HORIZONSHIELD ORIGINALS · BOOK 22

Security Architecture for Startups

Building Secure-by-Default from Day One

A practical zero-to-secure framework for startups — building security architecture, identity, data protection, and compliance foundations without enterprise budgets or dedicated security teams.

HORIZONSHIELD

FOUNDATIONAL

Contents

CHAPTER 01

Security Architecture Philosophy for Startups

Startups face a paradox: they move fast and can't afford security debt, yet they can't afford a CISO or security team either. The solution is building security into the foundation — not bolting it on later.

The Cost of Deferred Security

Stage	Security Effort	Relative Cost to Fix a Flaw
Design	Threat modeling, architecture review	1x — cheapest, most impactful
Development	SAST, code review, developer training	6x — still manageable
Testing/QA	DAST, penetration testing	15x — costly to rework
Production (pre-breach)	Bug bounty, vulnerability disclosure	30x — emergency patches
Post-breach	Incident response, legal, PR	100x+ — potentially company-ending

Security Architecture Principles for Startups

Default Deny
Start with no access; explicitly grant what's needed

Least Privilege
Every human and service gets minimum permissions required

Defense in Depth
Multiple controls — no single failure causes full compromise

Assume Breach
Design assuming attacker is already inside — limit blast radius

>

Security Champions Beat Security Teams: A startup can't afford a security team. Instead, make every developer a security owner. 4 hours of OWASP training per engineer per quarter + SAST in CI/CD + a weekly "security review" slot in sprint planning = enterprise-level security awareness at startup cost.

CHAPTER 02

Identity & Access — The Foundation

Identity is the most critical security investment for a startup. Get this right from day one and you prevent 60%+ of breaches before they happen.

Day 1 Identity Setup Checklist

- Choose IdP: Google Workspace or Microsoft 365 (not individual Gmail accounts)
- Enable MFA enforcement for all users — day 1, no exceptions
- Configure SSO for all SaaS tools (Slack, GitHub, AWS, Notion)
- Create a "security" admin account separate from personal account
- Set up break-glass procedure for admin account lockout
- Establish offboarding checklist — revoke ALL access within 1 hour of departure

Startup AWS IAM Baseline

```
# Never use root account for daily operations
# Create admin user immediately after root account setup

# Root account checklist:
# 1. Enable MFA on root (hardware key preferred)
# 2. Delete root access keys
# 3. Set billing alert at $50, $500, $5000
# 4. Enable CloudTrail
# 5. Enable GuardDuty
# 6. Block all public S3 access at account level

# Create admin user with least privilege
aws iam create-user --user-name startup-admin
aws iam attach-user-policy   --user-name startup-admin   --policy-arn arn:aws:iam::aws:policy/AdministratorAccess
# Require MFA for all actions (conditional policy)

# For CI/CD — use OIDC, not static access keys
# GitHub Actions to AWS OIDC (no long-lived credentials)
aws iam create-open-id-connect-provider   --url https://token.actions.githubusercontent.com   --client-id-list sts.amazo
```

CHAPTER 03

Startup Security Stack — Best Value

Startups can achieve excellent security posture with a carefully chosen set of tools, many of which are free or inexpensive. This curated stack delivers maximum security per dollar spent.

Recommended Startup Security Stack

Category	Free/Cheap Option	When to Upgrade
Identity/SSO	Google Workspace ($6/user/mo)	Scale or Microsoft shop
Password Manager	Bitwarden Teams ($3/user/mo)	At 200+ users or for advanced policies
Secrets Management	AWS Secrets Manager or GitHub Secrets	Add HashiCorp Vault at 50+ devs
SAST	Semgrep (free OSS tier) + GitHub CodeQL	Semgrep Pro at scale
SCA/Deps	Dependabot (free with GitHub)	Snyk or Socket at 10+ repos
Secrets scanning	Gitleaks + TruffleHog (free)	GitGuardian at scale
Cloud posture	Prowler (free OSS)	Wiz or Orca at Series B+
Endpoint	Microsoft Defender (free on Windows)	CrowdStrike/SentinelOne at 100+ endpoints
Phishing training	GoPhish (free self-hosted)	KnowBe4 at 50+ employees
Vulnerability scanning	Nuclei (free) + OpenVAS	Tenable or Qualys at enterprise

CHAPTER 04

Compliance Foundations for Startups

Enterprise customers and investors increasingly require security compliance. Preparing for SOC 2 or ISO 27001 early — as you build rather than after — is dramatically cheaper than retrofitting compliance onto an existing product.

Compliance Timeline for B2B SaaS Startups

```
Pre-Seed / Seed (0-18 months):
  - Enable audit logging on all systems
  - Document your architecture and data flows
  - Write 5 core policies (InfoSec, Access Control,
    Incident Response, Acceptable Use, Vendor Management)
  - Enable MFA everywhere, document it

Series A (12-24 months):
  - Begin SOC 2 Type I preparation
  - Use Vanta or Drata to automate evidence collection ($5K-15K/yr)
  - Annual penetration test (budget $15-30K)
  - Bug bounty program launch (HackerOne or Bugcrowd free tier)

Series B (24-36 months):
  - Complete SOC 2 Type II (12-month observation period)
  - ISO 27001 if selling to EU enterprises
  - Hire first security engineer or fractional CISO
```

>

SOC 2 as Competitive Advantage: A SOC 2 report answers 90% of enterprise security questionnaires in one document, eliminating weeks of back-and-forth with enterprise procurement teams. Startups with SOC 2 close enterprise deals 3x faster than those without. The ROI is measured in months, not years.

5 Security Policies Every Startup Needs Day 1

- **Information Security Policy** — top-level statement of security commitment
- **Access Control Policy** — who gets access, how, reviewed how often
- **Incident Response Policy** — how you handle and report security incidents
- **Acceptable Use Policy** — what employees can/cannot do with company systems
- **Vendor Management Policy** — how you assess and manage third-party security

HS

HORIZONSHIELD ORIGINALS

Complete Security Library

HorizonShield Originals are practitioner-written guides designed for real-world implementation — from SMB security foundations to advanced threat hunting, cloud architecture, and regulatory compliance.

AVAILABLE IN THIS SERIES

01 SMB Cybersecurity Guide 2026
02 Penetration Testing Checklist
03 Incident Response Playbook
04 DORA Compliance Guide
05 Cloud Security Hardening
06 Zero Trust Architecture
07 Threat Hunting SOC Operations
08 DevSecOps Implementation
09 Web Application Security
10 Network Security Fundamentals
11 Linux & Systems Security
12 Social Engineering & Human Hacking
13 Malware Analysis & Reverse Engineering
14 Digital Forensics & Incident Response
15 Applied Cryptography
16 Compliance Audit & Risk Management
17 AI & LLM Security Guide
18 OT & ICS Security
19 Mobile Security
20 Kubernetes Security
21 Bug Bounty Methodology
22 Security Architecture for Startups

horizonshield.net/library

Download all 16 books · Access labs · Track your progress

horizonshield.net