CONTINUOUS APPLICATION SECURITY AT SCALE WITH IAST AND RASP
ENTERPRISE APPLICATIONS ARE 37% OF IT SPEND ... AND GROWING 24.8% ANNUALLY

Every dollar spent on enterprise applications increases vulnerability
Application security has been the leading cause of breaches for the past nine years.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Organization</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>World Trade Org</td>
<td>U.S. Army</td>
<td>LinkedIn</td>
</tr>
<tr>
<td>SAP</td>
<td>United Nations</td>
<td>Royal Navy</td>
</tr>
<tr>
<td>Wall Street Journal</td>
<td>Heartland</td>
<td>JP Morgan</td>
</tr>
<tr>
<td>LivingSocial</td>
<td>TARGET</td>
<td>Diners Club</td>
</tr>
<tr>
<td>Tesla</td>
<td>JC Penney</td>
<td>PBS</td>
</tr>
<tr>
<td>JOHNS HOPKINS</td>
<td>Microsoft UK</td>
<td>VISA</td>
</tr>
<tr>
<td>Yahoo</td>
<td>NASDAQ</td>
<td>Sony Music</td>
</tr>
<tr>
<td>FBI</td>
<td>7-Eleven</td>
<td>Sony Playstation</td>
</tr>
<tr>
<td>HBGary Federal</td>
<td>Guess</td>
<td>Sony Pictures</td>
</tr>
<tr>
<td>NASA</td>
<td>Yahoo!</td>
<td>IRS</td>
</tr>
<tr>
<td>Adobe</td>
<td>eHarmony</td>
<td>U.S. Dept of Census</td>
</tr>
</tbody>
</table>

Source: 2016 Verizon Data Breach Investigation Report (DBIR)
TRADITIONAL APPSEC PROGRAMS ARE FAILING

Application Portfolio

Traditional AppSec Program

Awful Results

Assurance

Process Fit

Coverage

TRADITIONAL APPSEC PROGRAMS ARE FAILING

Application Portfolio

Traditional AppSec Program

Awful Results

Assurance

Process Fit

Coverage
A HISTORY OF APPLICATION SECURITY AUTOMATION

Development (find vulnerabilities)

- SAST (Static AppSec Testing)
- DAST (Dynamic AppSec Testing)
- IAST (Interactive AppSec Testing)

Operations (block attacks)

- WAF (Web Application Firewall)
- IDS/IPS (Intrusion Detection/Prevention System)
- RASP (Runtime Application Self-Protection)

Unified Agent IAST and RASP
SOFTWARE TRENDS CHALLENGING SAST/DAST/WAF

- **Libraries**: Explosive growth in libraries and frameworks.
  - SAST can’t handle scale and complexity of supply chain.

- **Services**: Microservices, APIs, REST/XML services.
  - SAST and DAST can’t handle API and web service complexity.

- **Cloud**: Rapidly growing use of cloud and containers.
  - WAF can’t handle infrastructure deployment pace and complexity.

- **Agile**: High speed software development.
  - SAST, DAST, and WAF all require experts in the critical path.
Contrast IAST & RASP deliver security where it’s needed.

Contrast IAST/RASP Agent instruments your application with sensors that protect against both vulnerabilities and attacks.

All agents report to Contrast TeamServer to protect the entire application portfolio in parallel.
DETECTING AND BLOCKING BOTH ATTACKS AND VULNERABILITIES

Sensors woven into running application

Security context assembled within Contrast Agent

- Developer
- Tester
- User
- Attacker

Controller, Validation, Session, Business Logic, Data Layer, SQL API

- HTTP Request
- Validation Tags
- Data Tracking
- Data Parsing
- Escaping Tags
- Query

Database

- Vulnerability?
- Attack?
Software is a black box.

ACCUACY: IAST/RASP HAS AN UNFAIR ADVANTAGE

IAST/RASP provide full visibility into running application
Contrast accurately identifies vulnerabilities in real-time without scanning or hacking.
Contrast blocks attacks efficiently and accurately with full application context.
Contrast instantly profiles all of your applications, open-source libraries, and servers.
IAST accuracy dominates SAST and DAST

OWASP Benchmark - 21,000 test cases across a range of vulnerabilities

Sponsored by DHS
**PERFORMANCE: IAST AND RASP ARE BLAZINGLY FAST**

<table>
<thead>
<tr>
<th>WebGoat</th>
<th>RASP Processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical traffic</td>
<td>50 microseconds</td>
</tr>
<tr>
<td>Mixed traffic</td>
<td>170 microseconds</td>
</tr>
<tr>
<td>Heavy attack traffic</td>
<td>230 microseconds</td>
</tr>
</tbody>
</table>

- Number of applications doesn’t matter
- As fast or faster than if it was coded by hand
- No bottleneck on either bandwidth or CPU (next slide)
Three problems:

1) Bottleneck
2) Impedance mismatch
3) False alarms – no context
IAST AND RASP ARE A DISTRIBUTED APPROACH

Enable application portfolio with IAST/RASP agents.

Continuous assessment and protection in parallel.

Assurance

Process Fit

Coverage
Imagine managing application security policy at scale

- Development
- Environment
- Continuous Integration
- Unit Testing
- QA Testing
- Performance and Usability Testing
- Staging and Acceptance
- Production

- External Apps
- Internal Apps
- Frameworks
- Third Party Apps
- Legacy Apps
- New Development
- Web Services/APIs
- Cloud/Mobile/IoT
- Web Apps

- application security
- development
- information security
- compliance
• Contrast offers a unified IAST and RASP product (SAAS and on-premise)
• Proven with high-profile customers in:
  – Global Financial Services
  – eCommerce/Retail
  – Healthcare
  – Software
  – Government/Defense
  – Many more...
• Continuously assessing and securing thousands of applications (10 billion SLOC)
• Discovering over 6,000 zero-day vulnerabilities monthly - ~72,000 annually
Are you ready for real application security?