

Lifecycle Management und Endpoint Security – Tivoli Endpoint Manager (TEM) basierend auf BigFix Technology





- Wer und was ist **BigFix**?



Fakten zu BigFix...

- 1997 in Emeryville, California gegründet
- Das erste Produkt war eine Self-Service System Management Applikation
- 2002 entstand daraus die Enterprise Software Plattform BigFix
- 2007 Erweiterung der Plattform gezielt in Richtung Security und System Vulnerability Management
- Mehr als 900 Kunden (Stand 2010)
- Am 20. Juli 2010 wurde BigFix an IBM verkauft
- Seit 1.2.2011 ist BigFix offiziell in IBM integriert.
BigFix heisst jetzt Tivoli Endpoint Manager



Klassischer Ansatz im
Bereich
Endpoint Mgmt.
(Security / Patch Mgmt.)



Klassische Softwareverteilung / Provisioning und Patch Mgmt.





Nachteile

- u.U. viel zu langwierig und teuer (an Ressourcen)
- Hohe Fehlerquoten
- Kein aktuelles Bild der Situation im Netz
- Schützt nicht vor Manipulationen
- Besitzt keine oder geringe Abwehrmechanismen
- Erfordern hohe Disziplin
- Basiert auf Vertrauen



Nachteile

- u.U. viel zu langwierig und teuer (an Ressourcen)
- Hohe Fehlerquoten
- Kein aktuelles Bild der Situation im Firmennetz
- Schützt nicht vor Manipulationen
- Besitzt keine oder geringe Abwehrmechanismen
- Erfordern hohe Disziplin
- Basiert auf Vertrauen

Im Security Umfeld ist die Kenntnis über die aktuelle Situation sowie die Möglichkeit zur schnellen Reaktion auf einen Incident entscheidend!



Was ist der Hauptunterschied von BigFix zu anderen Tools?



BigFix – ein Policy basierendes Modell!





Vorteile

- Sehr schnell und Ressourcen schonend
- Hohe Erfolgsquote schon beim ersten “Durchlauf”
- Ständig aktuelles Bild der Ist-Situation
- Schützt vor Manipulationen und Angriffen
- Besitzt Abwehrmechanismen (Agent)
- Agent setzt dauerhaft jede Policy durch / um
- Basiert auf ständiger Kontrolle



Tivoli Endpoint Manager: kontinuierliche Endpoint Compliance

Traditional compliance



Continuous compliance

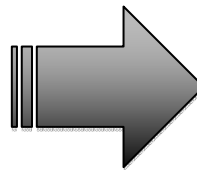


- Keine 'high-risk' Perioden
- Geringere Kosten
- Kontinuierliche Verbesserung



Closed Loop Speed is Our Advantage

Traditional Solutions



TEM

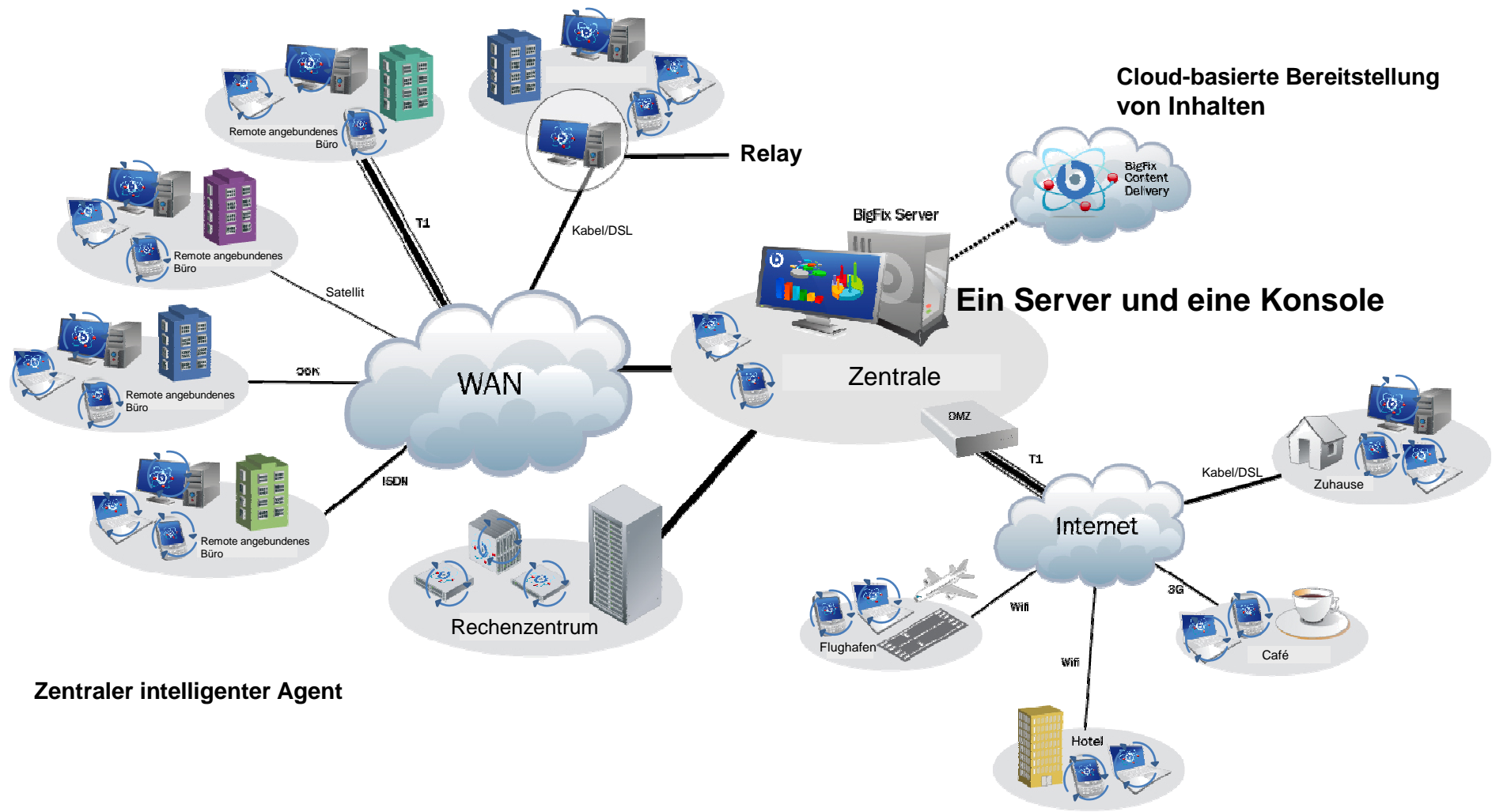


Challenge	Traditional client/server tools	TEM Platform
Complete the policy enforcement loop	Everything is controlled by the server, which is slow	Distributed computing with intelligent, universal agent
Increase the accuracy and speed of your knowledge	It can take days to accurately close the enforcement loop	Policy enforcement is accomplished and proven in minutes instead of days
Scalability cannot be attained without large infrastructure investments	Administrators are still managing tools instead of being productive	Distributed processing means scalability is unlimited
Adjust system policies depending on environment, location	Scan-based assessment, leading to stale data false sense of awareness	Real-time situational awareness



BigFix Architektur

Schlanke, leistungsfähige Infrastruktur



Cloud-basierte Bereitstellung von Inhalten

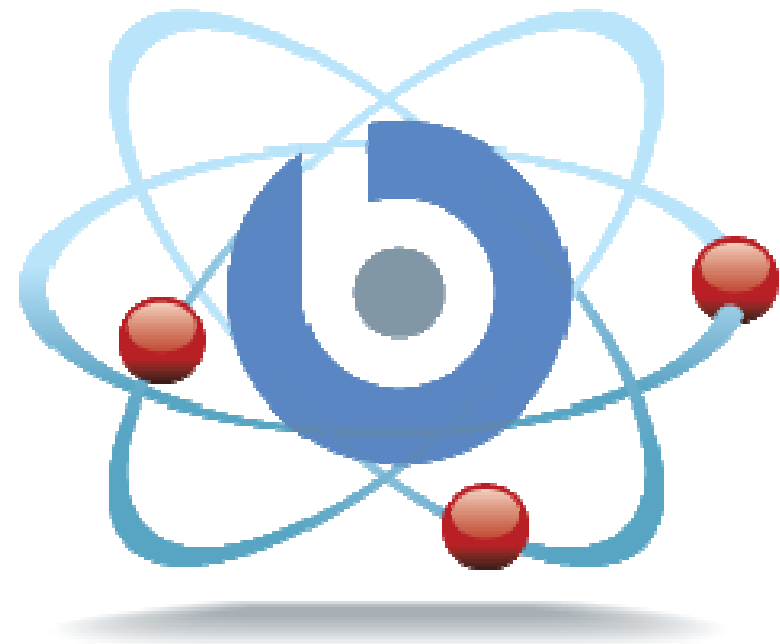
Ein Server und eine Konsole

Zentraler intelligenter Agent



BigFix erreicht die zeitnahe und zugleich hoch skalierbare Lifecycle Management Funktionalität durch seine intelligente Architektur

- Cloud basierte Bereitstellung von bekannten Software Korrekturen für Betriebssysteme und Anwendungen (Fixlets) erspart aufwändiges Erstellen von Paketen
- Zentrale Management Oberfläche optimiert auf das Management von tausenden von Systemen (bis zu 250.000 Systeme mit nur einem Server!)
- Extrem robuste Agententechnologie für maximale Zuverlässigkeit beim Ausführen von Aktionen
- Effektive Nutzung von zur Verfügung stehender Bandbreite und minimaler Footprint auf den administrierten Systemen





Ein Hauptanwendungsfall von BigFix ist die automatisierte Software- und Konfigurationspflege von Systemen

- Zentral bereitgestellte Bibliothek von typischen Fixes oder selbst erstellte Fixlets/Tasks
 - Multi Vendor (Microsoft, Adobe, Oracle, IBM,...) Multi OS (Win, Mac,...)
 - Eigene Erstellung über Wizards oder Script Sprache (Relevance)
- Statische oder dynamische Zuordnung von Systemgruppen
 - Alle Windows 7 Systeme, alle Test-Systeme, alle System mit 8 GB Hauptspeicher – per Query der erfassten Attribute völlig flexibel
- Festlegung der Installation
 - Sofort, zwingend, wahlfrei (als Angebot), in einem bestimmten Zeitfenster, nachts, ...
- Sofortige Rückmeldung des Systemstatus nach erfolgter Ausführung
 - Aktualisierung der Datenbank

The screenshot displays the BigFix Enterprise Console interface. The main window is titled "BigFix Enterprise Console" and features a menu bar (File, Edit, View, Go, Tools, Help) and navigation buttons (Back, Forward, Show Hidden Content, Show Non-Relevant Content, Refresh Console). The interface is divided into several sections:

- Patch Management:** A tree view on the left shows the hierarchy: Patch Management Domain, Application Vendors, OS Vendors, All Patch Management, Fixlets and Tasks (6,457), Baselines (1), Analyses (12), Actions (0), Dashboards, Wizards, Custom Content, Custom Filters, Computers (10), Computer Groups (0), and Sites (3).
- Fixlets and Tasks Table:** A table on the right lists various updates with columns for Name, Source, and Site. The table includes entries such as "Flash Player 10 Available - Internet Explorer", "MS10-042: Vulnerability in Help and Support Center Could...", "MS03-011: Flaw in Microsoft VM Could Enable System Com...", "MS10-035: Cumulative Security Update for Internet Explo...", "MS10-034: Cumulative Security Update of ActiveX Kill Bits...", "MS10-035: Cumulative Security Update for Internet Explo...", "MS10-033: Vulnerabilities in Media Decompression Could Al...", "MS10-033: Vulnerabilities in Media Decompression Could Al...", "MS10-034: Cumulative Security Update of ActiveX Kill Bits...", "MS10-033: Vulnerabilities in Media Decompression Could Al...", "MS10-033: Vulnerabilities in Media Decompression Could Al...", "MS10-033: Vulnerabilities in Media Decompression Could Al...", and "MS10-042: Vulnerability in Help and Support Center Could...".
- Fixlet Details:** Below the table, the selected fixlet "Flash Player 10 Available - Internet Explorer" is shown. It includes a "Description" tab, "Applicable Computers (4)", and "Action History (0)". The description text reads: "Adobe has released a new version of Flash Player (10.1.53 below to update the Flash Player ActiveX control to the latest version." It also includes an "Important Note" and a "Note" regarding affected computers and service interruptions.



BigFix bietet auch die Möglichkeit die erfassten Daten auszuwerten – interaktiv in der BigFix Konsole

- Grundsätzliche Erfassung der Computer Systeme mit ihren Eigenschaften erfolgt permanent aktuell, da BigFix die Daten für die Zuordnung der Fixlets auswertet
- Neben installierter Software werden auch Systemeigenschaften erfasst
 - Hardware Eigenschaften
 - z.B. auch angeschlossene USB Devices
- BigFix kann diese Informationen direkt verarbeiten
 - z.B. beim Anschluss eines USB Sticks eine Aktion ausführen

The screenshot displays the BigFix Enterprise Console interface. The main window shows a list of computers with columns for OS, IP Address, CPU, and Last Report Time. Below the list, a detailed view for a computer named 'GRIPHOOK' is shown, including a 'Computer Properties' section with 'Core Properties' such as OS (WinXP 5.1.2600), CPU (2700 MHz Xeon), and IP Address (192.168.119.35).

OS	IP Address	CPU	Last Report Time
Win2000 5.0.2195	192.168.119.110	2700 MHz Xeon	7/19/2010 2:07...
Win2000 5.0.2195	192.168.119.111	2700 MHz Xeon	7/19/2010 2:07...
Win2003 5.2.3790	192.168.119.15	2800 MHz Xeon	7/19/2010 2:10...
Win2003 5.2.3790	192.168.119.16	2800 MHz Xeon	7/19/2010 2:11...
Win2008 6.0.6002	192.168.119.115	2700 MHz Xeon	7/19/2010 2:03...
Win2008 6.0.6002	192.168.119.116	2700 MHz Xeon	7/19/2010 2:03...
WinXP 5.1.2600	192.168.119.35	2700 MHz Xeon	7/19/2010 2:11...
WinXP 5.1.2600	192.168.119.203	2700 MHz Xeon	7/19/2010 2:10...
WinXP 5.1.2600	192.168.119.120	2700 MHz Xeon	7/19/2010 2:08...
WinXP-2003 5.2.3790	192.168.119.121	2700 MHz Xeon	7/19/2010 2:07...

Computer: GRIPHOOK

Summary | Relevant Fixlet Messages (14) | Applicable Tasks (60) | Relevant Baselines (1)

Computer Properties

Core Properties

Active Directory Path	dracoprod / Computers / GRIPHOOK
OS	WinXP 5.1.2600
CPU	2700 MHz Xeon
DNS Name	Griphook.dracoprod.com
IP Address	192.168.119.35
Last Reported	7/19/2010 2:11:24 PM
Locked	No



Elemente der BigFix Plattform



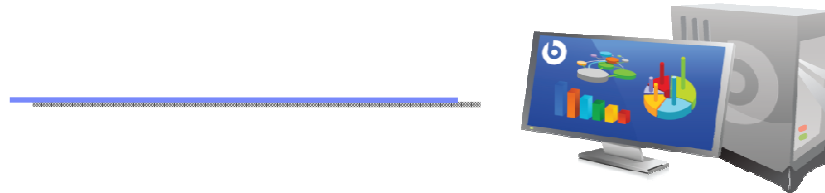
Intelligenter Agent

- Kontinuierliche Selbst-Überprüfung (Compliance)
- Kontinuierliche Richtlinien-Durchsetzung
- Geringe Systembelastung (<2% CPU)
- Gleicher Agent für verschiedene Plattformen



Leistungsfähige Richtlinien Sprache (Fixlets)

- Tausende vorgefertigte Richtlinien
- Zur Erfassung von Informationen, Ausführung von Programmen, Installation for Software
- Best Practices für Operating und Security Abteilung
- Einfache Richtlinienerstellung
- Leicht erweiterbar / anwendbar auf alle Plattformen



Nur ein Server & Konsolen

- Sehr sicher und hohe Verfügbarkeit
- Aggregiert Daten, analysiert und berichtet
- Management von mehr als 250.000 Endpunkten
- Echtzeit Transparenz und Kontrolle



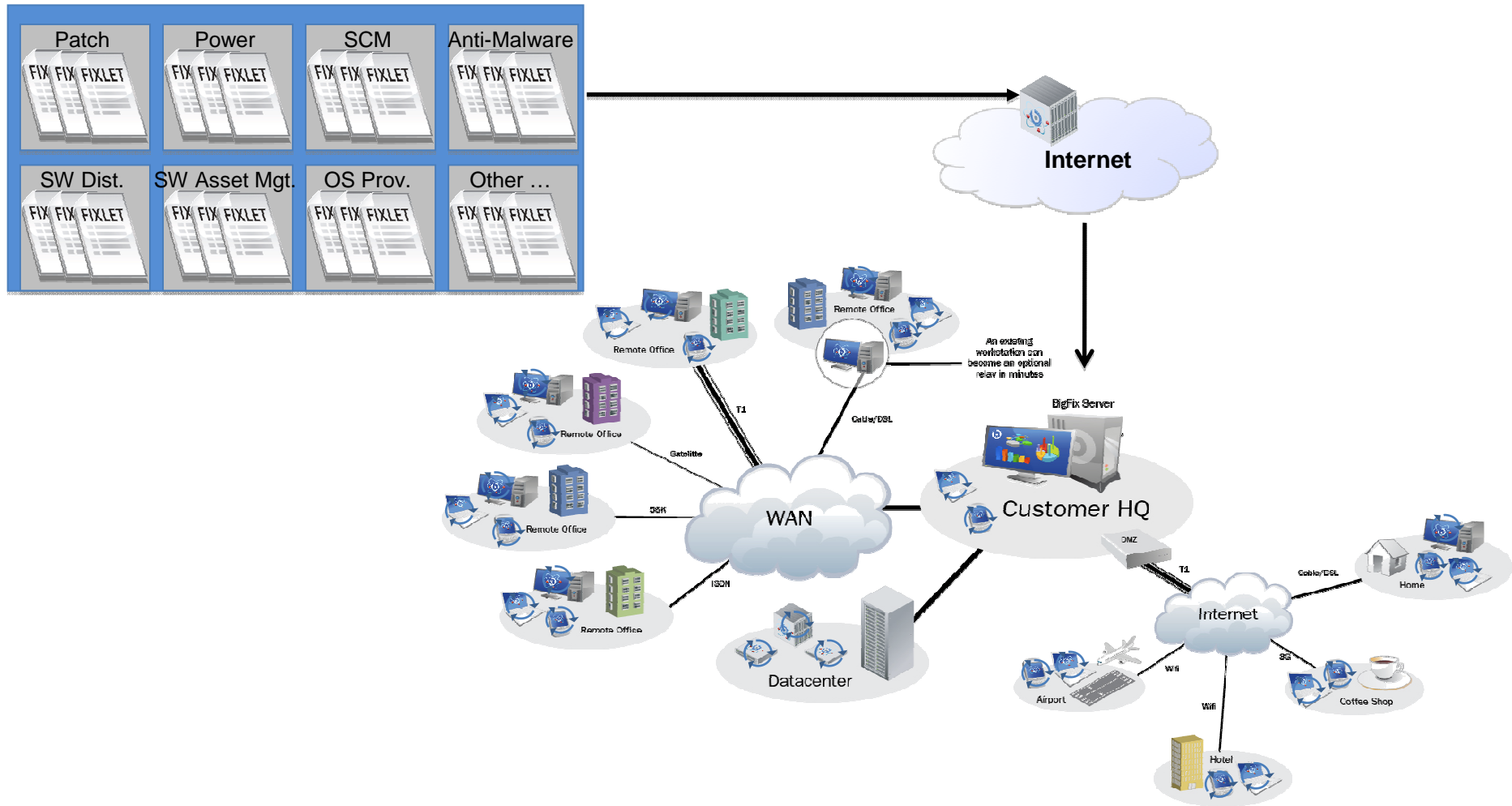
Virtuelle Infrastruktur

- Einsatz von BigFix Relays zur Entkopplung des Datenverkehrs vom Server
- höhere Verfügbarkeitsanforderungen (Failover)
- Nutzen von existierenden Systemen / gemeinsame Infrastruktur



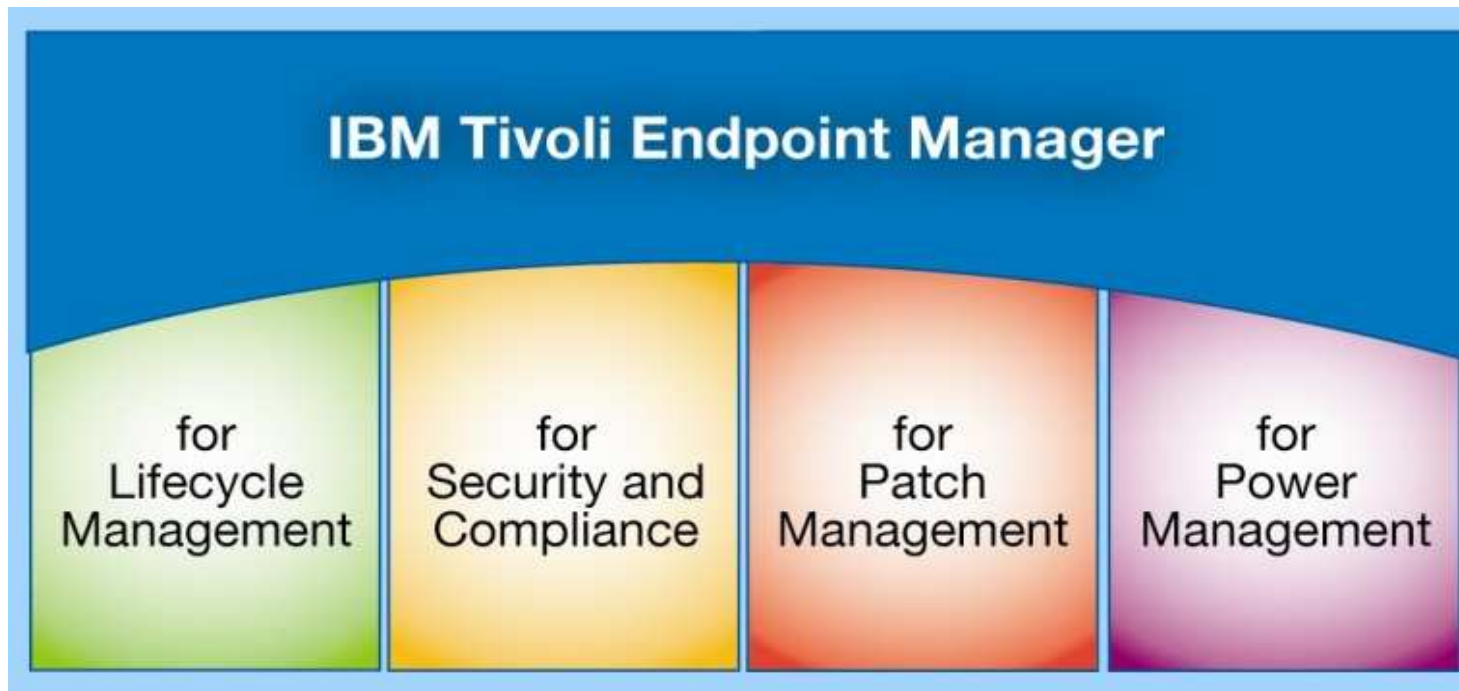
BigFix: “Content” basiertes Delivery Modell

BigFix Content Sites





Die vier Module von BigFix (TEM)



- Power Management ist nur in Zusammenhang mit einem der drei anderen Module verfügbar
- Patch Management ist bereits in den Modulen Lifecycle Mgmt. und Security and Compliance Mgmt. enthalten.



Tivoli Endpoint Manager: Intelligentes, autonomes und schnelles Endpoint Management

- Network Asset Discovery
- Endpoint HW, SW Inventory
- Patch Management
- Software Distribution
- OS Deployment
- Remote Desktop Control
- Software Use Analysis (add on)
- Power Management (add on)

- Patch Management
- Security Configuration Management
- Vulnerability Management
- Asset Management
- Network Self Quarantine
- Multi-Vendor Endpoint Protection Management
- Anti-Malware & Web Reputation Service (add on)



Zusammenfassung / Vorteile der BigFix Lösung

- Mit der Übernahme von BigFix verfügt IBM Tivoli über eine skalierbare und ausgereifte, umfassende und hochperformante End-to-End-Lifecycle Lösung
- Systemkonsolidierung: ein System für das gesamte Desktopmanagement
- Heterogene Landschaft wird unterstützt, ebenso wie mobile Endgeräte:
Windows-Desktopsysteme und -Server (einschließlich Win7), Windows Point of Sale und mobile Endgeräte, MacOS, Linux (RedHat, RedHat Enterprise, Fedora, SUSE/SLES, Oracle Linux, Ubuntu, Debian), zLinux, AIX, HP-UX und Solaris
- Echtzeit Kontrolle und Reporting
- Kontinuierliche richtlinienbasierte Überwachung und automatische Wiederherstellung mit über 175.000 sofort einsatzfähigen Richtlinien (sogenannte Fixlets) – täglich wachsend!
- Vollautomatisierte Basis Systembereitstellung und Migration
- Hochperformantes und skalierbares Patch Management für alle Plattformen
Vollständiger Patch Automation-Service bietet Alerts und automatische Downloads von Patches für alle unterstützten Plattformen
- Schnelle und günstige Projektrealisierung
- Kombination von BigFix mit der IBM Service Management-Strategie



Konsolidierung der Managementinfrastruktur

Vor dem TEM

Mit TEM

Software-
verteilung

e.g., LANDesk



Patch-Mgmt

e.g., Microsoft



Security-
Konfiguration

e.g., NetIQ, CA



Asset & License
Management

e.g., Altiris - Asset
Manager



Endpoint
Protection

e.g., McAfee
EPO



Mit TEM



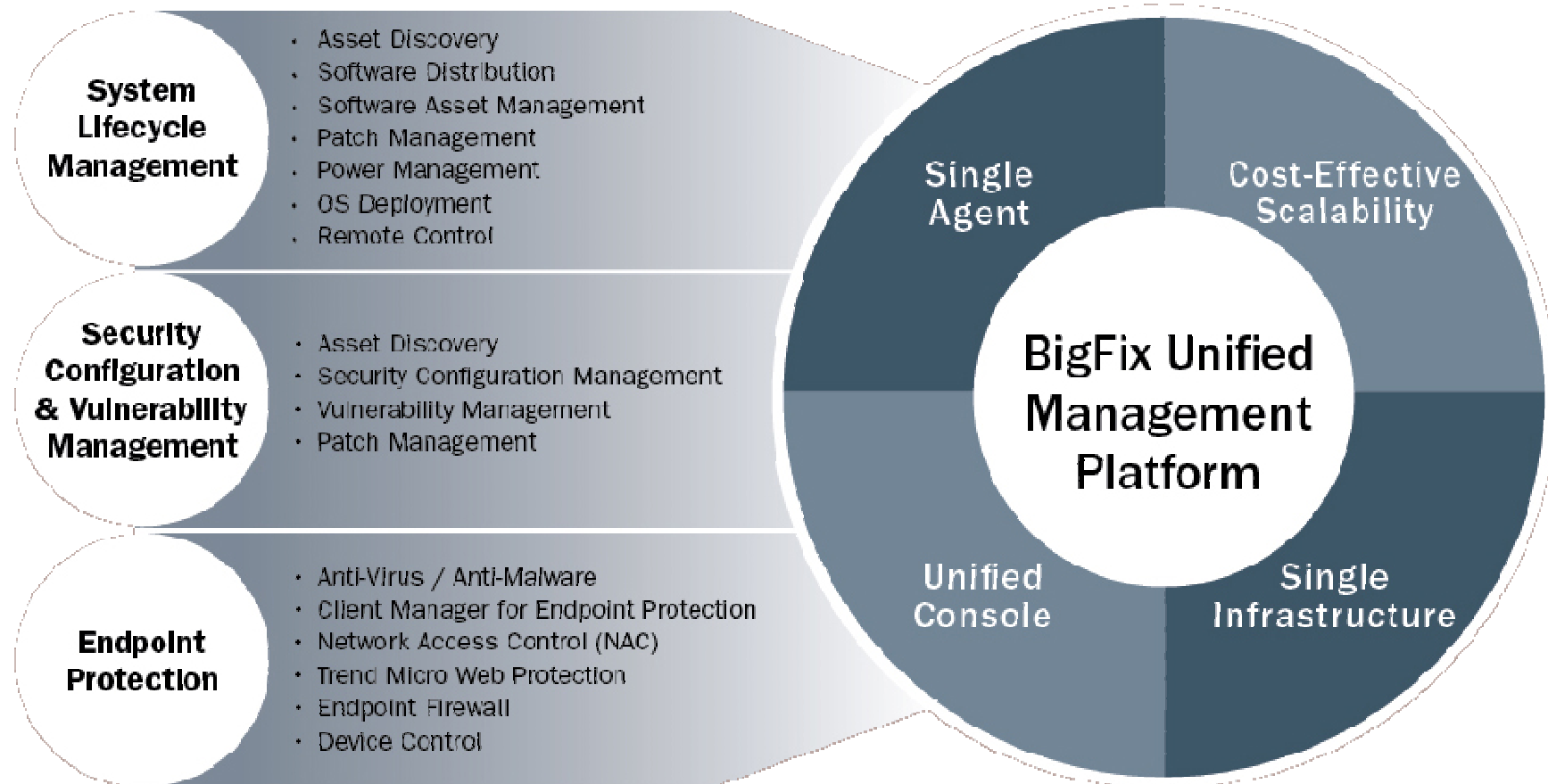
- 1 Server
- 1 Agent auf dem Endpoint
- 1 Konsole
- Implementiert in Wochen

100 - 125 Server / 5 verschiedene Konsolen / 5 Agenten auf dem Client, Implementiert in Jahren



Was BigFix bietet...

Die “Unified Management Platform” von BigFix bietet immer eine aktuelle Sicht auf und die Kontrolle über Ihre IT-Infrastruktur. Dies erfolgt mit Hilfe einer einzigen Konsole und nur eines Agenten pro Endgerät.





Schulungsangebote für den Tivoli Endpoint Manager

- 18.Juli IBM Tivoli Endpoint Manager 8.1 Introduction TP4110DE
- 19.Juli IBM Tivoli Endpoint Manager 8.1 Administration TP4210DE
- 20/21.Juli IBM Tivoli Endpoint Manager 8.1 Content Development TP4310DE
- 22. Juli IBM Tivoli Endpoint Manager 8.1 Advanced Master Operator TP4410DE

Weitere Informationen finden Sie unter:

<http://www.ibm.com/training/de/tivoli>



Roadshow für den Tivoli Endpoint Manager

Das IBM Software Partner Academy Programm freut sich, Sie zur System Management Roadshow - Patch-/Lifecycle- und Sicherheitskonfigurationsmanagement mit Tivoli Endpoint Manager im Juli & August 2011 einladen zu dürfen:

Mit Tivoli Endpoint Manager sind sie in der Lage gleich mehrere Agenten & Tools bei Ihren Kunden zu ersetzen. Tivoli Endpoint Manager kann innerhalb von kürzester Zeit deployed werden und bietet damit einen einmalig schnellen ROI. Schauen sie vorbei, erfahren sie mehr.

- **Agenda:**

09:45 - 10:00	Begrüßung
10:00 - 11:00	Tivoli Endpoint Manager - Vorstellung (Sales Pitch)
11:00 - 11:15	Pause
11:15 - 12:15	Tivoli Endpoint Manager - Demo
12:15 - 13:00	Mittag
13:00 - 13:30	Fragen & Antworten

- **Zielpublikum:** Business Partner & Kunde



Roadshow für den Tivoli Endpoint Manager

- aktuelle geplante Termine:

Hamburg 19. Juli 2011

<https://www-927.ibm.com/servers/eserver/storageplaza/BERT.nsf/pages/abstractHAM?OpenDocument&EventID=890810F631CFA3648525789D00292920&lang=ge>

Berlin 20. Juli 2011

<https://www-927.ibm.com/servers/eserver/storageplaza/BERT.nsf/pages/abstractBLN?OpenDocument&EventID=136475A3CD7851968525789D005273F3&lang=ge>

Düsseldorf 25. Juli 2011

<https://www-927.ibm.com/servers/eserver/storageplaza/BERT.nsf/pages/abstractDUE?OpenDocument&EventID=A4E2099024F7331E8525789D0028F68D&lang=ge>

Ehningen 28. Juli 2011

<https://www-927.ibm.com/servers/eserver/storageplaza/BERT.nsf/pages/abstractSTU?OpenDocument&EventID=2E08BDBA6CC10C4D8525789C00390450&lang=ge>

München 02. August 2011

<https://www-927.ibm.com/servers/eserver/storageplaza/BERT.nsf/pages/abstractMUN?OpenDocument&EventID=F1D9C3EBA6AC0D1D8525789C004EE013&lang=ge>

Frankfurt am Main 03. August 2011

<https://www-927.ibm.com/servers/eserver/storageplaza/BERT.nsf/pages/abstractFRA?OpenDocument&EventID=8F094A86725BE24D8525789C003558DC&lang=ge>

Melden Sie sich heute noch an, Ihre IBM Software Partner Academy!

(Bei Fragen wenden Sie sich Bitte an die email: ibmpartneracademy@de.ibm.com)



Fragen?

- **Kontakt Daten:**

Sascha Buhr

Leading Solution Sales Professional - BigFix

+49 - 160 - 71 67 68 4

sascha.buhr@de.ibm.com

