Staying Ahead of Cybercrime: The Importance of Web Application Security

Danny Allan
Director of Security Research, IBM Rational
dallan@us.ibm.com

Rational. software

Go to IBM

Security and the Web

Rational. software

The Security Equation Has Changed

- How businesses look at security has changed
  - Security is now business-driven not technology driven
  - Security is now defined through risk management and compliance disciplines instead of threat and technology disciplines
- The threat landscape has changed
  - Attackers are now business-driven
    - Out for a profit instead of out for a laugh
  - Traditional operating system security risks have become somewhat passé
  - Client threats are now all about the browser environment
  - Server threats are now all about web applications

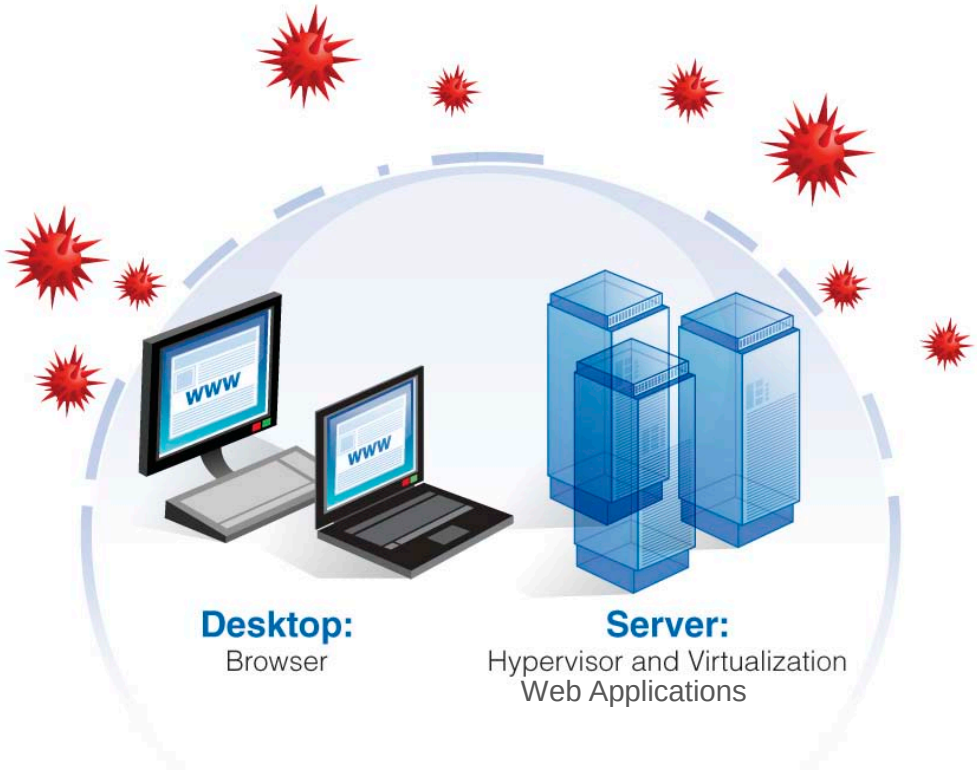
The Security Landscape of Old

- **Traditional Infrastructure was easier to protect . . .**
- Concrete entities that were easy to understand
- Attack surface and vectors were very well-defined
- Application footprint very static
- Perimeter defense was king

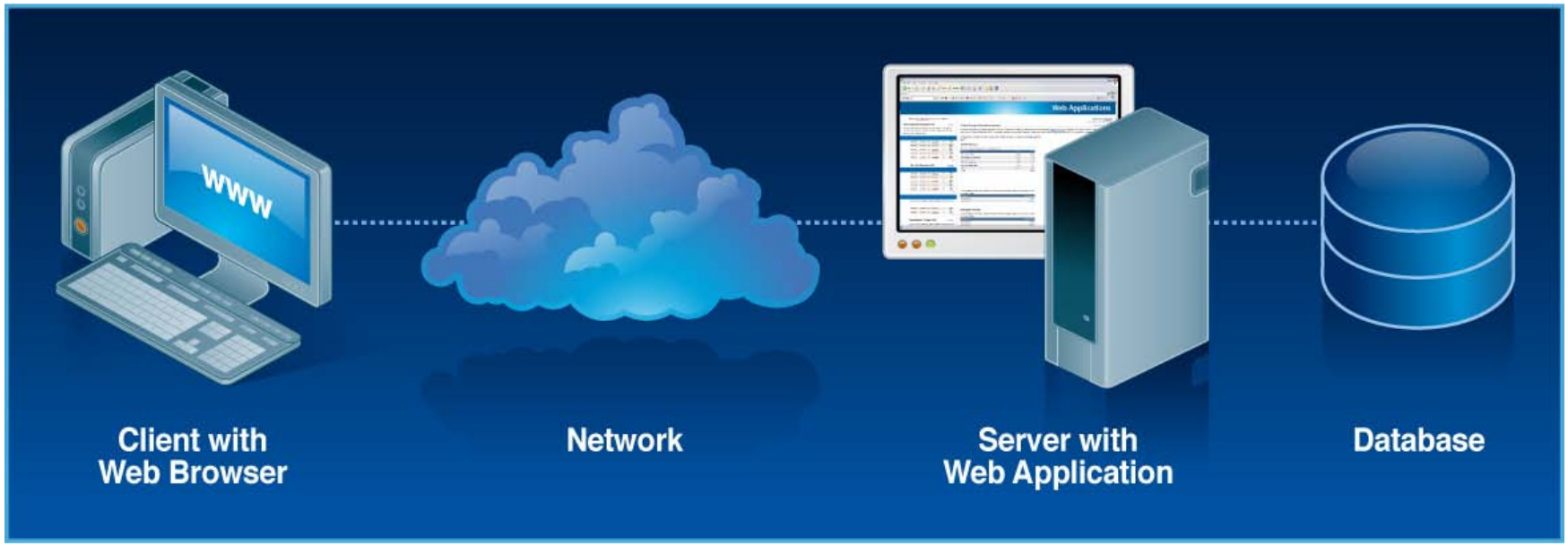
Changing Security Landscape of Today

“Webification” has changed everything ...

- Infrastructure is more abstract and less defined
- No more “inside” vs. “outside”
- Everything needs a web interface
- Traditional defenses no longer apply

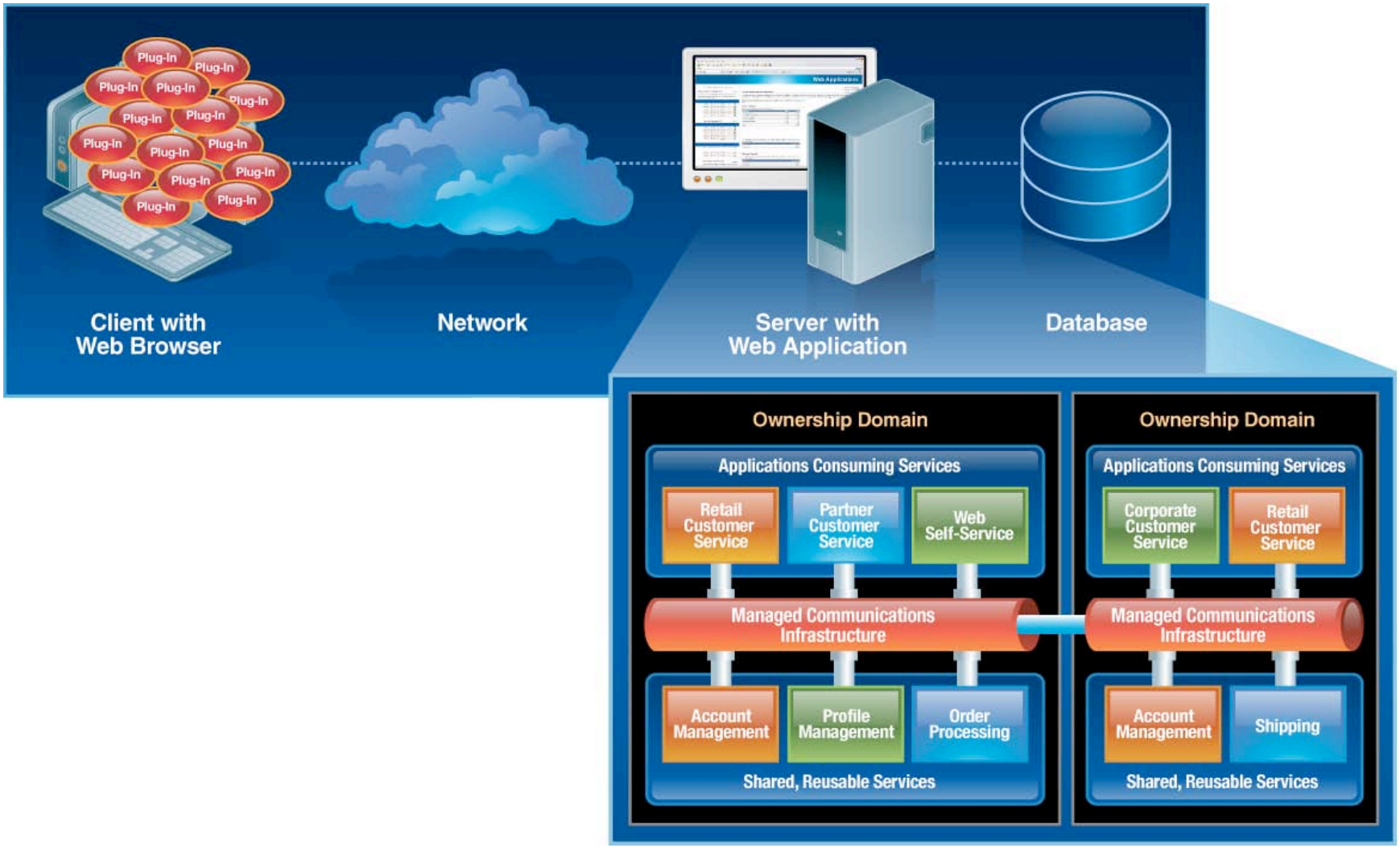


The Web Ecosystem (simple view)



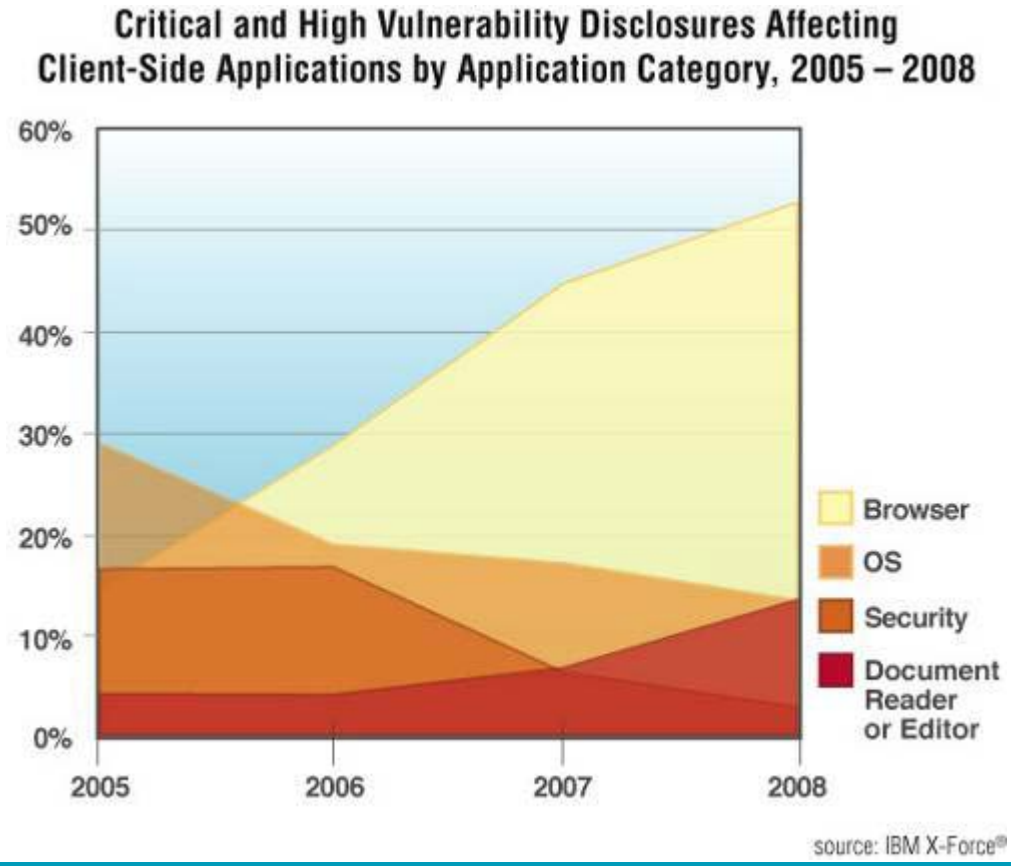
- Client with a web browser renders the content for a user
- Network transports content between the server and the client
- Server with the web application performs the required action
- Database stores information

The Web Ecosystem (complex view)



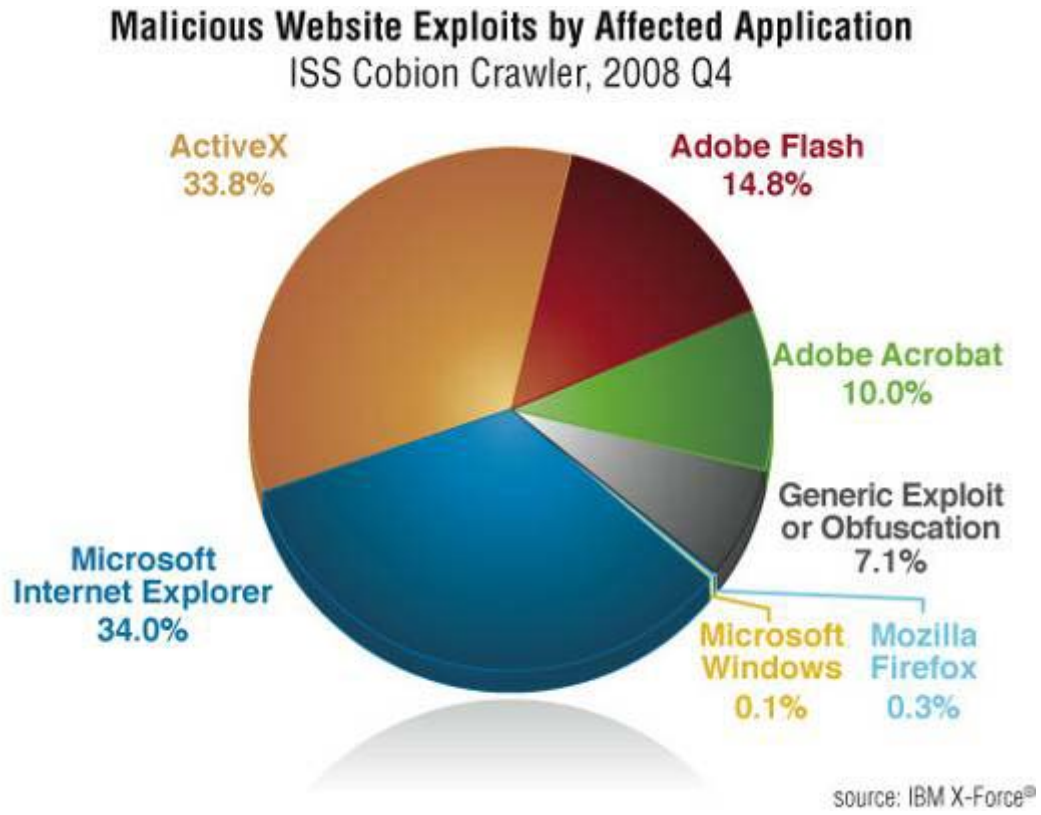
Client-side Vulnerability Landscape Has Changed

- Quick ROI comes from client exploits
  - Automated systems for attack (Web exploit toolkits)
  - Automated systems for compromise/revenue-generation like malware generator kits
- OS vulns are less of a problem
- Browser vulns are worse
- Document reader vulns are next



Malicious Linkland

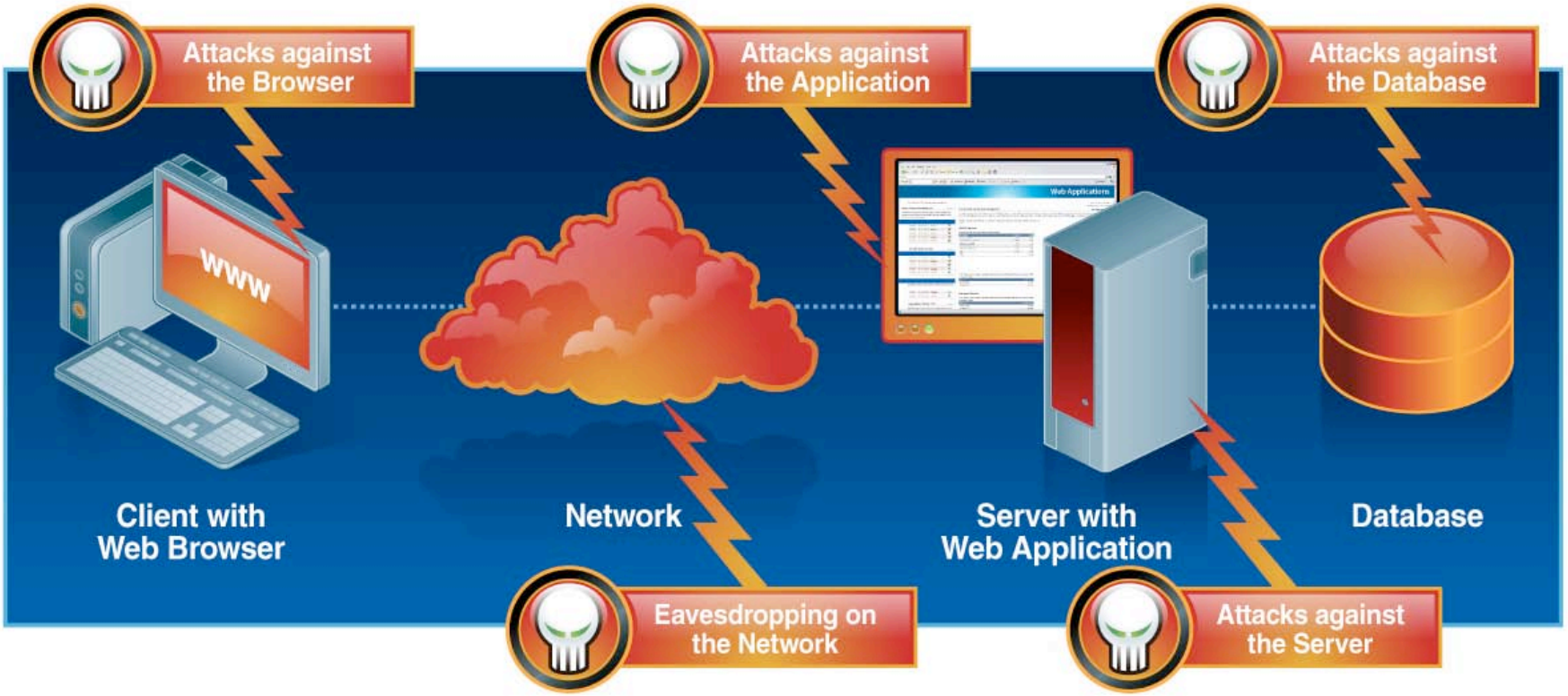
- Although most malicious websites focus on Microsoft Internet Explorer exploits (and ActiveX Controls), fast-growing categories are malicious PDFs and movies



Why Would an Attacker Care About My Web Site?

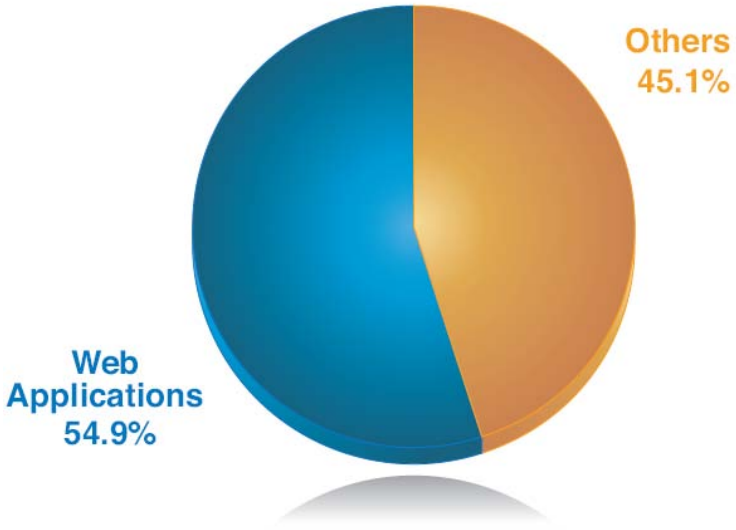
- Attackers are constantly challenged to find fresh targets
  - Spam and phishing not always effective
  - How to attract visitors to newly-created malicious Web sites?
- Established Web sites are a perfect target
  - Web applications are notoriously riddled with holes, many unpatchable
  - Users trust established Web sites (more likely to click that link, upload that plug-in or download that file)

Case in Point: Gumblar



2008 Web Threats Take Center Stage

- Web application vulnerabilities
  - Represent largest category in vuln disclosures (55% in 2008)
  - 74% of Web application vulnerabilities disclosed in 2008 have no patch to fix them



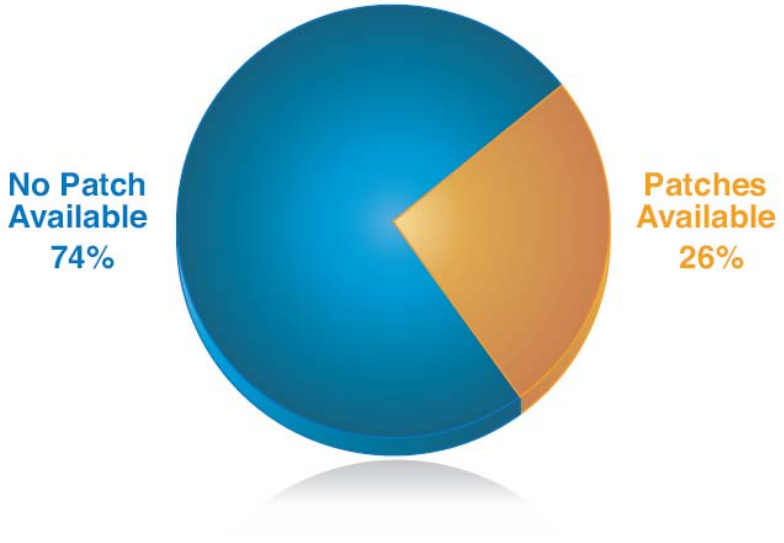
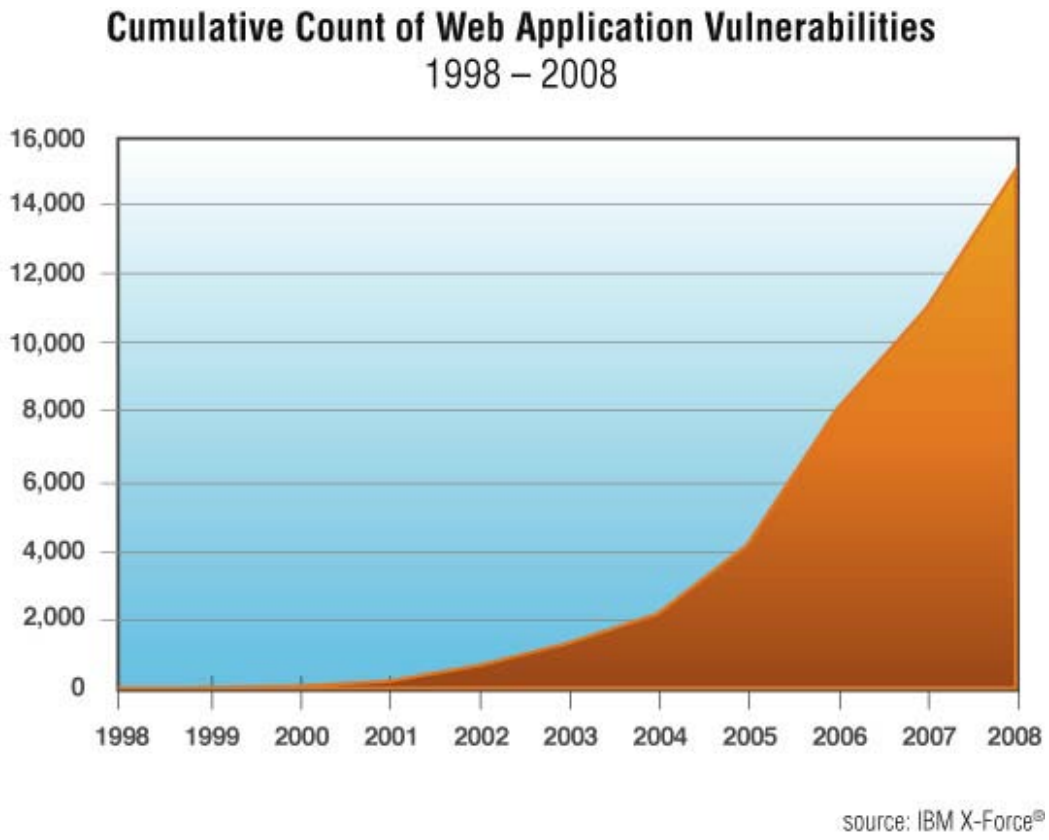


Figure 22: Percent of 2008 Web Application Vulnerabilities with No Vendor-Supplied Patch Available at the End of 2008

Growth of Web Application Vulnerabilities

- SQL injection vulnerability disclosures more than doubled in comparison to 2007



- The number of active, automated attacks on web servers was unprecedented

Attack Techniques are Plentiful and Trivial

- SQL injection and cross-site scripting are the two largest categories of Web application vulnerabilities
- SQL injection is fastest growing category (up 134% in 2008)

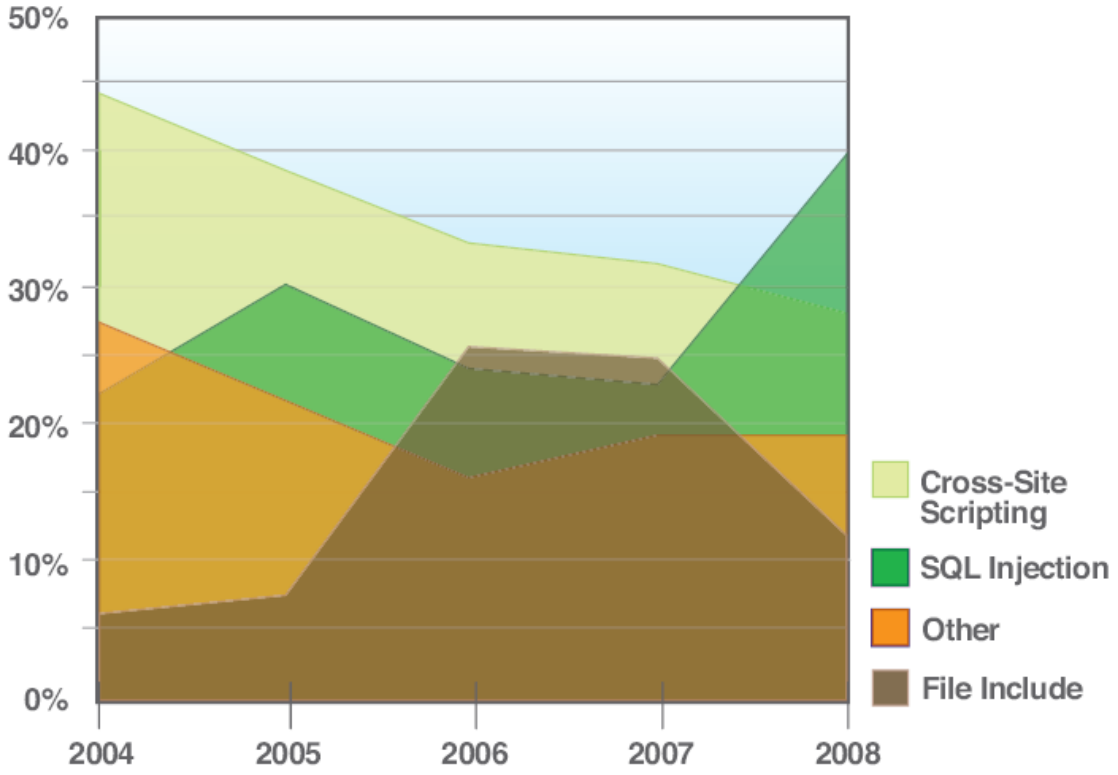


Figure 19: Web Application Vulnerabilities by Attack Technique, 2004 – 2008

Exploitation is Rampant

- Exploitation of SQL injection skyrocketed in 2008
  - Increased by 30x from the midyear to the end of 2008

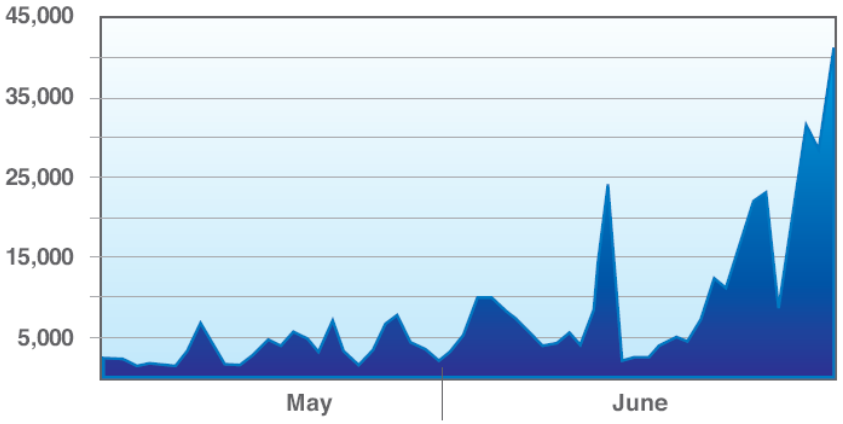


Figure 20: Initial SQL Injection Attacks Monitored by IBM ISS Managed Security Services, May – June 2008

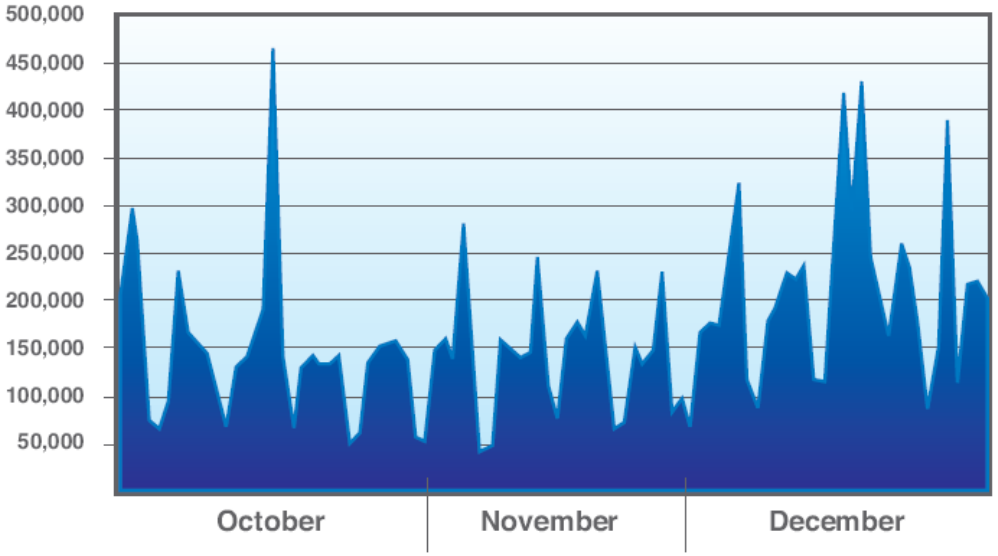
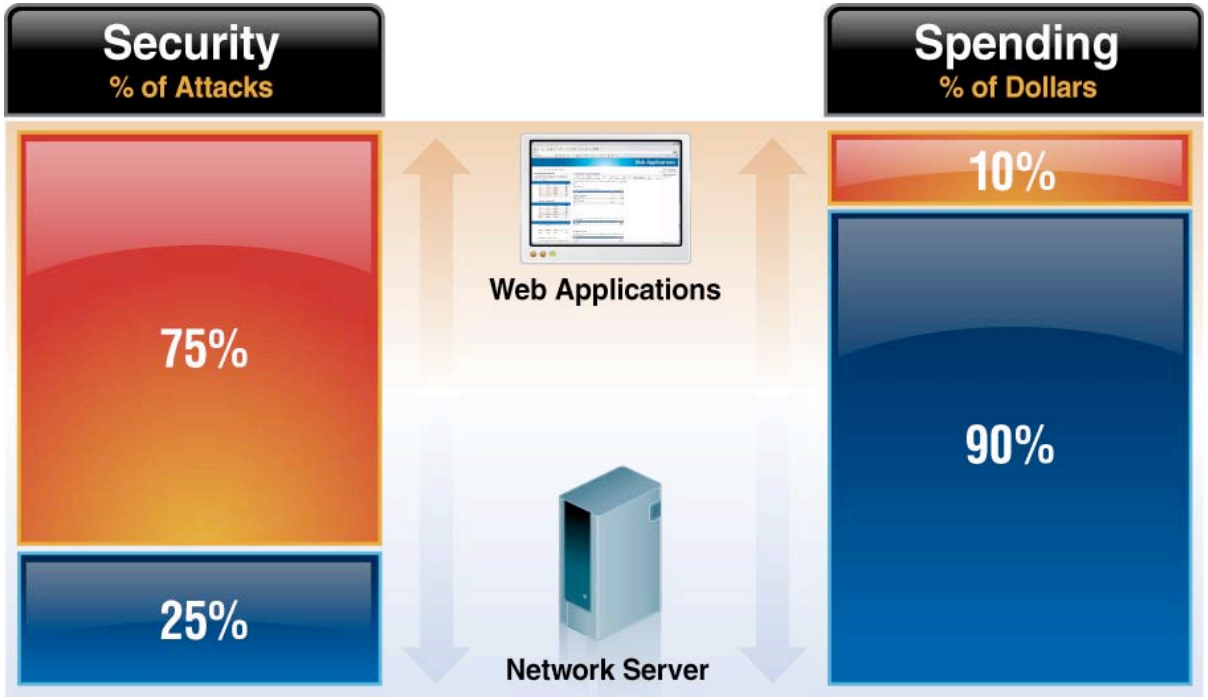


Figure 21: SQL Injection Attacks Monitored by IBM ISS Managed Security Services, Q4 2008

Reality: Security and Spending Are Unbalanced



75% **of All Attacks on Information Security are Directed to the Web Application Layer**

2/3 **of All Web Applications are Vulnerable** ***Gartner**

The Conundrum

- How security professionals and businesses prioritize risk and threats haven't changed with the overall landscape
- Businesses and professionals still tend to prioritize risk against an outdated traditional infrastructure viewpoint
- Businesses and professionals still tend to implement security solutions that focus on traditional threats and vectors
- Big blind spots
  - Browsers, document readers and editors, and web applications are still largely ignored or prioritized below other infrastructure from a security perspective

Web Threats Will Become Increasingly Complex

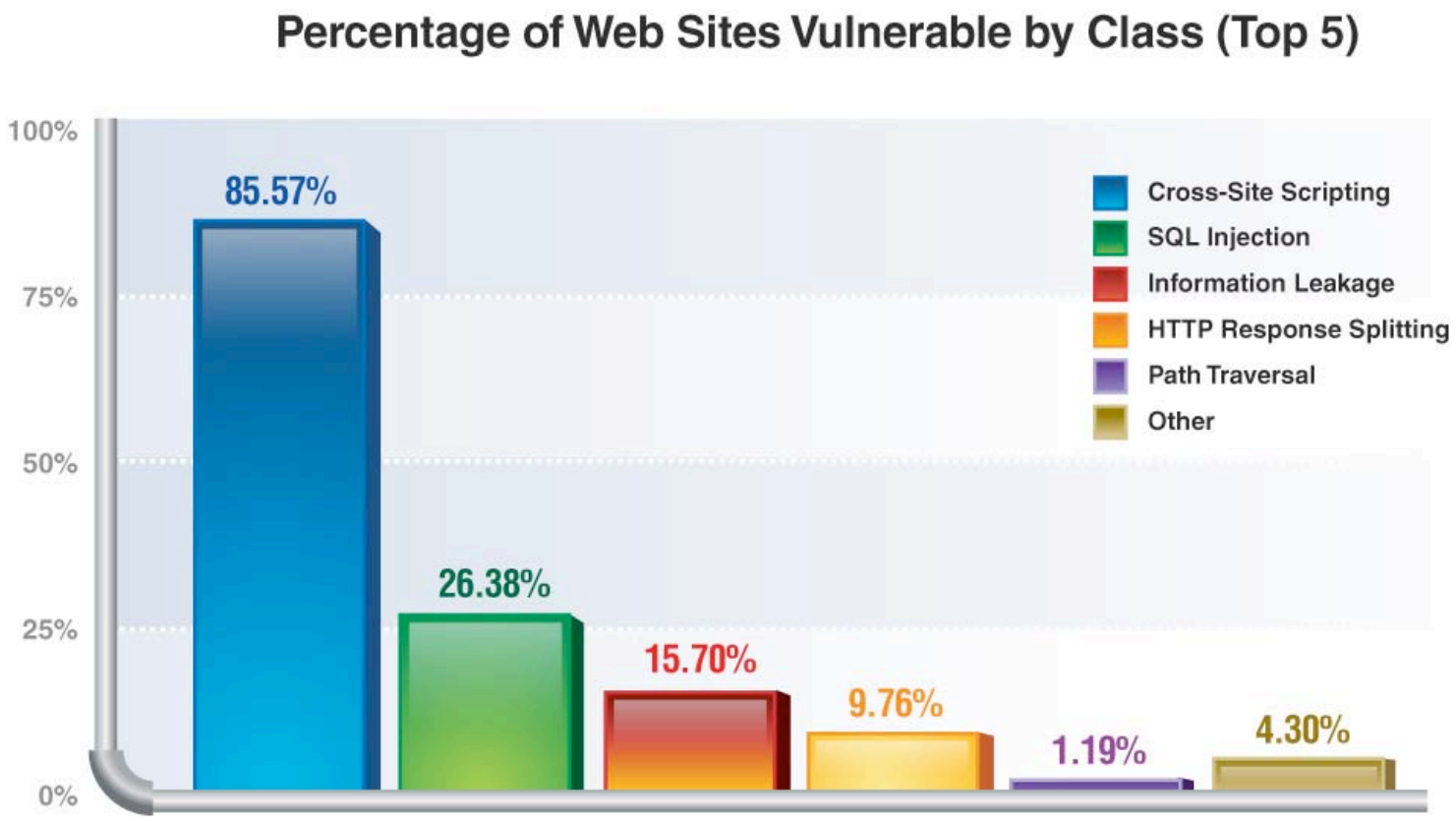
- Web becoming main application delivery interface and ecosystem
- Popularization of new web technologies (Web 2.0) growing attack surface
- New techniques and scenarios for targeting web infrastructure

Web Protection Does Not Have To …

Web Application Security

Rational. software

Vulnerability Probability (31,373 sites)



Source: WASC 2006 Web Application Security Statistics

1. Cross-Site Scripting (XSS)

- What is it?
  - Malicious script echoed back into HTML returned from a trusted site, and runs under trusted context
- What are the implications?
  - Steal your cookies for the domain you're browsing
  - Completely modify the content of any page you see on this domain
  - Track every action you do in that browser from now on
  - Redirect you to a Phishing site
  - Exploit browser vulnerabilities to take over machine

2. Injection Flaws

- What is it?
  - User-supplied data is sent to an interpreter as part of a command, query or data.
- Many kinds of injection flaws
  - LDAP, XPath, SSI, MX (Mail)…
  - HTML Injection (Cross Site Scripting)
  - HTTP Injection (HTTP Response Splitting)
- What are the implications?
  - SQL Injection – Access/modify data in DB
  - SSI Injection – Execute commands / access sensitive data
  - LDAP Injection – Bypass authentication


DEMO

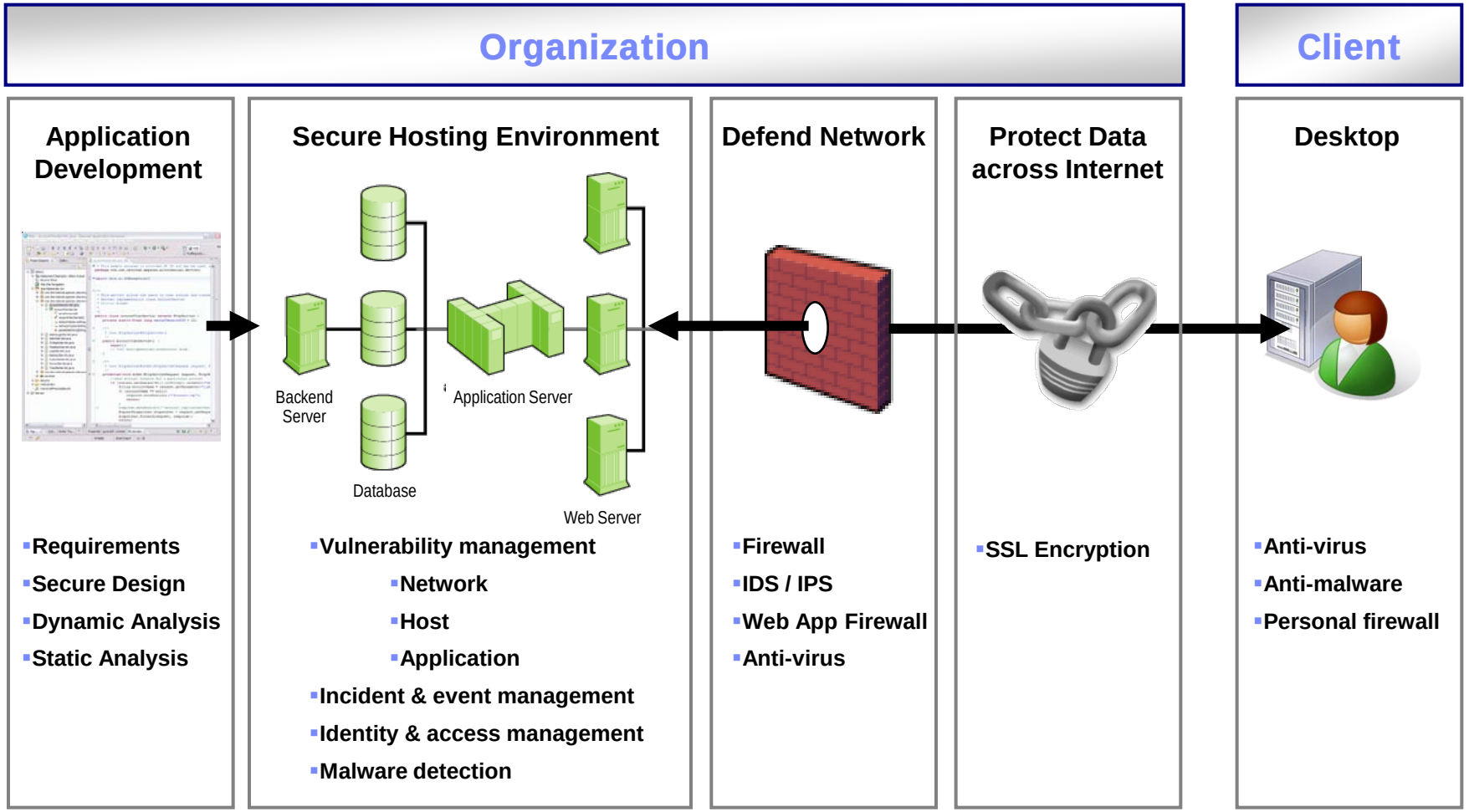
How does Application Security Testing work?

1. Explore source code and/or web site to detect structure

2. Identify Vulnerabilities ranked after severity and show how it was identified

3. Advanced remediation, fix recommendations and security enablement

Secure Web Applications: Who is responsible?

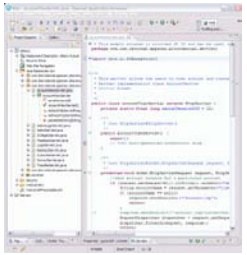


Secure Application Development

Rational. AppScan.

- Challenge
  - Ensure the creation of high quality, secure and compliant software
  - Ensure effective management of secure requirements, design and testing
  - Lifecycle management of vulnerabilities
  - Application Lifecycle Management (ALM)
- IBM Solutions
  - IBM Rational AppScan
    - Dynamic Analysis
    - Static Analysis
    - Runtime Analysis

Application Development



- **Requirements**
- **Secure Design**
- **Dynamic Analysis**
- **Static Analysis**

Required Technologies for Securing the SDLC

- Tier 1: Source Control & Change Request Management
  - Rational ClearQuest
  - Rational ClearCase
- Tier 2: Requirements & Test Management
  - Rational RequisitePro
  - Rational AppScan
  - Rational Quality Manager
- Tier 3: Build Management
  - Rational Build Forge
- Tier 4: Architectural & Asset Management
  - Rational Asset Manager
  - Rational Software Architect

Secure Hosting Environment

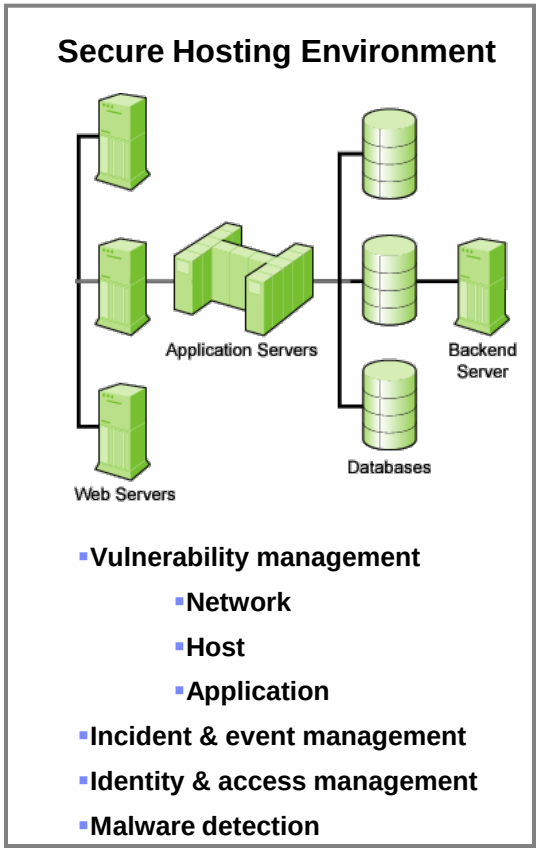
- Challenges
  - Maintain a secure environment
  - Ensure security policies are implemented and enforced
  - Lifecycle management of vulnerabilities and incidents
  - Assess production systems for malware
- IBM Solutions

Tivoli. software

Rational. software

WebSphere. software

IBM Internet Security Systems
Ahead of the threat.™



Required Technologies for Secure Operations

- Protect
  - Block and Enforce
    - ISS Proventia Server*
- Assess
  - Host Configuration
    - Tivoli Security Compliance Manager
  - Network*
    - ISS Proventia Network Enterprise Scanner
  - Application
    - Rational AppScan Enterprise
- Manage
  - Vulnerabilities*
    - ISS Proventia Site Protector
  - Incidents*
    - Tivoli Security Operations Manager

**** Can be managed through IBM ISS Managed Security Services!***

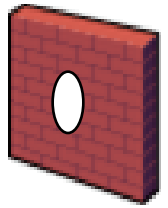
Defending the Network

proventia network
Multi-Function Security

- Challenge
  - Protect your business from Internet threats without jeopardizing bandwidth or availability
  - Protect your end users from spam and other productivity drainers
  - Conserve resources by eliminating the need for specialized security expertise

- IBM Solutions
  - IBM Proventia® Network Multi-Function Security (MFS)
    - Complete protection from Internet threats including firewall, intrusion prevention and anti-virus
    - Define Web access policies
  - IBM Proventia® Network Intrusion Prevention System (IPS)
    - Provides Web Application Firewalling functionality without the additional point product investment of a WAF
    - Provides inline network protection against all major categories of Web application vulnerabilities and attacks

Defend Network



- **Firewall**
- **IDS / IPS**
- **Web App Firewall**
- **Anti-virus**

Encrypting transmission across the Internet

WebSphere software

- Challenge
  - Ensuring data and intellectual property is not stolen while crossing the Internet
  - Ensuring that data is not tampered with or altered between the server and client
  - Ensure that a malicious site does not impersonate the legitimate server and establish communication with the client
- IBM Solutions
  - IBM Websphere Application Server
  - IBM Websphere DataPower XML Security Gateway

Protect Data across Internet

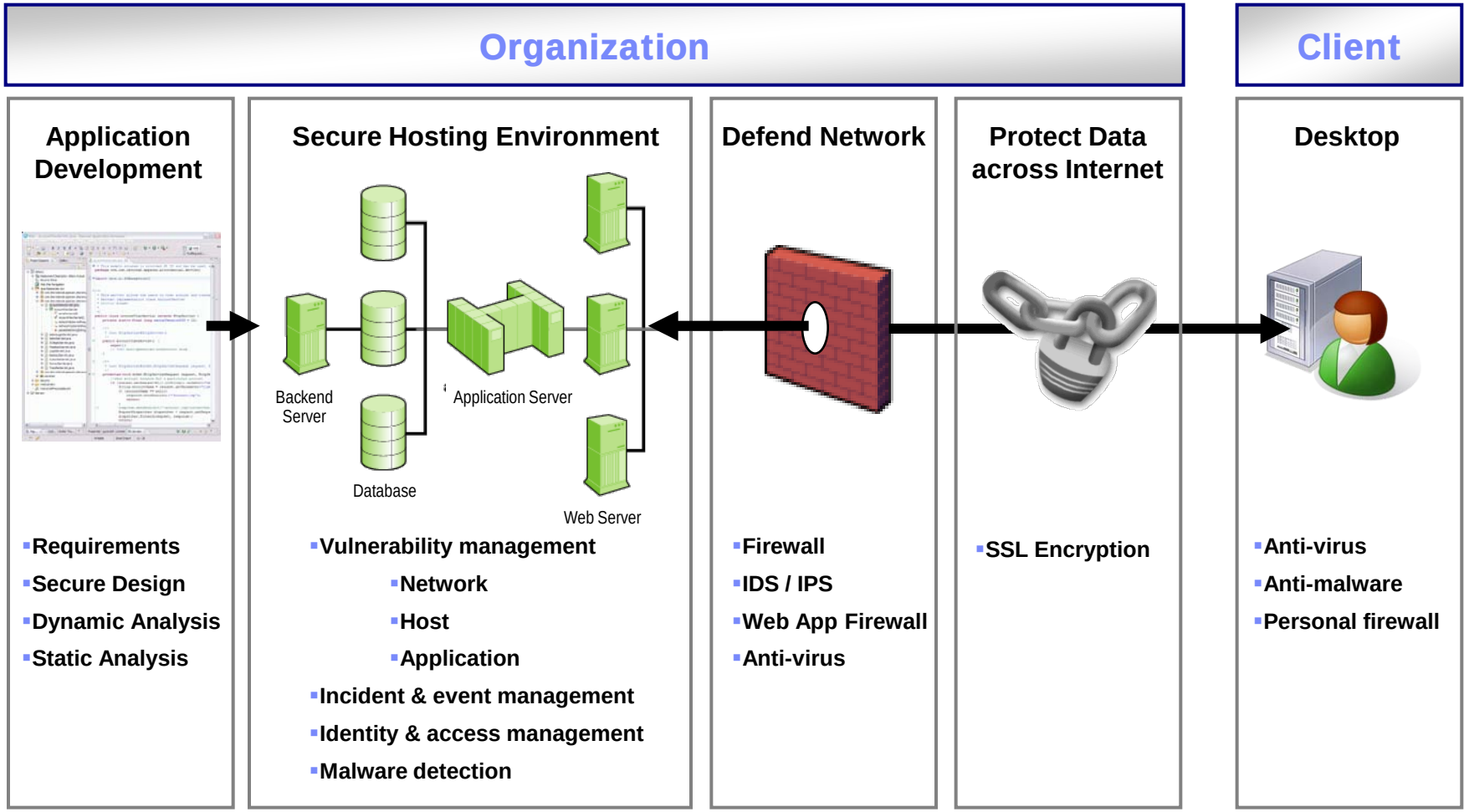
- **SSL Encryption**

Client-side Security

proventia desktop Endpoint Security

- Organization can not control their external clients
- Internal client challenges
  - Mitigating risks posed by zero-day, targeted attacks
  - Protecting critical data and intellectual property
  - Minimizing costs and lost productivity associated with remediating infected endpoints
  - Reducing help desk calls
- IBM Solution
  - IBM ISS Proventia Desktop and Server
    - Multi-layered protection in a single agent
    - Mitigates against application and network vector attacks
    - Patented Virus Prevention System blocks malware based on behavior
    - Includes signature anti-virus/anti-malware signatures

Secure Web Applications: A Complete Approach




Questions


Welcome to Innovation 2009
IBM Rational Software Conference