

Sicher in virtuellen Umgebungen

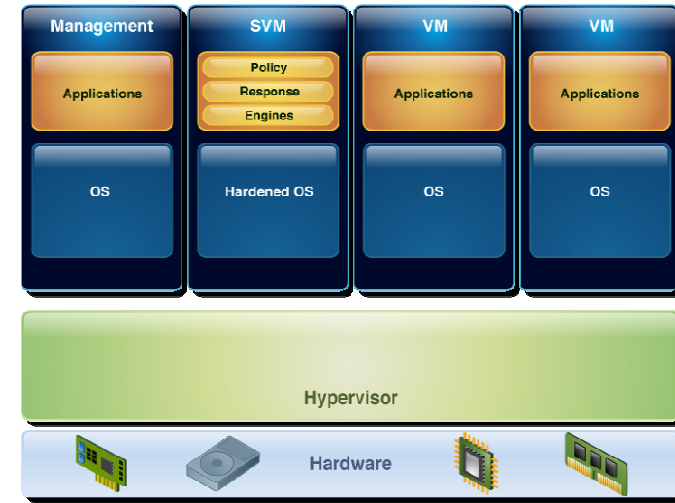
IBM Security Virtual Server Protection for VMware

Peter Häufel,
Senior Solution Sales Professional
IBM Security Solutions
haeufel@de.ibm.com,
Tel: 0175-7252260

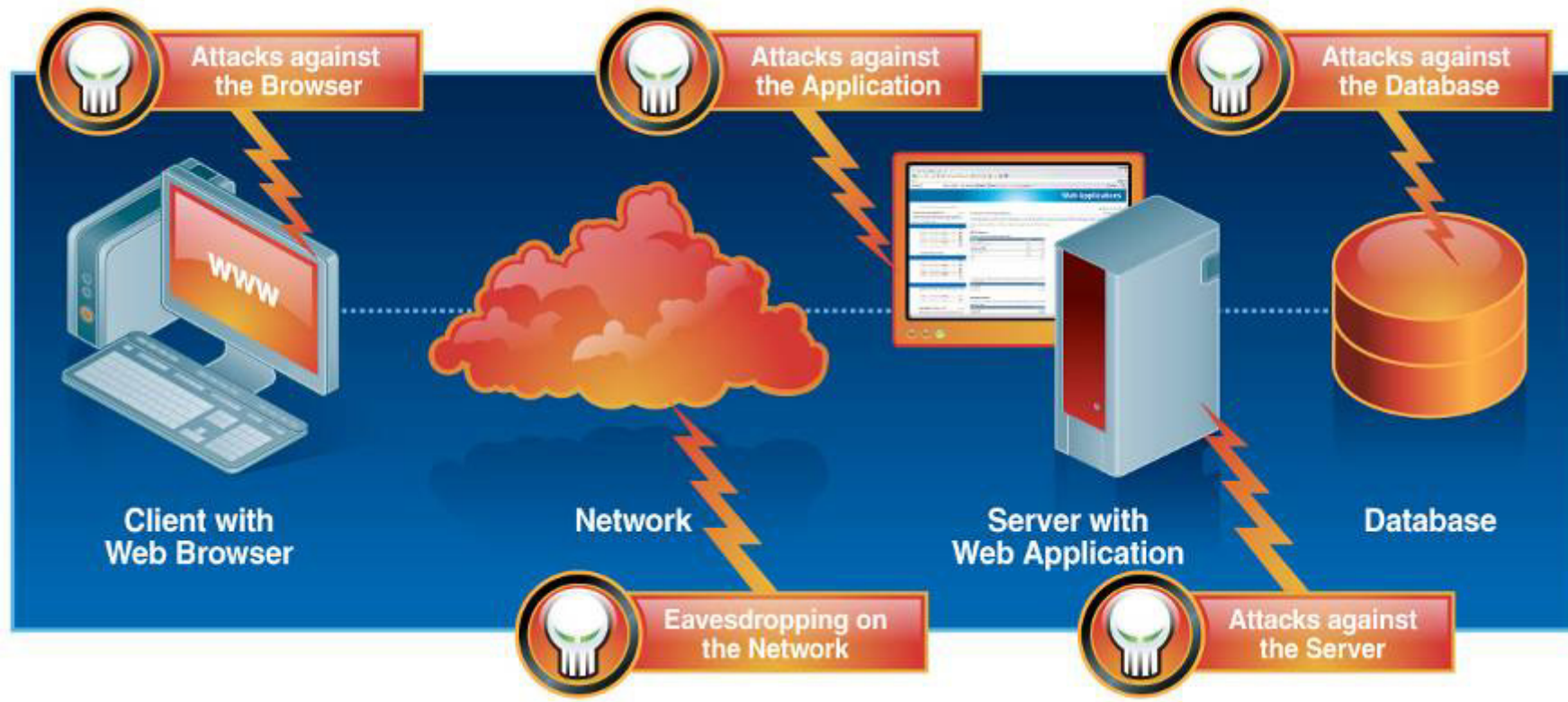


Problemstellung beim Kunden

- Neue Gefahrenquellen
- Mangelnde Transparenz
- Betriebskosten / Patch Pain
- Schwierige Umsetzung der Compliance Strategie
- Kundenzufriedenheit
- Verfügbarkeit
- Virtueller Patch, auch wenn noch kein Patch verfügbar ist



Angriffsziele



IBM security reach



IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security

Zeus Crimeware Service

Member slots filled: 3 / 30

[Q] What is
[A] is a mix between the ZeuS Trojan and MalKit. A browser attack t
computer and start logging all outgoing connections.

[Q] How much does it cost?
[A] Hosting fo costs \$50 for 3 months. This includes the following:

- Fully set up ZeuS Trojan with configured FUD binary.
- Log all information via internet explorer
- Log all FTP connections
- Steal banking data
- Steal credit cards
- Phish US, UK and RU banks
- Host file override
- All other ZeuS Trojan features
- Fully set up MalKit with stats viewer inter graded.
- 10 IE 4/5/6/7 exploits
- 2 Firefox exploits
- 1 Opera exploit
- Admin area to view statistics

[Q] Can i see a demo?
[A] Yes you can, there is a demo set up [here](#) (Comming soon)

Methods of payment:

- Moneybookers.com
- LibertyReserve.com
- WestemU
- Alertpay

Zeus :: Logs search

Information:
We also host Profile:
This includes GMT date:
GMT time:

Statistics:
Summary

Botnet:
Online bots
Remote commands

Logs:
→ Search
Search with template
Uploaded files
Logout

Hosting for costs \$50 for 3 months.

This includes the following:

- # Fully set up ZeuS Trojan with configured FUD binary.
- # Log all information via internet explorer
- # Log all FTP connections
- # Steal banking data
- # Steal credit cards
- # Phish US, UK and RU banks
- # Host file override
- # All other ZeuS Trojan features
- # Fully set up MalKit with stats viewer inter graded.
- # 10 IE 4/5/6/7 exploits
- # 2 Firefox exploits
- # 1 Opera exploit“

We also host normal ZeuS clients for \$10/month.

This includes a fully set up zeus panel/configured

binary

Reset

POPs

Grabbed data

Protected Storage

IE history

Other

Search

MassInfect

Internet Explorer, Firefox, Opera - 2008

bits	Infects
3	0
7	0
3	0
3	0
2	0
1	0
1	0
1	0
1	0
1	0
8	0
1	0
5	0
1	0

Importance of Day Zero Web App Protection

Reference -> <http://www.darkreading.com/vulnerability-management/167901026/security/application-security/217400256/index.html>

- Estimated based on input from 1000+ twitter users conducted by Jeremiah Grossman.
- Answers ranged from 2 to 80 hours, 40 hours selected as a conservative value paired with a \$100 per hour in hard development costs.
 - Average cost to fix single vulnerability -> **\$4,000 40 man-hours x \$100 hour**
 - Average cost to fix seven vulnerabilities per web site -> **\$28,000**

“Gartner, meanwhile, doesn't calculate actual application repair costs because they can vary so widely, but Joseph Feiman, a vice president and Gartner fellow, says Grossman's estimates are realistic”

Web Application Repair Tasks	
Vulnerability Verification - Investigation - Testing	Pre Deployment QA
Fix vulnerable software (patch or development)	Change management - Fix initiation approvals - Deployment approvals
(Optional) Vulnerability Awareness for IT Admin	(Optional) Vulnerability Awareness for Developers

Web App Engine Performance 100% Day Zero for 2011	
Fix vulnerable software (patch or development/programming)	Change management Fix initiation approvals Deployment approvals
(Optional) Vulnerability Awareness for IT Admin	(Optional) Vulnerability Awareness for Developers

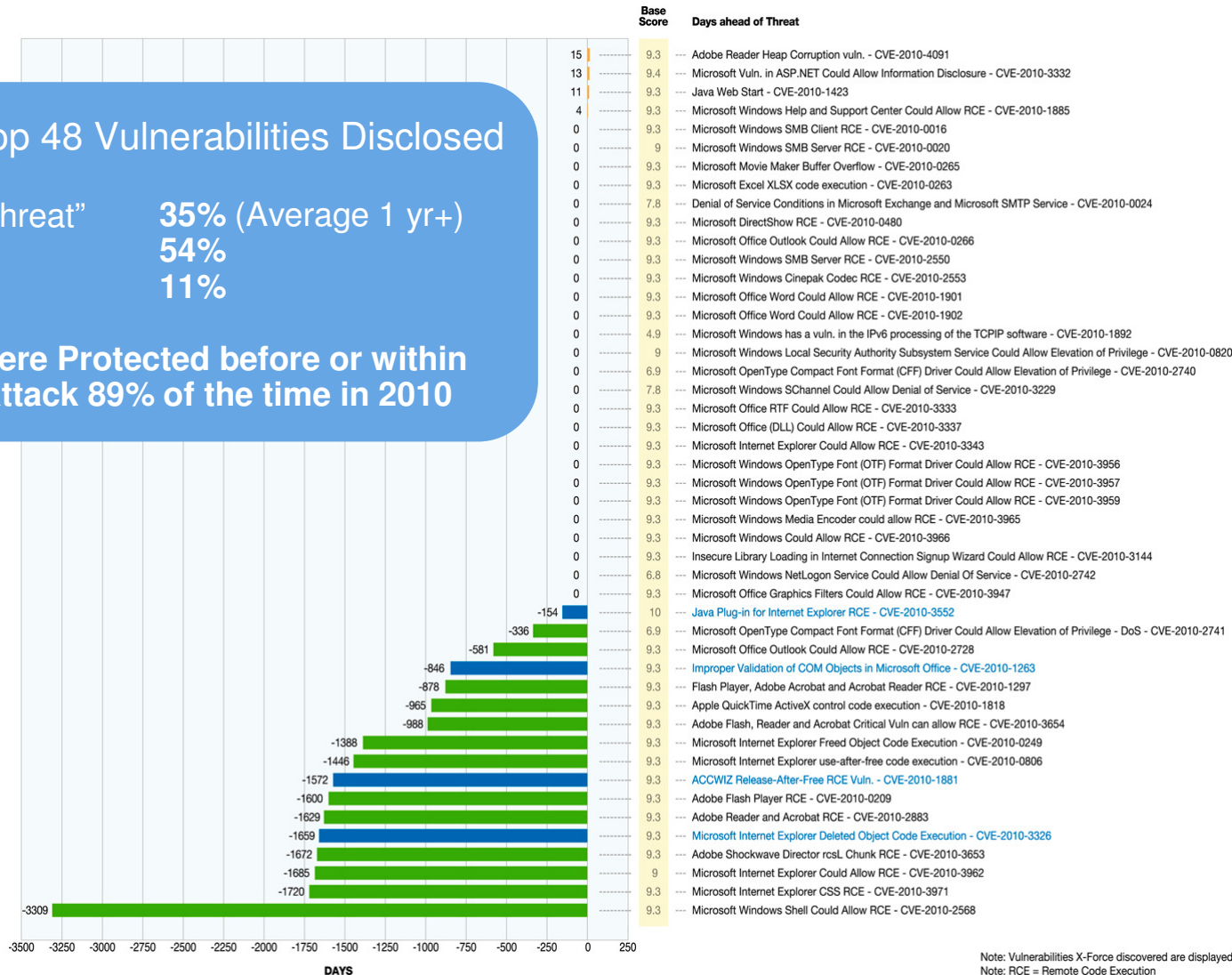
The Result? IBM Delivers Real-World Security Effectiveness

Protecting our Clients “Ahead of the Threat” in 2010 and Beyond

Out of the Top 48 Vulnerabilities Disclosed

“Ahead of the Threat” 35% (Average 1 yr+)
 Same Day 54%
 Within 15 Days 11%

IBM Clients were Protected before or within 24hrs of an attack 89% of the time in 2010



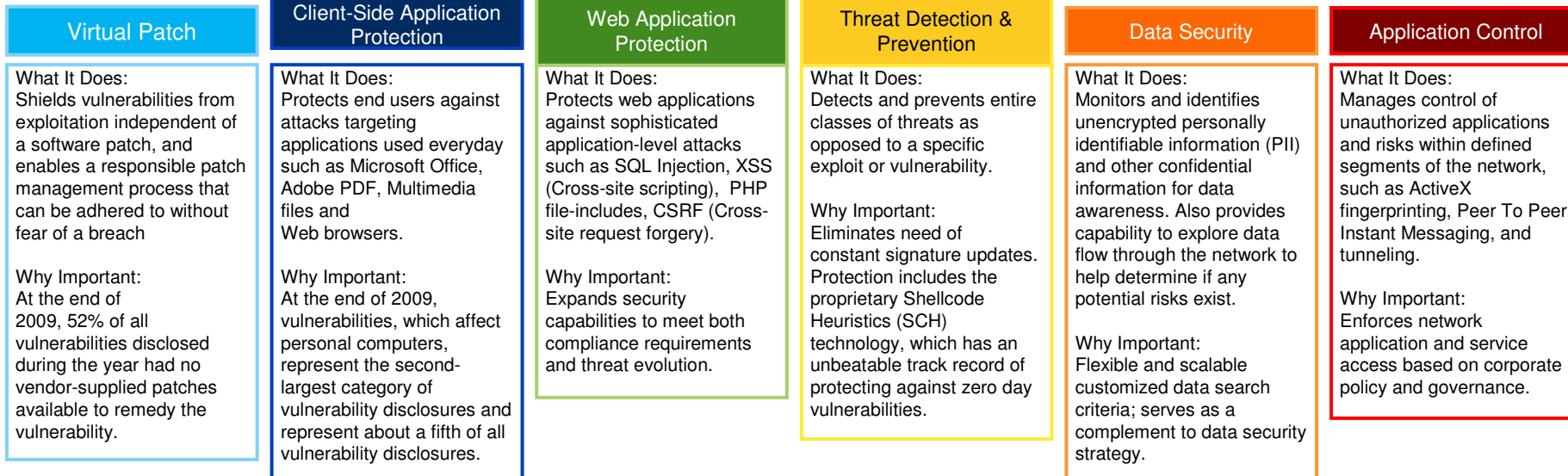
Source: IBM X-Force

Note: Vulnerabilities X-Force discovered are displayed in blue
 Note: RCE = Remote Code Execution

Our Protocol Analysis Module is the engine behind our products

Intrusion prevention just got smarter with extensible protection backed by the power of X-Force

IBM Protocol Analysis Modular Technology



Funktionsweise Intrusion Prevention

Virtual Patch

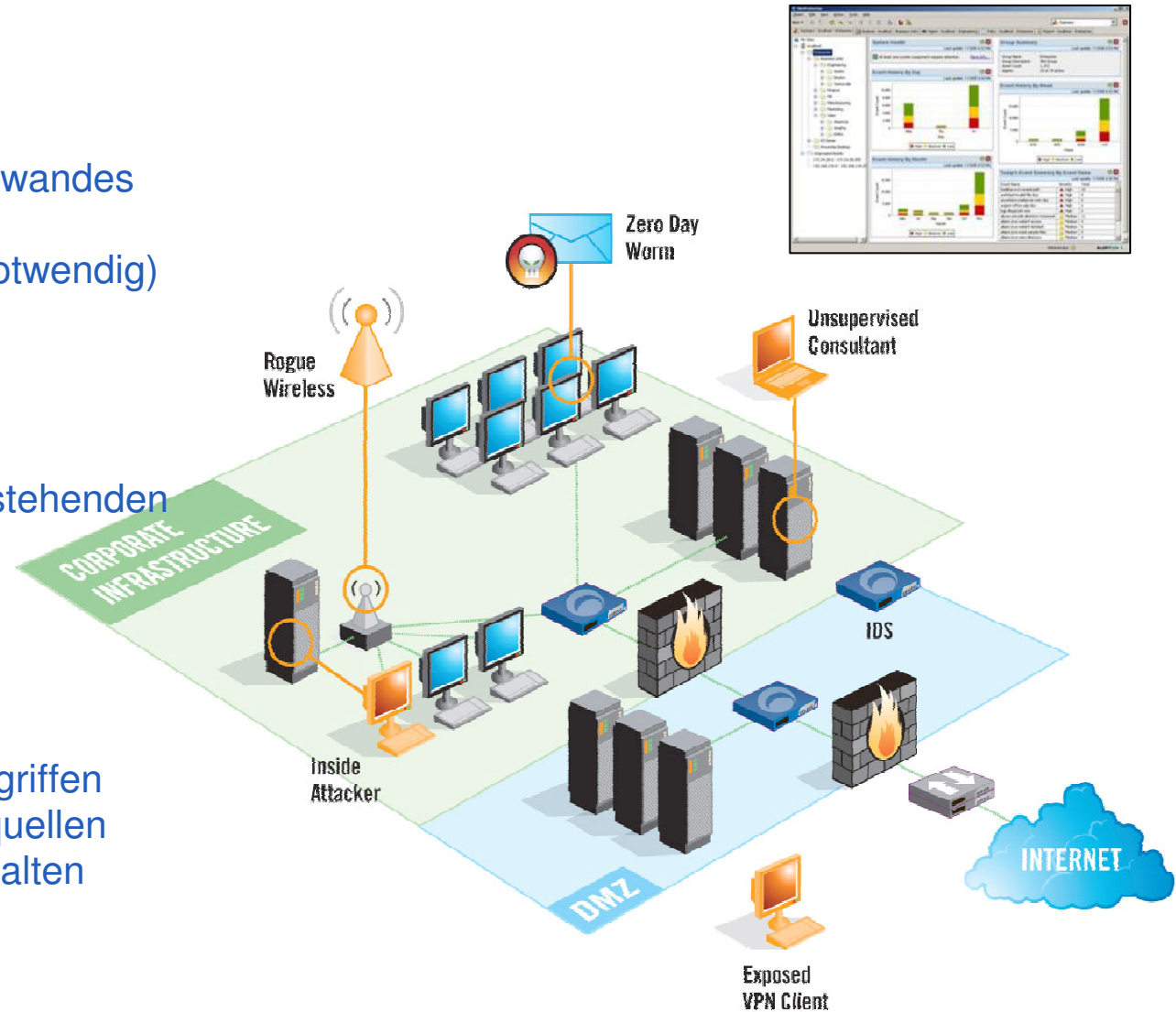
- Reduzierung des Patchaufwandes
- Frühzeitiger Schutz
- Schnelles Roll-Out (falls notwendig)

Abwehr von Angriffen

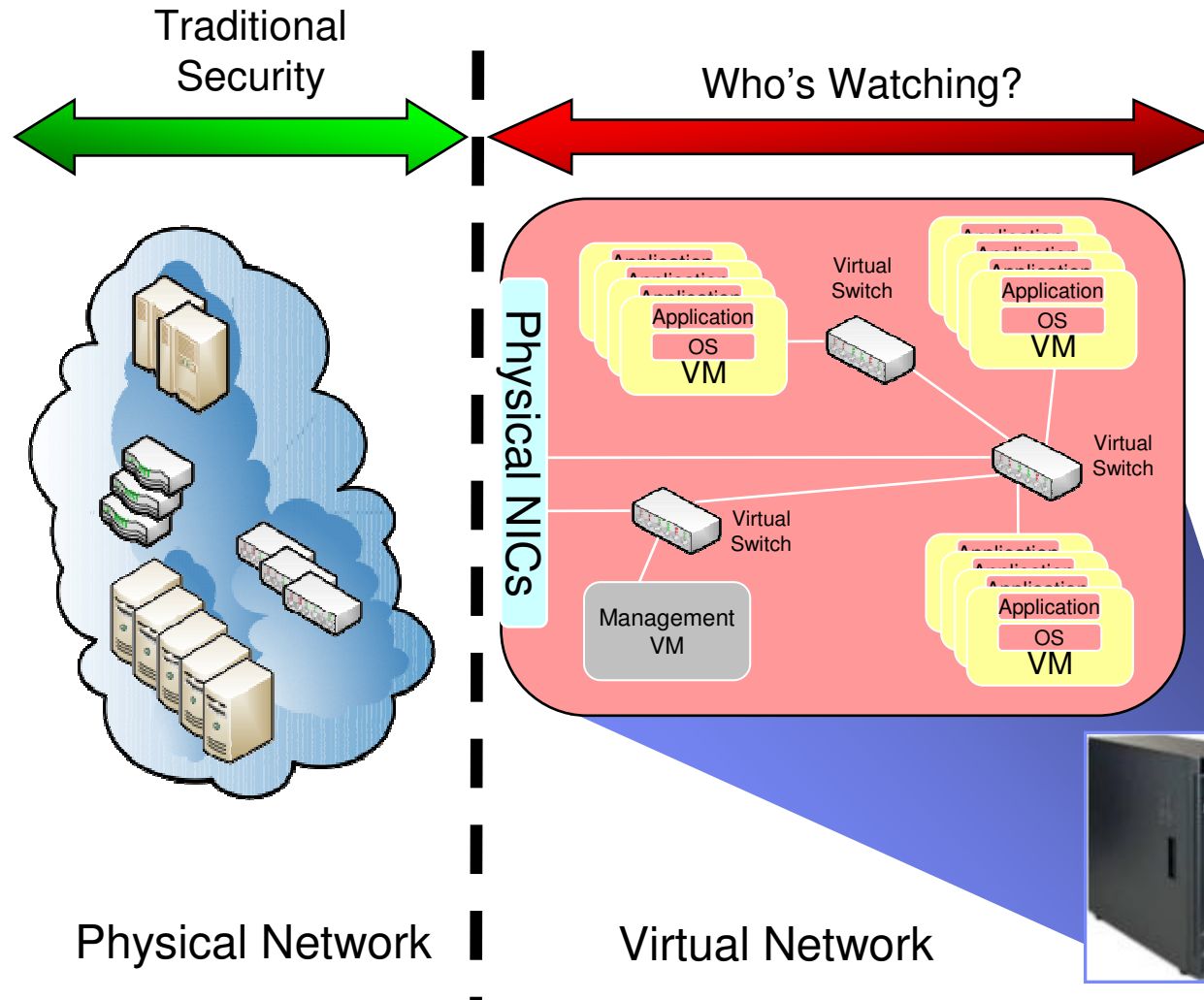
- Blocken von Angriffen
- Keine Ausnutzung von bestehenden Schwachstellen
- Herausfiltern von Malware

Transparenz

- Erkennen von internen Angriffen
- Identifizieren von Angriffsquellen
- Identifizieren von Fehlverhalten



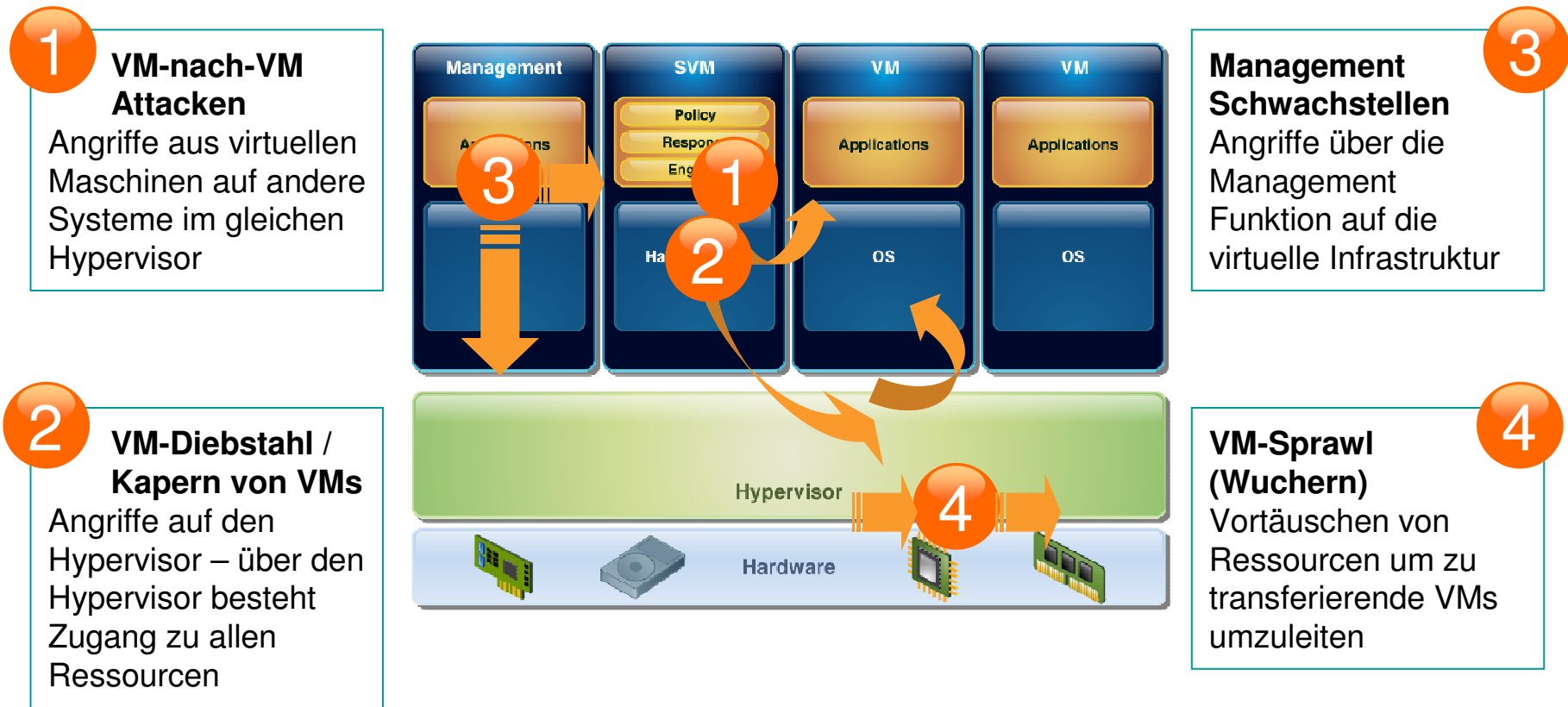
Server and Network Convergence



- Security “blind spots” are created as portions of the network becomes part of the server
 - Who owns the virtual network?
- Physical network IDP devices do not provide coverage for inter-VM communication
- Routing virtual network traffic to an external physical device is not practical

VM sprawl risks
 – what you cannot see
 will hurt you

Zugriffsschutz – Was gilt es in virtualisierten Umgebungen besonders zu beachten?



Neue Sicherheitslücken die mit bestehender Sicherheitsinfrastruktur nicht oder nur sehr aufwändig ermittelt werden können, da sie innerhalb des Hypervisors stattfinden

Schwachstellen in Virtualisierungsplattformen

Analyse von 80 bekannten Schwachstellen

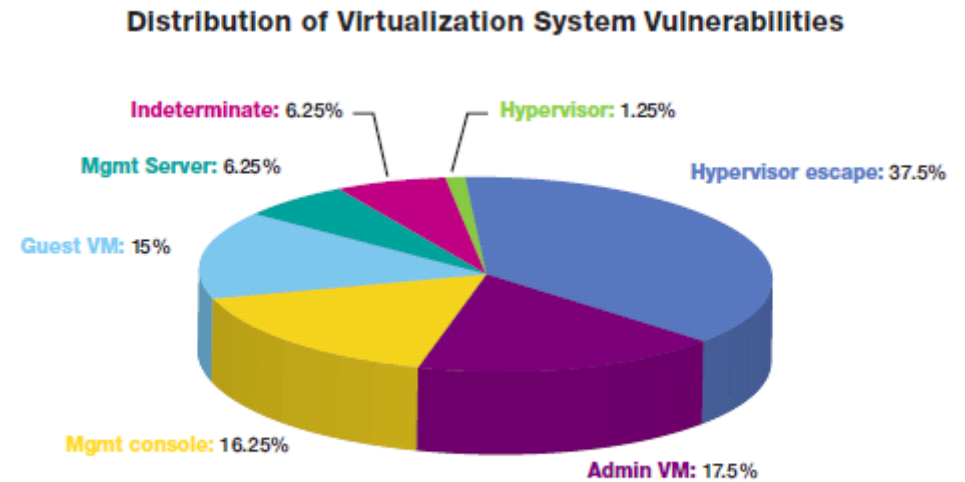
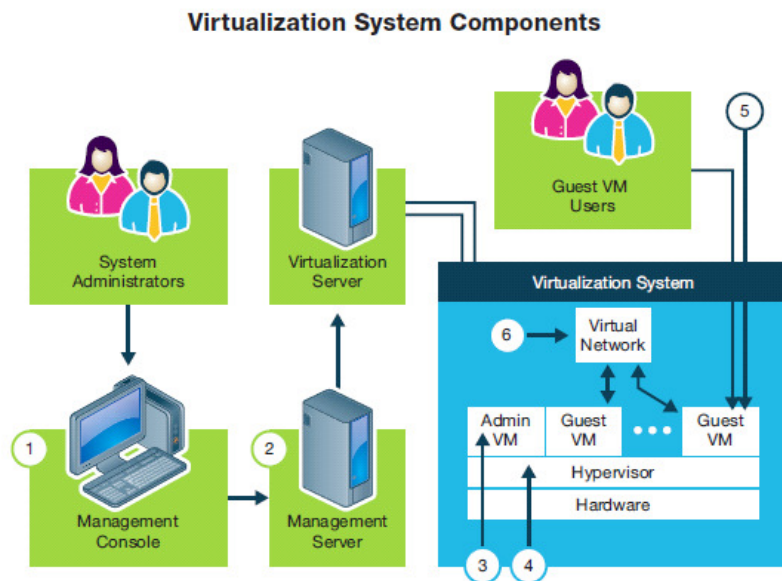
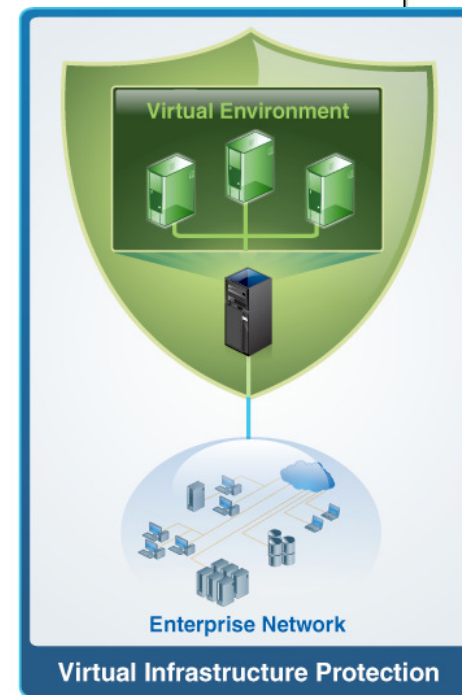


Figure 66: Distribution of Virtualization System Vulnerabilities

IBM ISS Virtualization Solutions: Three solutions

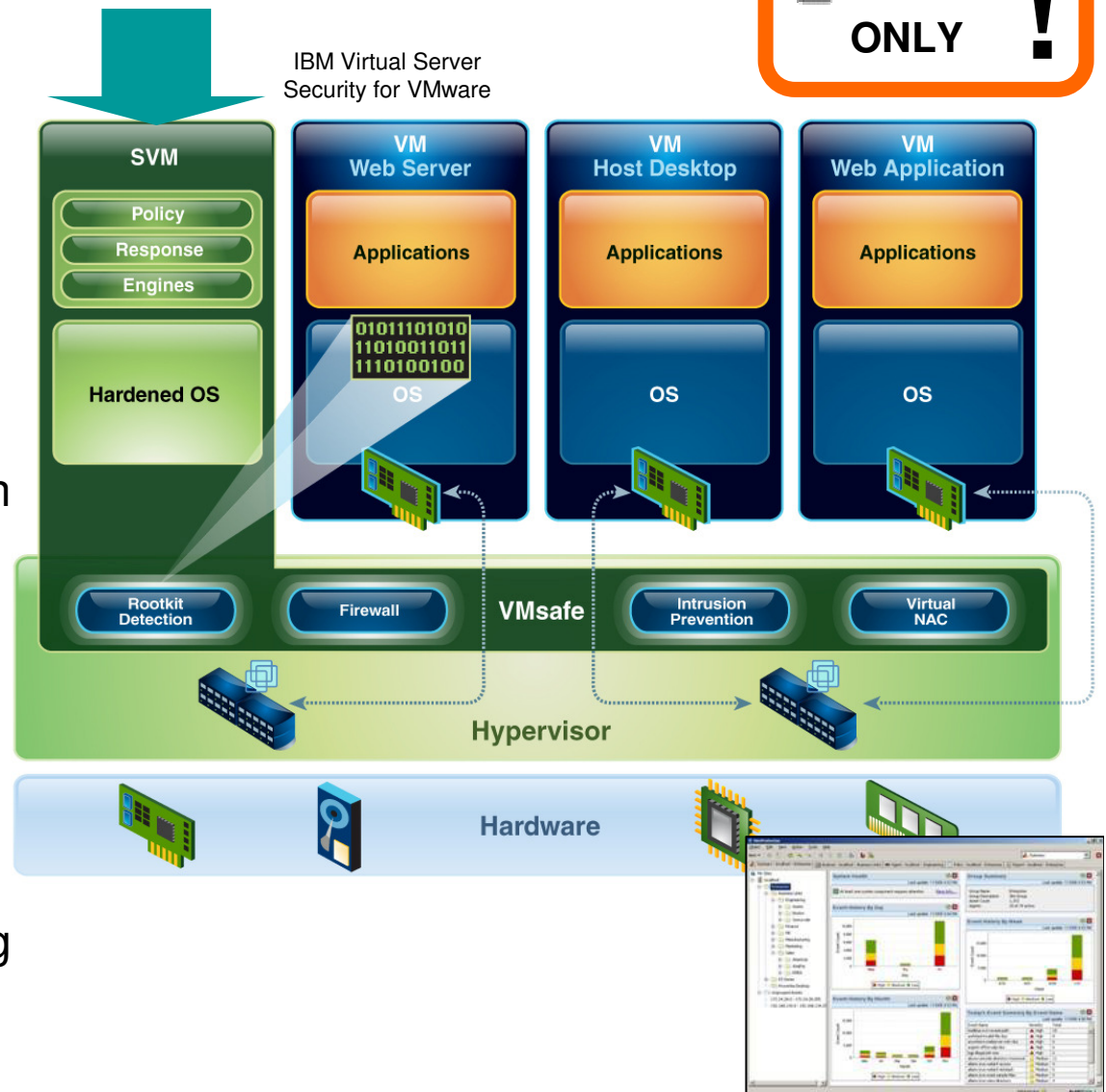
- Protect the Virtual Systems using our HIPS portfolio
- The Virtual Proventia NIPS gives you the flexibility to protect traffic inside the virtual environment
- Hypervisor HIPS brings perimeter protection to the virtual environment



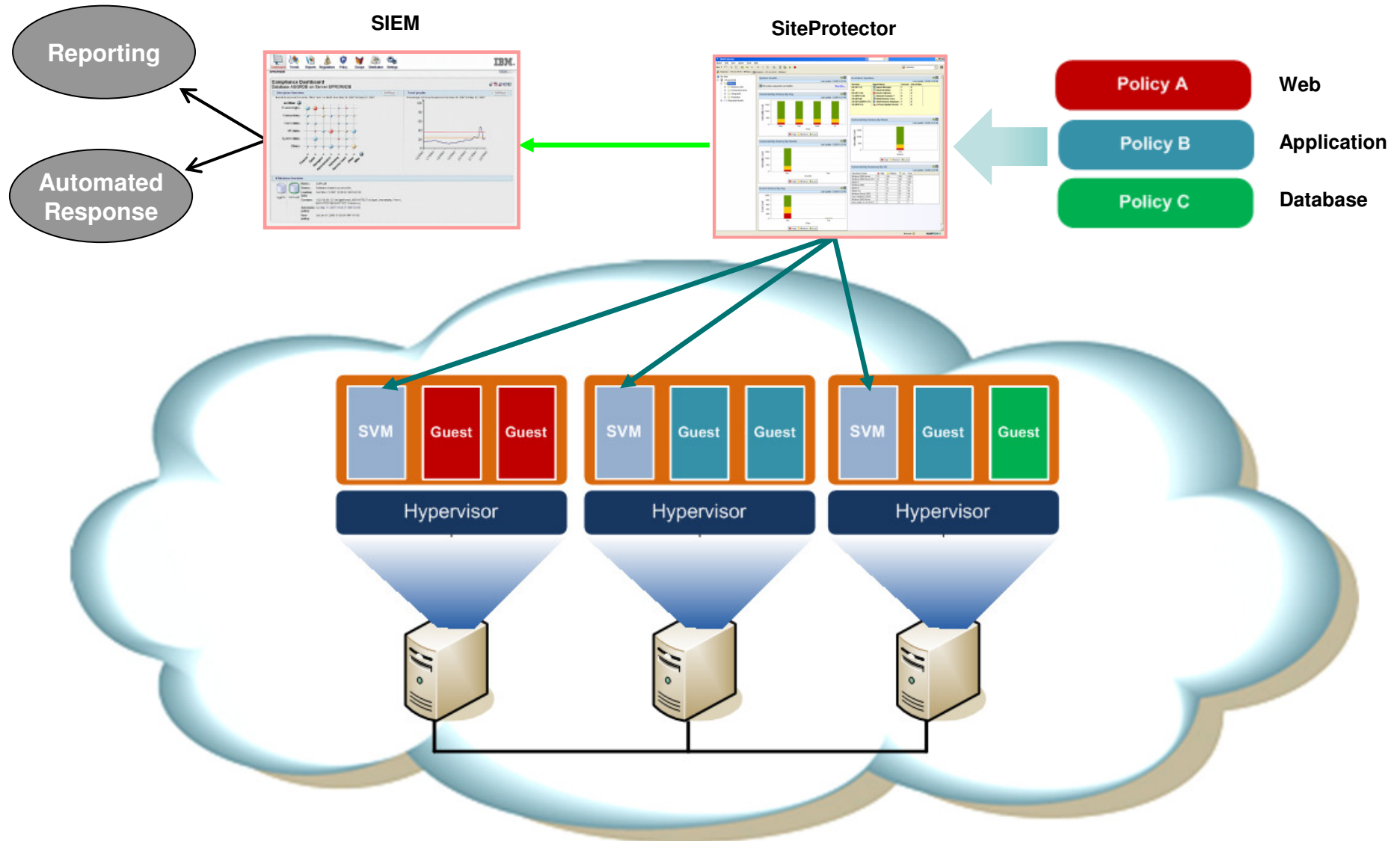
Lösungsansatz: Die Sicherheitslösung klinkt sich in die Virtualisierungsplattform ein



- Unterdrückung der Malware-Verbreitung innerhalb virtueller Server
- Dynamische Erkennung und Absicherung von neuen virtuellen Ressourcen
 - Auch mobiler VMs (VMotion)
- Eine umfassende Sicherheitslösung für VMWare beinhaltet
 - Firewall, Intrusion Prevention mit Virtuellem Patch Management
 - Rootkit Detection
 - Inter-VM Traffic Analysis
 - Virtual Network Segment Protection
 - Virtual Network-Level Protection
 - Virtual Infrastructure Auditing (Privileged User)
 - Virtual Network Access Control



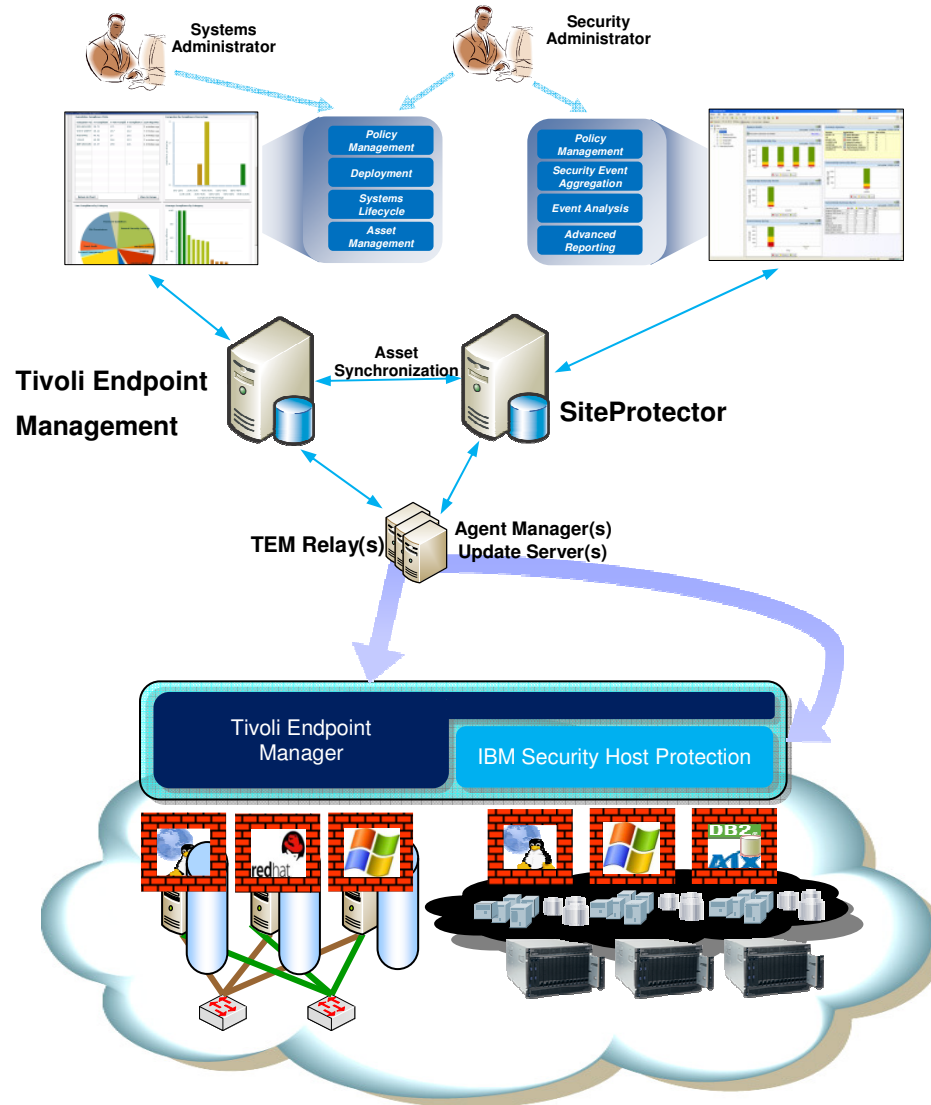
Schutz einer Dynamischen, verteilten Installation



Nutzen für unsere Kunden

- Optimale Absicherung - Ahead of the Threat
- Kosteneinsparung durch Unterstützung im Patchmanagement
- Geringe Betriebskosten durch ausgereifte Technik
- Erfahrung aus eigenem Betrieb im Großkonzern in Produkt eingeflossen
- Stabiler und verlässlicher Partner
- Reduzierung des Unternehmerischen Risikos
- Einhaltung der Sicherheitsrichtlinien
- Transparenz und Unterstützung der Compiancerichtlinie
- Erhöhung der Verfügbarkeit
- Kundenzufriedenheit
- Erweiterte Ausnutzung des Einsparpotential von Virtualisierung
- Vermeidung negativer Presse

Evolutionsschritt in Vorbereitung





Peter Häufel – Senior Solution Sales Professional
IBM Security Solutions
haeufel@de.ibm.com
Tel: +49.175.7252260

Fragen?

