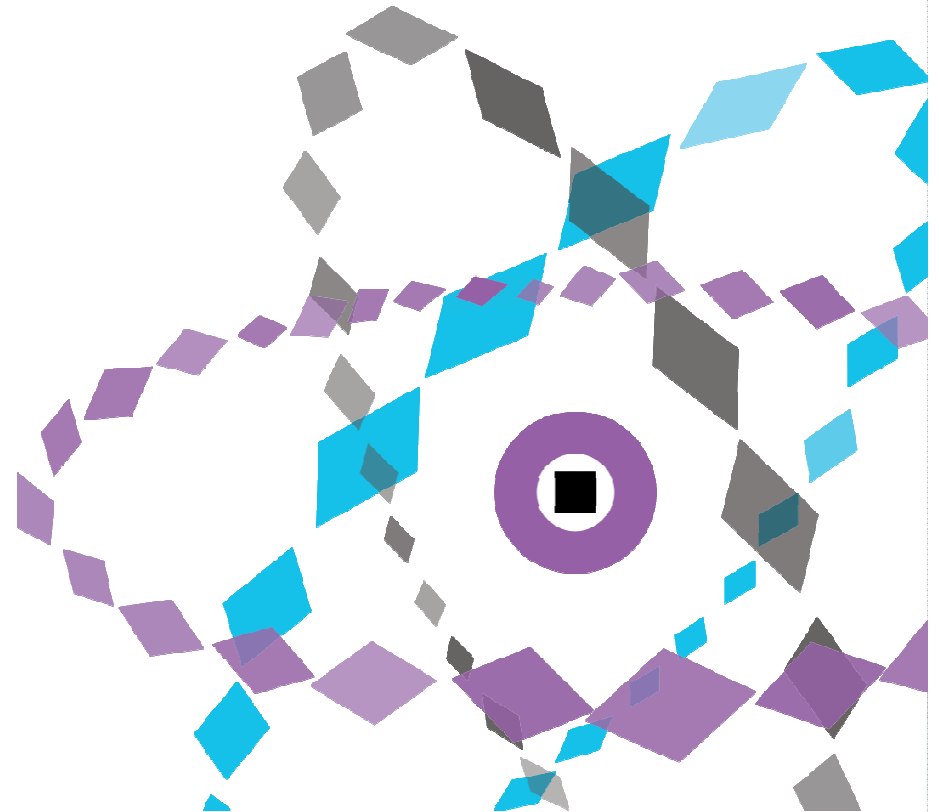


Smarter technology for a smarter planet.

**IBM Tivoli®  
Endpoint Manager**

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

Sascha Buhr, Sales Leader Tivoli Endpoint Manager, IBM





# Herausforderungen

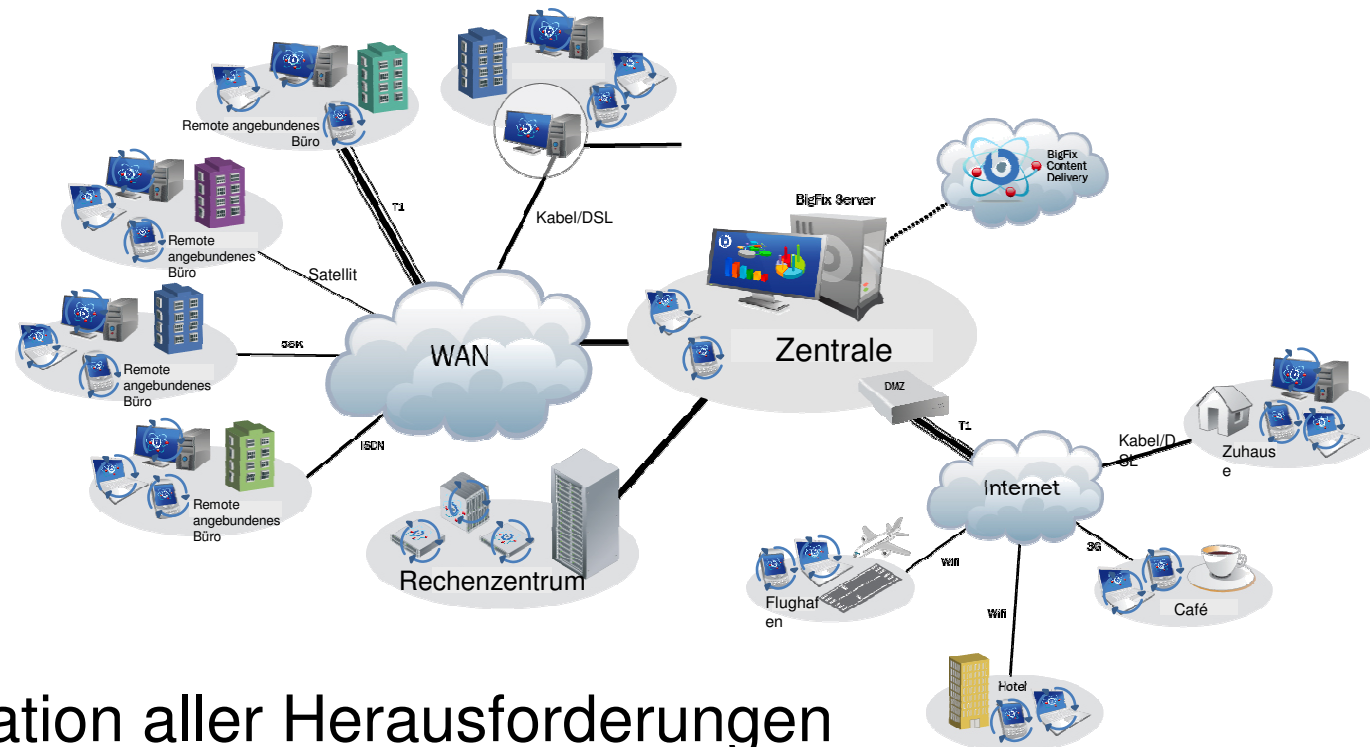
---

- Heterogene Infrastrukturen (Betriebssysteme, Software)
- Erreichbarkeit
- Kontinuität
- Lifecycle / Ständige Veränderung
- Gefahrenpotentiale
- Unterschiedliche Bedrohungsszenarien
- Verfügbare Ressourcen
- Aktualität
- Reaktionsgeschwindigkeit





# Die eigentliche Herausforderung



Die Kombination aller Herausforderungen in einer sich ständig verändernden IT-Landschaft mit neuen Produkten und Anforderungen an Mobilität, Virtualisierung (Cloud) und ständiger Verfügbarkeit.





## Welche Lösung bietet IBM?

---

└ im Oktober 2010 kauft IBM  
BigFix...





---

└ Wer und was ist  
**BigFix?**



# Fakten zu BigFix... IBM Tivoli® Endpoint Manager



- 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





---

Traditioneller  
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





---

# Was ist der Hauptunterschi ed 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





# Die wichtigsten Gesichtspunkte

---

- **Geschwindigkeit**

Die Zeit von der Erkennung eines Incidents bis zur Ergreifung von Abwehrmaßnahmen

- **Nachhaltigkeit**

Dauerhafte Abwehr bzw. Schließen einer Sicherheitslücke

- **Wirtschaftlichkeit**

Einschätzen des möglichen Schadens in Relation zu den möglichen Kosten einer Gegenmaßnahme





# Closed Loop Speed is Our Advantage

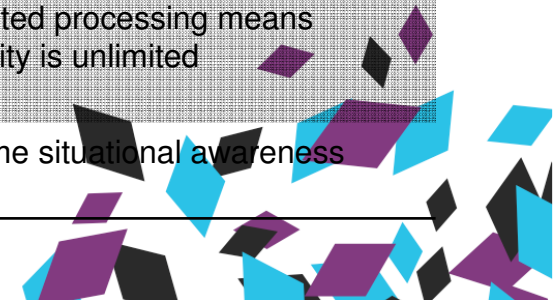
## Traditional Solutions



## TEM



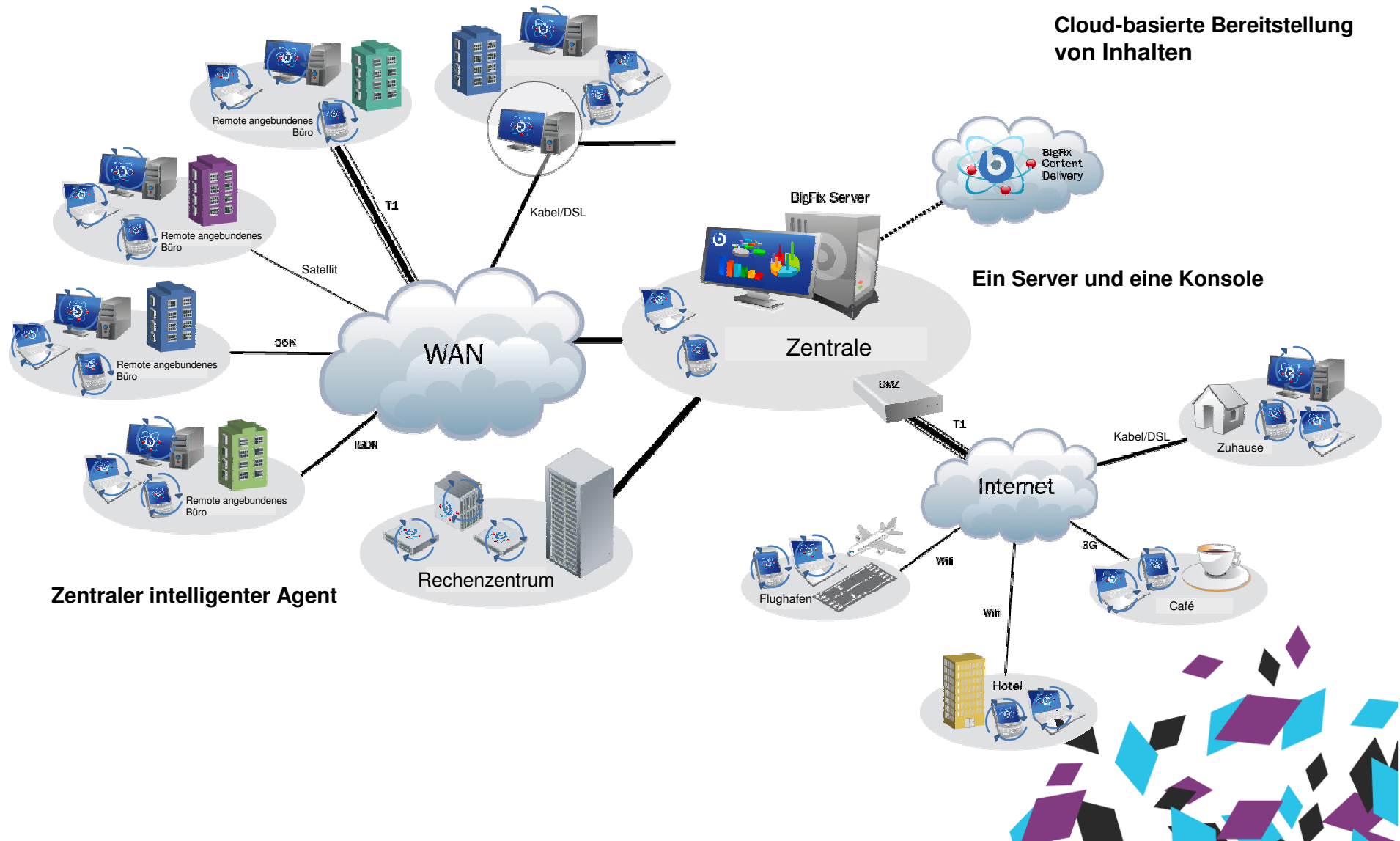
Challenge	Traditional client/server tools	TEM Platform
Complete the policy enforcement loop	Everything is controlled by the server, which is slow	Distributed computing with intelligent, universal agent
Increase the accuracy and speed of your knowledge	It can take days to accurately close the enforcement 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

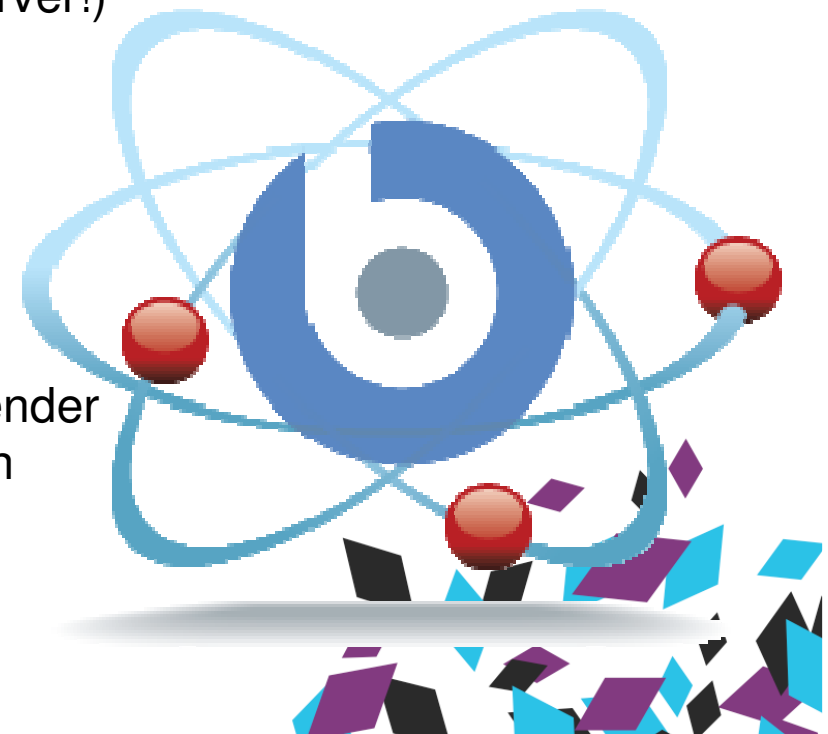




## BigFix erreicht die zeitnahe und zugleich hoch skalierbare Lifecycle Management Funktionalität durch seine intelligente Architektur

---

- 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







**BigFix Enterprise Console**

File Edit View Go Tools Help

Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console

All Content << Computers

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

Edit Settings Remove From Database Send Refresh

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

All Content  
BigFix Management  
Endpoint Protection  
Patch Management





# 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



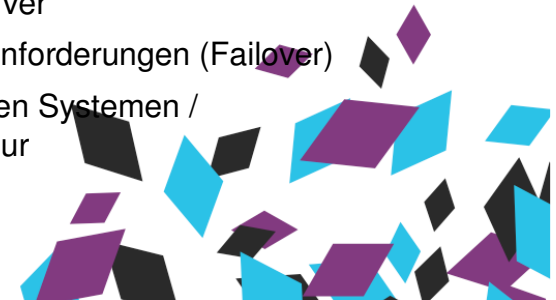
## Nur ein Server & Konsolen

- 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

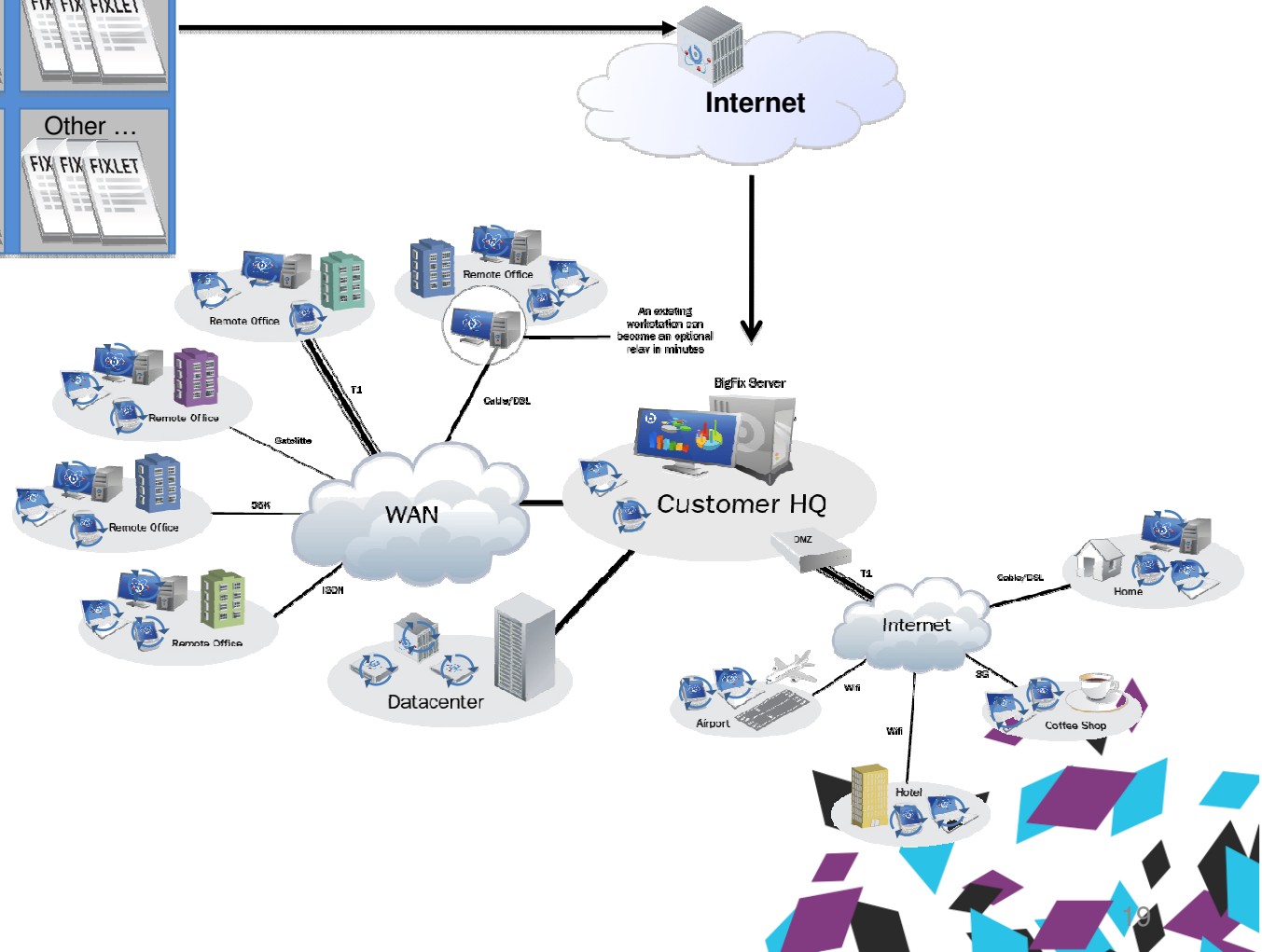
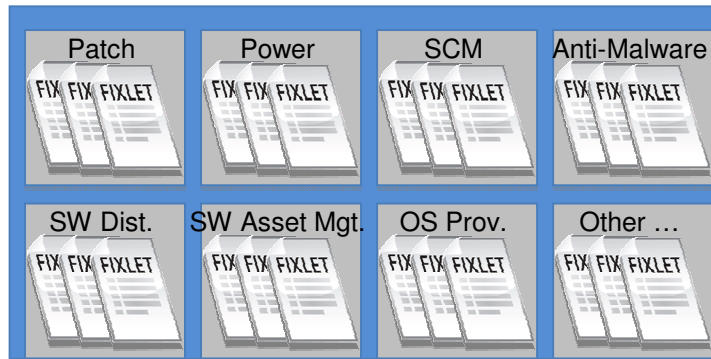


# BigFix: “Content” basiertes Delivery Modell

BigFix® Endpoint Manager

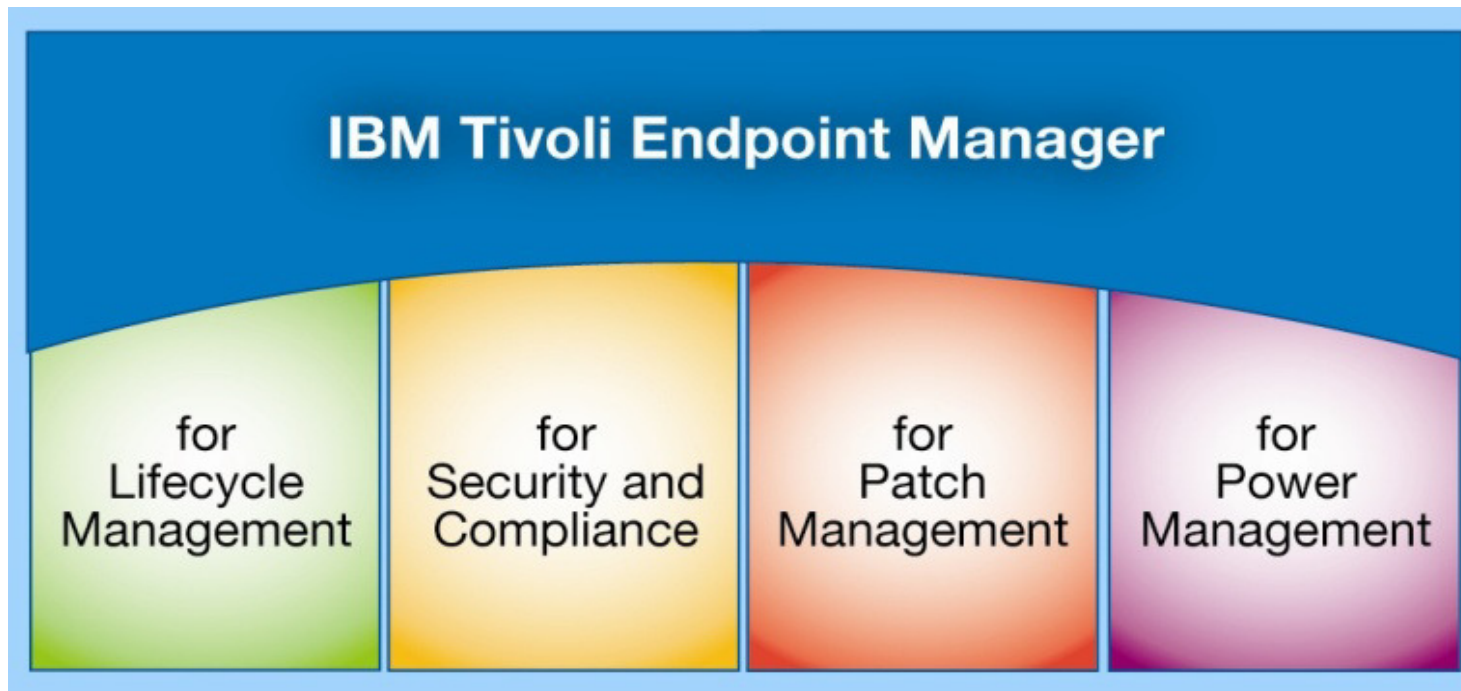


## BigFix Content Sites





# Die vier Module von BigFix (TEM)



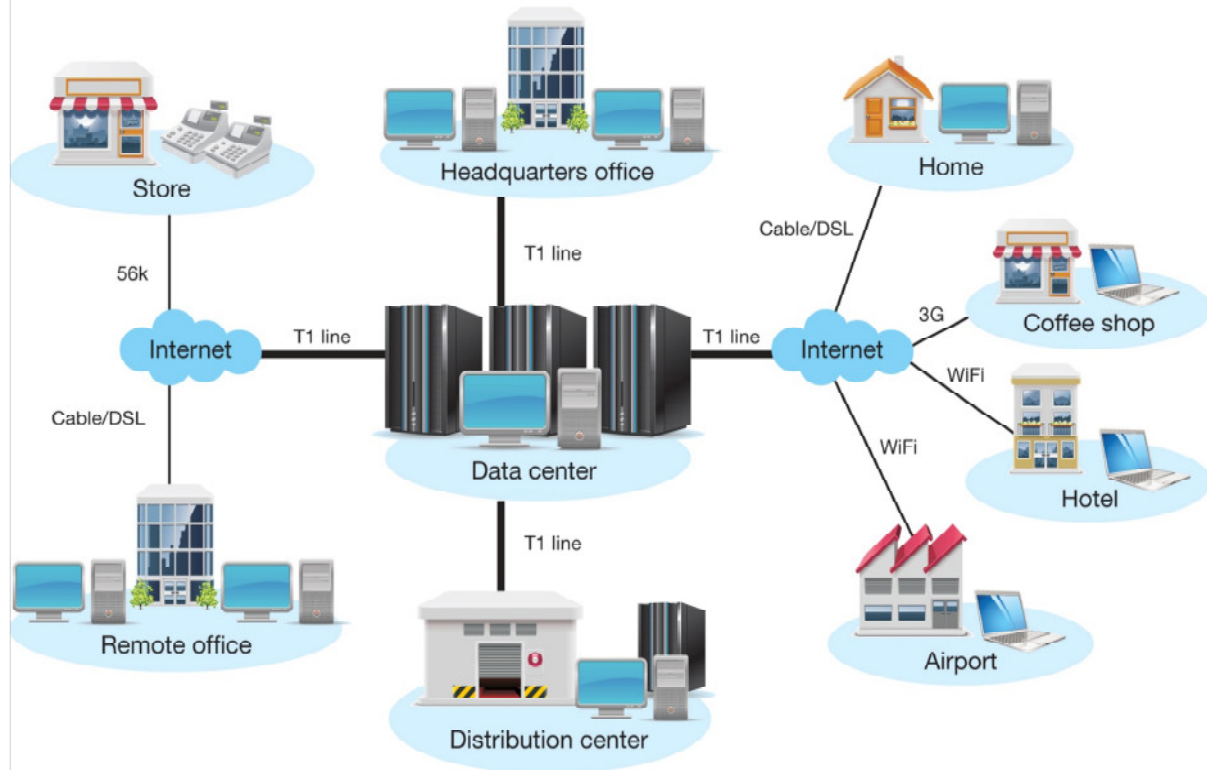
- ▮ Power Management ist nur in Zusammenhang mit einem der drei anderen Module verfügbar
- ▮ Patch Management ist bereits in den Modulen Lifecycle Mgmt. und Security and Compliance Mgmt. enthalten.





# 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)



Unabhängig von Standort, Betriebssystem und Uhrzeit – Alle Systeme sind Permanent unter der sicheren Kontrolle des BigFix Agenten.

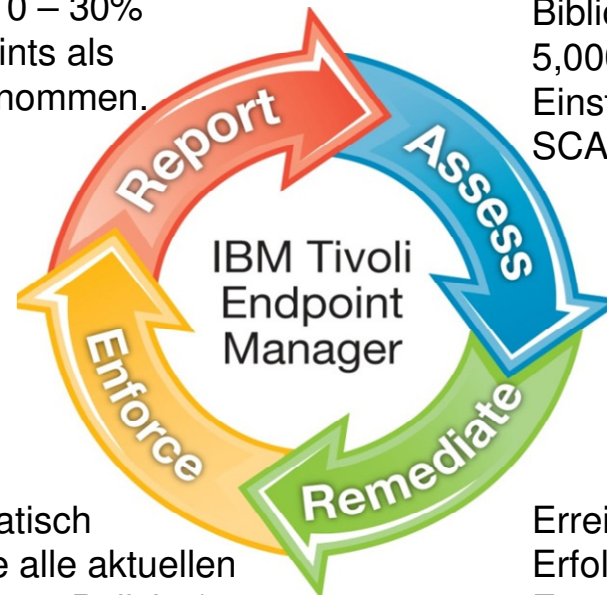




## Tivoli Endpoint Manager: Alle Endpoints im sicheren Überblick

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

TEM findet 10 – 30% mehr Endpoints als vorher angenommen.



Bibliothek mit mehr als 5,000+ Compliance Einstellungen, u.a. für FDCC SCAP, DISA STIG

Setzt automatisch und ständige alle aktuellen Richtlinien (sog. Policies) auf allen Systemen durch.

Erreicht bis zu 95%+ Erfolgsquote beim Erstdurchlauf einer Policy oder eines Patch Deployments





## Tivoli Endpoint Manager: kontinuierliche Endpoint Compliance

**Traditional compliance**



**Continuous compliance**



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





## 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

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



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

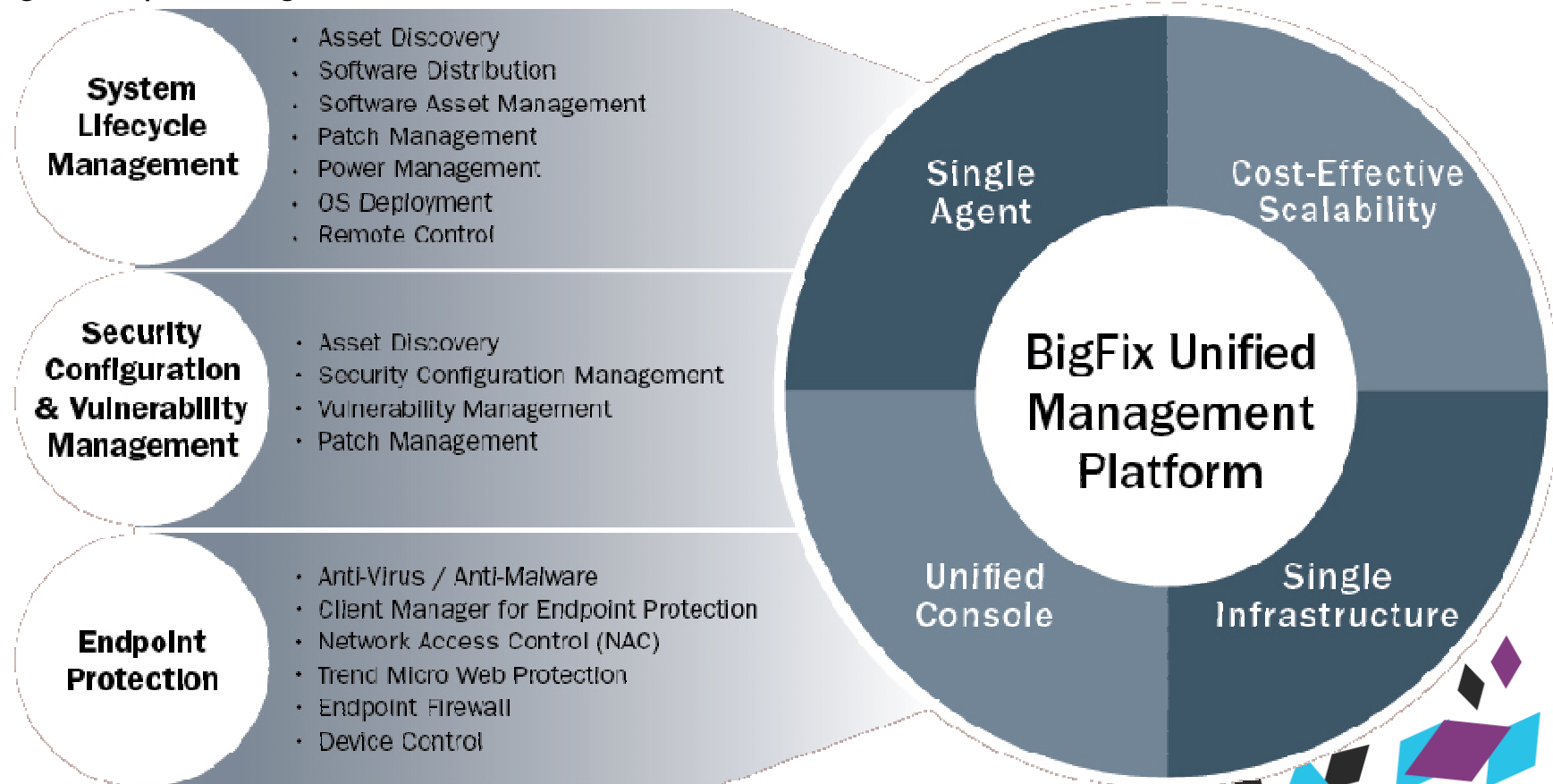
*100 - 125 Server / 5 verschiedene Konsolen / 5 Agenten auf dem Client, Implementiert in Jahren*





# 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.





# Die wichtigsten Gesichtspunkte

---

- **Geschwindigkeit**

Die Zeit von der Erkennung eines Incidents bis zur Ergreifung von Abwehrmaßnahmen

- **Nachhaltigkeit**

Dauerhafte Abwehr bzw. Schließen einer Sicherheitslücke

- **Wirtschaftlichkeit**

Einschätzen des möglichen Schadens in Relation zu den möglichen Kosten einer Gegenmaßnahme





# Die drei wichtigsten Kernelemente



## Lifecycle Management

- Inventarisierung
- Patch Management
- Softwareverteilung
- OS Deployment
- Fernwartung
- Software-Nutzungsanalyse



## Security and Compliance

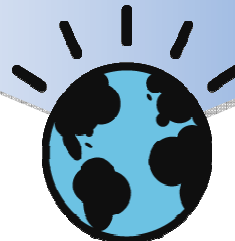
- Inventarisierung
- Patch Management
- Sicherheits- und Konfigurationsmanagement
- Vulnerability Management
- Herstellerneutrale Verwaltung der Endpoint Protection



## Patch Management

- Patch Management für Windows, Linux, Unix und Mac
- Echtzeit Verteilung und Überwachung
- Anpassbare Patches

Intelligentes, schnelles Endpoint Management





- **Kontakt Daten:**

**Sascha Buhr**

Sales Leader Tivoli Endpoint Manager

+49 - 160 - 71 67 68 4

[sascha.buhr@de.ibm.com](mailto:sascha.buhr@de.ibm.com)







# Was sollte eine Lösung berücksichtigen?

---

Fünf wichtige Kriterien:

- Eine zentrale Konsole für alle Endgeräte
- Aktualität der Daten (Echtzeitfähig)
- Alle Endgeräte einbeziehen!
- Richtlinienbasiert („company rules“) für alle bindend
- Gleichzeitig flexibel anpassbar (Akzeptanz der Anwender)

