Virtual Server Protection für VMware

Sprecher: Peter Häufel, Senior Solution Sales Professional

Agenda

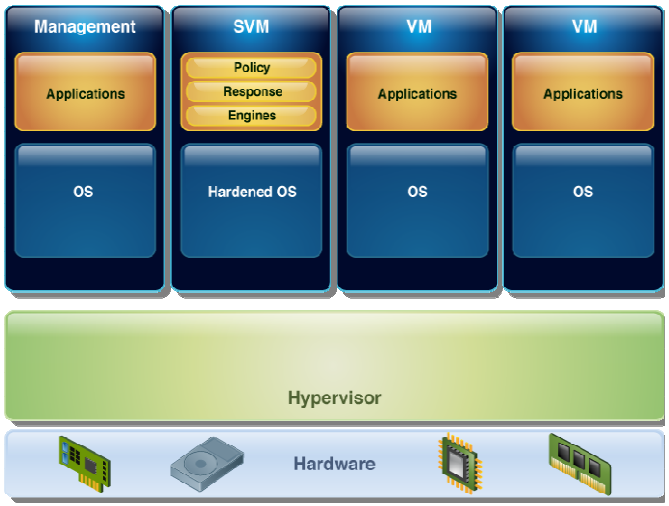
- Zielkunden / Quickwins
- Problemstellung beim Kunden
- Lösungsvorstellung *IBM Security Virtual Server Protection*
- Alleinstellungsmerkmale
- Projektvorstellung
- Ablauf PoC / Teamunterstützung
- Call to Action / Wer sind die Ansprechpartner beim Kunden?

Zielkunden

Wann ist Virtual Server Protection eine Lösung für meine Kunden?

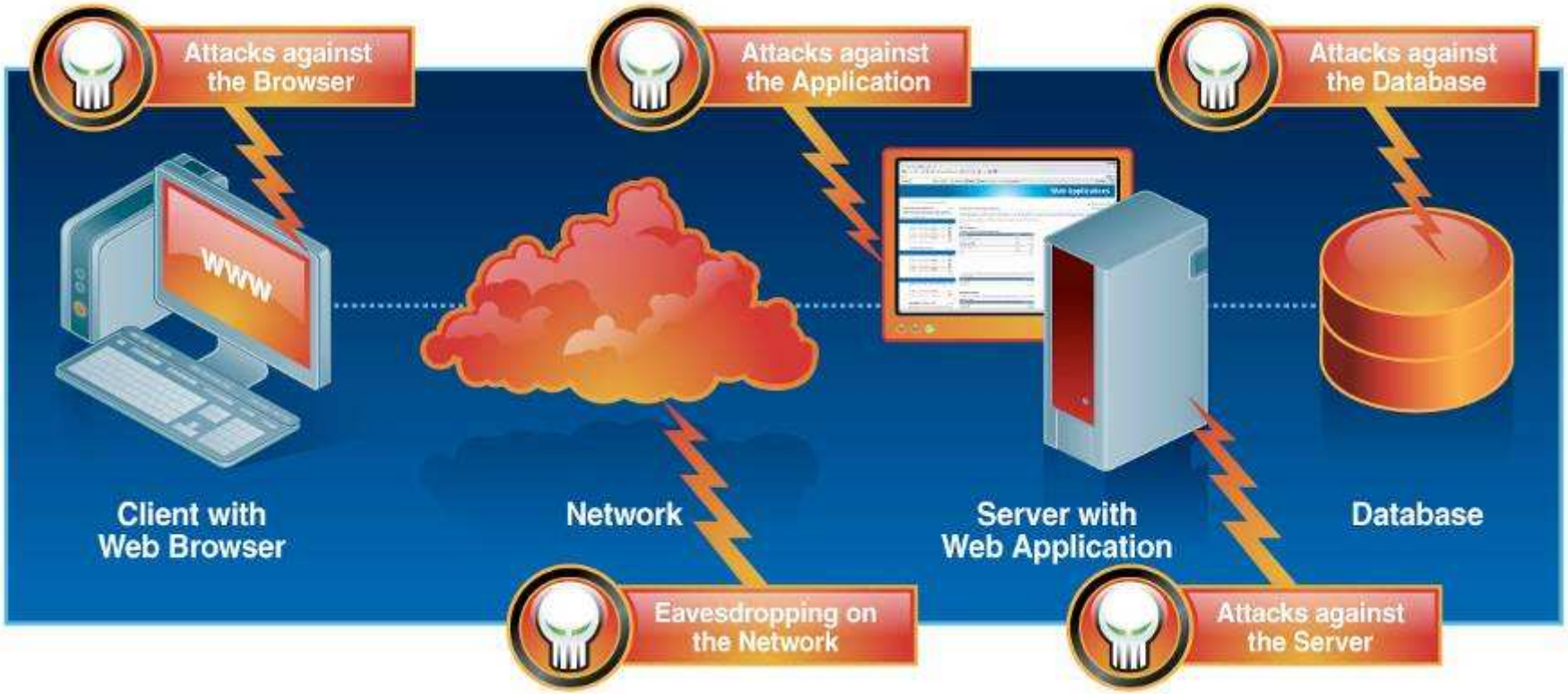
- Ab Gehobenem Mittelstand
- Kunde muss Virtualisierung auf X-Series oder vergleichbar nutzen oder planen
- VMware als Virtualisierungsplattform (VSphere 4 oder höher)
- Quickwins:
  - Security Vorfall
  - Compliance
  - Dediziertes Security Team
  - FSS, IndCom
  - Betrieb von Portalen
  - Kunde weiß, dass er schützenswerte Daten besitzt

Problemstellung beim Kunden



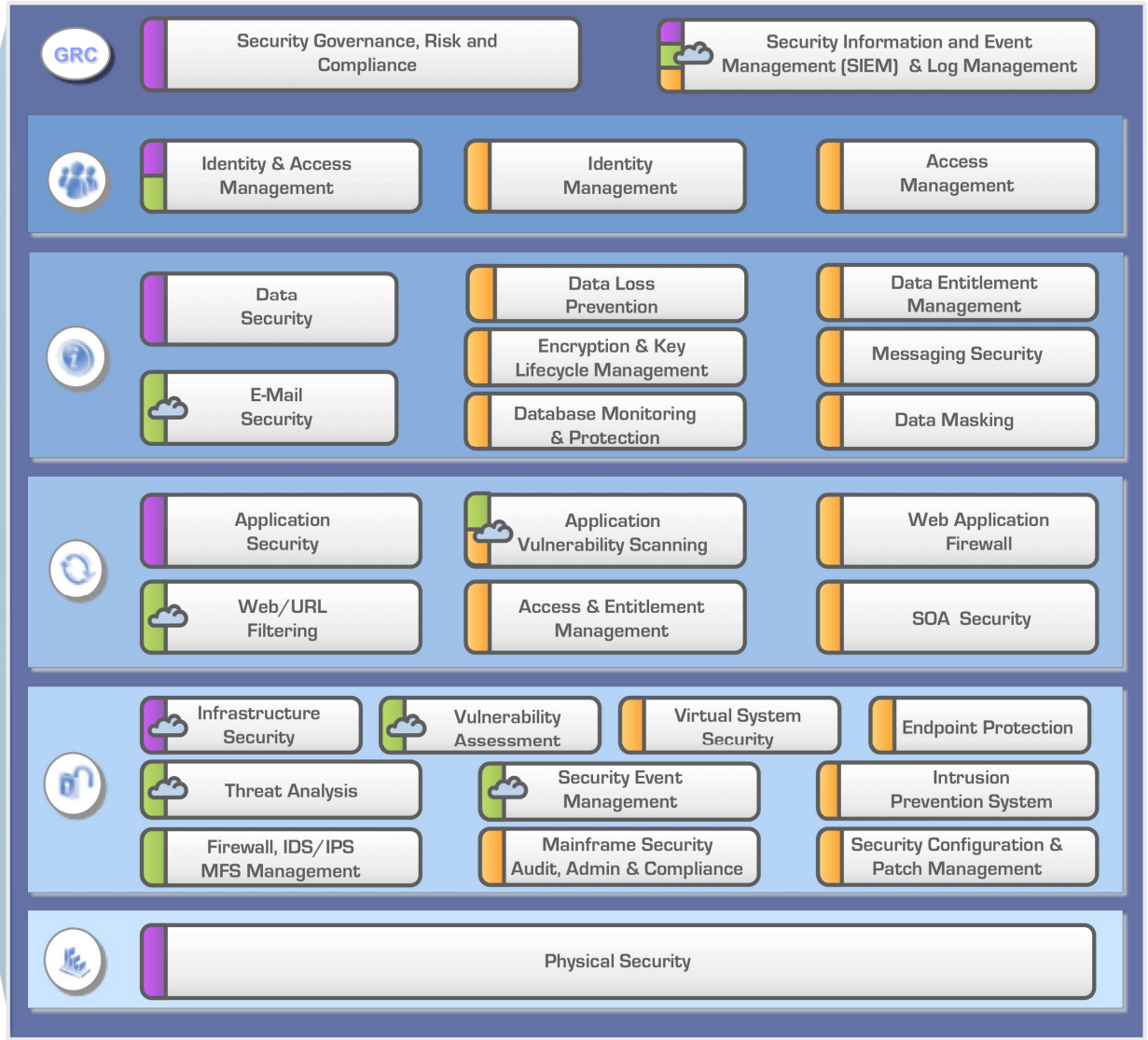
- Neue Gefahrenquellen
- Angst vor Cloud Burst Attack
- Mangelnde Transparenz
- Mangelnde Überwachung der Virtuellen Maschinen
- Betriebskosten / Patch Pain
- Schwierige Umsetzung der Compliance Strategie
- IPS reduziert das unternehmerische Risiko
- Virtueller Patch, auch wenn noch kein Patch verfügbar ist
- Der Wert eines Unternehmens liegt in seinen Mitarbeitern und in der Zuverlässigkeit seiner Daten

Attack Vectors



IBM Security Portfolio

- Professional Services
- Managed Services
- Products
- Cloud Delivered



IBM hat beispiellose Erfahrung in Security

9 Security Operations Centers + 9 Security Research Centers + 133 Monitored Countries + 24,000+ Devices under Contract + 3,700+ MSS Clients Worldwide + 8 Billion+ Events Per Day

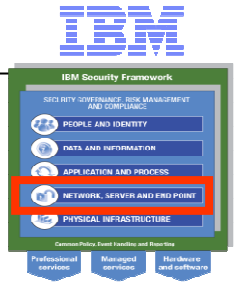
3000+ Security & Risk Management Patente

200+ Security Kunden-referenzen

15.000 Forscher, Entwickler und SMEs in Security

40+ Jahre erfolg-reiche Sicherheit für den Host

2008 für Security 1.8 Milliarden $ investiert



Patches Still Unavailable for Over Half of Vulnerabilities

Over half (55%) of all vulnerabilities disclosed in the 1st half of 2010 had no vendor-supplied patches to remedy the vulnerability. 71% of critical & high vulnerabilities have no patch.

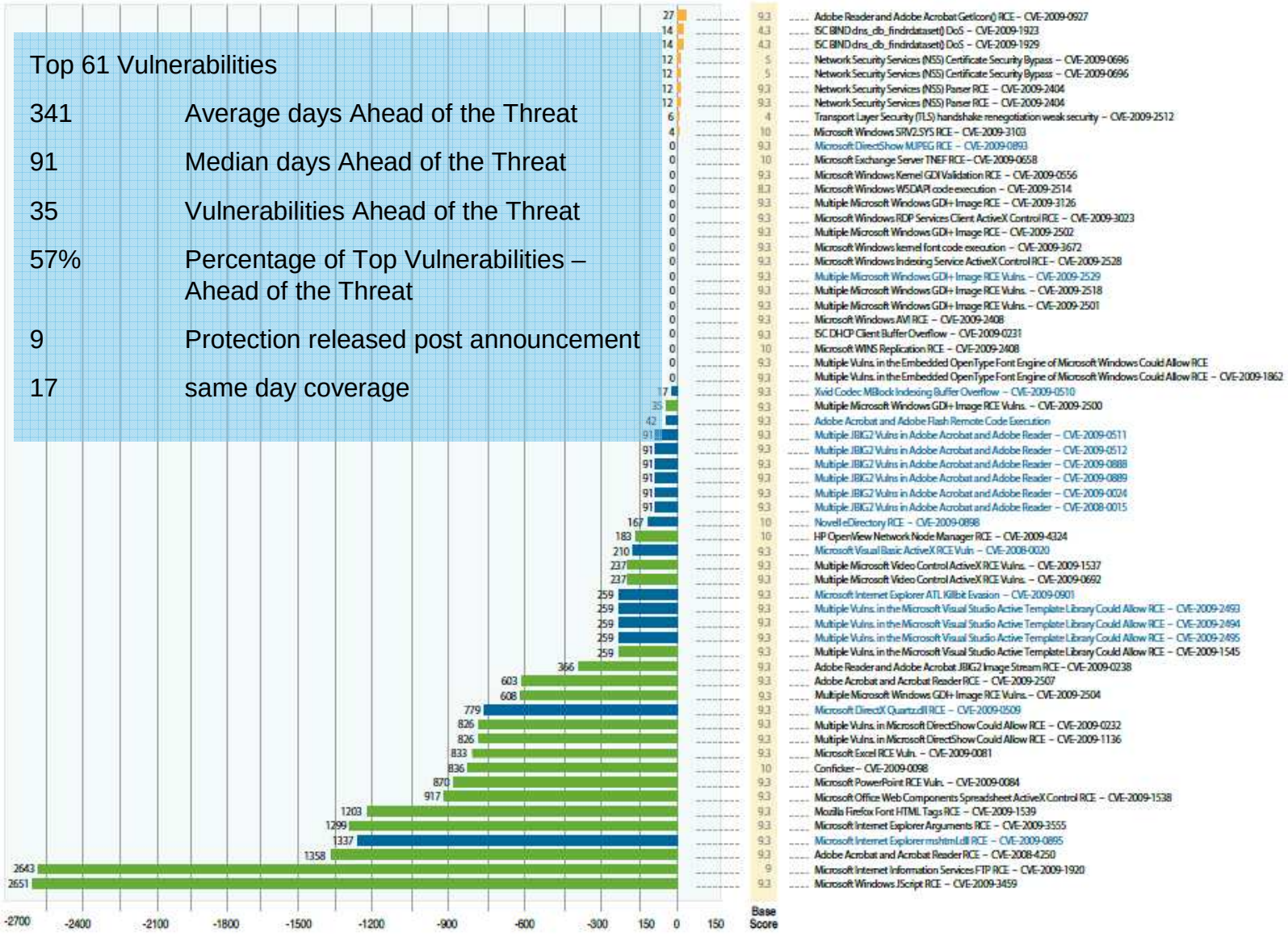
Top five operating systems account for 98% of all critical and high operating system disclosures in the first half of 2010. The top five operating systems account for 95% of all operating system vulnerability disclosures.

Operating System	Percentage of Critical and High	Percentage of all OS Vulnerabilities
Microsoft	73%	27%
Apple	9%	29%
Linux	16%	31%
Sun Solaris	0%	4%
BSD	0%	4%
IBM AIX	0%	2%
HP-UX	2%	1%
Others	2%	4%

Vendor	Percent of 2010 H1 Disclosures with No Patch	Percent of Critical & High 2010 H1 Disclosures with No Patch
All Vendors - 2010 H1 Average	55%	71%
Sun	24%	9%
Microsoft	23%	11%
Mozilla	21%	4%
Apple	13%	0%
IBM	10%	29%
Google	9%	33%
Linux	8%	20%
Oracle	7%	22%
HP	7%	5%
Cisco	6%	2%
Novell	5%	10%
Adobe	3%	2%

Security Effectiveness - Ahead of the Threat

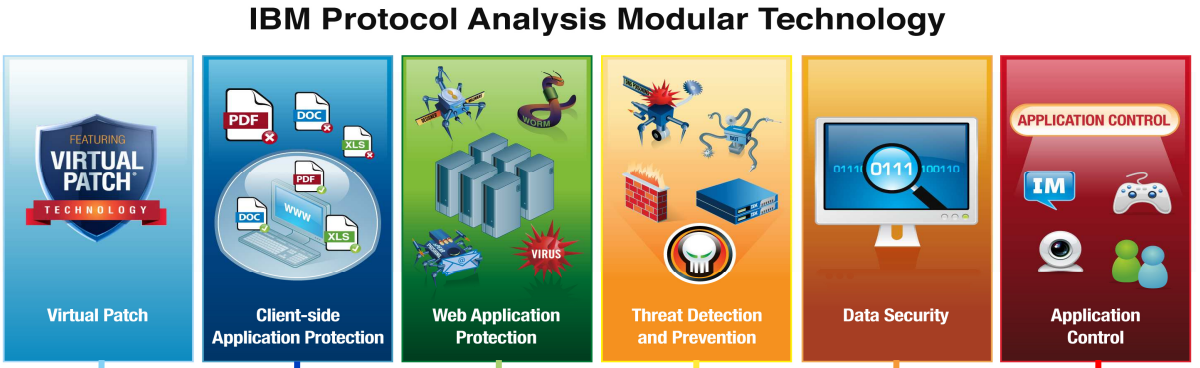
Top 61 Vulnerabilities	
341	Average days Ahead of the Threat
91	Median days Ahead of the Threat
35	Vulnerabilities Ahead of the Threat
57%	Percentage of Top Vulnerabilities – Ahead of the Threat
9	Protection released post announcement
17	same day coverage



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



Virtual Patch

What It Does:
Shields vulnerabilities from exploitation independent of a software patch, and enables a responsible patch management process that can be adhered to without fear of a breach

Why Important:
At the end of 2009, 52% of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability.

Client-Side Application Protection

What It Does:
Protects end users against attacks targeting applications used everyday such as Microsoft Office, Adobe PDF, Multimedia files and Web browsers.

Why Important:
At the end of 2009, vulnerabilities, which affect personal computers, represent the second-largest category of vulnerability disclosures and represent about a fifth of all vulnerability disclosures.

Web Application Protection

What It Does:
Protects web applications against sophisticated application-level attacks such as SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery).

Why Important:
Expands security capabilities to meet both compliance requirements and threat evolution.

Threat Detection & Prevention

What It Does:
Detects and prevents entire classes of threats as opposed to a specific exploit or vulnerability.

Why Important:
Eliminates need of constant signature updates. Protection includes the proprietary Shellcode Heuristics (SCH) technology, which has an unbeatable track record of protecting against zero day vulnerabilities.

Data Security

What It Does:
Monitors and identifies unencrypted personally identifiable information (PII) and other confidential information for data awareness. Also provides capability to explore data flow through the network to help determine if any potential risks exist.

Why Important:
Flexible and scalable customized data search criteria; serves as a complement to data security strategy.

Application Control

What It Does:
Manages control of unauthorized applications and risks within defined segments of the network, such as ActiveX fingerprinting, Peer To Peer, Instant Messaging, and tunneling.

Why Important:
Enforces network application and service access based on corporate policy and governance.

Virtual Patch

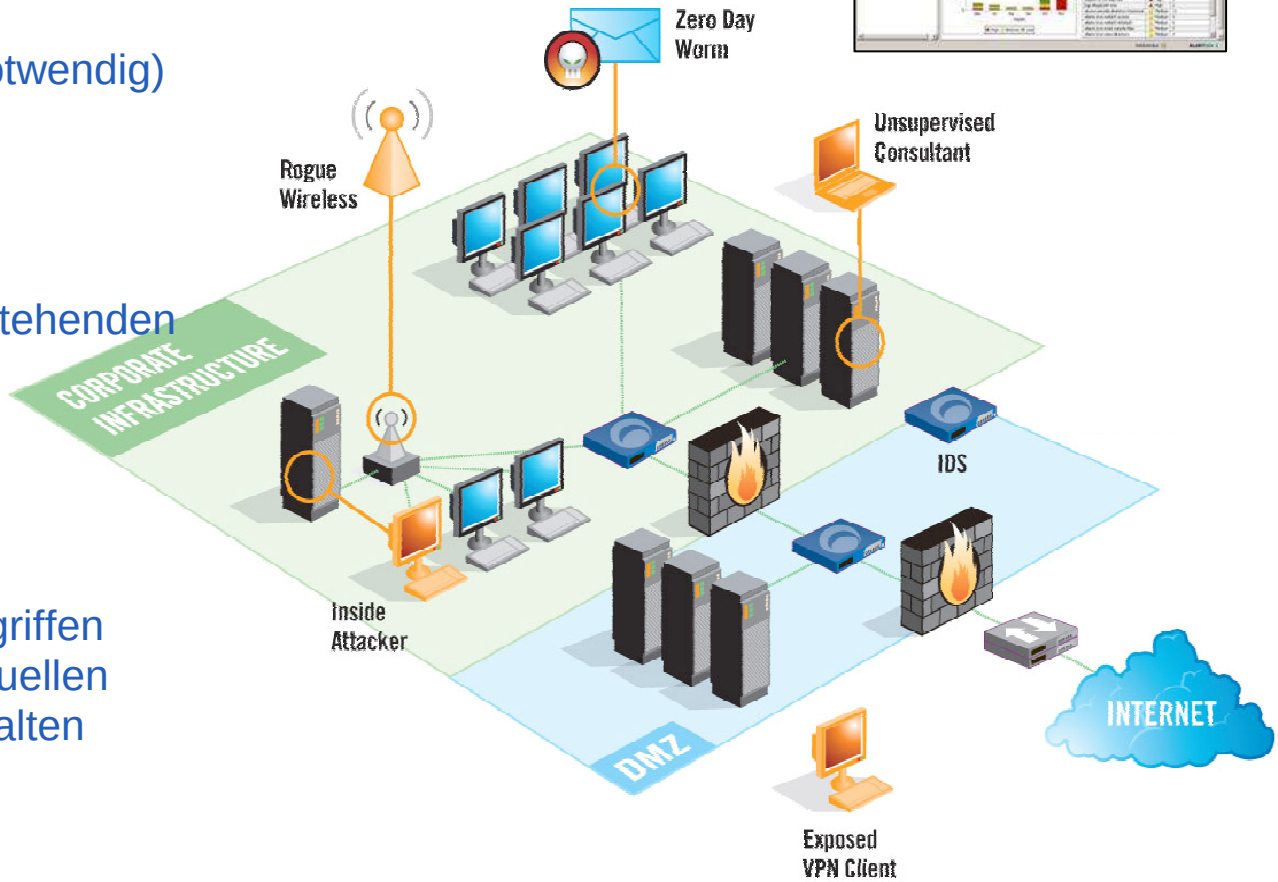
- Reduzierung des Patchaufwandes
- Frühzeitiger Schutz
- Schnelles Roll-Out (falls notwendig)

Abwehr von Angriffen

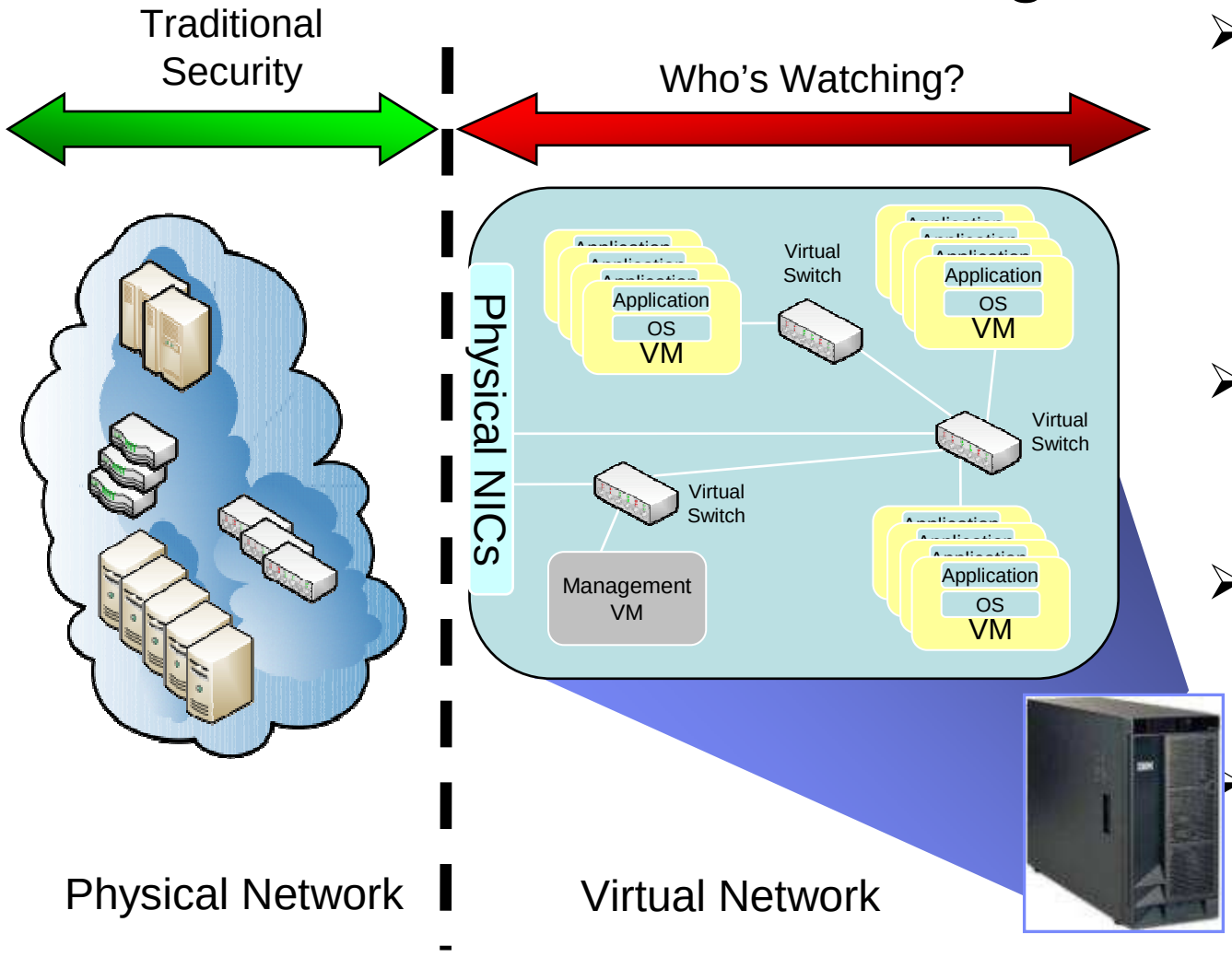
- Blocken von Angriffen
- Keine Ausnutzung von bestehenden Schwachstellen
- Herausfiltern von Malware

Transparenz

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



Server and Network Convergence

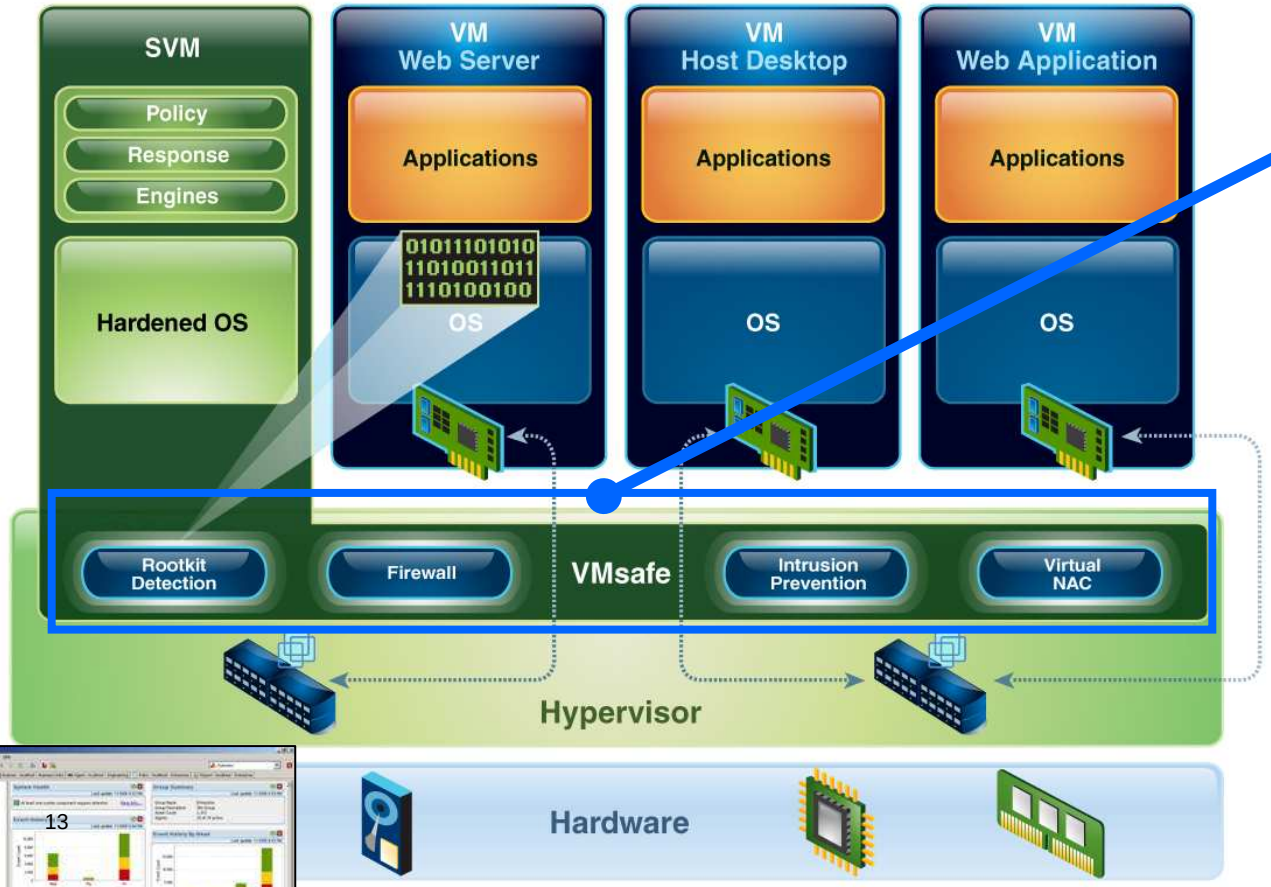


- Security "blind spots" are created as portions of the network becomes part of the server
  - Who owns the virtual network?
- Physical network IDP devices do not provide coverage for inter-VM communication
- Routing virtual network traffic to an external physical device is not practical
- VM sprawl risks
  - what you cannot see will hurt you

IBM Virtual Server Security for VMware

Integrated threat protection for VMware ESX and ESXi

Helps customers to be more secure, compliant and cost-effective by delivering integrated and optimized security for virtual data centers.



IBM Virtual Server Security for VMware

- VMsafe Integration
- Firewall and Intrusion Prevention
- Rootkit Detection/Prevention
- Inter-VM Traffic Analysis
- Automated Protection for Mobile VMs (VMotion)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Infrastructure Auditing (Privileged User)
- Virtual Network Access Control

Nutzen für unsere Kunden

- Optimale Absicherung - Ahead of the Threat
- Geringe Betriebskosten durch ausgereifte Technik
- Erfahrung aus eigenem Betrieb in Produkt eingeflossen
- Reduzierung des Unternehmerischen Risikos
- Einhaltung der Sicherheitsrichtlinien aus physikalischer Infratruktur
- Transparenz und Unterstützung der Compliancerichtlinie
- Erhöhung der Verfügbarkeit
- Ausnutzung des Einsparpotentials aus Virtualisierung

Projektablauf Beispiel

- Definition Projektumfang
- Definition gewünschte Testergebnisse
- Testinstallation in Kundenumgebung mit VMware vSphere 4 oder höher (2 Tage)
- Roll-Out Planung
- Auswertung der Ergebnisse aus Testinstalltion (ca. 3 Wochen nach Inst.)
- Roll-Out abhängig von Kundenumgebung

Teamunterstützung / PoC

- Es steht Ihnen ein Team von Kollegen zur Verfügung, die vom Ersttermin über PoC bis zum Projektabschluss sowohl vertrieblich als auch technisch begleiten.
- PoC ist für den Kunden kostenfrei! MS-SQL Server muss Kunde stellen, natürlich auch den VMware Server
- Dauer PoC: 1 – 2 Tage Installation vor Ort, 3 – 4 Wochen Betrieb, 1 Tag Auswertung
- Typische Projektlaufzeit: 3+ Monate

Call to Action

- Wecken Sie das Interesse Ihrer Kunden!
- Nehmen sie uns mit zu Ihren Kundenterminen
- Bieten sie Ihren Kunden einen kostenfreien PoC an
- Sprechen sie mit uns!
- Merke: Die IT-Lösungen unserer Kunden sind nur dann wirtschaftlich, wenn sie sicher betrieben werden können.

- Einstiegsfragen:
  - Es werden pro Jahr ca. 8000 Schwachstellen dokumentiert, wie bewertet Ihr Unternehmen diese Bedrohung Tag für Tag?
  - Wie begegnen sie den Gefahren, die in Virtualisierung stecken?
  - In Virtualisierung steckt viel Einsparpotential, aber wie haben sie Ihre Sicherheitstrategie und Ihre Compliancestrategie in einer virtuellen Umgebung umgesetzt?
  - Nutzen sie schon das volle Einsparpotential, dass in Virtualisierung steckt?

Need to know

- VSP ist PA
- Berechnung nach PVU
- SVI berechtigt (Security oder ISS Zertifizierung)
- Open Distribution

IBM Virtual Server Protection for VMware

http://www-01.ibm.com/software/tivoli/products/virtual-server-protection/

Solution Description

Warum bringt IBM Virtual Server Protection for VMware mehrSicherheit invirtuellen Umgebungen?

IBM Virtual Server Protection for VMware, ist eine der führenden Solution im Security Markt und eine Erweiterung der hostbasierenden Intrusion Detectionund Intrusion Prevention Systeme.
Diese Solution beinhaltet Threat Protection und Security Compliance für VMware vSphere™ 4 und höher. Diese bietet Ihnen **Best of Breed Security** im Reselling, im On Site Betrieb beim Kunden und im Outsourcing. Im Einzelnen sind dies:

- **Reselling**: Sie partizipieren an den günstigen Einkaufskonditionen der IBM und haben einen leistungsfähigen und erfahrenen 2nd Level Support, da diese Solution auch in den eigenen Dynamic Computing Rechenzentren eingesetzt werden kann.
- **On Site Betrieb**: Auch in Ihren Rechenzentren kann die Kompetenz und langjährige Erfahrung unser Technikabteilung z.B. im Intrusion Prevention Bereich 7 x 24 genutzt werden.
- **Outsourcing**: Wenn Sie Ihre Applikationen in die Rechenzentren der IBM auslagern und die Dynamic Computing Plattform mit VMware nutzen, profitieren Sie automatisch/ auf Wunsch von der erhöhten Sicherheit dieser Solution.

Welche Security Herausforderungen sind in einer virtuellen Umgebung zu bewältigen?

Neben den enormen Einsparpotentialen der virtualisierten Umgebungen werden Sie mit enormer Komplexität und bedingt dadurch mit völlig neuen Risiken konfrontiert.

- **Neue Komplexität**
  - Dynamische Verlagerung von VMs.
  - Steigende Anzahl von Layern sind zu managen und zu schützen.
  - Viele Betriebssysteme und Applikationen sind auf einem physikalischen Server.
  - Physikalische Verbindungen zwischen den Systemen sind eliminiert bzw. virtuell.
  - Tracken von Software und Konfigurationen, insbesondere aktuellen Patches.
- **Neue Risiken**
  - Virtuelles Ausbreiten (Sprawl), dynamisches Reloaden und damit verbunden Angriffe auf/ oder Diebstahl von VMs.
  - Angriffe aufs Management von Storage und Management Daten auf VMs.
  - Bedingt durch das Ressourcen Sharing ist der Hypervisor Single Point of Failure für Angriffe.
  - Virtuelle NICs und virtuelle Hardware sind Ziele von Angriffen und heimliche Rootkits in der Hardware.

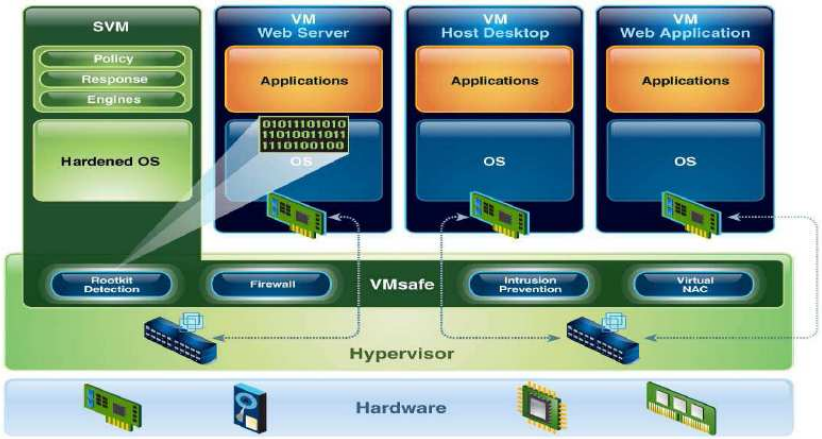
Business Benefits

Virtual Server Protection for VMware ermöglicht Ihnen, die Vorteile der Virtualisierung zu nutzen, ohne gleichzeitig die Sicherheit zu reduzieren.

Jeder Layer der dynamischen Infrastruktur wird auch dynamisch gesichert. Dies sind im Einzelnen:Hypervisor, Betriebssystem, Netzwerk, Applikation, Vituelle Maschine (VM),Inter VM Traffic

Wem bringt die IBM Virtual Server Protection for VMware welche Vorteile?

- CEO:
  - Erfüllen Sie auch in Ihren virtuellen Umgebungen die **Compliance-Anforderungen** die Ihnen aus Ihrer Company und besonders aus den Regelungen und Gesetzen erwachsen. Mit Virtual Server Protection for VMware entstehen keine Lücken, keine Angreifbarkeit und damit für Siekeine persönliche Haftung.
  - Die Szene der Angreifer wird immer krimineller. Beim Bekanntwerden von gelungenen Angriffen droht Ihnen und Ihrer Firma großer **Imageverlust**. Obwohl dieser nicht sofort finanziell benennbar ist, wirkt er sich doch in Form von **Produktions- und /oder Umsatzverlust** für die Company aus.
- IT Manager
  - **Entlasten Sie Ihr IT Budget**, denn konventionelle, nicht virtualisierte Security kostet Sie letztendlich mehr Budget bei gleichzeitig nicht optimalem Sicherheitslevel.
  - Behalten Sie **einfach den Überblick** über Ihre Security, da alle Features über nur eine homogene Solution erbracht werden und damit Monitoring und Reporting einheitlich erbracht werden können.
- Admins
  - **Minimierung von Fehlverhalten** bringt auch Sicherheit und Entlastung in die Administration und gleichzeitig wird **schnelles und effektives Reagieren** bei Angriffen sichergestellt.



Peter Häufel
Senior Solution Sales Professional
IBM Security Solutions

Mobile 0175-7252260
Email haeufel@de.ibm.com

Thank you !