StrongKeep

Technical Product Fact Sheet

Executive Overview

- StrongKeep provides detection, protection, awareness training, credential management, server scans, and compliance management through a single, easy to manage interface.
- The platform bundles an endpoint agent solution to protect devices against malware [Cortex XDR] and a DNS firewall to block phishing / malicious URLs [ControlD]
- The platform is engineered to deliver simple, affordable, effective cybersecurity for SMBs.

Subscription Plans

PROTECTION

Best for business owners who want fast cybersecurity. Block threats, train staff, and sleep better at night.

What you get:

- ✓ Prevent phishing & malware
  - Endpoint protection (up to 5 endpoint devices + ~~$6~~ **$5/month/device**)
  - DNS firewall
  - Website & Email security scans (up to 10 verified domains)
- ✓ Secure your employees
  - Password manager
  - Cyber awareness training
  - Phishing simulator
- ✓ Ensure you are prepared
  - Crisis playbooks
  - Incident diagnostic tool

- The **Protection Plan** provides a good foundation for safeguarding your business against everyday threats.
- It includes essential elements such as a firewall, regular backups, endpoint protection, and comprehensive staff training.

Subscription Plans

COMPLIANCE

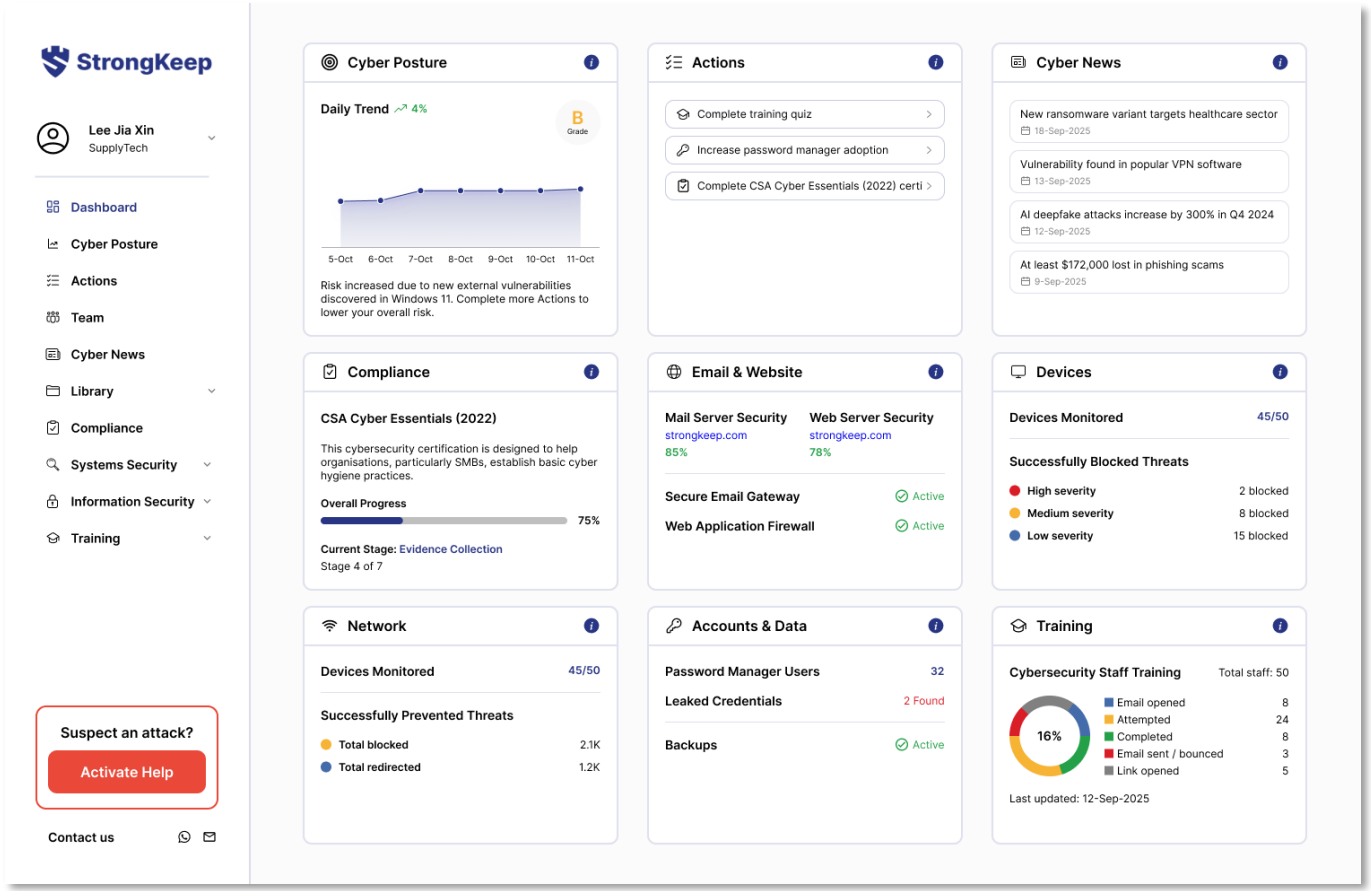
Best for clinics and vendors who need to pass audits or get insured. Fast-track certification and save $10,000 vs. audit firms.

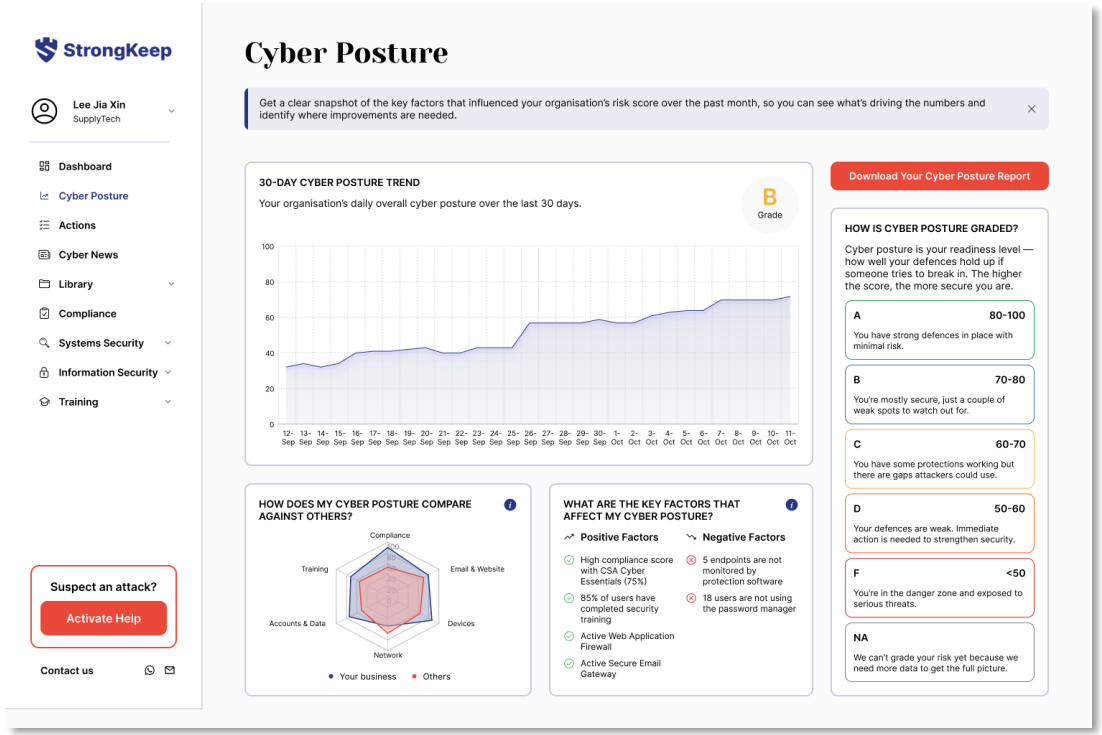
All Protection features, plus:

- ✓ Get certified
  - CSA Cyber Essentials certification
  - *MOH Health Information Bill (coming soon)*
  - *Data Privacy Essentials certification (coming soon)*
- ✓ Adopt best-in-class SOPs
- ✓ Stay compliant with ease
  - Evidence tracking
  - Regular reminders
  - Audit logs
- ✓ Access to cyber insurance
  - Fast underwriting
  - Lower premiums

- The **Compliance Plan** transforms robust security measures into verifiable security standards.
- It uses AI and automation to speed up the certification process (generating policies, collective evidence, submitting applicaiton) while keeping costs significantly lower than hiring a CISO or a consultant.

Dashboard: Unified Cybersecurity

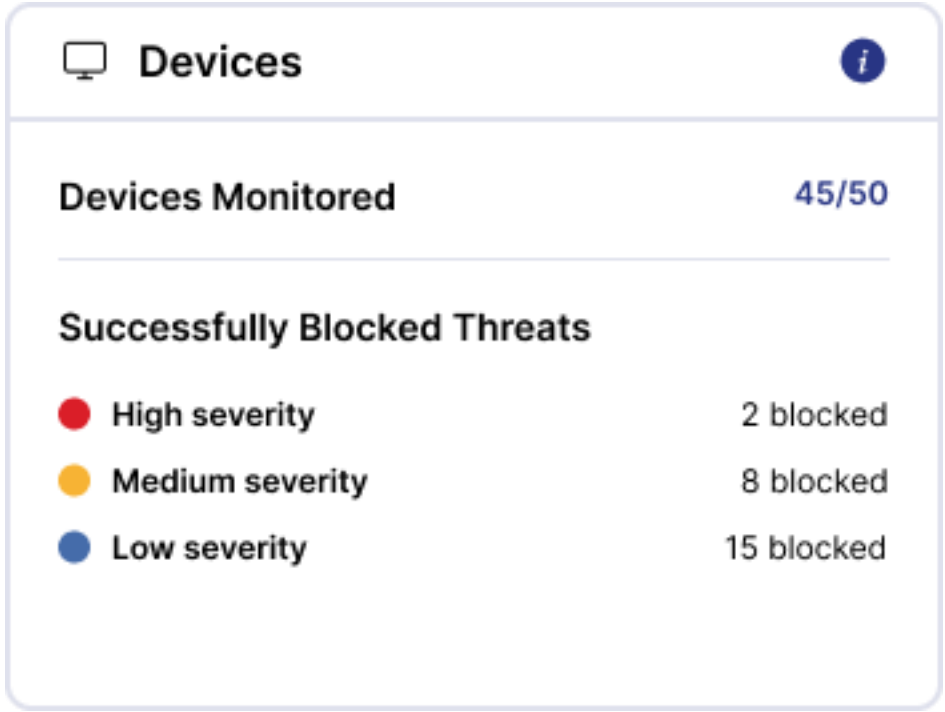


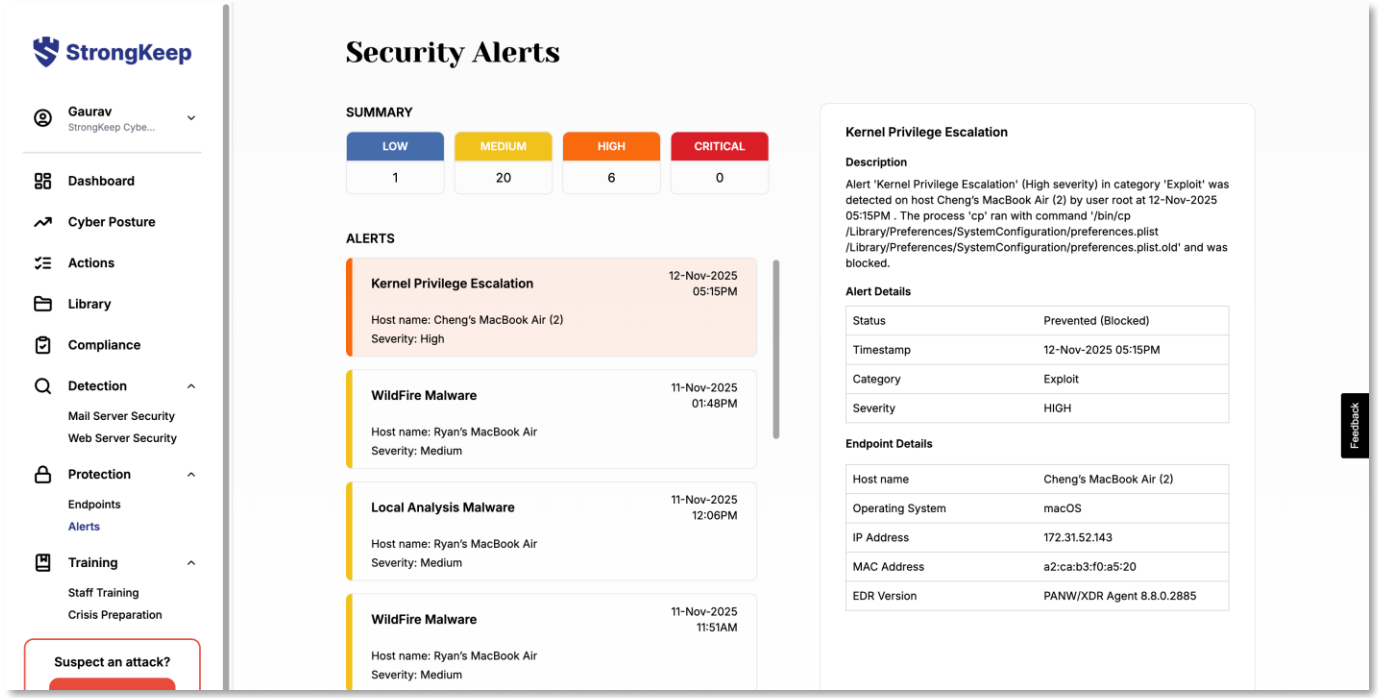


Dashboard: Unified Cybersecurity

Capability	StrongKeep Description
Holistic security posture visibility	Dashboard aggregates endpoint, network, accounts, data, training and compliance metrics into a single view so SMBs can see "how safe we are" at a glance.
Actionable next-steps guidance	The "Actions" panel recommends prioritized tasks (e.g., complete quiz, increase password manager adoption) so users know what to do next without specialist input.
Compliance status tracking	Shows current certification stage (e.g., CSA Cyber Essentials), percent progress and stage number, so SMBs can monitor audit readiness.
Threat/incident alert readiness	Through cards like "Devices" and "Network" the dashboard surfaces blocked threats, redirect counts and device coverage to show active protection in action.
Training & human risk insights	The "Training" card tracks staff training metrics (email opened, attempted, completed, links clicked) giving a view of human-factor risk.
Credential & data hygiene visibility	The "Accounts & Data" card displays stats like number of password manager users, leaked credentials found, backup status – showing how well credentials/data are protected.
Web & email asset health	The "Email & Website" card shows mail server and web server security percentages, and status of Secure Email Gateway/WAF, helping assess external asset exposure.
Trend monitoring for progress	The "Cyber Posture" card includes a trend line and grade to show whether the organisation's posture is improving or slipping over time.
News & awareness integration	The "Cyber News" card surfaces relevant threat/industry headlines, keeping users informed and reinforcing the dashboard as a living tool, not static.

Device Protection: CORTEX XDR Pro

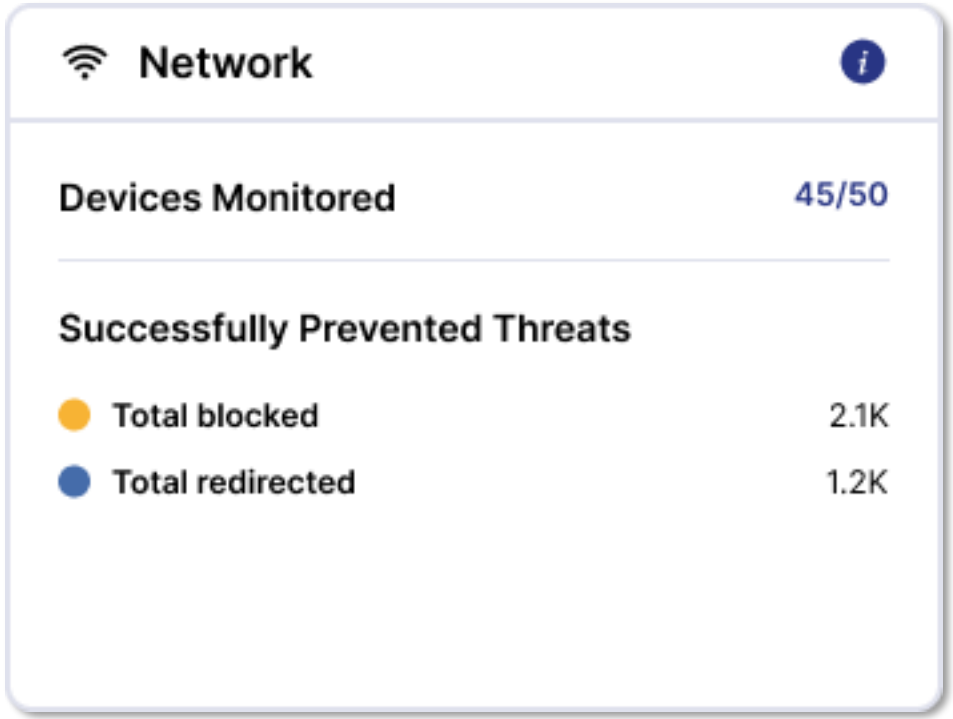


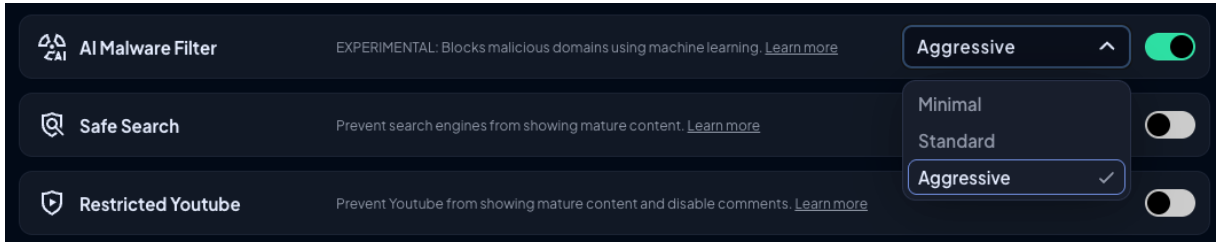


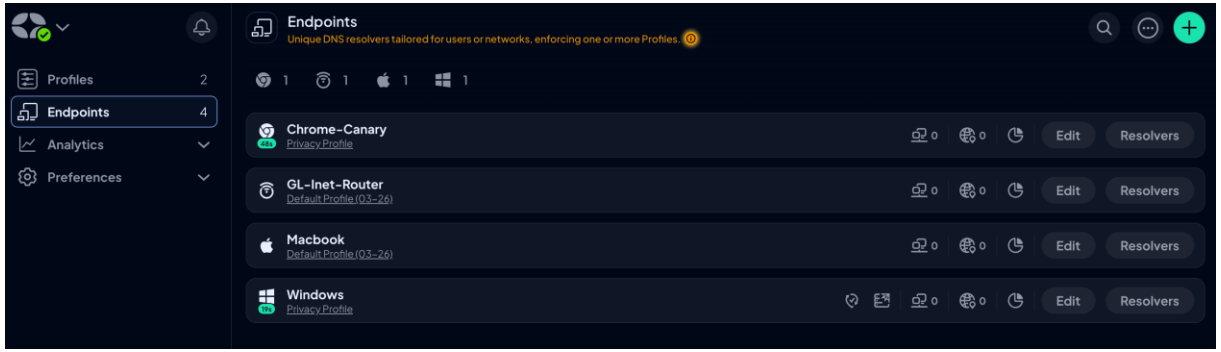
Device Protection: CORTEX XDR Pro

Capability	StrongKeep Description
Signature-less next-gen AV	Behavioural Analytics + AI and integrated threat intelligence (IoCs + Palto Alto research team)
Endpoint Detection & Response	Using XDR capability
Automatic attack disruption	Proactive threat blocking and risk prioritization
Cloud-scale threat intel	Integrated threat intelligence (IoCs + Palto Alto research team)
Multi-platform OS support	Windows, macOS, Linux, Mobile
False-positive handling	Alert grouping to reduce noise, policy is based on blocked by default
Data retention	Kept for active subscription + 90 days for export after termination, then hard-deleted
Roadmap: Device USB Lockdown	*Protection profile available upon request (2 days lead time)*
Roadmap: Application whitelisting	*Protection profile available upon request*

Network Protection: ControlD DNS Firewall



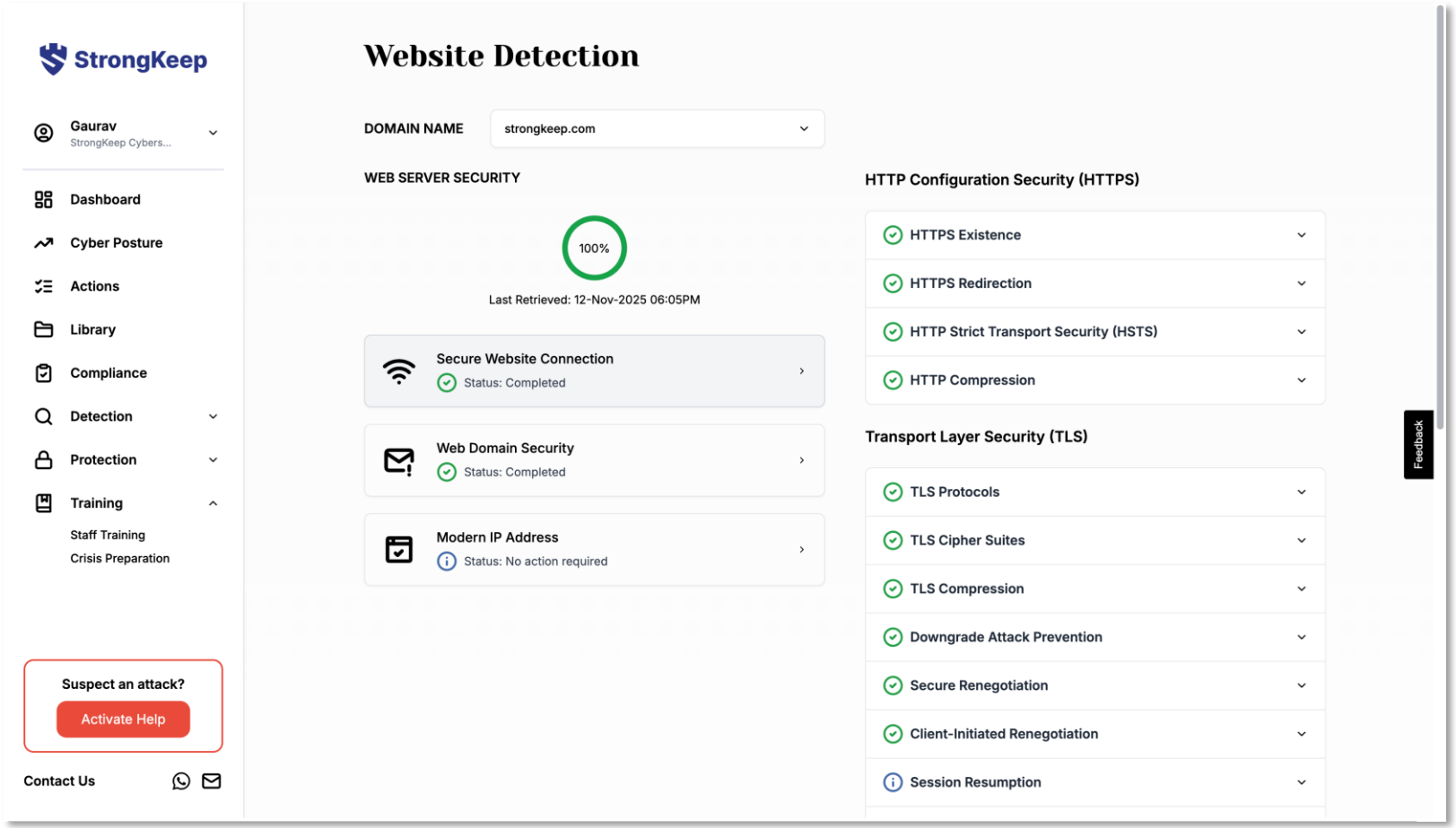




Network Protection: ControlD DNS Firewall

Capability	StrongKeep Description
Threat-based filtering	Automatically blocks known malware, phishing sites, command-and-control (C2) domains, and botnet infrastructure using real-time ControlD threat feeds.
Content category filtering	Optional filtering for adult content, gambling, torrents, and other high-risk categories to reduce accidental exposure and policy violations.
Encrypted DNS (DoH / DoT)	All DNS queries are upgraded to secure DNS-over-HTTPS or DNS-over-TLS, preventing ISP snooping or manipulation.
Endpoint-enforced DNS protection	DNS policies enforced directly via the StrongKeep endpoint agent–works on corporate and BYOD devices regardless of network.
Network / Router-level protection	Support for router-level DNS deployment to protect unmanaged devices on office networks or guest Wi-Fi.
Cross-platform / BYOD support	Works on Windows, macOS, Linux, iOS, Android; also compatible with the lightweight ctrld daemon for servers and custom environments. Easily installed on BYOD.
DNS inspection & risk alerts	Suspicious or malicious DNS lookups flagged in StrongKeep console; risky events summarised for SMB-friendly visibility.
DNS activity reporting	StrongKeep displays key DNS security events; full detailed logs available as downloadable reports for compliance or investigations.
Cloud-based global filtering	Protection backed by ControlD's global Anycast DNS infrastructure for low-latency resolution and worldwide coverage.
Auto-roaming protection	Devices remain protected outside the office–DNS policy follows the user across home networks, public Wi-Fi, and overseas travel.
Data retention	DNS event metadata retained for active subscribers + 90 days for export after termination, then securely hard-deleted.
Future roadmap: Custom allow/deny lists	*Admins will be able to create custom blocklists and allowlists for fine-grained control of business-specific domains.*

Detection: Server Scans



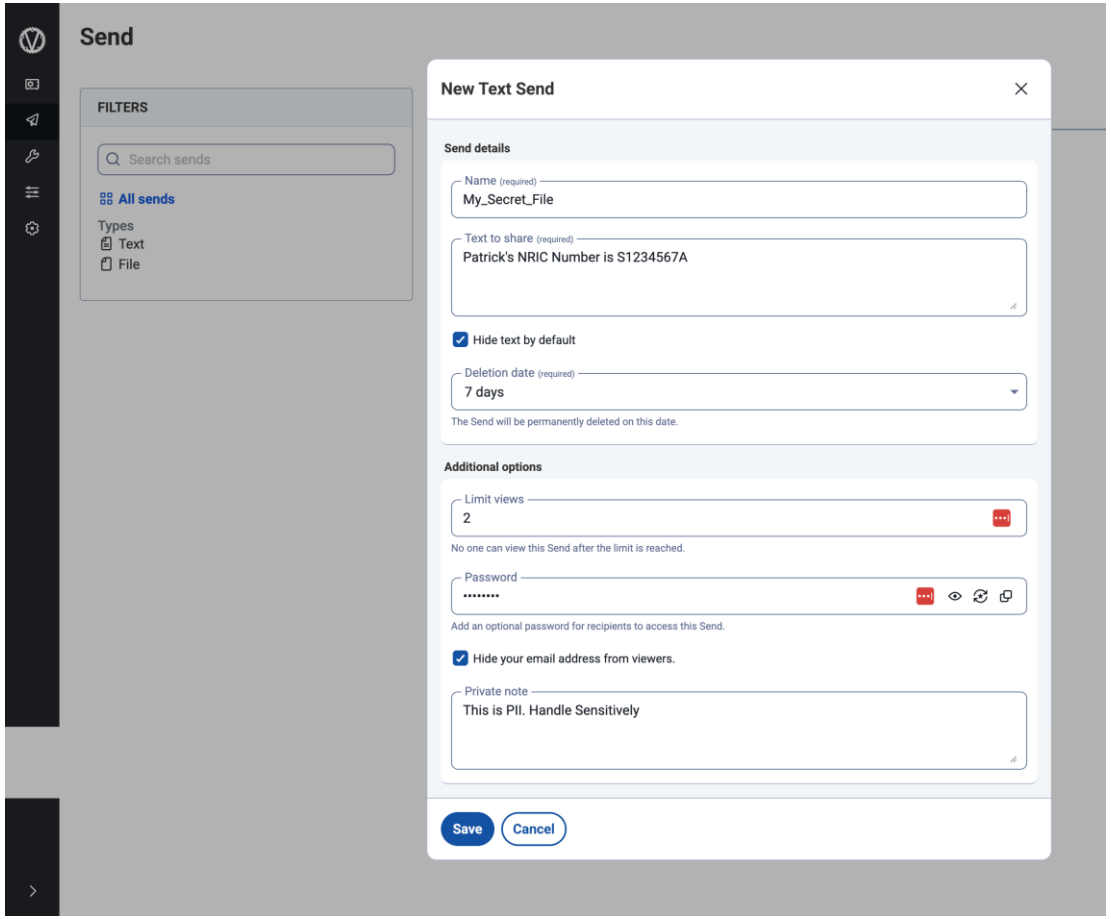
Powered by the
Cyber Security Agency of Singapore
Internet Hygiene Portal

Detection: Server Scans

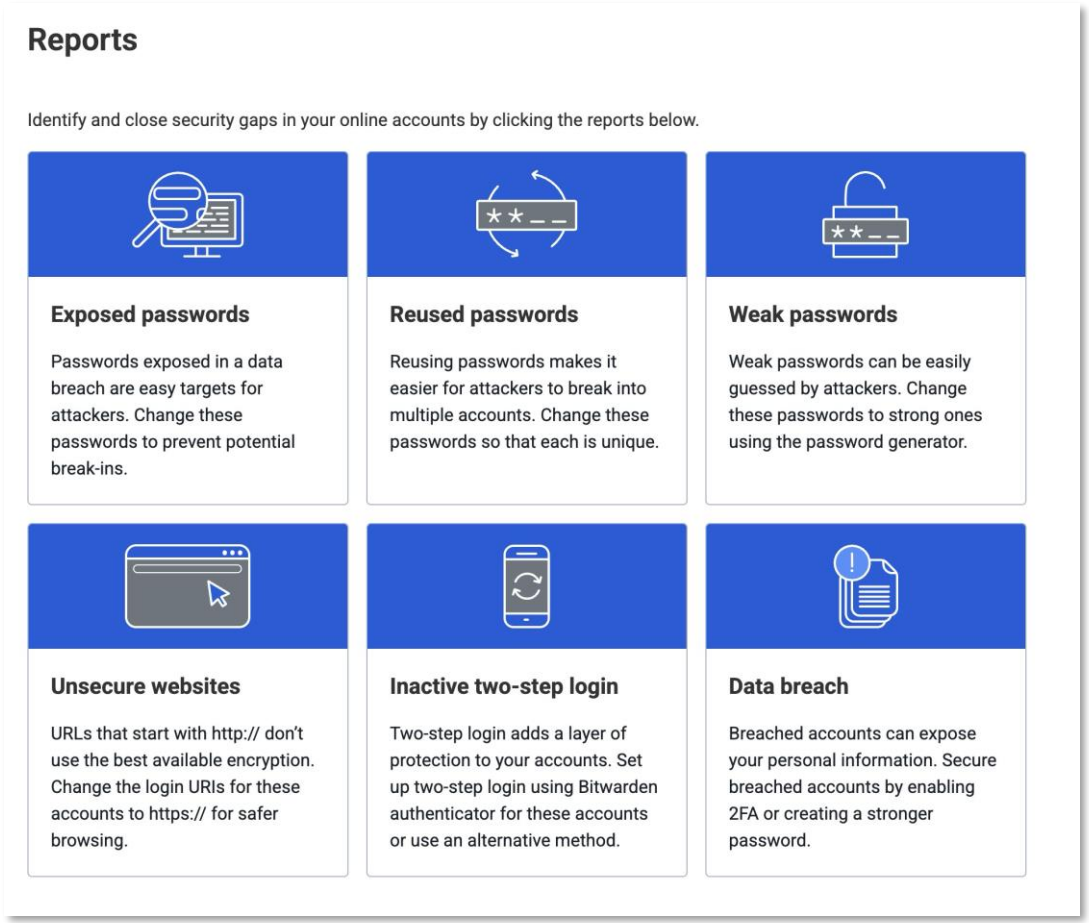
Capability	StrongKeep Description
Email authentication checks	Automated scanning of your domain's DMARC, SPF, DKIM setup to detect misconfigurations that enable spoofing or impersonation.
TLS/HTTPS configuration audit	Checks for SSL/TLS strength, certificate validity, HSTS, and other transport-layer hygiene signals aligned to CSA Internet Hygiene Portal guidance.
DNS hygiene validation	Evaluates DNS records like MX, CNAME, NS, and observes risky exposures such as dangling or misconfigured records.
Mailflow security insights	Detects insecure mail server configurations (e.g., open relays, outdated ciphers, weak STARTTLS policies) and suggests mitigation.
Web exposure & service enumeration	Identifies public-facing services (ports, protocols) and flags weak configurations that increase attack surface.
Automated fix-guides	For every failed check, StrongKeep provides step-by-step, SMB-friendly configuration guidance—no cybersecurity expertise required.
Continuous monitoring (Roadmap)	*Upcoming automated re-scans to track improvements, regressions, and compliance readiness over time.*
Secure Email Gateway (Roadmap)	*Cloudflare SEG integration to block phishing, spam, malware, and suspicious attachments before they reach inboxes.*
Web Application Firewall (Roadmap)	*Cloudflare WAF integration to protect websites and web apps from OWASP Top 10 threats, bots, and exploitation attempts.*
Compliance-ready reporting	One-click downloadable hygiene reports for tenders, audits, and CSA Cyber Essentials submission.

Protection: Credentials / Passwords

(powered by VaultWarden)



Encrypted File Send



Organisation-wide visibility

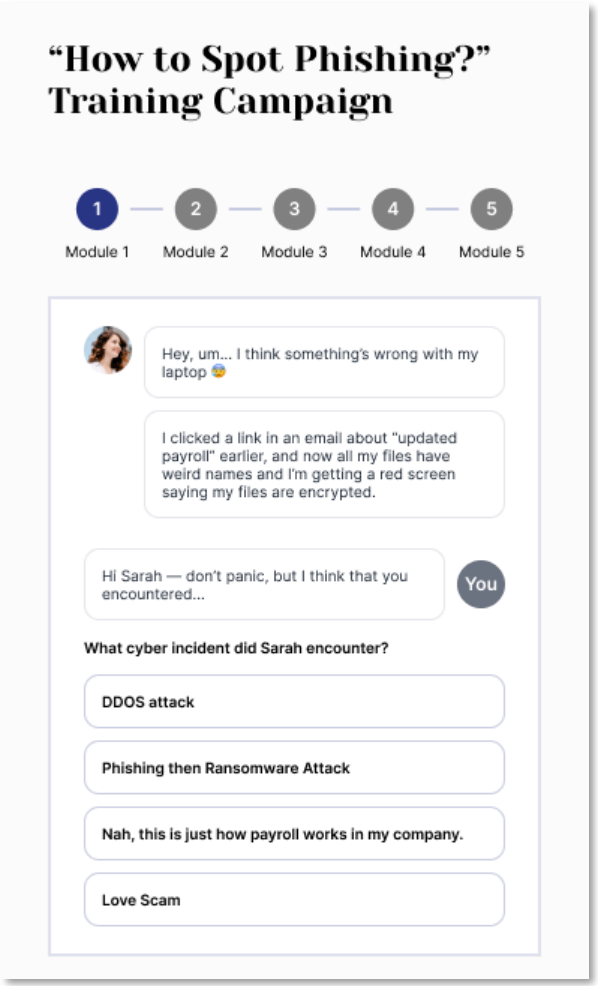
Vaultwarden

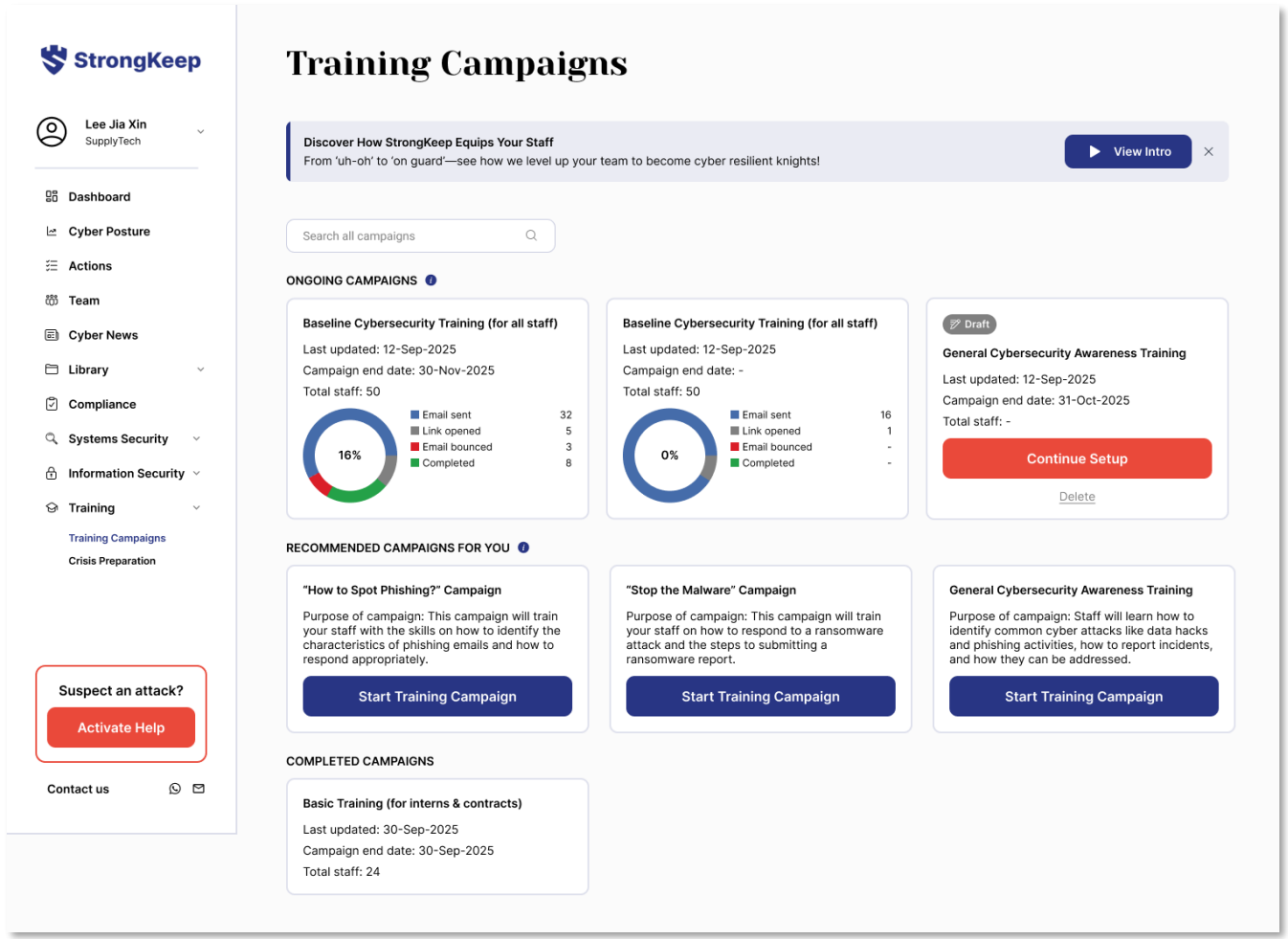
Protection: Credentials / Passwords

(powered by VaultWarden)

Capability	StrongKeep Description
End-to-end encrypted vault	All credentials, secrets, secure notes, and attachments are stored in the VaultWarden-based vault using zero-knowledge encryption – StrongKeep never sees plaintext content.
Cross-device & browser & BYOD support	Full compatibility with Bitwarden clients/extensions, enabling seamless sync across desktop, mobile, web browsers for users and teams.
Team sharing & access roles	Shared vault collections for teams, with role-based access, audit logs, and admin control incorporated in the StrongKeep Dashboard (leveraging VaultWarden's Org/Collections model).
Weak / leaked credential detection	Integrated service checking credentials against breach/leak datasets; alerts when stored credentials are weak, reused, or found in public breaches.
Two-factor & FIDO2 support	Support for 2FA authenticator apps, email 2FA, FIDO2/WebAuthn keys, YubiKey integrations for admin/users to strengthen vault access.
Securely Send PII / Secrets	Use the Vault to send PII and other secrets (PDPA and HIB compliant).
Credential hygiene dashboard	StrongKeep provides a dashboard for credential health: reused passwords, weak passwords, shared credentials, stale accounts, and remediation guidance.
Compliance & audit reporting	Exportable logs and reports of credential events (access, share, changes), supporting audits for ISO 27001, CSA Cyber Essentials, etc.
Roadmap: Passkey & Identity-less login support	*Planned enhancement: support passkeys (webauthn), aligning with next-gen credential management philosophy.*
Roadmap: Automated onboarding & provisioning support	*API or connector support to onboard new users, sync with identity systems (Microsoft 365 and Google Workspace) so credential management scales with accounts.*

Training: Quiz + Phishing + Crisis Prep

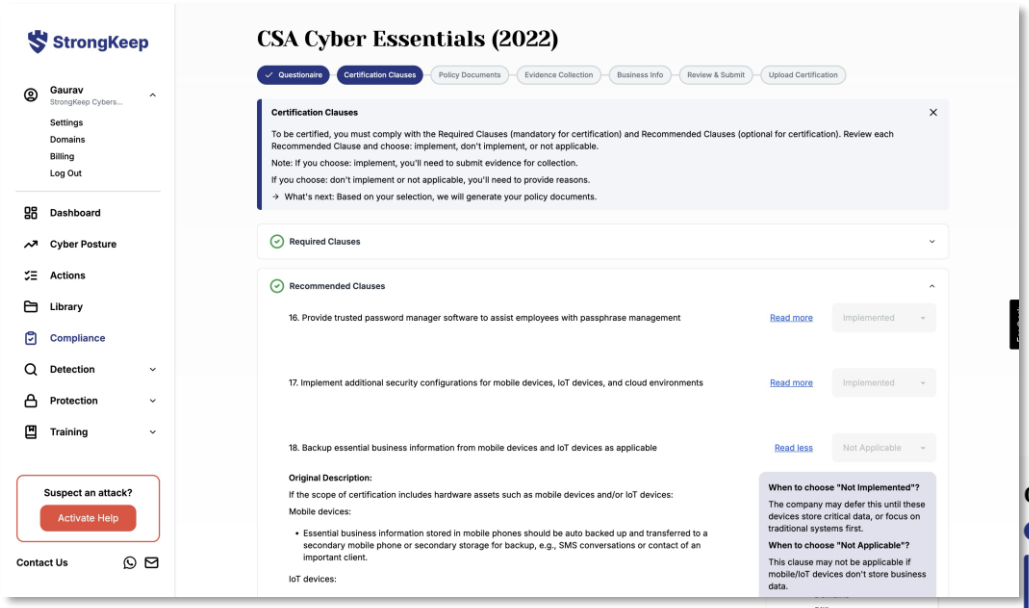


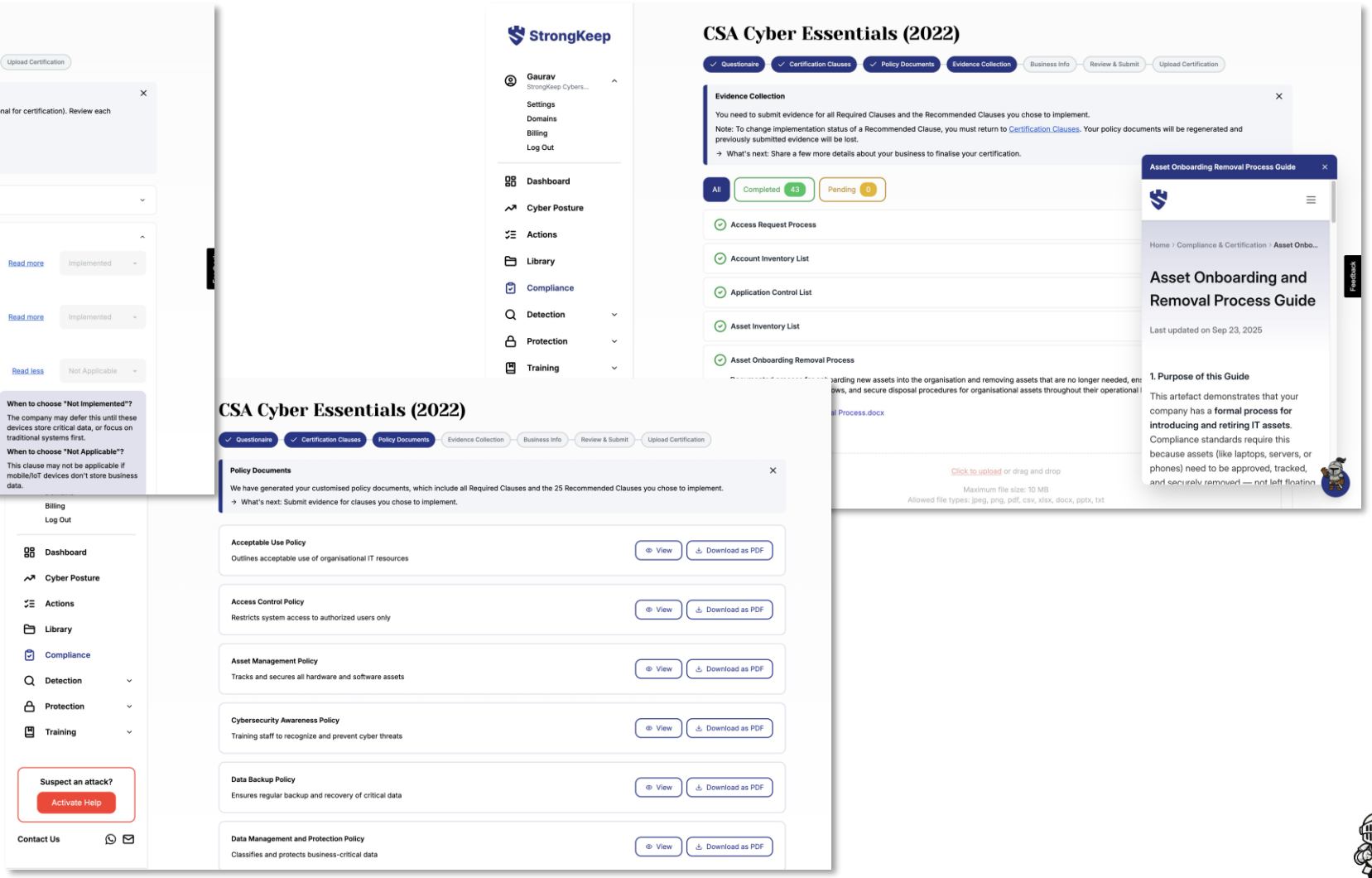


Training: Quiz + Phishing + Crisis Prep

Capability	StrongKeep Description
Interactive AI-generated company cyber crisis scenario training platform	Customisable live simulations with branching logic, where an AI-engine generates incident scenarios, event triggers and roles for participants to act in real time.
Facilitator-ready playbooks & content templates	Ready-to-use (and brandable) facilitation materials, scripts, presentation decks and trainer prompts included so SMBs can run exercises quickly.
Cross-platform quizzes & micro-learning	Accessible via browser or mobile devices, quizzes adapt automatically or via admin choice. Topics, difficulty and modules are auto-assigned or selectable.
User profiles & deep analytics	Each staff member has a profile; quiz results, scenario responses and progress are tracked and visualised across teams and groups.
Reporting, benchmarking & trends	Real-time dashboard + exportable reports (PDF/CSV) showing completion, risk-scores and benchmarking against other StrongKeep customers.
Roadmap: Phishing simulator & campaign integration	*Easy admin-config to launch phishing email campaigns; results feed into trainings–staff who click are routed into targeted modules.*
Roadmap: Gamification & engagement layer	*Badges, leaderboards, scoring, streaks and progress-tracking drive engagement and reduce training fatigue.*

Compliance: Cyber Certification

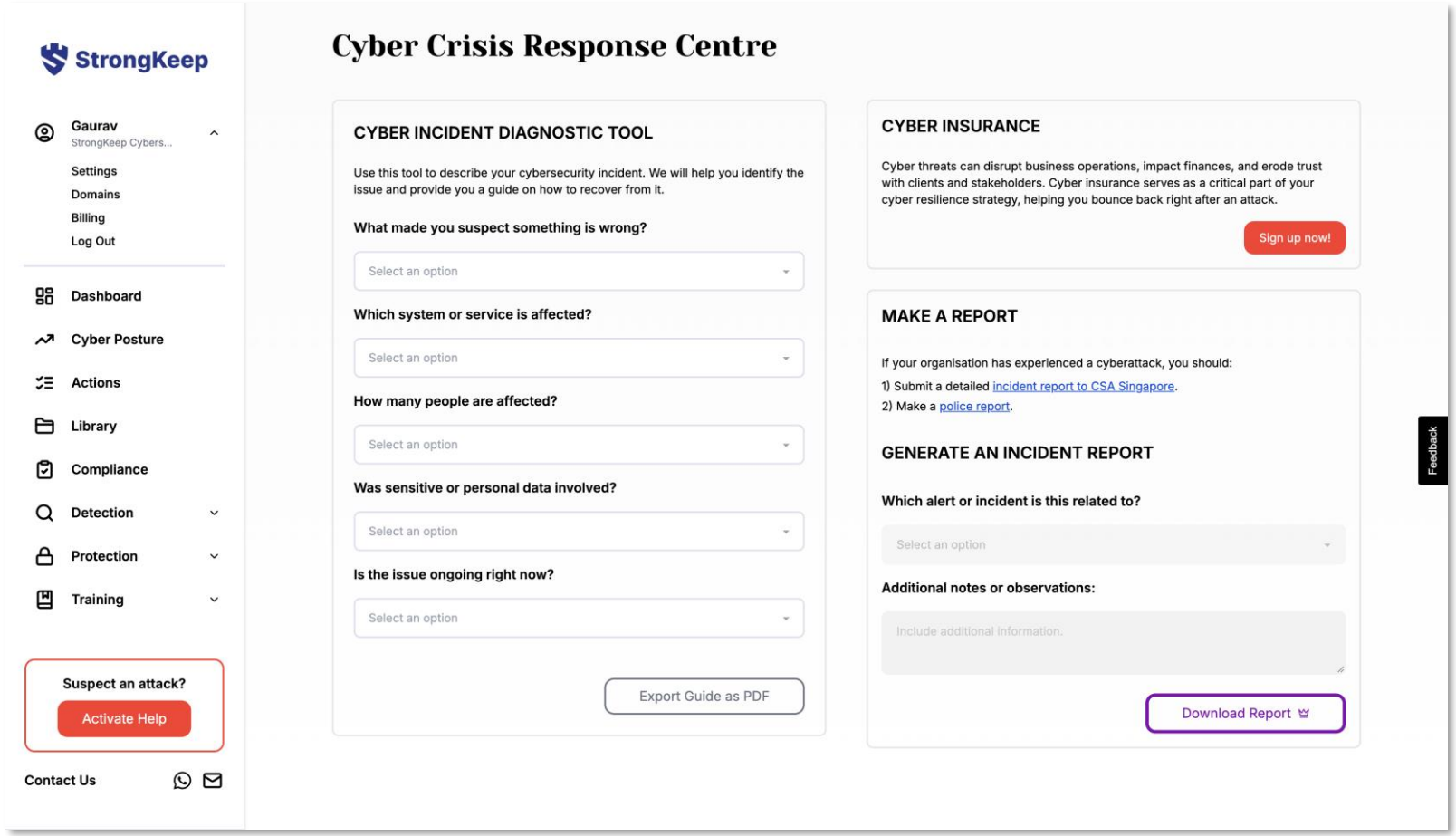




Compliance: Cyber Certification

Capability	StrongKeep Description
Framework support: Cyber Essentials (now), *HIB/ISO 27001/SOC2/MAS TRM (roadmap)*	Currently supports UK-focused Cyber Essentials; future releases will add frameworks such as HIB, ISO 27001, SOC2 and MAS TRM for broader compliance.
Pre-filled policy & procedure templates	Customers receive fully populated PDF templates (editable) for policies, procedures and records–reducing start-up time and removing blank-page syndrome.
Automated evidence generation from StrongKeep tools	The system pulls evidence automatically from our modules (e.g., Device Protection, Network Protection) to fulfil artefact requirements without manual uploads.
Guided artefact collection workflow	Where automatic collection is not possible, a step-by-step UI prompts users to upload, link or map required artefacts and tracks progress to audit-readiness.
One-click submission package for certification	With one click, the full compliance bundle (policies + artefacts + report) is generated in auditor-friendly format and submission-ready for certification bodies.
SaaS-hosted platform	Fully hosted by StrongKeep, accessible via browser. Role-based admin access ensures security and controlled delegation for SMBs without dedicated compliance teams.
Dashboard with status, tasks & benchmarking	A “single pane” dashboard shows which controls are complete, outstanding tasks, and benchmarking against peer SMB compliance performance.

Incident Response



ALL PLANS
(INSURANCE IS ADDITIONAL)

Incident Response

Capability	StrongKeep Description
Guided incident-diagnostic wizard	A web-based interactive tool prompts users to describe what they suspect ("Which system or service is affected?" etc), then helps map the incident type and recommended next steps.
Pre-configured incident playbooks	Pre-built response playbooks for common incidents (malware, phishing compromise, data breach) that guide users through containment, eradication, and recovery.
Integration with other modules	Telemetry from StrongKeep modules (e.g., Device Protection, Network Protection) is pulled where available to enrich the diagnostic and reduce manual data entry.
Roadmap: Automated incident report generation	*One-click generation of audit-ready PDF or interactive report: incident timeline, root cause, actions taken, remediation plan and insurer-ready documentation.*
Option: Insurance-top-up	Partnered with MSIG cyber insurance: StrongKeep facilitates insurer activation and provides one-click incident reporting and claims initiation.
Option: 24/7 escalation & full-service IR	On-demand escalation to external IR vendor through insurance (forensic, legal, communications) via the insurance add-on; SMBs get enterprise-grade response without full-time SOC.
Roadmap: Role-based notifications & escalation workflow	*Built-in notifications alert relevant stakeholders (IT admin, C-suite, insurer) and escalate according to incident type and severity.*

Protection: Data *(ROADMAP)*

Capability	StrongKeep Description
Business-critical data backup	*Focused on backing up files and data deemed "business-critical" (rather than full image backups), enabling simpler, cost-efficient protection.*
Point-in-time data restore	*Users can restore data to previous safe points in time (file-level), enabling recovery from accidental deletion or corruption.*
Retention & archival tiers	*Supports archival backup storage for long-term retention of critical business data, reducing worry about managing storage for small teams.*
Data Loss Protection (DLP) browser plugin	*A browser extension will monitor uploads/clipboard/actions in browsers and warn against PII data leakage*
Unified dashboard	*Backup and DLP features will appear in the same StrongKeep console.*

Agentic 24/7 virtual CISO

- Coming soon. Powered by joint R&D with A*STAR

Agency for Science, Technology and Research
SINGAPORE

Product Specifications / Requirements

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).

Product Specifications / Requirements

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:** sign up, connect domain, deploy agent/DNS; **first devices protected within ~2 hour** for most SMBs.

Assurance

- **We are Cyber Essentials certified** (using StrongKeep).

Project Roadmap

Timeline	Expected New Features*
Dec 2025	• **Integration with M365 and Google to allow automatic update of staff list.** This will enable Users to have a "staff level overview" on their cyber risk level (whether they have installed/completed the EDR, DNS, password manager, and training). This will also enable one-click reminders for staff to do training or complete onboarding for protection tools. • **New training system** This enables Users to select Training Quiz templates that have richer learning content (videos, images, interactive content) across a wider variety of cybersecurity topics. • **Automatic deployment of DNS Firewall** This enables users to deploy the DNS Firewall to staff from the StrongKeep dashboard. • **EDR UI refresh** This reduces the noise from the anti-malware solution and provides more useful insights and advice on the cases. • **Automatic population of Hardware Asset List** This allows users to auto-populate a hardware list (or manually import one) for StrongKeep's tracking of the asset inventory and management of protected devices within that list.
Jan 2025	• **New Standards: CE2025, DPE, HIB** • **Enhanced onboarding of users.** A wizard-based system will guide even non-technical Users to onboard themselves and their staff to all the tools in a seamless process. • **Automatic report generation / compliance evidence submission** Tools such as training, EDR, DNS, asset inventory, and staff list will generate reports that can be used for compliance or regular updates. • **Compliance: Bring Your Own Policies** Users can bring their existing policies for gap assessment with chosen standard.
Feb 2025	• **Compliance Evidence Assessment** Submitted artefacts will be evaluated to provide feedback to the user on whether the artefact is likely to comply with that clause or requires additional evidence. • **New Standards: ISO27001**
Q2 2025	• Agentic Training System, Agentic Threat Scanning (News & Alerts), Agentic Policy Gap Assessment, Data Loss Protection & Backups
Q3 2025	• Agentic & Integrated Protection Tools
Q4 2025	• Our cyber knights will be able to vanquish dragons and conquer the world.

* This chart represents our planned milestones and does not constitute an assurance or commitment to feature delivery.

StrongKeep

www.StrongKeep.com

Cybersecurity for small & medium businesses

54% of cyber attacks target SMBs. Most won't survive.

SMBs know that cybersecurity is important, and want to do something about it… but:

- **52% of SMBs say is too expensive** *(which it was, honestly)*
- **32% say it is too complicated** *(and hiring a cyber expert isn't an option)*
- **31% say it takes too much time** *(which is better spent on their business!)*

STRONGKEEP: A cyber security SaaS platform built for SMBs - simple to deploy, easy to use, and takes all the pain (and cyber risk) away.

Protection Plan

Prevent phishing & malware
Endpoint protection, network firewall, web & mail server scans

Train employees
Password manager, breach detection, staff training, phishing simulation

Ensure you are prepared
Crisis preparation training, incident diagnostics tool

$39/mo*

* Includes 5 devices, billed annually, +$5/mo for each additional device. Promotional pricing.

Compliance Plan

Everything in Protection Plan
+
Automated Certification
Cyber Essentials (coming soon - *Data Protection Essentials, HIB compliance)*

Stay compliant with ease
Evidence tracking, monthly reminders, audit logs

$159/mo*

* Includes 5 devices, billed annually, +$5/mo for each additional device. Promotional pricing.

Insurance

Cyber Insurance
(Additional **$75++/mo**)

MSIG

CSA SINGAPORE · ENSIGN INFOSECURITY · paloalto NETWORKS · CyberSG R&D Programme Office · A*STAR Agency for Science, Technology and Research SINGAPORE · SETSCO · aws

Simple. Affordable. Comprehensive.

- Ex-Deputy Commissioner & Deputy CEO of Cyber Security Agency, Singapore
- Ex-EVP (Advisory & “Product Development”), Ensign InfoSecurity
- ex-CIO, Republic of Singapore Air Force
- UN Expert on Emerging Cyber Threats
- Senior Adjunct Fellow, NTU
- ex-WEF Global Futures Council on Cybersecurity
- Board Cyber Advisor to Asia's Fortune 500
- Co-founder of national techforgood charity better.sg

Founder / CEO

BG(NS) **Gaurav Keerthi**

StrongKeep

hello@StrongKeep.com

www.StrongKeep.com