



Windows Vista™

Security and Compliance

Robert Nottoli | Principal Technology Specialist | Microsoft Corporation
robnotto@microsoft.com



Windows Vista™

DISCLAIMER FOR DOCUMENTATION REGARDING

PRE-RELEASED SOFTWARE

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release, including URL and other Internet Web sites referenced, and is the confidential and proprietary information of Microsoft Corporation. The entire risk of the use or the results from the use of this document remains with the user.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. 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 presented after the date of publication. Therefore, **MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.**

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

Copyright 2006 Microsoft Corporation. All rights reserved.

Microsoft and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Fundamentals

- Security Development Lifecycle
- Threat Modeling and Code Reviews
- Windows Service Hardening

Threat and Vulnerability Mitigation

- Internet Explorer Protected Mode
- Windows Defender
- Network Access Protection

Security and Compliance

Identity and Access Control

- User Account Control
- Plug and Play Smartcards
- Granular Auditing

Information Protection

- BitLocker™ Drive Encryption
- EFS Smartcards
- RMS Client

Fundamentals

- Improved Security Development Lifecycle (SDL) process for Windows Vista
 - Periodic mandatory security training
 - Assignment of security advisors for all components
 - Threat modeling as part of design phase
 - Security reviews and testing built into the schedule
 - Security metrics for product teams
- Common Criteria (CC) Certification

Windows Service Hardening

Defense in depth

- Services run with reduced privilege compared to Windows XP
- Windows services are profiled for allowed actions to the network, file system, and registry
- Designed to block attempts by malicious software to make a Windows service write to an area of the network, file system, or registry that isn't part of that service's profile



Mitigating Buffer Overruns With Hardware Protection

- NX enables software to mark sections of the computer's memory as exclusively for data, and the processor will prevent applications and services from executing any code there.
- Address Space Layout Randomization (ASLR) is another defense capability in Windows Vista that makes it harder for malicious code to exploit a system function. Whenever a Windows Vista computer is rebooted, ASLR randomly assigns executable images such as DLLs and EXEs to one of 256 possible locations in memory.



Threat And Vulnerability Mitigation

Protect against malware and intrusions

Internet Explorer 7



Social Engineering Protections



- Phishing Filter and Colored Address Bar
- Dangerous Settings Notification
- Secure defaults for IDN

Protection from Exploits

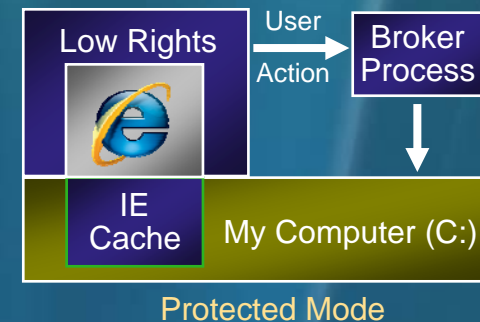
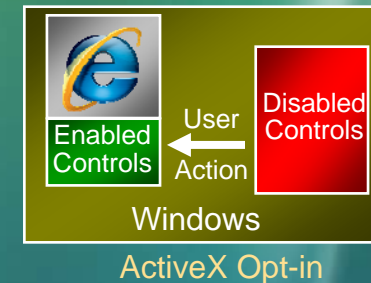
- Unified URL Parsing
- Code quality improvements (SDLC)
- ActiveX Opt-in
- Protected Mode to prevent malicious software



ActiveX Opt-in And Protected Mode

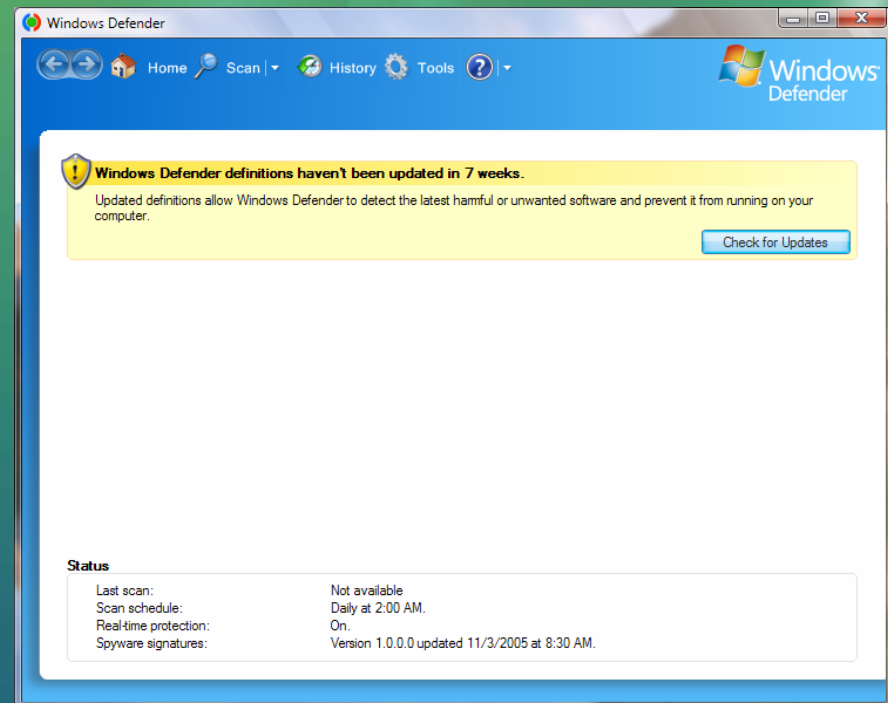
Defending systems from malicious attack

- **ActiveX Opt-in** puts users in control
- Reduces attack surface
- Previously unused controls disabled
- Retain ActiveX benefits, increase user security
- **Protected Mode** reduces severity of threats
- Eliminates silent malware install
- IE process 'sandboxed' to protect OS
- Designed for security and compatibility

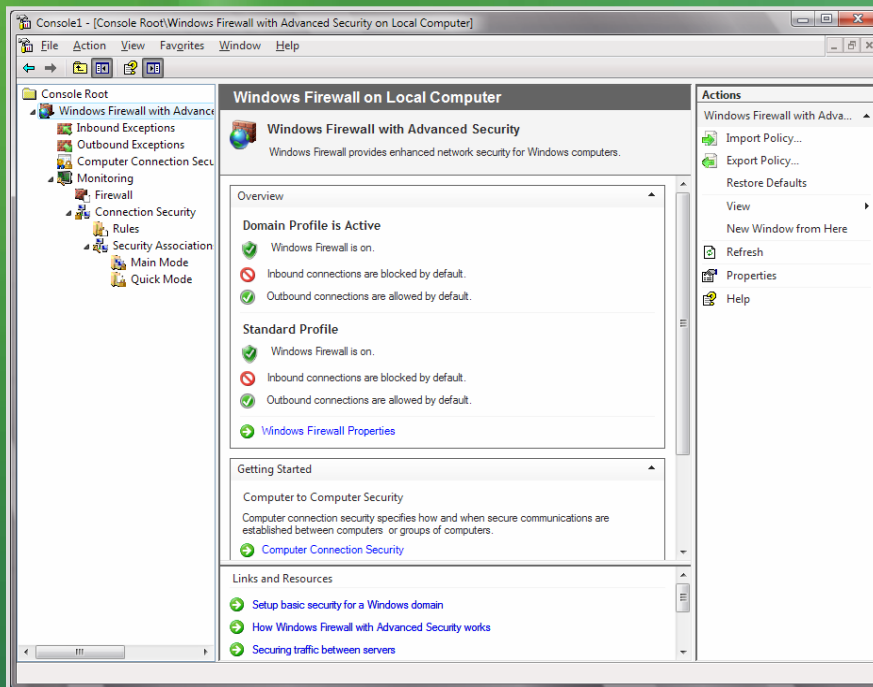


Windows Defender

- Improved Detection and Removal
- Redesigned and Simplified User Interface
- Protection for all users

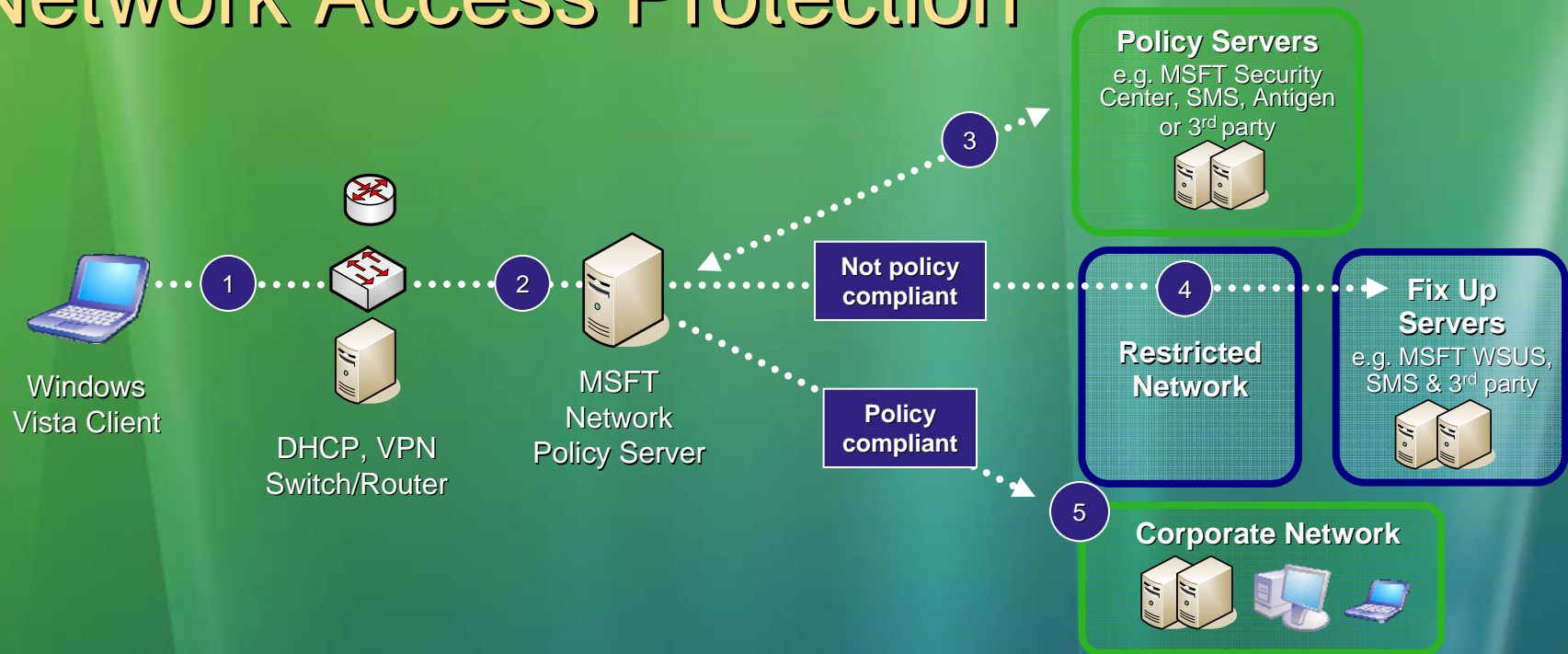


Windows Vista Firewall



- Combined firewall and IPsec management
 - New management tools – Windows Firewall with Advanced Security MMC snap-in
 - Reduces conflicts and coordination overhead between technologies
- Firewall rules become more intelligent
 - Specify security requirements such as authentication and encryption
 - Specify Active Directory computer or user groups
- Outbound filtering
 - Enterprise management feature – not for consumers
- Simplified protection policy reduces management overhead

Network Access Protection



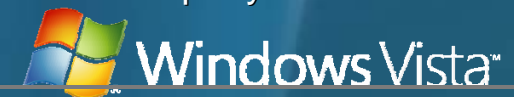
Customer Benefits

Enhanced Security

- All communications are authenticated, authorized & healthy
- Defense-in-depth on your terms with DHCP, VPN, IPsec, 802.1X
- Policy-based access that IT Pros can set and control

Increased Business Value

- Preserves user productivity
- Extends existing investments in Microsoft and 3rd party infrastructure
- Broad industry partnership





Identity And Access Control

Enable Secure Access to Information

Challenges

- Users running as admin = unmanaged desktops
 - Viruses and Spyware can damage the system when run with elevated privileges
 - Enterprise users running elevated privileges can compromise the corporation
 - Users can make changes that require re-imaging the machine to undo
- Line of Business (LoB) applications require elevated privileges to run
 - System security must be relaxed to run the LoB application
 - IT Administrators must reevaluate the LoB applications for each Operating System release due to inconsistent configuration settings
- Common Operating System Configuration tasks require elevated privilege
 - Corporations can't easily deploy applications unless they compromise Operating System Security
 - Simple scenarios like changing the time zone don't work
 - Users are not able to manage non-sensitive account information

User Account Control

- Goal: Allow businesses to move to a better-managed desktop and consumers to use parental controls
 - Make the system work well for standard users
 - Allow standard users to change time zone and power management settings, add printers, and connect to secure wireless networks
 - High application compatibility
 - Make it clear when elevation to admin is required and allow that to happen in-place without logging off
 - High application compatibility with file/registry virtualization
 - Administrators use full privilege only for administrative tasks or applications
 - User provides explicit consent before using elevated privilege



Improved Auditing

- More Granularity
 - Support for many auditing subcategories: Logon, logoff, file system access, registry access, use of administrative privilege
 - Previous versions of Windows only support high-level categories such as System, Logon/Logoff, and Object Access, with little granularity
- New Logging Infrastructure
 - Easier to filter out “noise” in logs and find the event you’re looking for
 - Tasks tied to events: When an event occurs, such as administrative privilege use, tasks such as sending an Email to an auditor can run automatically

Authentication Improvements

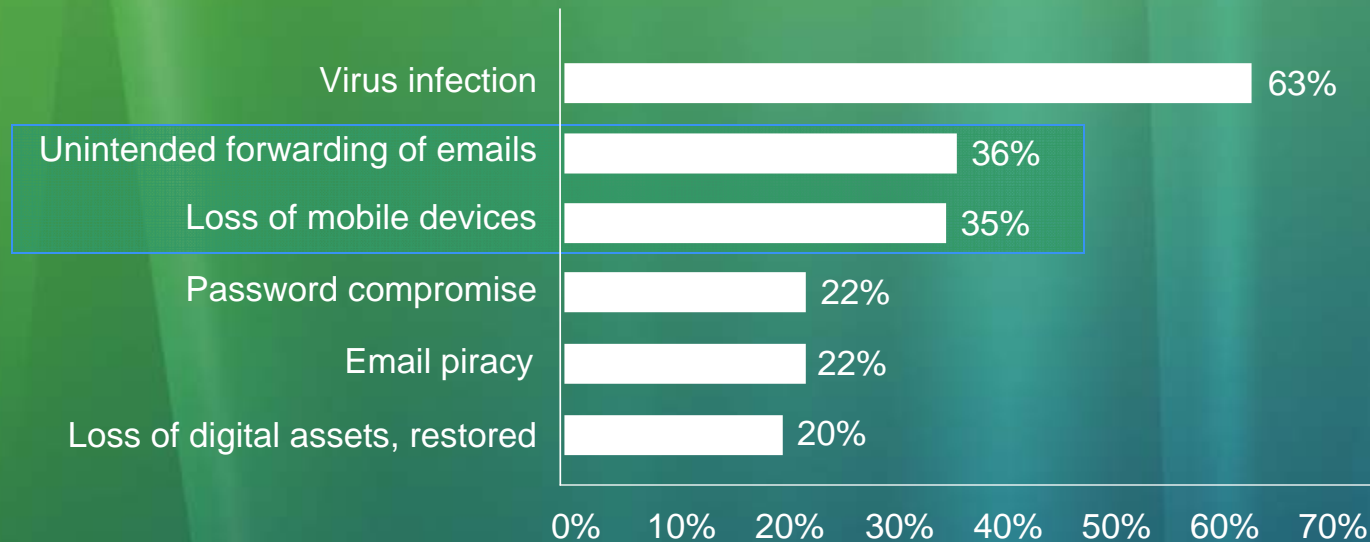
- Plug and Play Smart Cards
 - Drivers and Certificate Service Provider (CSP) included in Windows Vista
 - Login and credential prompts for User Account Control all support Smart Cards
- New logon architecture
 - GINA (the old Windows logon model) is gone.
 - Third parties can add biometrics, one-time password tokens, and other authentication methods to Windows with much less coding



Information Protection

Protect Corporate Intellectual Property and Customer Data

Information Leakage Is Top-of-mind With Business Decision Makers



“After virus infections, businesses report unintended forwarding of e-mails and loss of mobile devices more frequently than they do any other security breach”

Jupiter Research Report, 2004



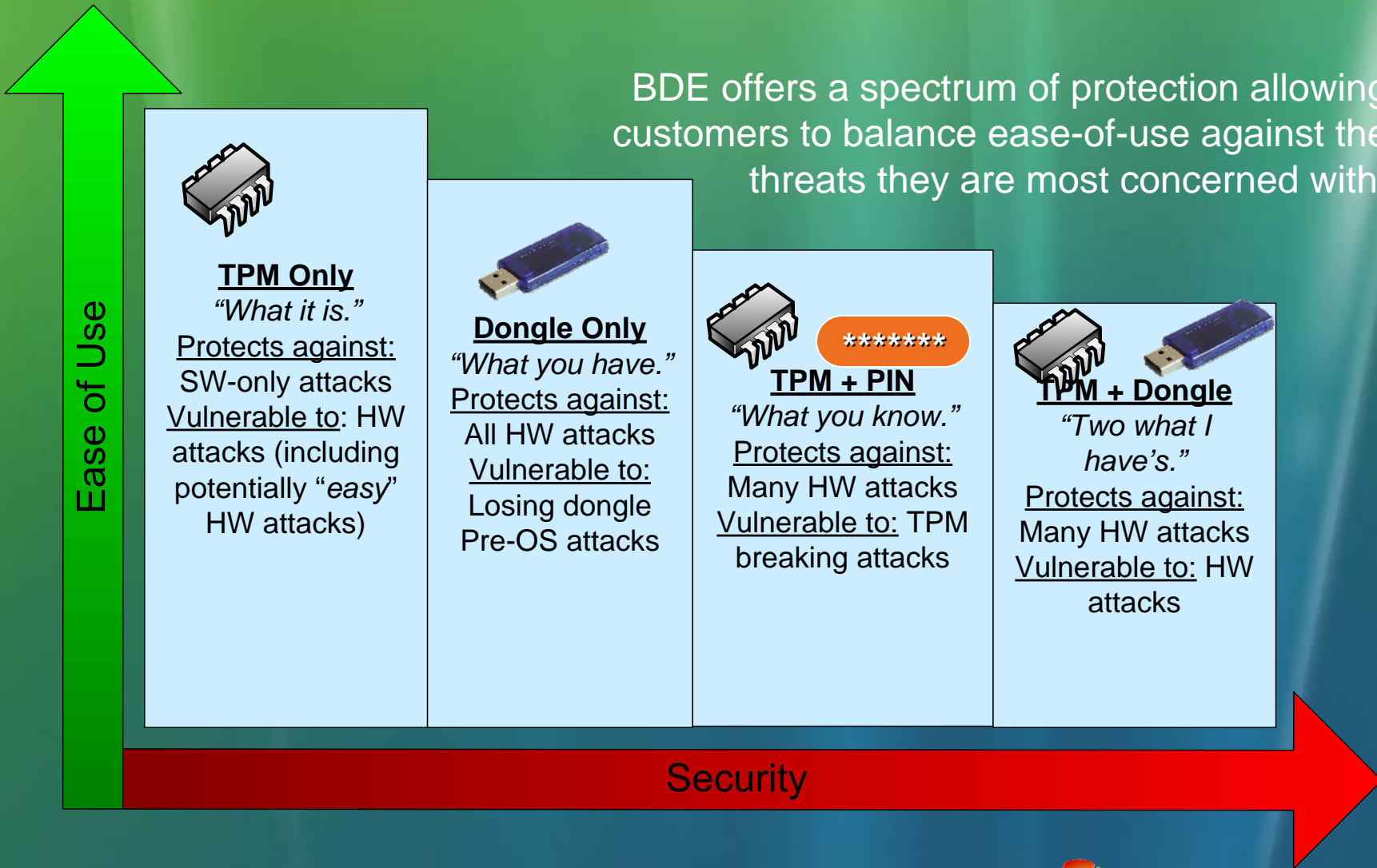
BitLocker™ Drive Encryption

- Designed specifically to prevent a thief who boots another Operating System or runs a hacking tool from breaking Windows file and system protections
- Provides data protection on your Windows client systems, even when the system is in unauthorized hands or is running a different or exploiting Operating System
- Uses a v1.2 TPM or USB flash drive for key storage



Spectrum Of Protection








BDE offers a spectrum of protection allowing customers to balance ease-of-use against the threats they are most concerned with.



Windows Vista Information Protection

Who are you protecting against?

- Other users or administrators on the machine? EFS
- Unauthorized users with physical access? BitLocker™

Scenarios	BitLocker	EFS	RMS
Laptops			
Branch office server			
Local <i>single-user</i> file & folder protection			
Local <i>multi-user</i> file & folder protection			
Remote file & folder protection			
Untrusted network admin			
Remote document policy enforcement			

Some cases can result in overlap. (e.g. Multi-user roaming laptops with untrusted network admins)

Recovery Options

- BitLocker™ setup will automatically escrow keys and passwords into AD
 - Centralized storage/management keys (EA SKU)
- Setup may also try (based on policy) to backup keys and passwords onto a USB dongle or to a file location
 - Default for non-domain-joined users
 - Exploring options for web service-based key escrow
- Recovery password known by the user/administrator
 - Recovery can occur “in the field”
 - Windows operation can continue as normal

Additional Data Protection

- EFS

- In Windows Vista, EFS supports storing user keys as well as administrative recovery keys on smart cards.
- EFS in Windows Vista can also be used to encrypt the system page file. The Client Side Cache, which stores offline copies of files from remote servers, can also be encrypted with EFS.
- A number of new Group Policy options have been added to help administrators define and implement organizational policies for EFS. These include the ability to require smart cards for EFS, enforce page file encryption, stipulate minimum key lengths for EFS, and enforce encryption of the user's Documents folder.

USB Device Control

- Windows Vista enables IT administrators to use Group Policy to manage or block the installation of unsupported or unauthorized devices. These policy settings can be applied individually on a single computer, or across large numbers of machines throughout the network.
- Administrators have a great deal of latitude in setting these policies — for example, they can allow installation of entire classes of devices (such as printers), disallow any kind of removable storage device, or disallow all unsupported or unauthorized devices.

DL1 Windows Vista Security Summary

Threat and Vulnerability Mitigation

- IE –protected mode/anti-phishing
- Windows Defender
- Bi-directional Firewall
- IPSEC improvements
- Network Access Protection (NAP)

Fundamentals

- SDL
- Service Hardening
- Code Scanning
- Default configuration
- Code Integrity

Identify and Access Control

- User Account Control
- Plug and Play Smartcards
- Simplified Logon architecture
- Bitlocker
- RMS Client



DL1

This sentence is incomplete in the section titled User Account Control:

Common tasks that require administrative privileges under Windows XP, such as installing printers, changing the time zone when traveling, changing power management settings, and adding a WEP key to connect to a secure wireless network.

Daney LaVigne, 2/18/2006



Q&A



Windows Vista™

© 2006 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



Microsoft®

Your potential. Our passion.™

© 2006 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

