

# Vista Security Overview

Presentation by:  
Miles Romello  
Information Security Manager  
CISSP, MCSE, MCDBA

# Introduction

## ■ BIO:

### Miles Romello, CISSP, MCSE, MCDBA

A trusted security professional with over 14 years of Systems Engineering and Security experience focusing on the Microsoft platform. In his experience he has been a successful architect securing infrastructures from small businesses to fortune 50 companies. These companies cover the government, services, energy, retail and financial industries. Currently he works as a Corporate Information Security Manager at a leading financial institution overseeing the team responsible for all Microsoft systems.

# Problem Statement

- **How quickly can you adopt VISTA in a corporate? And What makes it better?**
- **History**
  - **Windows XP Sp2 first wave of trusted computing initiative by Microsoft.**
  - **Typical usage of Windows incorrect**
    - **Users with Admin privileges, etc**
  - **Common issues with adopting single vendor dependencies.**

# Overview

- Why Vista?
  - Better Security
  - Better Integration
- Why Not?
  - Same Microsoft, Different OS
- Conclusion

# Better Security

## ■ User Account Controls (UAC)

- Reduces Malware infections
- Increases User frustration (misuse of OS)
- Reduction to call center workload???

## ■ Bit locker

- Requires TPM v 1.2
- Centralized through AD
- Self Service

## ■ Bi-Directional Firewall

# Better Security Cont'd

- **MS Defender Spyware Protection**
  - Centralized through AD and group policy
- **Network Access Protection (NAP)**
  - Interoperable with third party
- **MS Rights Management Services (RMS)**
  - Requires Active Directory and PKI infrastructure
- **Data Labeling**
  - Requires Vista and Windows 2008
  - In conjunction with System Center Operations Manager and RMS 07 it provides auditing and logging of sensitive data

# Better Integration

- Subsystems for UNIX applications
- Microsoft Desktop Optimization Pack (MDOP)
  - SoftGrid Technology (Application virtualization)
  - Group Policy Change Management (Formerly GPO Vault)
  - Desktop Error Monitoring (requires System Center 2007)
  - Asset Inventory Service (requires System Center 2007)
  - Microsoft Diagnostics and Recovery Tools (Formerly SystemInternals)

# Same Microsoft, Different OS

- Requires MDOP for many great features
- Requires Enterprise over Business for MDOP
- Already low level security flaws found
- MDOP additional cost
- Some components are not available independent of MDOP

# Closing

- What does it all mean?
  - While many are skeptical about moving to Vista. It is a product that will revolutionize desktops and enterprise collaboration.
  - Vista will cause a shift in paradigm. Many users will not adapt easy.
  - Executives will be nervous about bringing in full functionality of Vista.
- What can you do?
  - Use caution
  - Be optimistic and
  - **Test, test , test.**



Q&A