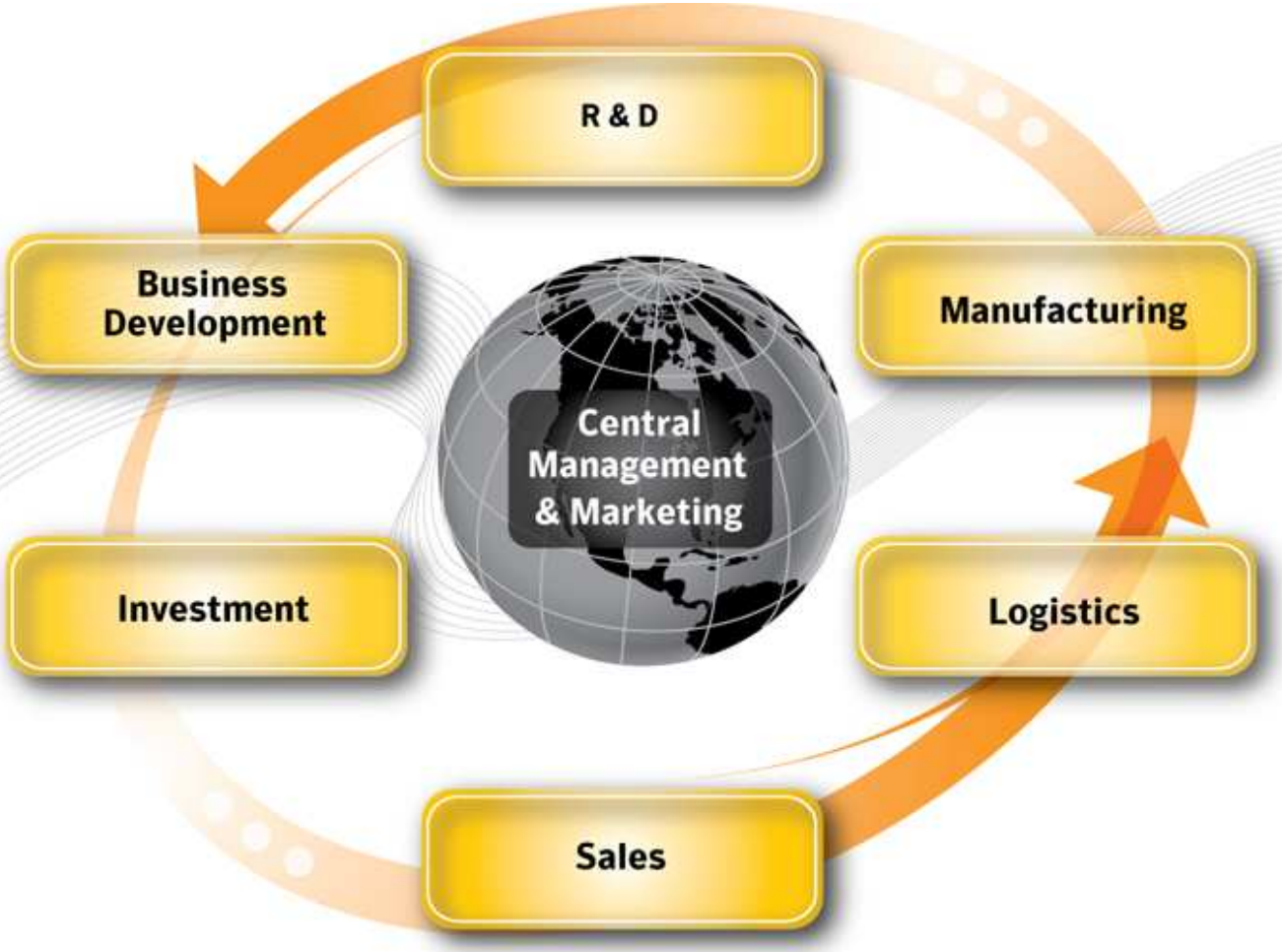
Confidence in a connected world.

Restricción y evidencia en la Web 2.0

Miguel Suárez / Alfredo Reino

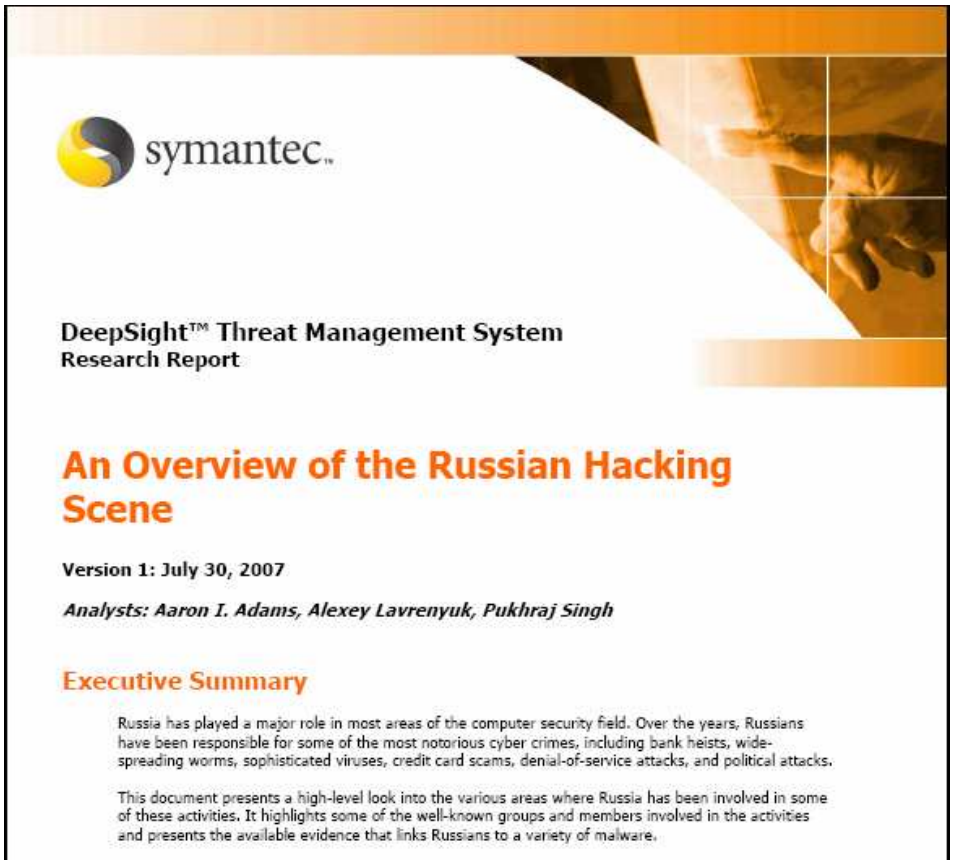
Symantec Iberia

Modelo de Negocio de Hoy



Modelo de Negocio del Cybercrimen

Los escenarios Ruso y Chino



symantec.

DeepSight™ Threat Management System
Research Report

An Overview of the Russian Hacking Scene

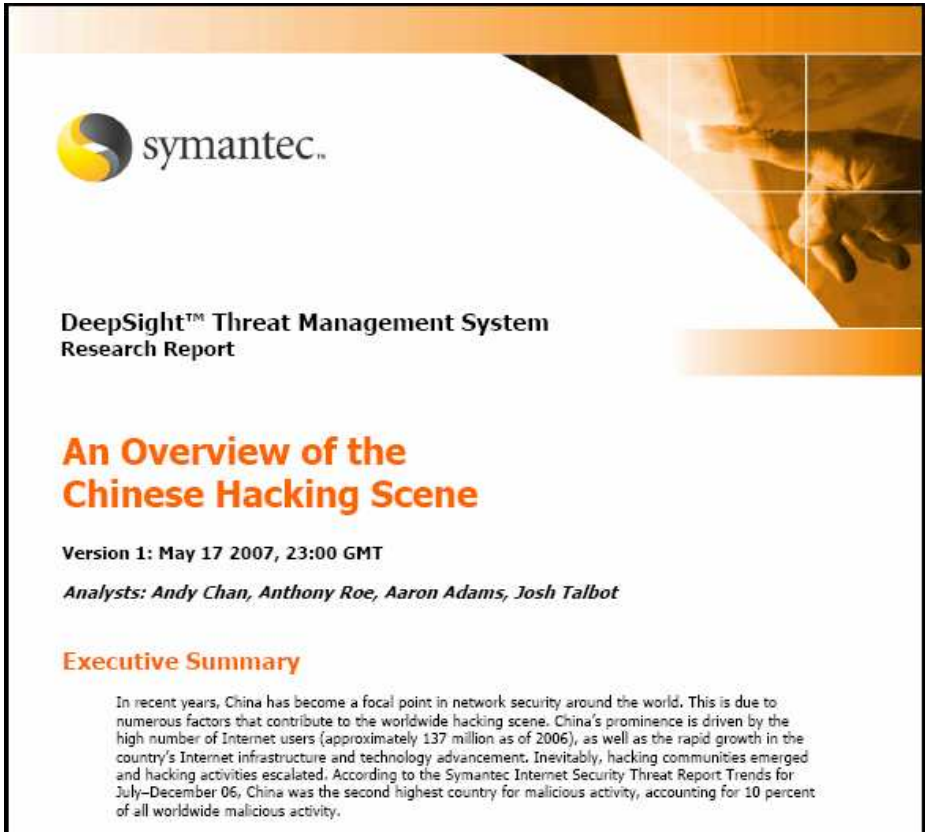
Version 1: July 30, 2007

Analysts: Aaron I. Adams, Alexey Lavrenyuk, Pukhraj Singh

Executive Summary

Russia has played a major role in most areas of the computer security field. Over the years, Russians have been responsible for some of the most notorious cyber crimes, including bank heists, wide-spreading worms, sophisticated viruses, credit card scams, denial-of-service attacks, and political attacks.

This document presents a high-level look into the various areas where Russia has been involved in some of these activities. It highlights some of the well-known groups and members involved in the activities and presents the available evidence that links Russians to a variety of malware.



symantec.

DeepSight™ Threat Management System
Research Report

An Overview of the Chinese Hacking Scene

Version 1: May 17 2007, 23:00 GMT

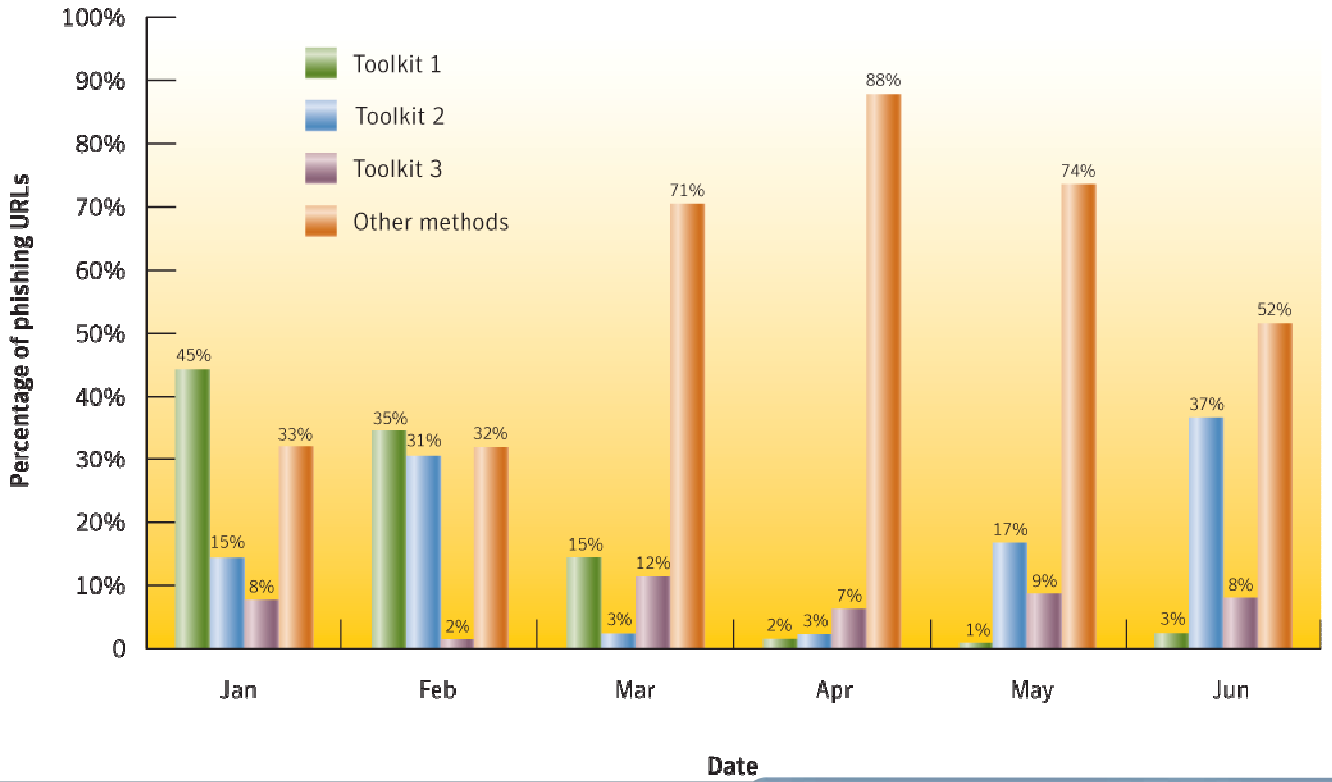
Analysts: Andy Chan, Anthony Roe, Aaron Adams, Josh Talbot

Executive Summary

In recent years, China has become a focal point in network security around the world. This is due to numerous factors that contribute to the worldwide hacking scene. China's prominence is driven by the high number of Internet users (approximately 137 million as of 2006), as well as the rapid growth in the country's Internet infrastructure and technology advancement. Inevitably, hacking communities emerged and hacking activities escalated. According to the Symantec Internet Security Threat Report Trends for July–December 06, China was the second highest country for malicious activity, accounting for 10 percent of all worldwide malicious activity.

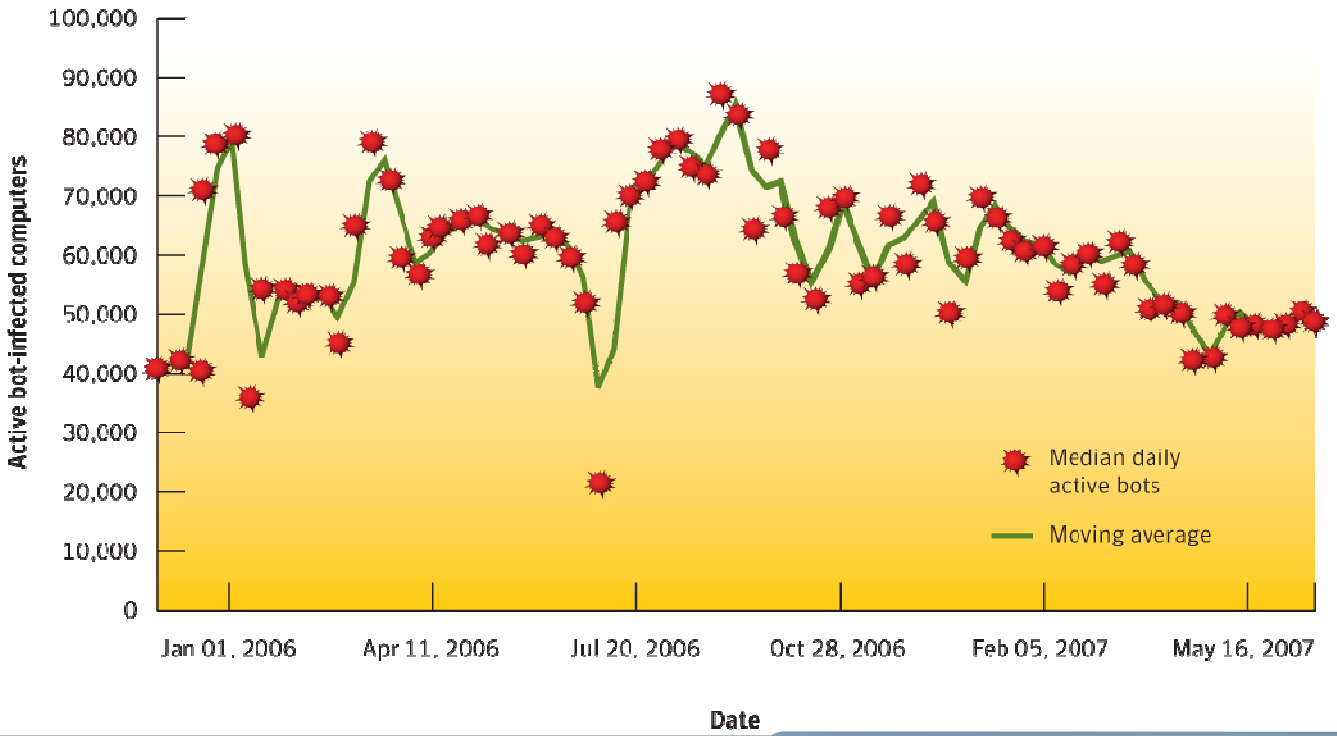
Informe de Amenazas en Internet

- Incremento de la profesionalización y comercialización de los atacantes.
- Ejemplo: Uso de toolkits para phishing toolkits y MPack



Informe de Amenazas en Internet

- Los atacantes intentan comprometer entidades confiables como Web sites conocidos para atacar indirectamente
- Este período acaba con menos bots activos lo que indica que los ataques tradicionales parecen ser menos efectivos que antes

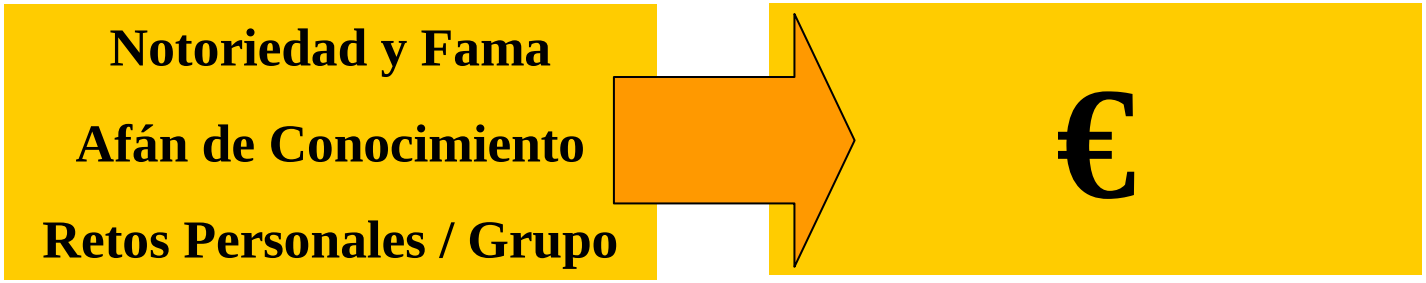


Los incidentes de seguridad modernos

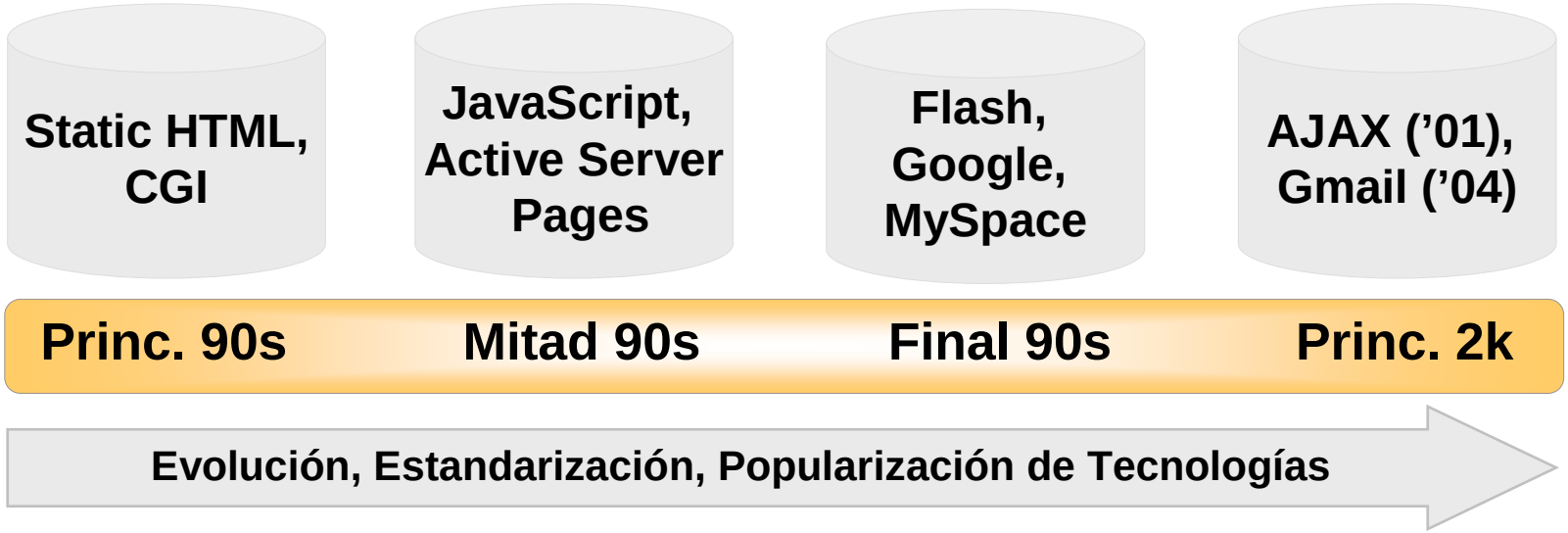
- En el pasado cercano (y todavía en el presente), los incidentes de seguridad son visibles. Incluso sin mecanismos de detección
  - Virus
  - Bromas
  - Troyanos
  - Gusanos (Flash-worms, Warhol-worms)

Los incidentes de seguridad modernos

- Actualmente, la tendencia ha cambiado debido a:
  - Aumento en complejidad de la tecnología
  - Mayor número de “canales” de distribución/propagación
    - Email, Web 2.0 / AJAX, Blogs, Twitter, Social Networks, SOAP, RSS, etc.
  - Cambios en la motivación de los atacantes



Evolución de la Web

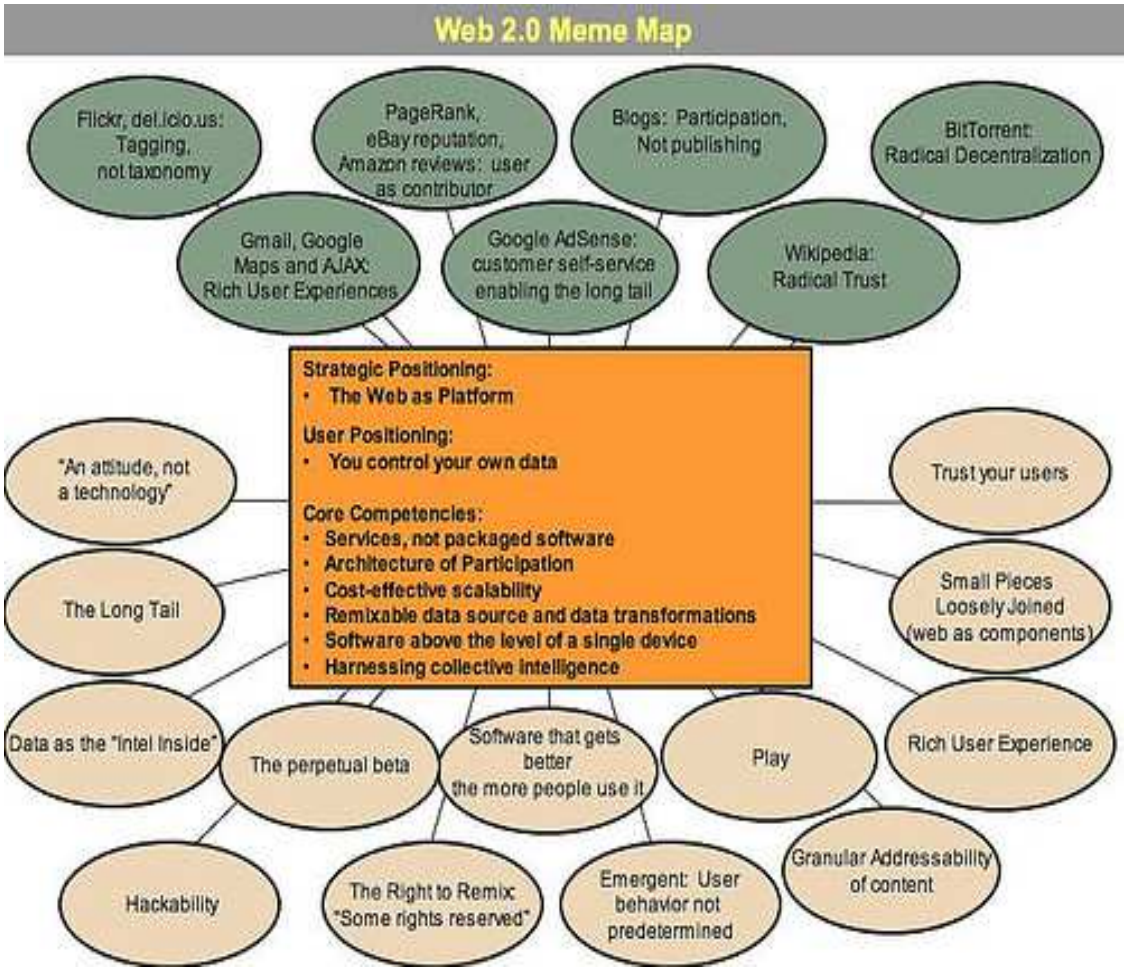


WEB 2.0

- Totalmente interactiva
- Contenido generado por el propio usuario (blogs, wikis, etc.)
- Networking "Social"
- Plug-ins, extensiones, BHOs
- Aplicaciones online/offline en el cliente (Google desktop)

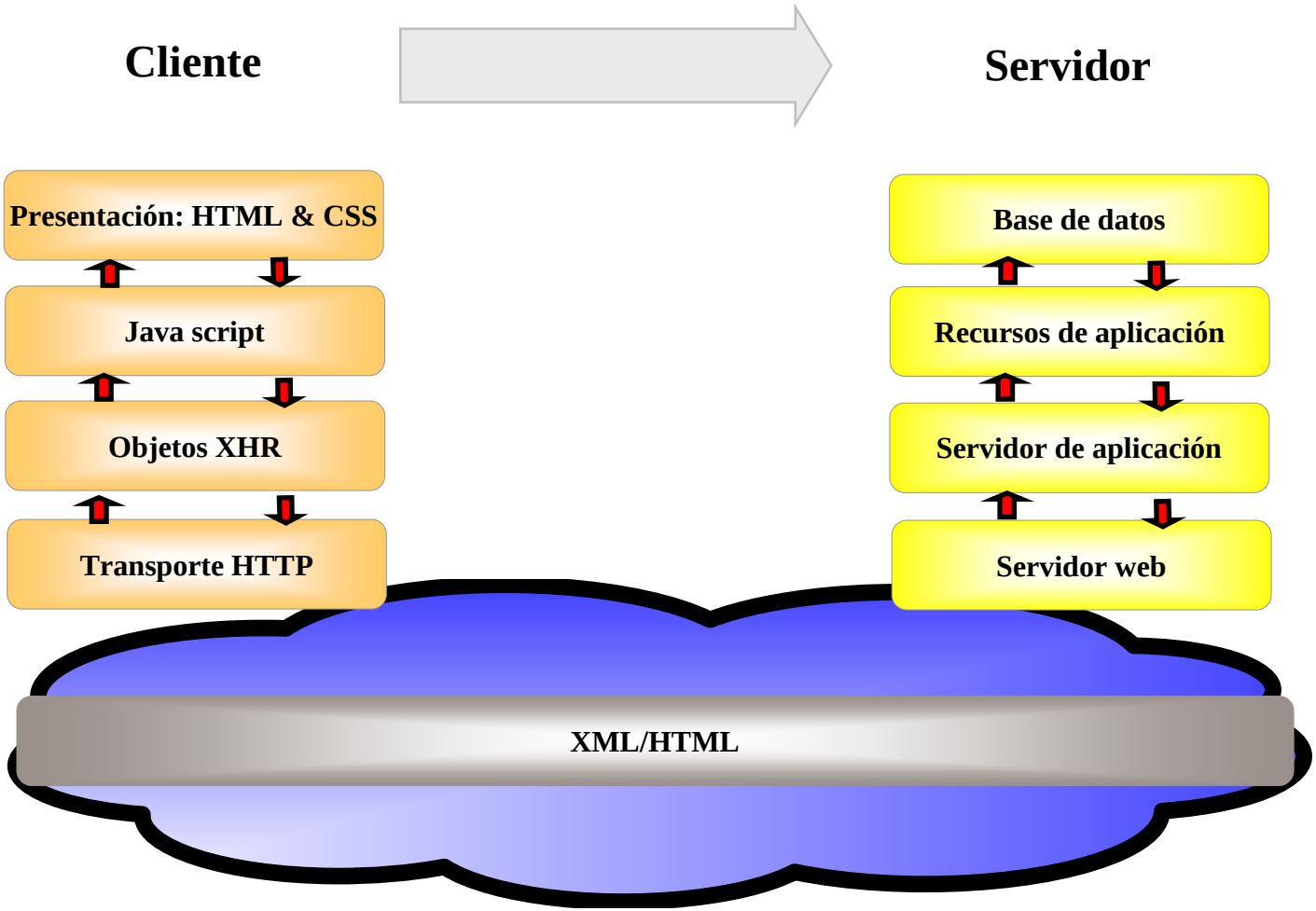
Web 2.0

"Web 2.0 es un conjunto de tendencias económicas, sociales y tecnológicas que de manera colectiva forman la próxima generación de Internet – un medio distintivo, más maduro y caracterizado por una total participación del usuario, más abierto y con mucho impacto en la red."

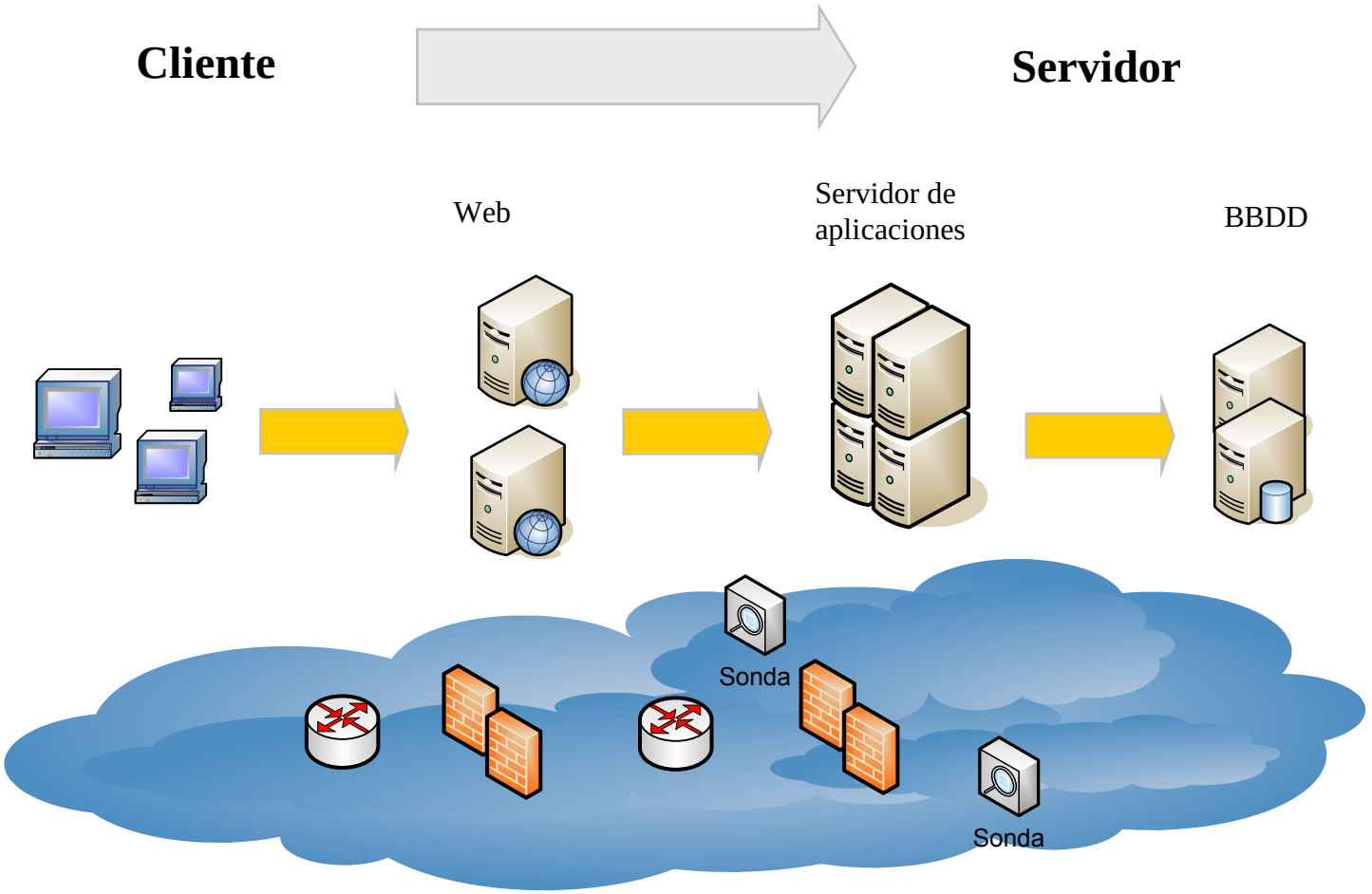


Fuente: O'Reilly

Arquitectura web 2.0



Infraestructura



Vulnerabilidades

- Código de APIs
- Control de acceso: autorización y autenticación
- Protocolos y algoritmos criptográficos
- Validación de datos de entrada
- Log y auditoría de la actividad
- Sincronización de tiempos
- Software base de soporte
- Gestión de errores
- Gestión de sesiones

Vulnerabilidades

ASP.NET Misconfiguration: Creating Debug Binary
ASP.NET Misconfiguration: Missing Custom Error Handling
ASP.NET Misconfiguration: Password in Configuration File
Access control enforced by presentation layer
Accidental leaking of sensitive information through data queries
Accidental leaking of sensitive information through error messages
Accidental leaking of sensitive information through sent data
Addition of data-structure sentinel
Algorithmic Complexity
Allowing External Setting Manipulation
Allowing password aging
Alternate Channel Race Condition
Alternate Encoding
Assigning instead of comparing
Authentication Bypass by Alternate Path/Channel
Authentication Bypass by Primary Weakness
Authentication Bypass via Assumed-Immutable Data
Authentication Error
Authentication Logic Error
Authentication bypass by alternate name
Authentication bypass by spoofing
Behavioral Change
Behavioral Discrepancy Infoleak
Behavioral problems
Buffer Overflow
Buffer over-read
Buffer overflow
Buffer under-read
Buffer underwrite
Bundling Issues
Byte/Object Code
CRLF Injection
Capture-replay
Case Sensitivity (lowercase, uppercase, mixed case)
Catch NullPointerException
Channel and Path Errors
Cleansing, Canonicalization, and Comparison Errors
Code Correctness: Call to System.gc()
Code Correctness: Call to Thread.run()
Code Correctness: Class Does Not Implement Cloneable
Code Correctness: Double-Checked Locking
Code Correctness: Erroneous String Compare
Code Correctness: Erroneous finalize() Method
Code Correctness: Misspelled Method Name
Code Correctness: null Argument to equals()
Collapse of Data into Unsafe Value
Common Special Element Manipulations
Comparing classes by name
Comparing instead of assigning
Comprehensive list of Threats to Authentication Procedures and Data
Context Switching Race Condition
Covert timing channel

Ataques

Absolute Path Traversal
Account lockout attack
Alternate XSS Syntax
Argument Injection or Modification
Asymmetric resource consumption (amplification)Blind SQL Injection
Blind XPath Injection
Brute force attack
Buffer overflow attack
CSRF
Cache Poisoning
Code Injection
Command Injection
Comment Element
Cross Site Tracing
Cross-Site Request Forgery
Cross-User Defacement
Cross-site-scripting
Cryptanalysis
Custom Special Character Injection
Direct Dynamic Code Evaluation ('Eval Injection')
Direct Static Code Injection
Double Encoding
Forced browsing
Format string attack
Full Path Disclosure
HTTP Request Smuggling
HTTP Response Splitting
Integer Overflows/Underflows
LDAP injection
Man-in-the-middle attack
Man-in-the-middle attack
Mobile code: invoking untrusted mobile code
Mobile code: non-final public field
Mobile code: object hijack
Network Eavesdropping
One-Click Attack
Overflow Binary Resource File
Parameter Delimiter
Path Manipulation
Path Traversal
Phishing
Relative Path Traversal
Repudiation Attack
Resource Injection
Reviewing code for XSS issues
SQL Injection
Server-Side Includes (SSI) Injection
Session fixation
Session hijacking attack
Setting Manipulation
Special Element Injection
Spyware
Traffic flood
Trojan Horse
Unicode Encoding
Web Parameter Tampering
XPATH Injection
XSRF
XSS in error pages
XSS using Script Via Encoded URI Schemes
XSS using Script in Attributes

Ataques

Cross-site scripting

- Ejecución de código JavaScript malicioso en el navegador del usuario
- Se propaga mediante su inclusión en mensajes de correo electrónico o en servidores web (por ejemplo en blogs)
- Para el envío remoto de información utilizan
  - Embedded HTML Tags

```
<img src="http://www.google.com/search?hl=en&q=symantec+security&btnG=Google+Search">
```

  - JavaScript y Document Object Model

```
img[0].src = http://www.google.com/search?hl=en&q=symantec+security&btnG=Google+Search;
```

  - XmlHttpRequest

```
var req = new XMLHttpRequest();
req.open('GET', ' http://www.google.com/search?hl=en&q=symantec+security&btnG=Google+Search', true);
req.onreadystatechange = function () {
if (req.readyState == 4) {
        alert(req.responseText);
        }
};
req.send(null);
```

Ataques

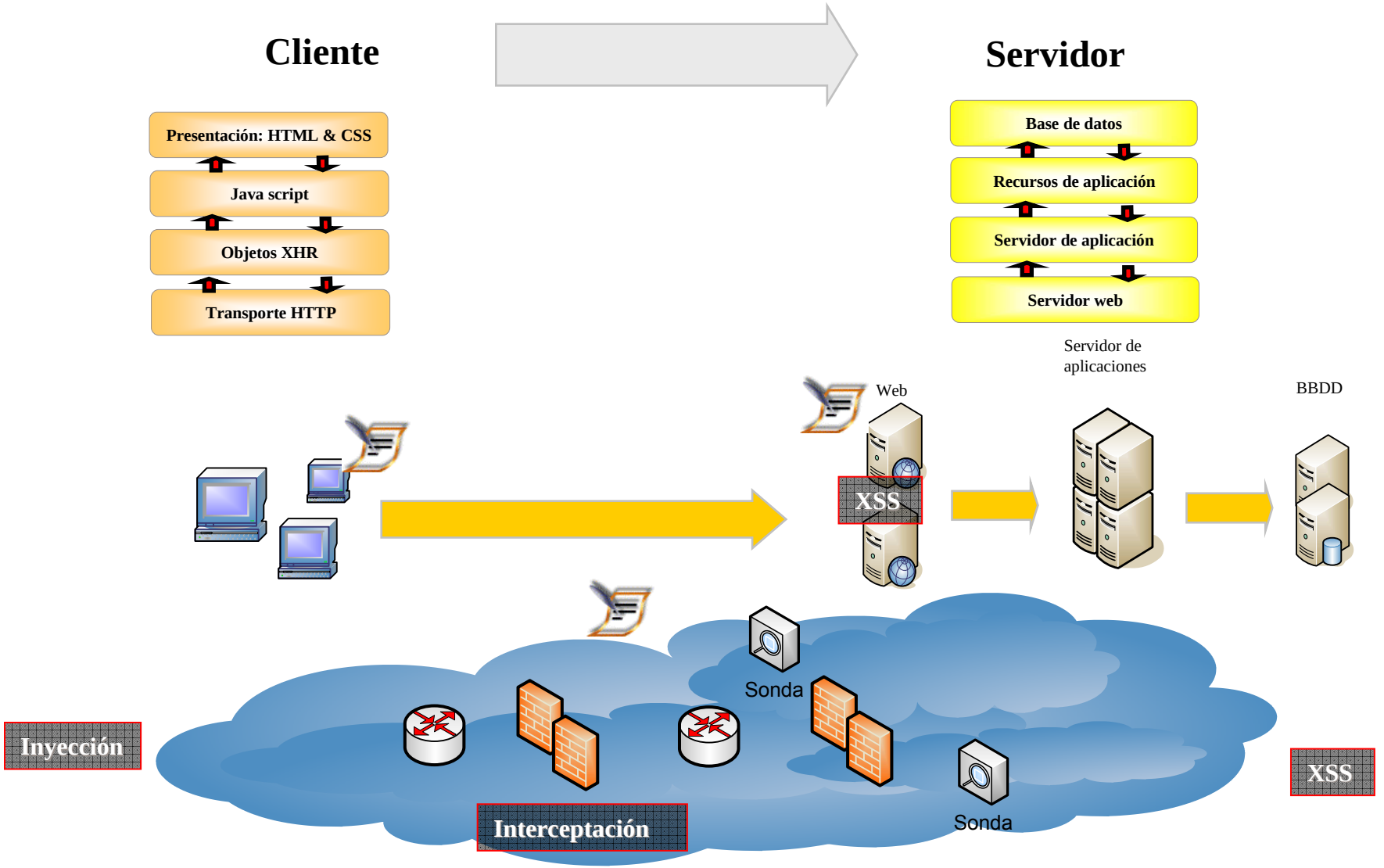
Inyección de código

- El objetivo es la infraestructura de servidor
- Busca normalmente el acceso indebido o la denegación del servicio
  - XPATH injection
  - Modificación de argumentos
  - XML Poisoning

Interceptación

- Interceptación de tráfico sensible
- Redirección de sesiones
  - Sniffing
  - Man in the middle
  -

Ataques


Cliente
Servidor
Presentación: HTML & CSS
Java script
Objetos XHR
Transporte HTTP
Base de datos
Recursos de aplicación
Servidor de aplicación
Servidor web
Servidor de aplicaciones
Web
BBDD
XSS
Sonda
Inyección
Interceptación
Sonda
XSS

Restricción. Contramedidas preventivas

- Mejora de la Seguridad de los Clientes Web
  - Mayor calidad
  - Mejores y más eficientes mecanismos de seguridad
  - Mayor control del usuario sobre conexiones
  - Mejor control de acceso a terceros dominios
  - Mayor visibilidad y control del usuario sobre conexiones en background

Restricción. Contramedidas preventivas

- Mejora de la Seguridad de las Aplicaciones Web 2.0
  - Mayor calidad del código y las prácticas de desarrollo
  - Evitar la existencia de vulnerabilidades de:
    - Inyección de SQL
    - Cross-Site Scripting (XSS)
    - Vulnerabilidades de Formato de Cadenas
    - Vulnerabilidades de Enumeración
  - Autenticación y autorización
  - Cifrado de información

Restricción - Contramedidas detectivas

- Detección de actividad anómala en el cliente
  - Sistemas Ant-Fraude, Anti-Phishing
  - Firewalls personales
  - Host IDS en el cliente
- Detección de actividad anómala en la red
  - Network IDS
- Detección de Actividad Anómala en la Aplicación
  - Mecanismos de detección integrados en las aplicaciones

La evidencia - El cliente

- “Histórico” del navegador web
  - Sólo se registra la conexión inicial a una página, no las llamadas realizadas por el código client-side (XMLHTTPRequest), por lo que no es de demasiada utilidad.

- “Cookies” en el navegador web
  - Evidencia de conexión a un “tercero” malicioso

La evidencia - El cliente

- Logs de firewalls personales
  - Dependiendo de la configuración, puede contener información sobre cada una de las conexiones TCP y UDP realizadas por el cliente.
- Logs de firewalls intermedios y perimetrales
  - Información sobre conexiones TCP y UDP realizadas por el cliente.
- Logs de proxies de salida
  - Contiene evidencia de las conexiones realizadas por el cliente (tanto iniciadas por el usuario, como conexiones en background de objetos XHR)
  - Contiene evidencia de la conexión del cliente a “terceros” no habituales.

La evidencia - El servidor

- Logs del servidor web
  - Dependiendo de la configuración, puede contener evidencia de todas las peticiones (interactivas o en background) realizadas por el cliente a la aplicación.
  - Lógicamente, no apareceran conexiones a “terceros” maliciosos.
- Logs de la aplicación
  - Depende de la aplicación. A veces los logs ni siquiera existen en este caso.
- Logs de la base de datos
  - Potencialmente podrían evidenciar ataques de SQL Injection.
  - Normalmente no se registran las consultas a las bases de datos en los logs (sólo errores e información de mantenimiento)

La evidencia - Infraestructura de red

- Logs y alertas de Network IDS
  - Evidencia de exploits conocidos o patrones de tráfico sospechosos (XSS, SQL Injection, etc.)
  - Siempre que no se use SSL, ¡claro!
- Logs y alertas de Host IDS
  - Evidencia de exploits conocidos o comportamientos sospechosos (XSS, SQL Injection, etc.)

La evidencia - Nuevas armas

- Correlación de Eventos de Fuentes Heterogéneas
  - Del lado del cliente (corporativo)
    - Eventos generados por firewalls y Network IDS
    - Eventos generados por firewalls e IDS de host
    - Información generada por proxies web de salida a Internet
  - Del lado del proveedor de la aplicación Web 2.0
    - Eventos generados por firewalls y Network IDS
    - Logs de pila de aplicación de todas las capas (base de datos, servidor, application server, webserver)
    - Logs generados por la propia aplicación, con contexto de negocio (transacciones sospechosas, errores de secuencia o validación, etc.)

La evidencia - Nuevas Armas

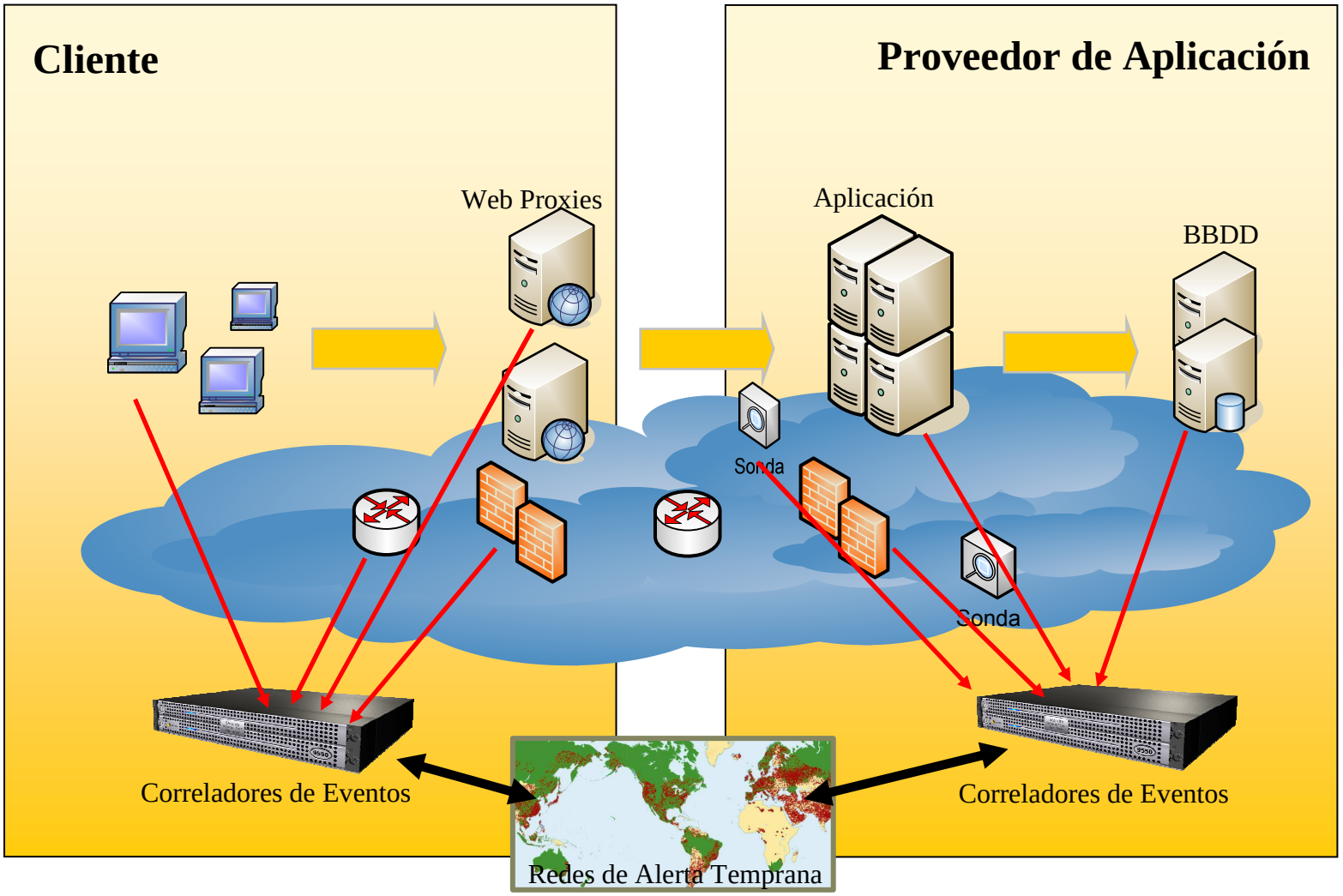
- Inteligencia Global / Redes de Alerta Temprana
  - Globalización de la información sobre actividad maliciosa o sospechosa en Internet
  - Un solo cliente afectado permite prevenir y tomar medidas al resto
  - Proporciona visibilidad a actividades silenciosas o de propagación lenta

Permite agregar, de forma anónima y segura, la información generada desde el lado del cliente, y del lado del proveedor de la aplicación Web 2.0

La evidencia - Correlación de Eventos

- Tradicionalmente, se usan sistemas de correlación para eventos generados por:
  - Firewalls
  - IDS
  - Servidores
  - Antivirus
- La actividad maliciosa relacionada con Web 2.0 requiere integrar más fuentes:
  - Firewalls / IDS de Cliente
  - Proxies Web
  - Logs de servidores Web y servidores de Aplicaciones
  - Logs de las Aplicaciones

La evidencia - Cerrar el Círculo



La evidencia - Correlación de Eventos

1 Firewall y 1 IDS, en 1 mes

9,500,000 eventos en log

620 eventos de seguridad identificados

55 riesgos de seguridad reales

Añadir:

450 Nuevos Virus

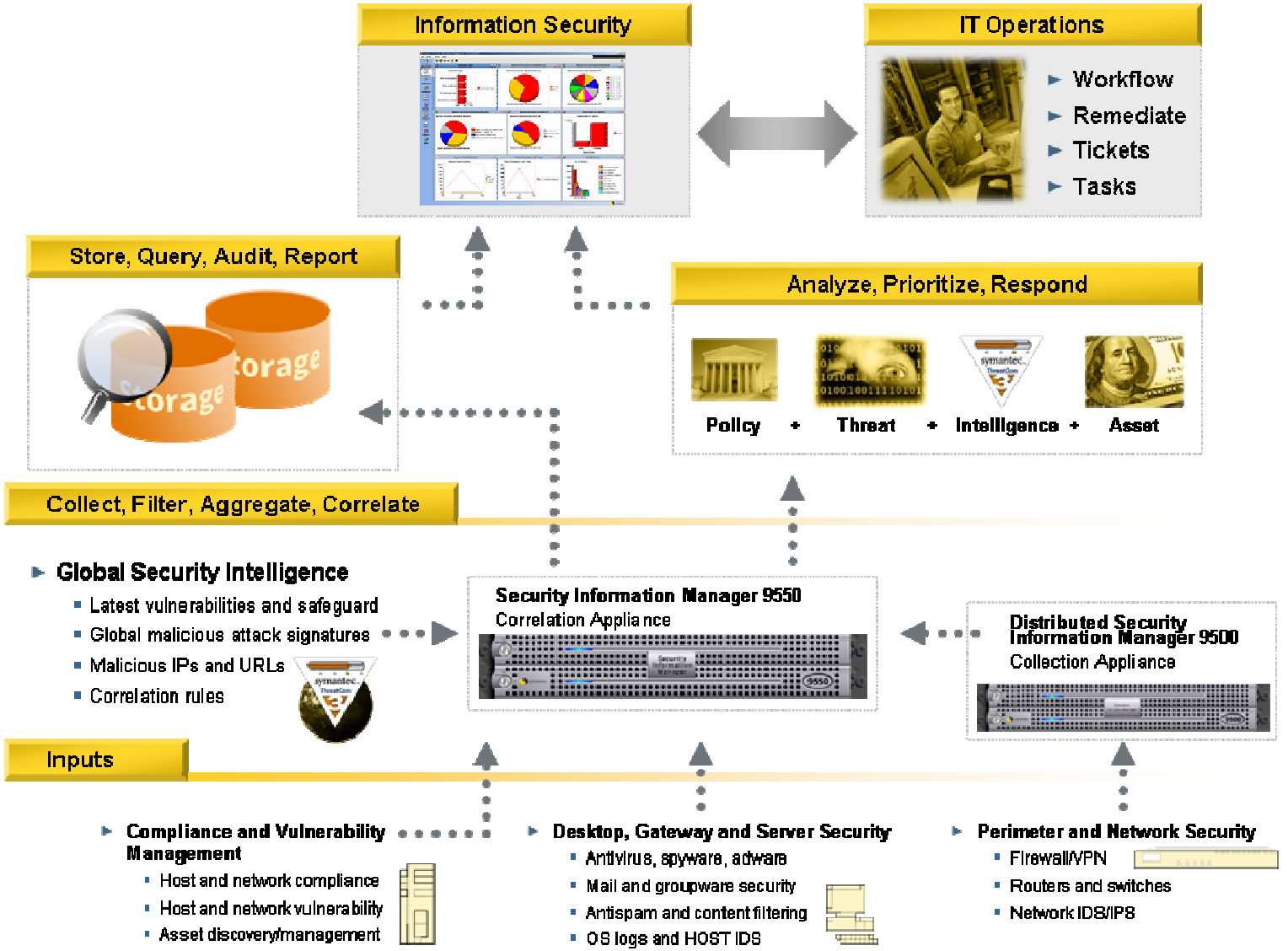
2 AMENAZAS URGENTES

Añadir:

250 Nuevas Vulnerabilidades

Y a esto hay que añadir lo que hemos mencionado (proxies, aplicaciones, firewall de cliente, etc.)

Symantec Security Information Manager



Symantec Security Information Manager

Seguridad

- Integración con la base de conocimientos de DeepSigth
- Flexible, multi-usuario, y informes de cumplimiento
- Priorización de incidencias basado en la criticidad y vulnerabilidad de activos

Escalabilidad

- Dispositivo dedicado con alto rendimiento
- Motor de correlación dinámica
- Filtrado y agregación

Simplicidad

- Instalación rápida y sencilla
- Interfaz amigable
- Directorio y BBDD enmbebidas

Symantec™ Global Intelligence Network

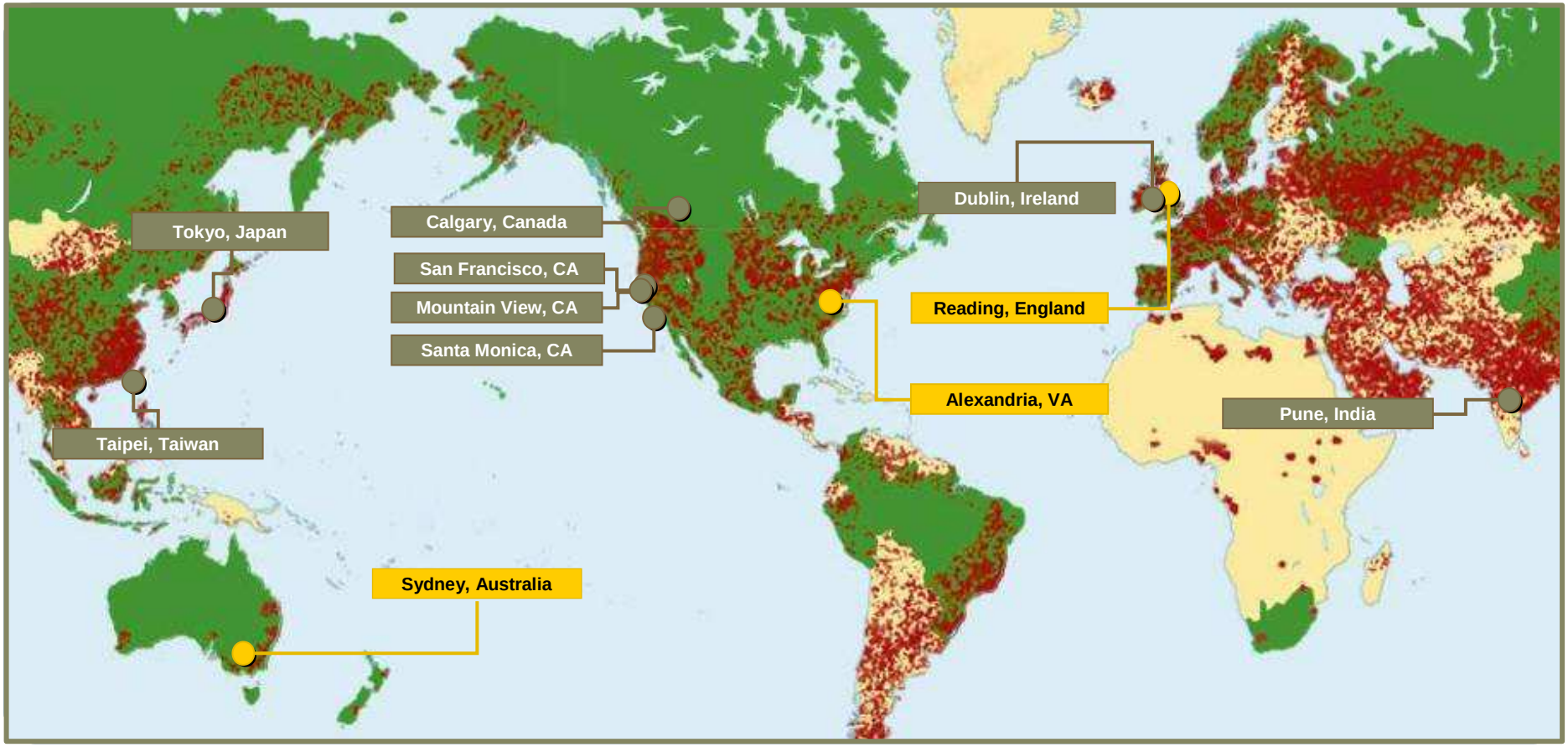
3 SOCs

80 Países Monitorizados por Symantec

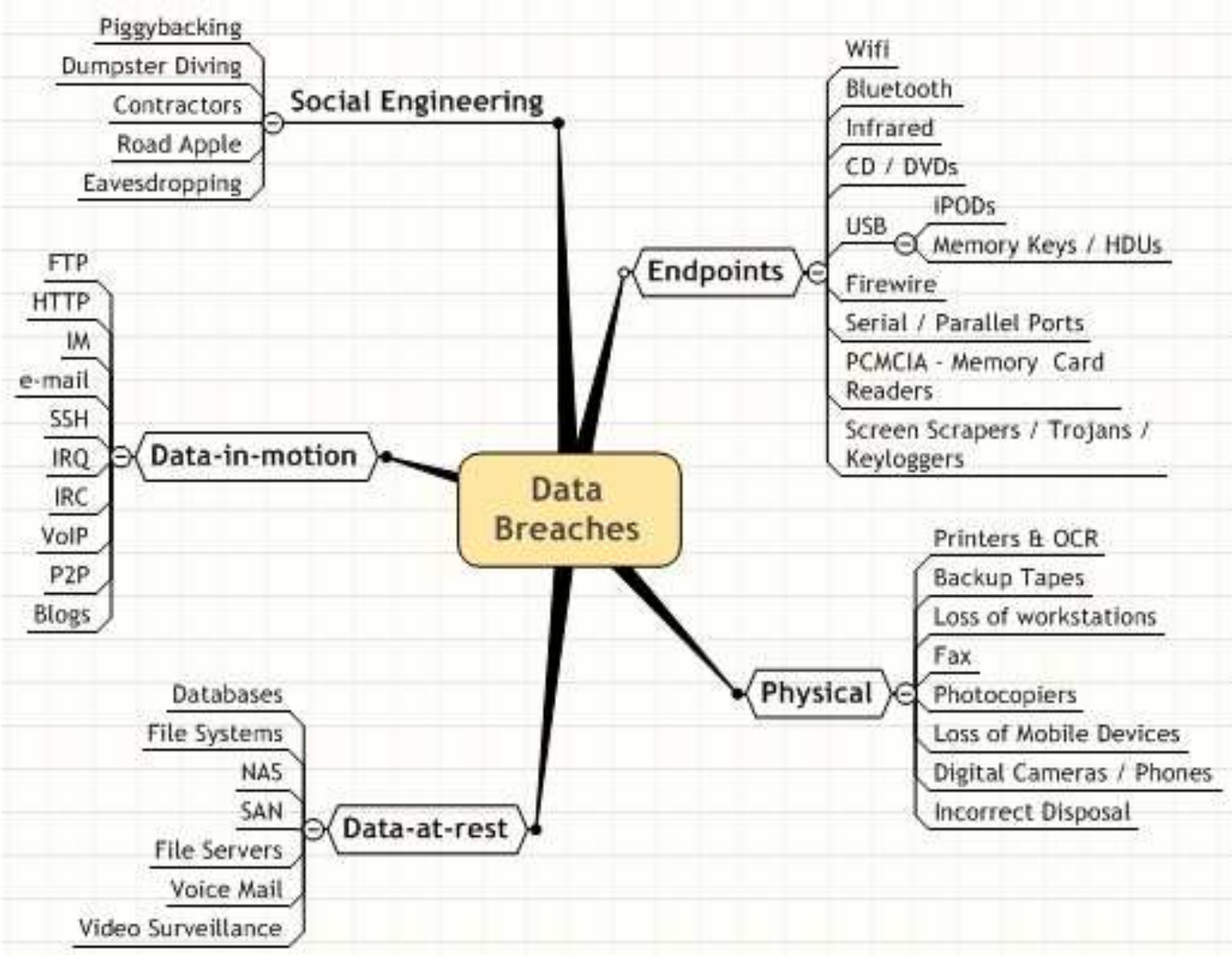
40,000+Sensores registrados en 180+ Países

8 Centros de Respuesta de Seguridad de Symantec

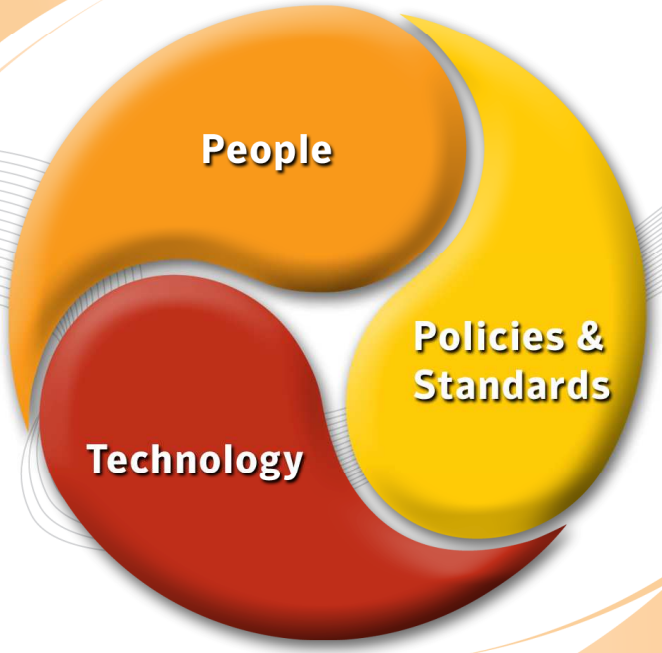
> 6,000 Disp. Seguridad Gestionados + 120 Millones de Sistemas + 30% del tráfico de correo mundial+ Red Honeypot



¿Todos los ángulos cubiertos?



La solución completa

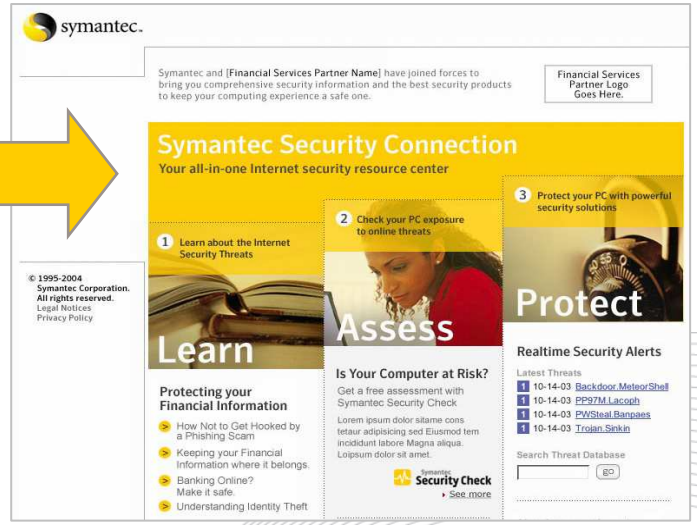


Una solución completa contiene todos los componentes incluyendo el factor “humano” en seguridad

Concienciación / Educación del Usuario

Symantec Security Connection

- Información específica o e-Learning



- Enlace a Symantec Security Check, herramienta online que evalúa el nivel actual de seguridad del PC del visitante

Conclusiones

- **Web 2.0**: Provee muchos servicios y oportunidades a empresas y consumidores pero también implica nuevos riesgos.
- **Crimen Organizado:** El desarrollo, distribución y uso de código malicioso por los atacantes es cada vez más comercial y profesional.
- **Solución Completa:** Es necesario una aproximación holística a la seguridad – Tecnología, Personas y Normativas
- **Internet Security Threat Report:** La Red Global de Inteligencia de Symantec es única.

¡Gracias!