

## Moving From a Reactive to a Proactive Security Model

Randy Sutherland  
Lumension Security





## ▣ State of Endpoint Security Market

- Customer Challenges
- Industry Trends

## ▣ A New Age of End-Point Security

- Taking a Positive, Proactive Approach
- Highly Secure, Highly Operational



# State of Endpoint Security Technology Market



# How much would you pay for this USB stick?





Some would pay

**\$15 BILLION**



**would!**

# 18 Year Employee Steals Over 320,000 Files

A King County jury began deliberations today in the case of a Boeing employee charged with leaking sensitive company

Boeing claimed that 16 stories in The Seattle Times contained information from downloaded documents

The host might feel the guest "violated his trust," she told jurors. "Maybe he kicks you out. But you don't get prosecuted."



# Can you guarantee that your CEO's laptop is not compromised?

## High Paid CEOs Targeted by Keyloggers

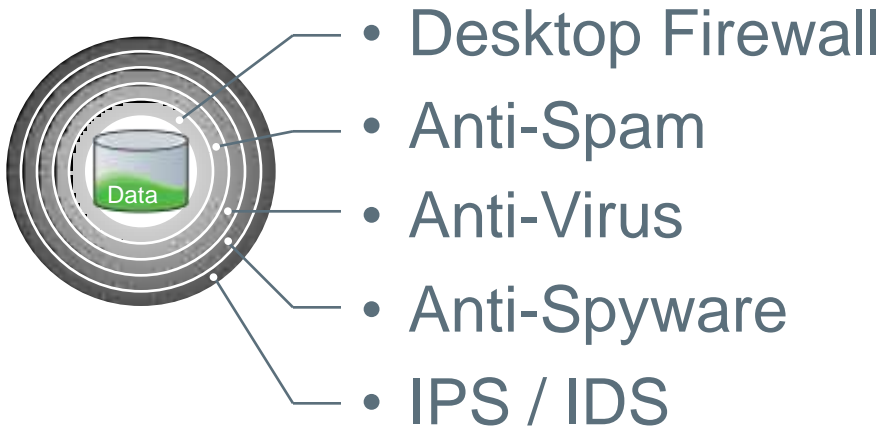
A King County jury began deliberations today in the case of a Boeing employee charged with leaking sensitive company information.

Boeing claimed that 16 stories in The Seattle Times contained information from downloaded documents.

The host might feel the guest "violated his trust," she told jurors. "Maybe he kicks you out. But you don't get prosecuted."



# Traditional Reactive Security has failed to stop these situations.



## Reactive Security POP QUIZ

When tested against 660,000 signatures, how many did “The Big 2” miss?

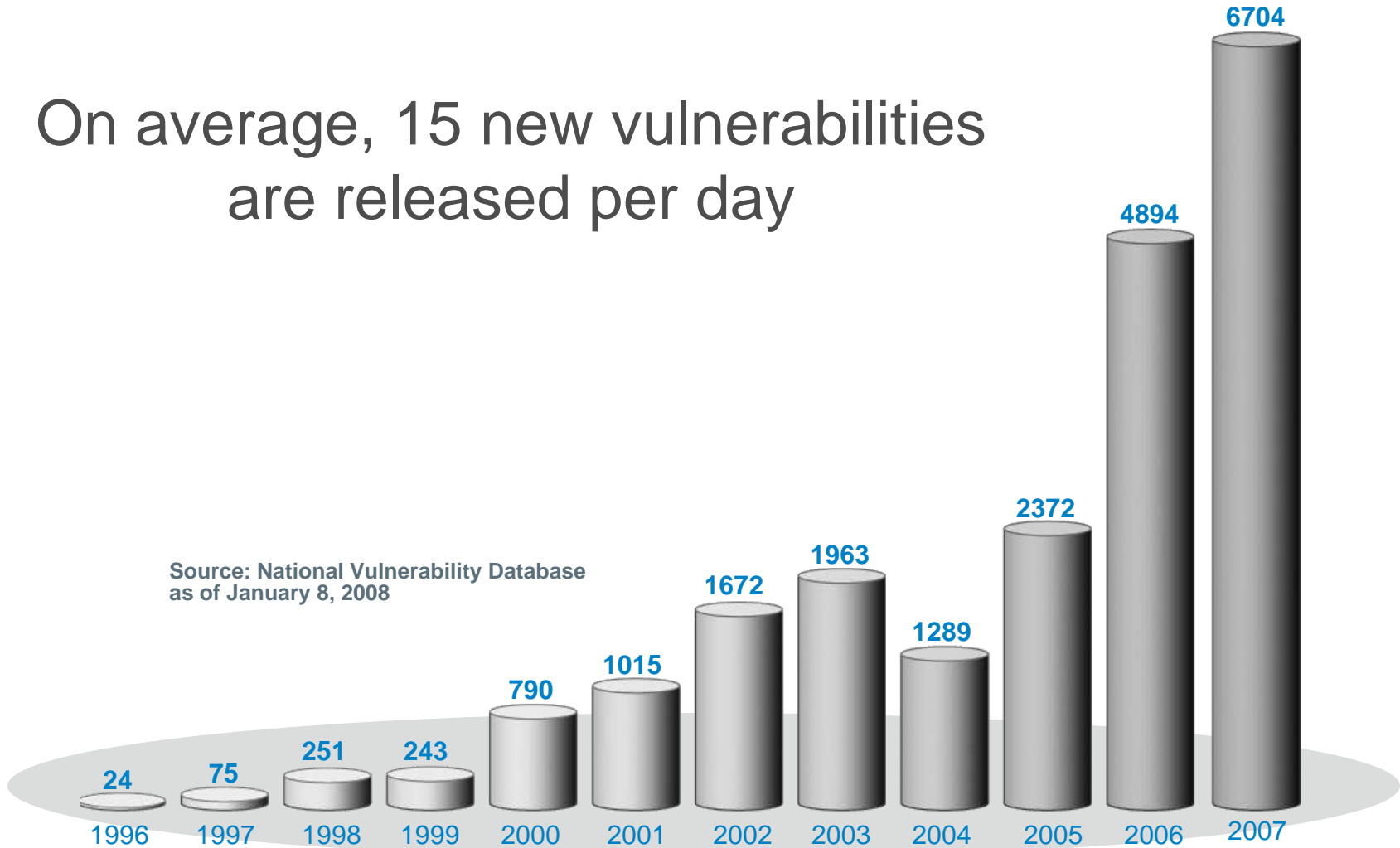
Missed Over  
30,000

Missed Over  
80,000

# Each Day, the Problem Gets Bigger



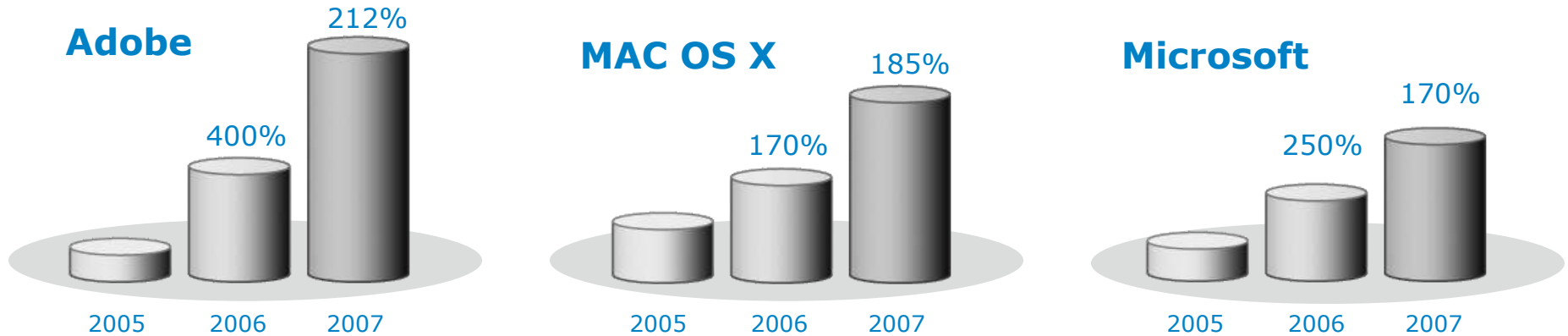
On average, 15 new vulnerabilities are released per day



# Hackers find New Avenues of Attack



▣ NVD reported 13,270 vulnerable applications as of 01/08/08



Source: National Vulnerability Database

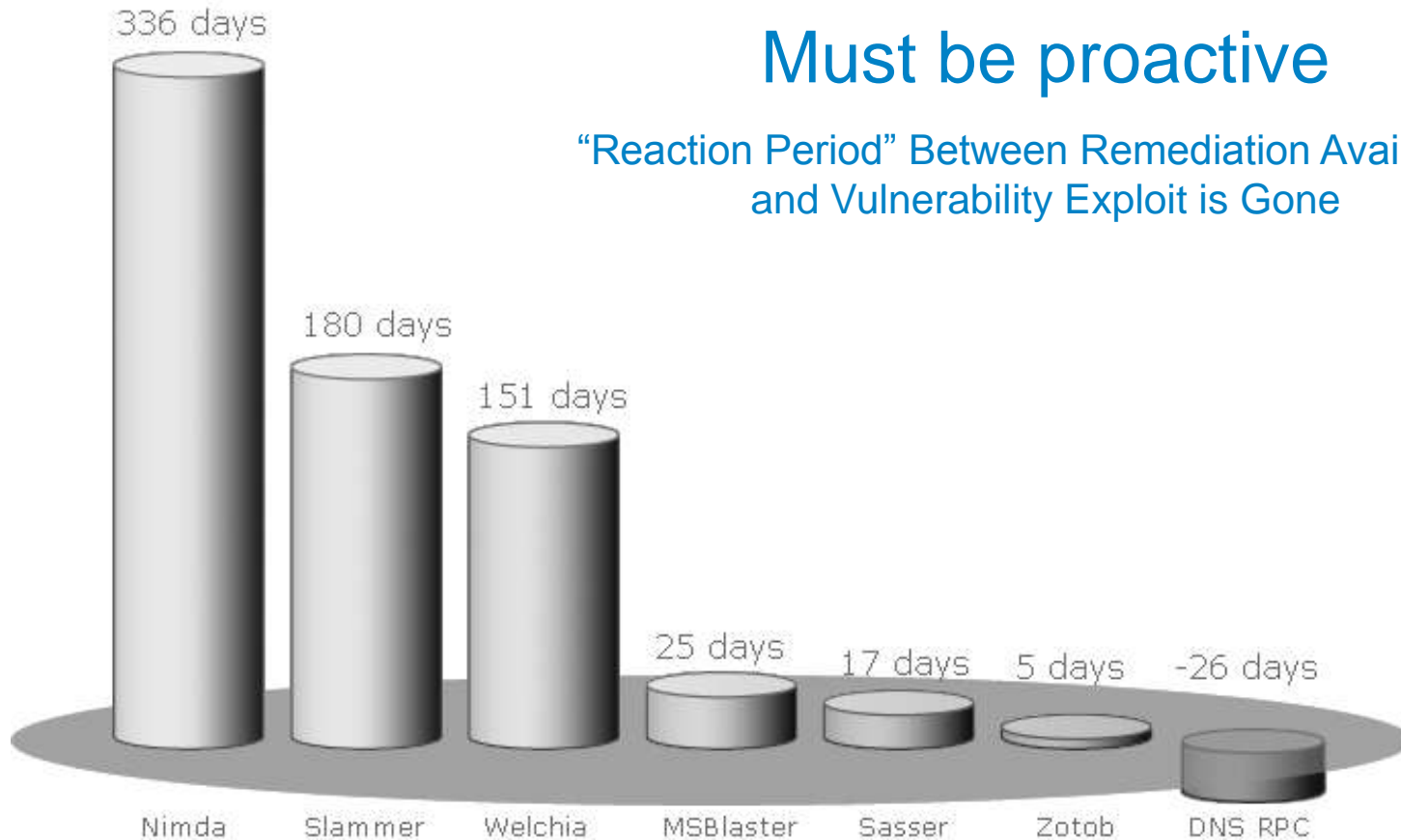
*“Adobe Acrobat/Reader PDF documents can be used to compromise your Windows box. Completely!!!”*

**TECHWORLD**

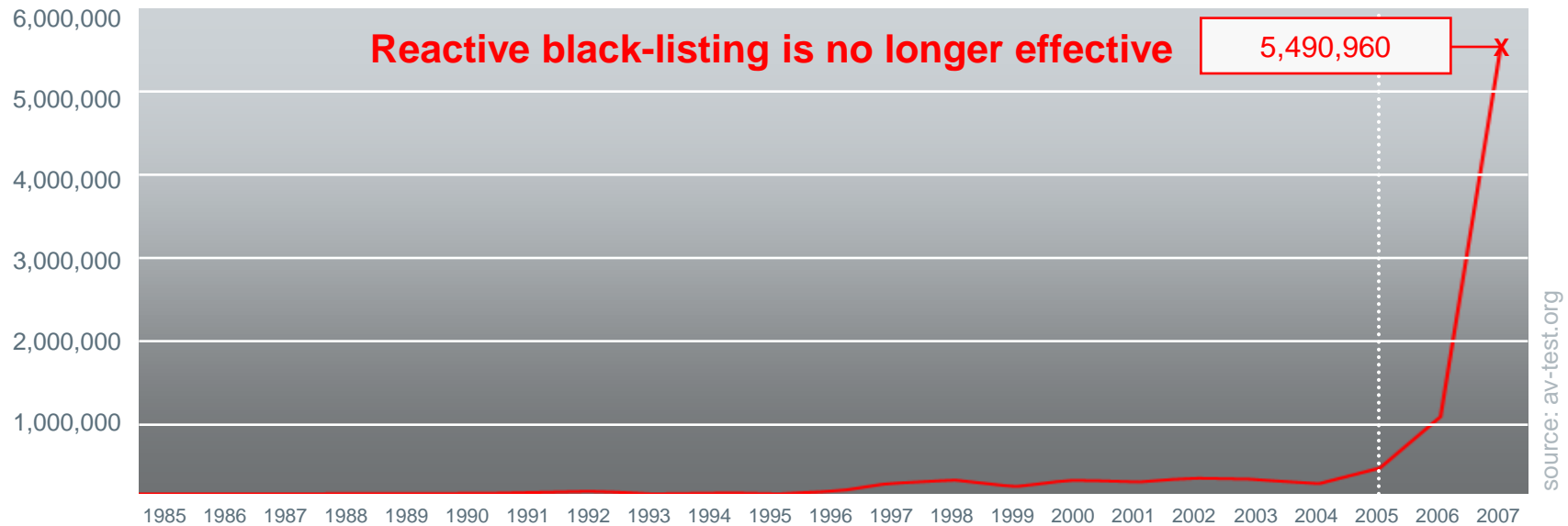


## Must be proactive

“Reaction Period” Between Remediation Availability and Vulnerability Exploit is Gone



# An Inconvenient Truth: Growth of Malware



## Traditional endpoint technology stacks do not solve this issue:

Anti-virus / Anti-malware / Heuristics / HIPS

- Resource intensive
- Susceptible to false-positives
- Can't defend against targeted attacks
- Won't scale with current threat rate
- Do not address underlying vulnerabilities



# What has changed

in today's environment that make:

## Traditional Security Approaches Fail

a single USB stick worth

# \$15 BILLION

and allows targeted Malware to affect even

# YOUR CEO?

# What has changed?

**Three things have changed that make reactive security obsolete.**

The  
Borderless  
Enterprise

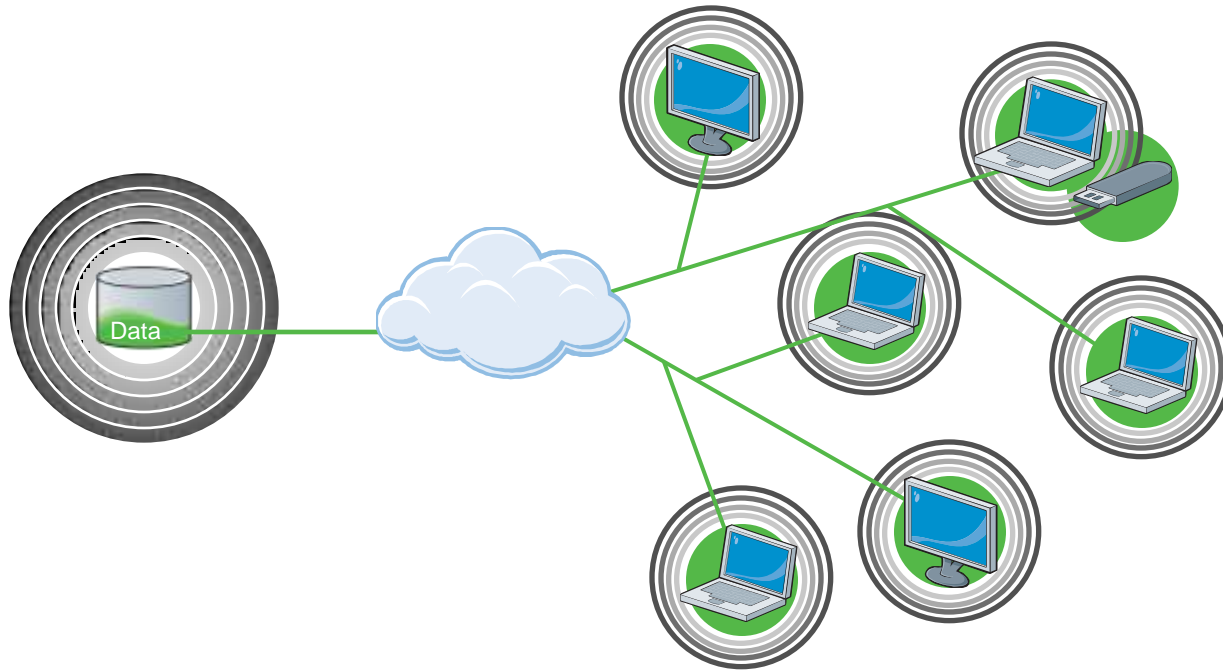
Increased  
Internal  
Risks

Organized  
External  
Threats

# The Borderless Enterprise

**Remote users and mobile technology.**

Data has moved beyond the enterprise firewall:  
Laptops / Home Offices  
USB Sticks / WiFi / VPN  
and more...



# New Technology - New Sources of Risk






Easy of Connectivity = Risk Increases

Increased Storage Capacity = Risk Increases





- Removable media stores more at lower cost than ever before and fits in your pocket

Physical Size	Storage Size	Per MB Price
		

- Plug and Play offers seamless support for removable media
- Removable media is significant to daily business operations
- Professional and personal use of removable media has merged

# Increasing Internal Risk

**Insiders have direct access to your most sensitive data.**

**70%** of all serious incidents are sparked by insiders.

IDC Worldwide Security Products and Services  
2007 Top 10 Predictions



**Lost Laptops  
& Devices**



**Disgruntled  
Employees**



**P2P File Sharing  
Software**

**48% of users utilize company tools for personal usage.**

# What Threat Does an Insider Pose?



- ▣ John's iPod might have 80 GB of his favorite music and video's or it might contain:
  - software he brought from home to install
  - malicious software, such as malware, spyware, crime ware
  - a virus or Trojan



- ▣ When John leaves at night it might have:
  - your customer database
  - financial data
  - intellectual property

***53% of organizations would NEVER know what data was on a lost USB device <sup>1</sup>***

Source:

1- Ponemon Institute, 2006 Cost of Data Breach Study

# External Threats

The hackers you face are no longer just Gary and Wyatt...



# Organized External Threats

Well Funded.  
Organized.  
Financially Motivated.





Data is not just going out on Mobile Devices.

Malware coming in on Mobile Devices as Well

**New form of Social Engineering**

**Leaving USB drives in parking lots of Targeted Companies with Malware installed**



What do these removable devices all have in common?



All came pre-installed with viruses capable of stealing passwords and opening doors for hackers





☐ Data breaches remain the leading cause of financial losses <sup>1</sup>

☐ Data breach costs continue to increase <sup>2</sup>

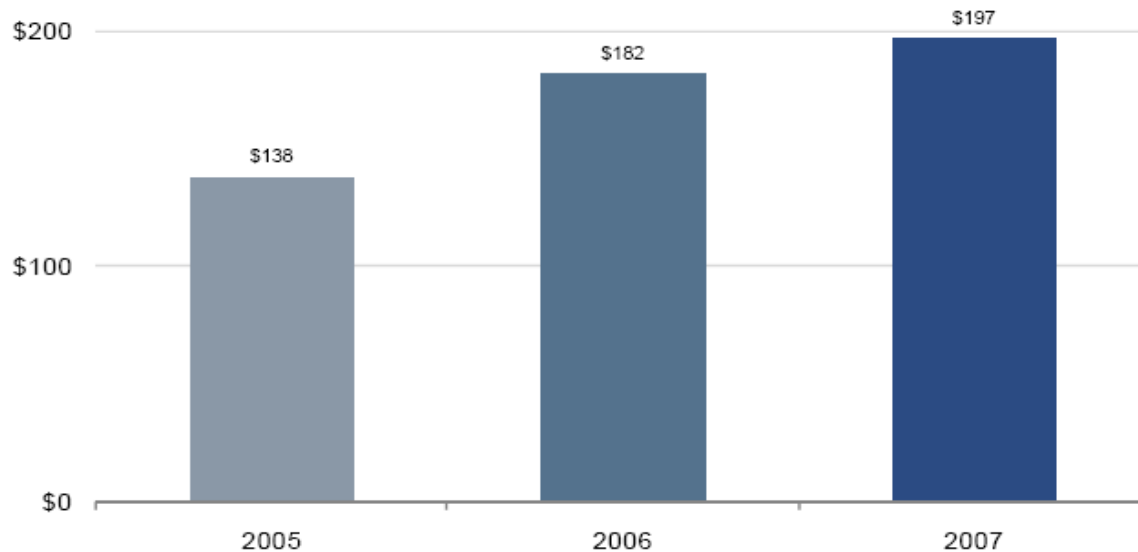


Figure 1: Average per-record cost of a data breach, 2005–2007

Source:

1 - 2006 CSI/FBI Computer Crime and Security Survey

2 - Ponemon Institute, 2007 Cost of Data Breach Study



☐ Lost business accounts for 65% of data breach costs

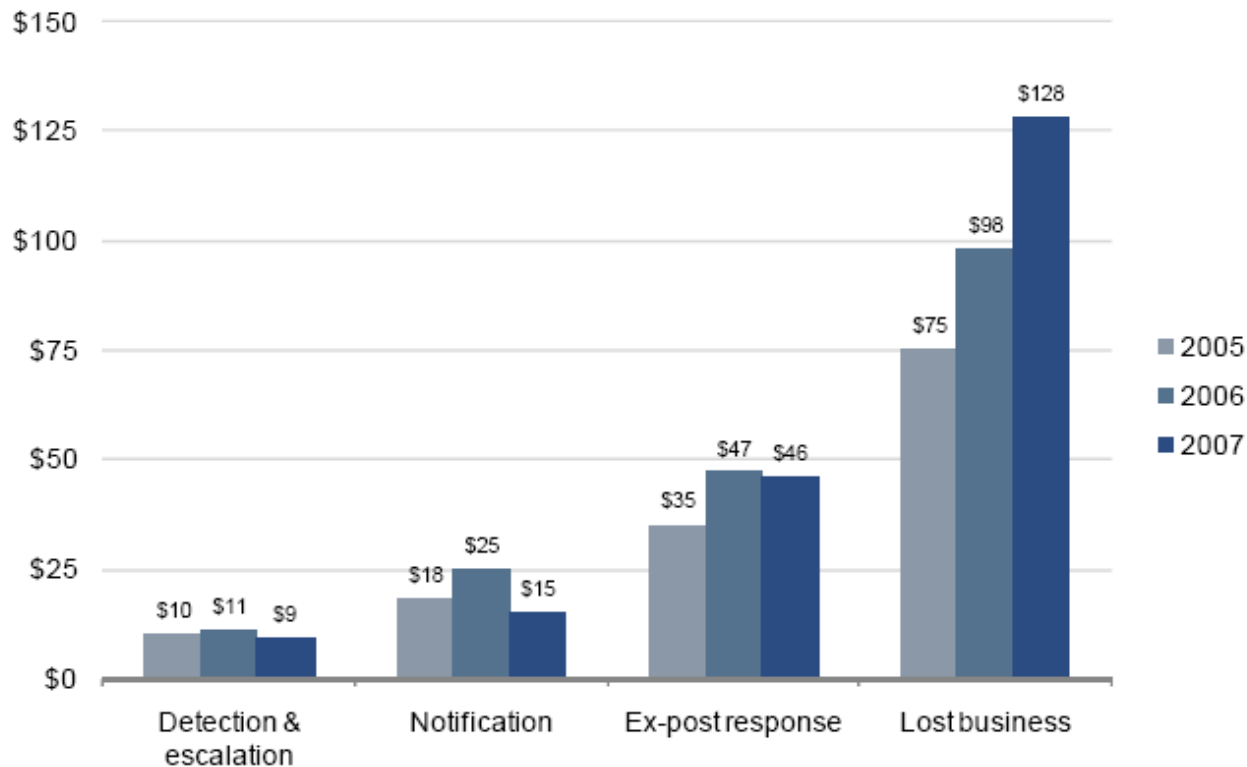


Figure 2: Data breach costs by center per record compromised, 2005–2007

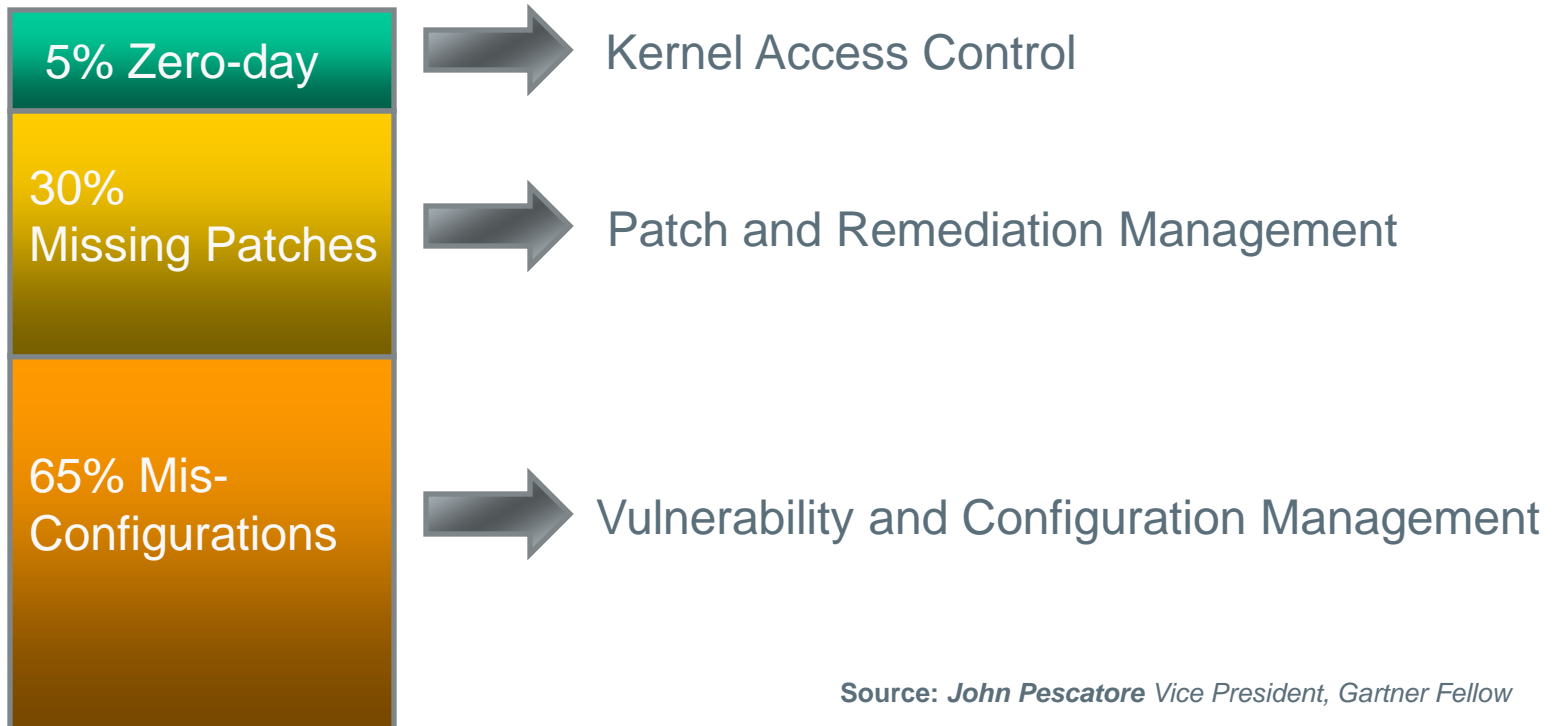
Source:  
Ponemon Institute, 2007 Cost of Data Breach Study



**How do you address  
the new security challenges  
in today's environment?**



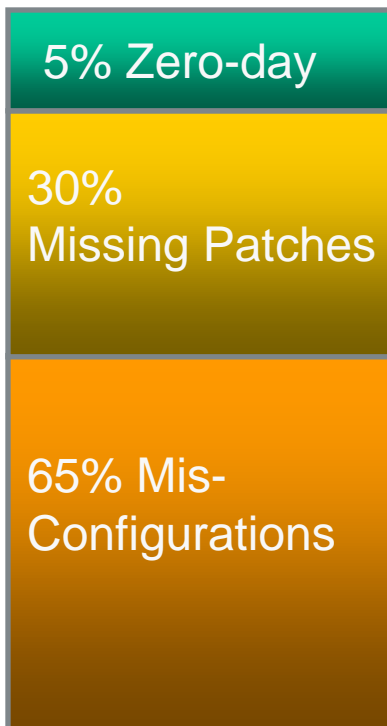
Attacks Exploit  
Risks at the Core



Source: *John Pescatore* Vice President, Gartner Fellow



Attacks Exploit  
Risks at the Core



The OS / Sources of Risk



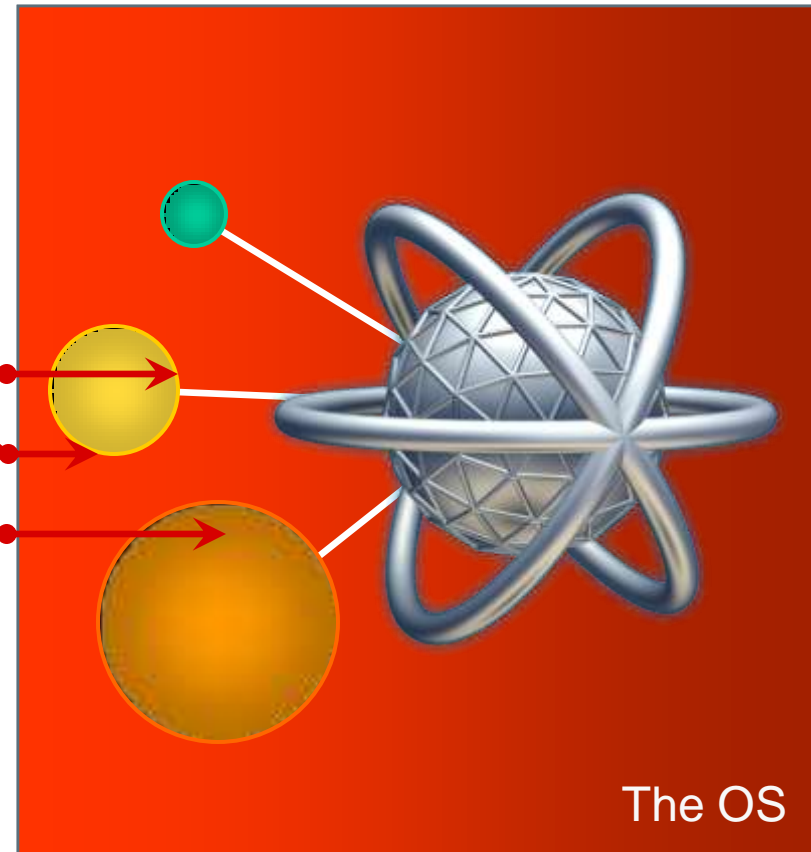
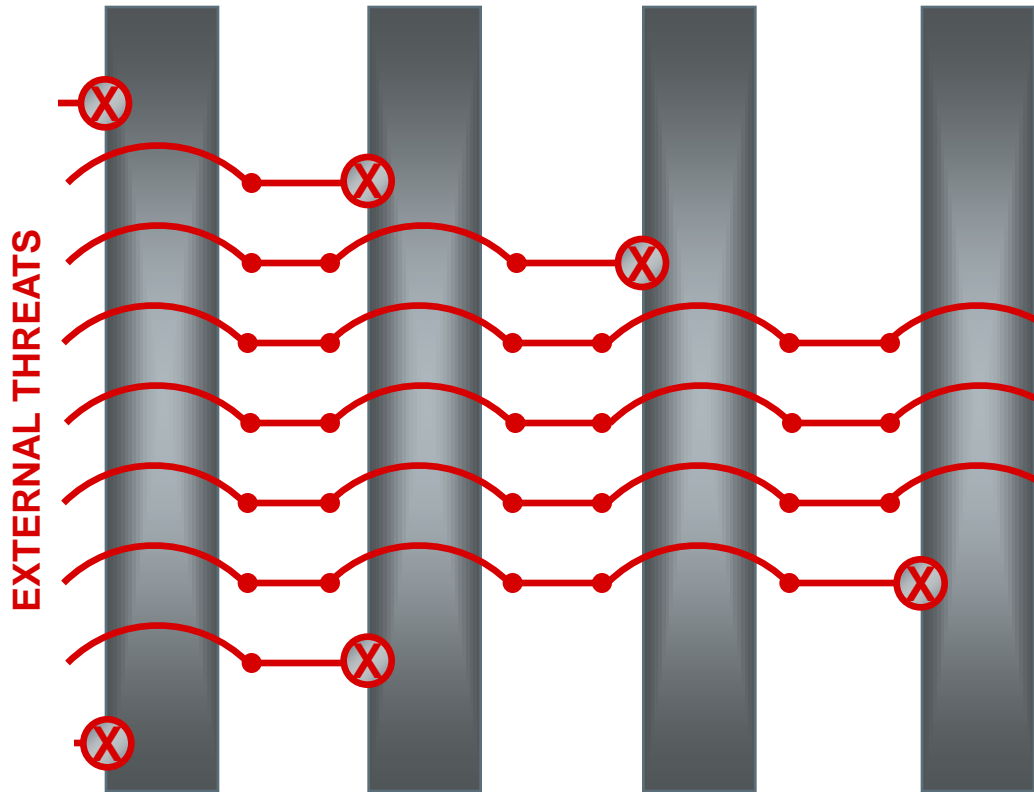
# UPC – Traditional Approaches



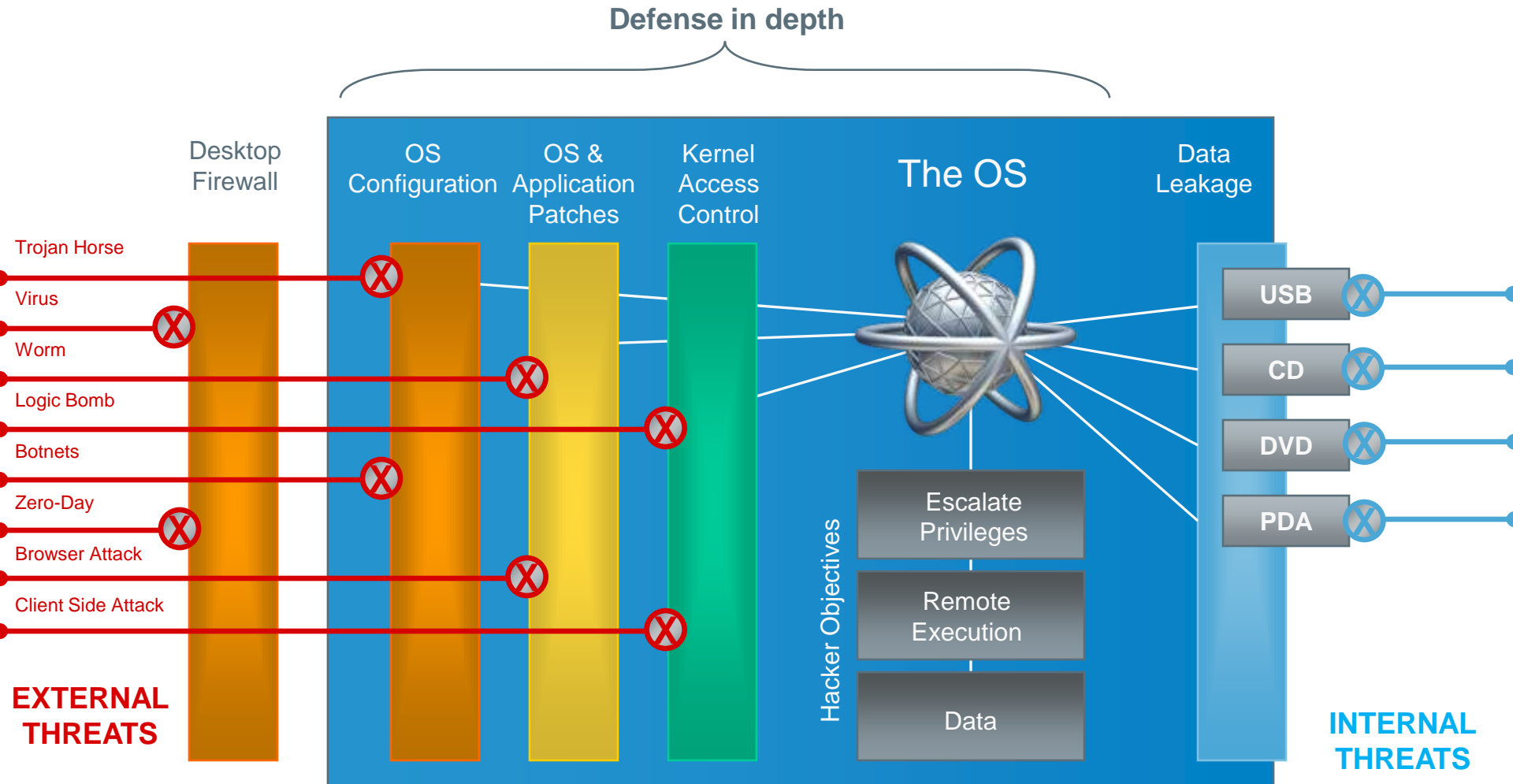
Traditional Depth in Defense Security Add-on Solutions

The OS / Sources of Risk

Desktop Firewall    Anti-Virus Spyware    IPS Heuristics    Application Blacklist



# Proactive, Operational End Point Security Approach



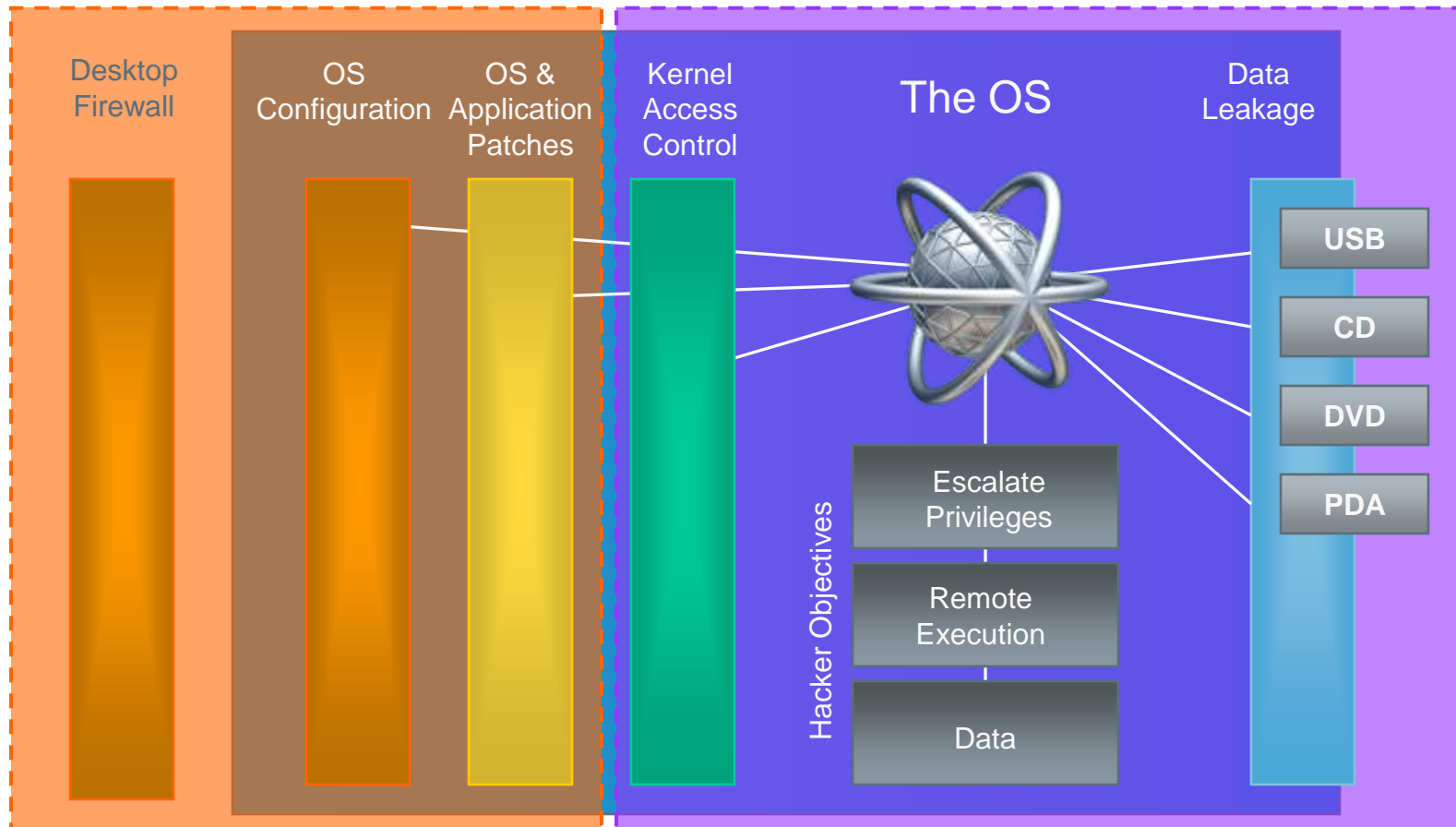


## PatchLink Suite

Scan / Security Configuration Management / Update

## Sanctuary Suite

Application Control / Device Control

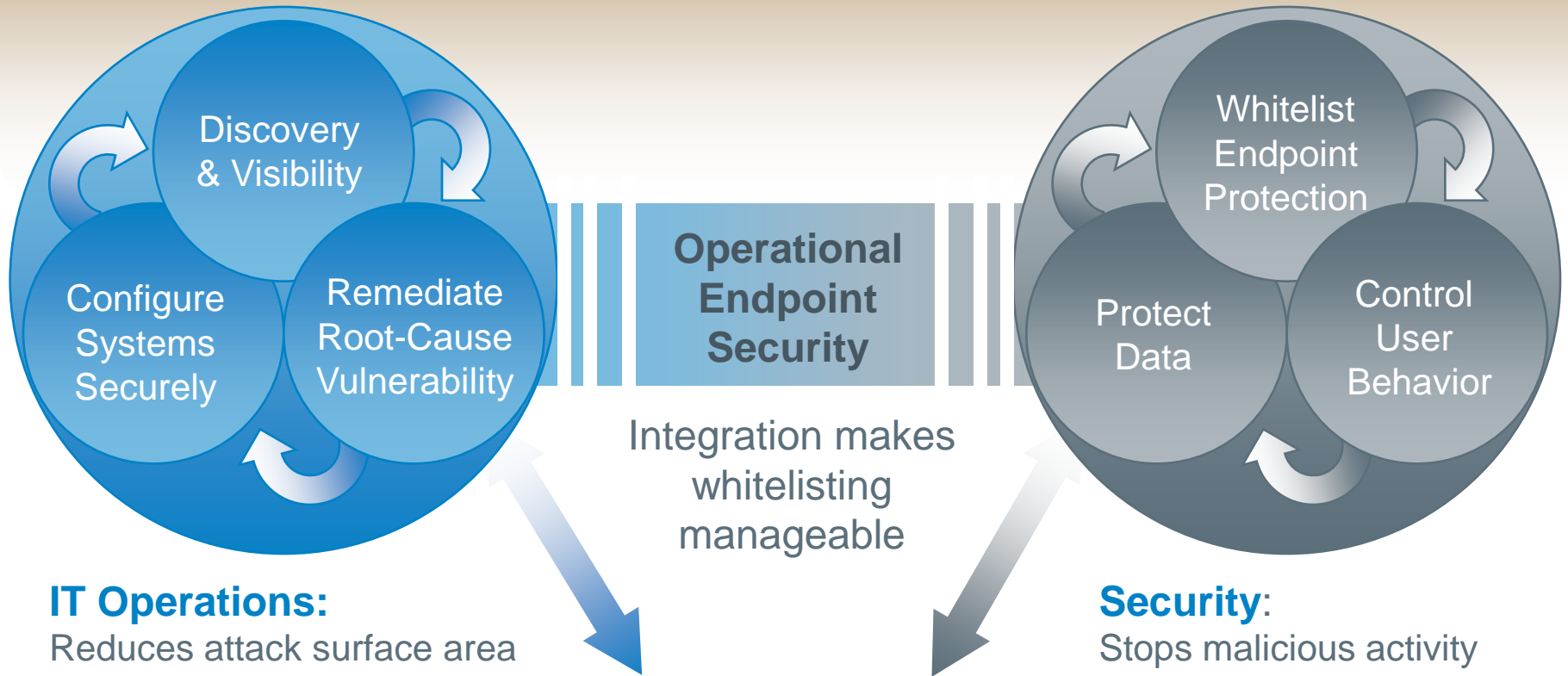


**YOU HAVE TO  
Get Proactive.**

# Lumension's Operational Security Approach



## Policy Compliance Reporting



Integration = maximum security, flexibility and productivity

# **The Lumension Security Advantage**

**Stops Targeted Attacks  
Eliminates Insider Threats  
Prevents Data Loss  
Defends Against Zero-Day Exploits**

# Shrink the Target



## Operational Security Management

Enables proactive discovery, assessment, remediation and secure configuration



**Vulnerability  
Assessment**

**Patch  
Management**

**Security  
Configuration  
Management**

- ▣ Provides complete visibility of your risk posture through continuous discovery and vulnerability assessment
- ▣ Delivers real time patching and remediation with ongoing validation
- ▣ Reduces Endpoint Risk by Fortifying OS and Application Configurations

# Shrink the Target / Stop the Bullets



## Data Security

Protects data from theft or loss.



### Device Control

Whole Disk  
Encryption

Data Leakage  
Prevention

- ☐ Controls the flow of data to devices  
(inbound and outbound data including port access)
- ☐ Encrypts data (moved onto removable devices)
- ☐ Detailed forensics and auditing  
(of data moved to / from a device)
- ☐ Enables Compliance  
(Data Protection Regulations and Standards)

# Stop the Bullets



## Endpoint Security

Defines trusted applications and denies all unknown, unauthorized and malicious threats.



Application  
Control

Device  
Control

- ▣ Allows only explicitly authorized application to execute
- ▣ Prohibits unwanted or illegal applications to install or run
- ▣ Prevents unwanted or unmanaged removable devices to introduce malicious code

# Continuous Monitoring and Reinforcement



## Security Compliance Reporting

Reduces the cost of compliance management while providing enterprise-wide visibility over your security environment.

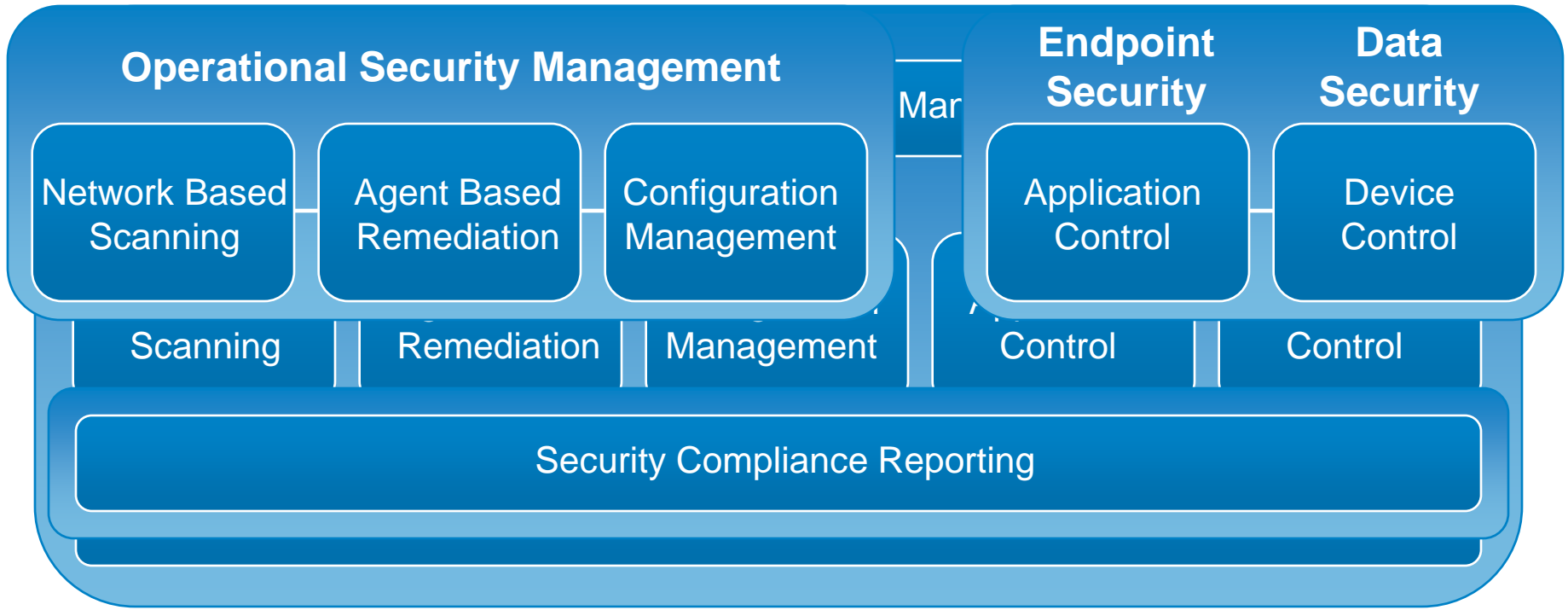


Enterprise  
Reporting

Security  
Configuration  
Management

- ▣ Aggregates and centralizes security configuration states for actionable reporting
- ▣ Enables continuous audit-readiness
- ▣ Facilitates compliance reporting and checks with security regulations or standards

# Lumension Proactive Security Approach



**Superior Security:**

**Scalable / Greater Enterprise Visibility**

**Improved Productivity / Lower TCO**

# **The Lumension Security Advantage**

**Stops Targeted Attacks  
Eliminates Insider Threats  
Prevents Data Loss  
Defends Against Zero-Day Exploits**

# Get Proactive.



Check out Lumension's  
Proactive Security Solutions.

or visit us at [lumension.com](http://lumension.com)



- ▣ Every device isn't there to harm you, John might need a...
  - USB drive
    - to easily move large files
    - to take work on the road with you
    - it lets him modify files, unlike burning the files to a cd/dvd's
    - he might carry a “toolkit” with him to support other users
    - he can use it to backup data
  - iPod's
    - to watch a video training
    - to listen to a company podcast
    - to listen to a class he is taking





- ▣ Organizations need to ask themselves...”do we need to allow access to these devices?”
  
- ▣ If yes,
  - Who should have access – everyone, specific groups or users
  - What devices should be allowed – usb drives, mp3 players, etc.
  - When should access be allowed - 24/7, Mon. - Fri., 9 to 5
  - Where should they be used – every machine or specific machines
  - How should they be used – read only or read/write permission
  
- ▣ If not, how are you going to deny access to the devices



## How would you control these devices?

- Order machines without USB ports
- Physically blocking the USB ports
- Disabling the USB ports in the Bios
- Disable the USB ports in the registry
- Ban portable storage devices
- Use a software based tool to control access
- Do nothing



## **Discovery**

Know what applications and devices are in use on endpoints

## **Policy Establishment**

Develop company-wide, group and/or user-specific policies that reduce, or eliminate endpoint security issues

## **Policy Enforcement**

Enforce and administer endpoint security policies and the flexibility to seamlessly make policy changes as appropriate, reducing end users' need for involvement

## **Policy Monitoring and Compliance Reporting**

Understand the effectiveness of endpoint policies and to know when they have been violated