

Moving From a Reactive to a Proactive Security Model

Scott Van Horne
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 End-Point Security
 - A Positive, Proactive Approach





State of Endpoint Security Technology Market



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

So, with all this end-points should be secure, right?

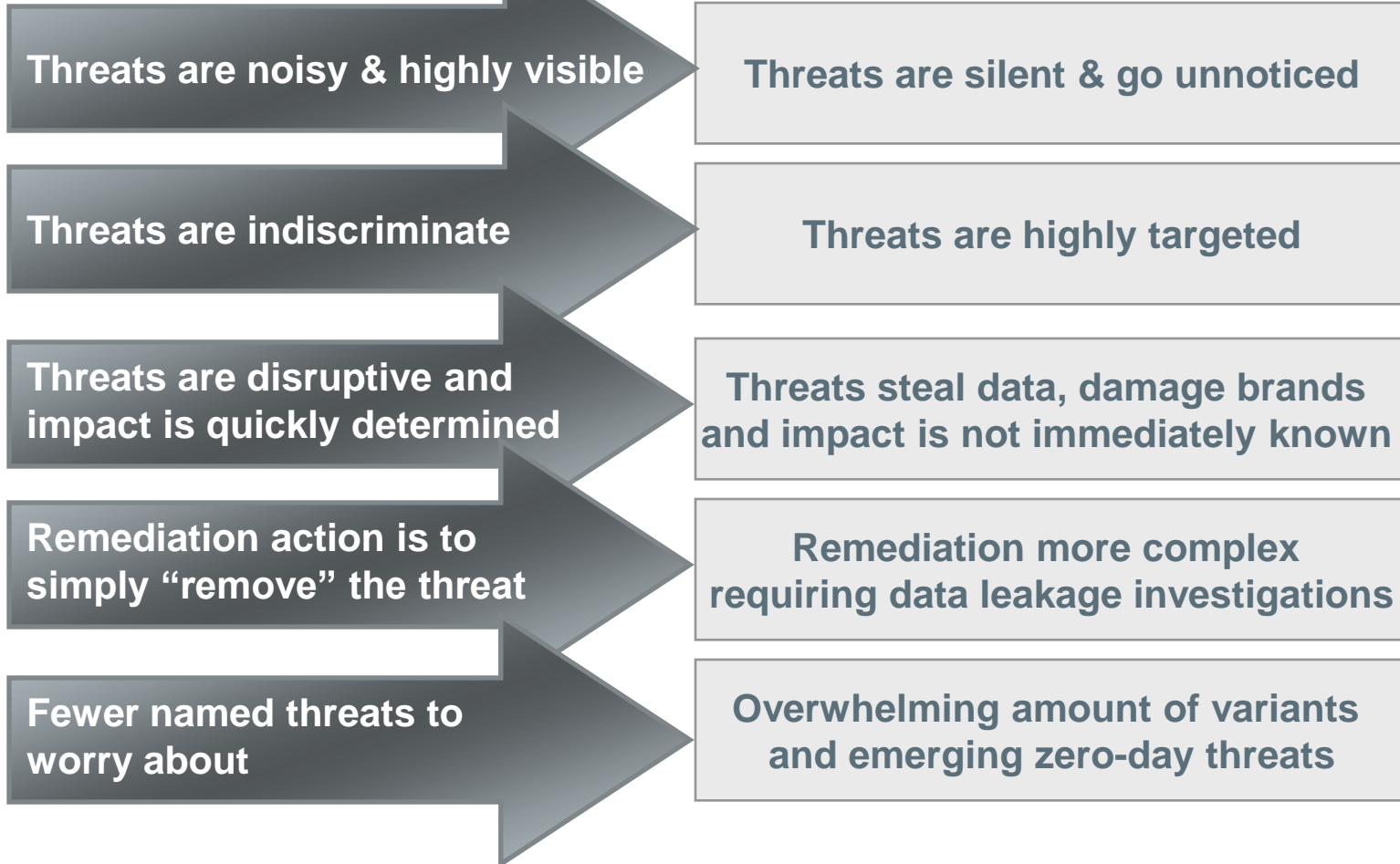
Security Landscape is Changing



Source: IDC

Old Landscape

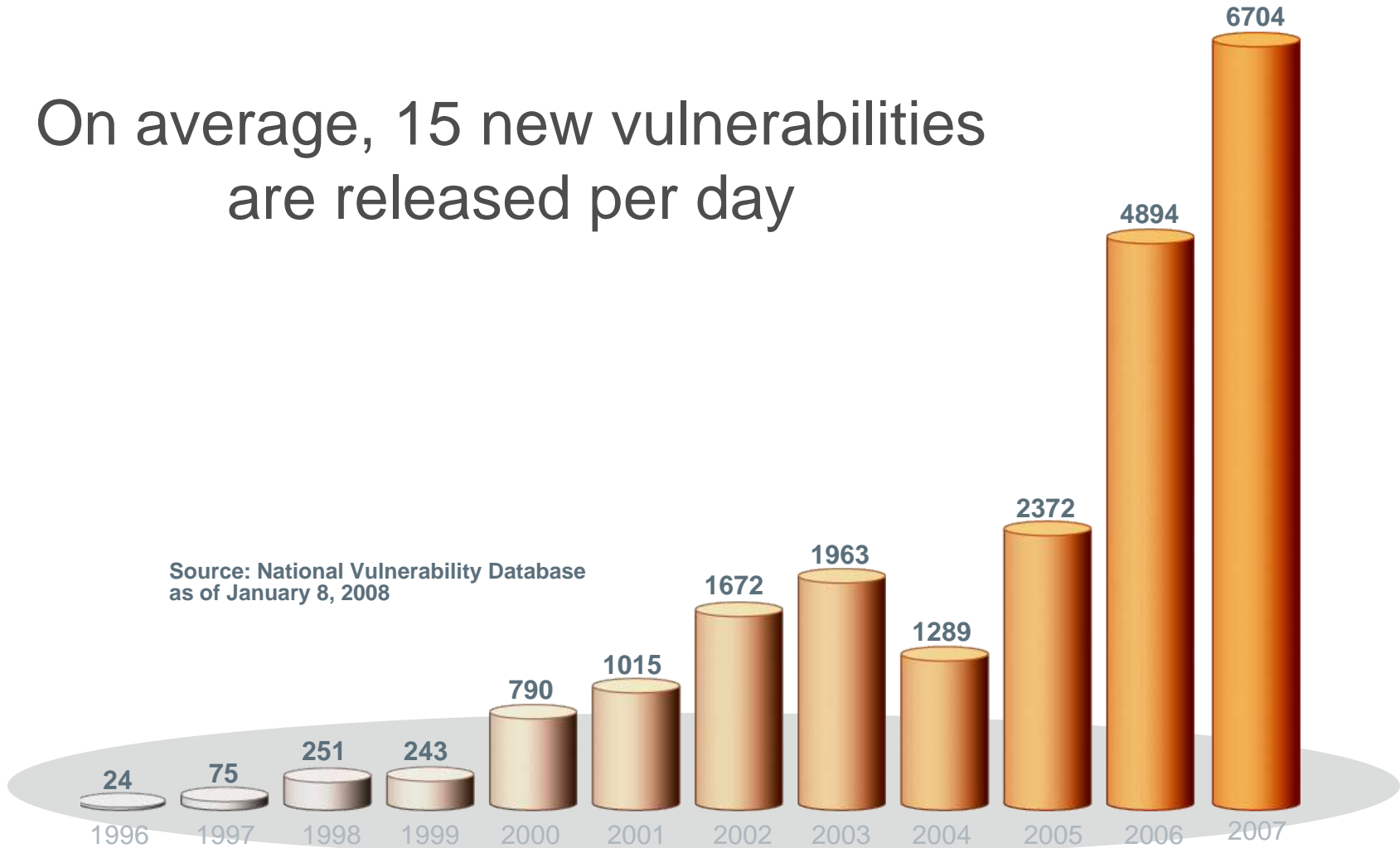
New Landscape



Each Day, the Problem Gets Bigger



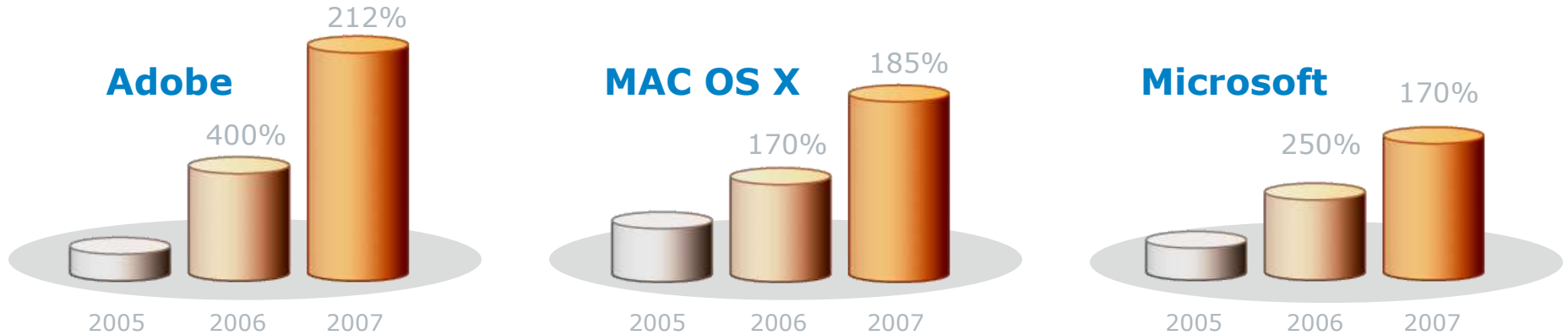
On average, 15 new vulnerabilities are released per day



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**



Hackers hijack Windows Update's downloader

May 10, 2007

COMPUTERWORLD

“Attackers are leveraging components and becoming more and more modular in how they create software. They’re simply following the trend of traditional software development.”

Like eBay for Malware: Computer Crime is

Slicker Than You Think

August 15, 2007

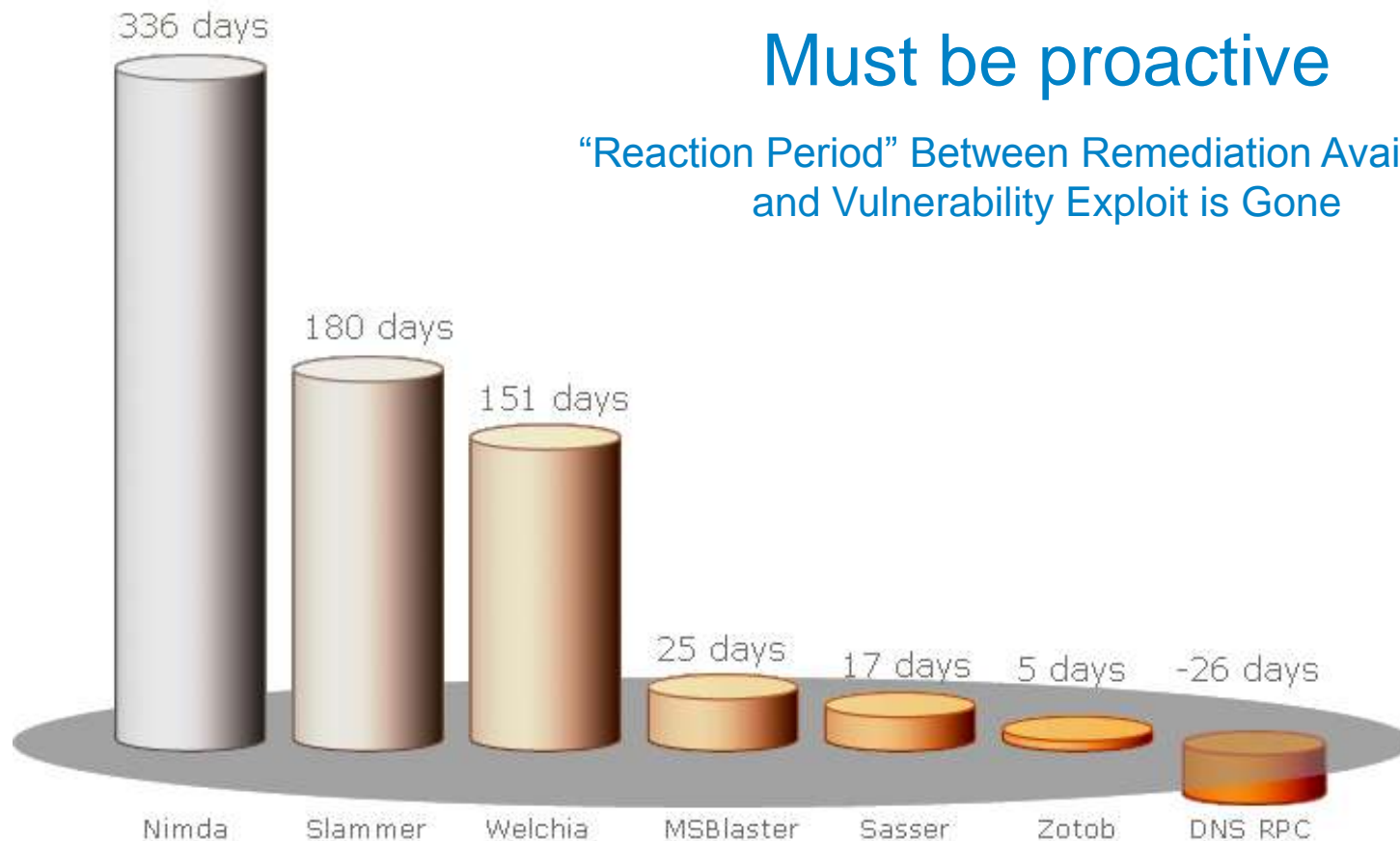
ChannelWeb NETWORK

If you want to break into a computer or steal credit card numbers, you can buy the necessary software online, just like almost anything else. More than that, you can find user friendly, point-and-click attack applications that have been pre-tested and reviewed by experts, and read through customer feedback before making your purchase.



Must be proactive

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





February 2007



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

www.av-comparatives.org

**Out of the 99% of enterprises
with AV/AS, 62% suffered an
infection 4**

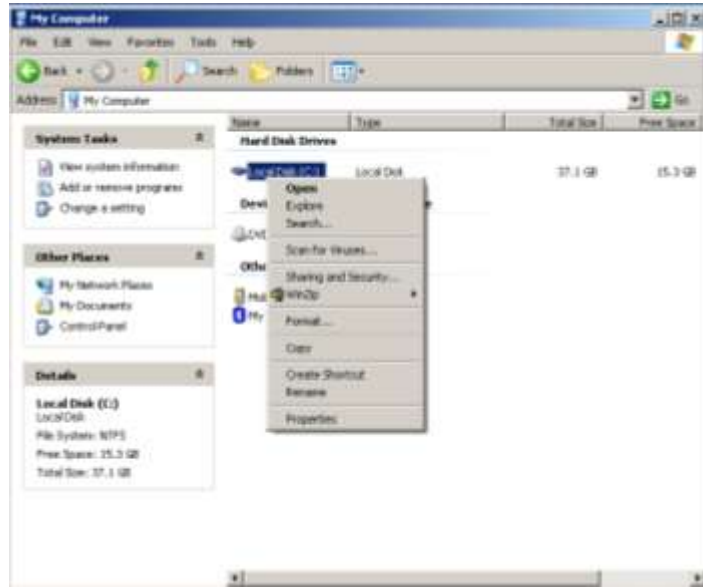
The largest viral database
had over 662,000 signatures
..... **HOW BIG IS BIG
ENOUGH?**

Total Detection Rates

Symantec
MISSED over 30,000 ...

McAfee
MISSED over 80,000...

Key Challenge – Data Loss is Exploding



Customer Secrets to Go!



- ▣ Endpoints are the likeliest entry point for malware ²
- ▣ 43% of firms reported laptops were most common source of worm attacks ³
- ▣ 75% of enterprises “will be infected with undetected, financially motivated, targeted malware that evaded traditional perimeter and host defenses.” ⁵
- ▣ The average loss from a data breach is \$167,713 per incident ⁶
- ▣ 75 percent of Fortune 1000 companies fell victim to data leakage ⁶



Sources:

1 – National Vulnerability Database

2 - Yankee Group, 2005 Security Leaders and Laggards Survey

3 – Enterprise Strategy Group

4 – www.av-comparatives.org

5 – Gartner Research, “Gartner’s Top Predictions for IT Organizations and Users, 2007 and Beyond,” Daryl C. Plummer, December 1, 2006

6 2006 CSI/FBI Computer Crime and Security Survey

Customer Impact - Compliance is Coming



20% of the 161 exabytes of data created in 2006 are subject to compliance guidelines

- ▣ Privacy legislation requiring that companies publicly disclose information security breaches to customers is also in effect in 31 states
 - Compliance experts expect that it will not be long before all 50 states have such laws in place
- ▣ Regulatory Compliance policies are become more specific
 - IT accounted for 5% of a SOX audit three years ago, but now accounts for about 30%
- ▣ Visa offers merchants and transaction services providers \$20 million in incentives to comply with PCI regulations











- Companies rebuild 85% of their laptops and desktops each year ¹
- Average enterprise downtime = 23 person days ¹
- Average time to achieve full recovery = 31 person days ¹

¹ Yankee Group

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”

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



Early Stage:
“Reactive”

Mature Stage:
“Proactive”

Policy Philosophy	Applications that require admin privileges are normal	With rare exceptions, applications run in user mode
Resources Access or Consumption	Running applications have access to most system resources	Protected memory and system resource access
Enforcement Approach	None: End-users demand admin privileges	Approved application list: run well w/ only user privileges
Cost Curve		



- ❏ 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 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

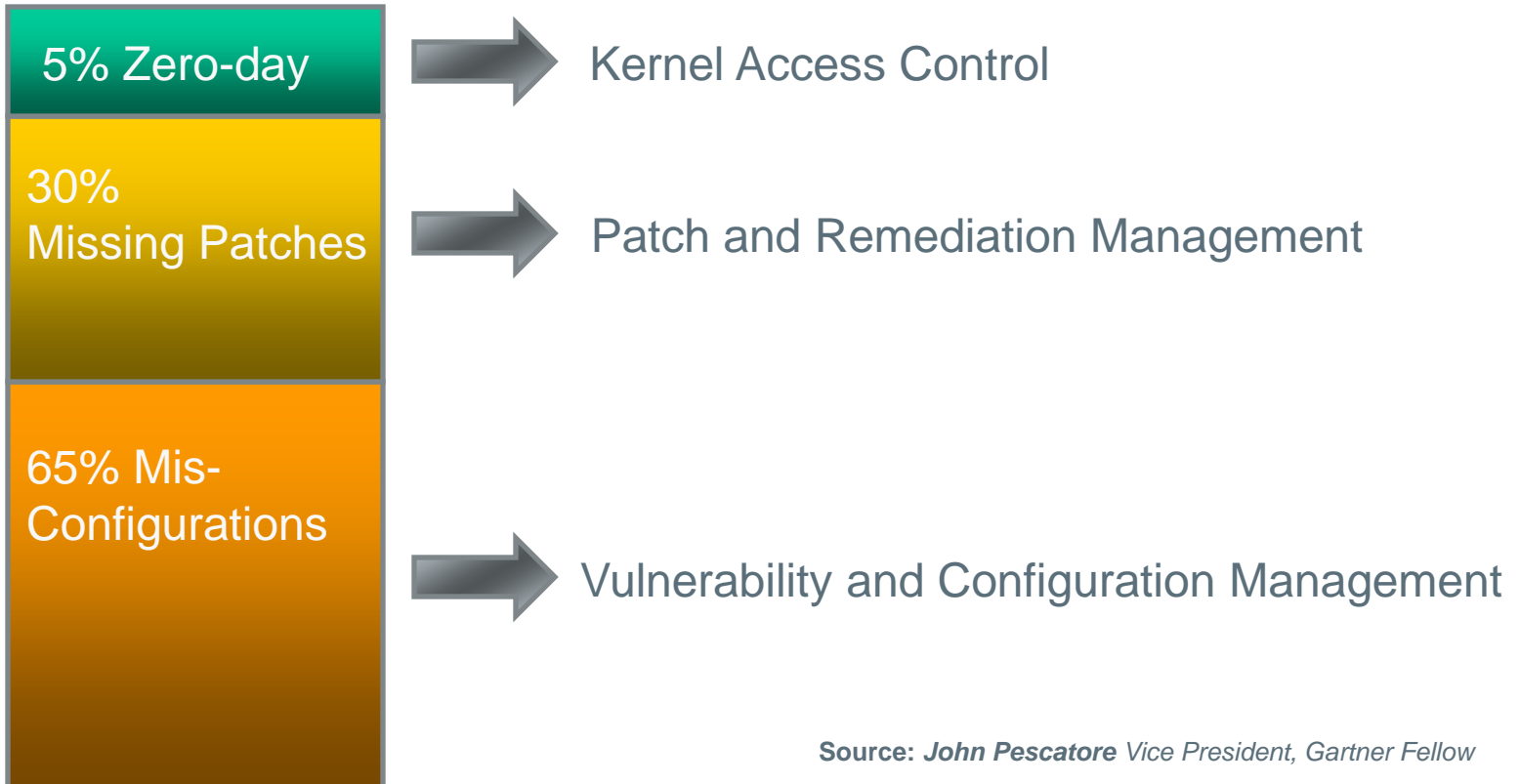


A New Age of End-Point Security

A Positive, Proactive Approach



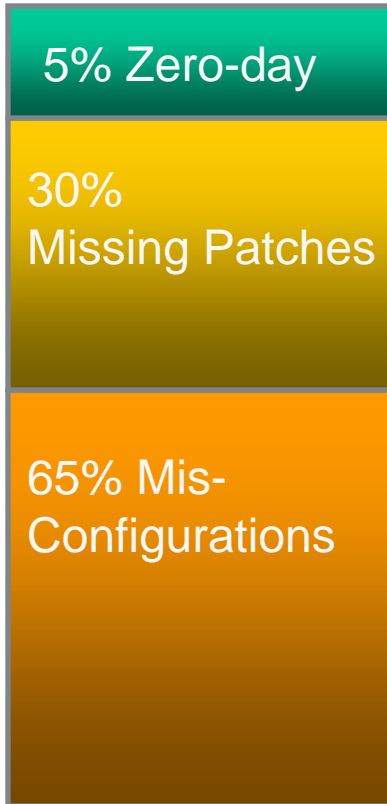
Attacks Exploit
Risks at the Core



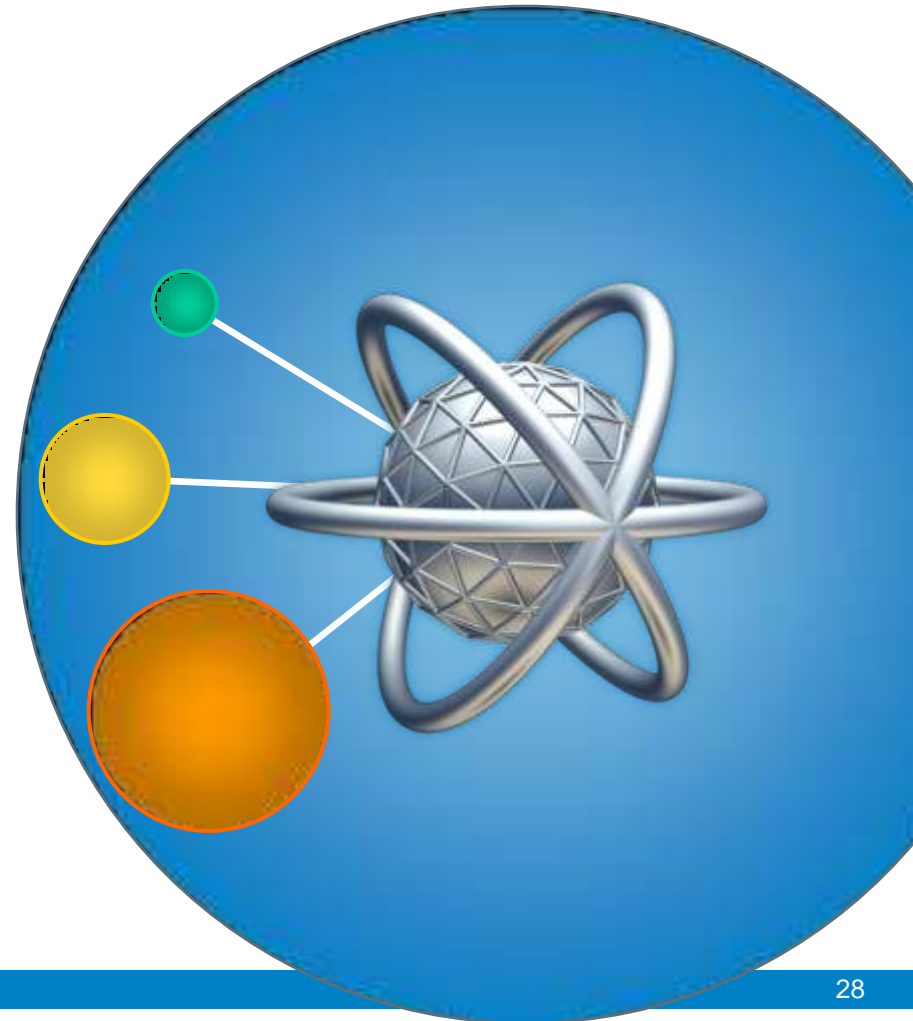
Source: *John Pescatore* Vice President, Gartner Fellow



Attacks Exploit
Risks at the Core



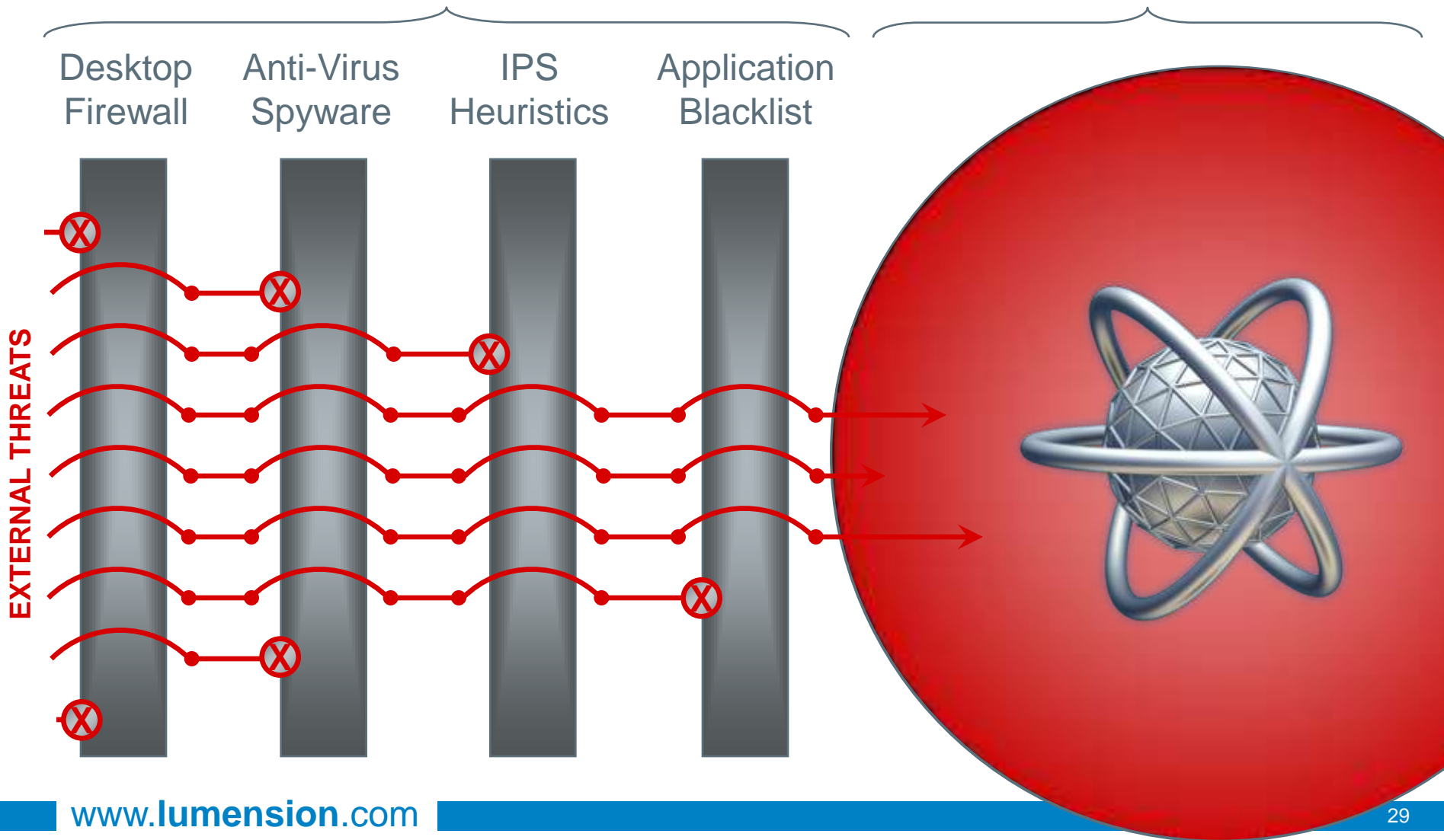
The CORE / Sources of Risk





Security Add-on Solutions

The CORE / Sources of Risk



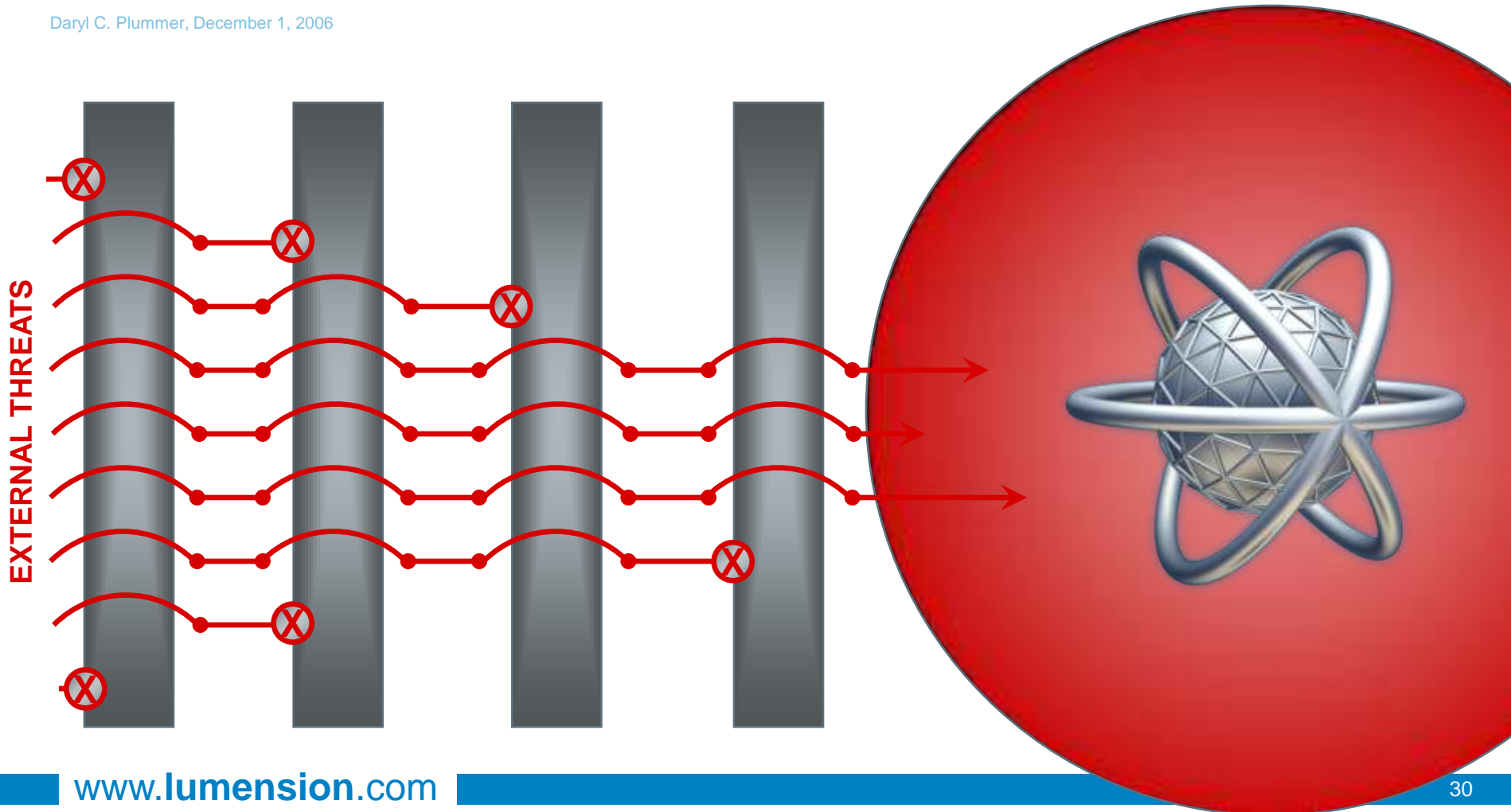
UPC – Traditional Approaches



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

Gartner Research, “Gartner’s Top Predictions for IT Organizations and Users, 2007 and Beyond,”

Daryl C. Plummer, December 1, 2006

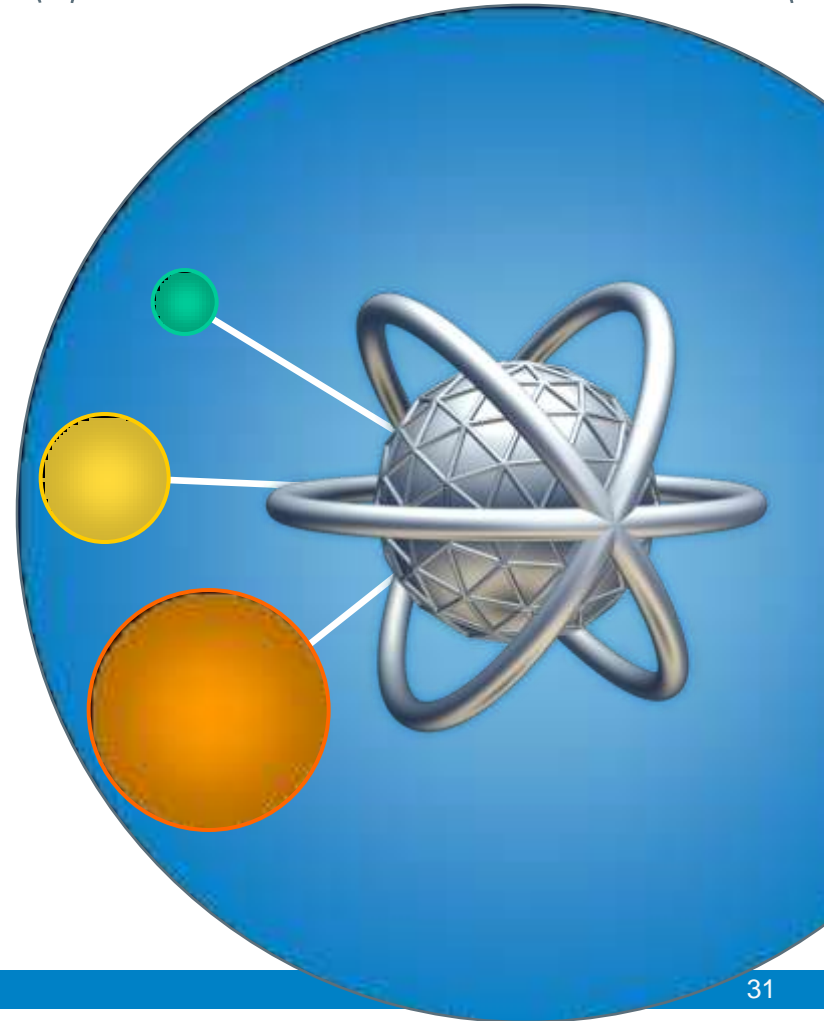




Sources of RISK

- Kernel Access Control
- Software Vulnerability
- Configuration Vulnerability

The CORE



UPC – Lumension’s Operational Approach



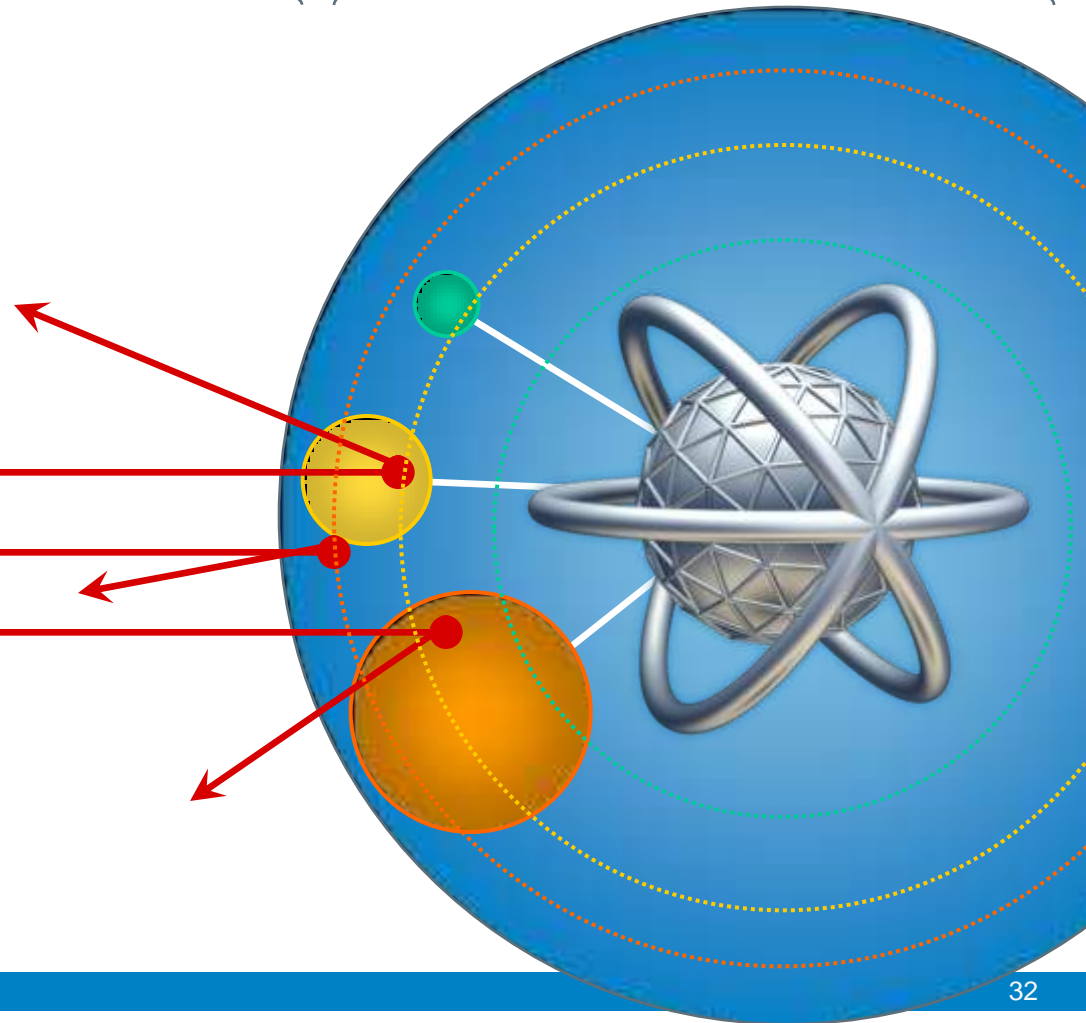
External Threats: Mitigate Risks at the Source

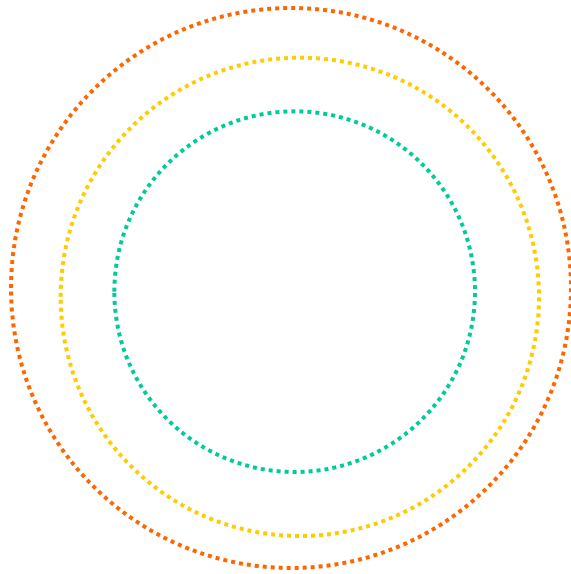
~~Business~~ **RISKY**

The CORE

- Application Control
- Availability
- Configuration

EXTERNAL THREATS





UPC – Lumension's Operational Approach



Internal Threats: Enforce Application & Device Use Policies

Machine Security

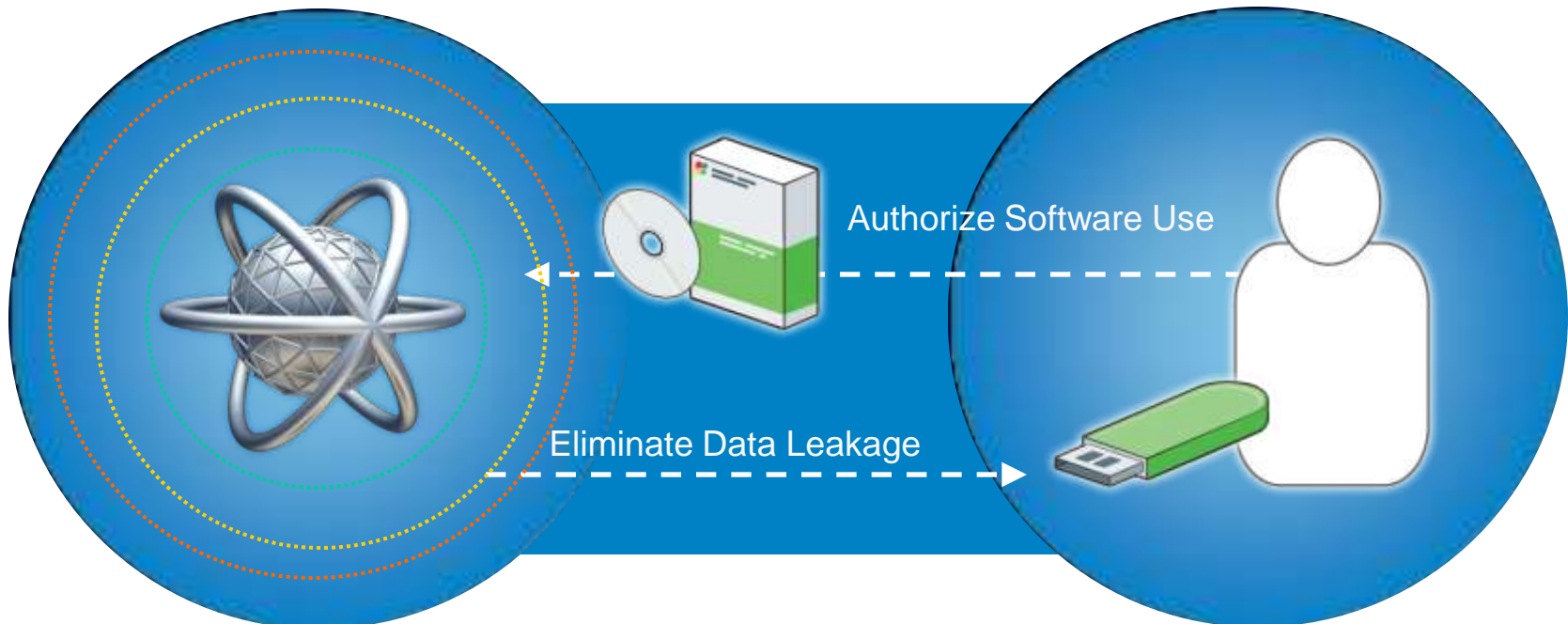
Application Control
Patch Management
Security Configuration
Device Control (Wireless – Future)

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



Moving From the Reactive to the Proactive Endpoint Security Model

Q&A

www.lumension.com

carlos.sanz@lumension.com