

# Reputation in the Cloud: Leveraging Reputation-based Services to Strengthen Your Security Posture

November 19, 2009

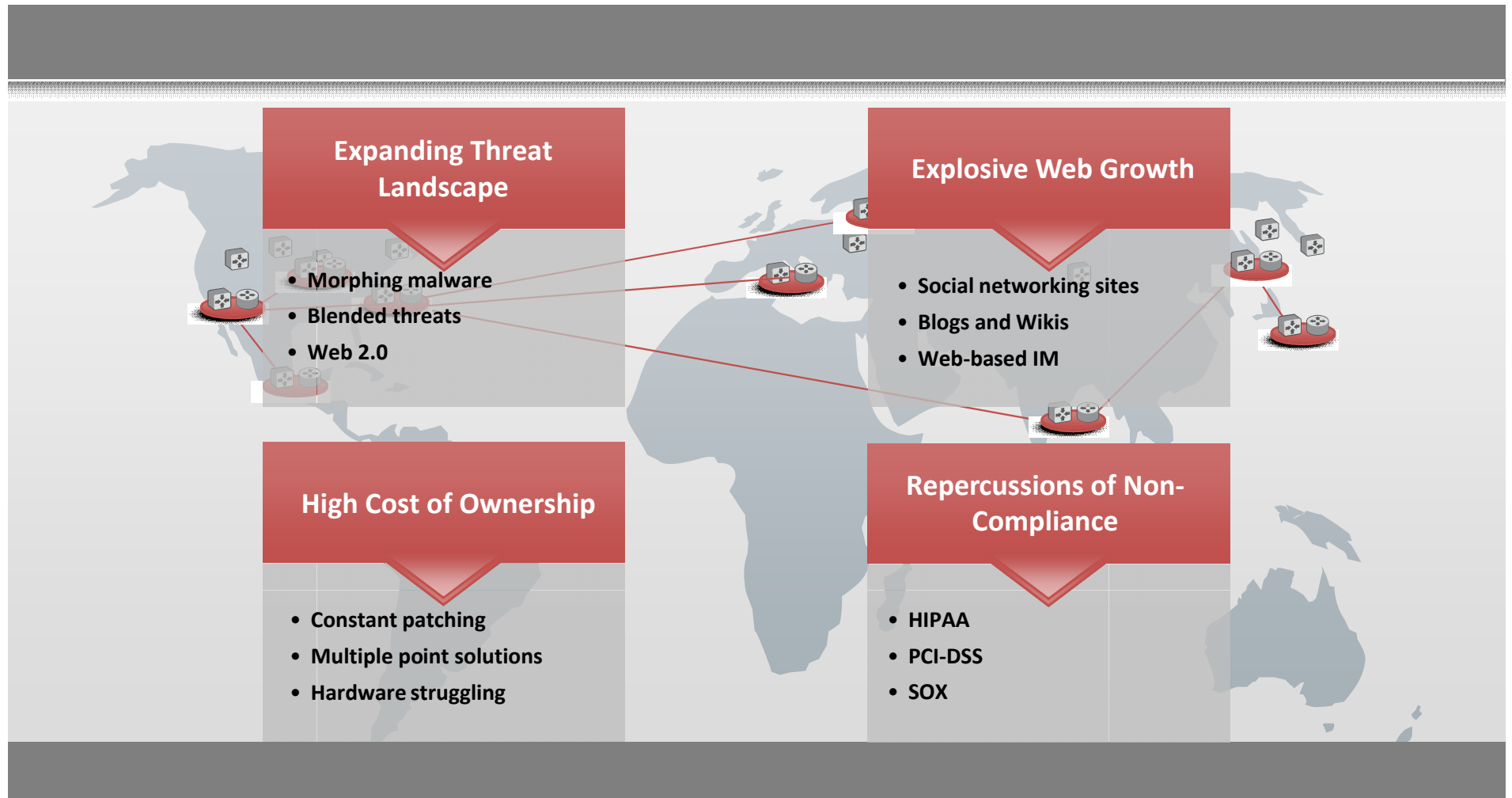
# About the Speaker

- Bryan Nairn, CISSP
- Over 12 years information security experience
- Security Engineering & Product Management
- WatchGuard Technologies

# Agenda

- Framing the Challenge
- Why Cloud-based Services
- History of Reputation Services
- Components of a Reputation Service
- How Reputation Improves Security
- Reputation Services Tomorrow

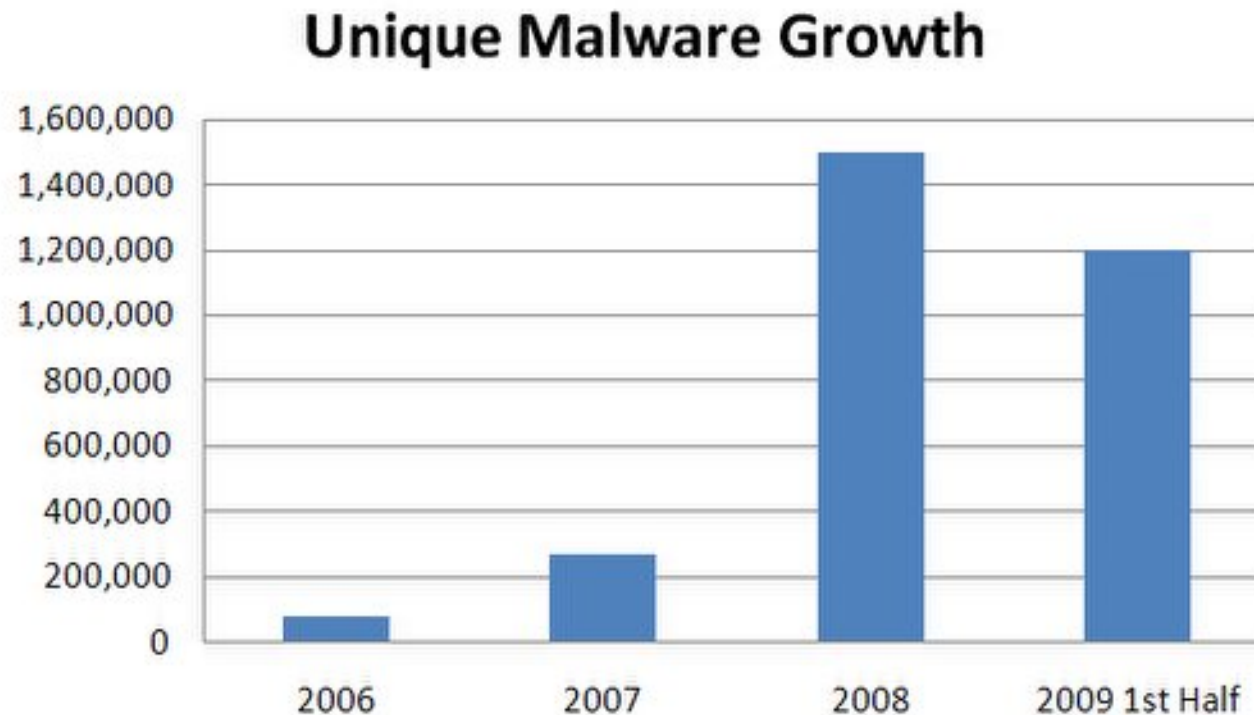
# What's creating pressure to move security into the cloud?



# Expanding Threat Landscape

Malware Volume is Out of Control

- Tripled first half 2009
- Server-side Polymorphism (packing and crypting)



# Expanding Threat Landscape

The Web is *THE* BattleGround

- Widespread Virus/Worms on the downturn
- Attackers move to greener pastures (the Web)
- Browsers consolidate many apps, large attack surface
- Web 2.0 and complex web apps increase risk
- Two-Stage Web attack
  - Exploit Web-app vuln to hijack web server
  - Exploit browser vuln or SocEng to hijack client
- Attackers automate web app attacks

# Explosive Web Growth

## Web 1.0 is Challenging

- 1 Trillion web pages
- 120M domains
- 450M authorities
- Public sites 25% CAGR
- 1M new domains daily

## Web 2.0 is Really Challenging

- Social networking
- User-generated pages
- Dynamic content
- Mash-ups

## The Internet of 2012 is Difficult to Imagine

- 5x as hard
- 3 Trillion pages
- 300M+ domains
- 1B+ authorities

# Explosive Web Growth

## Cyber Fraud

- ▶ Websites infected with malware increased to a staggering number of 166,000 in October 2007  
SANS Internet Storm Institute's Mark Hofman, Nov 2007
- ▶ 12 million bot-infected computers are being used to send spam  
Federal Trade Commission, July 2007
- ▶ 30% of mobile workers “hardly ever” consider security risks and proper behavior  
2007 National Cyber Security Alliance study
- ▶ 64% of enterprise users are not currently protecting their PDAs or smartphones from virus or spam threats  
Sophos User Study, Jan 2007

## Facebook Example

- ▶ Over 90% of Facebook’s most popular application have access to users’ private data, whether they need it or not!  
Dark Reading – Jan 31<sup>st</sup> 2008
- ▶ Facebook hit by 5 security problems in 1 week!  
PC World – Mar 3<sup>rd</sup>, 2009
- ▶ Application allows for hijacking of Facebook accounts  
Cnet – May 6<sup>th</sup>, 2009
- ▶ Widespread Facebook application installs adware – Secret Crush leads to unwanted advertising  
Sophos – Jan 1<sup>st</sup>, 2008

# How Can Cloud-based Reputation Services Help?

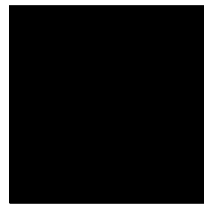
- Faster, more dynamic security
- Less infrastructure to manage and update
- Reduces bandwidth utilization
- Frees up security appliance work load
- Only pay for what you need
- Quick and easy deployment

# What is a Reputation Service?

- 50% - 80% Effective
- DNS Blacklisting (DNS BL) Only



- 70% - 80% Effective
- DNS BL + Volume



- 93% - 98.3% Effective
- DNS BL + Volume + Content Inspection + Behavioral Analysis



# How Are Reputation Services Deployed?

## Hosted Service

All request go through hosted service

- Small footprint
- No latency issues
- Most up to date data
- Customized local db

## Local Service

Local database cache and daily updates

- Real-time updates
- Limited connectivity
- Legacy migration path

## Hybrid Service

Local database and hosted service

- Best of both worlds
- Falls back to hosted
- No constraints
- High performance

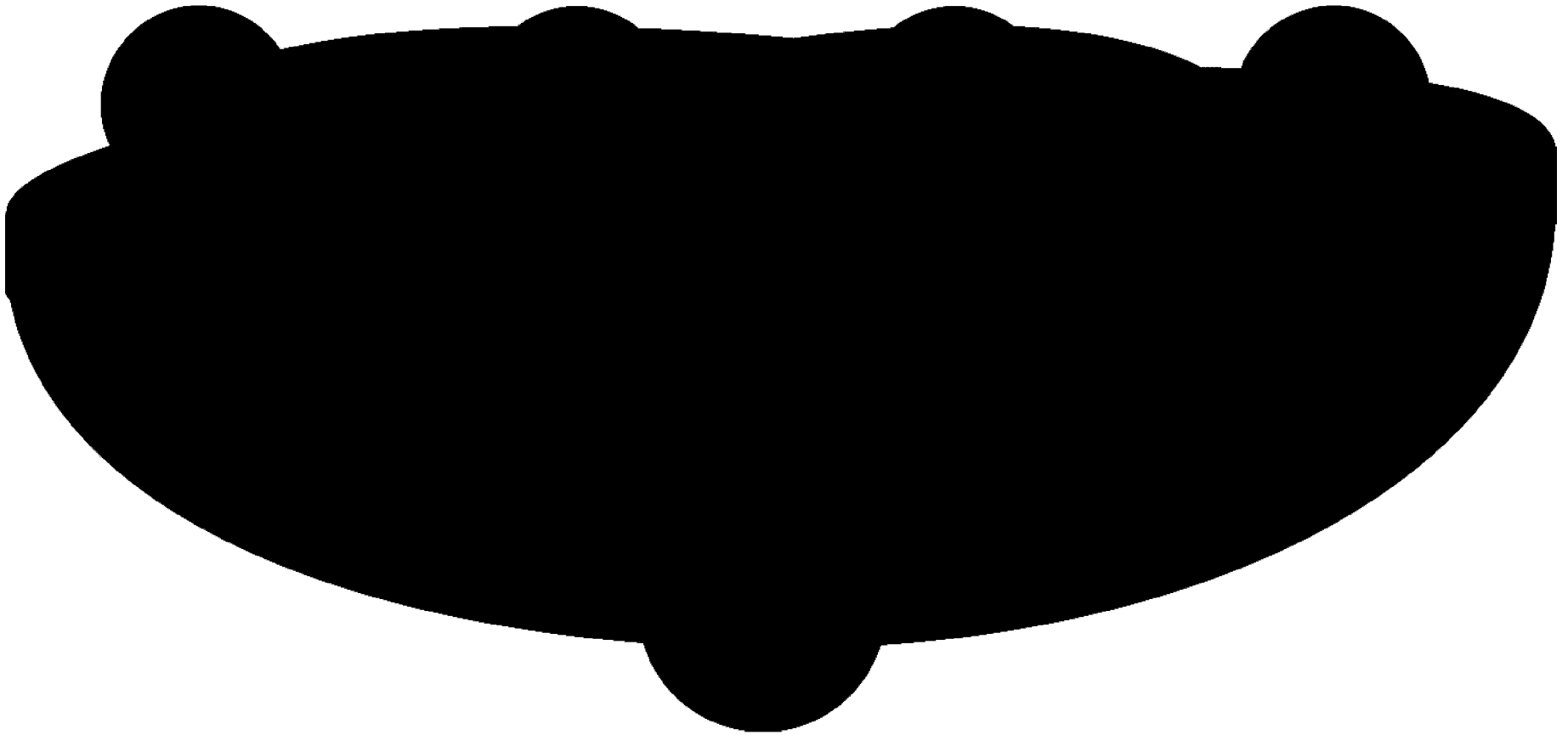
# What's In A Reputation Service

Threat Prevention

DNS Black List  
Clearinghouses

Behavioral Analysis

Customers



# Eliminate the Known: IP Reputation

- Historically Bad
  - Spammers
  - Categorized Web Sites
  - General Bad-Guys
- Credit Bureau Approach
  - Who and what is bad months and years ago
  - Not real-time, dynamic

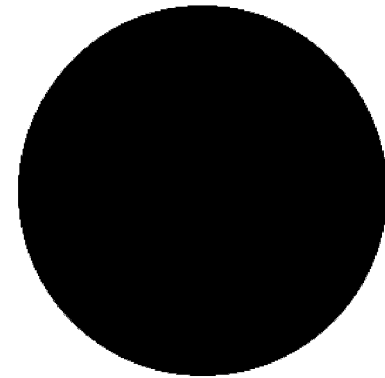
DNS Black List  
Clearinghouses



# Patented Intelligence: Content Analysis

- Domain & Sender Inspection
  - Proactive anti-phishing
  - Identifies new web pages to block malicious and inappropriate sites
- Sees the Big Picture
  - Rejects network attacks, such as DoS, DHA...
  - Identifies unknown recipients to reject spammer-probing

Threat Prevention

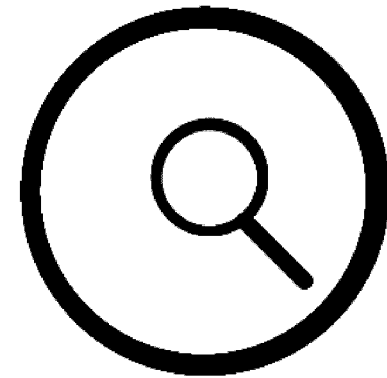


Content Analysis

# Leveraging Signatures: Behavioral Analysis

- Email Rejection
  - Examines embedded links
  - Inspects headers and content
  - Malware, Spyware and Spam signature scanning
- Web Rejection
  - URL Filtering
  - Malware, Spyware and Crimeware signature scanning

Behavioral Analysis

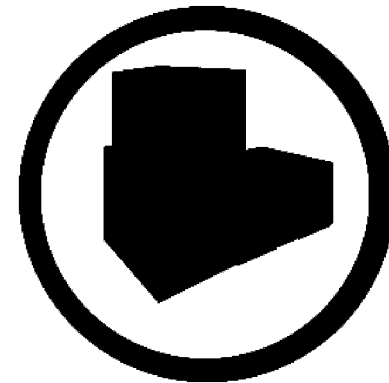


Real-Time Analysis

# Uniqueness: Contribution to the System

- Deep Content Inspection
  - Integration with email and web security appliances
  - Thorough inspection with threat prevention engines
- Auto Updates
  - Attacks first identified by one customer, real-time automatically rejects at the perimeter for all other customers
  - Ideal defense for BotNets

Customers

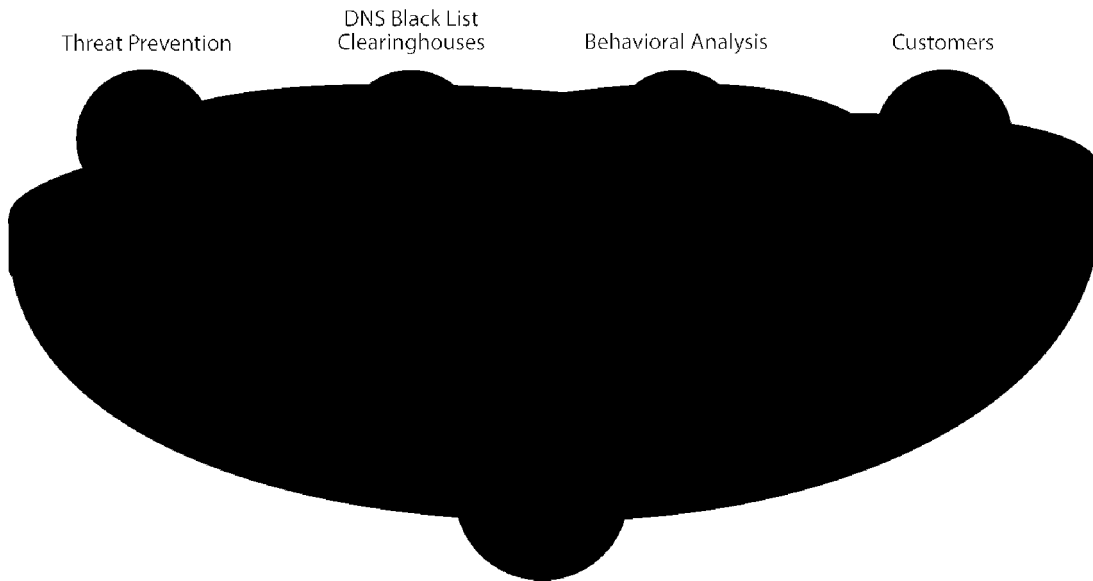


Instant Updating

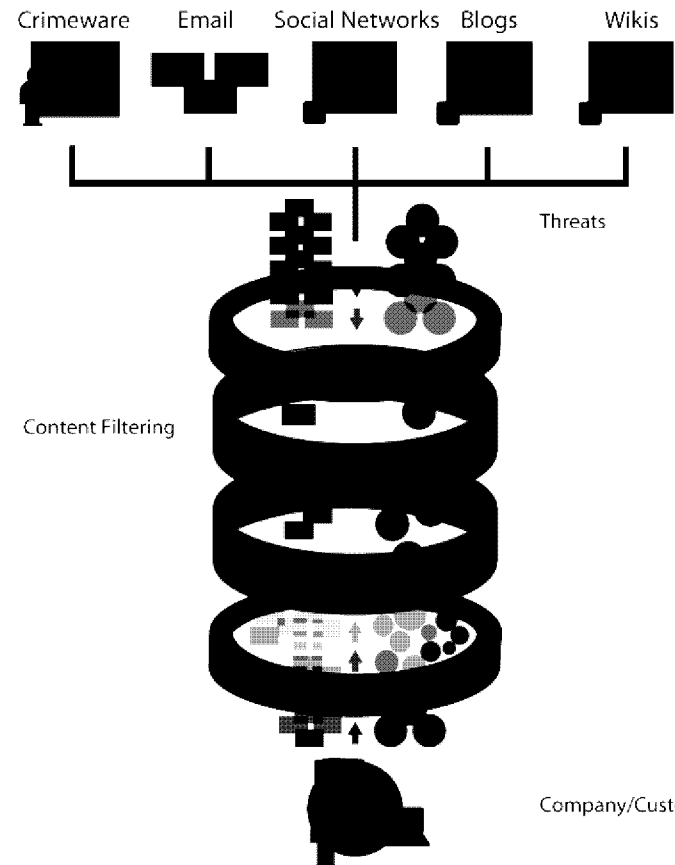
# Defense-in-Depth

## Leverage Reputation Services for Superior Security

### First Line of Defense



### Deep Content Inspection Added Protection for Spam and Malware



# How it Works

## (Email Example)

- Connection made to perimeter email security device
- Device waits until it receives the MAIL FROM<>
- Email security devices queries the reputation service with [user@example.com](#), 207.236.65.232
- Reputation service analyzes received data
- Reputation service returns score and a decision to reject is made

# How it Works

- Reputation Services can collect information from over 1 billion sources
  - Email, network and Web security devices send information back to reputation servers over port 443
  - 3<sup>rd</sup> party synchronizations, such as Spamhaus and Sorbs
  - Spam traps and honey pot domains
- Correlates all information together using content as the key driver in determining an overall reputation score

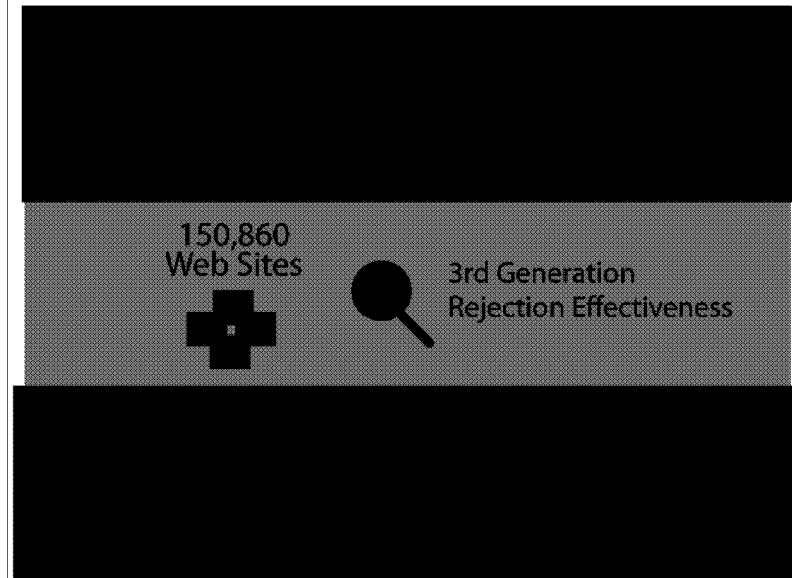
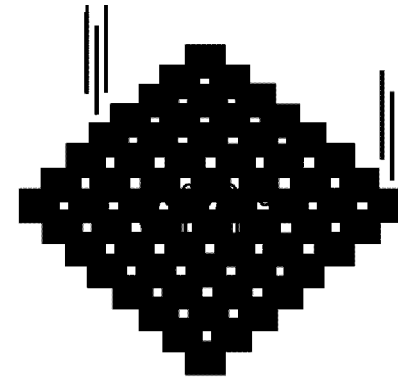
# Power of Email Reputation

- Did You Know...
  - More than 90% of email is spam
  - Email is now the delivery vehicle for
- Do the Math...
  - For every 100 emails, more than 90 are unwanted; nearly 89 are caught and rejected at the perimeter by a reputation service



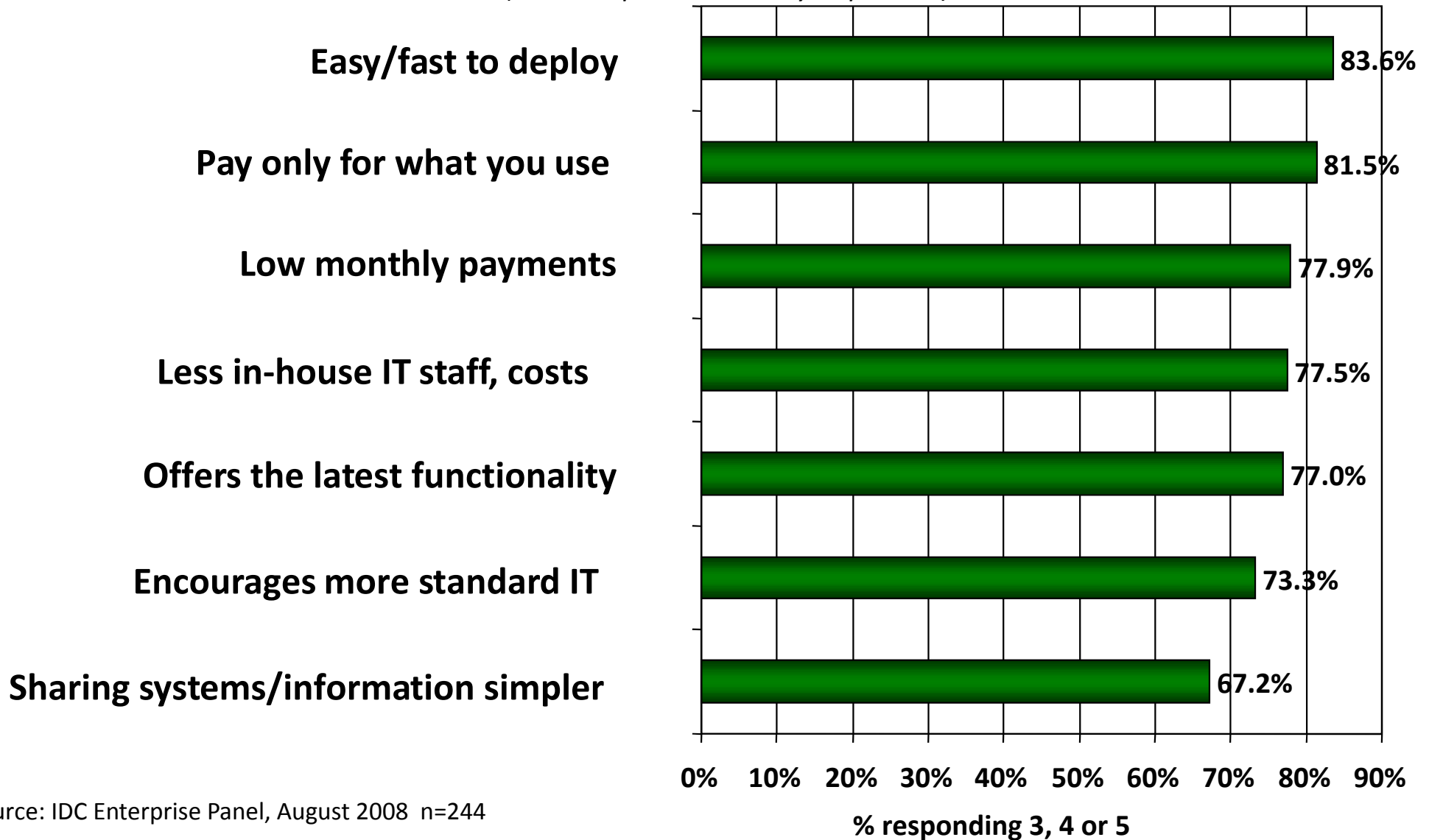
# Power of Web Reputation

- Did You Know...
  - The internet grows at a rate of nearly 40% annually
  - More malicious code is found on the web than in email
- Do the Math...
  - For every 100 web pages, more than 38 are unwanted; and 37 are identified and rejected at the perimeter by a reputation service



# Benefits of Moving to the Cloud

Q: Rate the *benefits* commonly ascribed to the 'cloud'/on-demand model  
(1=not important, 5=very important)



# Don't Take My Word For It

Related acquisitions in 2H'09

<b>WatchGuard Technologies</b>	Acquires BorderWare in August 2009
<b>Barracuda Networks</b>	Acquires Purewire in October 2009
<b>Cisco Systems</b>	Acquires ScanSafe in October 2009

# The Future of Reputation Services

## Today's Reputation Service

- Historical Data
- Content Inspection
- Behavioral Analysis
- Natural Feedback

## SDK Access for Everyone

- Outsource reputation
- Interface & structures
- New business models

## More Protocols and Applications

- Web 2.0 apps
- App awareness
- Rate limiting/hybrid



# Benefit Summary

<b>Greater Security</b>	<ul style="list-style-type: none"><li>• Access to the latest security software and updates</li><li>• Feedback loop means cloud gets smarter</li><li>• Easy to add functionality within updating CPE</li></ul>
<b>Cost Savings</b>	<ul style="list-style-type: none"><li>• Only pay for what you use</li><li>• Reduce unwanted bandwidth hitting the network</li><li>• Alleviate security appliance work load</li></ul>
<b>Easy-to-use</b>	<ul style="list-style-type: none"><li>• Easy rollout and integration</li><li>• No need for multiple point products</li><li>• Eliminates need for specialized knowledge</li></ul>

**Questions?**