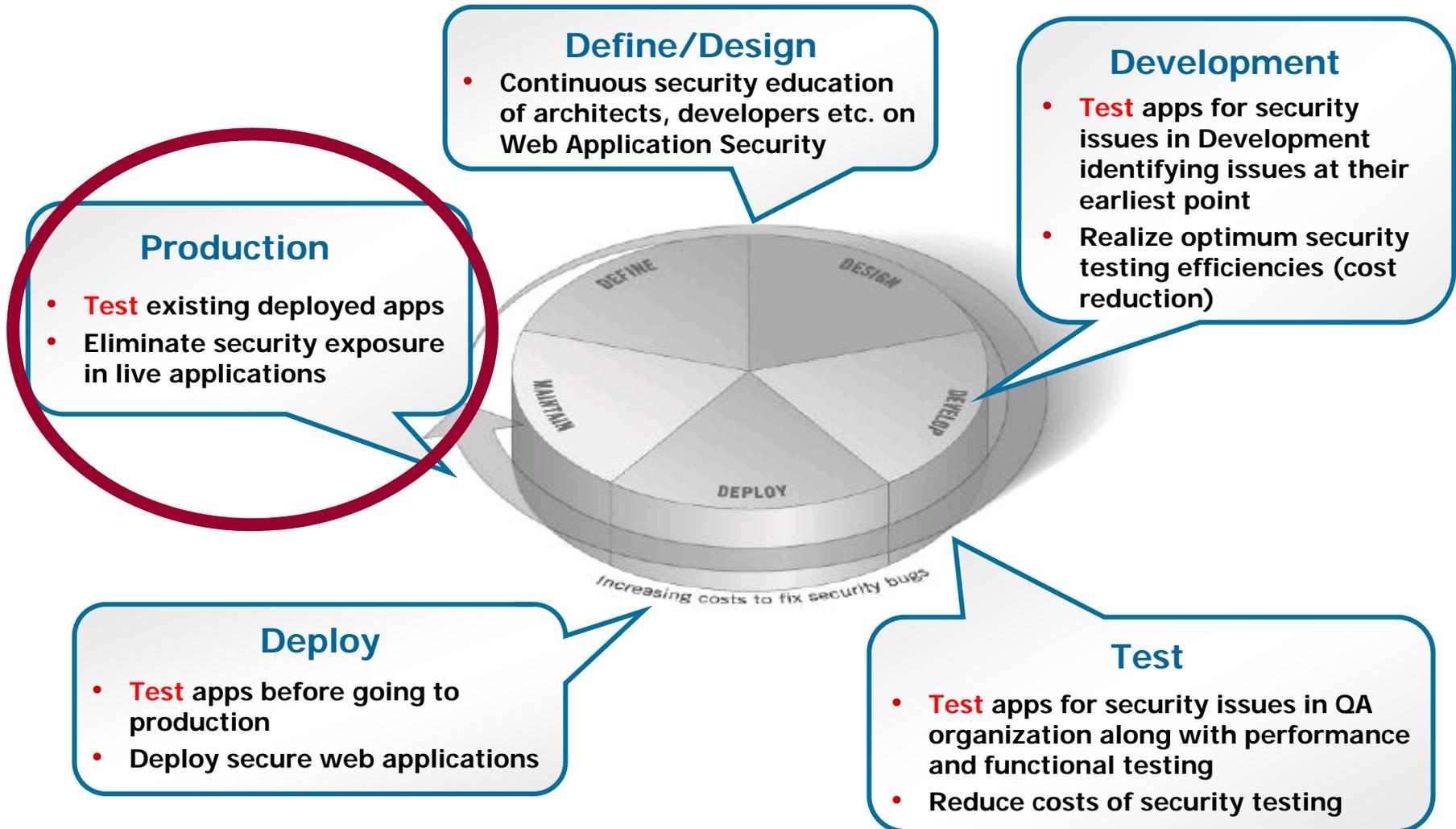




Production Security and the SDLC

Mark Kraynak
Sr. Dir. Strategic Marketing
Imperva
mark@imperva.com

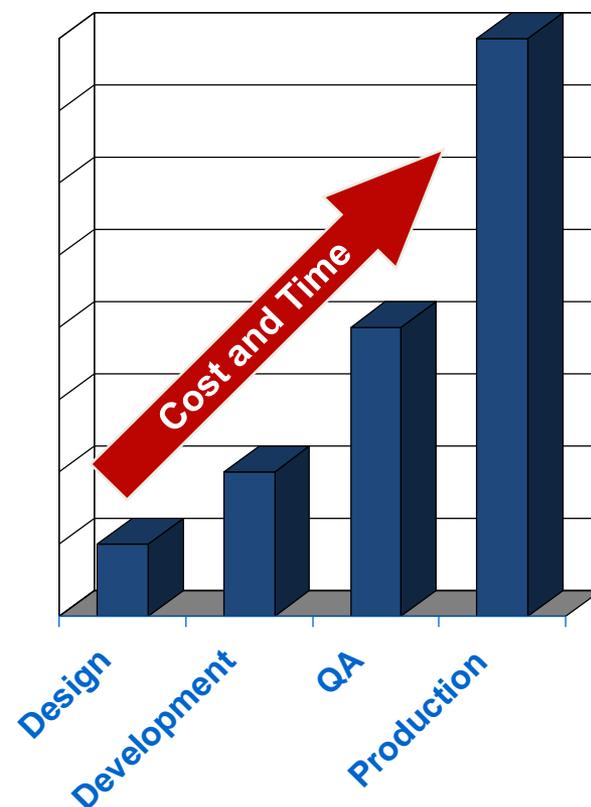
Building Security Into the Development Process



Fixing Production Vulnerabilities is Costly

- Cost Increases Over Life Cycle
- Many Vulnerabilities Only Found in Production Environment
 - + Complexity of entire infrastructure
 - + Identified by new attacks and probes
- Cost = Fix and Test + Risk
 - + Cost diverting development & QA staff
 - + Risk of attack before fix in production
 - + Risk of "rush" fix without full testing

Cost and Time to Fix Vulnerability



...and Difficult

- 92% of Web applications have vulnerabilities
 - + Cross Site Scripting (XSS) – 80%
 - + SQL Injection – 62%
 - + Parameter Tampering – 60%
- 93% of vulnerable sites - still vulnerable after code fixes
- Do not take my word for it
 - + Check other sources
 - + Ask your security operations team

Why Can't We Get This Right?

Ideal

- Custom code is **immediately** fixed by programmers and application is redeployed
- Patches for 3rd party components are **immediately** installed

Reality

- Resource allocation
 - + New Projects & Staff Turnover
- Coding & Deployment time span
- Cost
- Patch (non) availability
- Deployment time span
- Stability

Address Risks through External Mitigation

Assess

- Scan application for vulnerabilities
- Describe remediation steps for app developers
- Export vulnerability results for proactive protection

Set Policies/Controls

- Dynamically learn app structure
- Apply granular controls based on discovered vulnerabilities
- Recognize application changes
- Implement code fixes on developers' schedule

PRODUCTION APPLICATION SECURITY LIFECYCLE

Measure

- Built in & custom reports
- Roll-up & drill down of data
- Security event analysis

Monitor and Enforce

- Alert and block in real-time
- Ensure end user accountability
- Capture full details
- Provide security at all layers



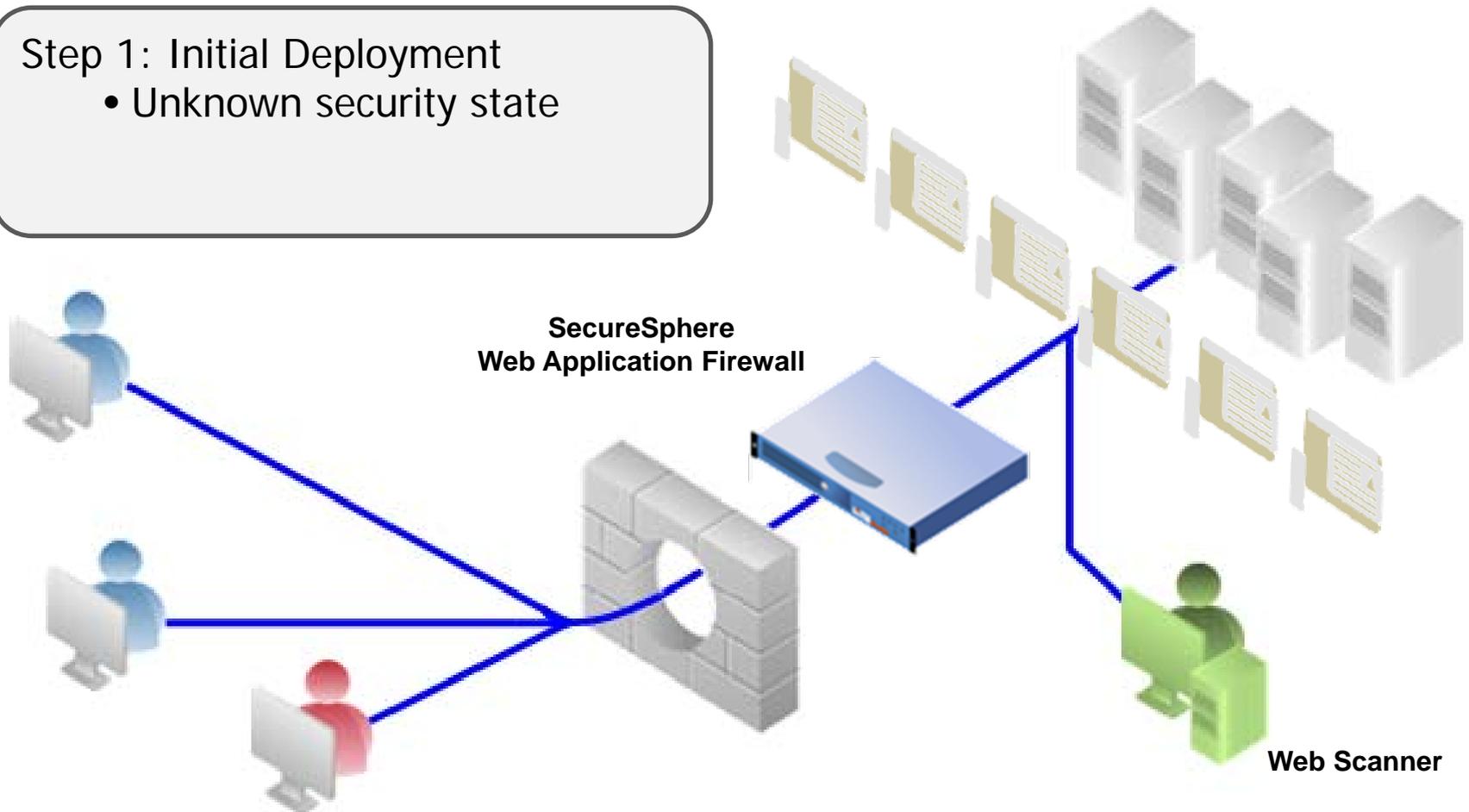
Example 1

Integrating WAF and Scanning

Web Security Lifecycle

Step 1: Initial Deployment

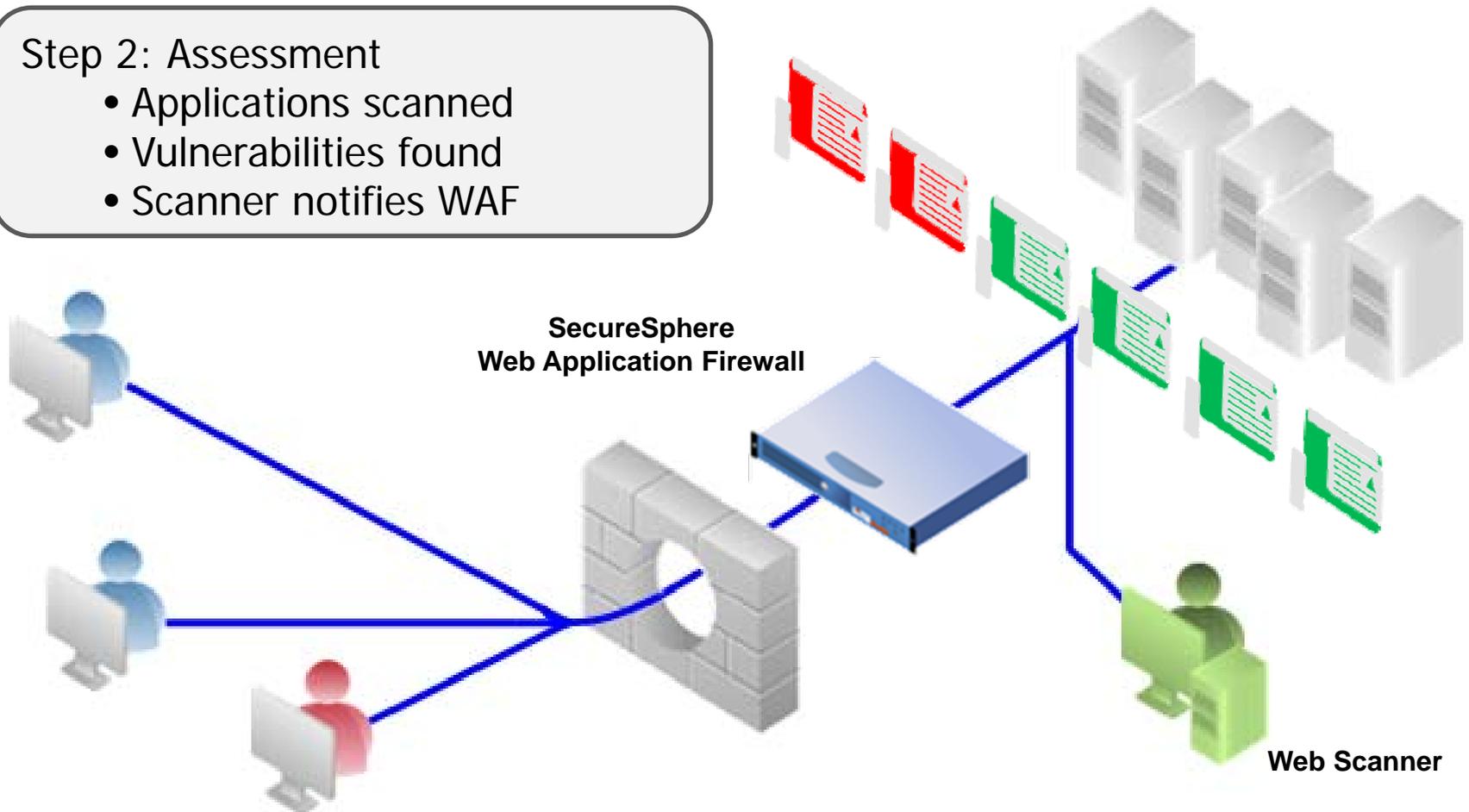
- Unknown security state



Web Security Lifecycle

Step 2: Assessment

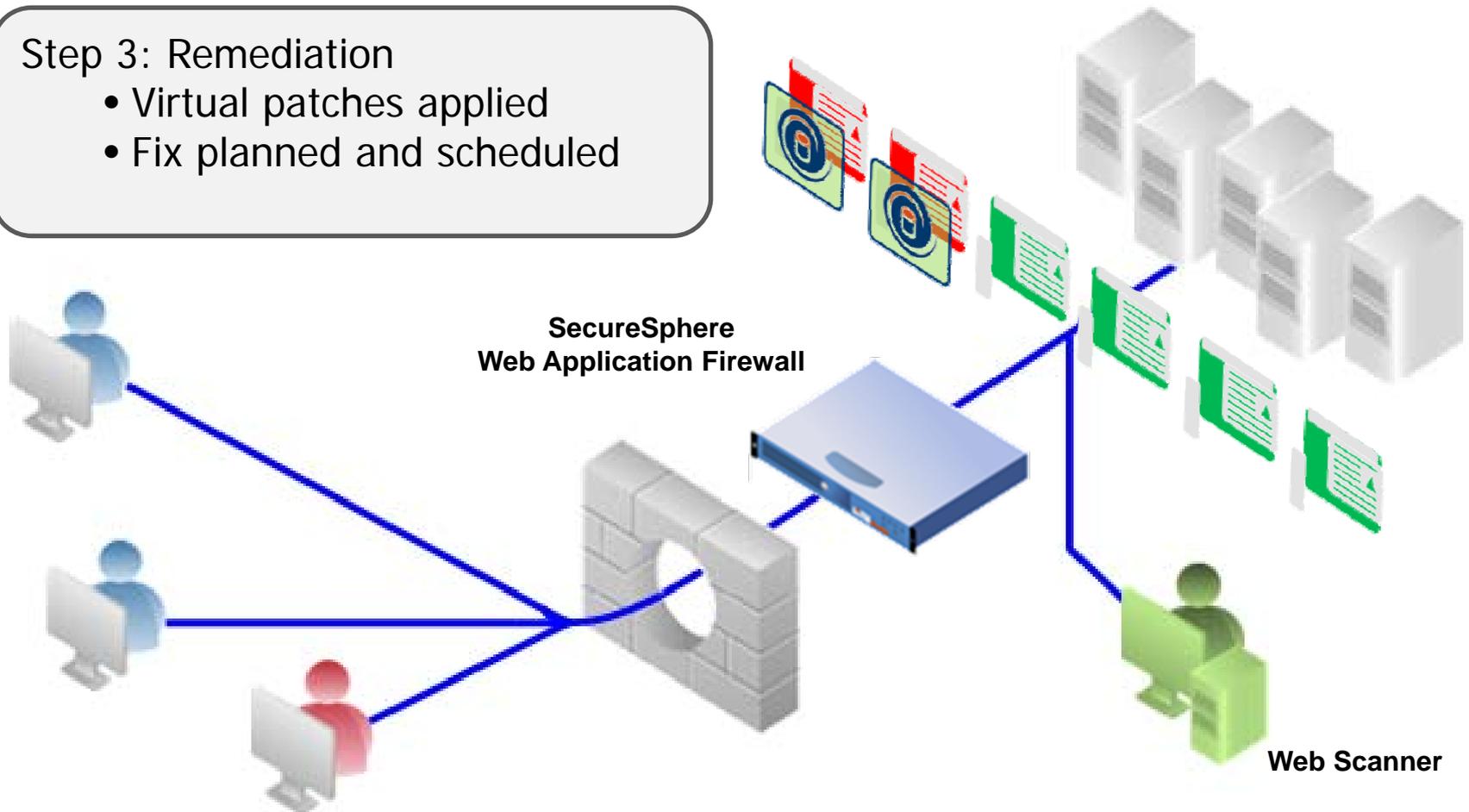
- Applications scanned
- Vulnerabilities found
- Scanner notifies WAF



Web Security Lifecycle

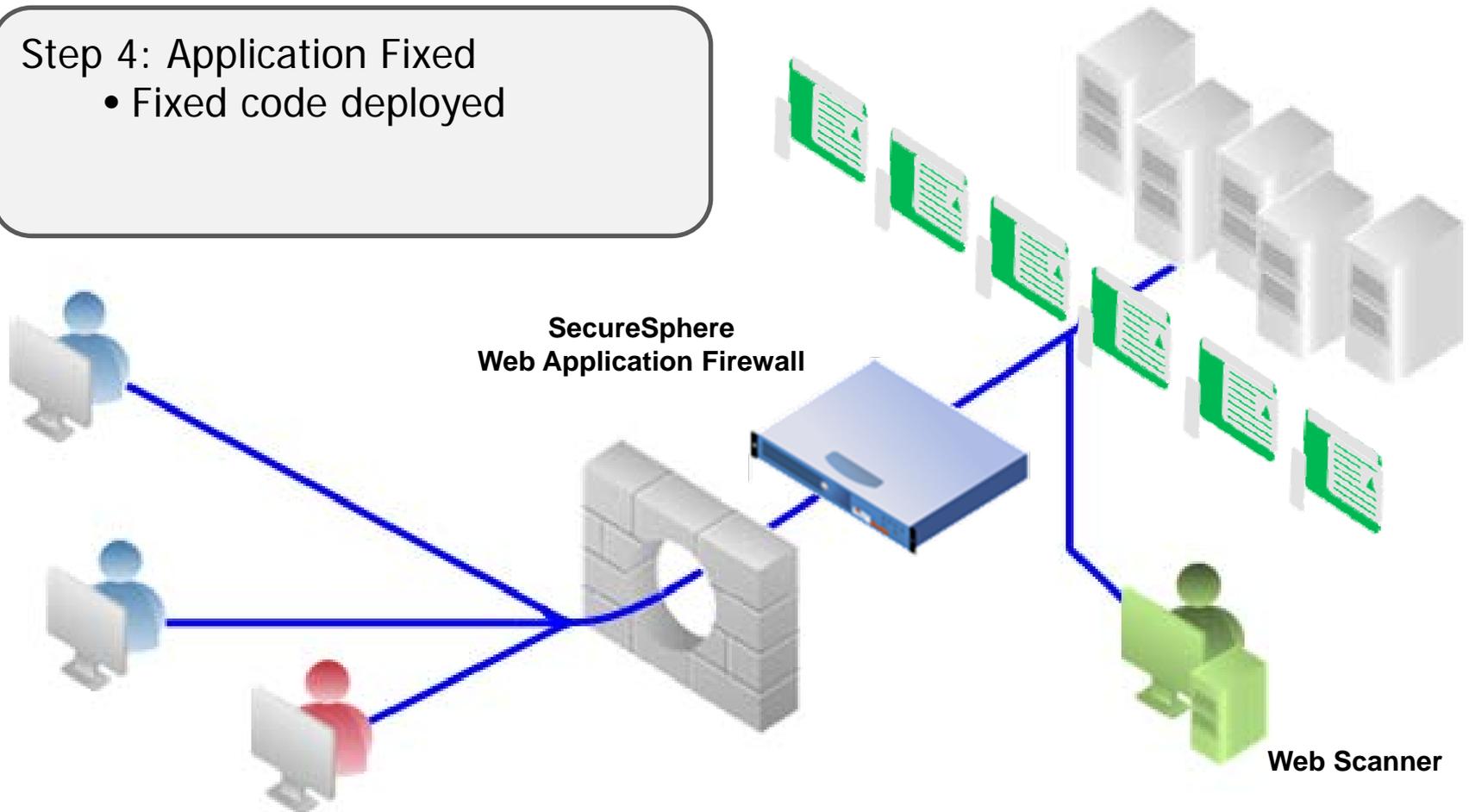
Step 3: Remediation

- Virtual patches applied
- Fix planned and scheduled



Web Security Lifecycle

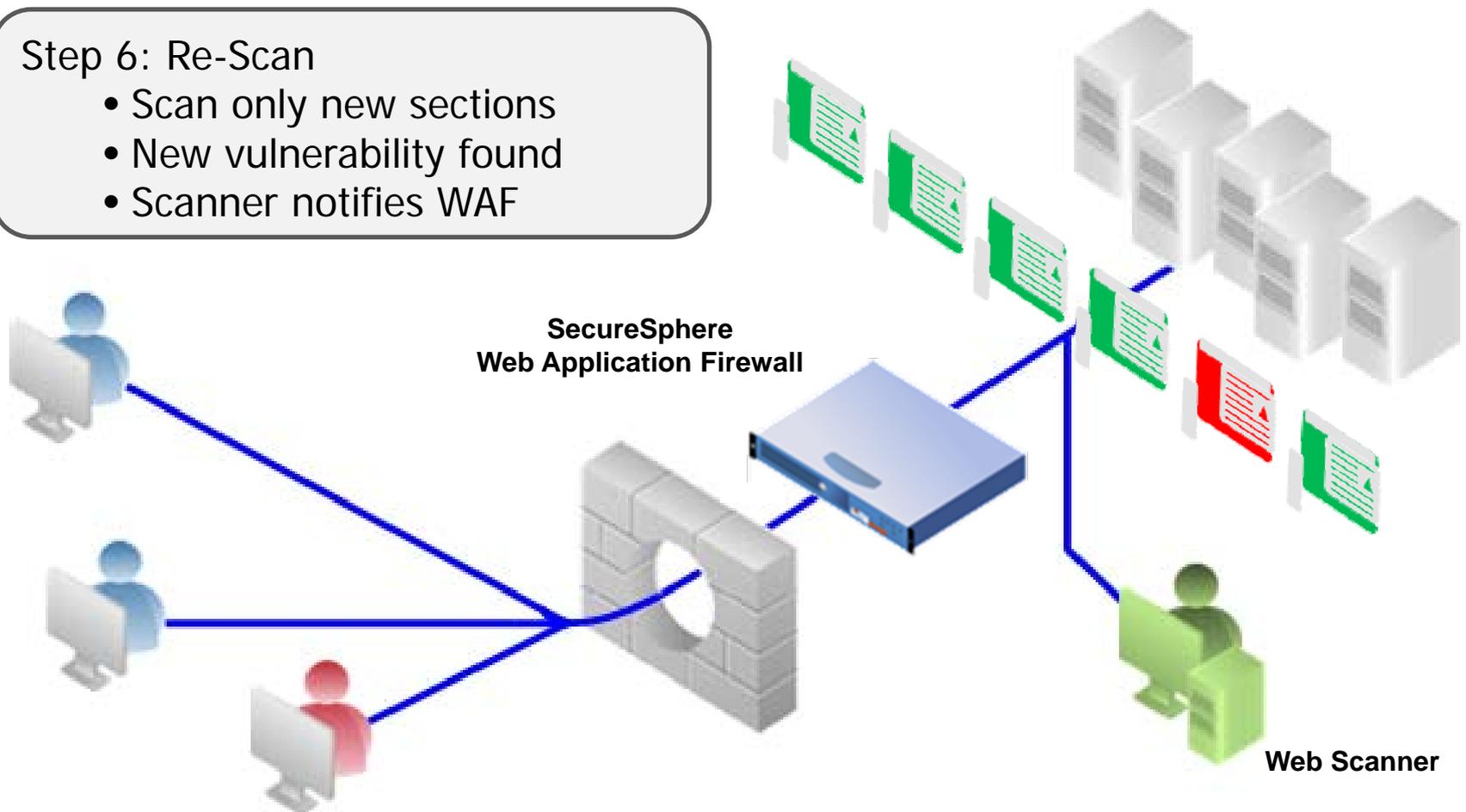
Step 4: Application Fixed
• Fixed code deployed



Web Security Lifecycle

Step 6: Re-Scan

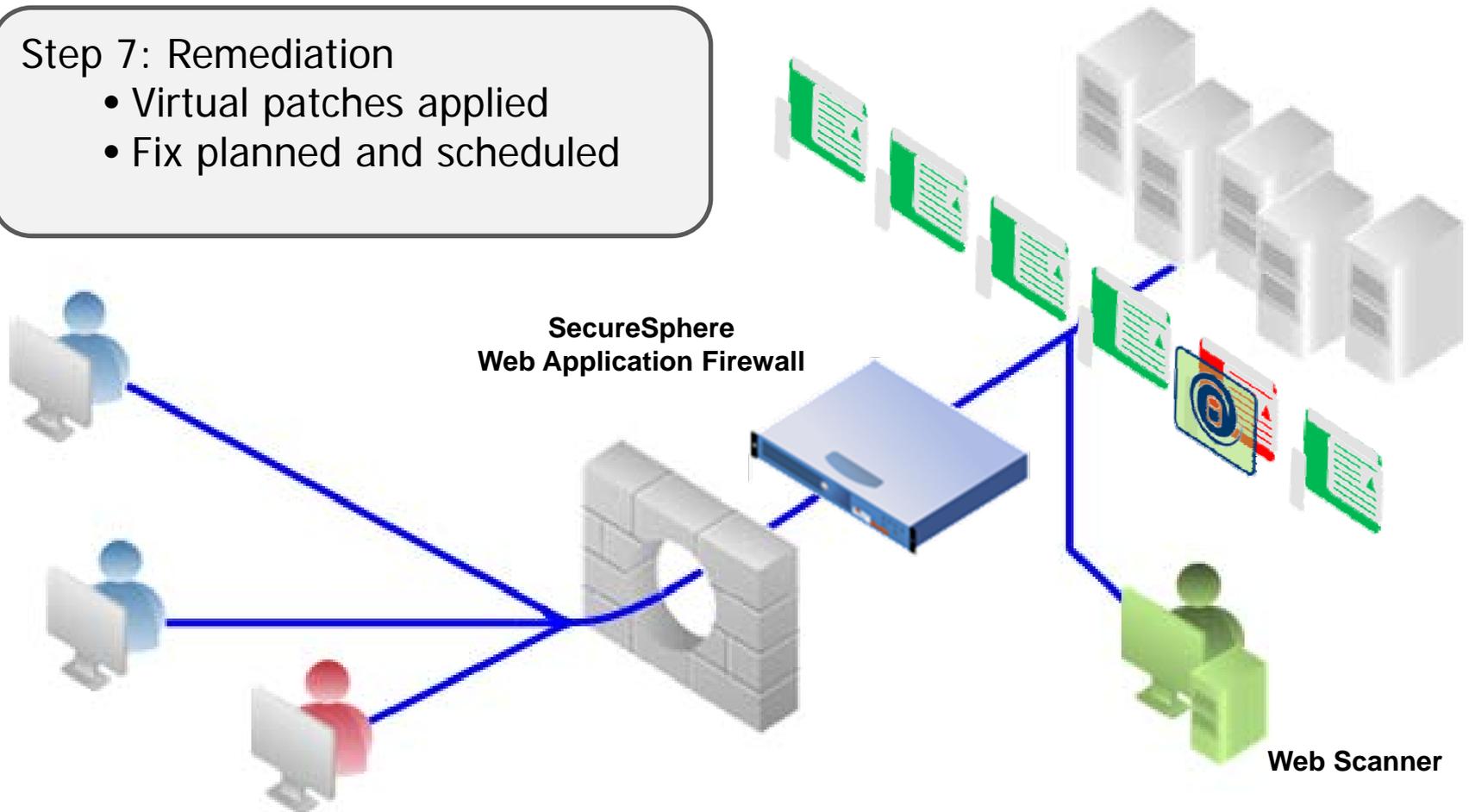
- Scan only new sections
- New vulnerability found
- Scanner notifies WAF



Web Security Lifecycle

Step 7: Remediation

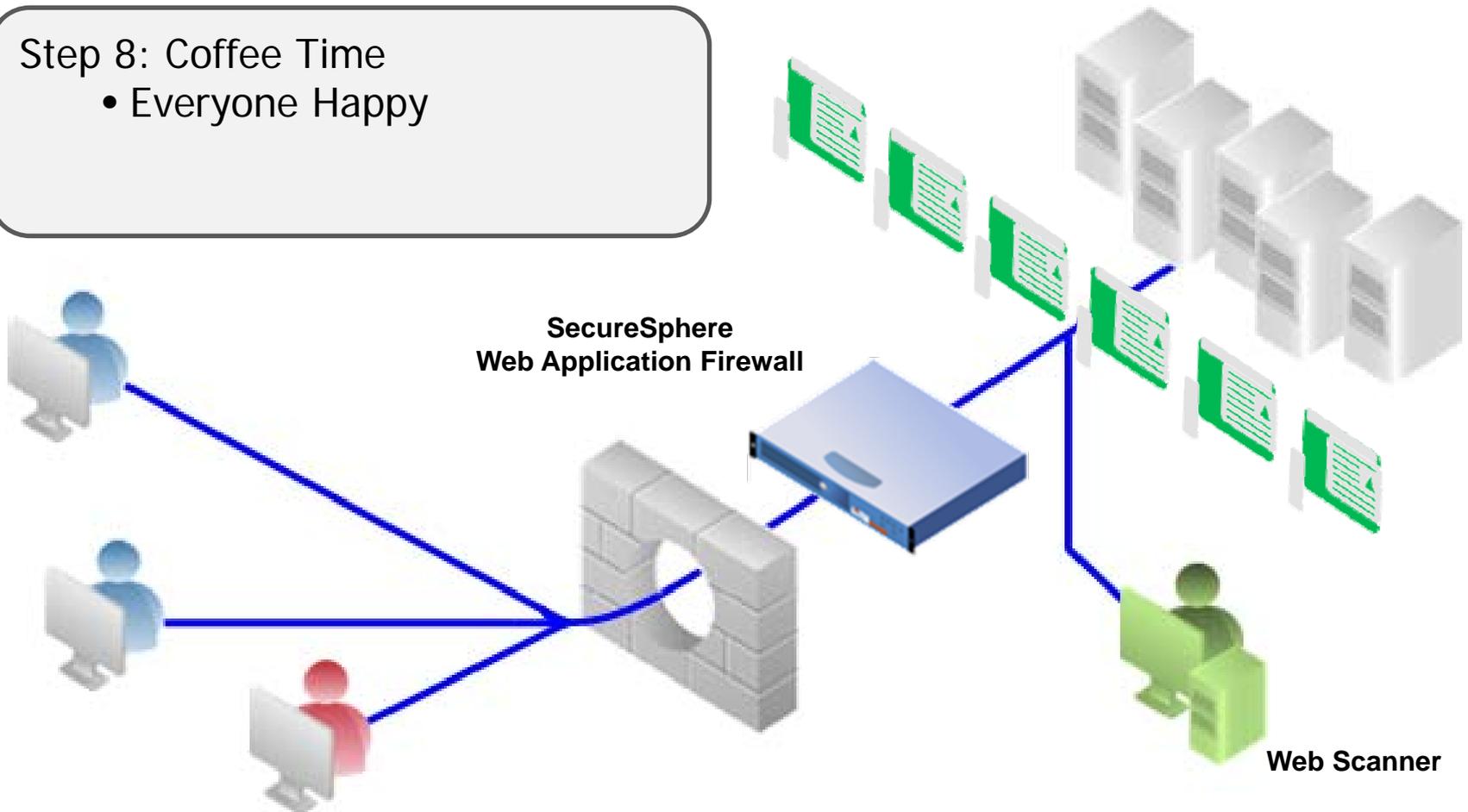
- Virtual patches applied
- Fix planned and scheduled



Web Security Lifecycle

Step 8: Coffee Time

- Everyone Happy





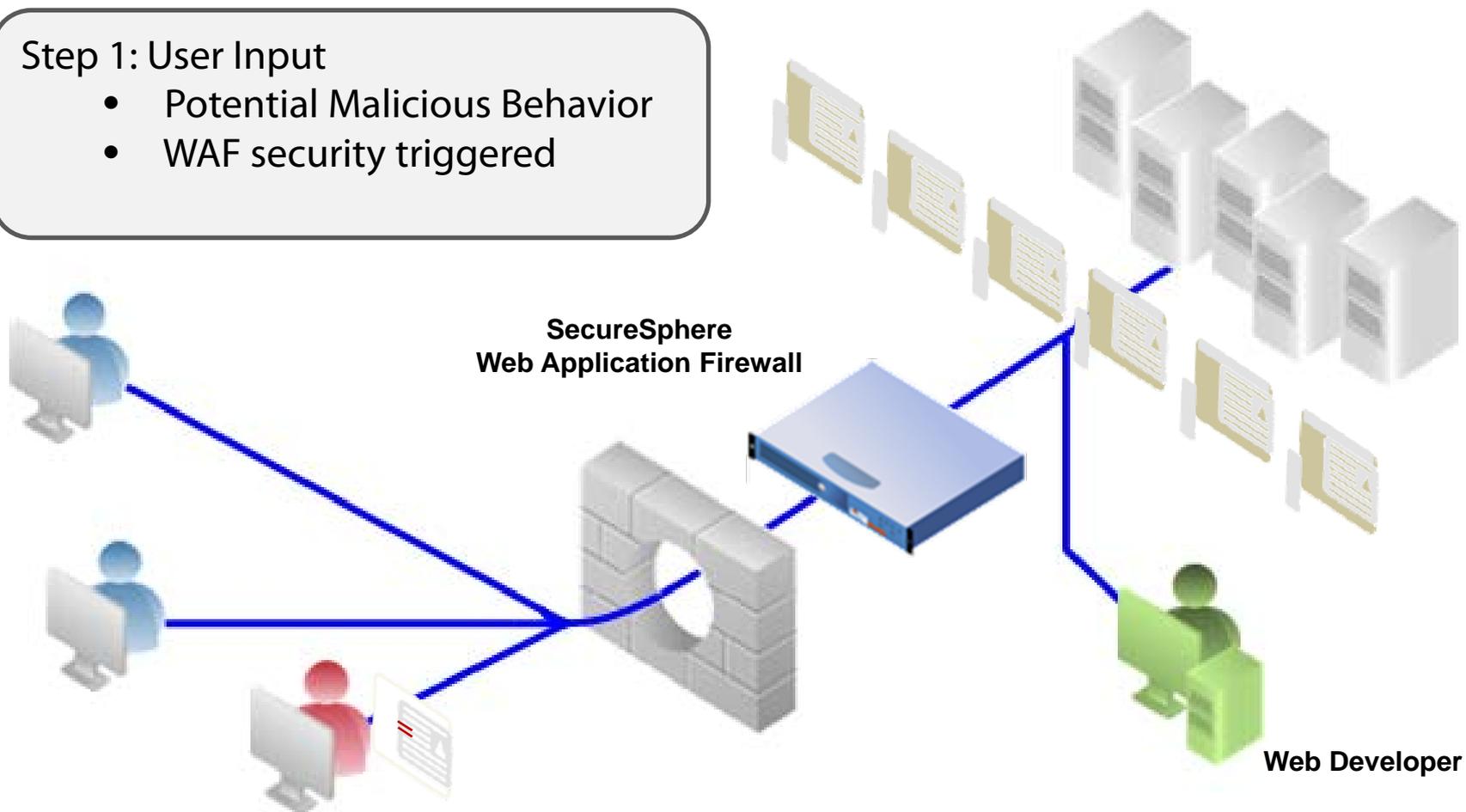
Example 2:

Web Activity Monitoring Feeding SDLC

WAM

Step 1: User Input

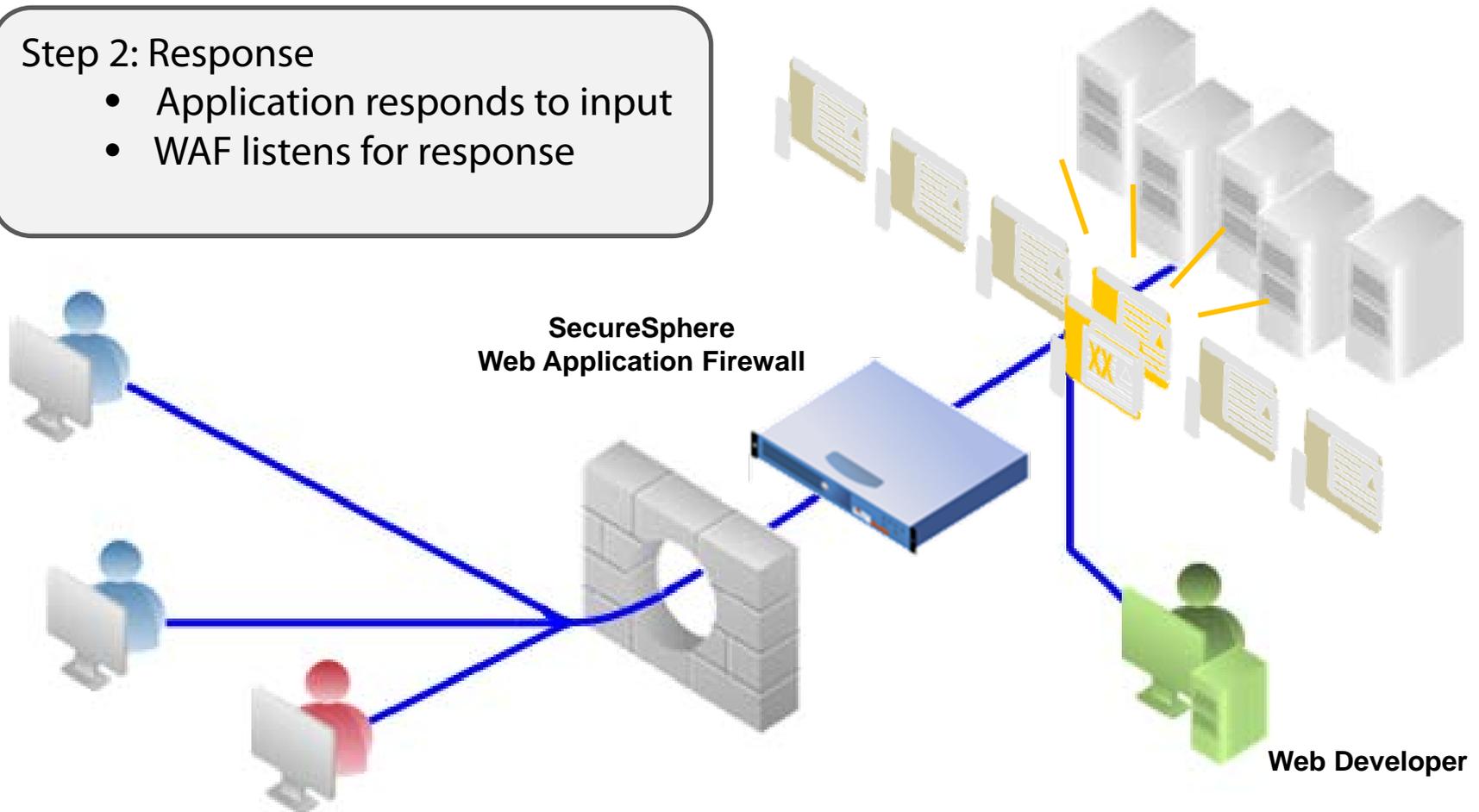
- Potential Malicious Behavior
- WAF security triggered



Web Security Lifecycle

Step 2: Response

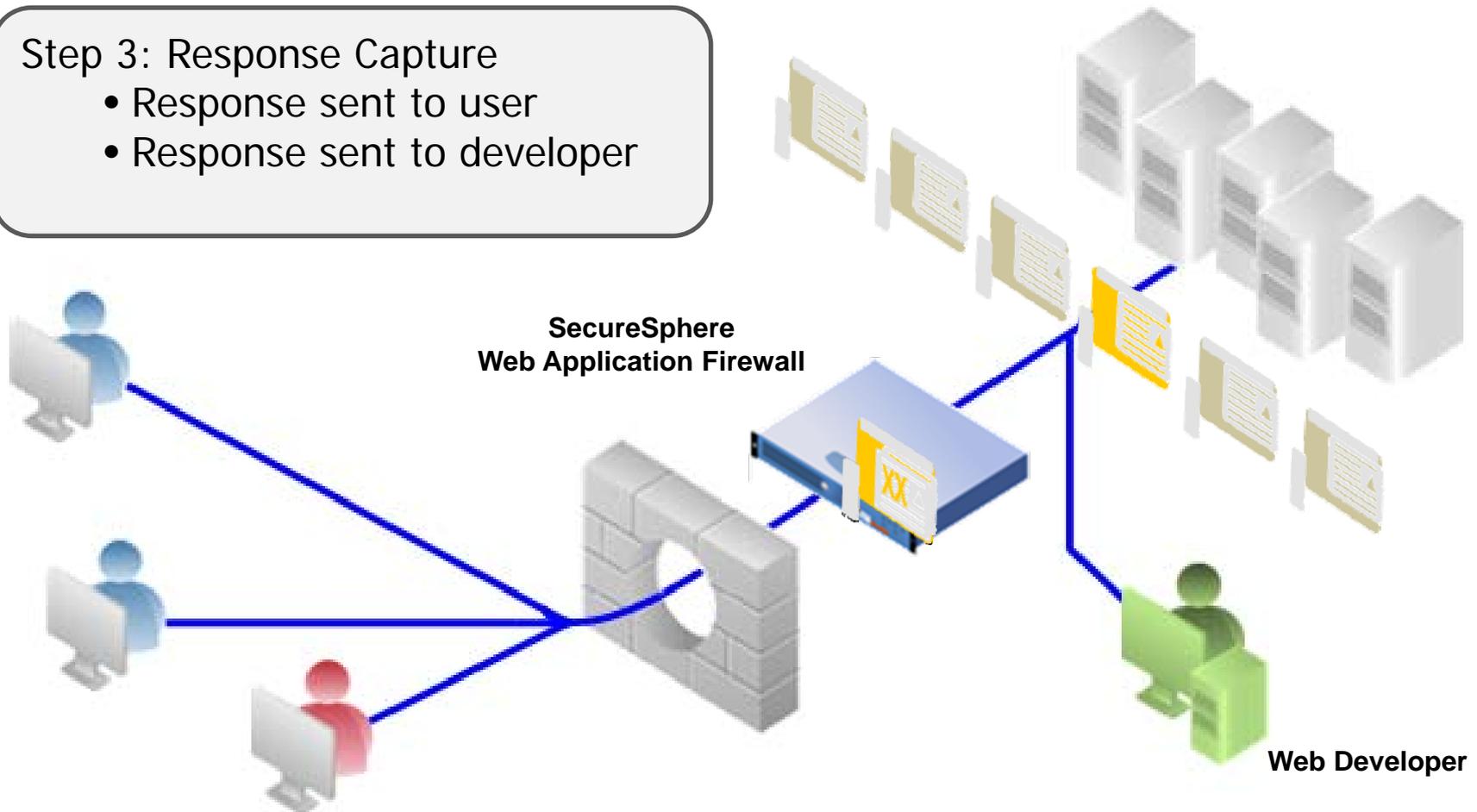
- Application responds to input
- WAF listens for response



Web Security Lifecycle

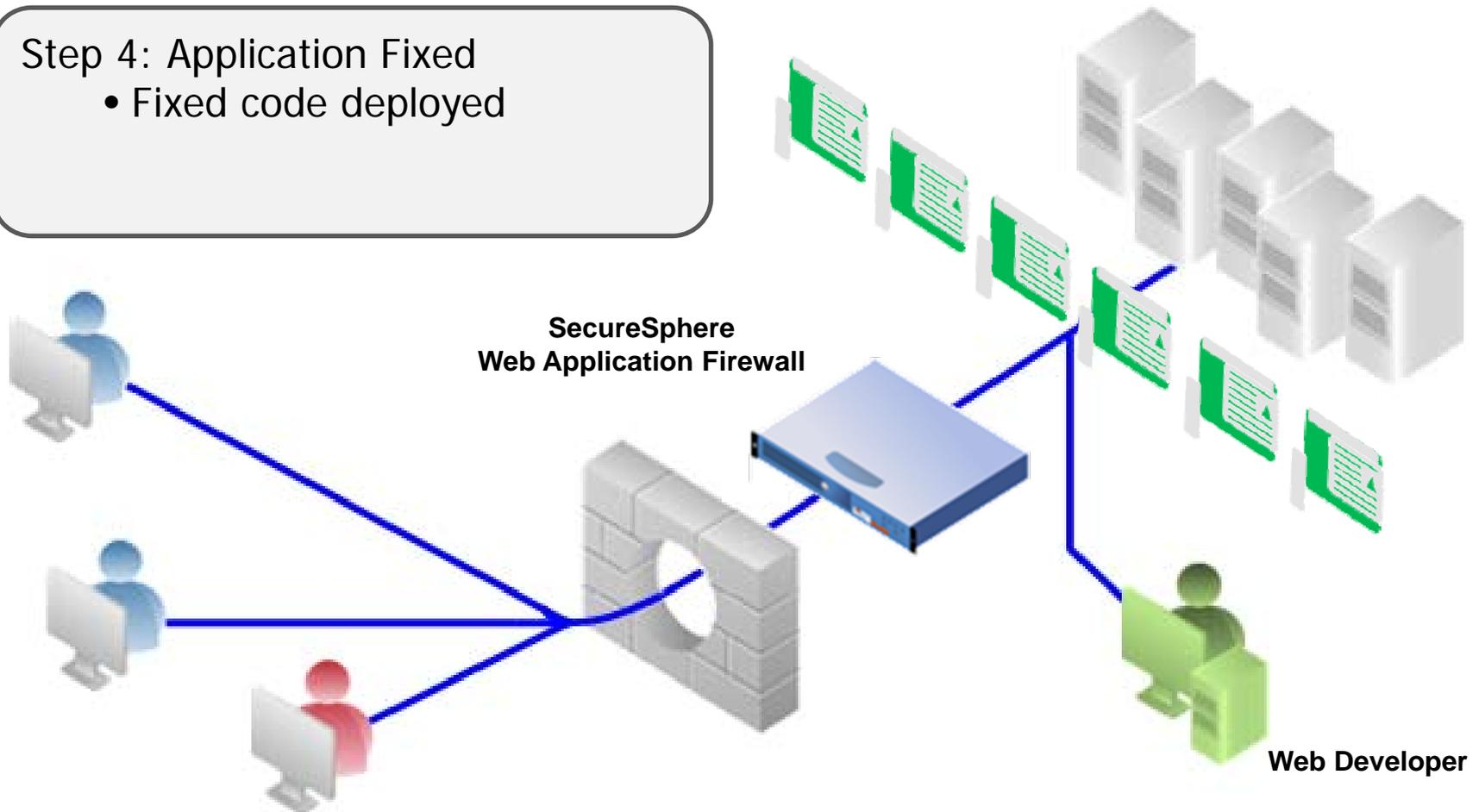
Step 3: Response Capture

- Response sent to user
- Response sent to developer



Web Security Lifecycle

Step 4: Application Fixed
• Fixed code deployed



The Market Leader in Application Data Security

Only complete solution for visibility and control over business data

- Consistent industry recognition of technical superiority



More application data security deployments than any other vendor

- Over 600 direct customers
- 54 Fortune 1000
- 86 Global 2000
- Over 4500 protected organizations

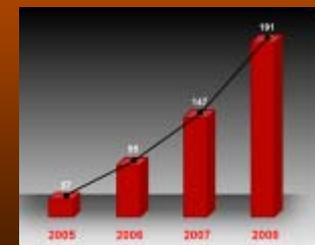
Veteran leadership with deep industry expertise

- Approximately 200 employees
- Only research team dedicated to application data security



Consistent growth fueled by:

- Surge in data breaches
- Regulatory compliance requirements
- Tightening Data Security legislation



Imperva SecureSphere Product Line

