

# Moving From a Reactive to a Proactive Endpoint Security Model

Carlos Sanz  
Lumension Security





- ▣ State of Endpoint Security Technology Market
  - Customer Challenges
- ▣ Security Technology Maturation
  - Natural Shift from Reactive to Proactive Security Model
- ▣ A New Age of Endpoint Security
  - A Proactive, Operational Approach

Say Goodbye to  
the **DARK AGES**

LUMENSION IS PUTTING SECURITY IN A POSITIVE LIGHT  
The traditional reactive security model  
no longer provides a viable defense.



# State of Endpoint Security Technology Market



- ☐ Anti-Virus
- ☐ Anti-Spyware
- ☐ Personal Firewall
- ☐ IPS/IDS
- ☐ Secure password enforcement
- ☐ Domain policies
- ☐ Disabled USB ports

***With all of these solutions  
endpoints should be secure, right?***

# Security Landscape is Changing



Source: IDC

## Old Landscape

## New Landscape





- ▣ More remote employees than ever before
  - More than 44 million teleworkers in the US <sup>1</sup>
  - More than 100 million teleworkers expected by 2010 <sup>2</sup>
  
- ▣ Widespread availability and use of mobile technology
  - Laptops
  - USB Sticks
  - iPods
  - Bluetooth
  - And many more

***Endpoints are the likeliest entry point for malware*** <sup>3</sup>

Sources:

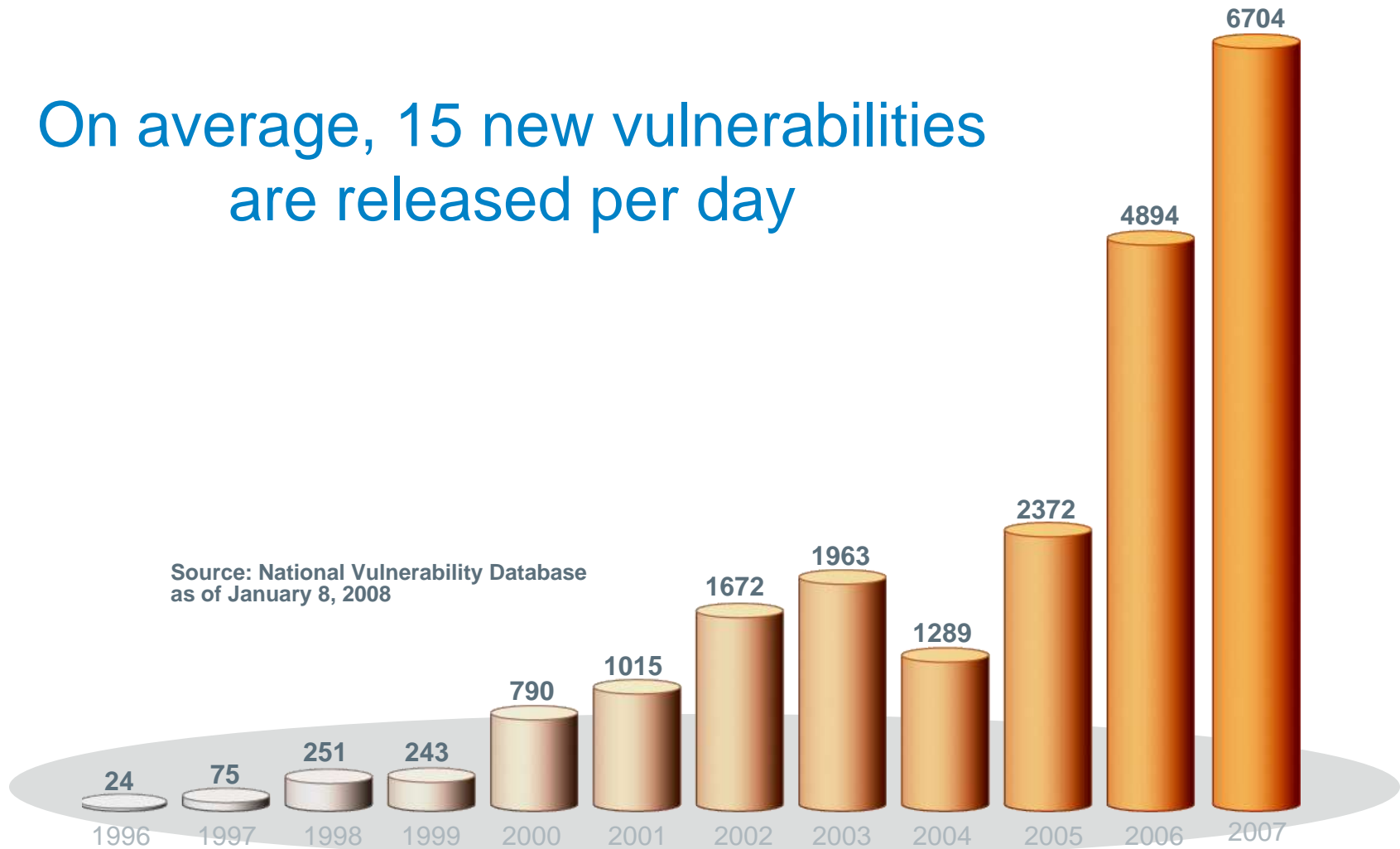
1 – Dieringer Research Group

2 – WorldatWork's Telework Trendlines 2007

3 – Yankee Group

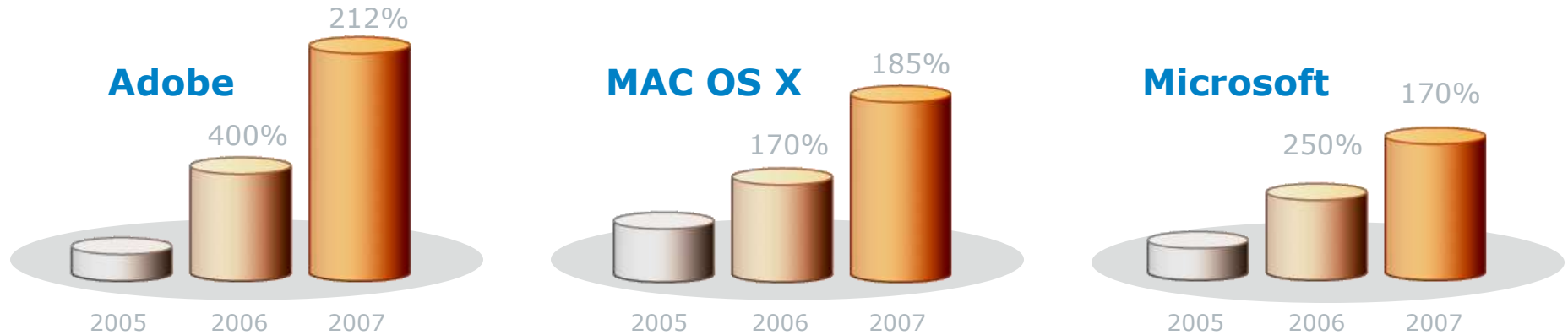


On average, 15 new vulnerabilities  
are released per day





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



Source: National Vulnerability Database

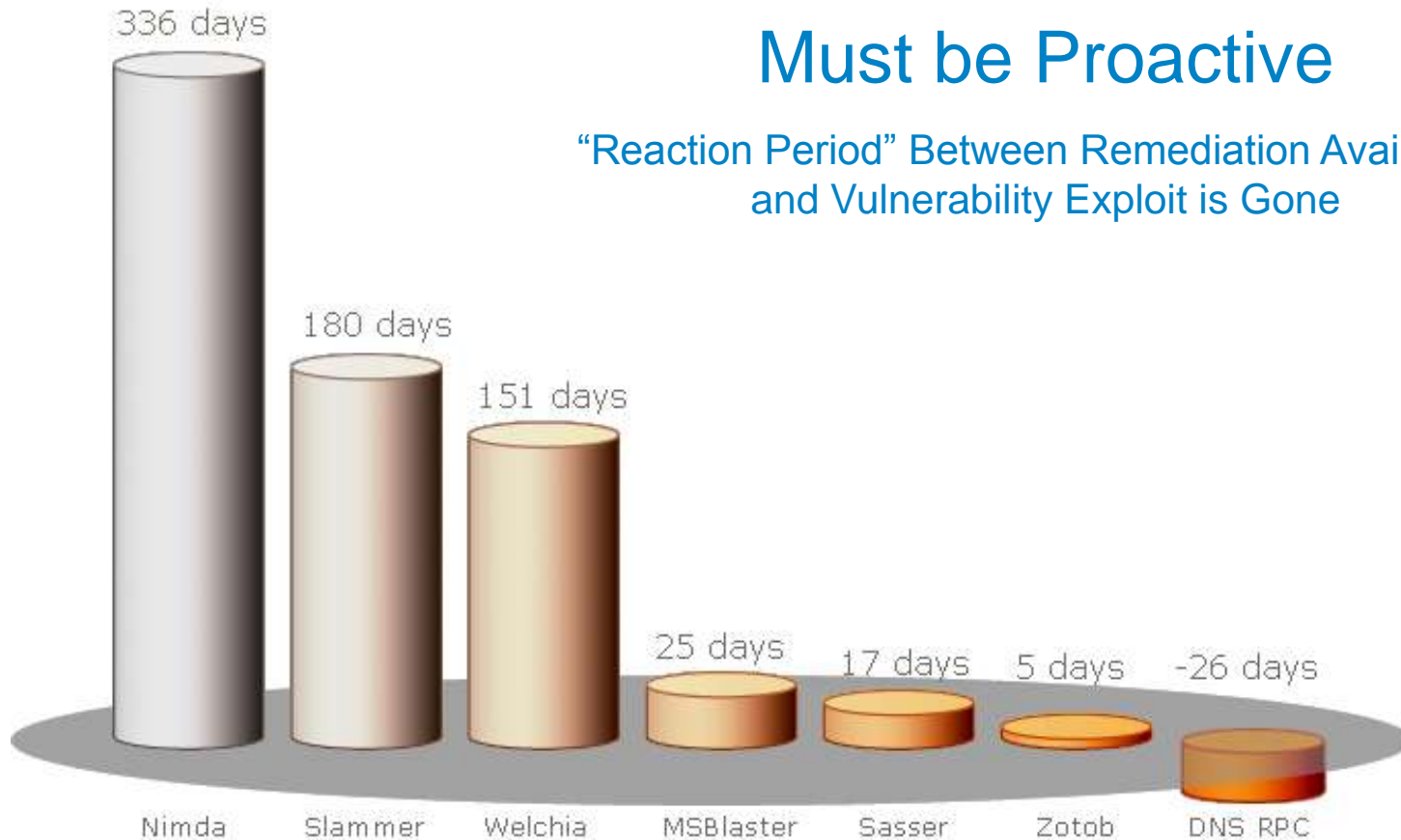
*“Adobe Acrobat/Reader PDF documents can be used to compromise your Windows box. Completely!!!”*

**TECHWORLD**



## Must be Proactive

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





- 70% of all serious incidents are sparked by insiders <sup>1</sup>
- 53% of organizations would NEVER know what data was lost/stolen on a USB device <sup>2</sup>



**Corporate IP or Financial Data to Go!**

Sources:

1 – IDC Worldwide Security Products and Services 2007 Top 10 Predictions

2 – Ponemon Institute, 2006 Cost of Data Breach Study



- ▣ Targeted attacks are a reality and are starting to be quantified
  - 18% of respondents suffered a “targeted attack,” defined as a malware attack aimed exclusively at their organization <sup>1</sup>
  
- ▣ More advanced, more varied and much harder to detect
  - Polymorphic attacks and botnets used to gather personal data for identity theft, distribute spam, spyware and DOS attacks
  
- ▣ Specific sources of risk within an organization’s environment are targeted
  - Zero-day threats
  - Missing patches
  - System mis-configurations



Source:

1 – 2007 CSI Computer Crime and Security Survey

# Regulatory Compliance is Coming



- ▣ 20% of the 161 exabytes of data created in 2006 are subject to compliance guidelines
- ▣ Privacy legislation requiring companies to publicly disclose security breaches to customers is in effect in 31 states
- ▣ Regulations becoming more specific
- ▣ Visa offers merchants and transaction services providers \$20 million in incentives to comply with PCI regulations





February 2007



tested **15 leading anti-virus vendors**  
against **481,850 pieces**  
of **known malicious software**

[www.av-comparatives.org](http://www.av-comparatives.org)

---

**“75% of enterprises will be infected with undetected, financially motivated, targeted malware that evaded traditional perimeter and host defenses.”**

Gartner, Inc.

The largest viral database had over 662,000 signatures .....  
**HOW BIG IS BIG ENOUGH?**

## Total Detection Rates

Symantec  
**MISSED over 30,000 ...**

McAfee  
**MISSED over 80,000...**



- ☐ Ineffective security impacts the bottom line
  - Loss of customer trust, discontinued relationship with organization
  - Increased cost to rebuild corporate brand and image
- ☐ Increased support costs to rebuild machines
  - 85% of laptops/desktops are rebuilt each year <sup>1</sup>
  - Average enterprise downtime = 23 person days <sup>1</sup>
  - Average time to full recovery = 31 person days <sup>1</sup>
- ☐ Data breach costs continue to increase <sup>2</sup>

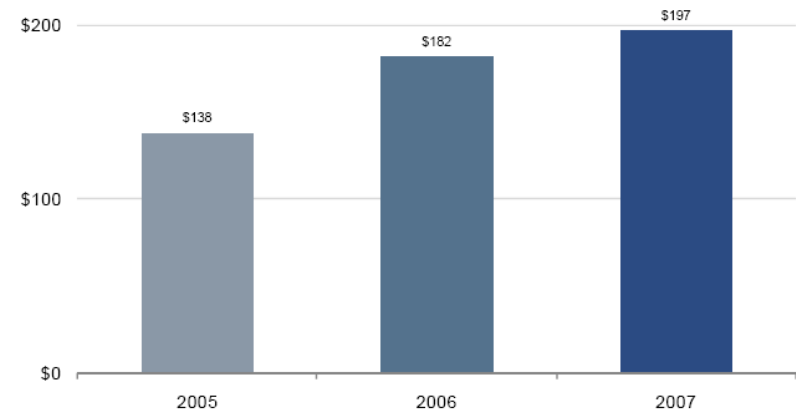








Figure 1: Average per-record cost of a data breach, 2005–2007

Sources:

- 1 – Yankee Group, 2005 Security Leaders and Laggards Survey
- 2 – Ponemon Institute, 2007 Cost of Data Breach Study

# Short List of Recent Attacks



	Dolphins' sites serves up malicious JavaScript code that exploits two known Windows vulnerabilities and installs a Trojan downloader and a password stealing program on the victim's computer.
	A disgruntled Boeing transferred 320,000 company files over the course of more than two years to a thumb drive and then removed it from company property. Boeing estimated that if only a portion of the stolen documents were given to competitors, it could cost the company between \$5-\$15 billion.
	6.3 million customers affected by the security lapse, where attackers had access to a database that included personal information, account numbers and Social Security numbers of customers.
	Hackers stole legitimate credentials from Monster's job-seekers to plant malware on the site and execute a phishing scheme.
	Hacker accessed credit card numbers and other personal information in a December incident. Ironically, the website features the "hacker safe" notification from McAfee ScanAlert.
	SQL injection attack on Microsoft's SQL Server database product to compromise 70,000+ sites, including CA. Hijacked visitors' PCs with a variety of exploits



# Security Technology Maturation



As technologies mature, they invariably move from a “reactive” to a “proactive” security model

## ☐ “Early Stage” - Negative/Reactive Model

- Security: trumped by need for productivity
- Costs: Focus on low acquisition, unknown TCO
- Security Philosophy: Trust all, **reactively block** the “known bad” as soon as it is identified



## ☐ “Mature Stage” – Positive/Proactive Model

- Security: Equal in status to productivity
- Costs: Focus on lowering true TCO
- Security Philosophy: Suspect all, **proactively allow** only the “known good” through policy enforcement





Early Stage:  
“Reactive”

Mature Stage:  
“Proactive”

<b>Policy Philosophy</b>	Productivity and flexibility at the expense of security	Flexibility and productivity - within established bounds
<b>Resources Access or Consumption</b>	Trust anyone	Protect everyone by verifying everyone
<b>Enforcement Approach</b>	Block “known bad” if/when they are identified	Allow “known good” (block all bad - both known & unknown)
<b>Cost Curve</b>		



- ❏ Negative/reactive security models are the simplest to implement and are used in the early stages of a technology
- ❏ Over time negative/reactive security models do not scale in terms of effectiveness, performance, or cost
- ❏ Out of necessity, vendors turn to a positive/proactive model as products mature
- ❏ Only positive/proactive security models can eliminate known and unknown threats and the associated risks
- ❏ Products are forced to adopt a positive security model to meet customer demands for effectiveness, performance, and reduction in TCO

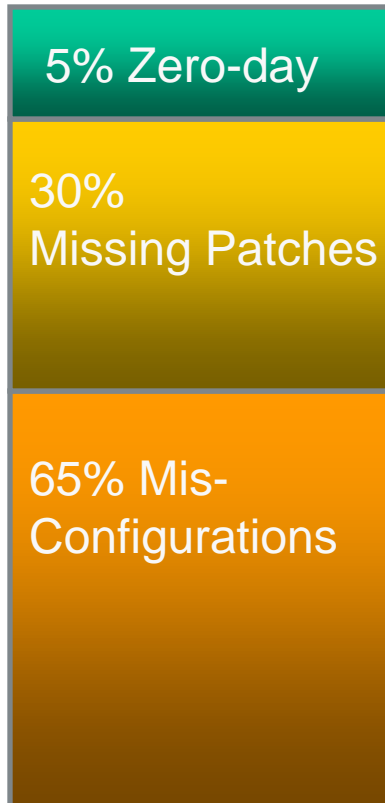


# A New Age of Endpoint Security via A Proactive Approach

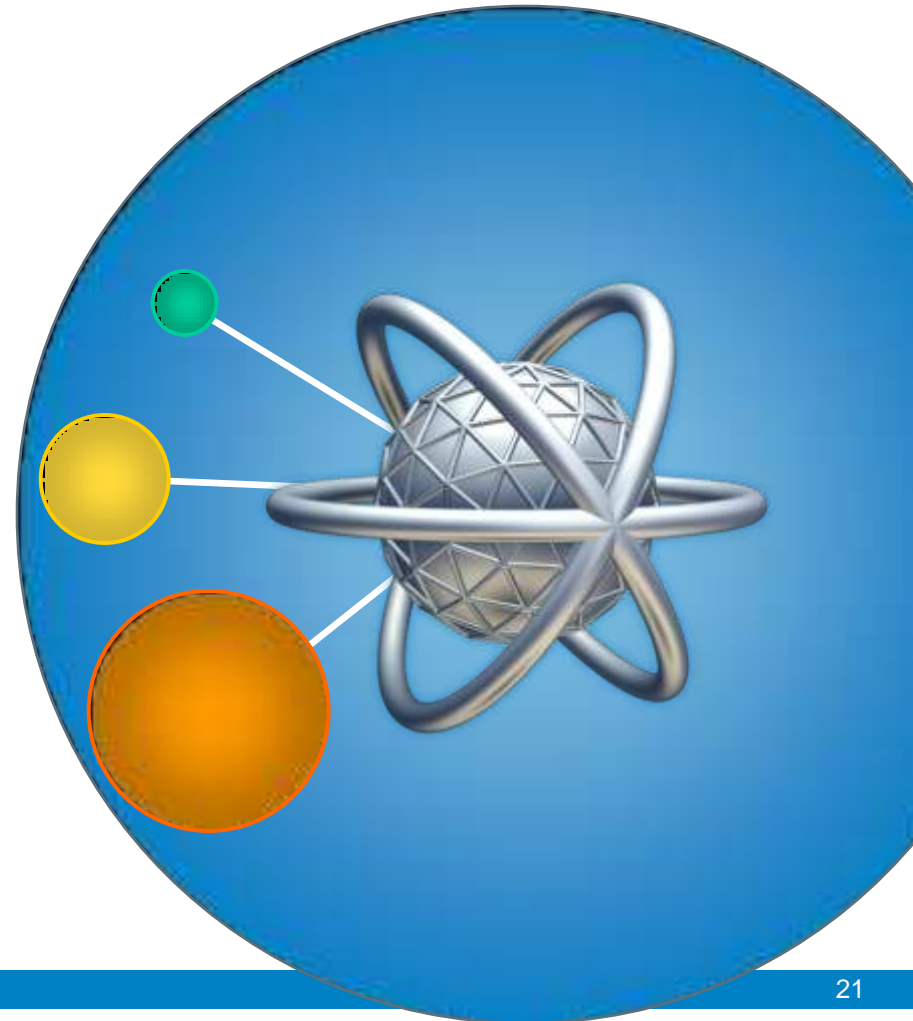
# What Sources of Endpoint Risk do Threats Target?



Attacks Exploit  
Risks at the Core



The CORE / Sources of Risk



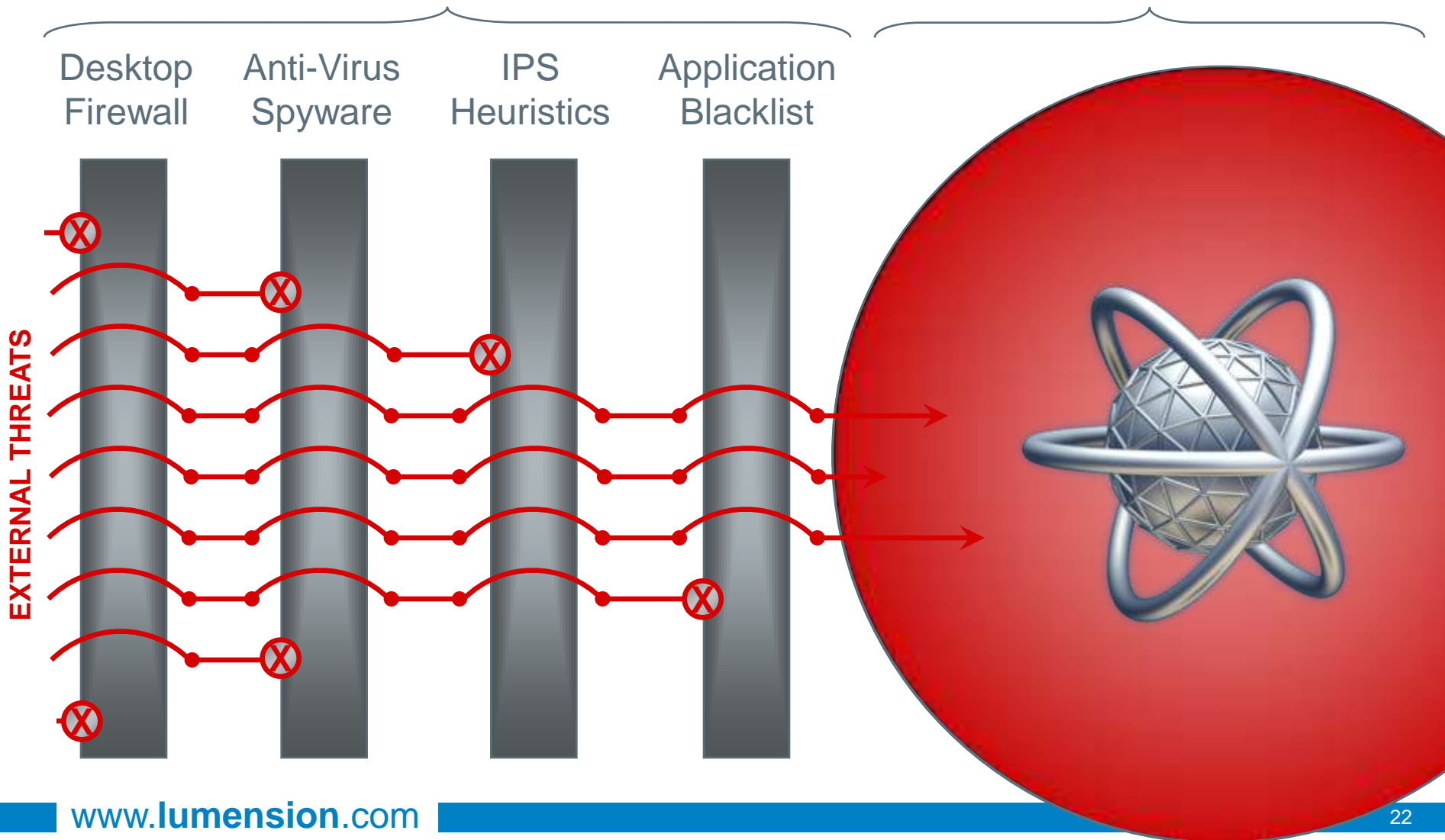
Source: *John Pescatore* Vice President, Gartner Fellow

# Traditional, Reactive Security Approaches



## Security Add-on Solutions

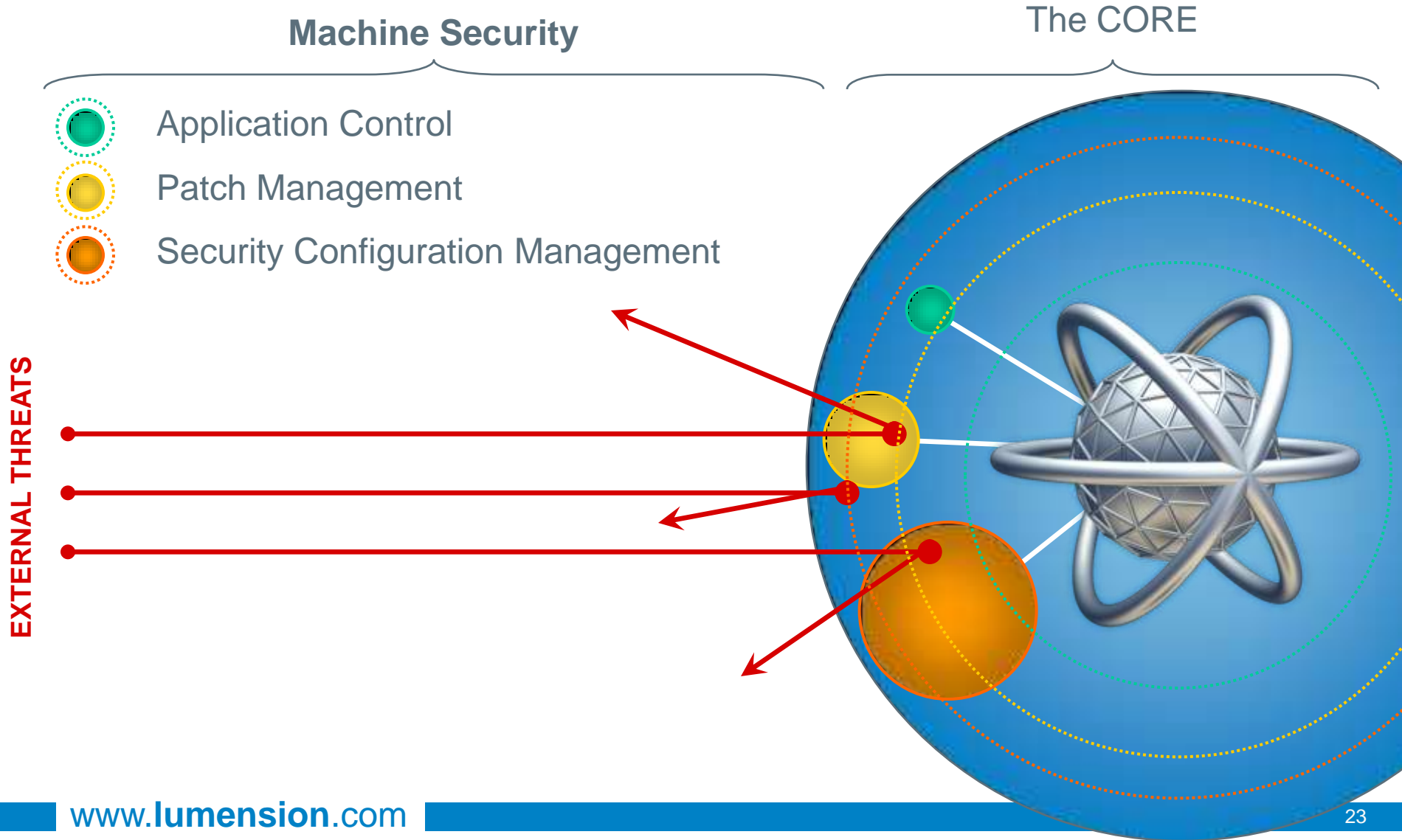
## The CORE / Sources of Risk

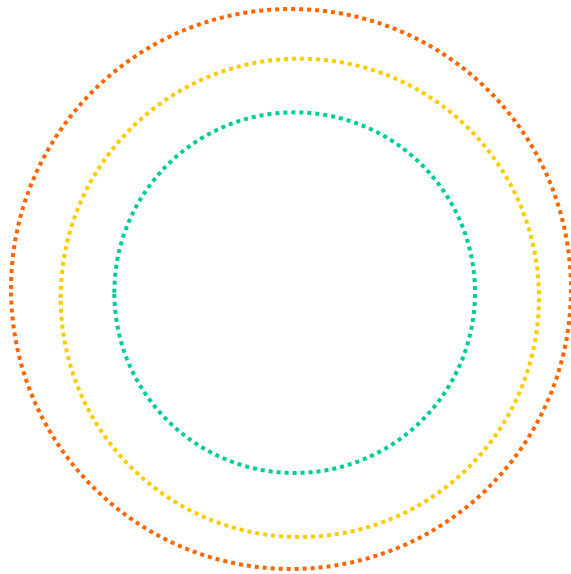


# Lumension's Proactive, Operational Approach



## External Threats: Mitigate Risks at the Source





# Lumension's Proactive, Operational Approach



## Internal Threats: Enforce Application & Device Use Policies

### Machine Security

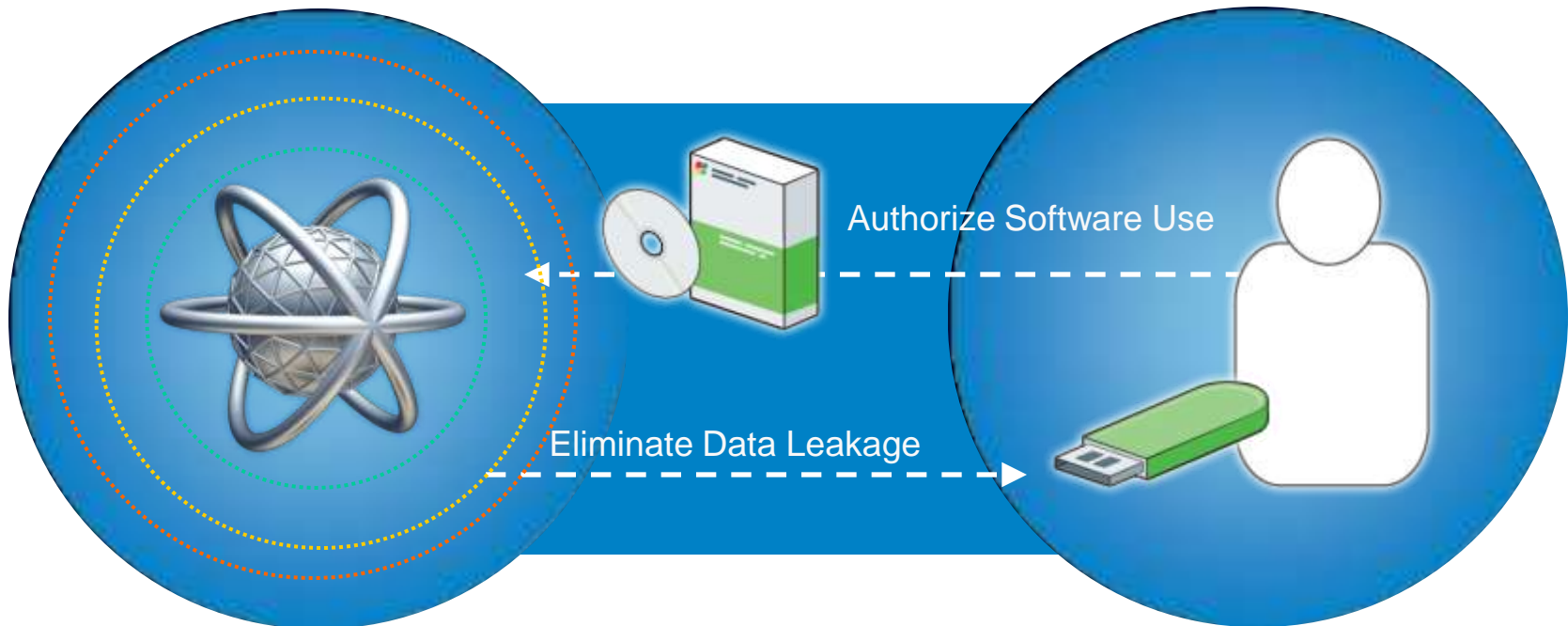
Application Control  
Patch Management  
Security Configuration  
Device Control

### User Security

Application Control  
& Device Control

### Data Security

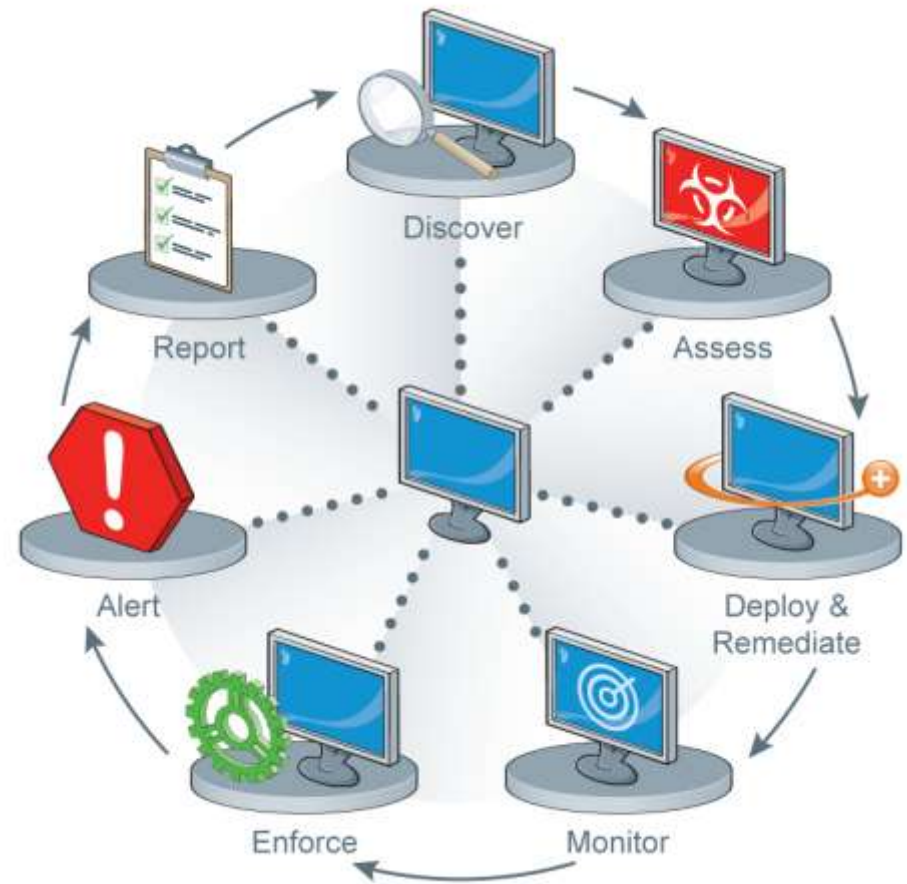
Device Control  
\* Content Monitor Filter : Websense  
\* Encryption : PGP  
\* Partners \*



# Powerful Universal Platform – Common Actions



- ▣ *Discover*
- ▣ *Assess*
- ▣ *Remediate*
- ▣ *Deploy*
  - Patch, Software, Scripts, Agent (SW)
- ▣ *Monitor*
  - Audit/Log, Shadow Data, User Actions
- ▣ *Enforce*
  - Baseline
    - Software Version, Configuration, Device, Authorized Applications
  - Block = devices, application
  - Ask = trusted users
- ▣ *Alert*
  - Admin Alert, Message to End-user
- ▣ *Report*



Lumension Security Platform  
*Deliver – Monitor – Enforce - Report*



## Policy Requirements

## Solution

### Discover & Assess

all assets for policy compliance



PatchLink  
Scan

### Remediate and Maintain Software

to mitigate threats



PatchLink  
Update

### Assess Security Configurations

for compliance



PatchLink  
SCM

### Enforce Security Configurations

on all endpoints



PatchLink  
Developers Kit

### Enable Authorized Device Use/Behaviors

for all peripheral devices



Sanctuary  
Device  
Control

### Impose Authorized Software Use

for all applications



Sanctuary  
Application  
Control

# Case Study: John C. Lincoln Health Network



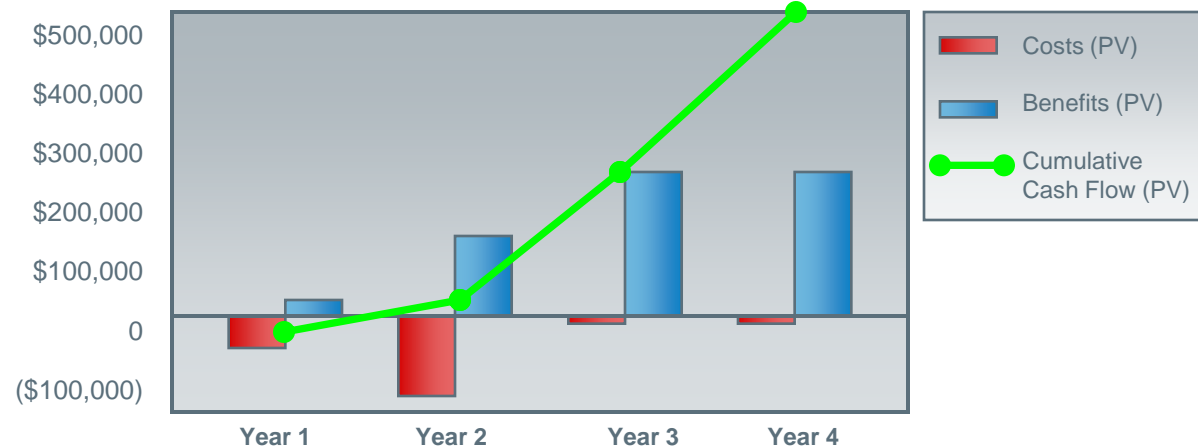
Table 1: Company ROI, Original and Risk-Adjusted

Summary Financial Results	Unadjusted (best case)	Risk-Adjusted
ROI (four year)	372%	365%
Payback*	16 month	19 months
Total four-year costs (PV)	(\$140,384)	(\$136,040)
Total four-year benefits (PV)	\$662,092	\$632,966
Total four-year net savings (PV)	\$521,709	\$496,926



\*Note: Payback would have been faster, had deployment not been spread out over two years.  
Source: Forrester Research, Inc.

Summary Financial Results, Risk Adjusted





# Moving From the Reactive to the Proactive Endpoint Security Model

Q&A

[www.lumension.com](http://www.lumension.com)

[carlos.sanz@lumension.com](mailto:carlos.sanz@lumension.com)