

# The Future of Malicious Code

Neil MacDonald



Midsized Enterprise  
Summit. 2007



# Key Issues

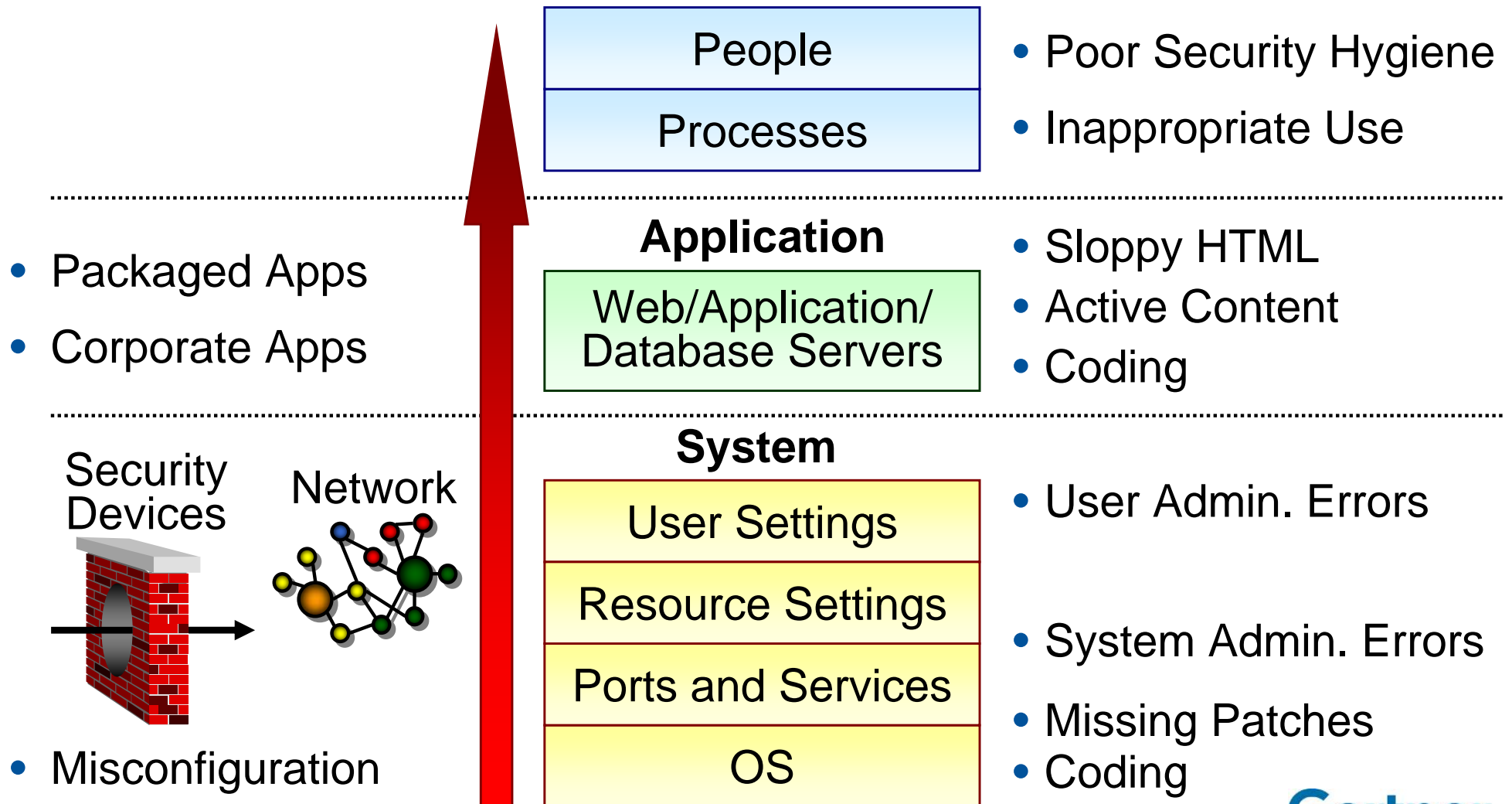
1. How will the changing threat environment render traditional protection mechanisms obsolete?
2. How will other styles of protection on the endpoint evolve?
3. How will Microsoft impact your security spending?

# Key Issues

1. How will the changing threat environment render traditional protection mechanisms obsolete?
2. How will other styles of protection on the endpoint evolve?
3. How will Microsoft impact your security spending?

# The Motivations of Hackers Are Changing and Attacks Are Moving 'Up the Stack'

**Vulnerability:** A weakness in process, administration or technology that can be exploited to compromise IT security.



## Strategic Planning Assumption

By 2010, financially motivated Internet-based attacks will represent 70% of total incidents and will represent 80% of the incident costs incurred by enterprises (0.6 probability).

# Existing Antivirus Security Technology Is Fundamentally Flawed

**It can't stop what it doesn't know is a threat.**



## Signature-based techniques (such as AV)

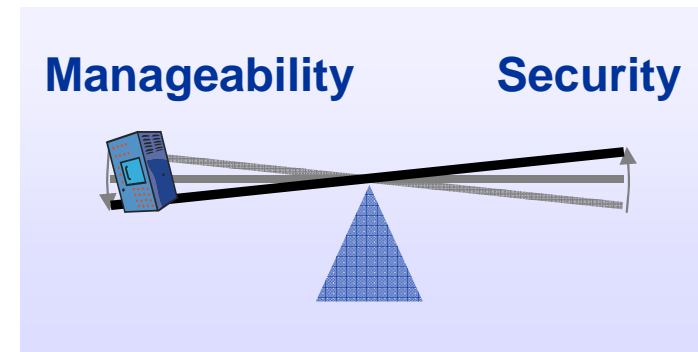
- Are based on enough people being hit somewhere so that a signature is developed
- This model breaks down for targeted and zero-day attacks
- Is reactive, not proactive
- Signature-based models also break down when overloaded by variants
- New variants appear before signatures can be created for the previous variant
- Removal is getting difficult, especially rootkits
- Automated "malware delivery systems"
- Check out [www.metasploit.org](http://www.metasploit.org)

# Traditional Port-Based Personal Firewalls Help, but Also Have Limitations

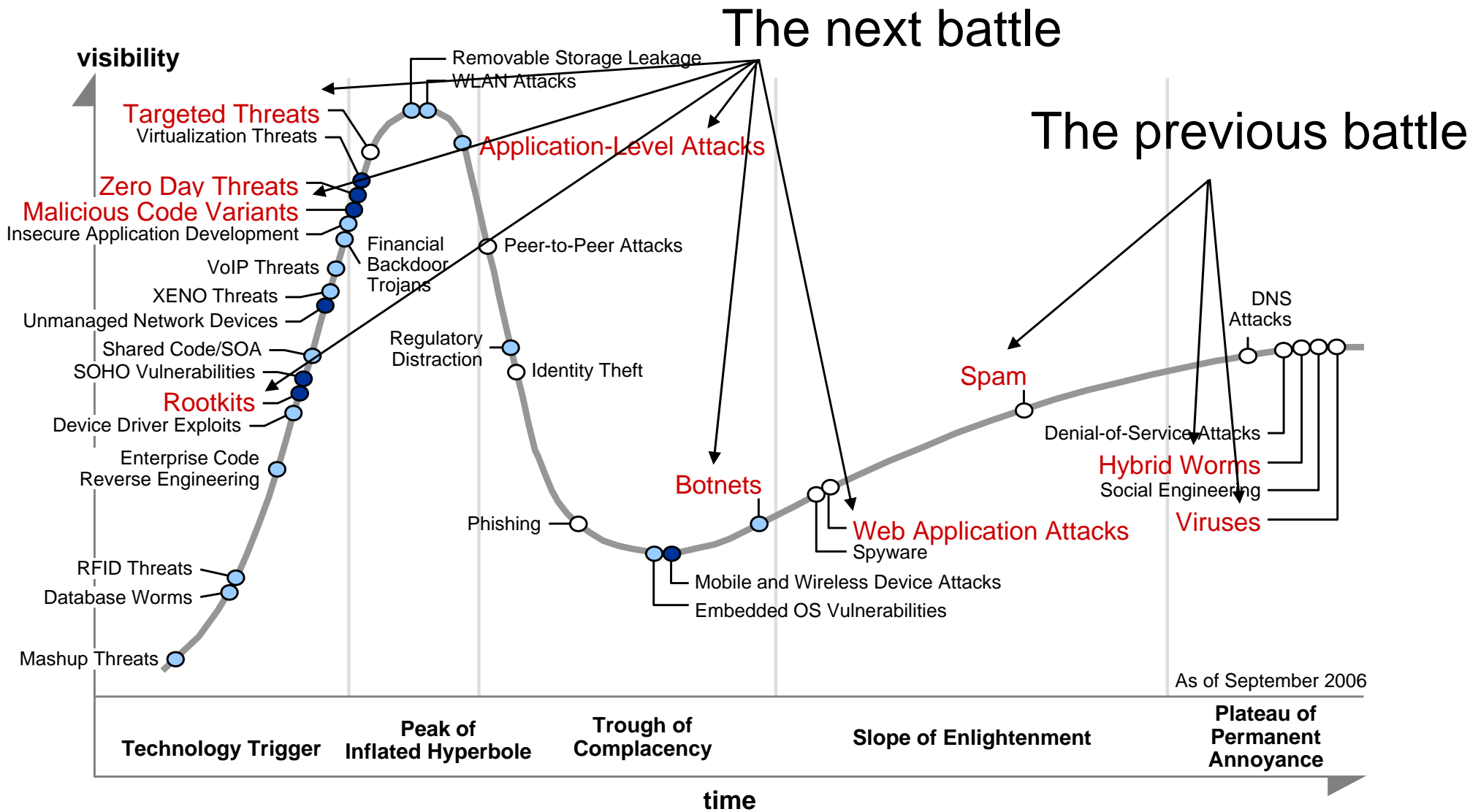
## Security/Manageability Trade-off

### Rules-based techniques (like firewalls)

- Provide some protection, but the bad guys figure out how to do bad things within the allowable rules
  - For example, attacks on Microsoft's RPC protocol where the ports are typically open
- Create a fundamental trade-off between manageability and security, leaving bigger holes for hackers
  - More "lockdown" creates more rules to maintain
  - More "lockdown" makes things harder to change
  - The average user/consumer doesn't know the "right" rules versus the "wrong" rules
- Windows Vista helps, but is only a partial solution



# Gartner 2006 Information Security Threats Hype Cycle



**Years to mainstream adoption:**

○ less than 2 years

● 2 to 5 years

● 5 to 10 years

▲ more than 10 years

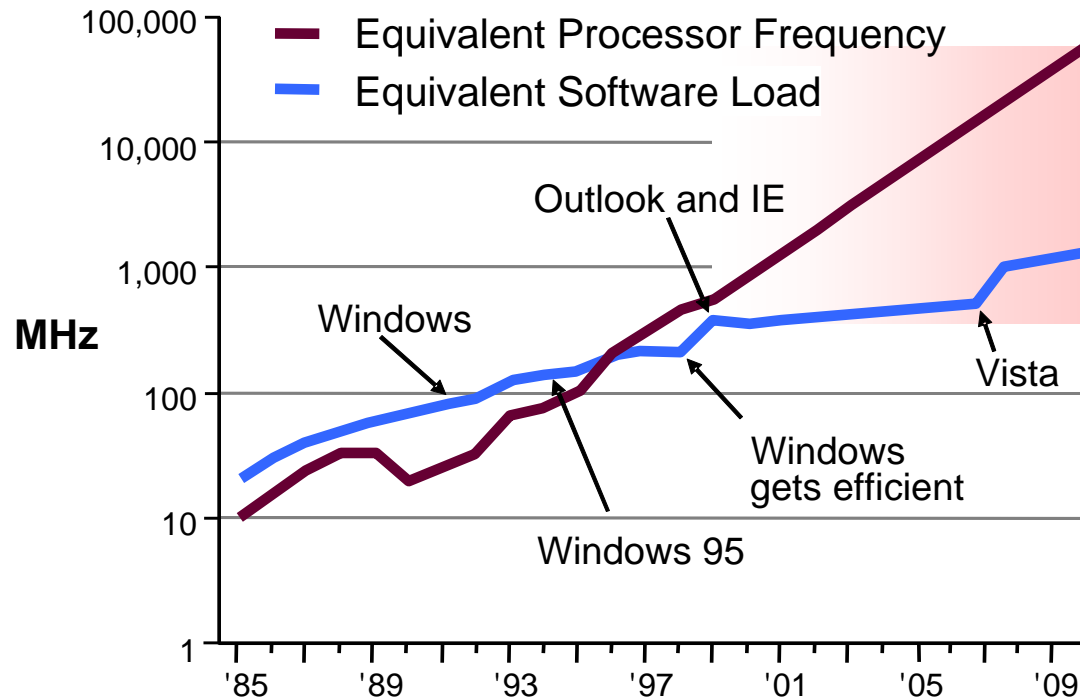
⊗ obsolete  
before plateau

# Strategic Planning Assumption

By the end of 2007, 75% of enterprises will be infected with undetected, financially motivated, targeted malware that evaded their traditional perimeter and host defenses.

# Good News: More Horsepower for Security Protection Stuff at the Endpoints

## Moore's Law — set to hold true through 2016



### New Opportunities

- Faster encryption
- Less intrusive security tools and backup procedures

### New Challenges

- Makes existing encryption algorithms easier to break
- Disks get bigger too — cheaper to store files than decide what to delete
- More performance for hackers

### As performance and capacity go up, balance points move:

- How much and how strongly do you need to encrypt?
- Is deep packet inspection on endpoints a possibility?
- Is behavioral monitoring of endpoints a possibility?

# Key Issues

1. How will the changing threat environment render traditional protection mechanisms obsolete?
2. How will other styles of protection on the endpoint evolve?
3. How will Microsoft impact your security spending?

# Converging End-Node Protection Technologies

AV & Spyware  
Personal Firewall  
HIPS

**Security**

Inventory  
Vulnerability  
Configuration  
Application  
NAC

**Operations**

Data leak prevention  
Encryption



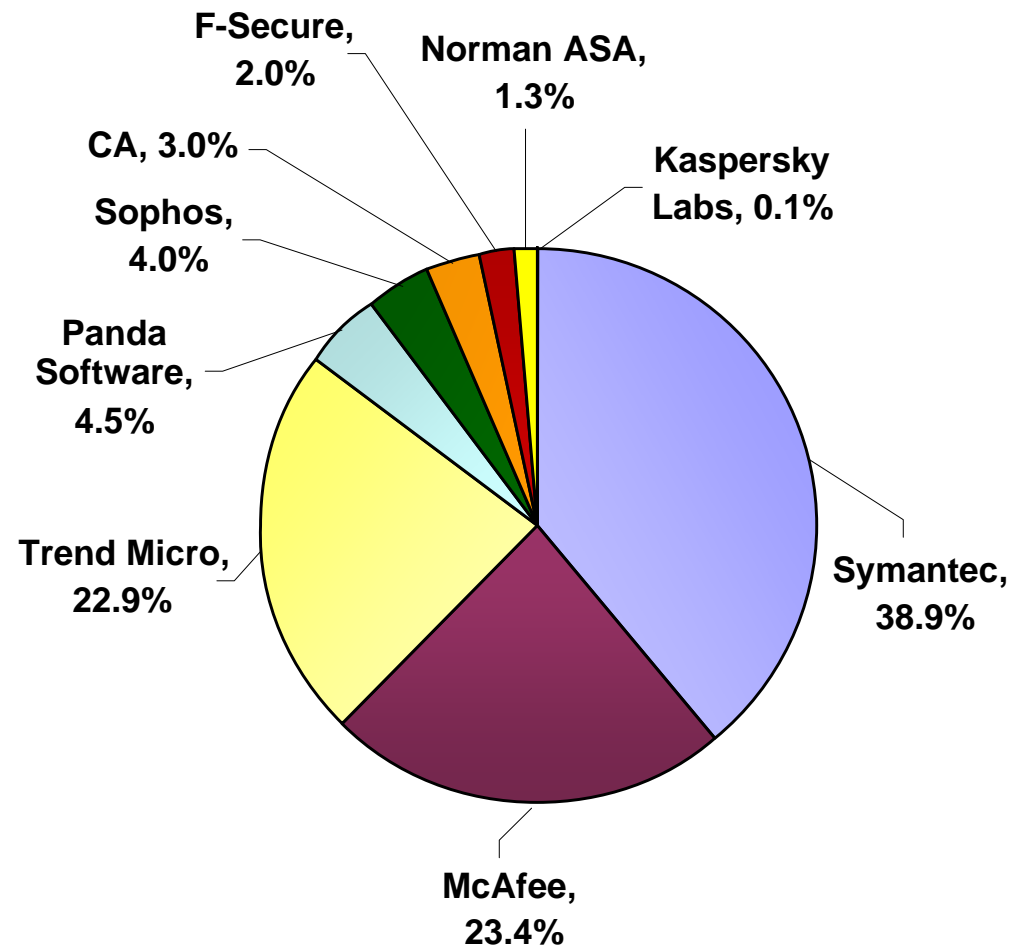
## Strategic Planning Assumption

The market for stand-alone, signature-based AV products for business and consumers will be reduced by more than 80% by YE08 (0.8 probability). The market for stand-alone anti-spyware products for business and consumers will be reduced by more than 90% by YE08 (0.8 probability).

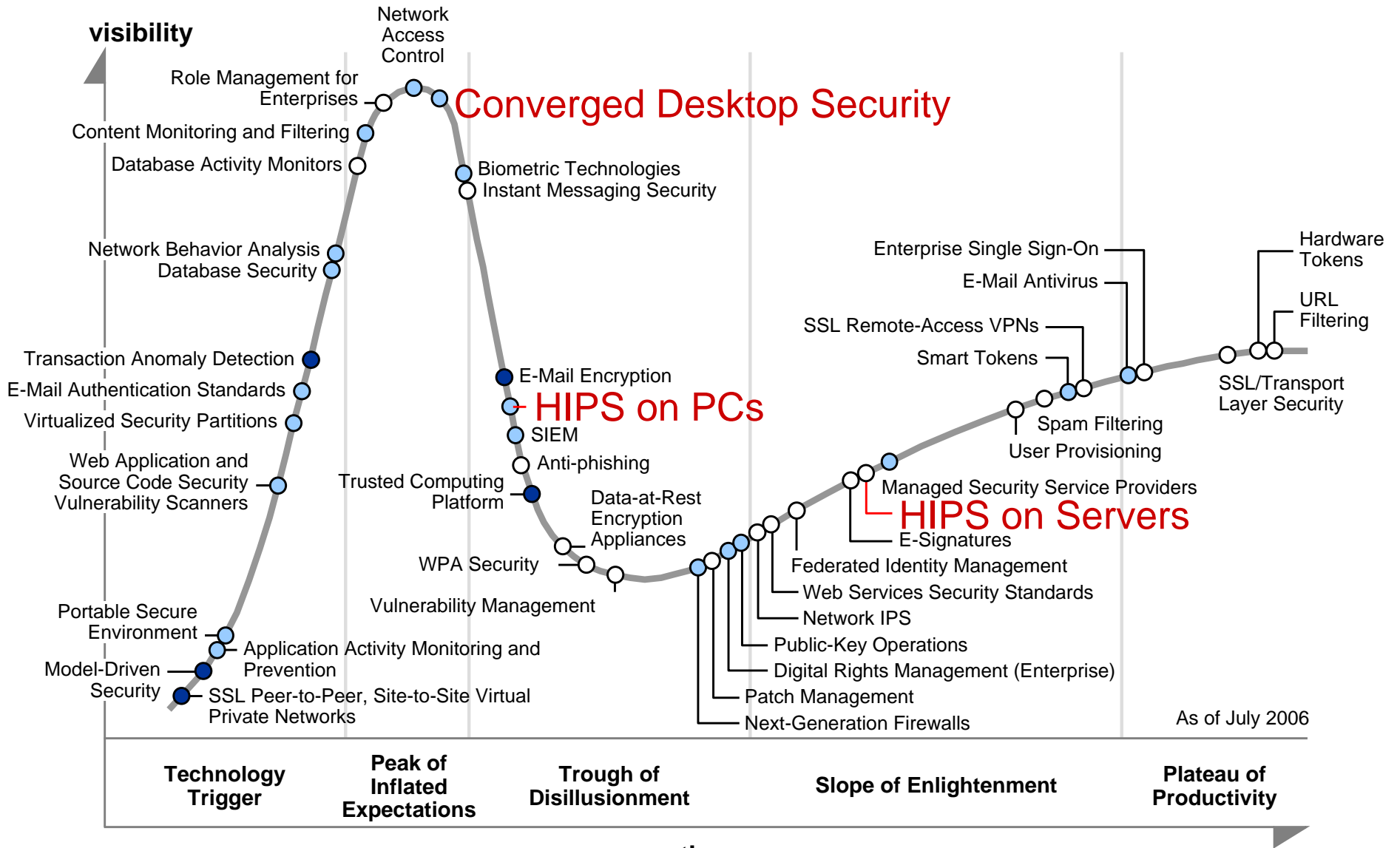
# AV Marketplace — Changes Ahead, but the Big Three Still Dominate

- Symantec — Busy with acquisitions
  - Sygate and Whole best of breed
  - Integration challenges
- McAfee — Good focus
  - Strong IPS
  - New policy enforcement
  - Vulnerability detection, Foundstone
- Trend Micro — Converging slowly
  - Intermute anti-spyware
- Sophos, F-Secure, Panda — OEM, SMB and consumer
- Microsoft enters the consumer market

## Global Enterprise Market Share



# Gartner 2006 Information Security Technology Hype Cycle



Years to mainstream adoption:

○ less than 2 years

◐ 2 to 5 years

● 5 to 10 years

▲ more than 10 years

⊗ obsolete before plateau

# Host-Based Intrusion Prevention: One Term, Many Meanings

	<b>Allow Known Good</b> (Block All Else)	<b>Block Known Bad</b> (Allow All Else)	<b>Unknown</b>
<b>Execution-Level</b>	7 Application Control	8 Resource Shielding	9 Behavioral Containment  Passive → Active
<b>Application-Level</b>	4 Application and System Hardening	5 Antivirus	6 Application Inspection
<b>Network-Level</b>	1 Personal Firewall	2 Attack-Facing Network Inspection	3 Vulnerability-Facing Network Inspection

# Mapping HIPS Vendors and Solutions to the Gartner HIPS Nine-Style Framework

## Lead with "behavioral" enforcement capabilities:

- Cisco CSA
- Sana Security
- Determina Memory Firewall
- GreenBorder
- Prevx Pinnacle
- Windows NX and Services Hardening
- Symantec Critical System Protection
- Symantec WholeSecurity

## Lead with AV capabilities:

- Symantec "Hamlet"
- McAfee 8.5i and Total Protection
- Sophos w/ Genotyping
- Panda TruPrevent
- CA eTrust Client Security

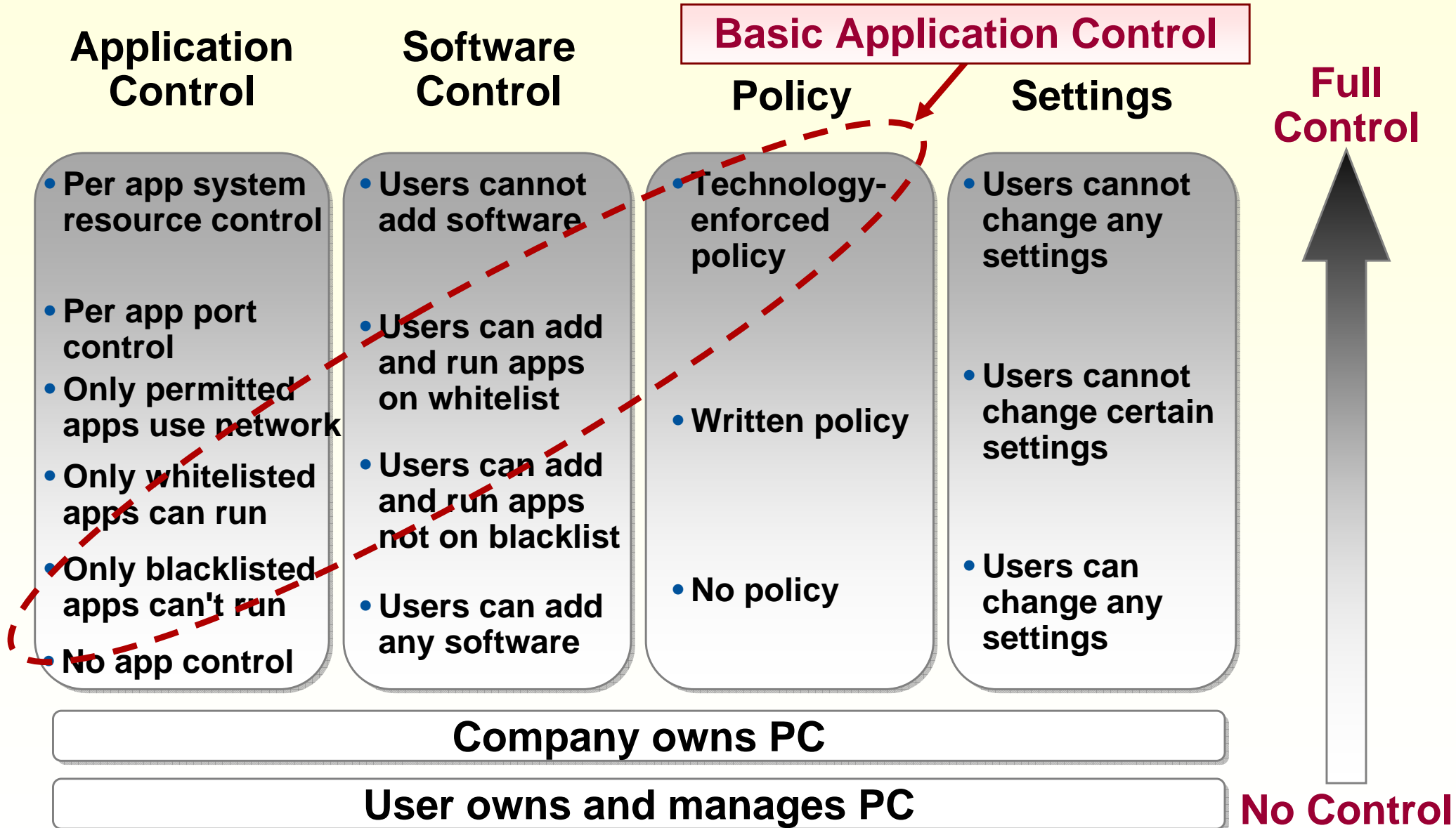
## Lead with deep-packet inspection firewall capabilities:

- eEye Blink
- ISS Proventia
- Check Point Integrity
- Third Brigade
- Symantec Sygate
- NETASQ NetASQ Shield

MES

"suite spot"

# Windows Application Control Solutions: An Alternative to Desktop Lockdown

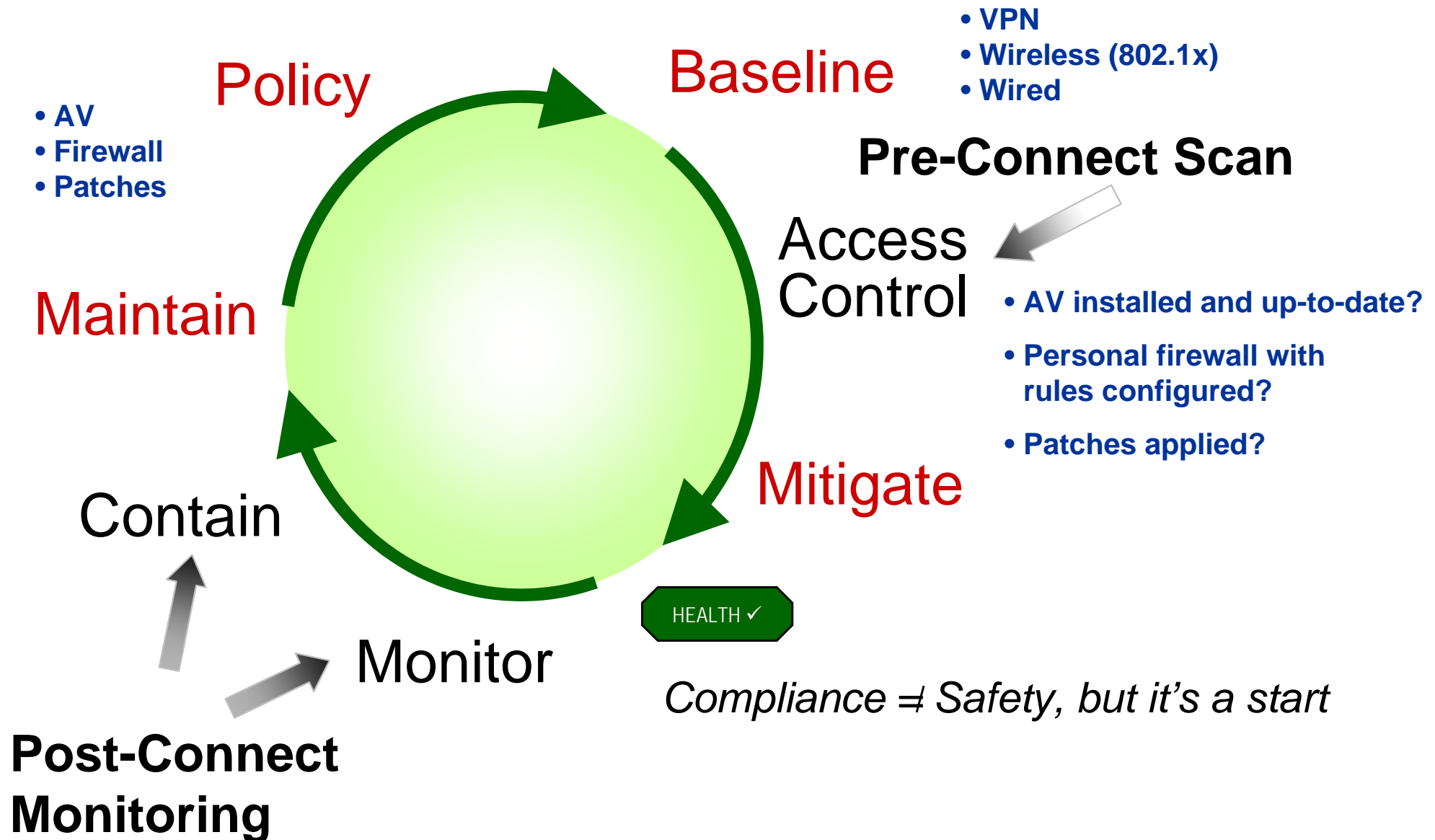


# Full Disk Encryption

- Emerging focus on data protection
- Encryption Mandatory for mobile devices
- Full Disk Encryption attractive
- Overlap with Firewall capabilities
- Vista Bit Locker — 2009
- Common management
- Desktop presence
- Operational impact



# Network Access Control: Minimum Device Compliance at Connect; Ongoing Monitoring



# Key Issues

1. How will the changing threat environment render traditional protection mechanisms obsolete?
2. How will other styles of protection on the endpoint evolve?
- 3. How will Microsoft impact your security spending?**

# Windows Vista: Why You Should and Shouldn't Care (From a Security Perspective)

- **Why You Should Care:**

- Integrated Search
- User Account Control (UAC)
- IE 7 running in "protected mode"
- Bidirectional personal firewall
- Video drivers in user mode

- **Why You Shouldn't Care:**

- Good desktop search products today. Metadata problem gets worse before it gets better.
- Doesn't solve the political problems and isn't a complete solution.
- IE gets better. Upgrade now on XP SP2.
- You probably have a more-capable solution on laptops. Not managed by Microsoft Forefront. Really needs deep-packet inspection capabilities.
- Didn't we just put these in kernel mode? Watch out for driver compatibility.



# Strategic Planning Assumption

Thirty percent of Windows XP enterprises will choose to skip Windows Vista entirely (0.7 probability).

# Windows Vista: Why You Should and Shouldn't Care (From a Security Perspective)

- **Why You Should Care:**

- Windows Services Hardening (WSH)
- BitLocker (Full Volume Encryption)
- USB Device Control
- Windows Defender
- Integrated Network Access Protection Client



- **Why You Shouldn't Care:**

- Okena five years later. What about applications?
- Requires Software Assurance. Third-party products available today. TPM 1.2 and BIOS-equipped machines are hard to find.
- Good, but yet more GPOs to manage. Needs more granularity. What about other paths to/from machine?
- The EU cares. Seriously, free anti-spyware is a good thing. Want AV? Want enterprise manageability? Purchase Forefront Client Security.

## Strategic Planning Assumption

Windows Vista will not reach a 10% installed base in large enterprises until at least 24 months after it ships (0.7 probability). Windows Vista and subsequent releases will not reach a 50% installed base in large enterprises until at least 2011 (0.7 probability).

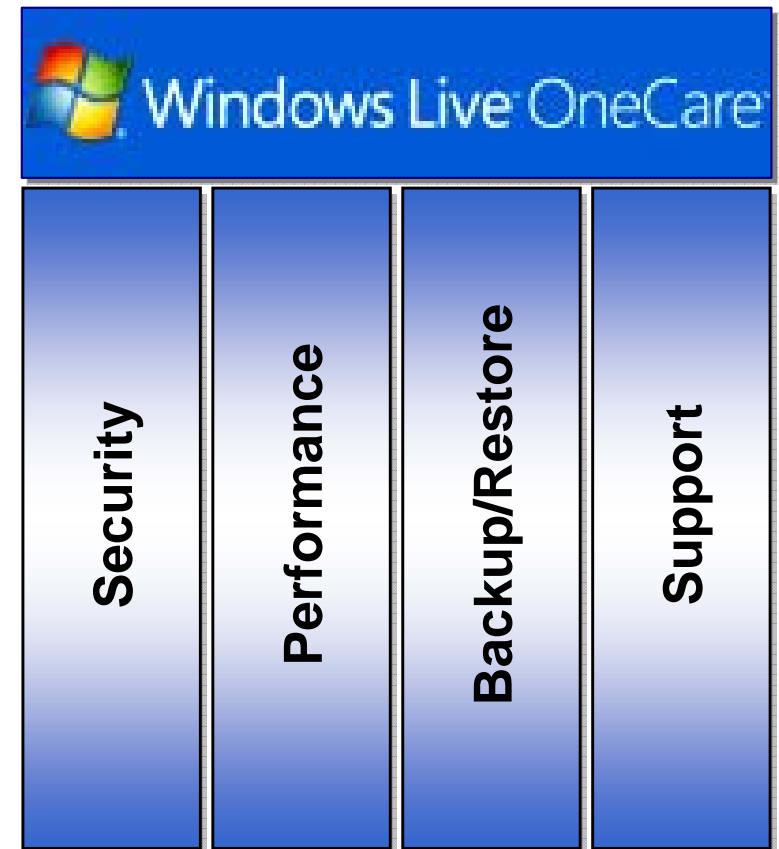
# Security as a Service (Software and Service): Microsoft Windows Live OneCare

## Strengths:

- Defining a new market — the problem is not just security
- Most consumers go without active security protection
- Aggressive pricing

## Weaknesses:

- North America only initially
- Locally attached network storage only
- Multimachine management
- Where does OS support stop and hardware support start?



# Navigating Vendor Pricing Games

- Start early and negotiate with multiple vendors
- Get perpetual licenses
- Get extras
  - Premium support, deployment assistance, training, home users, etc.
- Demand anti-spyware
- License desktop and e-mail by seats and servers by CPU, or get enterprise licenses
- Don't increase seat count to match price list
- You only get to negotiate a perpetual license once
  - Pen in renewal caps
  - Negotiate functionality replacement clauses

**AV Companies Have a Healthy 60% Gross Profit Margin**

# Recommendations

- ✓ Traditional AV and personal firewall protection are no longer sufficient for endpoint protection. Demand non-signature-based protections.
- ✓ There is no security "silver bullet"
  - No single protection style alone provides sufficient protection.
  - Each style has its strengths and weaknesses.
  - Different organizations have different needs
  - Start HIPS deployments slow and grow
- ✓ Desktop encryption should be considered mandatory.
- ✓ Convergence means you shouldn't have to pay extra for each of the nine styles of protection. Demand more from your incumbent AV provider. Pay the same, get more!
- ✓ If you are a larger enterprise, Microsoft's entry into the security market offers an immediate opportunity to negotiate better pricing with your incumbent providers.
- ✓ Push vendors and be open to change. Watch operational upstarts (Microsoft, LANDesk, BigFix, Checkpoint)

# The Future of Malicious Code

Neil MacDonald



Midsized Enterprise  
Summit. 2007



# The Future of Malicious Code

Neil MacDonald



Midsized Enterprise  
Summit. 2007

