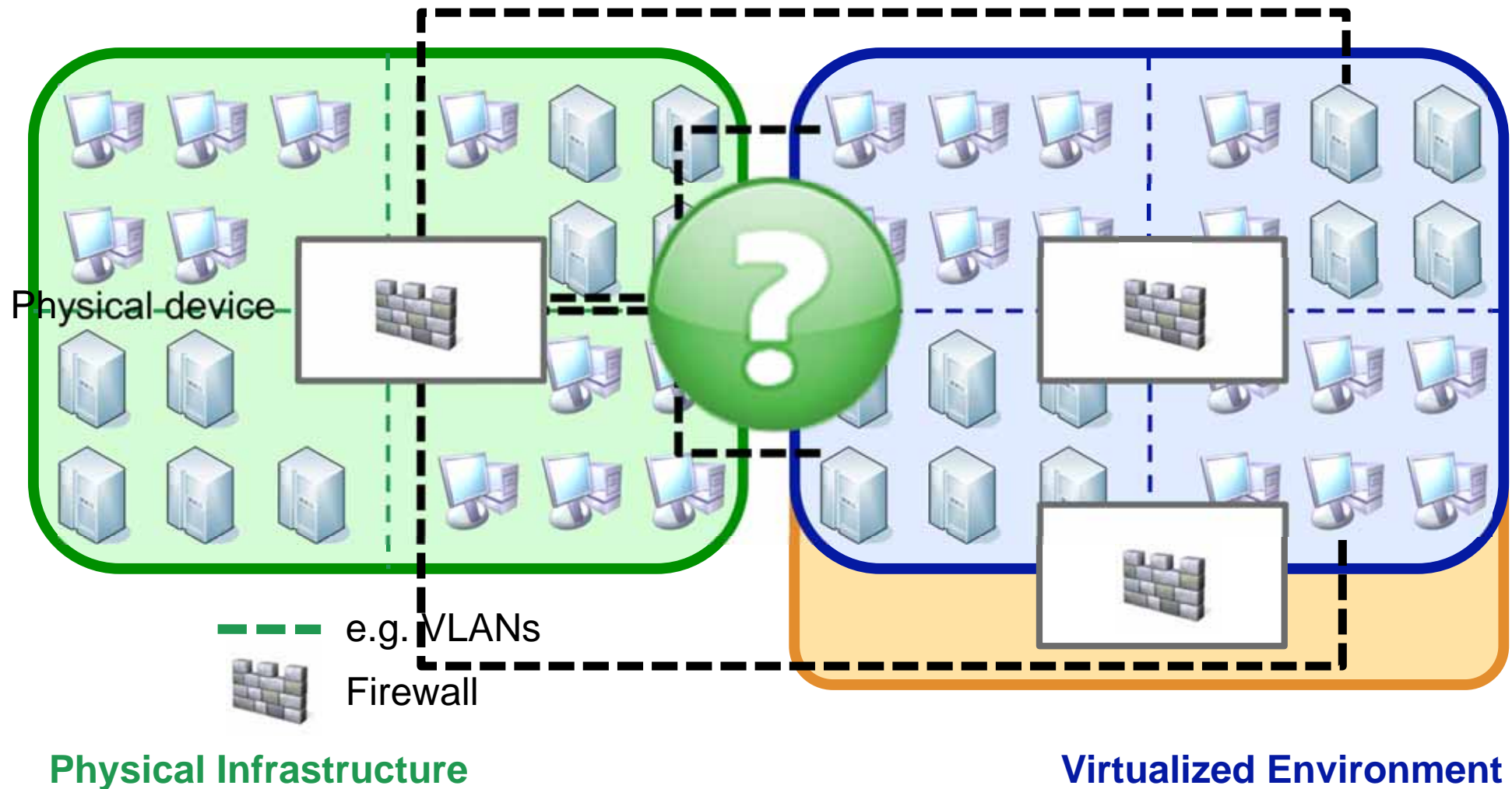
- **Storage**



# Isolation, change in virt\_world

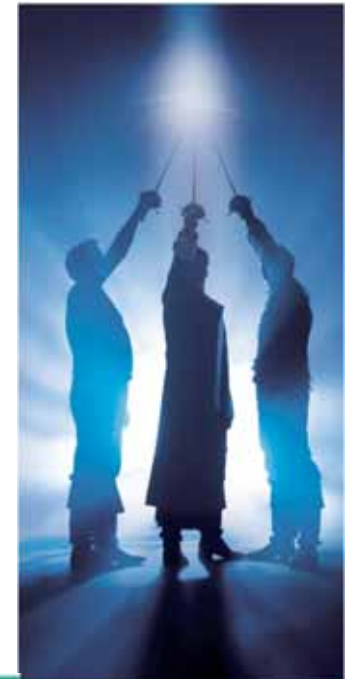


# Restriction, change in virt\_world



## Interim conclusion

- **The role of the *seven sisters* changes in the virt\_world.**
  - Maybe it's *three musketeers* now? ;-)
- **Just transforming the old controls to the new world (mostly) will *not* work.**
  - Complexity kills.
  - COMPLEXITY KILLS.
  - LET ME STATE THIS CLEARLY: COMPLEXITY KILLS!
  - If \$YOUR\_OUTSOURCED\_SERVICE\_PROVIDER sells you this, think about it. What's *their* agenda?
    - Right! More complexity → More service. → More \$\$\$.
    - Better security? Bah...

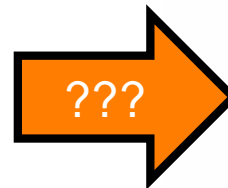


Back again, let's have a look at a that particular tricky one: "isolation"

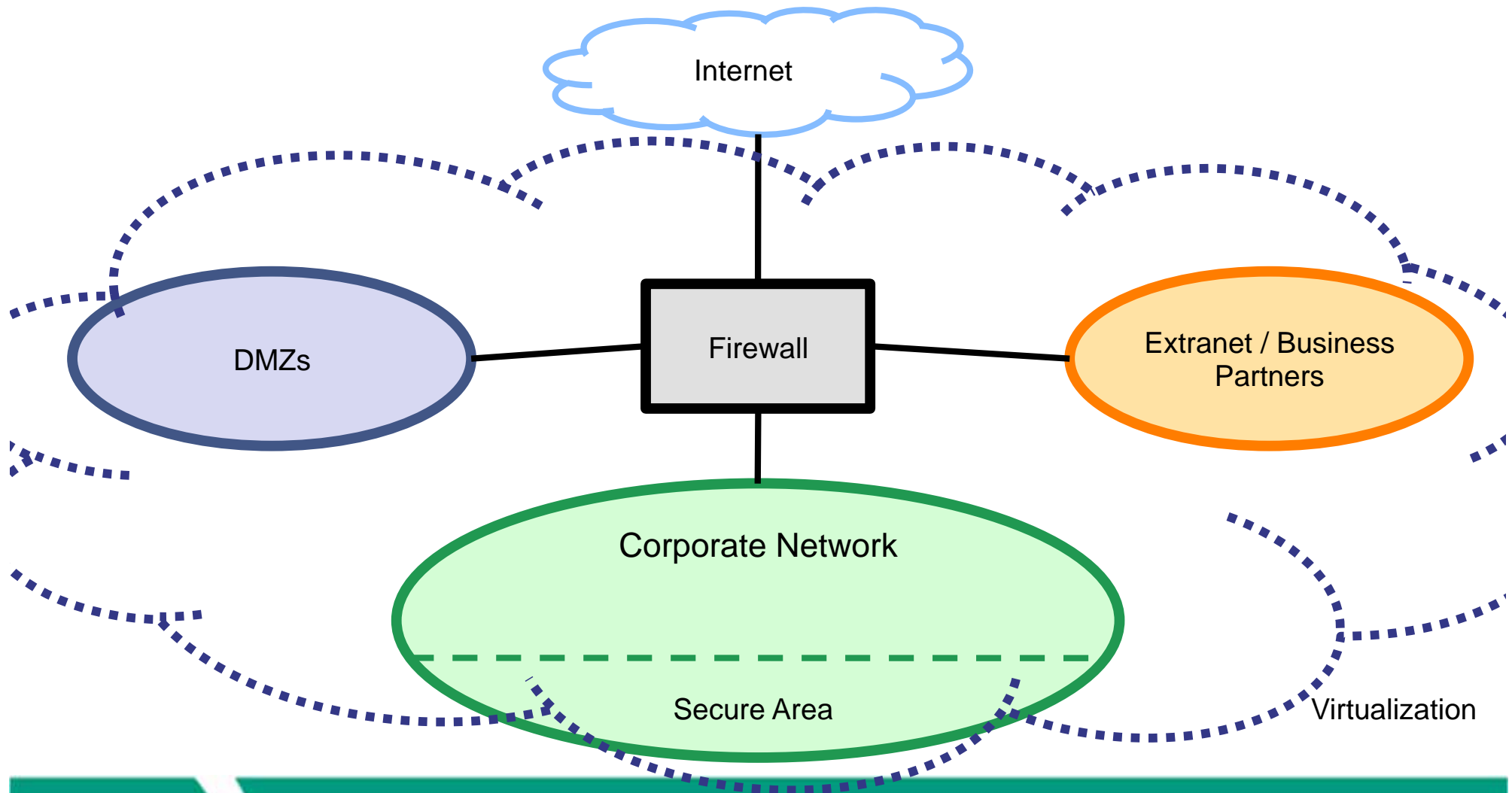
- Quite frequently, this is the source of grim debates between **\$CORP\_HOSTING** and **\$CORP\_INFO\_SEC**

NOBODY  
WILL EVER  
TRY TO  
DO THIS

YOU'RE  
PARANOID



# How to “virtualize” this?



# Our way to approach this

- **Three relevant factors:**

- **Protection need**

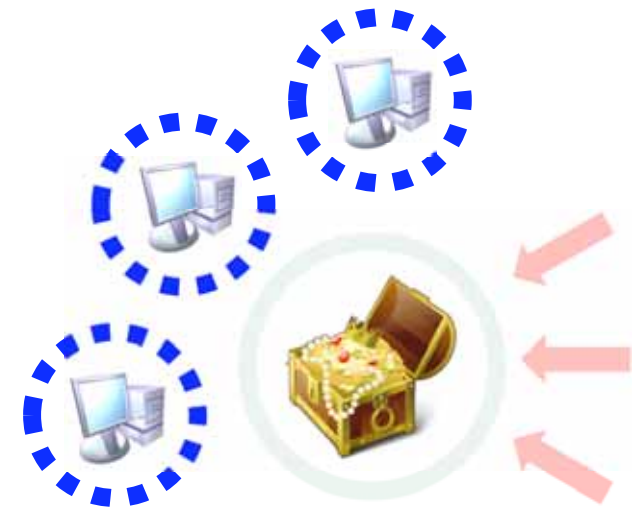


- **Threat potential**



- **Trust (worthiness)**

- “How much can we trust the systems in this zone?”



# Example

Number	Name	Protection Need	Threat Potential	Level of Trust
5	Public Internet	low	high	low
4	External DMZs	high	medium	medium
3	Business Partner DMZs	medium	medium	medium
2	Internal default, CN	high	low -medium	medium-high
1	Secure Area	high	low	high

Thank you, sir, but there must be “industry best practices” for this as well?

- **Well...**

- We’ll get back to this in a second

- **Overall there’s not that many different variants anyway**

- One cluster (cloud) for everything
- One cluster (cloud) per sec\_level
- Something in between



- **BUT: given (usually) there’s no bells+whistles for “strong memory protection” and (infosec) resource constraints prevail we (you) ’re desperately left alone as for the main risk, that is “compromised hypervisor”. So, in the end of the day...**

# It's all about the "Gretchenfrage"

- Does server virtualization *isolate* in a sufficient manner?

## BSI:

“Wurden vor der Virtualisierung Netze aufgrund unterschiedlichen Schutzbedarfs physikalisch getrennt, müssen diese Netze auch in virtuellen Umgebungen voneinander isoliert werden. Es ist dann zu prüfen, ob die Mechanismen zur Netztrennung, sowie der Kapselung und Isolation der virtuellen IT-Systeme in der eingesetzten Virtualisierungslösung ausreichen, um virtuelle IT-Systeme mit hohem Schutzbedarf gemeinsam mit solchen niedrigen Schutzbedarfs auf einem Virtualisierungsserver betreiben zu können.

Ha Ha Ha!

Diese Prüfung kann z. B. darin bestehen, dass der Hersteller [...] die genannten Mechanismen für diesen Einsatzzweck [...] als geeignet bezeichnet und dies durch eine entsprechende Zertifizierung nachweist.“

Do you trust me?



# NIST SP800-125, SSDD

Having separate partitions for resource is an important part of isolating guest OSs. Isolation also involves limiting guest OS communications and the access that each guest OS has to the other guest OSs, to the hypervisor, and to the host OS (if present). Hypervisors can theoretically support a level of logical isolation nearly equivalent to physical isolation, mediating all communications from each guest OS to have full control over each guest OS's actions. Hypervisors can permit interactions between guest OSs as needed, such as allowing two desktop OSs to share a file system. Hypervisors can also dynamically alter isolation for each guest OS as needed—for example, enabling and disabling networking at specific times. Isolation has obvious security benefits, but it can also increase the reliability of a host by preventing actions in one guest OS from directly affecting another. For example, if one guest OS crashes because of an application fault or an attack, the other guest OSs on that host are unlikely to be affected. Isolating each guest OS from the others and restricting what resources they can access and what privileges they have is also known as *sandboxing*.



Many thanks for the comprehensive guidance!

# Implement \$SOME\_SECURITY\_CONTROLS [previous slide, slightly modified]



- **There are different flavors of this one, too.**
  - Use (architecture level) controls “that we’ve been using before”
    - “ERNW’s seven sisters” or similar stuff comes to mind.  
→ Unfortunately, their role has massively changed
  - Follow “Industry Best Practices”
    - “What’s in the standards?”
    - ISO xy, NIST SP800-125, *IT-Grundschutz-Kataloge* etc.,  
(depending the part of the world you’re in)  
→ Unfortunately, they don’t (can’t) provide guidance.





# What next?

- **It might be time for a new paradigm.**



# Trust & Control

- In the end of the day what everybody involved in infosec (like everybody else as well) looks for is ... *confidence*.
- *Confidence* means “having a positive attitude with regard to the expected outcome”. Sleep well, as “the world is ok”.
- This confidence can be based on two major ingredients
  - Trust 
  - Control 
- **Both are valid sources for confidence.**
  - Infosec people usually give preference for the control approach though.

There's environments where trusting is easy...



Home



Datacenter



...whereas in others it might not be the proper path to *confidence* ;-)

Home



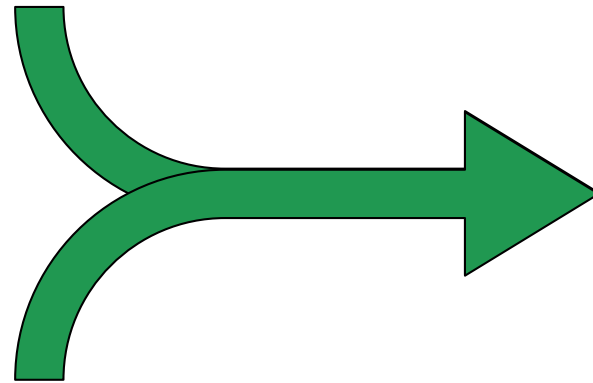
Datacenter



# Trust, Control & Confidence



**TRUST**



**CONTROL**



**CONFIDENCE**

# The general problem of *trust*

- **Diego Gambetta:**  
**"trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action".**
- **Something non-*subjective* might be helpful.**
- **This could be some way of documenting *reasons for trust*.**



# Problems of “the control approach”

- **Costs!**



- **Operational impact**

- Business might feel obstructed.



- **Usually controls increase overall complexity**

- → might be bad for overall security.

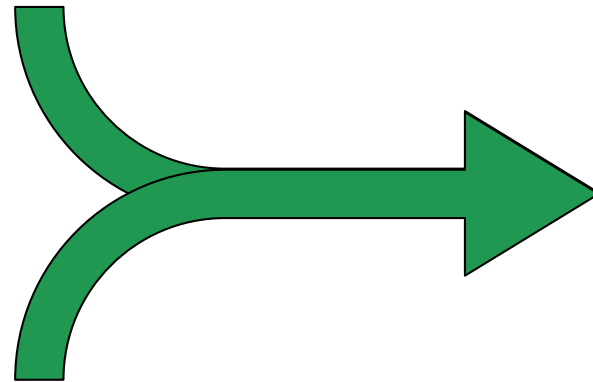


- **AND: in the new world it might... just... not ... work!**

So, apply \$ELEMENT where appropriate



TRUST



CONTROL



CONFIDENCE

# Back to trust


- **Trust needs evidence.**
  - Otherwise it would be *faith*.



- **What could that be?**

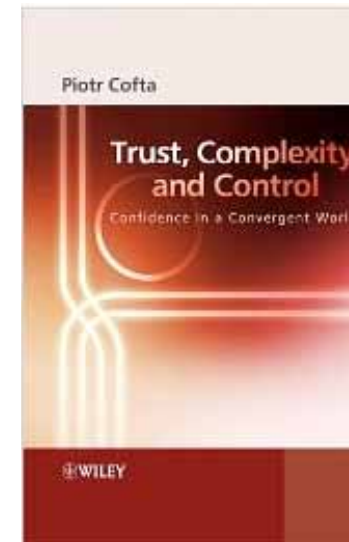


# Factors of trust, approaches

- 
  - ~~Size~~
  - Symmetry
  - Transparency
  - ~~Control~~
  - Consistency
  - Integrity
  - ~~Offsets~~
  - Value of Reward
  - Components
  - Porosity

- **Piotr Cofta**

- Continuity
- Competence
- Motivation



## And how this can be transformed into a checklist / metric

- **Symmetry: Do they trust us?**
- **Transparency: How much do we know about \$TRUSTEE?**
- **Consistency: What happened in the past?**
- **Integrity: (How) Do we notice if \$TRUSTEE changes?**
- **Value of Reward: What do we gain by trusting?**
- **Components: Which resources does \$TRUSTEE rely on?**
- **Porosity: How separated is \$TRUSTEE from it's environment?**
  
- **Continuity: How long will we work together?**
- **Competence: Can \$TRUSTEE provide what we expect?**
- **Motivation: What's \$TRUSTEE's motivation?**



# And how this can be transformed into a checklist / metric, Example

	VMware ESX	Xen	MS Hyper-V
Symmetry	3	3	3
Transparency	2	4	4
Consistency	2	3	4
Integrity	2	3	4
Value of Reward	5	4	3
Components	2	2	2
Porosity	3	2	3
<b>Trust Factor</b>	<b>19</b>	<b>21</b>	<b>23</b>

**Note 1:** Obviously your mileage might vary. Still, this sample was filled out by a “group of involved experts”.

**Note 2:** Factors, in particular *value of reward* might be weighted to reflect your objectives/requirements.



# Still, you have to take decisions

- **But those are justified more properly.**
- **You might have a clearer understanding of the areas where to apply additional controls**
  - The blind spots in the list of trust factors.
- **Basis for decision will be documented!**



Let's take this one step further



## In the cloud...

- **...you don't own the hardware/computing engine/RAM.**
  - you **can not** *control* it.
  - did you get that? You **can not**!
- **... you don't own the network.**
  - you **can not** *control* it.
- **... you don't own the facilities.**
  - ...
  - You don't even know where they are.
- **... you don't employ the administrators.**
- **... you don't own the processes.**
- **Yadda yadda yadda**



So, again

- **With the tools from the old world...**
- **... we're desperately left alone, out there.** 



→ **(Qualified) Trust is your only hope**



# Applying the trust metric to the “cloud”

- **In the past I had the pleasure to deal with three different cloud providers [on behalf of very large customers]**
  - Amazon WS
  - salesforce
  - Some\_other\_SAAS\_provider\_not\_to\_be\_disclosed
    - We just finished a pentest of their main app (on behalf of customer).
    - Letting us do this (in particular on customer's behalf) is remarkable.
    - Unfortunately the results were... devastating...  
hence no mention here who they are.



# Applying the metric

	Amazon WS	salesforce	\$SOME_SAAS
Symmetry	2	3	4
Transparency	1	5	4
Consistency	2	3	1
Integrity	2	4	2
Value of Reward	5	3	3
Components	4	3	2
Porosity	3	3	2
<b>Trust Factor</b>	<b>19</b>	<b>24</b>	<b>18</b>

**Note 1:** Obviously your mileage might vary. Still, this sample was filled out by a “group of involved experts”.

**Note 2:** Factors, in particular *value of reward* might be weighted to reflect your objectives/requirements.



## Looking at the results

- **Who would you trust?**

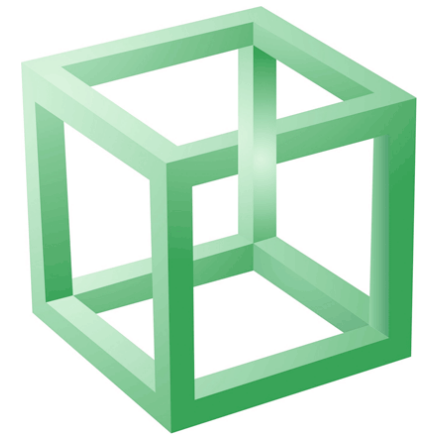


- **Sure, your CIO might jump in: “we’ll do it differently”.**
- **Still, from our understanding, this is the only feasible way of “approaching security [confidence!] in times of the cloud”.**

# Summary

---

- **Virtualization and “the cloud” will change the shape of our IT environments dramatically.**
- **Striving for “security” (*confidence*) will have to reflect this.**
- **You can’t apply security controls to “the cloud”.  
But you can rate the trustworthiness of it’s providers.**



There's never enough time...



**THANK YOU...**



**...for yours!**



# What else can we do for you?

- **ERNW Virt-Audit Checklist**
  - Pls contact us if you want to get it.
  
- **Troopers 2011 ;-))**



[www.troopers.de](http://www.troopers.de)

# References

- **Vorabversion des Grundschutzbausteins B3.40 *Virtualisierung*:**  
[https://www.bsi.bund.de/cae/servlet/contentblob/938954/publicationFile/60461/baustein\\_virtualisierung\\_entwurf.pdf](https://www.bsi.bund.de/cae/servlet/contentblob/938954/publicationFile/60461/baustein_virtualisierung_entwurf.pdf)
- **NIST Special Publication 800-125 (Draft): Guide to Security for Full Virtualization Technologies (Draft) Recommendations:**  
<http://csrc.nist.gov/publications/drafts/800-125/Draft-SP800-125.pdf>
- **Claudio Criscione:  
The Good, The Bad, The Virtual**  
[http://troopers.de/content/e728/e897/e911/TROOPERS10\\_The\\_Good\\_The\\_Bad\\_The\\_Virtual\\_Claudio\\_Criscione.pdf](http://troopers.de/content/e728/e897/e911/TROOPERS10_The_Good_The_Bad_The_Virtual_Claudio_Criscione.pdf)
- **DayCon 2008:  
Microsoft Hyper-V – A first Security Inspection**  
[http://ernw.de/content/e7/e181/e1245/download1351/ERNW\\_DayConII\\_microsoft\\_hyperV\\_security\\_ger.pdf](http://ernw.de/content/e7/e181/e1245/download1351/ERNW_DayConII_microsoft_hyperV_security_ger.pdf)
- **Security Day:  
Virtualisierungs-Sicherheit**  
[http://ernw.de/content/e7/e181/e1391/download1393/ERNW\\_BechtleSecDay\\_Virtualisierungssicherheit\\_ger.pdf](http://ernw.de/content/e7/e181/e1391/download1393/ERNW_BechtleSecDay_Virtualisierungssicherheit_ger.pdf)



# TROOPERS II, 03/28-04/01/2011 Heidelberg, Germany



Subscribe to the newsletter at [www.troopers.de](http://www.troopers.de),  
follow us on Twitter [@WEareTROOPERS](https://twitter.com/WEareTROOPERS)  
and meet with experts from around the world at TROOPERS11 at Heidelberg, Germany.