



**SYMANTEC
ENGAGE
HONG KONG** **2010**

Symantec Protection Suite The New Complete Protection for Enterprise

John Bai

Senior Manager, Security Technology & Response



Security Technology And Response

Primary Areas of Oversight

- **Technology**

- Oversees R&D of security technologies across Symantec products
- Malware Engines: Antivirus, Antispyware, Intrusion Prevention, Behavioral and Heuristic Engines
- New technologies: Whitelisting, Reputation-based security, etc.
- Common components: Common Client, LiveUpdate, Decomposer, etc.

- **Content**

- Security updates for new threats across all products
- Signatures for all threat classes (e.g., spyware, adware, viruses, spam, etc.)
- 24/7 global support for customer threat issues

- **Infrastructure**

- Infrastructure to streamline all Response support operations (customer issues, sample processing, etc.)
- Global data feeds (DeepSight, etc.)

- **Visibility**

- Response website, weblog, publication of malicious trends, global PR, etc.



Cyber security

2009 by the numbers

3,200,000,000

attacks blocked by Symantec in 2009

- 12 new 0day vulnerabilities
- 14 new public SCADA vulnerabilities
- 321 browser plug-in vulnerabilities
- 4,501 new vulnerabilities
- 17,432 new bot C&C servers
- 30,000 domains hosting malware
- 59,526 phishing hosts
- 2,895,802 new AV signatures
- 6,798,338 bot infected computers
- 73,000,000 new malware variants

in the time it takes to give this presentation
we will block more than 500,000 attacks!

we will block more than 200,000 attacks!

Threat Landscape

A fundamental shift...



Old Motivation

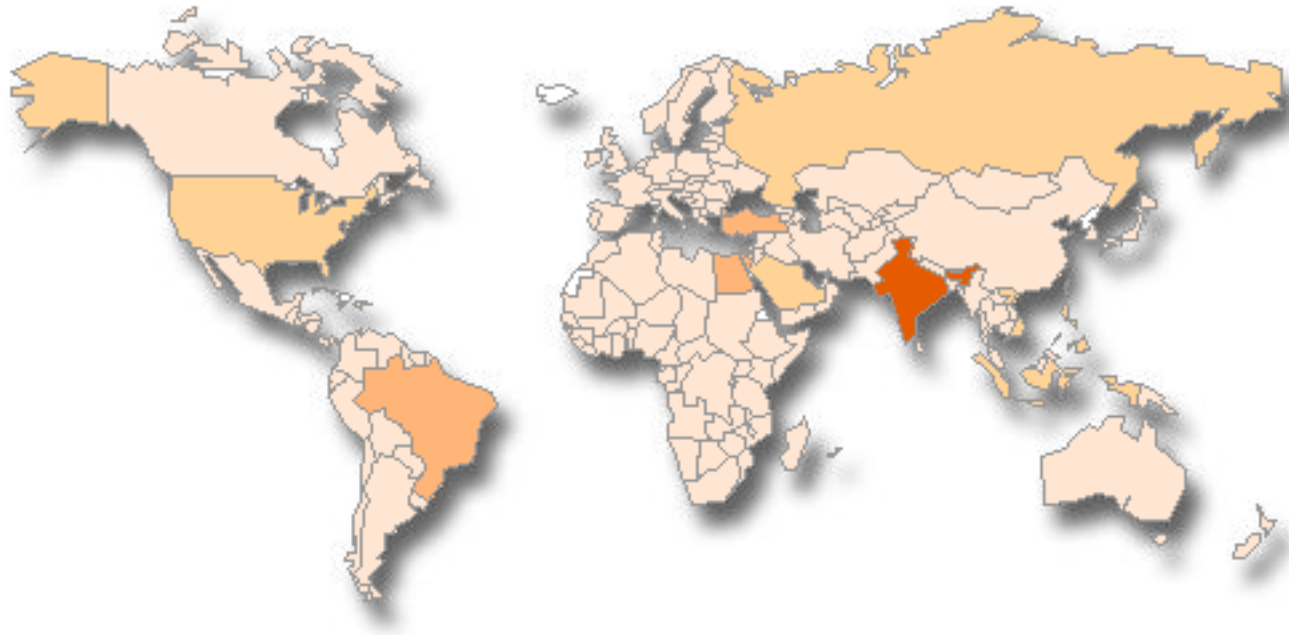
Hacking

Cyber Crime

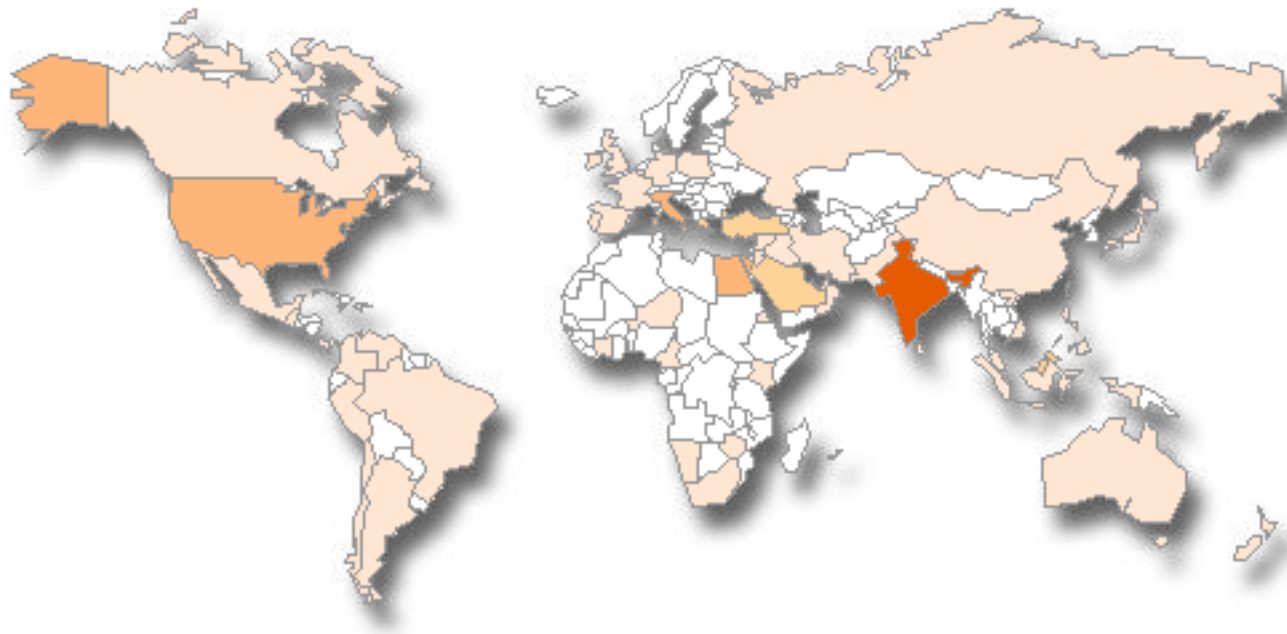
Cyber Espionage

Cyber Warfare

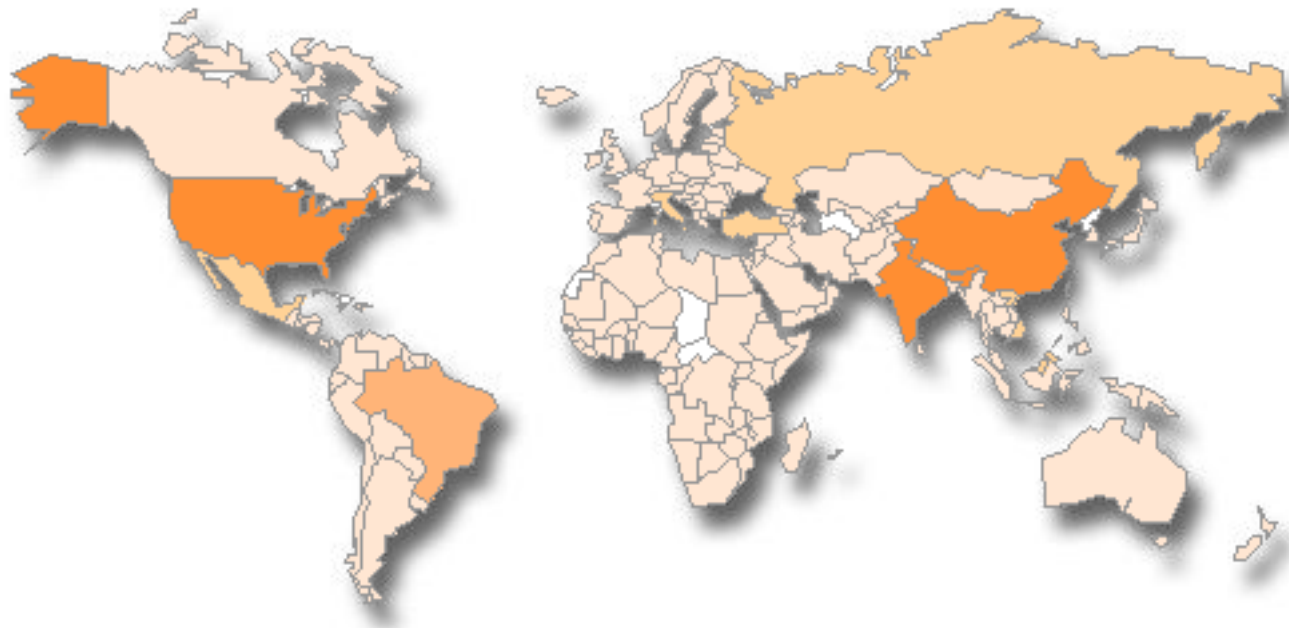
W32.Sality Infection 'heat map'



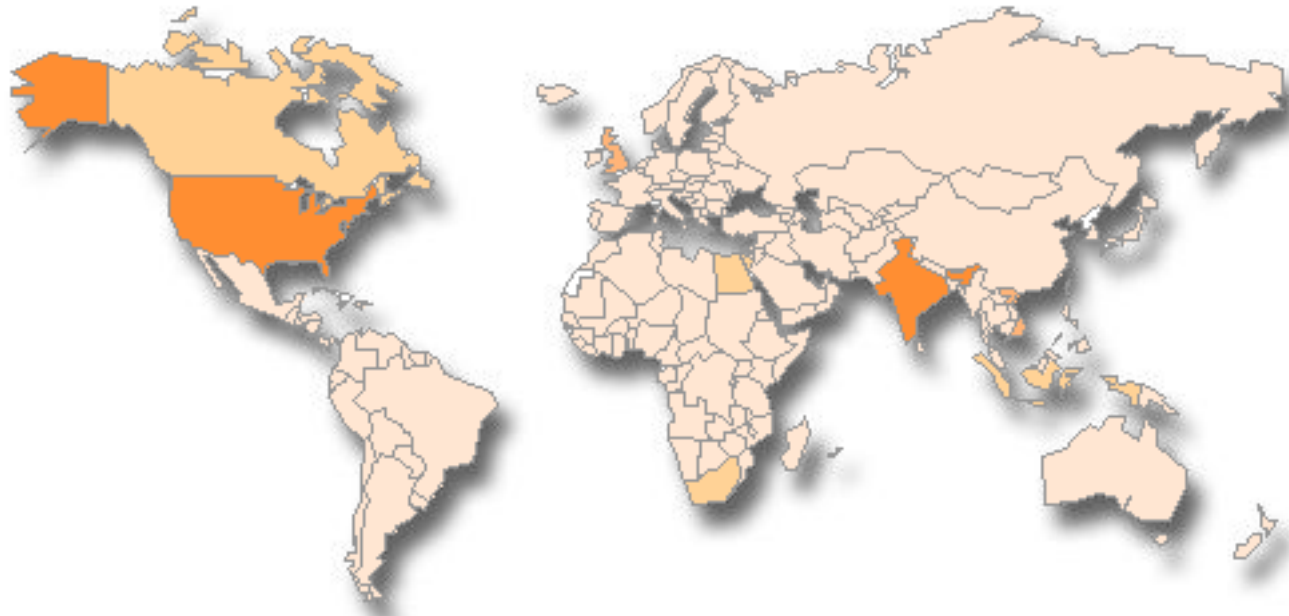
W32.Blackmal (aka Kama Sutra worm) 'heat map'



W32.Downadup (aka 'Conficker worm) 'heat map'



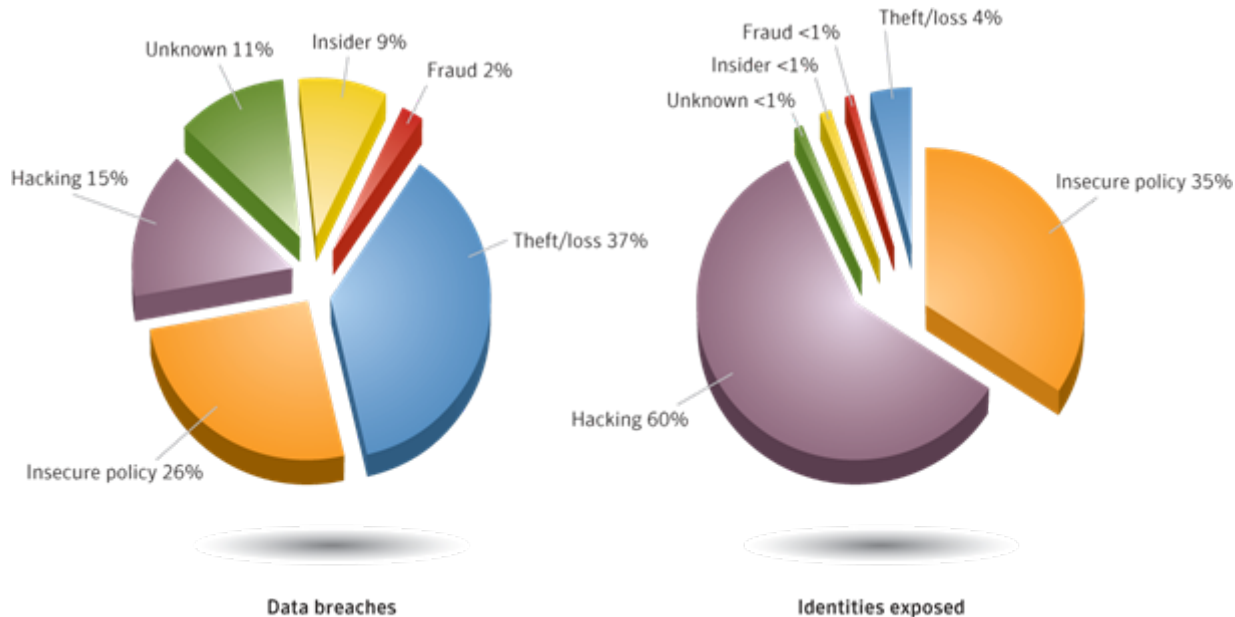
W32.Virut 'heat map'



Threat Landscape

Targeted attacks focus on enterprises

- Frequently carried out by Advanced Persistent Threats (APTs).
- These threats remain undetected to penetrate deeply into the network.



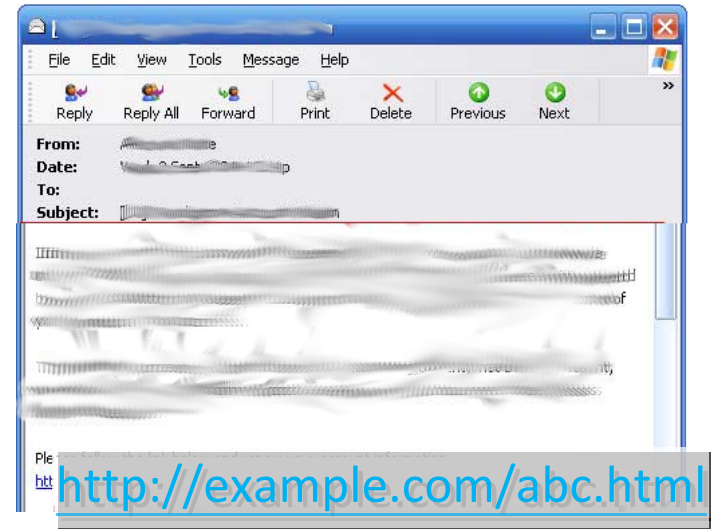
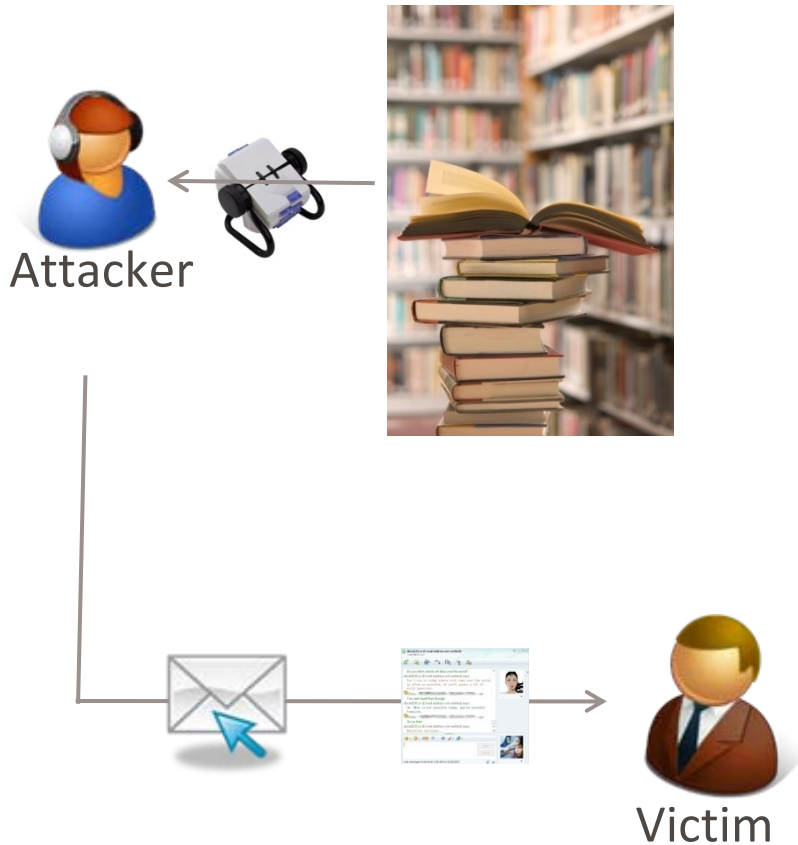
Targeted Attack Methodology

Mass Attacks vs. Targeted Attacks

Phase	Mass Attack	Targeted Attack
Incursion	Generic social engineering By-chance infection	Handcrafted and personalized methods of delivery
Discovery	Typically no discovery, assumes content is in a predefined and predictable location	Examination of the infected resource, monitoring of the user to determine additional accessible resources, and network enumeration
Capture	Predefined specific data or data which matches a predefined pattern such as a credit card number	Manual analysis and inspection of the data
Exfiltration	Information sent to a dump site often with little protection and dump site serves as long term storage	Information sent back directly to the attacker and not stored in a known location for an extended period

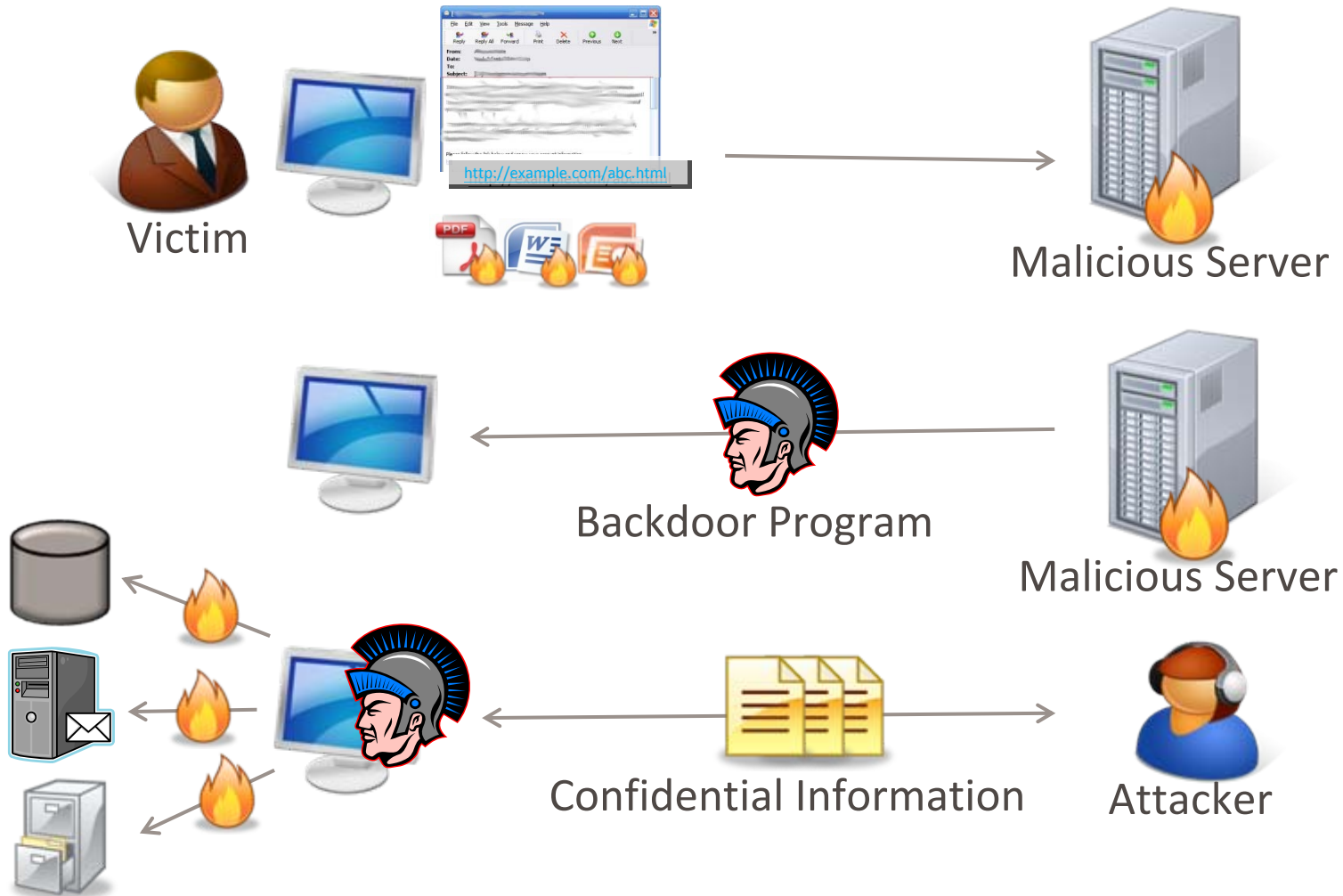
Targeted Attack Methodology

Social Engineering

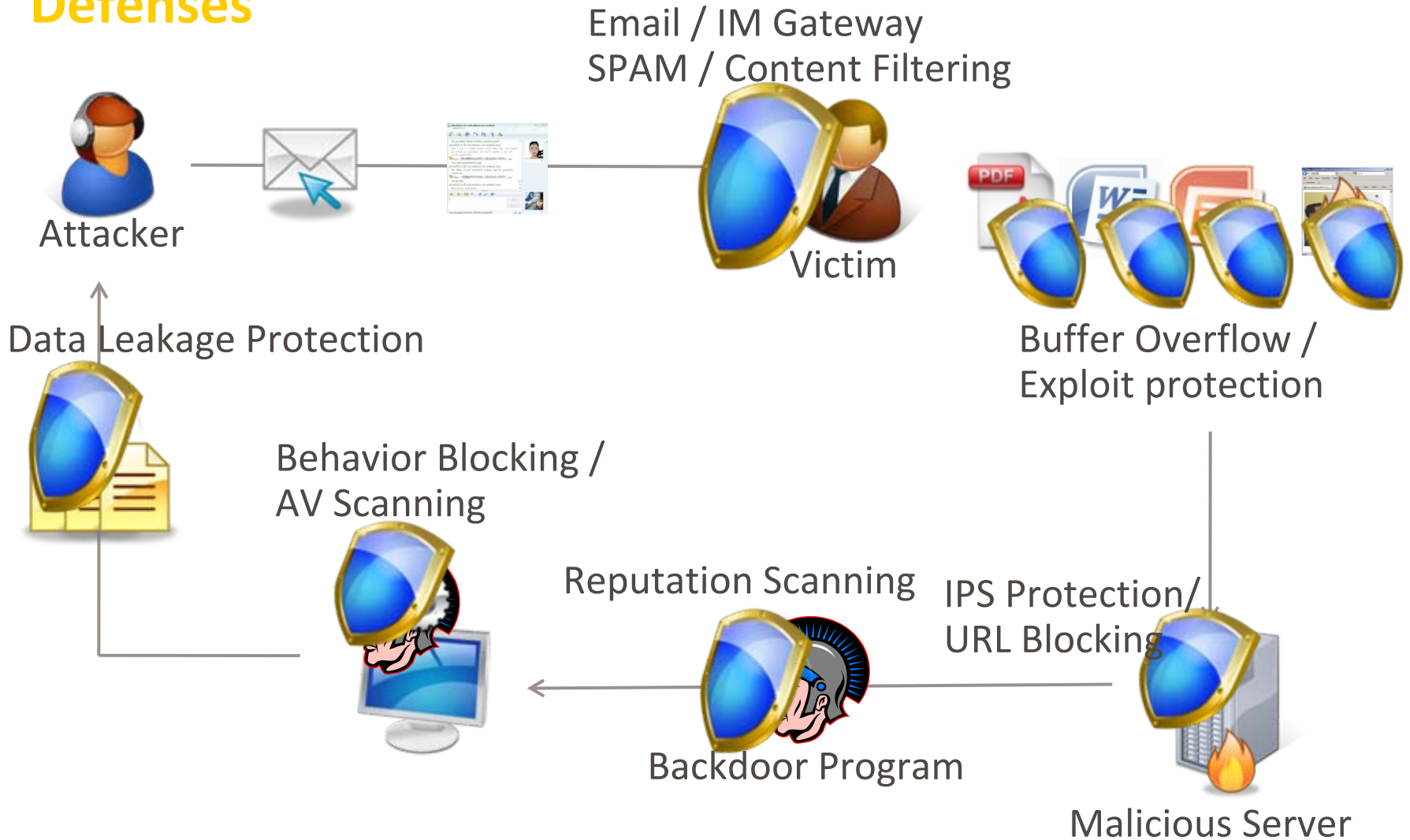


Targeted Attack Methodology

Payload Install and Execution



Defenses



Comprehensive Security Strategy is Required



Risk Based and Policy Driven

IT Governance, Risk and Compliance



Information - Centric

Information Risk Management



Operationalized

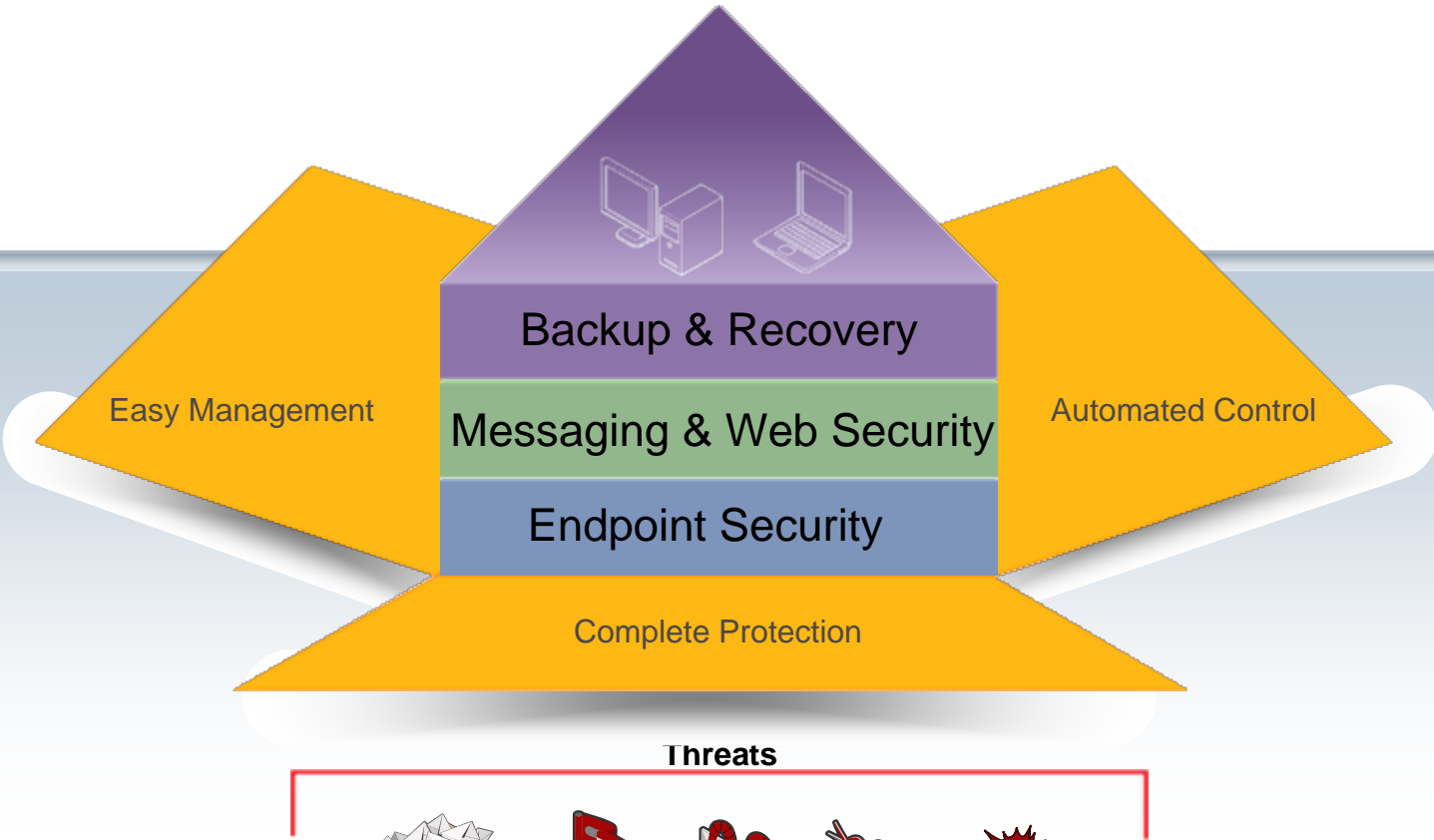
Infrastructure Management



Well Managed Infrastructure

Infrastructure Protection

Symantec Protection Suite



Backup & Recovery

- Backup live desktops & laptops
- Restore to any hardware
- Take threat-driven backups

Messaging & Web Security

- Antivirus, antispam, antiphishing, botnet protection
- Reputation-based spam filtering
- Data loss prevention
- Exchange, Domino, Gateway

Endpoint Security

- Antivirus, antispyware
- Desktop firewall
- Intrusion prevention
- Device and application control
- Network access control

Complete Protection

- Protect from endpoint to gateway
- Proven technologies
- Protect against more threats
- Safeguard intellectual property
- Rapidly recover with ease
- Rely on trusted research

Easy Management

- Simplify implementation & operations
- Streamline management
- Flexible and scalable configuration
- Eliminate environment complexity
- Reduce operational costs

Automated Control

- Ensure compliance
- Regulate sensitive information
- Effortlessly update
- Increase visibility
- Minimize downtime



Symantec Recommends

Four Pillars of Information Security Protection

Protect the Infrastructure

- Secure endpoints
- Protect email and Web
- Defend critical internal servers
- Backup and recover data

Protect the Information

- Discover sensitive information
- Monitor how data is being used
- Protect sensitive information from loss

Develop and Enforce IT Policies

- Define risk and develop IT policies
- Assess infrastructure and processes
- Report, monitor and show due care
- Remediate

Effectively Manage Systems

- Implement secure OS
- Distribute and enforce patches
- Automate processes to streamline
- Monitor and report on status

Symantec Global Intelligence Network

Monitor, Analysis, Protection, 24 x 7 x 365

Relevancy

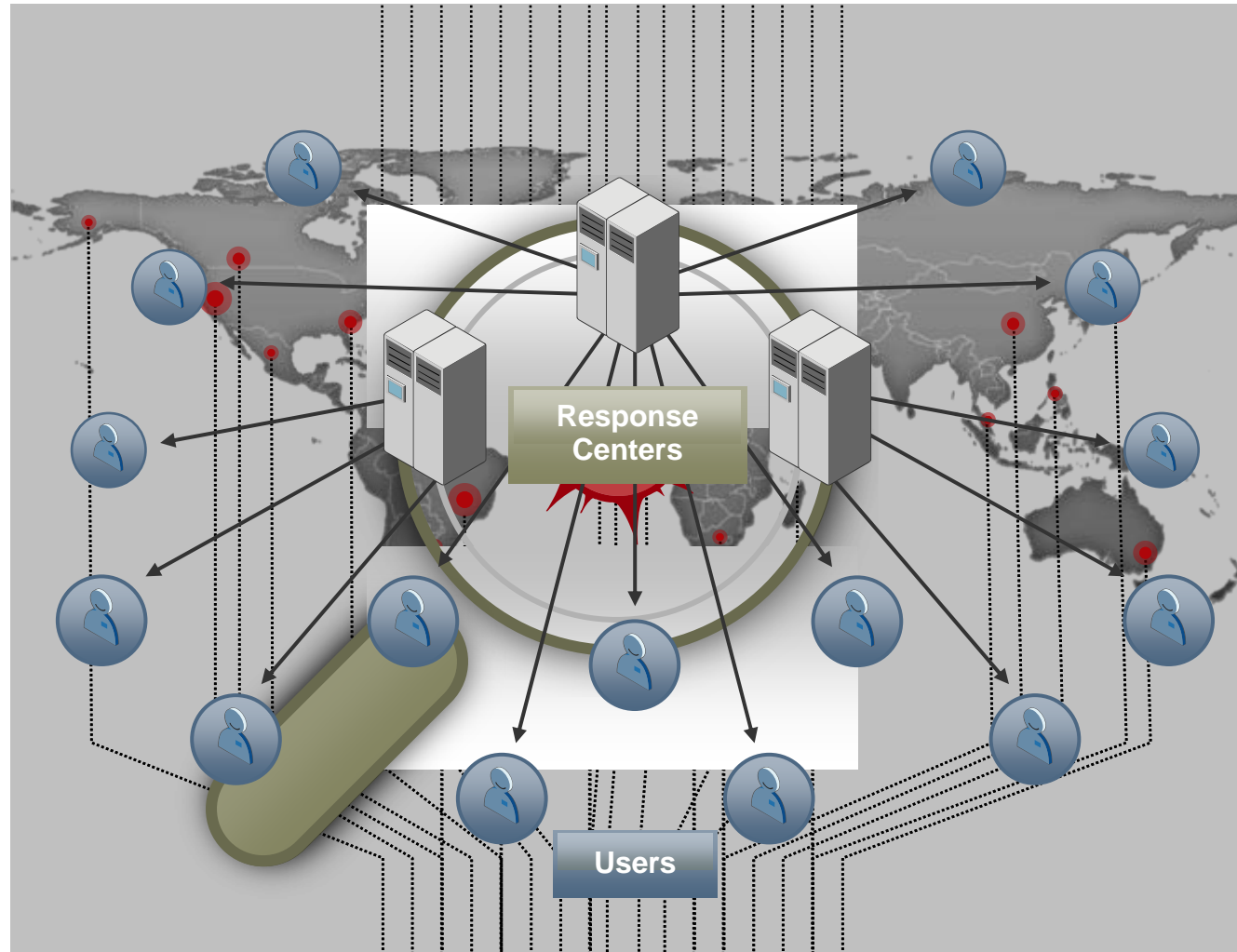
- Global Expertise
- More researchers
- Comprehensive data sources
- More virus samples analyzed
- Extensive customer support

Accuracy

- In-depth Analysis
- Signatures: AV,AS,IPS,GEB, SPAM, White lists
- DeepSight Database
- IT Policies and Controls
- Rigorous False Positive Testing

Protection

- Automated Updates
- Fast & Accurate
- Variety of Distribution Methods
- Relevant Information





Questions?



Thank you!

John Bai

Senior Manager, Security Technology & Response

john_bai@symantec.com

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.