Client-Side Defense Sizing

F5 Distributed Cloud Client-Side Defense provides protection against Magecart, formjacking, digital skimming, and other malicious JavaScript supply chain attacks.

Requirements Assessment

Client-Side Security Concerns

What client-side threats are you concerned about?

- **Magecart attacks** - Credit card skimming via JavaScript
- **Formjacking** - Credential theft from forms
- **Digital skimming** - PII harvesting
- **Supply chain attacks** - Compromised third-party scripts
- **Data exfiltration** - Unauthorized data transmission
- **Page tampering** - Unauthorized DOM modifications

Have you experienced client-side attacks?

- Yes - Describe:
- No
- Unknown

Application Scope

Pages Requiring Protection

Which pages handle sensitive data and require protection?

PAGE TYPE	URL PATTERN	SENSITIVE DATA TYPE
Login pages	Enter value	☐ Credentials
Registration forms	Enter value	☐ PII
Checkout/Payment	Enter value	☐ Payment card data
Account settings	Enter value	☐ PII ☐ Financial
Contact forms	Enter value	☐ PII
Other: Enter value	Enter value	Enter value

Transaction Volume

Estimated monthly transactions on protected pages:

METRIC	MONTHLY VOLUME
Total page views (protected pages)	Enter value
Form submissions	Enter value
Payment transactions	Enter value

Base Package

Client-Side Defense includes 1 million transactions in the base package.

JavaScript Environment

Third-Party Scripts

How many third-party JavaScript resources are loaded on your pages?

CATEGORY	ESTIMATED COUNT
Analytics (Google Analytics, etc.)	Enter value
Marketing/Advertising	Enter value
Social media widgets	Enter value
Chat/Support widgets	Enter value
Payment processors	Enter value
A/B testing tools	Enter value
Other third-party scripts	Enter value
Total third-party scripts	Enter value

Script Sources

Where do your JavaScript resources come from?

- First-party (your own domains)
- CDN-hosted (cdnjs, jsdelivr, etc.)
- Direct third-party domains
- Tag managers (Google Tag Manager, etc.)

List critical third-party script sources:

SCRIPT PURPOSE	SOURCE DOMAIN	CRITICAL?
Enter value	Enter value	☐ Yes ☐ No
Enter value	Enter value	☐ Yes ☐ No
Enter value	Enter value	☐ Yes ☐ No
Enter value	Enter value	☐ Yes ☐ No

Content Security Policy (CSP)

Do you currently have a Content Security Policy?

- Yes - Strict CSP
- Yes - Reporting-only mode
- No - No CSP implemented
- Unknown

Compliance Requirements

PCI-DSS Requirements

Are you subject to PCI-DSS compliance?

- Yes - PCI-DSS Level 1
- Yes - PCI-DSS Level 2
- Yes - PCI-DSS Level 3-4
- No

> **PCI-DSS 4.0**
>
> PCI-DSS 4.0 includes requirements (6.4.3 and 11.6.1) for monitoring and controlling client-side scripts on payment pages.

Other Compliance

Which other compliance frameworks apply?

- GDPR
- CCPA
- HIPAA
- SOC 2
- Other: _____

Detection and Alerting

Detection Capabilities

What detection capabilities do you need?

- **Script behavior monitoring** - Detect changes in script behavior
- **Network request monitoring** - Detect unauthorized data exfiltration
- **Form field monitoring** - Detect unauthorized form reads
- **DOM manipulation detection** - Detect unauthorized page changes
- **Page tamper detection** - Detect payment page modifications

Alerting Requirements

How should you be notified of detected threats?

- Email alerts
- F5 XC Console alerts
- Webhook integration

- SIEM integration

Alert severity thresholds:

ALERT TYPE	SEVERITY
New third-party script detected	☐ Critical ☐ High ☐ Medium ☐ Low
Script behavior change	☐ Critical ☐ High ☐ Medium ☐ Low
Data exfiltration attempt	☐ Critical ☐ High ☐ Medium ☐ Low
Page tampering detected	☐ Critical ☐ High ☐ Medium ☐ Low

Mitigation Actions

Response Actions

What actions should be taken when threats are detected?

THREAT TYPE	ACTION
Malicious script detected	☐ Block ☐ Alert only
Data exfiltration attempt	☐ Block ☐ Alert only
Unauthorized form access	☐ Block ☐ Alert only
Page tampering	☐ Block ☐ Alert only

Blocking Method

If blocking, how should blocking be implemented?

- **Block network calls** - Prevent exfiltration to malicious domains

- **Remove malicious script** - Strip script from page
- **Redirect to safe page** - Show user a warning

Integration

Deployment Method

How will Client-Side Defense be deployed?

- F5 XC proxy (automatic JavaScript injection)
- Manual JavaScript tag insertion
- BIG-IP integration (iApp or native module)
- CDN integration

Existing BIG-IP

Do you have F5 BIG-IP that could integrate with Client-Side Defense?

- Yes - BIG-IP version: _____
- No

Page Tamper Protection

Payment Page Monitoring

If yes, provide payment page URLs:

PAYMENT PAGE URL	EXPECTED UPDATE FREQUENCY
Enter value	☐ Rarely ☐ Monthly ☐ Weekly ☐ Daily
Enter value	☐ Rarely ☐ Monthly ☐ Weekly ☐ Daily

Baseline Management

How often do your payment pages legitimately change?

- Rarely (quarterly or less)
- Monthly
- Weekly
- Frequently (daily or more)

Summary: Client-Side Defense Requirements

REQUIREMENT	VALUE
Number of Protected Pages	Enter value
Estimated Monthly Transactions	Enter value
Third-Party Scripts to Monitor	Enter value
PCI-DSS Compliance Required	☐ Yes ☐ No
Page Tamper Protection Required	☐ Yes ☐ No
Detection Mode	☐ Monitor ☐ Block

Critical pages requiring protection:

1.
2.
3.

Additional notes or special requirements: