



# Comprehensive Security Testing for Modern Enterprises

Application, API, Testing

43%

of all breaches result from application layer attacks—while only 21% of organizations are able to detect API layer compromises.

Modern enterprises operate across browsers, APIs, cloud workloads, and OT networks. Plurilock™ delivers world-class application, API, and integration testing to uncover risk before attackers do—across your full stack.

**Trusted by U.S. and Canadian federal agencies and multiple S&P 500 enterprises**, Plurilock brings unmatched depth across IT, OT/ICS, and application environments.

## Application Testing

Plurilock's testing covers client, server, and integration layers under real-world conditions.

- **Client + Front-End:** DOM-based XSS, expose secrets, insecure JS or APIs
- **Authentication + Sessions:** MFA, token, cookie handling; session fixation
- **Access Control:** IDOR, privilege escalation, RBAC flaws, API permissions
- **Input + Injection:** SQL, command, XML, and template injection
- **Business Logic:** Workflow bypasses, race conditions, abuse of functions
- **Uploads + Downloads:** Path traversal, unrestricted uploads, malicious files
- **Dependencies:** Vulnerable libraries, compromised packages, EOL components
- **Misconfiguration:** Default credentials, CSP/HSTS headers, open directories
- **Infrastructure:** Container, CI/CD, and cloud deployment vulnerabilities
- **Cryptography:** Weak algorithms, poor key handling, cert validation issues

## API Testing

APIs enable your business, but they also expand your attack surface. Plurilock's API assessments validate controls at every layer.

- **Authentication + Authorization:** JWT + OAuth flaws, BOLA/BFLA
- **Injection + Input Validation:** SQL/NoSQL, XML ext. entity, parameter pollution
- **Rate Limiting + Resources:** DoS resilience, large queries or payloads
- **Data Exposure:** Excessive response data, sensitive info in logs or URLs
- **Business Logic:** Sequence manipulation, state tampering, race conditions
- **Misconfiguration:** Verbose errors, insecure HTTP methods, weak CORS
- **GraphQL & Microservices:** Introspection abuse, query complexity, internal API exposure



## The Plurilock Advantage

- ✓ Senior Tier-1 professionals on every engagement
- ✓ Extensive enterprise, public sector experience
- ✓ Proven in government, defense, finance, manufacturing
- ✓ Rapid mobilization—days, not weeks or months
- ✓ Cross-domain coverage—IT, OT/ICS, and app layer
- ✓ Actionable results and next steps

Test and secure every layer of your technology stack—end-to-end.

[sales@plurilock.com](mailto:sales@plurilock.com)

## Contact Us

+1 (888) 776-9234 (Plurilock)  
+1 (310) 530-8260 (USA)  
+1 (613) 526-4945 (Canada)

Advanced cybersecurity and Zero Trust Security assessments and consulting  
IT products and solutions  
Professional services  
Managed services

# Plurilock Services

## Zero Trust

Design and implementation of zero trust architectures (ZTAs)

## Data Protection

Protection of intellectual property and digital assets

## Identity and Access Management

Design, implementation, and integration of complete identity and access management (IAM)

## Public Key Infrastructure

Design and implementation of modern public key infrastructure (PKI) deployments

## Offensive Security

Security assessments and tests with a hacker mindset

## Penetration Testing as a Service (PTaaS)

Managed service providing continuous penetration testing to rapidly surface emerging vulnerabilities

## Data Protection as a Service (DPaaS)

Managed data protection service to operate DLP and insider threat capabilities as a service

## Emergency Support

Immediate, cross functional team for urgent and high impact IT and cyber problems



Selection of current and past customers that can be publicly represented