Introduction to AppScan Enterprise
Contents

- The Application Security Problem
- What is AppScan Enterprise?
- Main Features
- How does AppScan Enterprise work?
- Key Concepts and Terminology
- User Interface Tour
The Web Application Security Reality

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

2/3 of All Web Applications Are Vulnerable

Sources: Gartner, Watchfire
Web Application Security Challenges

1. Security Team Has Become a Bottleneck
2. Lack of Control and Visibility
3. Catching Problems Late in the Cycle
4. Not Monitoring Deployed Applications
5. Difficulty Managing 3rd Party Vendors
Solving The Problem Requires a Strategic Approach

Web Application Security Evolution

- **Strategic**
  - Enterprise-Wide
  - Scalable Solution

- **Tactical**
  - Manual Efforts, Desktop Audit Tools
  - 2-3 Internal Security Experts

- **Outsourced**
  - Consultants
  - Pen Testing

- **Unaware**
What is AppScan Enterprise?

**Scale**
- Reuse and Run Multiple Scans Across Applications

**Inform**
- Push Reports to Developers, QA, and Non-Security Staff

**Monitor**
- Manage Problem Resolution Through Trending Reports

AppScan Enterprise

Security Team

Integrate Web Application Security in the SDLC
AppScan Enterprise – Key Features & Benefits

1. Controlled, Web-based Application Testing
   - Enable Development and QA to perform testing during SDLC
   - Control what applications each user can test

2. Controlled, Web-based Report Distribution
   - Easily distribute reports
   - Control the access to information

3. Enterprise Metrics and Visibility
   - Increase visibility and better understand enterprise risks

4. Issue Management
   - Focus on fixing issues, not just finding issues
Multiple Report Levels

- Dashboards
- Report Pack Summaries
- Detailed Reports
- About this… Reports
Report Categories

- Inventory Reports
  - Broken Links
  - Hosts
  - Pages
  - etc.

- Security Reports
  - Application Security Issues
  - Infrastructure Security Issues
  - Remediation Tasks
  - Security Risk Assessment

- Compliance Reports
  - Safe Harbour
  - Sarbanes-Oxley Act (SOX)
  - Visa CISP
  - etc.
User Roles and Access Permissions

- Control access to information
- Assign user roles
- Specify what applications a user can scan
- Specify what types of tests a user can perform
What does AppScan Enterprise test for?

AppScan Enterprise

- Web Applications
- Third-party Components
- Web Server Configuration
- Web Server
- Database
- Applications
- Operating System
- Network
How does AppScan Enterprise work?

- Traverses a web application
- Approaches an application as a black-box
- Tests by sending modified HTTP requests
- Thousands of tests for identifying hundreds of vulnerabilities
AppScan Enterprise Architecture

Clients
- Developer
- Compliance Officer
- QA Specialist
- Pen Tester

AppScan Enterprise
- ASE Control Center Server
- ASE Database Server
- ASE Agent Servers

Target Sites
- Web Servers
Terminology

- Content Scan Job
- Infrastructure Scan Job
- Import Job
- Report Pack
- Dashboard
- Folder
Jobs, Report Packs, Reports & Dashboards

Job1
Security Scan

Job2
Security Data Import

Job3
Security Scan

Job4
Infrastructure Scan

Global Scan Data

Reports

Report Pack 1

Report Pack 2

Report Pack 3

Dashboard 1

Dashboard 2
Web-Based User Interface

Navigate to AppScan Enterprise, e.g. http://aseserver/appscan

Enter your user name and password
Quick Scan vs. Advanced View

- The UI mode is set in the user’s properties

Quick Scan View
- Makes it easier to create a scan by abstracting complexity
- Leverages scan templates created by the administrator
- Reduces the scan configuration time
- Suitable for developers, QA specialists who create ad-hoc scans

Advanced View
- Exposes all scan options
- Suitable for administrators and advanced users