EXFILTRA

We Secure What Powers Your Business

Expert-led assessments, actionable remediation plans, and continuous protection ensuring your cloud and applications stay resilient against evolving threats

Cloud & Application Security - From Assessment to Remediation

About Exfiltra & Why Businesses Trust Us

About Exfiltra

Who are we?

Exfiltra is a specialized cybersecurity firm focused on cloud and application security. Our team blends offensive hacking expertise with defensive engineering skills to deliver end-to-end protection. From identifying vulnerabilities to providing step-by-step remediation, we go beyond compliance checklists - we secure what matters.

Why Businesses Trust Us

Why Leading Organizations Choose Exfiltra

Hacker Credibility

- **We Build & Break** – Contributors to industry-standard tools like OWASP ZAP.
- **Proven in the Wild** – Ethical hacks against U.S. DoD & global enterprises.
- **Real-World Threat Perspective** – Our methods mirror actual attacker behavior.

Business Value

- **Cloud-Native Security Expertise** – AWS, Azure, GCP secured at scale.
- **Certified Security Professionals** – Industry-recognized credentials.
- **Trusted by 50+ Clients** – Over 5 years securing critical applications.

Quote / Impact Statement

We don’t just find your weaknesses - we help you fix them before anyone else can exploit them

Our Core Services

Your Security, Strengthened at Every Layer

StackGuardian – Managed App & Cloud Security

Ongoing expert-led services to keep your applications and cloud environments secure and compliant.

SecProof – Organizational Security Assessments & Penetration Tests

We assess your entire security posture, fix vulnerabilities, and provide a verified security certificate - proof your customers can trust.

PatchOps – Remediation as a Service

Because 'fixed' is the only status that matters.

FOSS Guard – Affordable, Vendor-Independent Security Stack

Build a resilient security setup without costly vendor lock-ins using a free and open-source stack

DevShield – Secure SDLC Implementation

Embed security into your development lifecycle from the first commit.

GapLock - SecProof + PatchOps

Our 2 services packaged into one. First get your environment assessed, and then fix the security findings.

From assessment to protection - we secure, remediate, and safeguard your business

EXFILTRA

03

Stack Guardian

Never Let Your Security Regress - From Code to Cloud, We've Got You Covered

The Problem

Security is not a one-time project.
You can pass an assessment today and still be vulnerable next month. Code changes, new dependencies, and cloud misconfigurations silently creep in - and before you know it, your "secure" stack has holes big enough for attackers to walk through.

Hiring a full-time security team is expensive. Doing nothing is dangerous.
StackGuardian™ is your third option.

The Promise

Continuous, cloud-native and application-aware security engineering - so your protection grows with your business, not against it.
No 24/7 SOC noise. No shelfware tools you'll never use. Just focused, ongoing work that keeps you secure and compliant while you scale

What We Deliver

Every month, we work as your hands-on security team, covering both cloud and application layers:

Application Layers

- **Pipeline & IaC Security Checks** - Find and fix risks before deployment.
- **Dependency & SCA Scanning** - Keep vulnerable libraries out of production.
- **Secure SDLC Support** - Guidance from design to deployment.

Cloud Security

- **Cloud Hardening Cadence** - Ongoing misconfiguration fixes, identity & access clean-up.
- **Quarterly Architecture Reviews** - Ensure your environment evolves securely.
- **Private Endpoint & Network Security Reviews** - Lock down data pathways.

Stack Guardian

Never Let Your Security Regress - From Code to Cloud, We've Got You Covered

Across Both

- **Vulnerability Triage & Prioritization -** Focus on what really matters.
- **Monthly Security Report + Roadmap -** Transparent progress, measurable results.
- **Patch & Remediation Support -** Option to include dedicated remediation hours.

Who It's For

SaaS companies and digital businesses who:

- Deploy code and cloud changes regularly.
- Want continuous improvement without hiring a full-time security engineer.
- Care about protecting customer trust and avoiding costly breaches.

How It Works

1. **Onboarding & Baseline Hardening (4–8 weeks)**
   We assess and fix your most critical gaps fast.
2. **Ongoing Monthly Cycle**
   Proactive checks, triage, fixes, and roadmap updates.
3. **Quarterly Deep Dives**
   Strategic architecture reviews to prevent security drift.

Why StackGuardian™

- **No Downtime to Your Team** - We work alongside your dev & ops teams without slowing releases.
- **Independent & Vendor Neutral** - We pick the right tools for you, not for a sales quota.
- **Built for SaaS Growth** - Security that scales as fast as your business.

SecProof – Organizational Security Assessments & Penetration Tests

Proof your customers can trust.

The Problem

Most organizations don't know how secure they really are. Breaches often happen because vulnerabilities go unnoticed - or take weeks to fix. And when customers ask for proof of your security posture, you're left scrambling.

Our Solution

SecProof assesses your entire security posture, helps you fix vulnerabilities, and issues a verified security certificate you can show to customers, partners, and regulators.
We combine technical testing with organizational review so you get both depth and breadth - then validate fixes before certification.

Who It's For

- Businesses that want to focus on growth without worrying about security.
- SaaS & tech companies needing security assurance to close deals.
- Organizations aiming for compliance readiness (ISO 27001, SOC 2, HIPAA, etc.).

What You Get

- **Full organizational security assessment** – Cloud, app, infrastructure, and policy review.
- **Remediation guidance** – Prioritized, actionable fixes.
- **Re-test & certification** – Verified SecProof Certificate, valid for 6 months.

Why We're Different

- **ZeroDelay Pentest –** Few in the industry offer live vulnerability alerts during testing. You get an immediate edge in fixing issues before they're exploited. It is an optional add-on though.
- **Developers at core –** We've built apps and systems ourselves, so we know the exact mistakes developers make - and we can spot and fix them quickly.

SecProof – Organizational Security Assessments & Penetration Tests

Proof your customers can trust.

Why We're Different

- **Code-level remediation –** We don't just point out problems; we can step into your codebase and help patch vulnerabilities effectively.
- **Proven track record –** Discovered bugs in the U.S. DoD and multiple major platforms.
- **Competitive edge –** Active participation in hacking competitions keeps our skills razor-sharp.

PatchOps - Remediation As A Service

Because ‘fixed’ is the only status that matters

The Problem

Most security services stop at telling you what’s wrong. The result? A stack of vulnerability reports gathering dust, deadlines slipping, and security gaps staying open far too long. Meanwhile, attackers aren’t waiting.

Our Solution

PatchOps turns security findings into fixed code and hardened systems. We step in as your on-demand remediation team - closing vulnerabilities before they become incidents.

Here’s how we work:

- **Direct-to-Fix** – We take security reports (from us or any third party) and remediate issues in code, infrastructure, or configurations.
- **Developer-Aware Fixes** – As engineers ourselves, we write and test fixes that blend seamlessly with your stack and workflows.
- **Prioritized Patching** – We fix what matters most first, so your most critical risks disappear fastest.
- **Integration Friendly** – Works alongside your existing dev, ops, or security teams.

Optional Add-On – ZeroDelay Remediation

For clients who pair PatchOps with ZeroDelay Pentest or continuous assessments, we can patch vulnerabilities in near real-time as soon as they’re discovered - cutting average exposure from weeks to hours.

Who This Is For

- Teams who get security reports but lack the bandwidth or expertise to implement fixes.
- CTOs and founders who want vulnerabilities closed fast so they can focus on growth.
- SaaS companies preparing for enterprise onboarding or compliance audits.

PatchOps - Remediation As A Service

Because 'fixed' is the only status that matters

Why PatchOps is Different

- **We're Devs First, Security Second** – Our fixes aren't guesswork; they're production-ready.
- **Compliance-Ready Output** – Everything is documented for audit and proof to stakeholders.
- **Proven Track Record** – Our team has fixed vulnerabilities found in critical systems, including U.S. DoD apps, and consistently wins in hacking competitions.

FOSS Guard - Affordable, Open & Vendor-Independent Security Stack

Enterprise-grade security without the strings (or invoices) attached.

The Problem

Every month, security budgets quietly bleed out through vendor invoices:

CrowdStrike: $60–$180 per endpoint/year
SentinelOne: $180–$230 per endpoint/year
Qualys: $2000+/year for core modules

For a 50-person company, that's easily $20k–$35k annually - and you're still locked into proprietary platforms that can change pricing or features anytime.

The OpenShield™ Promise

Get full-spectrum enterprise security - endpoint, network, cloud, appsec, monitoring, built entirely on well-supported open-source tools.

✅ No vendor lock-in
✅ No per-user/endpoint tax
✅ Transparent & auditable
✅ Flexible integrations with your stack

We Love Open-Source ❤

We believe the future of security should be transparent, community-driven, and vendor-independent. That's why OpenShield™ is built on open-source projects we trust, contribute to, and stand behind.

And we're not just users - we give back. 5% of every OpenShield™ implementation fee is donated directly to the developers of the tools we deploy, ensuring these projects continue to grow and protect more organizations worldwide.

FOSS Guard - Affordable, Open & Vendor-Independent Security Stack

Enterprise-grade security without the strings (or invoices) attached.

What You Get

We design, deploy, and hand over a battle-tested open security stack tailored to your environment, including:

- Vulnerability & dependency scanning
- Cloud & infrastructure hardening policies
- Centralized logging & alerting
- CI/CD security gates
- Role-based access controls
- Integration with Slack, Teams, or email alerts

Plus:

- 📄 Full documentation
- 🧑‍💻 Admin training for your team
- 🛠️ 90-day included support
- 🔄 Optional ongoing management & updates

Who It's For

- Companies that want control over their security stack without relying on a single vendor.
- Teams with tight budgets but no compromise on protection.
- Organizations in regulated industries that value auditable, open-source transparency.
- Tech leaders who believe security should be a capability, not just a subscription.

GapLock – Cloud & Application Security Overhaul

We prove where you're exposed - then fix it - end-to-end. (SecProof + PatchOps)

Most security firms give you a report and leave you with a pile of problems. GapLock goes further - we identify, fix, and certify your security, giving you proof your customers and investors can trust.

Why GapLock Is Different

1. Full Problem Solving - Not Just Reports
Most assessments end with a "So what?" moment. We not only identify vulnerabilities we fix them and re-test so you know you're secure.

2. Confidence Through Direct Action
You don't have to chase multiple vendors or hope someone follows through. We take full responsibility for hardening your environment.

3. Higher Value for Your Investment
Audit + remediation means 2–5× the impact of an assessment alone, while saving you time and internal effort.

Our 2-Phase Process

Phase 1: Assessment & Proof

- Full security review of applications & cloud infrastructure
- Application penetration test (OWASP Top 10, authentication, business logic)
- Cloud configuration audit (IAM, storage, networking, security groups)
- IaC & pipeline scanning
- Prioritized remediation plan
- Initial "Exposure Report"

Phase 2: Remediation & Hardening

- Fix vulnerabilities & misconfigurations
- Deploy secure configurations and best practices
- Implement open-source/vendor-neutral security tooling
- Verification re-test to confirm fixes
- Final executive report
- Client-facing "Proof-of-Security" badge to share with customers

GapLock – Cloud & Application Security Overhaul

Enterprise-grade security without the strings (or invoices) attached.

Who It's For

Fast-growing SaaS & cloud-native companies who need to:

- Win bigger customers
- Satisfy investor due diligence
- Pass vendor security questionnaires without stress

What You Get

- Org-wide security assessment
- Fixes implemented by expert engineers
- Final security verification
- Shareable security certificate/badge
- Executive & technical reports

Timeframe

2–6 weeks depending on scope and complexity

EXFILTRA

For more information or to book a demo, contact najam@exfiltra.com