Cybersecurity designed for small & medium businesses

StrongKeep

STRONGKEEP FACTSHEET

Snapshot
All-in-one cybersecurity for small & medium businesses: Protection, Compliance, Training, Detection, and Response in one cloud console. Built for lean IT teams – no SOC required.

Who it's for
SMBs that need practical protection and fast, audit-ready compliance (CSA Cyber Essentials) to win tenders or qualify for cyber insurance. The CE mark is typically a desktop review and is valid for 2 years.

Plans & pricing (USD, billed annually)

Plan	Price	Included devices	Key inclusions
Protection	**US$39/mo**	5	Endpoint protection, network firewall, website & email hygiene scans, password manager, awareness training, phishing simulator, crisis playbooks and training. Extra endpoints **US$5/device/mo**
Compliance	**US$159/mo**	5	Everything in Protection **plus** Cyber / Data standard certification workflow, evidence tracking, reminders, audit logs. Extra endpoints **US$5/device/mo**
Resilience	TBA	5	Everything in Compliance **plus** agentic AI vCISO to manage all capabilities autonomously (roadmap)

Insurance add-on (indicative): *from* ***S$75/mo*** *for* ***S$250k*** *coverage. See pricing page for current offer and eligibility*

What you get (capabilities overview)

Platform. Daily company level cyber risk posture with staff level cyber posture, assessed across modules (e.g. device protection, password manager use, training results, phishing test); Aggregated cyber news feed.

Protection. Enterprise-grade endpoint agent and DNS protection to block phishing/malware; external website/email security scans. (Cortex XDR-class agent; DNS filtering via ControlD.) Resilience Plan adds 24/7 Agentic AI detection and response.

Compliance. Fully guided workflows from policy generation to evidence collection mapped to **CSA Cyber Essentials (CE 2025/ICT), Data Protection Essentials (DPE), Health Info Act Compliance (Coming soon)**; policy templates; evidence tracker; reminders; audit logs; includes submission to Certifying Body for audit and certification, where relevant (Compliance Plan)

Training. Gamified micro-lessons with MCQs, topic diagnostics; scheduled quizzes. **Resilience Plan** adds Agentic AI to personalise training.

Detection. External attack-surface checks aligned to CSA Internet Hygiene resources (DMARC/SPF/DKIM, TLS/HTTPS/HSTS/STARTTLS, DNSSEC) with fix-guides

Response. Self-help incident diagnostic and playbooks (Protection Plan); auto-generated incident reports for insurer/police/authorities (Compliance Plan).

Cybersecurity designed for small & medium businesses

StrongKeep

Deployment & coverage

- **Endpoint agent minimums**:
  - **Windows**: dual-core CPU (SSE2), 2 GB RAM min, 5 GB disk (20 GB rec.).
  - **macOS**: Intel or Apple Silicon, 512 MB RAM min (2 GB rec.), 5 GB disk (20 GB rec.).
  - **Linux**: x86-64, ~2.3 GHz dual-core, 4 GB RAM (8 GB rec.), 10 GB disk
  - **Mobile**: iOS and Android
- **Email & domain scan:** we scan DMARC, SPF, DKIM configuration and related hygiene signals; we do not read email.
- **Network/DNS protection:** deploy via endpoint agent **or** change device/router DNS to assigned resolvers; roaming and BYO devices are covered. ControlD also provides a lightweight **ctrld** daemon for diverse platforms.

Compliance & evidence

- **Supported today:** CSA Cyber Essentials.
- **Standards:** Data Protection Essentials (DPE), MOH Health Information Bill (HIB), UK Cyber Essentials, plus others on request.
- **Evidence automation:** auto-collects for endpoint/network/server security, training and credentials; templates & guides for all other controls.
- **Certification:** CE submission documents prepared and submitted automatically. Assessment via desktop review and verification by an appointed body (costs included in Compliance Plan).

Security & privacy

- **Data residency**: Primary & backups - AWS Asia Pacific (Singapore) ap-southeast-1; optional integration: Control-D (DNS filtering) is hosted in Australia
- **Encryption**: In transit: TLS 1.2+ (with some 1.1 moving to 1.2). At rest: AES-256 (AWS KMS-managed) for DB, object storage, and backups
- **Retention:** Customer content (policies, artefacts, evidence): Kept for active subscription + 90 days for export after termination, then hard-deleted (unless legal hold).
- **Sub-processors:**
  - Cloud infrastructure: Amazon Web Services, EKS (Fargate), Lambda/EC2, S3, CloudWatch, KMS (region per Data residency).
  - Database: MongoDB Atlas, in-region cluster; encryption at rest with KMS/KMIP.
  - Email delivery: Amazon SES, transactional & training emails (SPF/DKIM/DMARC in place).
  - Security integrations: Palo Alto Cortex XDR (optional per customer), telemetry ingestion for managed security.

Support & onboarding

- **Support:** WhatsApp chat during office hours (SGT); email support available.
- **Onboarding & time-to-value:** Self serve onboarding flow upon sign up to connect staff with native integrations for **Microsoft 365** and **Google Workspace;** guided workflow to setup device protection (EDR / DNS Firewall), Password Manager and launch Training campaign; **first devices protected within ~2 hour** for most SMBs.

Roadmap & integrations

Vulnerability Assessment & Penetration Testing, integration with backup solutions (Protection Plan), ISO 27001 (Compliance Plan). Customer-requested features can be considered.

Assurance. We are Cyber Essentials certified (using StrongKeep).

Contact hello@strongkeep.com | www.strongkeep.com