

Microsoft®
Forefront™

Business Ready Security

Steve Scholz
Microsoft Education
steve.scholz@microsoft.com

Business Ready Security

Help securely enable business by managing risk and empowering people

Protect everywhere,
access anywhere



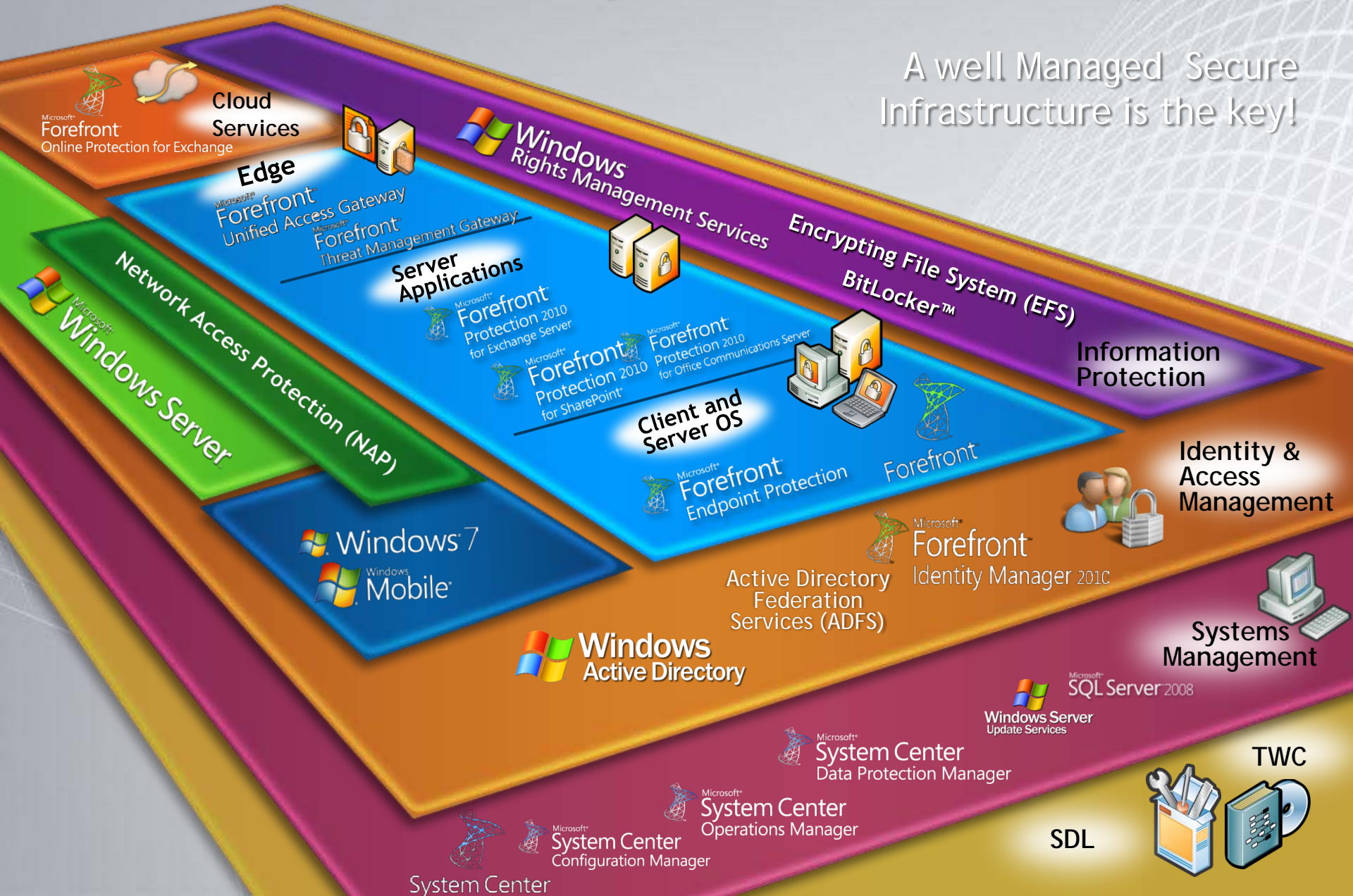
Simplify the security
experience,
manage compliance

Integrate and extend
security across the
enterprise

<i>from:</i>	<i>to:</i>
Block	Enable
Cost	Value
Siloed	Seamless

Microsoft Security: Defense In Depth

A well Managed Secure Infrastructure is the key!

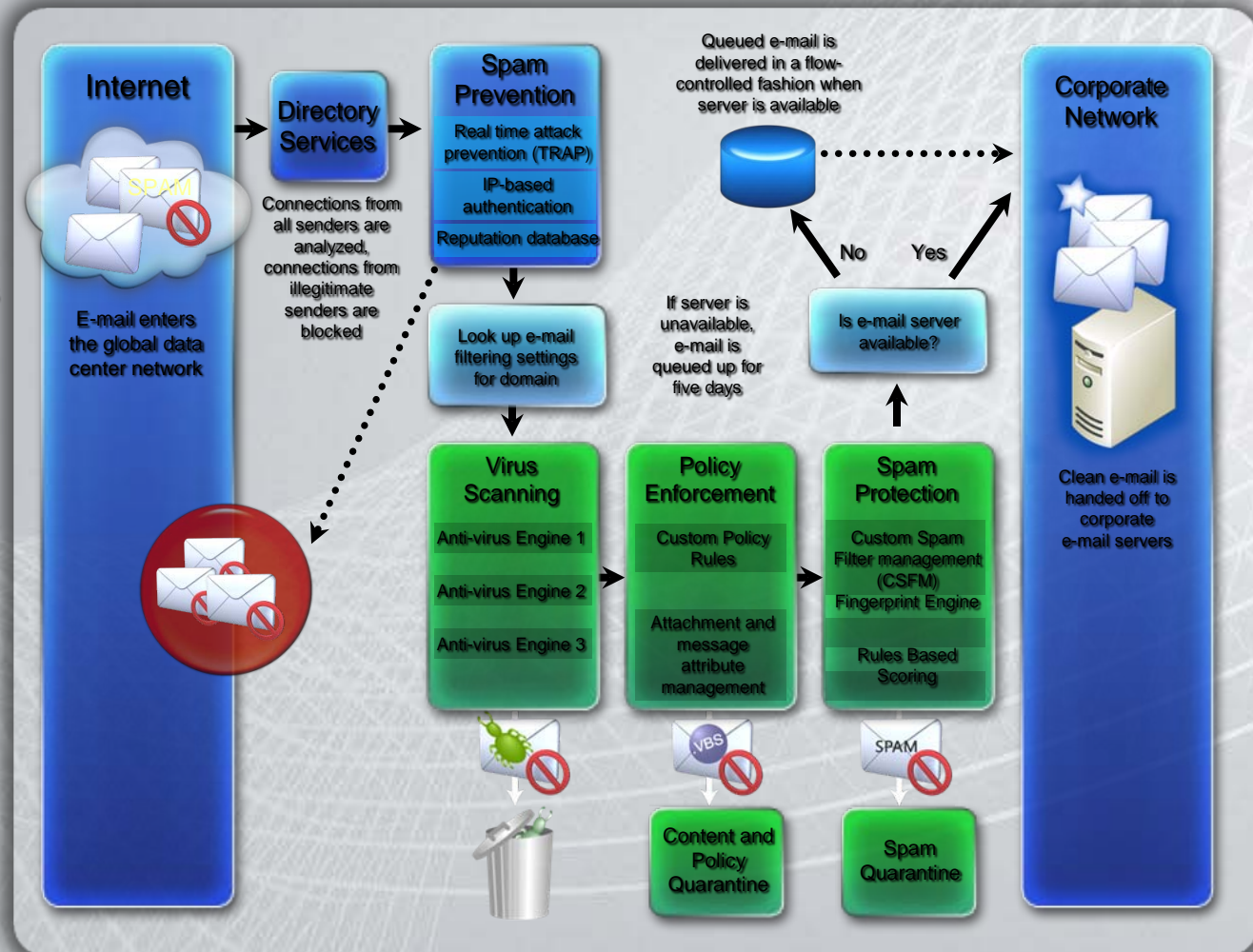


Forefront Online Protection for Exchange

Multilayer spam and virus protection/content and policy enforcement

Solution Overview

- A simple MX record is all it takes to begin filtering
- Real-time Attack Prevention (RTAP) and Directory Services protect against the largest attacks
- Virus filter delivers zero-day protection using multiple, complementary anti-virus engines
- Flexible policy filter to enforce corporate e-mail-use policies
- High-accuracy spam filtering
- E-mail queuing ensures mail is never lost



Our Difference

Enterprise-class reliability and performance

High-Availability, High-Security and High-Performance for Billions of E-mail



- 99.999% service level uptime guarantees and performance SLAs for spam filtering effectiveness
- SAS 70 Type II and ISO 17799 compliant data centers
- More than 6 billion messages processed per month

Dedicated Expertise Available for Thousands of Customers, 24/7



- Real-time security updates and network performance monitoring
- 24/7 customer support and dedicated account managers for qualifying accounts

Investment from Microsoft; Integration with Software and Services

Microsoft[®]

Your potential. Our passion.™

- Investment and resources to ensure superior QoS
- Tight integration with Microsoft Exchange and other Microsoft products and services
- Roadmap to be the message management service for unified communications

Forefront Threat Management Gateway 2010

Forefront Threat Management Gateway allows employees to safely use the Internet without worrying about malware and other threats.

Web Security

- Reputation Based URL Filtering
- Web Anti-Virus, Malware Inspection
- Inspection of HTTP and HTTPS traffic

Intrusion Prevention

- Protection for desktops and servers from intrusion attempts (Network Inspection System)

Enhanced Protection

- Includes built-in, proven network protection technologies of ISA 2006
- New enhancements for Firewall, Remote Access & E-Mail Protection

Simplified Management & Deployment

- Easier management with Scenario UI & Wizards
- Enhanced reporting
- Array Management Capabilities

TMG New Feature Drill Down

- HTTP Anti-virus/spyware
- URL Filtering
- HTTPS forward inspection

Secure Web Access



- VoIP traversal (SIP)
- Enhanced NAT
- ISP Link Redundancy
- SQL logging
- Updated firewall client

Firewall



- Exchange Edge/FSE integration
- Anti-Virus
- Anti-spam

E-mail Protection



- Network Inspection System (NIS)
- Security Assessment and Response

Intrusion Prevention



- NAP integration with VPN role

Remote Access



- Array Management
- Scenario UI & Wizards
- Change tracking
- Enhanced reporting
- W2K8, native 64-bit

Deployment & Management



- Update Center :
 - HTTP: AV+URL Filtering
 - Email: AV+Anti-Spam
 - NIS signatures

Subscription Services



Advanced Threat Protection

Threat
Vector

Content Files and Streaming Traffic

Viruses

Worms

Protocol Exploits

Scripts

Encrypted Web

Inspection
Technology

HTTP and HTTPS Inspection

Microsoft
Antimalware

Network Inspection
System

Application Layer
Proxy

Coverage for Streaming and Content-based traffic

- Zero-day and Variant Protection
 - Generic and Specific Signatures
 - Protocol Analysis
 - Heuristic
- Granular control of Web traffic
- Extensible as new threats appear



Microsoft®

Forefront™

Unified Access Gateway

UAG delivers secure, anywhere access to messaging, collaboration and other applications, increasing productivity while maintaining compliance with policy.

Application Publishing

- Granular Application Filtering
- Session cleanup and removal
- Remote Desktop and RemoteApp integration
- Multiple tunnels allowing various levels of client/server and network access

DirectAccess

- Extends DirectAccess to legacy applications and platforms
- Simplifies DirectAccess deployments with wizards and automated policies
- Scales DirectAccess through built in load balancing and array management

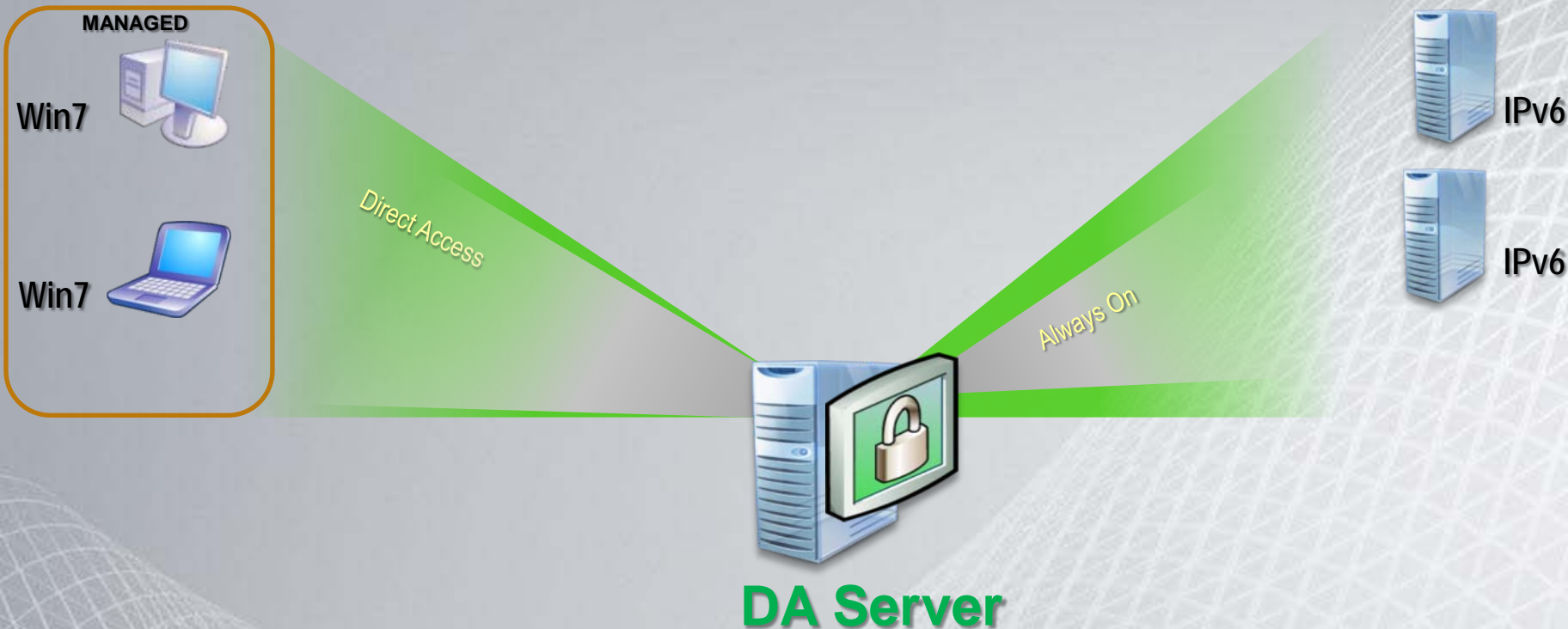
End Point Access Controls

- Extensive and granular end point health detection
- Integrated with Network Access Protection (NAP) policies

Scale and Management

- Built in load balancing
- Array management capabilities
- Enhanced monitoring and management (SCOM)

Direct Access – Platform



DA Server

Comprehensive anywhere access solution available in Windows 7 and Windows Server 2008 R2

- Provides seamless, always-on, secure connectivity to on-premise and remote users alike
- Eliminates the need to connect explicitly to corpnet while remote
- Facilitates secure, end-to-end communication and collaboration
- Leverages a policy-based network access approach
- Enables IT to easily service/secure/update/provision mobile machines whether they are inside or outside the network

Direct Access – Solution

UAG Benefits for DA:


1. Improves adoption and extends access
2. Access for down level and non Windows clients
3. Enhances scalability and management
4. Simplifies deployment and administration
5. Improves security


MANAGED


Win7 

Win7 

UNMANAGED

Vista XP 

Non Windows 

PDA 



Direct Access Server

Microsoft
Forefront
Unified Access Gateway



IPv6



IPv6



IPv4



IPv4



IPv4

Direct Ac

Always On

SSL VPN

Extend support to IPv4 servers

UAG is a hardened and edge-ready appliance available in HW and virtual options

Forefront Protection 2010 for Exchange

Forefront Protection 2010 for Exchange

Forefront security solutions help organizations protect their messaging and collaboration servers against viruses, worms, spam, and inappropriate content.

Advanced Protection

Multiple scan engines at multiple layers throughout the e-mail infrastructure provide improved protection against e-mail threats.

Availability & Control

Tight integration with Microsoft Exchange and Windows-based SMTP servers maximizes availability and management control.

Secure Content

Helps organizations eliminate inappropriate language and dangerous attachments from internal and external communications

What's New

Forefront Protection for Exchange 2010

Forefront Protection 2010 for Exchange Server combines real-time antivirus, antispyware, antispam, and content filtering in a single solution to provide comprehensive protection against the latest threats to your messaging infrastructure.

New features include:

- Premium antispam protection, with 99 percent detection rate, less than 1 in 250,000 false positives, and backscatter filtering.
- New user interface with dashboard view of detection statistics and health monitoring.
- Antispyware scanning provided by the Microsoft Antimalware Engine.
- Integrated provisioning and management of Forefront Online Protection for Exchange (FOPE) for hybrid, on-premise/hosted protection.
- Support for Exchange 2010 and Exchange 2007, Windows PowerShell, and Hyper-V.
- Standardized installation using MSI installer

Microsoft Forefront Protection 2010 for Exchange Server

SC rate: 99.93%

SC rate (VB corpus): 97.35%

SC rate (image spam): 99.77%

SC rate (large spam): 99.90%

FP rate: 0.23%

FP rate (VB corpus): 0.79%

Final score: 99.25



Microsoft's Forefront Protection 2010 for Exchange Server was the clear winner of the last test, achieving the highest final score by some distance. The final scores of the various products were closer this month, but with the second highest spam catch rate and just a handful of false positives, *Forefront* was yet again the product with the highest final score and adds another VBSpam award to its collection.

CONCLUSION

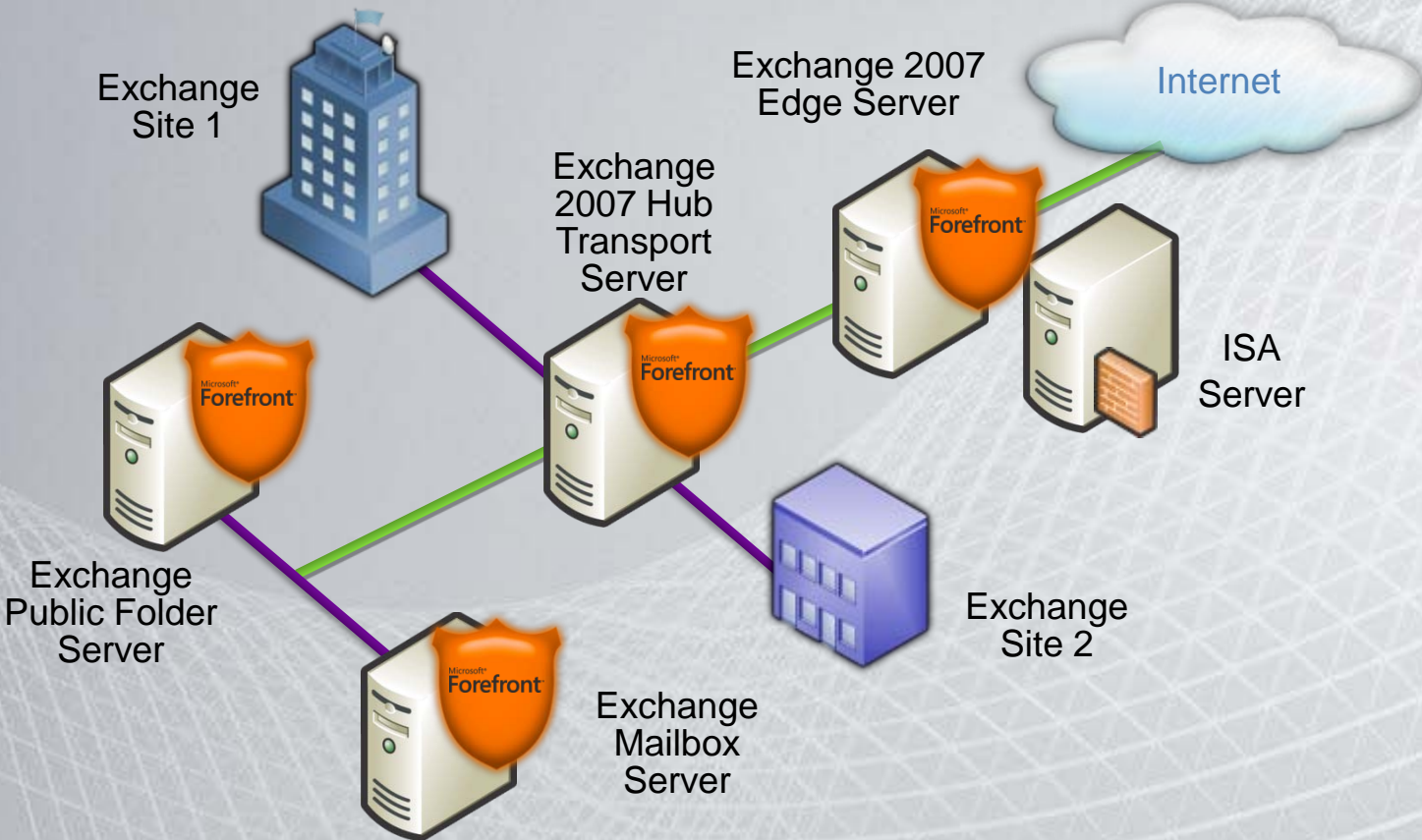
Products ranked by final score	Final score
MS Forefront	99.25
BitDefender	99.14
Libra Esva	99.13
Vamsoft ORF	99.13
Symantec Brightmail	99.12
Sophos	99.00
Spamhaus	98.68
MXTools Suite	98.67
M86 MailMarshal	98.46
Webroot	98.30
McAfee EWS	98.29
Vade Retro	98.18
The Email Laundry	98.15
SpamTitan	98.11
Kaspersky	98.01
McAfee Email Gateway	97.83
FortiMail	97.32
SPAMfighter	96.79
Sunbelt VIPRE	95.43
modusGate	94.60
MessageStream	93.86

This month saw several significant changes to the test corpora, and it was interesting to see how products coped with a more international corpus of legitimate emails including different character sets.

The developers of the products that did not perform so well on this occasion will be eager to show in the next test that this was due to settings needing to be tweaked rather than a fault in the product. The top performers, of course, will need to demonstrate that their results weren't just a coincidence and that they can perform well consistently; a complete picture of the quality of a product can only be gained by looking at the results of several VBSpam reviews and monitoring the performance of products over time.

As always, comments and suggestions from vendors, researchers and end-users are welcome. The next test is set to run throughout June; the deadline for product submission is 25 May 2010. Any developers interested in submitting a product should email martijn.grooten@virusbtn.com.

Layered Protection Across Exchange Roles



Forefront Protection 2010 for SharePoint

Forefront Protection 2010 for SharePoint

Microsoft Forefront Security for SharePoint integrates multiple scan engines from industry-leading vendors and content controls to help businesses protect their Microsoft SharePoint collaboration environments by eliminating documents containing malicious code, confidential information, and inappropriate content.

Comprehensive Protection

- Multiple industry-leading antivirus engines
- File & Content Keyword Filtering
- Support for Open XML & IRM-protected docs

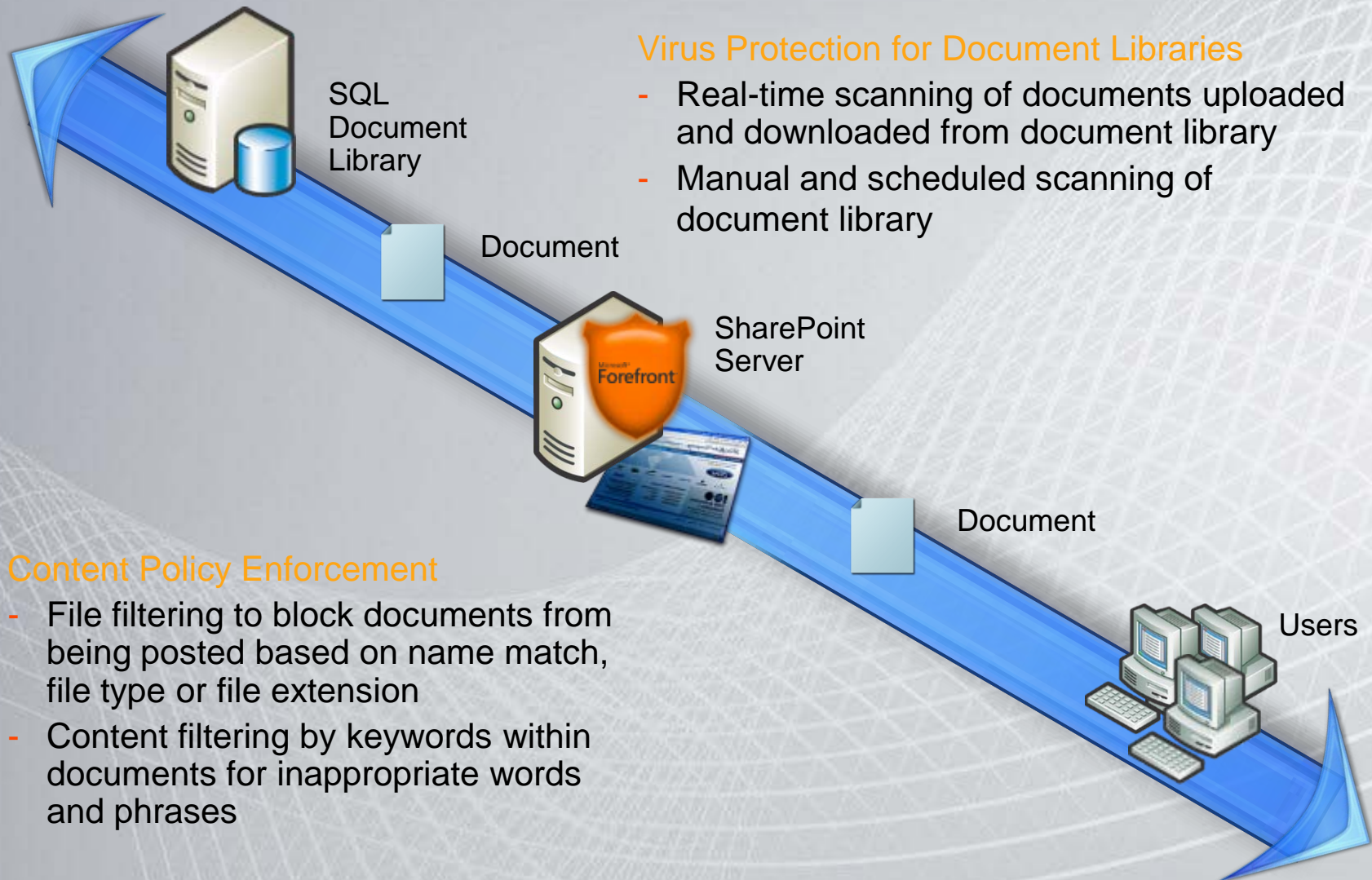
Optimized Performance

- Deep integration with SharePoint Server
- Scanning innovations and performance controls
- Continuous scanning during engine updates

Simplified Management

- Administration console for easy setup and management
- Automated signature updates
- Centralized reporting, notifications and alerts

Forefront Security for SharePoint



Virus Protection for Document Libraries

- Real-time scanning of documents uploaded and downloaded from document library
- Manual and scheduled scanning of document library

Content Policy Enforcement

- File filtering to block documents from being posted based on name match, file type or file extension
- Content filtering by keywords within documents for inappropriate words and phrases

Forefront Protection for OCS



Microsoft®

Forefront™

Security for Office Communications Server

Microsoft Forefront Security for Office Communications Server provides fast and effective protection against IM-based malware by including multiple scanning engines from industry-leading security partners in a single solution and helps reduce corporate liability by blocking IM messaging containing inappropriate content.

Comprehensive Protection

- Integrates multiple antimalware engines
- Blocks transfer of dangerous file types
- Prevents sharing of out-of-policy content

Optimized Performance

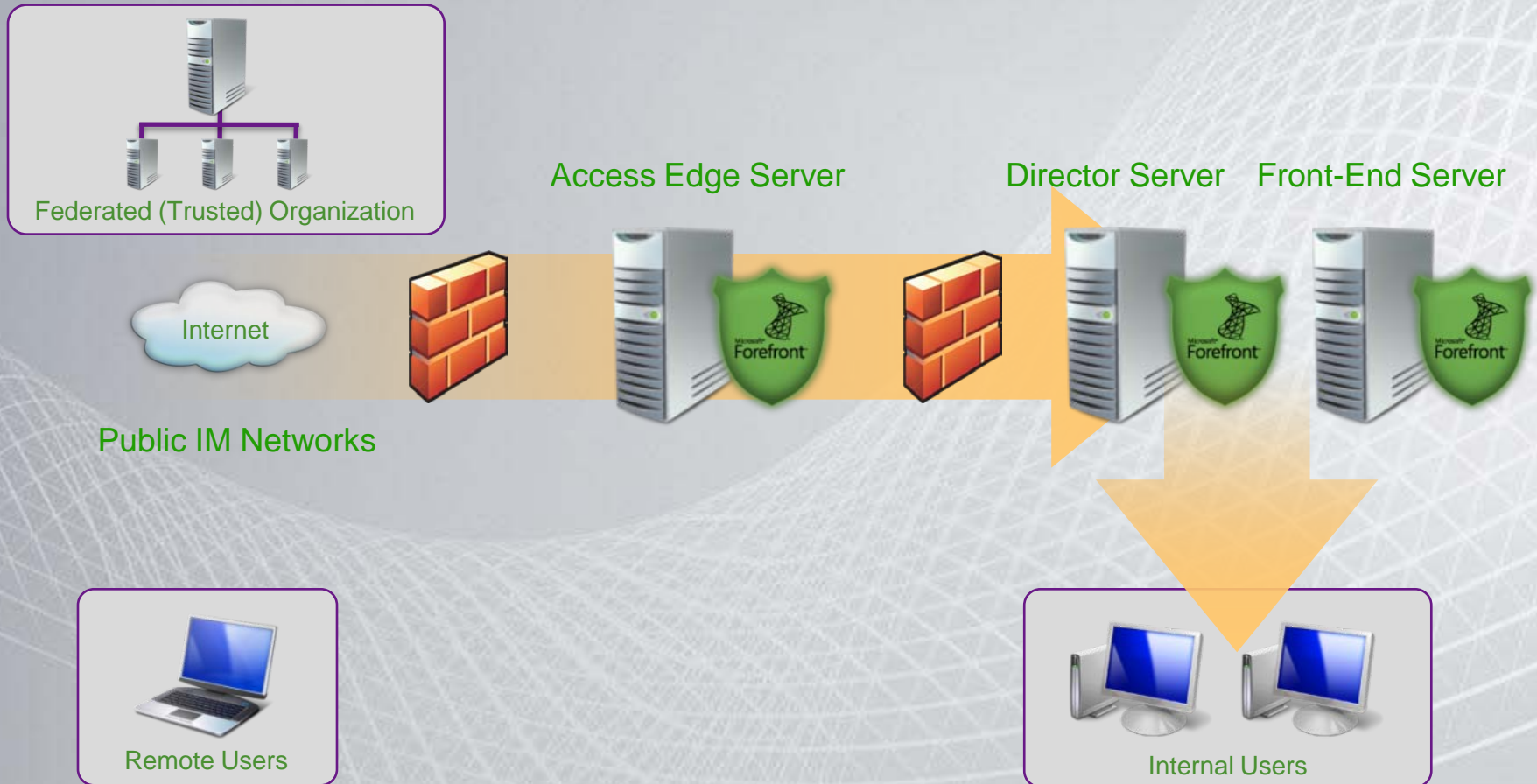
- Optimizes virus scanning on OCS 2007
- Integrates with multiple server roles
- Protects federated connections and public IM

Simplified Management

- Built-in administrator console
- Automated signature updates
- IM notifications for out-of-policy activity

OCS 2007 Enterprise Integration

FSOCS protects each instance of Standard Edition, Front End, Director and Access Edge server roles, with support for OCS 2007 and OCS 2007 R2 and Lync 2010 soon.



Forefront End Point Protection

Forefront Endpoint Protection 2010



Lower Cost of Deployment

- Built on Configuration Manager software distribution infrastructure
- Supports all Configuration Manager topologies including Branch Office and Non-Domain-Joined
- Ease of migration
- Deployed across various operating systems (Windows Client & Server)



Be Protected and Stay Productive

- Protect your desktops against viruses, spyware, rootkits, and malware
- Productivity oriented default configuration
- Integrated host firewall management
- Backed by global Malware Research and Response



Unified Desktop Management

- Unified management interface targeted for the desktop admin
- Actionable and timely alerting
- Simple operation-oriented policy administration
- Historic reporting for security administrator

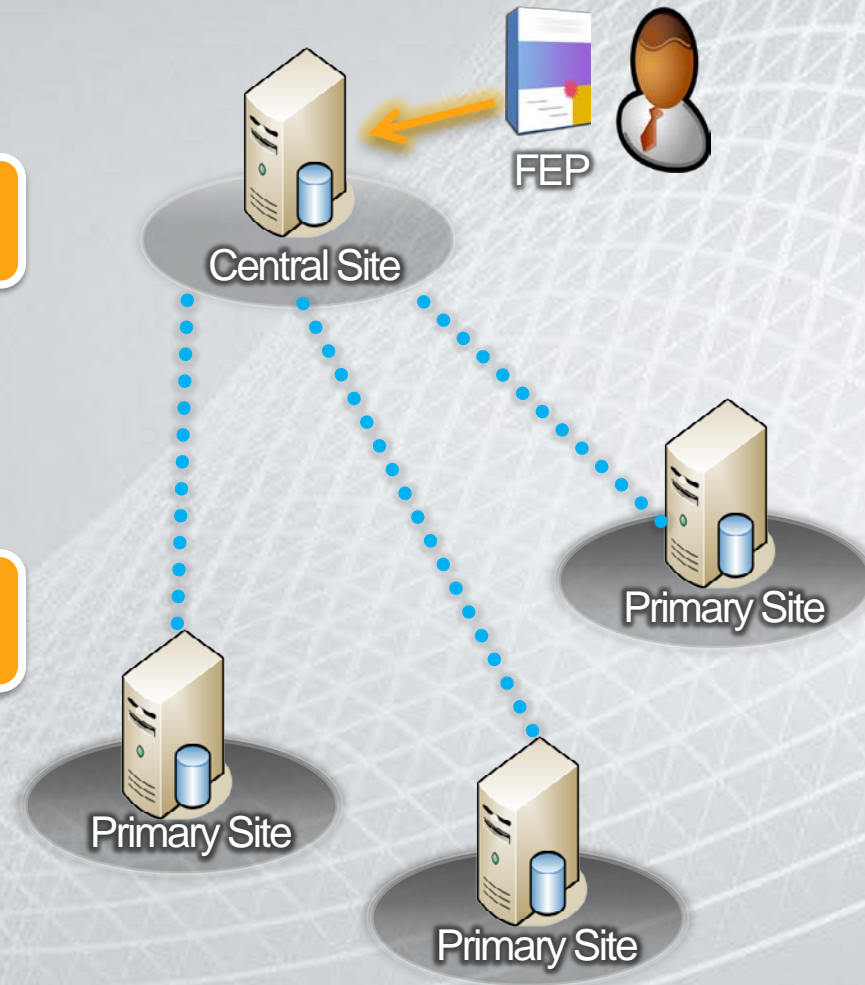
Building Endpoint Protection On ConfigMgr 2007

Uses the existing infrastructure

- No new servers
- Integrated management experience

Simple deployment process

- Installs on to existing ConfigMgr roles
- Client deployment using the existing infrastructure, tools & processes



Client Deployment Overview

- Built on ConfigMgr Software Distribution
- Supports existing topologies including NDJ, Branch
- Automatically switches existing client install base:
 - Upgrade from Forefront Client Security v.1
 - Switch from Symantec, McAfee and TrendMicro clients
- Also supports deployment on clients not managed via ConfigMgr

Switching from other security providers

- **Switching challenges**
 - Different products, managed by different systems
 - Vulnerability window during replacement
 - Complex, error prone to automate

- **Switching functionality in FEP 2010**
 - Integrated with deployment, not a standalone tool
 - Fully automated
 - Encapsulates the complexities of switching
 - Reduces the overall deployment costs

Microsoft Forefront Identity Manager 2010

Microsoft Forefront Identity Manager

Microsoft® Identity Lifecycle Manager 2007



- Identity Synchronization
- User Provisioning
- Certificate and Smartcard Management



Microsoft® Forefront™ Identity Manager 2010



User Management



Credential Management



Common Platform
Workflow
Connectors
Logging
Web Service API
Synchronization



Group Management



Policy Management

- Office Integration for Self-Service
- Support for 3rd Party CAs
- Codeless Provisioning
- Group & DL Management
- Workflow and Policy

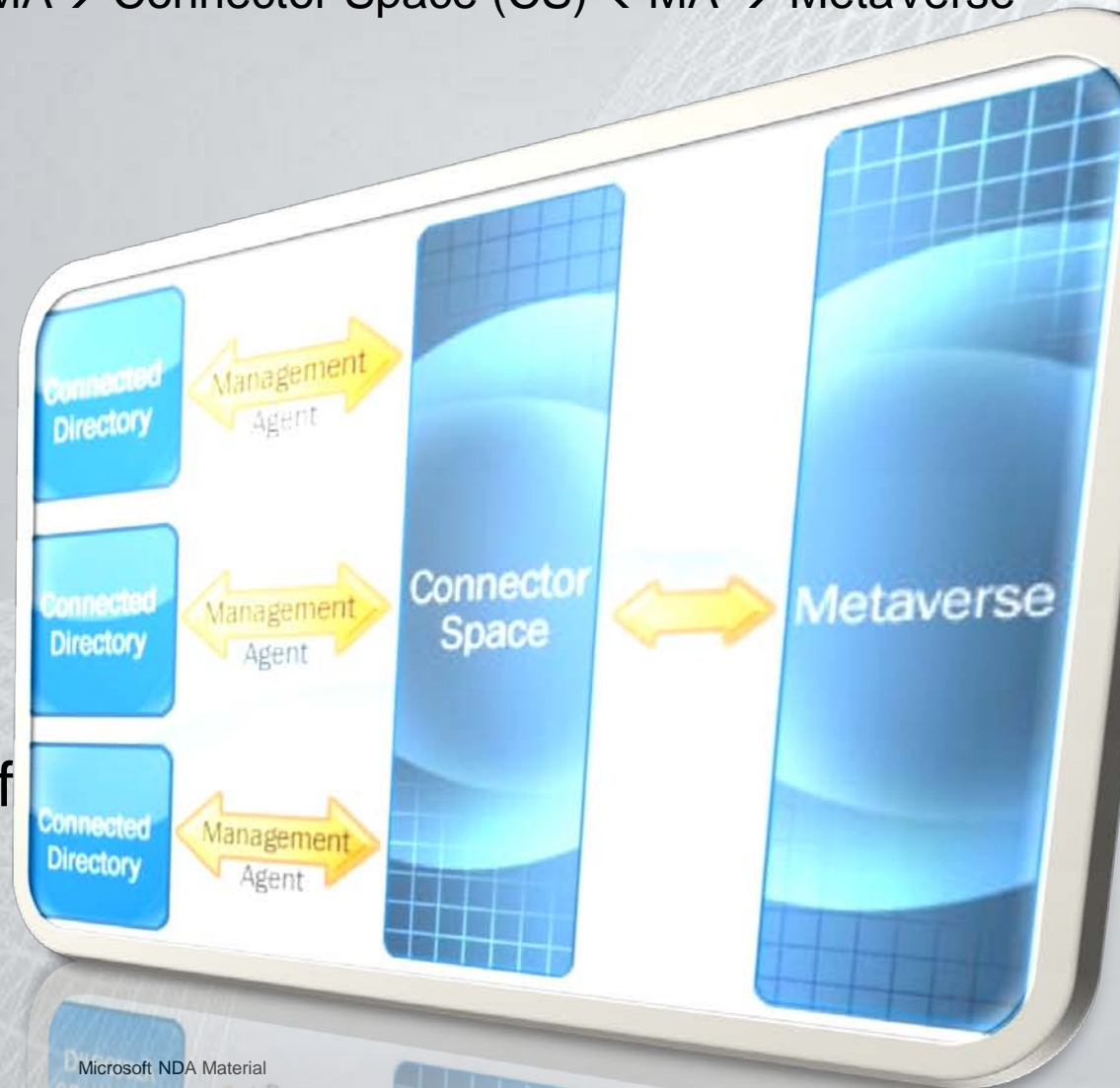
FIM 2010 Components

- **Synchronization Service**
 - Provisioning / De-provisioning
 - Password Synchronization
- **Identity Portal**
 - Password Self-Service
 - Group Management
 - Workflow
- **Certificate Management**
 - Strong authentication

Sync. Service: FIM 2010 Data Flow

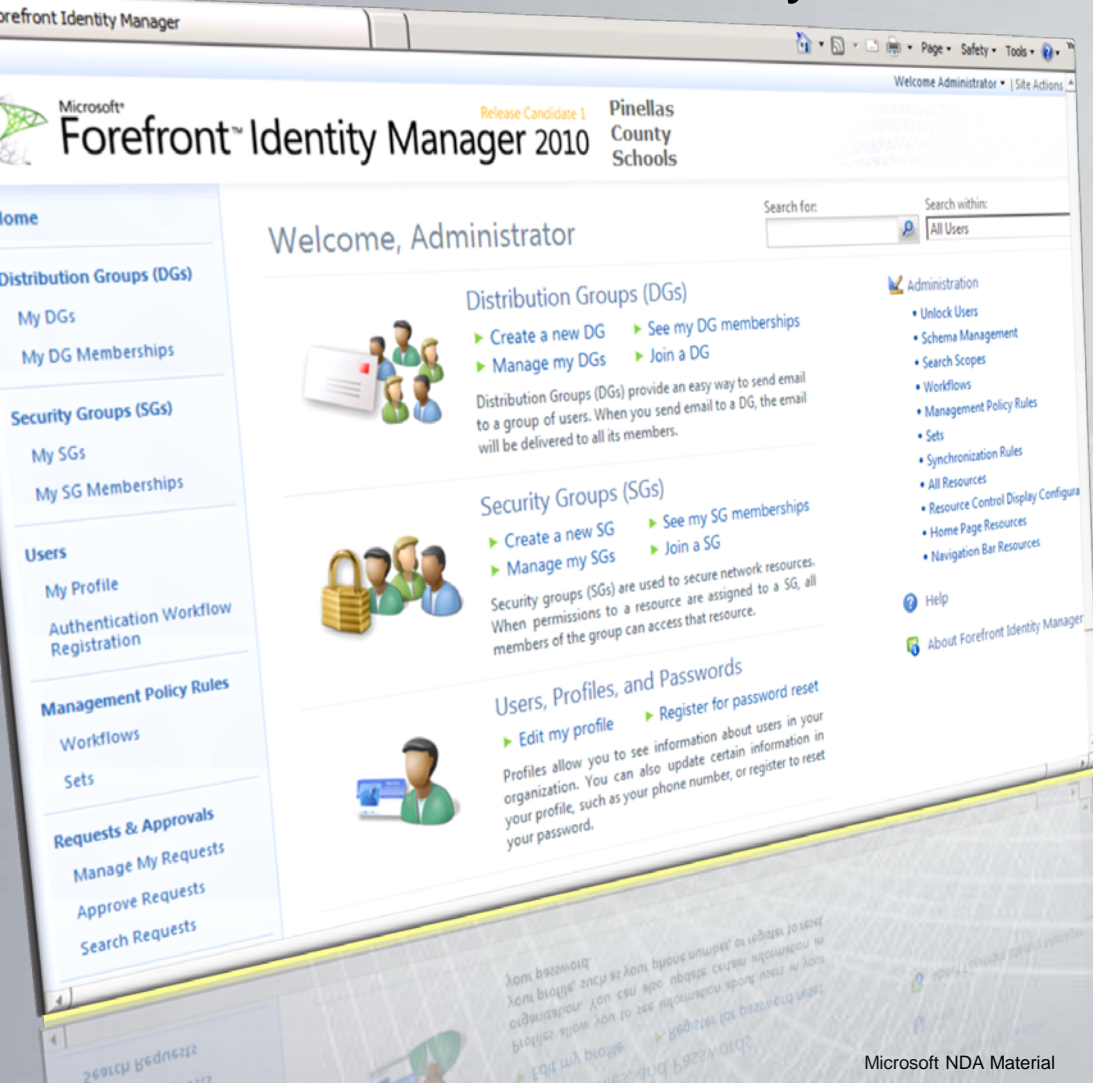
Connected Data Source (CDS) \leftarrow MA \rightarrow Connector Space (CS) \leftarrow MA \rightarrow MetaVerse

- Management Agent governs data flow
- SQL Server 2008 Backend
 - Connector Spaces & MetaVerse
 - Each Management Agent has its own Connector Space
- Architecture is designed to allow for processing of business rules before synchronization



Identity Portal: Make it Yours!

SharePoint-based Identity Portal for Management and Self



How you extend it

- Add your own portal pages or web parts
- Build new custom solutions
- Expose new attributes to manage by extending FIM 2010 schema
- Choose SharePoint theme to customize look and feel

Microsoft[®]

Your potential. Our passion.[®]

© 2009 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.