Forefront Endpoint Protection Overview

Adwait Joshi (AJ)
Sr. Technical Product Manager
Microsoft Corporation

Shai Kariv
Group Program Manager
Microsoft Corporation

Natan Kfir
Sr. Program Manager
Microsoft Corporation
Session Objectives and Takeaways

Session Objectives:
- Overview of Forefront Endpoint Protection (FEP)
- Understand how to use System Center Configuration Manager to manage antimalware protection

Key Takeaways:
- Convergence of Forefront Endpoint Protection with System Center Configuration Manager:
  - Lowers ownership costs
  - Delivers simplified management and ease of deployment
  - Enables improved visibility for identifying and safeguarding potentially vulnerable endpoints
Forefront Endpoint Protection 2010
One infrastructure for desktop management and protection

Ease of Deployment
• Built on top of Microsoft® System Center Configuration Manager
• Supports all System Center Configuration Manager topologies and scale
• Facilitates easy migration
• Deploy across various operating systems Windows® client and Server

Enhanced Protection
• Protection against all type of malware
• Proactive security against zero day threats
• Productivity-oriented default configuration
• Integrated management of host firewall
• Backed by Microsoft Malware Protection Center

Simplified Desktop Management
• Unified management interface for desktop administrators
• Effective alerts
• Simple, operation-oriented policy administration
• Historical reporting for security administrators
Ease of Deployment
Management Models

Centralized Management and Reporting
- Enables consolidated management on a central site

Decentralized Management and Reporting
- Enables distributed management of endpoint security
- Minimum impact on the Config Manager sites performance

Decentralized Policy Management with Centralized Reporting
- Consolidated reporting on the central site for enterprise wide visibility

Hierarchical Deployment for Distributed Management
FEP Server Installation Options

Microsoft Forefront Endpoint Protection 2010

Deployment Options

Select the topology that you want to configure:

- Basic topology
  Installs Microsoft Forefront Endpoint Protection 2010 Database, Site Server Extension, Console Extension, Reporting components, and Reporting database based on your current Configuration Manager deployment.

- Basic topology with remote reporting database
  Installs the basic topology, and allows the installation of the reporting database on a different computer.

- Advanced topology
  Allows customized installation.

- Configuration Manager Console FEP 2010 Extension only
  Installs Forefront Endpoint Protection 2010 extension for the Configuration Manager console.

< Back  |  Next >  |  Cancel
Simplified Client Distribution

Configuration Manager integration
- Same software distribution process to deploy FEP Clients
- Support for all topologies, including Branch Office and Non-Domain-Joined

Flexible deployment and migration
- Deploy across Windows client and Windows Server
- Support for FEP pre-installation on golden image
- Support for standalone unmanaged deployment without Configuration Manager

Easy migration from existing solutions and automatic removal of existing clients
- Symantec
- McAfee
- TrendMicro
- Forefront Client Security
Multiple update sources

- Configurable priority for sources
- Uses existing infrastructure of Microsoft Windows Server Update Services (Software Update Management)
- Improved size of signature downloads reduces bandwidth use
- Delta updates to recent definitions ~50 KB - 2048 KB
FEP 2010

FEP 2010 Client Deployment
Enhanced Protection
Comprehensive Protection Stack

**Reactive Techniques** (Against Known Threats)
- Data Execution Prevention
- Address Space Layout Randomization
- Windows Resource Protection

**Behavior Monitoring**

**Proactive Techniques** (Against Unknown Threats)
- Anti-malware
  - Windows Internet Explorer® 8 SmartScreen
- Dynamic Translation and Emulation
  - Microsoft AppLocker™

**Application**

**File System**

**Network**
- Vulnerability Shielding (Network Inspection System)
- Windows Firewall Centralized Management

**Dynamic Signature Service**

**Dynamic Cloud Updates**

**Forefront Endpoint Protection**

**Windows 7**
Protect Clients with Reduced Complexity

Simple interface
- Minimal, high-level user interactions
- Only necessary interactions

Administration options
- User configurability controls
- Central policy enforcement

Maintains high productivity
- CPU throttling during scans
- Faster scans through advanced caching
Simplified Management
Unified Management Interface

- **Simplified operations in one console**
  - Deployment issues
  - Protection status
  - Antimalware activity issues
  - Definitions updates issues
  - Policy distribution issues
  - Visibility to FEP DCM baselines

- **Launchpad to ConfigMgr collections**
  - Drill down to ConfigMgr collections
  - Refresh operation statistics on demand

- **Manual remediation actions**:
  - Full/Quick scan
  - Signature update
Centralized Policy Management

Author policies and edit policy settings:
- Forefront Endpoint Protection – Configuration Manager
- Group Policy – GPEDIT + ADMX

Deploy policies via:
- Configuration Manager
- Group Policy
- Command-line
  - During install (FEPInstall.exe /policy <policy>)
  - After Install (ConfigSecurityPolicy.exe <policy>)

Preconfigured templates for server roles:
- Performance, security, or by server role template
- Sixteen templates provide best practices based on server roles
Historical Reports

Rich SQL Reporting Services-based information about:

- Malware incidents
- Protection status
- Security compliance
- Policy distribution
- Alerts

Customizable filters and views, easily extensible for use in other tools

Available in multiple formats

Workbook for custom reports and schema published

Critical Alerts

Set levels for critical security alerts, including:

- Malware outbreak
- Malware detection
- Multiple malware detection
- Machines with repeated infections

Receive email notifications of malware activity
FEP 2010

FEP policy management
FEP management
and reporting
Forefront Endpoint Protection 2012
One infrastructure for desktop management and protection: ConfigMgr 2012

Ease of Deployment:
- Built on top of System Center Configuration Manager
- Supports all CM topologies and scale
- Supports various operating systems Windows® Client and Server
- Facilitates easy migration from previous versions and 3rd parties

Enhanced Protection:
- Protection against all types of malware
- Proactive security against zero day threats
- Productivity-oriented default configuration
- Integrated management of host firewall
- Backed by Microsoft Malware Protection Center

Simplified Desktop Management:
- Unified experience for desktop administrators
- Simple, operation-oriented policy administration
- Historical reporting for security administrators
Forefront Endpoint Protection 2012
One infrastructure for desktop management and protection: ConfigMgr 2012

Ease of Deployment
- Built on top of System Center Configuration Manager
- Supports all CM topologies and scale
- Supports various operating systems Windows® Client and Server
- Facilitates easy migration from previous versions and 3rd parties
- User- and device-based roll out of client updates, sigs, policies
- Enables migration from FEP 2010 without client roll out

Enhanced Protection
- Protection against all types of malware
- Proactive security against zero day threats
- Productivity-oriented default configuration
- Integrated management of host firewall
- Backed by Microsoft Malware Protection Center

Simplified Desktop Management
- Unified experience for desktop administrators
- Simple, operation-oriented policy administration
- Historical reporting for security administrators
Forefront Endpoint Protection 2012
One infrastructure for desktop management and protection: ConfigMgr 2012

**Ease of Deployment**
- Built on top of System Center Configuration Manager
- Supports all CM topologies and scale
- Supports various operating systems Windows® Client and Server
- Facilitates easy migration from previous versions and 3rd parties
- User- and device-based roll out of client updates, sigs, policies
- Enables migration from FEP 2010 without client roll out

**Enhanced Protection**
- Protection against all types of malware
- Proactive security against zero day threats
- Productivity-oriented default configuration
- Integrated management of host firewall
- Backed by Microsoft Malware Protection Center
- Additional server role protection: TMG, OCS
- Multi-role server protection

**Simplified Desktop Management**
- Unified experience for desktop administrators
- Simple, operation-oriented policy administration
- Historical reporting for security administrators
Forefront Endpoint Protection 2012
One infrastructure for desktop management and protection: ConfigMgr 2012

Ease of Deployment
- Built on top of System Center Configuration Manager
- Supports all CM topologies and scale
- Supports various operating systems Windows® Client and Server
- Facilitates easy migration from previous versions and 3rd parties
- User- and device-based roll out of client updates, sigs, policies
- Enables migration from FEP 2010 without client roll out

Enhanced Protection
- Protection against all types of malware
- Proactive security against zero day threats
- Productivity-oriented default configuration
- Integrated management of host firewall
- Backed by Microsoft Malware Protection Center
- Additional server role protection: TMG, OCS
- Multi-role server protection

Simplified Desktop Management
- Unified experience for desktop administrators
- Simple, operation-oriented policy administration
- Historical reporting for security administrators
- Real-time security alerts
- Role-based security administration with CM RBA
- Signatures managed via CM Auto Deployment Rules
- User- and device-view in security reports
Simplified Deployment and Migration

**Simplified installation using existing infrastructure**
- Install once – work everywhere
- Full functionality at all sites
- Supports all Configuration Manager Topologies
- No additional infrastructure deployment

**Built-in migration from FEP 2010:**
- Works with FEP 2010 client
- Policy & Alert migration support

**Replacement of 3rd party during install**
- Additional versions on top of FEP 2010
- Additional vendors on top of FEP 2010
Role-Based Security Administration

- Top customer ask is role separation across 2 personas: security versus desktop admin
- CM 2012 provides RBA capabilities: permissions on objects, scoped to specific collections
  - FEP object types: FEP Client, FEP Operations, FEP Alerts, FEP Policies
  - Permissions: Create, Modify, Deploy, Read
  - Scope: collections e.g., All Users in Japan, All Systems in Germany
  - FEP extends CM with 2 custom roles: policy author and policy deployment manager

Security Administrator

- Create new policies
- Modify default policies
- Modify custom policies
- Modify Precedence

Policy Deployment Manager

- Assign policy to collection
- Operate policy roll out
Signature Update via Distribution Points

- Definition content delivered through Config Manager distribution points, to minimize network impact
- Support for automatic approval
- Admin controls schedule of definition download, distribution to DPs, delivery to clients
- Fallback support to WSUS, UNC & Microsoft Update
FEP 2012

FEP 2012 Dashboard
FEP 2012 Policy Management
FEP 2012 Integrated Alerts
Summary

- Convergence of Forefront Endpoint Protection with System Center Configuration Manager:
  - Lowers ownership costs
  - Delivers simplified management and ease of deployment
  - Enables improved visibility for identifying and safeguarding potentially vulnerable endpoints

- FEP 2010 available to you now! Released in December 2010

- FEP 2012 planned release timeframe similar to ConfigMgr 2012
  - Public beta in May
Please Complete an Evaluation Form

Your feedback is important!

Be eligible to win great daily prizes!

For more information please refer to your Conference Guide

- Two ways to access online evaluation forms:
  - CommNet stations located throughout the Mandalay Bay Convention Center
  - From any wired or wireless connection to www.mms-2011.com
Microsoft Management Summit 2011

March 21-25
2011

You. Empowered.