Microsoft Forefront

MARC GROTE
IT TRAINING GROTE
DEZEMBER 2009

Because it's everybody's business

Microsoft Forefront

Because it's everybody's business

Agenda

Ueberblick ueber die Forefront Produktpalette

Demos

- Forefront TMG 2010
- UAG 2010
- Forefront Protection 2010 for Exchange
- Forefront Client Security

Zunehmende Herausforderungen für die Sicherheitsumgebung

Gefährlichere Bedrohungen

- Fortgeschrittenerer
- Anwendungsorientierter
- Häufiger
- Auf Profit abzielend

Fragmentierung von Sicherheitstechnologie

- Zu viele Einzelprodukte
- Dürftige Interoperabilität
- Fehlende Integration
- Fehleranfällige Verwendung

Schwierige Verwaltung und Bereitstellung

- Mehrere Konsolen
- Ereignis-Reporting und -analyse unkoordiniert
- Hohe Kosten und Komplexität

Die Anforderungen

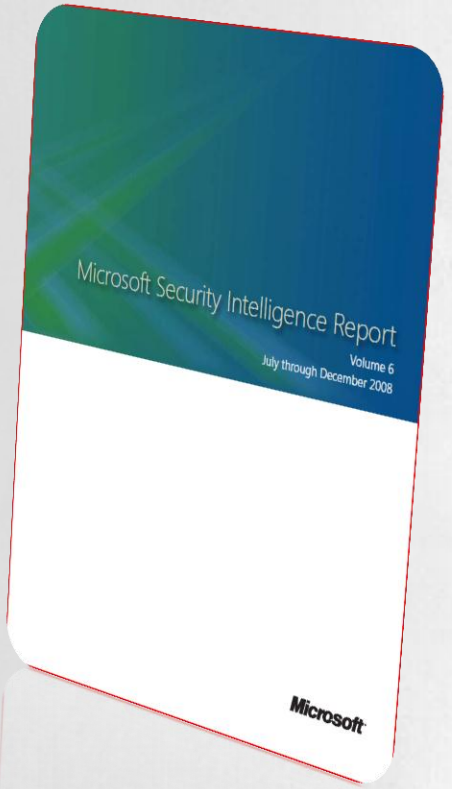
Die Microsoft-Initiativen zur IT-Sicherheit

Security Development Lifecycle

- Definiertes Vorgehen
- Sicheres Design bereitstellen und Risiken frühzeitig reduzieren

Security Intelligence Report

- Halbjährlich erscheinender Report des Microsoft Malware Protection Teams
- www.microsoft.com/sir



Engagement in Standardisierung, Strafverfolgung und Endanwender-Sensibilisierung und –Schutz

- www.microsoft.de/mse

Eingebaute Sicherheitsfunktionalitäten

- Etwa bei Windows 7, Windows Server 2008 R2, Microsoft Office, SharePoint

Was ist Microsoft Forefront?

Because it's everybody's business

Microsoft® Forefront™

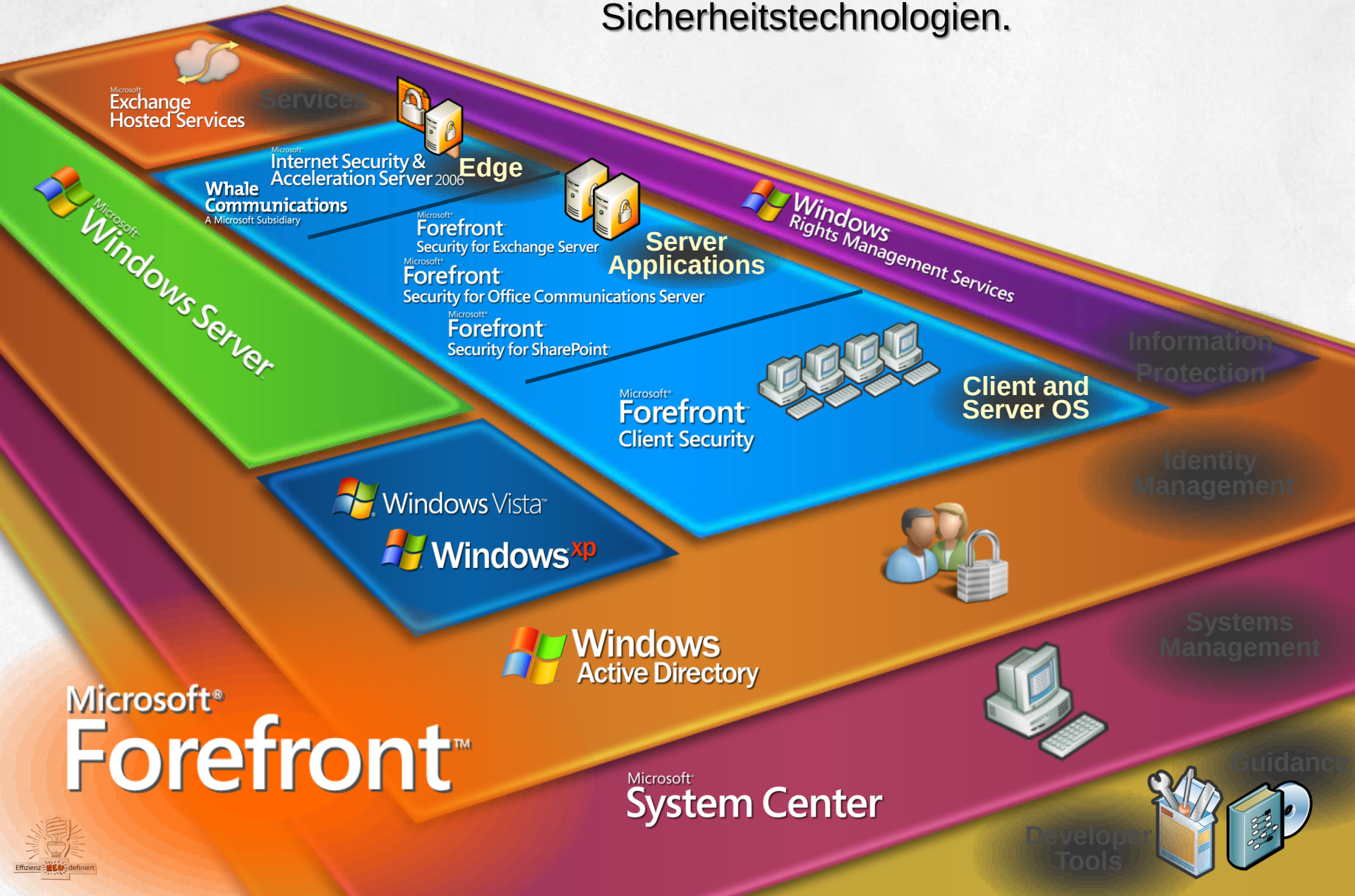
Microsoft® Forefront™

Eine umfassende Familie von Sicherheitsprodukten für die Öffentliche Verwaltung und Unternehmen, die durch enge Integration und vereinfachte Verwaltung einen größeren Schutz ermöglichen.

Effizienz – NEU – definiert

Because it's everybody's business

Microsoft vereint branchenführende, durchgängige und effiziente Sicherheitstechnologien.



Das bisherige Forefront Identitäts- und Sicherheitsangebot

Endpunkt

Microsoft® Forefront™ Client Security

Netz-werk

Microsoft® Internet Security & Acceleration Server 2006

Intelligent Application Gateway 2007

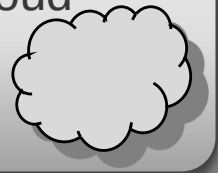
Server

Microsoft® Forefront™ Security for SharePoint®

Microsoft® Forefront™ Security for Office Communications Server

Microsoft® Forefront™ Security for Exchange Server

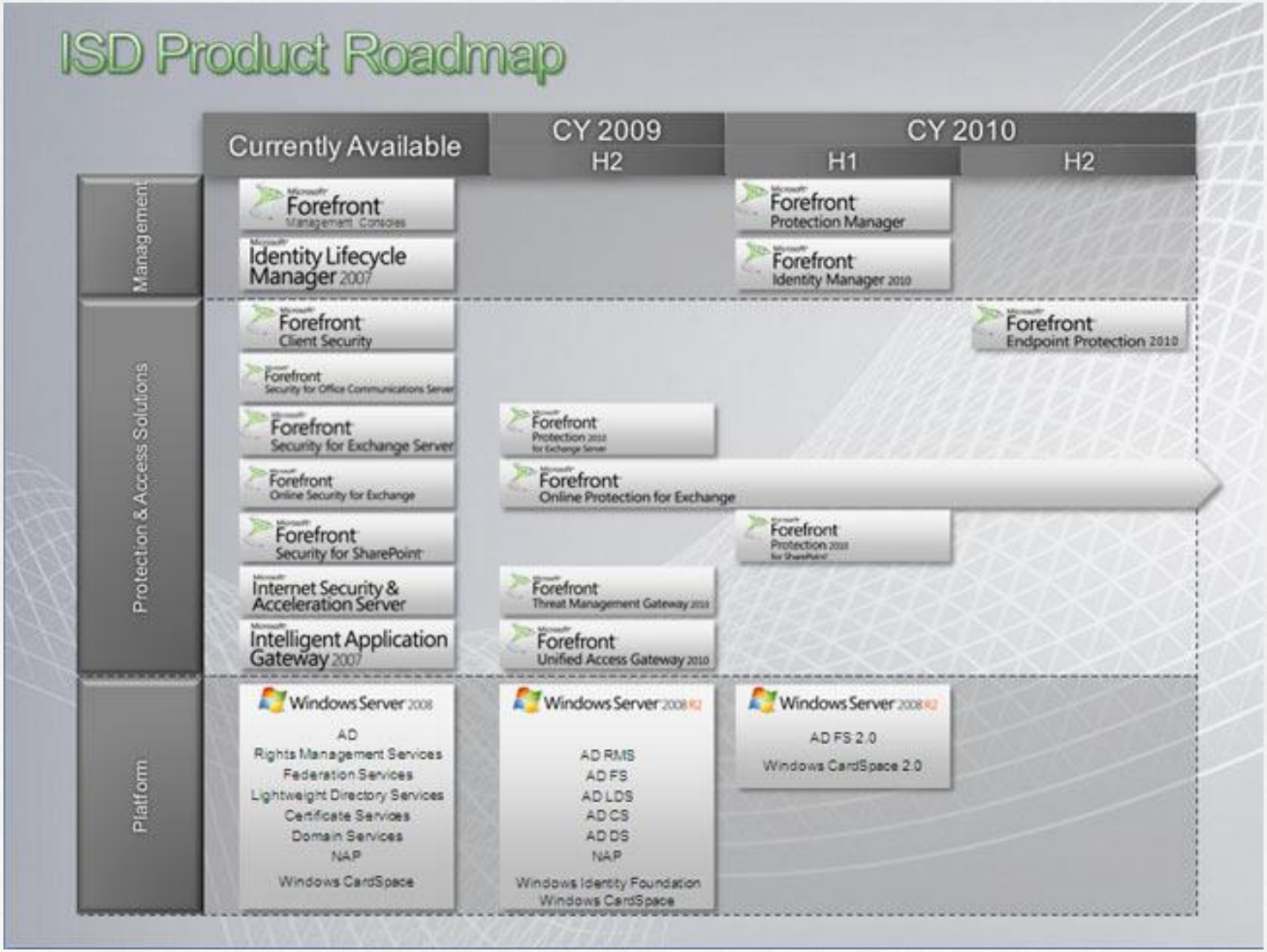
Cloud



Microsoft® Forefront™ Online Security for Exchange

Weitere Lösungen:
- Identity Management
- Rights Management
- NAP …

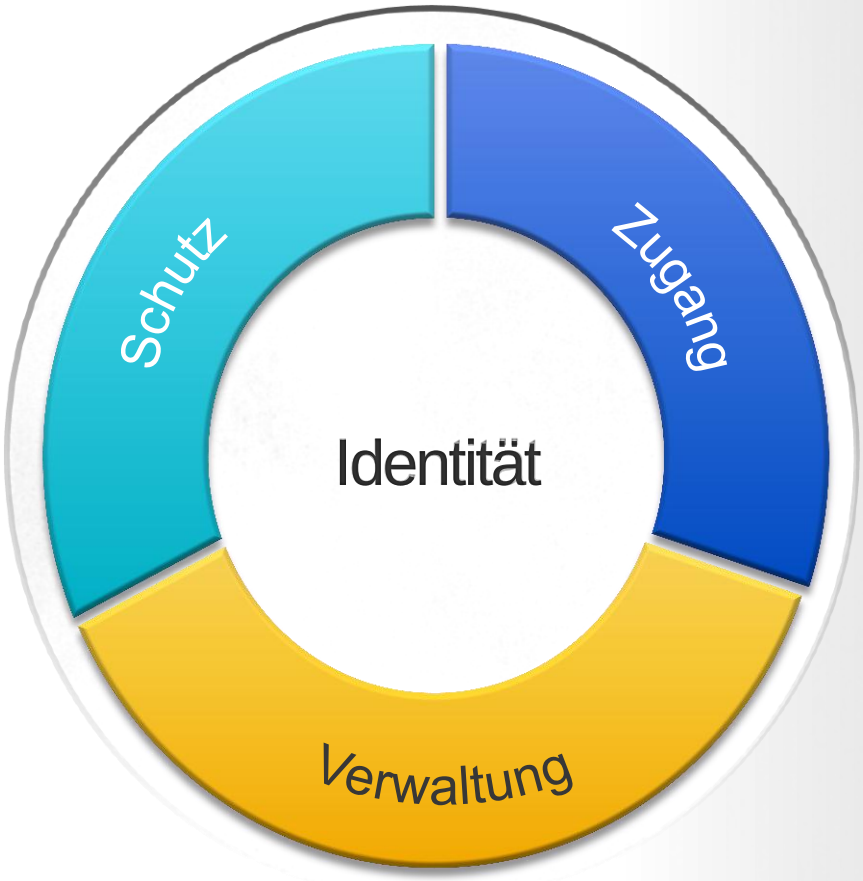
Realitaet und (nahe) Zukunft



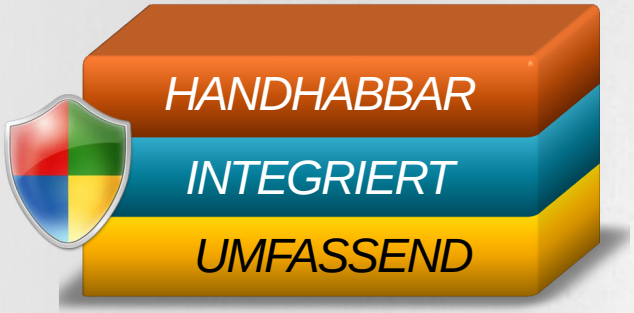
Unser Ansatz:
Business Ready Security

Because it's everybody's business

Microsoft Forefront



Sicherheits- und Identitäts-Lösungen bilden eine untrennbare Einheit.



Effizienz – IEEU – definiert

Because it's everybody's business

Forefront Protection Suite – Architektur

Because it's everybody's business

Microsoft Forefront

Vereinheitlichte Verwaltung

Ausführliches Reporting

Unternehmensweite Analyse

Forefront Protection Manager
(zentrale Verwaltungkonsole)

Security Assessment Sharing (SAS)

Client- & Server-OS

Microsoft Forefront Endpoint Protection 2010

Server-anwendungen

Microsoft Forefront Protection 2010 for Exchange Server

Microsoft Forefront Protection 2010 for SharePoint

Microsoft Forefront Online Protection for Exchange

Netzwerk (Edge)

Microsoft Forefront Threat Management Gateway

Lösungen von Drittanbietern

TippingPoint

RSA SECURITY

Guardium

Juniper NETWORKS

Integration Microsoft-Infrastruktur

- Active Directory
- Netzwerk-zugriffsschutz (NAP)

Effizienz – IEEU – definiert

Because it's everybody's business

Forefront Protection Suite: Sicherheitstechnologien

Because it's everybody's business

Microsoft Forefront

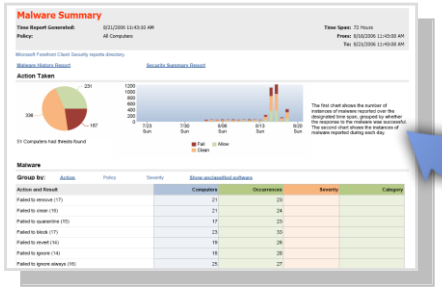
Effizienz – IEEU – definiert

Because it's everybody's business

Forefront Protection Manager

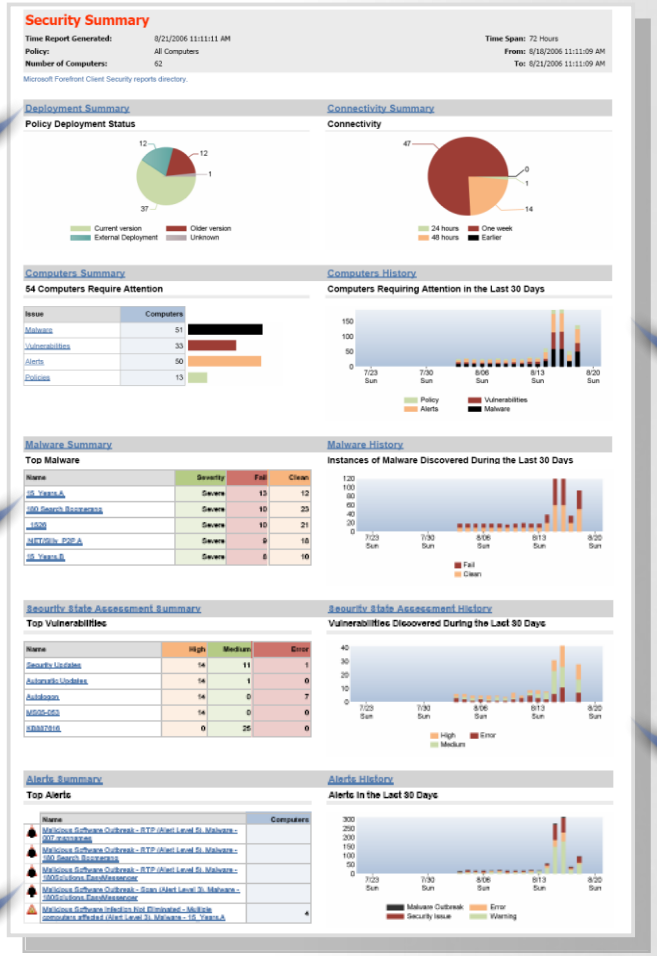
Zentrale Administration und umfangreiches Reporting

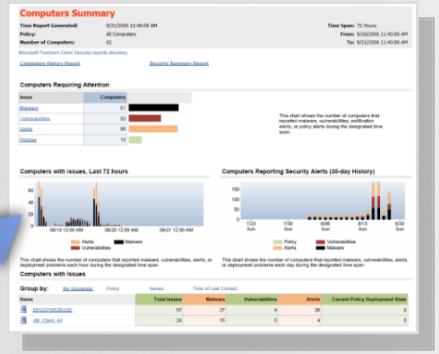
Übersicht Verteilung



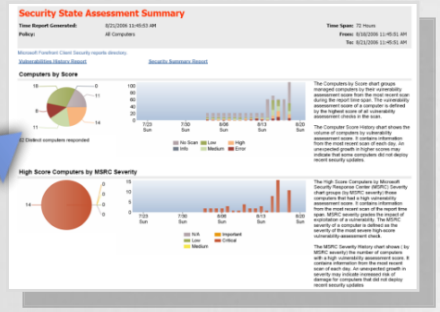
Überblick Schadsoftware

Alarmierungen





Übersicht Sicherheits-status Endgeräte



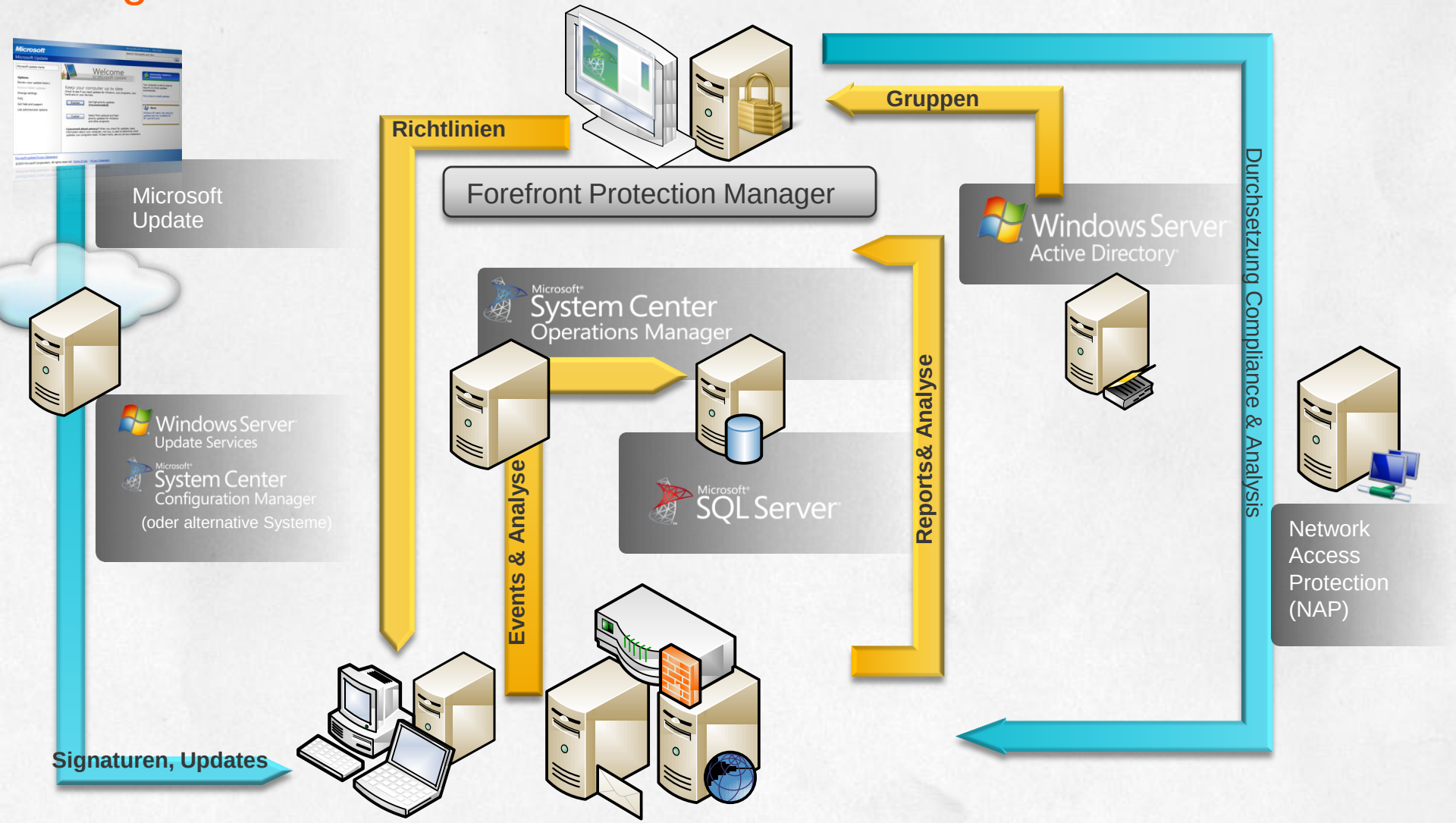
Gesamt-sicherheitsreport

Effizienz-NEO-definiert

Because it's everybody's business

Forefront Protection Suite

Integration in die Infrastruktur



Die Stärke mehrerer `Engines` nutzbar machen

Forefront Server Protection beinhaltet und nutzt fünf Antivirus-Engines führender Hersteller

Microsoft

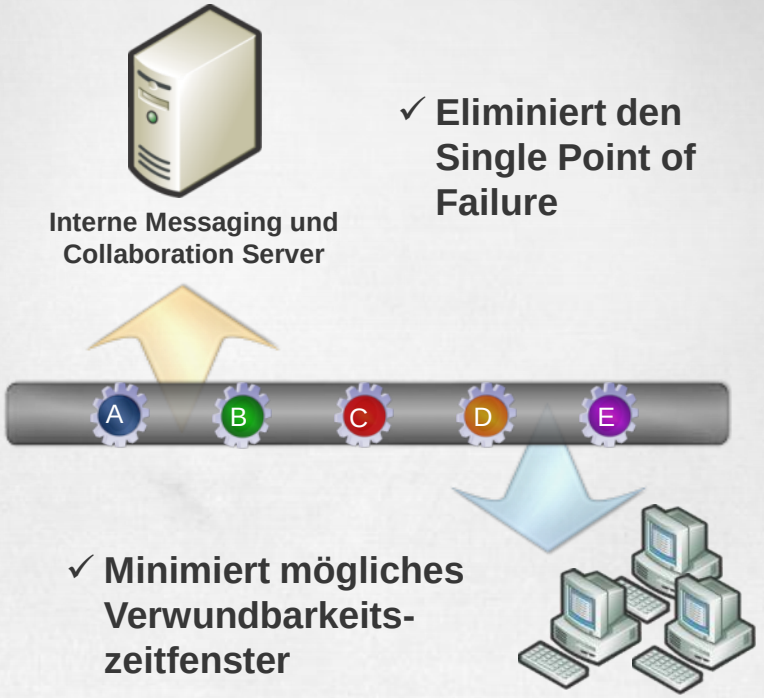
KASPERSKY lab

authentium

VirusBuster
www.virusbuster.hu

NORMAN
DATA DEFENSE SYSTEMS

Jeder Scan-Job bei Forefront Server Protection kann bis zu fünf Engines gleichzeitig verwenden



✓ **Eliminiert den Single Point of Failure**

✓ **Minimiert mögliches Verwundbarkeits-zeitfenster**

Forefront: Der Multi-Scan-Engine-Vorteil

- Schnelle Reaktion auf neue Bedrohungen
- Engines bieten gegenseites “Backup”
- Vorteil durch Unterschiedlichkeit der AV-Engines und Heuristiken

Weniger als 5 Stunden

5 bis 24 Stunden

Mehr als 24 Stunden

Reaktionszeit[1] (in Stunden)

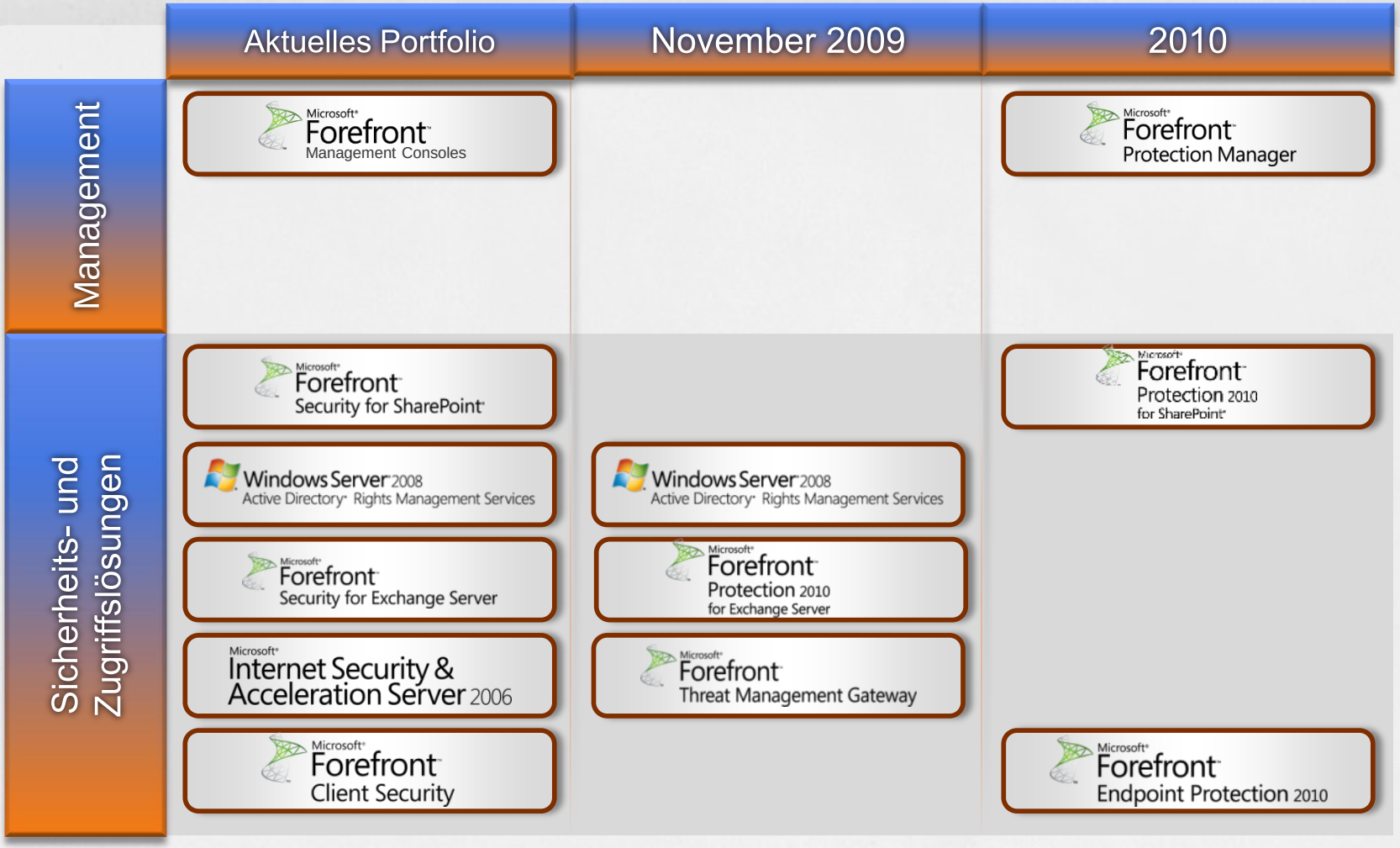
`Single-Engine` Lösung

WildList Number	Malware Name	Forefront Engines	Vendor A	Vendor B	Vendor C
01/09	autorun_itw542.ex_	0.00	1185.47	89.83	1161.83
01/09	buzus_itw3.ex_	0.00	2.92	10.87	53.98
01/09	conficker_itw5.dl_	0.00	0.00	113.55	0.00
01/09	koobface_itw18.ex_	0.00	360.65	0.00	1050.18
01/09	momibot_itw2.ex_	0.00	0.00	0.00	982.05
01/09	pinit_itw2.ex_	42.85	205.03	0.00	873.23
01/09	zbot_itw30.ex_	0.00	0.00	0.00	0.00
01/09	zbot_itw31.ex_	0.67	990.50	1.17	53.75
01/09	zbot_itw39.ex_	0.00	946.40	0.00	0.00
02/09	agent_itw94.ex_	0.00	0.00	204.17	723.10
02/09	autorun_itw580.ex_	0.00	341.37	917.60	336.67
02/09	autorun_itw585.ex_	0.00	602.93	0.00	0.00
02/09	autorun_itw594.ex_	0.00	704.05	0.00	42.40
02/09	magania_itw21.ex_	0.00	0.00	0.00	522.60
02/09	onlinegames_itw624.ex_	0.00	386.88	22.12	0.00
02/09	onlinegames_itw627.ex_	0.00	207.33	60.88	7.42
02/09	onlinegames_itw643.ex_	0.00	22.13	6.22	32.18
02/09	zbot_itw42.ex_	0.00	1120.87	0.00	0.00
03/09	autoit_itw90.ex_	0.00	0.00	0.00	1101.62
03/09	autorun_itw597.ex_	0.00	555.12	0.00	16.88
03/09	autorun_itw598.ex_	0.00	2.88	187.27	667.85
03/09	autorun_itw601.ex_	0.00	510.32	0.00	0.00
03/09	autorun_itw616.ex_	0.00	555.12	0.00	16.88
03/09	ircbot_itw485.ex_	0.00	3.37	0.37	79.05
03/09	mariof_itw2.ex_	0.00	309.40	945.95	653.03
03/09	onlinegames_itw651.ex_	0.00	0.00	145.48	55.47
03/09	zbot_itw43.ex_	0.00	757.28	0.00	0.00

** 0.00 denotes proactive detection

[1] Source: AV-Test.org 2009 (www.av-test.org)

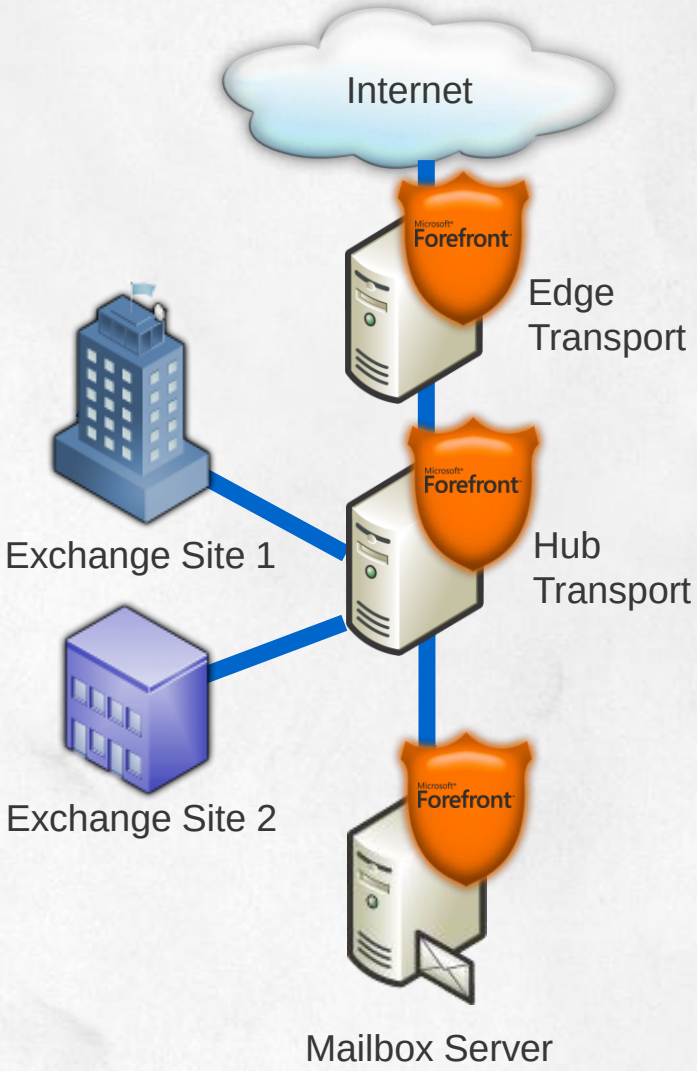
Die Forefront Roadmap – Business Ready Security



bitte beachten: Änderungen vorbehalten

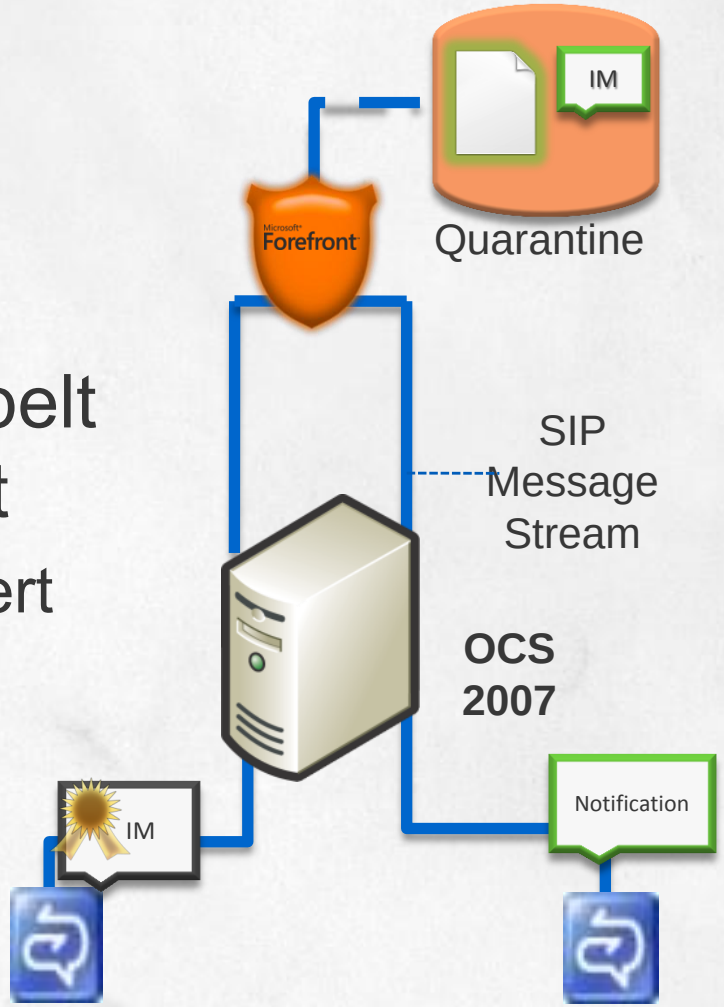
Forefront Security for Exchange Server

- Optimale Performance
  - Erkennung der Exchange-Rolle
  - AV-Stamping
  - Bias-Einstellung
- Maximale Sicherheit
  - Intelligentes Hintergrund-Scannen
  - Scan-On Scanner Update-Scanning
  - Proaktives Scanning
  - Echte Dateifiliterung
  - Premium-AntiSpam für Exchange



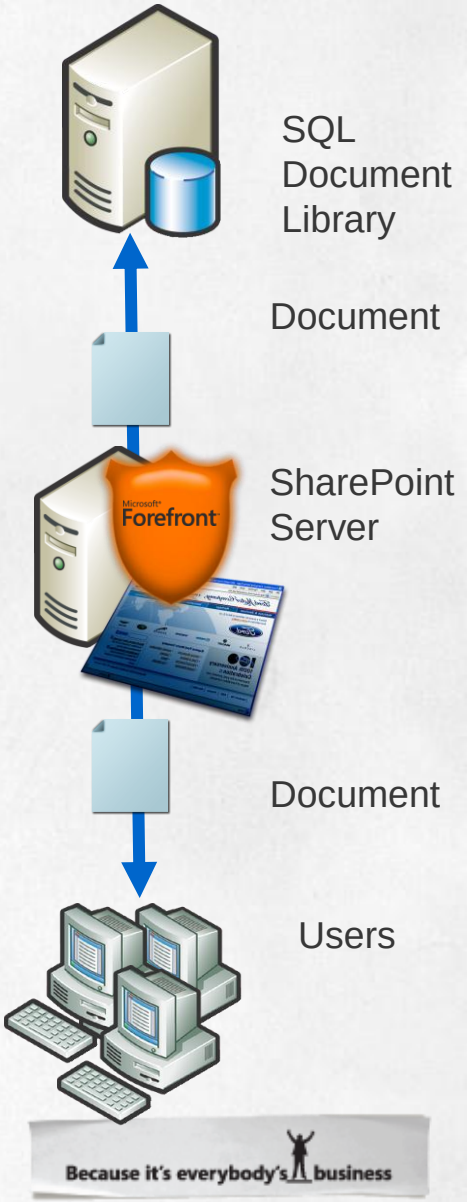
Forefront Security for OCS

- SIP-Nachrichtenstrom wird durch FSOCS geroutet
- Geprüfte Nachrichten und Filetransfers werden gestempelt und durch OCS weitergeleitet
  - Infizierte Dateien werden blockiert und/oder in Quarantäne gestellt
  - Benachrichtigung wird an den Administrator gesendet



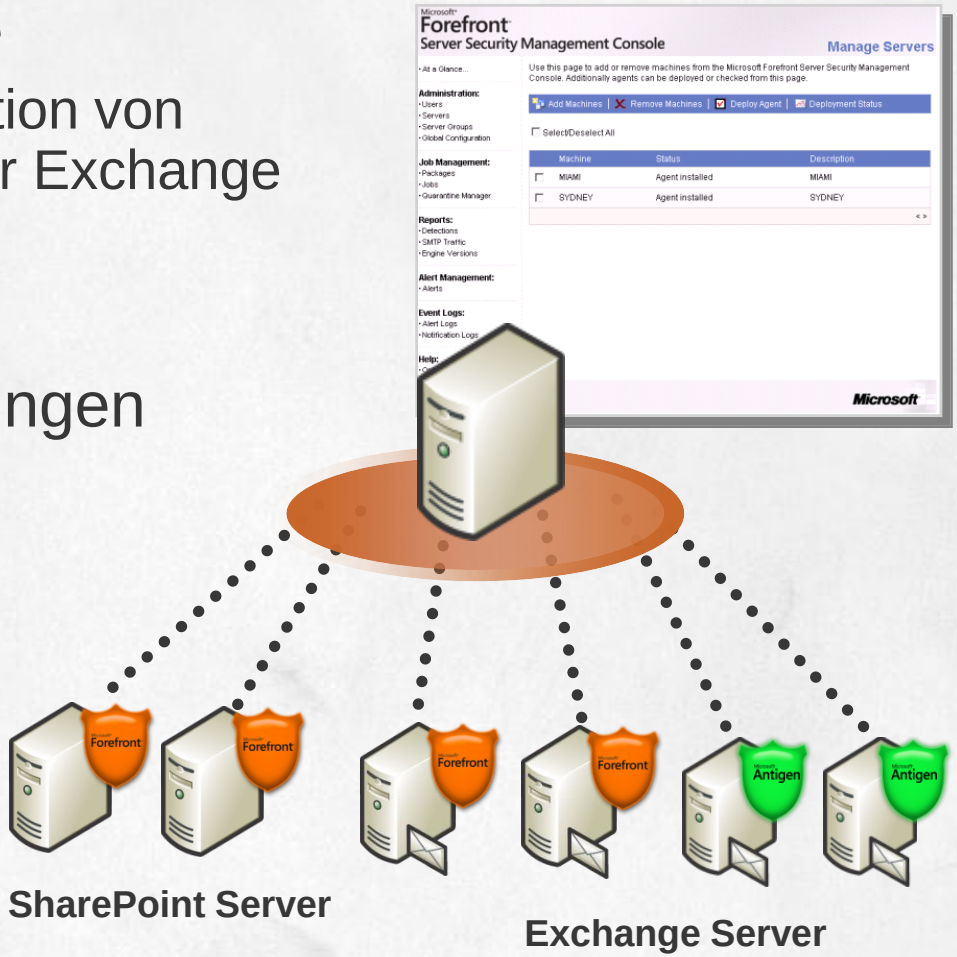
Forefront Security SharePoint Server

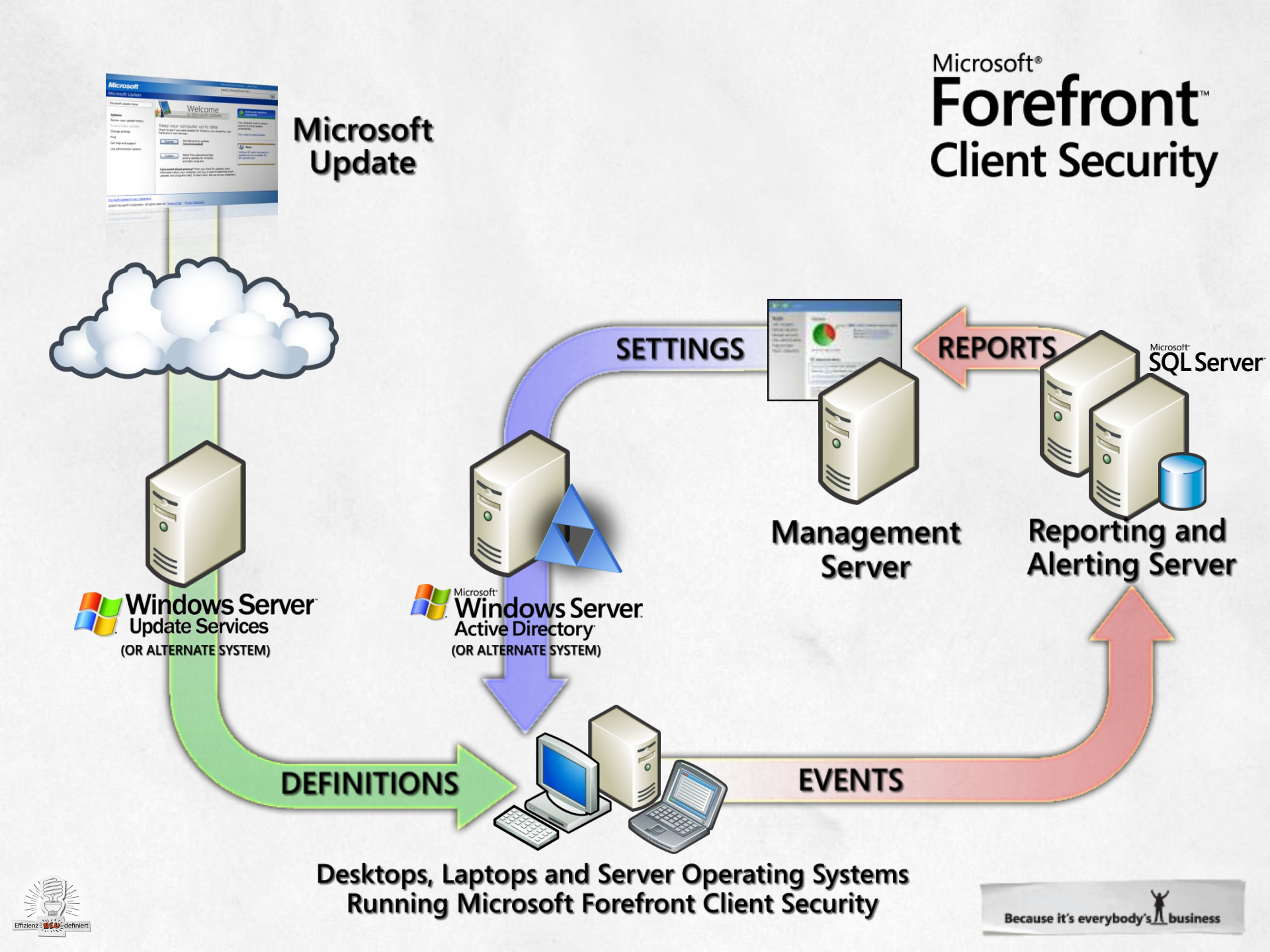
- Virenschutz für die Dokumenten-Bibliothek
  - Echtzeitschutz beim Up-und Download von Dokumenten in die SQL-Datenbank
  - Manuelle und zeitgesteuerte Scans
- Durchsetzen von inhaltlichen Richtlinien
  - Dateifilter können auf Basis von Dateinamen, Dateiendung und Dateityp angewendet werden
  - Filterung nach ungewollten Inhalten ist auch innerhalb von Dokumenten möglich



Forefront Server Security Management Console

- Zentrale Verwaltungskonsole
  - Bereitstellung und Konfiguration von Forefront/Antigen Security for Exchange und SharePoint Server
- Automatisiert die Aktualisierungen im gesamten Netzwerk
- Ermöglicht umfangreiches Reporting und Festlegung von Outbreak Alerts



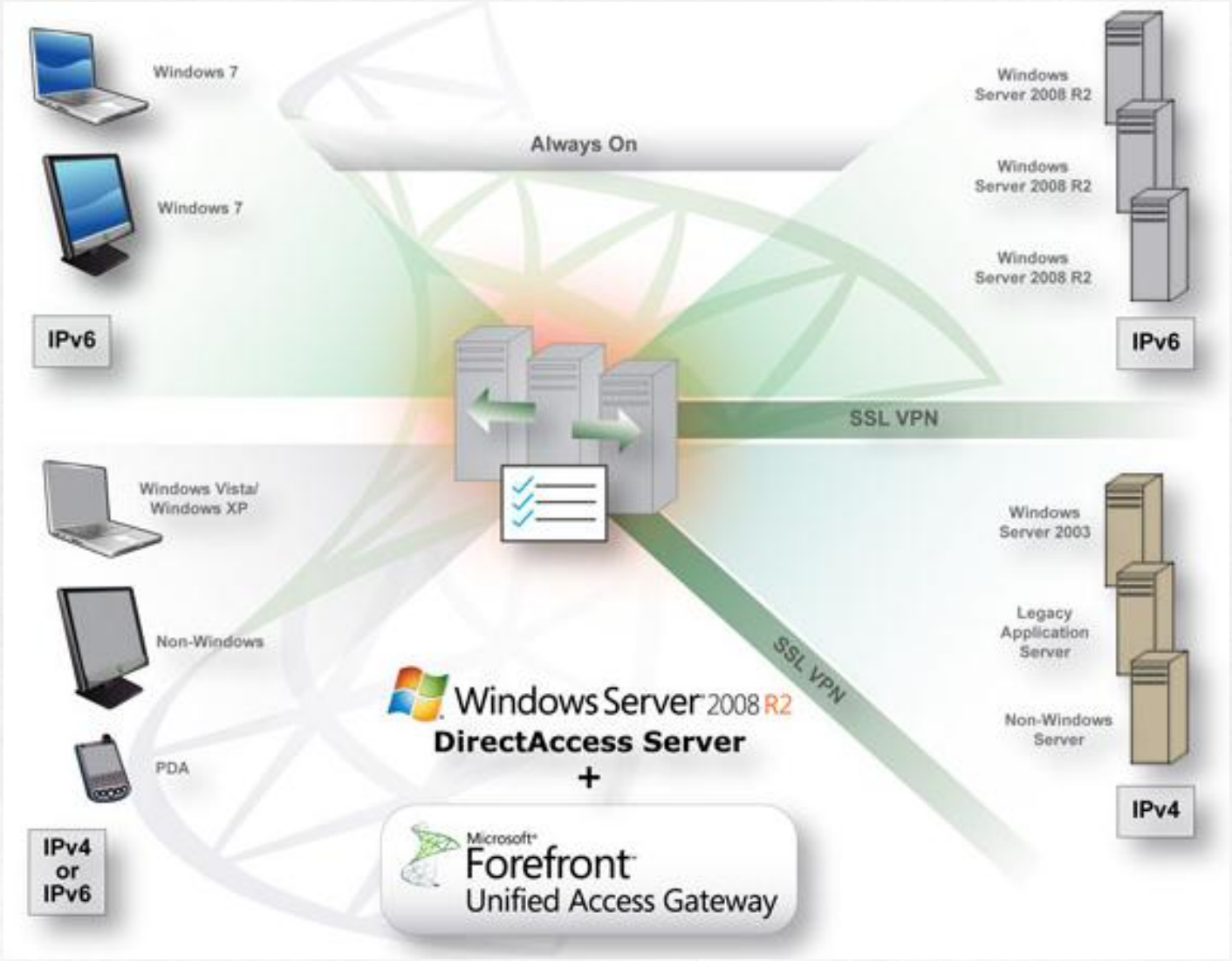

Microsoft Update
Microsoft® Forefront™ Client Security
SETTINGS
REPORTS
Microsoft SQL Server
Management Server
Reporting and Alerting Server
Windows Server Update Services
(OR ALTERNATE SYSTEM)
Microsoft Windows Server Active Directory
(OR ALTERNATE SYSTEM)
DEFINITIONS
EVENTS
Desktops, Laptops and Server Operating Systems
Running Microsoft Forefront Client Security
Effizienz – NEU – definiert
Because it's everybody's business

Forefront Client Security

Anti-Malware-Schutz der Client- und Server-Betriebssysteme

Einheitlicher Schutz	Eine Lösung für Viren- und Spyware-Schutz Überwachung des Systemzustands Eigene Research- & Response-Zentren
Vereinfachte Verwaltung	Eine Konsole für einfache, zentrale Verwaltung Leichte Signatur- und Richtlinien-Verteilung Integriert sich in bestehende Infrastrukturen
Überblick & Kontrolle	Ein Cockpit bietet kompletten Überblick Aussagekräftige Berichte (z.B. täglich per Email) Stets auf dem aktuellen Stand &Trends sichbar

Forefront UAG



Lust auf Links?

ISA / TMG

www.microsoft.com/tmg – Herstellerwebsite, Produktinfos, FAQ

www.microsoft.com/isa – Herstellerwebsite, Produktinfos, FAQ

www.msisafaq.de – Artikel und jede Menge Infos rund um den ISA-Server

www.isaserver.org – Eine der englischsprachigen Ressourcen zum Thema

www.isatools.org – Jim Harrison's Toolsammlung

www.isascripts.org – Scriptsammlungen von Jason Fossen

www.isaserver.bm – Tools und Destination Sets

microsoft.public.de.german.isaserver – Deutschsprachige ISA/TMG-Newsgroup

social.technet.microsoft.com/forums/isa – Microsoft ISA-Forum

social.technet.microsoft.com/forums/tmg – Microsoft TMG-Forum

ISA / TMG Blogs

blogs.technet.com/isablog – Forefront TMG (ISA Server) Product Team Blog

www.carbonwind.net/blog – Blog von Adrian Dimcev

blog.msfirewall.org.uk – Blog von Jason Jones

tmgblog.richardhicks.com – Blog von Richard Hicks

blogs.technet.com/yuridiogenes – Blog von Yuri Diogenes

msmvps.com/blogs/rauscher – Blog von Dieter Rauscher

Forefront / IT-Security

www.microsoft.com/forefront – Englische Microsoft Forefront-Website

www.microsoft.com/germany/forefront – Deutsche Microsoft Forefront-Website

www.findproxyforurl.com – Site zum Thema proxy.pac und wpad.dat

technet.microsoft.com – Forefront Edge Security

Partner

www.it-training-grote.de – Training, Consulting, Infos

www.aixperts.de – Training und Consulting

www.hentrup.net – Qualifikationsprofil Hentrup

www.secureguard.at – Hersteller von ISA/TMG Appliances

Marc Grote

Microsoft Forefront

www.forefront.de

www.microsoft.com/forefront