

# Host-Based Intrusion Prevention Systems (HIPS) Update: Why Antivirus and Personal Firewall Technologies Aren't Enough

Neil MacDonald  
25 January 2007

# Existing Antivirus Security Technology Is Fundamentally Flawed

# 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
- The model is reactive, not proactive

# Existing Antivirus Security Technology Is Fundamentally Flawed

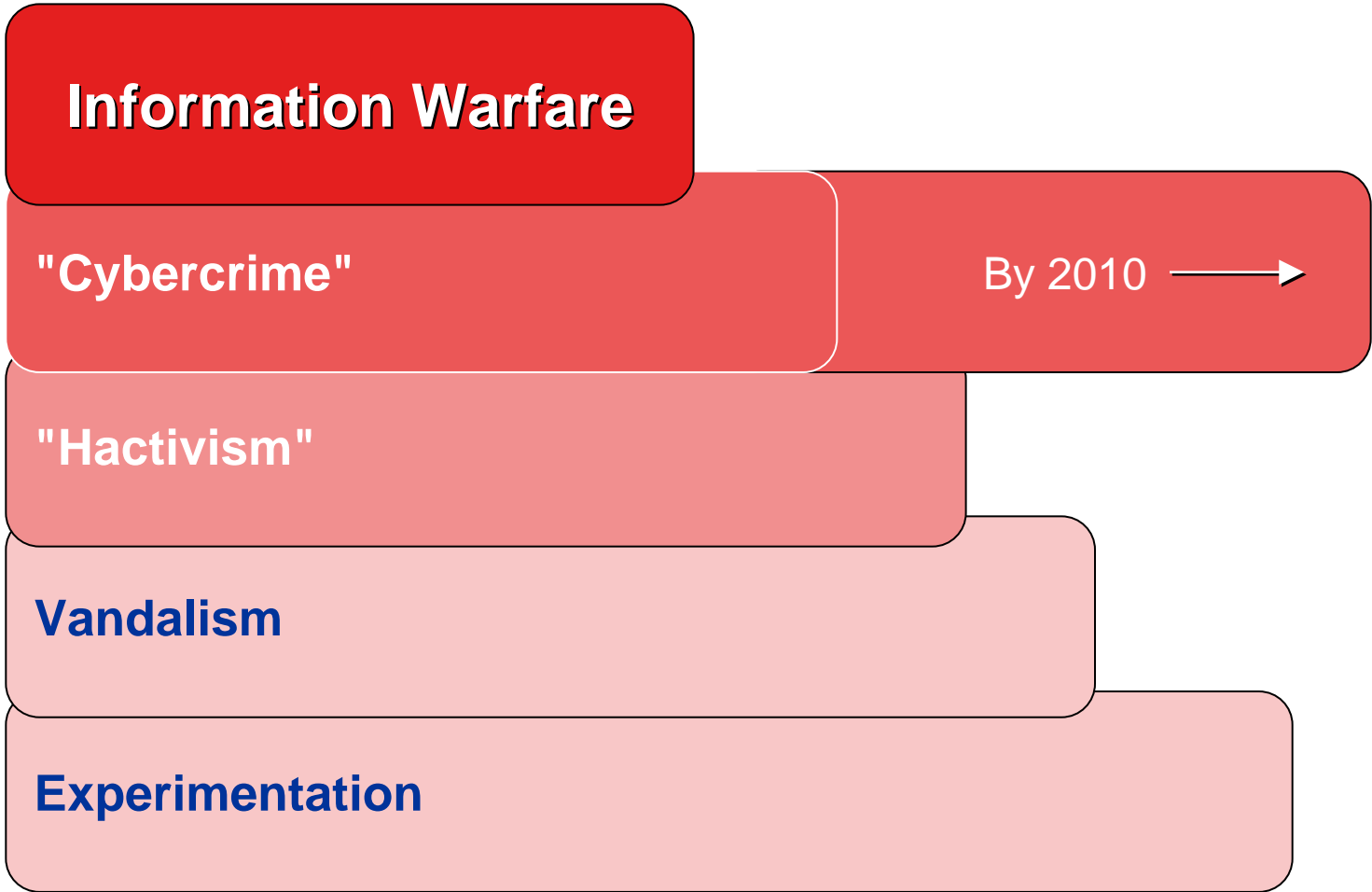
## It can't stop what it doesn't know is a threat.

### 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
- The model 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
- Automated "malware delivery systems"
- Check out [www.metasploit.org](http://www.metasploit.org)

# The Motivations of Hackers Are Changing

Impact



Frequency

Gartner

# Security in the News: Custom Trojans

**28 May 2005**

- Two people arrested, 21 people detained
- Custom Trojan
- Industrial Espionage
  - Television station
  - Automobile importer
  - Utilities
- Undetected for 18 to 24 months
- Tens of thousands of pilfered documents recovered
- In a part of the world that is extremely aware of security threats ...

# Security in the News: The New York Times

**7 January 2007**

**"Attack of the Zombie Computers Is a Growing Threat, Experts Say"**

- **Rise in BotNets**
- **Windows Rootkits — undetectable by traditional techniques**

# Firewalls Help, but also Have Limitations

## Security/Manageability Trade-off

### Rule-based techniques (such as 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 more difficult to change
  - The average user/consumer doesn't know the "right" rules vs. the "wrong" rules

# Windows Vista Helps, but More Is Needed

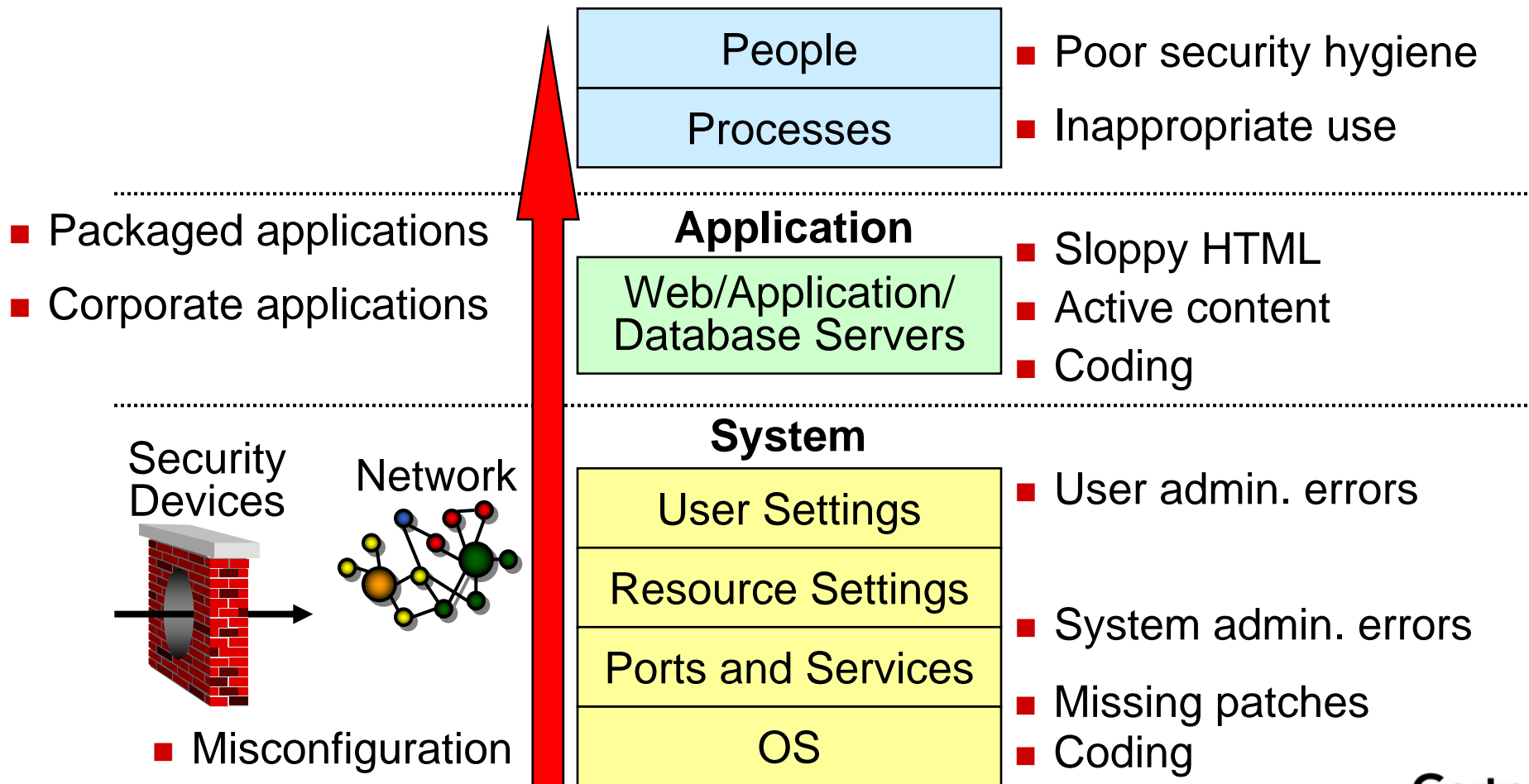
## The Windows Vista Effect

Free bidirectional personal firewall and anti-spyware ... but

- No antivirus
- Limited zero-day or targeted attack protection
- Even with User Account Control, standard users can still install and run arbitrary software
- Most enterprise users (and consumers) still run as administrator
- Some of the features (e.g., BitLocker) are only available to subscribers of Software Assurance

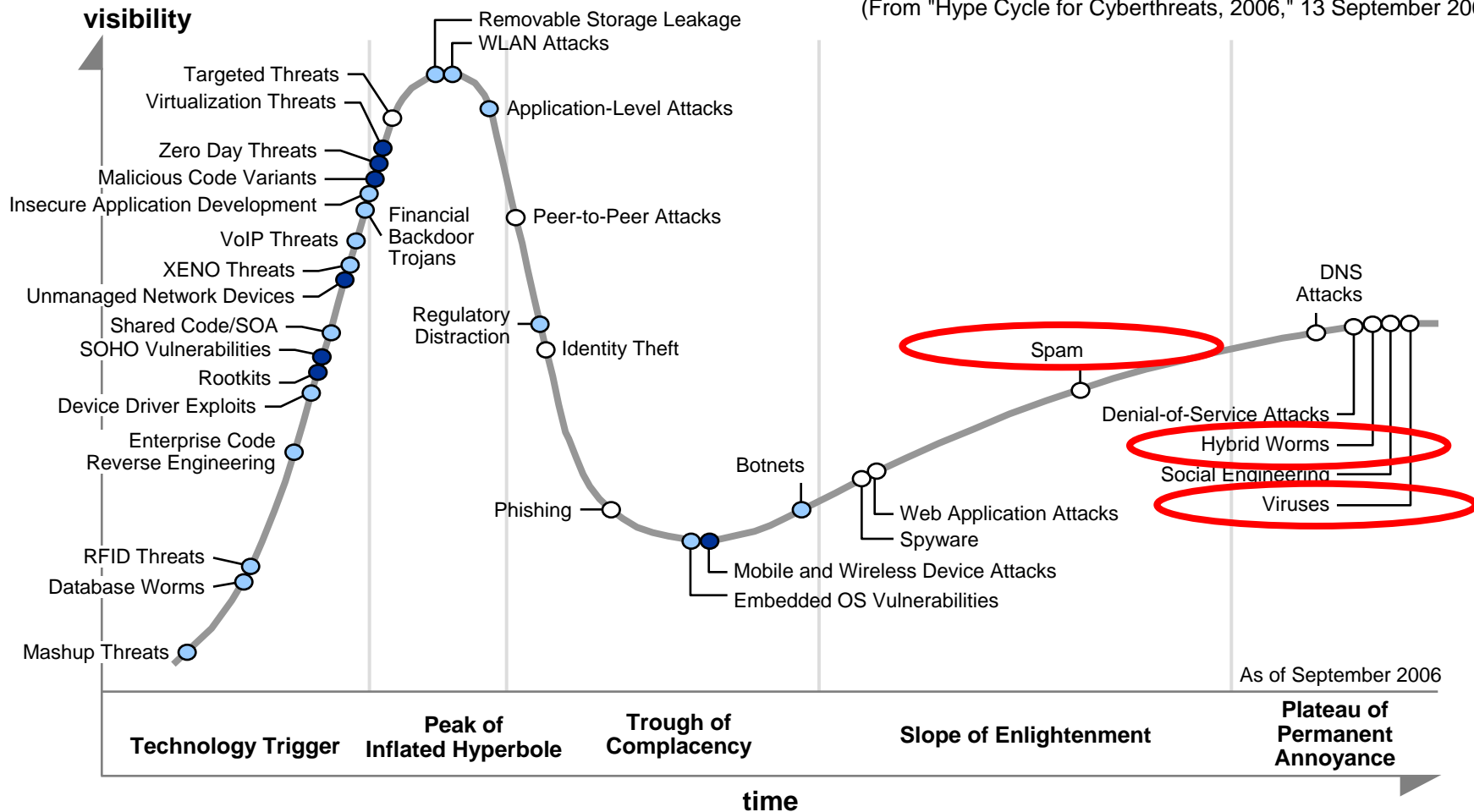
# Attacks Are Moving 'Up the Stack'

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



# Gartner 2006 Information Security Threats Hype Cycle

(From "Hype Cycle for Cyberthreats, 2006," 13 September 2006)



As of September 2006

Years to mainstream adoption:

○ less than 2 years

● 2 to 5 years

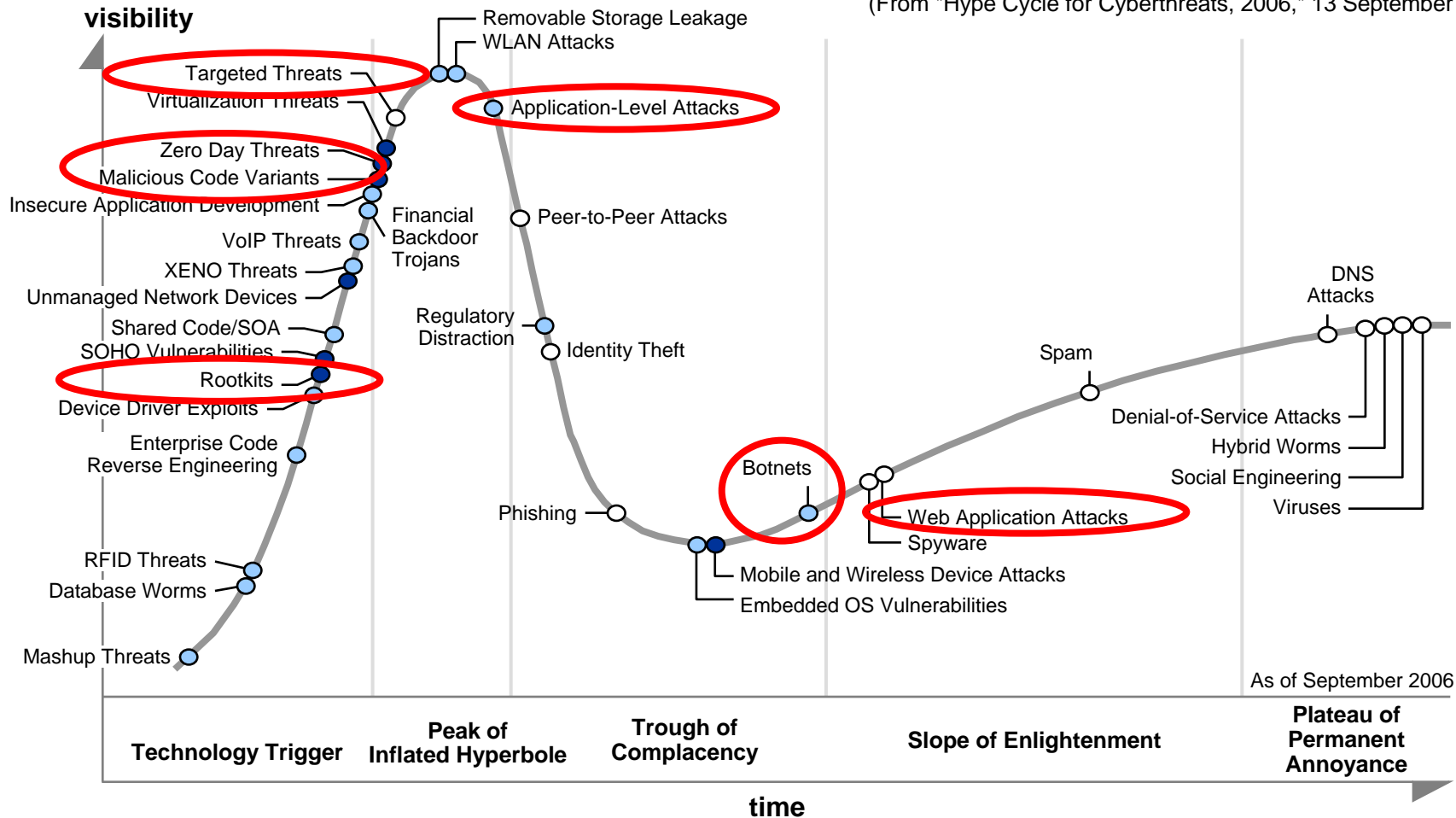
● 5 to 10 years

▲ more than 10 years

○ obsolete  
⊗ before plateau

# Gartner 2006 Information Security Threats Hype Cycle

(From "Hype Cycle for Cyberthreats, 2006," 13 September 2006)



Years to mainstream adoption:

○ less than 2 years

● 2 to 5 years

● 5 to 10 years

▲ more than 10 years

⊗ obsolete before plateau

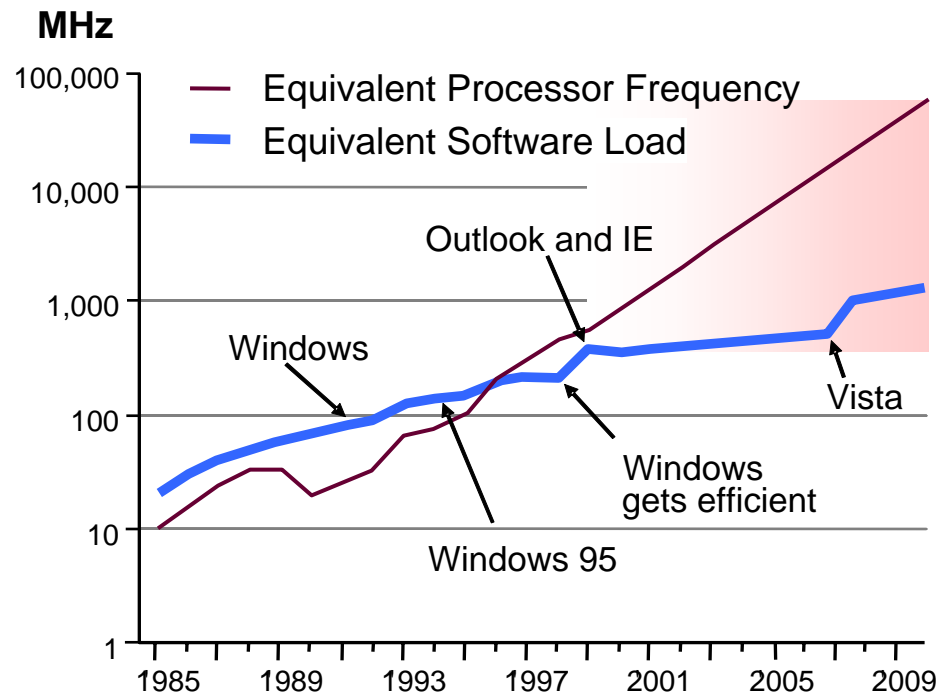
# Creating Millions of Unaware Users at Risk: Enterprises and Consumers

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).

By year-end 2007, 75% of enterprises will be infected with undetected, financially motivated, targeted malware that evaded their traditional perimeter and host defenses (0.6 probability).

# Good News: More Horsepower for Security Protection 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:

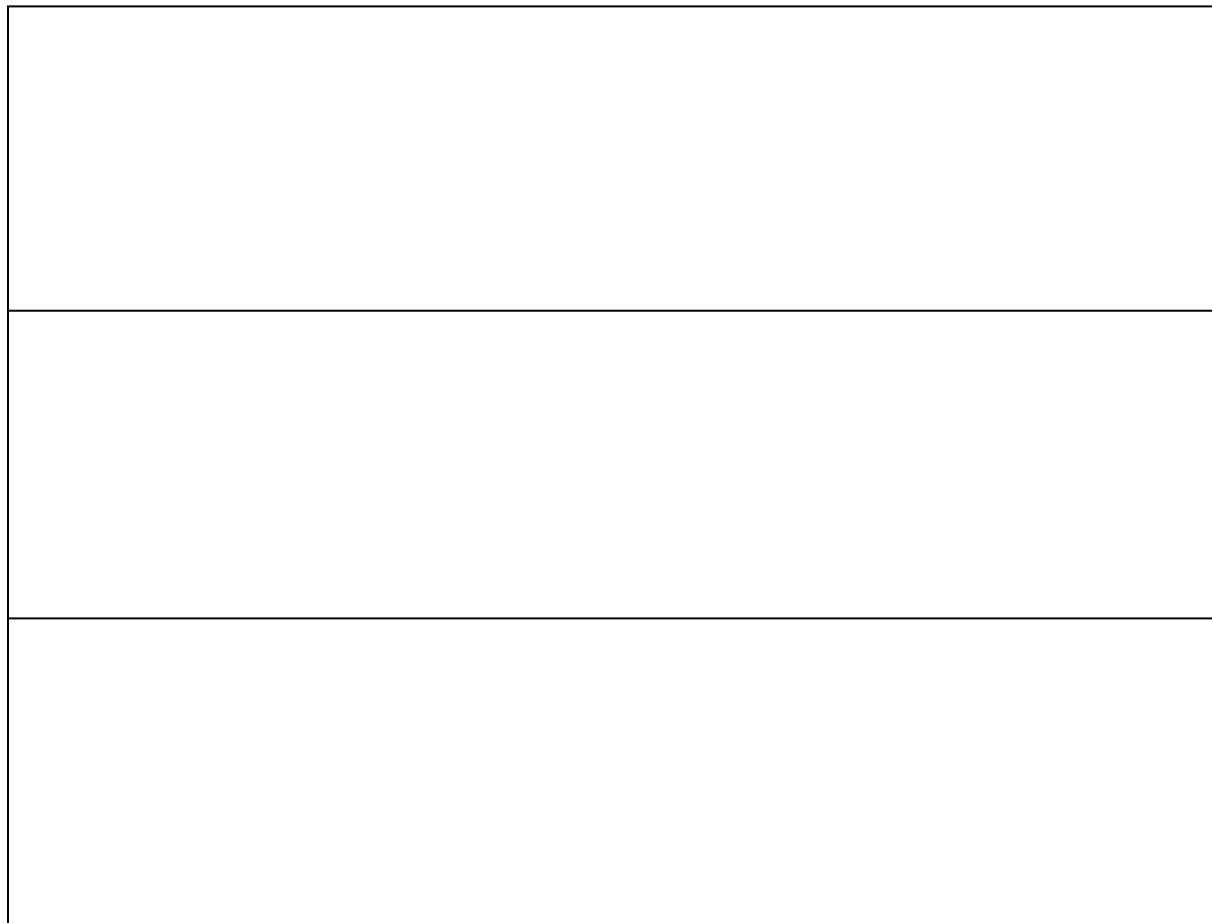
- How much and how strongly do you need to encrypt?
- Is deep-packet inspection on endpoints a possibility?
- Is behavioral monitoring of endpoints a possibility?

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

**Execution  
Level**

**Application  
Level**

**Network  
Level**



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

	<b>Allow Known</b> <b>Good</b> (Block All Else)	<b>Block Known</b> <b>Bad</b> (Allow All Else)	<b>Unknown</b>
<b>Execution Level</b>			
<b>Application Level</b>			
<b>Network Level</b>			

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

	<b>Allow Known Good (Block All Else)</b>	<b>Block Known Bad (Allow All Else)</b>	<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

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

	<b>Allow Known</b> <b>Good</b> (Block All Else)	<b>Block Known</b> <b>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 Host Firewall	2 Attack-Facing Network Inspection	3 Vulnerability-Facing Network Inspection

# Third Brigade

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

# eEye Digital Security's Blink

	<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 Host Firewall	2 Attack-Facing Network Inspection	3 Vulnerability-Facing Network Inspection

# Check Point Integrity

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

# ISS Proventia Desktop

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

# Cisco Security Agent

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

# Sana Security

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

# Symantec Client Security

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

Passive → Active

# Symantec Client Security + Symantec Critical System Protection

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

# Symantec Client Security + Symantec Critical System Protection + Sygate

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

# Symantec Client Security + Symantec Critical System Protection + Sygate + Whole Security

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

# McAfee VirusScan Enterprise 8.0i

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

Passive → Active

# McAfee HIPS

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

# McAfee Total Protection (8.0i + HIPS + Full Anti-spyware + NAC)

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

# Panda TruPrevent

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

# SolidCore for System Hardening

## V.i.Laboratories for Application Hardening

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

# Determina Memory Firewall + Determina Vulnerability Protection System

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

# HIPS Myths and Realities

- Myth

All HIPS solutions prevent intrusions and remove the malicious software.

- Reality

Some do. Some don't.

# HIPS Myths and Realities

- Myth

HIPS solutions require too much administrative overhead to install and maintain.

- Reality

If HIPS are implemented following best practices, administrative time does not have to be high. In most failed cases we have seen, organizations try to control applications too tightly.

# HIPS Myths and Realities

- Myth

HIPS solutions create too many false positives to be considered on production systems.

- Reality

The risk of false positives is higher in some HIPS styles than others, especially those styles in the third column that use heuristics, learning and models to determine whether behavior is good or bad.

# HIPS Myths and Realities

- Myth

HIPS solutions incur too much of a performance hit or are too unstable for production systems.

- Reality

Although some HIPS can kill performance if the system is already overloaded, others have modest impact. The most processor-intensive HIPS solutions perform deep-packet inspection (DPI) on the incoming network traffic stream.

# HIPS Myths and Realities

- Myth

All HIPS will provide proactive protection (shielding) from attacks on known vulnerabilities.

- Reality

Although this capability is a primary operational driver of HIPS purchases, not all HIPS solutions do this well. This type of vulnerability-facing protection is typically provided in HIPS solutions that provide DPI.

# HIPS Myths and Realities

- Myth

All HIPS products will provide zero-day protection from attacks on previously unknown vulnerabilities.

- Reality

Execution-level HIPS solutions are best-suited to protect against attacks on unknown vulnerabilities. Nothing catches all zero-day attacks, but buffer overflow protection protects against a large percentage of malicious code.

# HIPS Myths and Realities

- Myth

HIPS solutions are only suitable for servers.

- Reality

HIPS solutions on servers are more mature, but desktop solutions are now viable.

# HIPS Myths and Realities

- Myth

I will have to purchase and install an additional HIPS agent(s) on all my machines.

- Reality

Vendors want this, but ...

- OS vendors are providing more
- AV vendors are providing more
- Think "convergence"

# HIPS Myths and Realities

- Myth

I have network-based IPS so I don't need host-based IPS.

- Reality

Organizations need both.

- Mobile workstations
- Encrypted traffic
- Alternative entry points (wireless, Universal Serial Bus, compact disc)

# HIPS Best Practices

Plan

Longer-term  
Considerations



Evaluate

Deploy and  
Operate

# HIPS Best Practices: Planning

- **Prioritize: What's the problem you are trying to solve?**

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

# HIPS Best Practices: Planning

- Combine multiple styles of protection
  - Balance strengths and cautions
  - Balance false positives and false negatives
- Match the HIPS deployment plan to the organization's computing environment
  - Start with critical servers
  - Then move on to controlled desktops
  - Desktops where users run as administrators should minimize rules
  - Design to minimize administration overhead

# HIPS Best Practices: Planning

- Consider buffer overflow protection a "must have"
- Consider DPI with vulnerability-facing filters a "should have"
- Don't overlook the protection of embedded or older systems
- Consider leveraging what the organization's incumbent OS, antivirus or personal firewall vendor provides for "free"
- Plan for modification of IT operations processes

# HIPS Best Practices: Evaluating Solutions

- Plan and test for potential application denial of service
- Test malicious-code removal capabilities
- Test for tamper resistance
- Test the mechanism for signature, rule and engine updates
- Clarify what the yearly subscription fee provides
- Enter into short-term contracts only
- Desktop operation experience with a platform should be weighted accordingly

# HIPS Best Practices: Deploy and Operate

- Balance security and manageability
- Activate vulnerability-facing signatures
- Modify IT operation processes for HIPS
  - Testing signature, rule and engine updates
  - Testing updates from the OS vendor
  - Updating configuration for new or modified applications
- Ensure HIPS software is still running and up-to-date

# HIPS Best Practices: Longer Term

- Leverage convergence. Monitor what your AV and OS provider deliver for "free"
- Plan for network-based IPS and HIPS
- Look for emerging solutions that share information between network-based IPS and HIPS solutions
- Look for HIPS solutions that are able to link new applications to security protection
  - Automatic rules configuration
  - IBM? Microsoft?

# Recommendations

- ✓ **Traditional AV and personal firewall protection are no longer sufficient for endpoint protection.**
- ✓ **There is no security "silver bullet."**
  - No single protection style alone provides sufficient protection.
  - Each style has its strengths and cautions.
  - Different organizations have different needs.
  - By combining styles, you balance these for a more-effective intrusion prevention *system* — the "S" in HIPS.
- ✓ **Use Gartner's nine-style model to help design comprehensive protection strategies for embedded devices, servers, nonmobile desktops and laptops.**
- ✓ **Follow Gartner's suggested best practices for successful HIPS implementation.**
- ✓ **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!**