



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 application) while keeping costs significantly lower than hiring a CISO or a consultant.



Dashboard: Unified Cybersecurity



StrongKeep

Lee Jia Xin
SupplyTech

- Dashboard
- Cyber Posture
- Actions
- Team
- Cyber News
- Library
- Compliance
- Systems Security
- Information Security
- Training

Suspect an attack?
Activate Help

Contact us

Cyber Posture

Daily Trend ↗ 4% B Grade

Risk increased due to new external vulnerabilities discovered in Windows 11. Complete more Actions to lower your overall risk.

Actions

- Complete training quiz
- Increase password manager adoption
- Complete CSA Cyber Essentials (2022) certi

Cyber News

- New ransomware variant targets healthcare sector
- Vulnerability found in popular VPN software
- AI deepfake attacks increase by 300% in Q4 2024
- At least \$172,000 lost in phishing scams

Compliance

CSA Cyber Essentials (2022)

Overall Progress: 75%

Current Stage: Evidence Collection
Stage 4 of 7

Email & Website

Mail Server Security: 85%
Web Server Security: 78%

Secure Email Gateway: Active
Web Application Firewall: Active

Devices

Devices Monitored: 45/50

Successfully Blocked Threats:

- High severity: 2 blocked
- Medium severity: 8 blocked
- Low severity: 15 blocked

Network

Devices Monitored: 45/50

Successfully Prevented Threats:

- Total blocked: 2.1K
- Total redirected: 1.2K

Accounts & Data

Password Manager Users: 32
Leaked Credentials: 2 Found
Backups: Active

Training

Cybersecurity Staff Training: Total staff: 50

16%

- Email opened: 8
- Attempted: 24
- Completed: 8
- Email sent / bounced: 3
- Link opened: 5

Last updated: 12-Sep-2025

StrongKeep

Lee Jia Xin
SupplyTech

- Dashboard
- Cyber Posture
- Actions
- Cyber News
- Library
- Compliance
- Systems Security
- Information Security
- Training

Suspect an attack?
Activate Help

Contact us

Cyber Posture

Get a clear snapshot of the key factors that influenced your organisation's risk score over the past month, so you can see what's driving the numbers and identify where improvements are needed.

30-DAY CYBER POSTURE TREND

Your organisation's daily overall cyber posture over the last 30 days.

B Grade

HOW DOES MY CYBER POSTURE COMPARE AGAINST OTHERS?

WHAT ARE THE KEY FACTORS THAT AFFECT MY CYBER POSTURE?

- Positive Factors:**
 - High compliance score with CSA Cyber Essentials (75%)
 - 85% of users have completed security training
 - Active Web Application Firewall
 - Active Secure Email Gateway
- Negative Factors:**
 - 5 endpoints are not monitored by protection software
 - 18 users are not using the password manager

HOW IS CYBER POSTURE GRADED?

Cyber posture is your readiness level — how well your defences hold up if someone tries to break in. The higher the score, the more secure you are.

- A 80-100**: You have strong defences in place with minimal risk.
- B 70-80**: You're mostly secure, just a couple of weak spots to watch out for.
- C 60-70**: You have some protections working but there are gaps attackers could use.
- D 50-60**: Your defences are weak. Immediate action is needed to strengthen security.
- F <50**: You're in the danger zone and exposed to serious threats.
- NA**: We can't grade your risk yet because we need more data to get the full picture.

Download Your Cyber Posture Report

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

Devices

Devices Monitored

Successfully Blocked Threats

- High severity 2 blocked
- Medium severity 8 blocked
- Low severity 15 blocked

45/50

StrongKeep

Gaurav
StrongKeep Cybe...

- Dashboard
- Cyber Posture
- Actions
- Library
- Compliance
- Detection
 - Mail Server Security
 - Web Server Security
- Protection
 - Endpoints
 - Alerts
- Training
 - Staff Training
 - Crisis Preparation

Suspect an attack?

Security Alerts

SUMMARY

LOW	MEDIUM	HIGH	CRITICAL
1	20	6	0

ALERTS

Kernel Privilege Escalation 12-Nov-2025 05:15PM

Host name: Cheng's MacBook Air (2)
Severity: High

WildFire Malware 11-Nov-2025 01:48PM

Host name: Ryan's MacBook Air
Severity: Medium

Local Analysis Malware 11-Nov-2025 12:06PM

Host name: Ryan's MacBook Air
Severity: Medium

WildFire Malware 11-Nov-2025 11:51AM

Host name: Ryan's MacBook Air
Severity: Medium

Kernel Privilege Escalation

Description

Alert 'Kernel Privilege Escalation' (High severity) in category 'Exploit' was detected on host Cheng's MacBook Air (2) by user root at 12-Nov-2025 05:15PM . The process 'cp' ran with command '/bin/cp /Library/Preferences/SystemConfiguration/preferences.plist /Library/Preferences/SystemConfiguration/preferences.plist.old' and was blocked.

Alert Details

Status	Prevented (Blocked)
Timestamp	12-Nov-2025 05:15PM
Category	Exploit
Severity	HIGH

Endpoint Details

Host name	Cheng's MacBook Air (2)
Operating System	macOS
IP Address	172.31.52.143
MAC Address	a2:ca:b3:f0:a5:20
EDR Version	PANW/XDR Agent 8.8.0.2885

Feedback



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	<i>Protection profile available upon request (2 days lead time)</i>
Roadmap: Application whitelisting	<i>Protection profile available upon request</i>



Network Protection: ControlD DNS Firewall



Network

Devices Monitored 45/50

Successfully Prevented Threats

- Total blocked 2.1K
- Total redirected 1.2K

AI Malware Filter EXPERIMENTAL: Blocks malicious domains using machine learning. [Learn more](#) Aggressive

Safe Search Prevent search engines from showing mature content. [Learn more](#) Minimal
Standard

Restricted Youtube Prevent Youtube from showing mature content and disable comments. [Learn more](#) Aggressive

Endpoints

Unique DNS resolvers tailored for users or networks, enforcing one or more Profiles.

- Chrome-Canary Privacy Profile
- GL-Inet-Router Default Profile (03-26)
- Macbook Default Profile (03-26)
- Windows Privacy Profile



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	<i>Admins will be able to create custom blocklists and allowlists for fine-grained control of business-specific domains.</i>



Detection: Server Scans



StrongKeep

Gaurav
StrongKeep Cybers...

- Dashboard
- Cyber Posture
- Actions
- Library
- Compliance
- Detection
- Protection
- Training
 - Staff Training
 - Crisis Preparation

Website Detection

DOMAIN NAME: strongkeep.com

WEB SERVER SECURITY

100%

Last Retrieved: 12-Nov-2025 06:05PM

- Secure Website Connection
Status: Completed
- Web Domain Security
Status: Completed
- Modern IP Address
Status: No action required

HTTP Configuration Security (HTTPS)

- HTTPS Existence
- HTTPS Redirection
- HTTP Strict Transport Security (HSTS)
- HTTP Compression

Transport Layer Security (TLS)

- TLS Protocols
- TLS Cipher Suites
- TLS Compression
- Downgrade Attack Prevention
- Secure Renegotiation
- Client-Initiated Renegotiation
- Session Resumption

Suspect an attack?
Activate Help

Contact Us

Feedback



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)	<i>Upcoming automated re-scans to track improvements, regressions, and compliance readiness over time.</i>
Secure Email Gateway (Roadmap)	<i>Cloudflare SEG integration to block phishing, spam, malware, and suspicious attachments before they reach inboxes.</i>
Web Application Firewall (Roadmap)	<i>Cloudflare WAF integration to protect websites and web apps from OWASP Top 10 threats, bots, and exploitation attempts.</i>
Compliance-ready reporting	One-click downloadable hygiene reports for tenders, audits, and CSA Cyber Essentials submission.



Protection: Credentials / Passwords

(powered by VaultWarden)



Send

FILTERS

Search sends

All sends

Types

- Text
- File

New Text Send

Send details

Name (required)
My_Secret_File

Text to share (required)
Patrick's NRIC Number is S1234567A

Hide text by default

Deletion date (required)
7 days
The Send will be permanently deleted on this date.

Additional options

Limit views
2
No one can view this Send after the limit is reached.

Password
.....
Add an optional password for recipients to access this Send.

Hide your email address from viewers.







Private note
This is PII. Handle Sensitive

Save Cancel

Encrypted File Send

Reports

Identify and close security gaps in your online accounts by clicking the reports below.

 <p>Exposed passwords</p> <p>Passwords exposed in a data breach are easy targets for attackers. Change these passwords to prevent potential break-ins.</p>	 <p>Reused passwords</p> <p>Reusing passwords makes it easier for attackers to break into multiple accounts. Change these passwords so that each is unique.</p>	 <p>Weak passwords</p> <p>Weak passwords can be easily guessed by attackers. Change these passwords to strong ones using the password generator.</p>
 <p>Insecure websites</p> <p>URLs that start with http:// don't use the best available encryption. Change the login URIs for these accounts to https:// for safer browsing.</p>	 <p>Inactive two-step login</p> <p>Two-step login adds a layer of protection to your accounts. Set up two-step login using Bitwarden authenticator for these accounts or use an alternative method.</p>	 <p>Data breach</p> <p>Breached accounts can expose your personal information. Secure breached accounts by enabling 2FA or creating a stronger password.</p>

Organisation-wide visibility



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	<i>Planned enhancement: support passkeys (webauthn), aligning with next-gen credential management philosophy.</i>
Roadmap: Automated onboarding & provisioning support	<i>API or connector support to onboard new users, sync with identity systems (Microsoft 365 and Google Workspace) so credential management scales with accounts.</i>





Training: Quiz + Phishing + Crisis Prep

“How to Spot Phishing?” Training Campaign

- 1 Module 1
- 2 Module 2
- 3 Module 3
- 4 Module 4
- 5 Module 5



Hey, um... I think something's wrong with my laptop 🤔

I clicked a link in an email about "updated payroll" earlier, and now all my files have weird names and I'm getting a red screen saying my files are encrypted.

Hi Sarah — don't panic, but I think that you encountered...



What cyber incident did Sarah encounter?

- DDOS attack
- Phishing then Ransomware Attack
- Nah, this is just how payroll works in my company.
- Love Scam



Lee Jia Xin
SupplyTech

- Dashboard
- Cyber Posture
- Actions
- Team
- Cyber News
- Library
- Compliance
- Systems Security
- Information Security
- Training
 - Training Campaigns
 - Crisis Preparation

Suspect an attack?
Activate Help

Contact us

Training Campaigns

Discover How StrongKeep Equips Your Staff
From 'uh-oh' to 'on guard'—see how we level up your team to become cyber resilient knights!

[View Intro](#)

Search all campaigns

ONGOING CAMPAIGNS

Baseline Cybersecurity Training (for all staff)
Last updated: 12-Sep-2025
Campaign end date: 30-Nov-2025
Total staff: 50

Email sent	32
Link opened	5
Email bounced	3
Completed	8

16%

Baseline Cybersecurity Training (for all staff)
Last updated: 12-Sep-2025
Campaign end date: -
Total staff: 50

Email sent	16
Link opened	1
Email bounced	-
Completed	-

0%

General Cybersecurity Awareness Training
Last updated: 12-Sep-2025
Campaign end date: 31-Oct-2025
Total staff: -

[Continue Setup](#)

[Delete](#)

RECOMMENDED CAMPAIGNS FOR YOU

“How to Spot Phishing?” Campaign
Purpose of campaign: This campaign will train your staff with the skills on how to identify the characteristics of phishing emails and how to respond appropriately.

[Start Training Campaign](#)

“Stop the Malware” Campaign
Purpose of campaign: This campaign will train your staff on how to respond to a ransomware attack and the steps to submitting a ransomware report.

[Start Training Campaign](#)

General Cybersecurity Awareness Training
Purpose of campaign: Staff will learn how to identify common cyber attacks like data hacks and phishing activities, how to report incidents, and how they can be addressed.

[Start Training Campaign](#)

COMPLETED CAMPAIGNS

Basic Training (for interns & contracts)
Last updated: 30-Sep-2025
Campaign end date: 30-Sep-2025
Total staff: 24



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	<i>Easy admin-config to launch phishing email campaigns; results feed into trainings—staff who click are routed into targeted modules.</i>
Roadmap: Gamification & engagement layer	<i>Badges, leaderboards, scoring, streaks and progress-tracking drive engagement and reduce training fatigue.</i>



Compliance: Cyber Certification



CSA Cyber Essentials (2022)

Questionnaire Certification Clauses Policy Documents Evidence Collection Business Info Review & Submit Upload Certification

Certification Clauses

To be certified, you must comply with the Required Clauses (mandatory for certification) and Recommended Clauses (optional for certification). Review each Recommended Clause and choose: implement, don't implement, or not applicable.

Note: If you choose: implement, you'll need to submit evidence for collection.
If you choose: don't implement or not applicable, you'll need to provide reasons.
→ What's next: Based on your selection, we will generate your policy documents.

Required Clauses

Recommended Clauses

- 16. Provide trusted password manager software to assist employees with passphrase management. [Read more](#) Implemented
- 17. Implement additional security configurations for mobile devices, IoT devices, and cloud environments. [Read more](#) Implemented
- 18. Backup essential business information from mobile devices and IoT devices as applicable. [Read less](#) Not Applicable

Original Description:
If the scope of certification includes hardware assets such as mobile devices and/or IoT devices:
Mobile devices:
• Essential business information stored in mobile phones should be auto backed up and transferred to a secondary mobile phone or secondary storage for backup, e.g., SMS conversations or contact of an important client.
IoT devices:

When to choose "Not Implemented"?
The company may defer this until these devices store critical data, or focus on traditional systems first.

When to choose "Not Applicable"?
This clause may not be applicable if mobile/IoT devices don't store business data.

CSA Cyber Essentials (2022)

Questionnaire Certification Clauses Policy Documents Evidence Collection Business Info Review & Submit Upload Certification

Evidence Collection

You need to submit evidence for all Required Clauses and the Recommended Clauses you chose to implement.
Note: To change implementation status of a Recommended Clause, you must return to [Certification Clauses](#). Your policy documents will be regenerated and previously submitted evidence will be lost.
→ What's next: Share a few more details about your business to finalise your certification.

All Completed 43 Pending 0

- Access Request Process
- Account Inventory List
- Application Control List
- Asset Inventory List
- Asset Onboarding Removal Process

Asset Onboarding and Removal Process Guide

Home > Compliance & Certification > Asset Onbo...

Last updated on Sep 23, 2025

1. Purpose of this Guide

This artefact demonstrates that your company has a formal process for introducing and retiring IT assets. Compliance standards require this because assets (like laptops, servers, or phones) need to be approved, tracked, and securely removed — not left floating...

Policy Documents

We have generated your customised policy documents, which include all Required Clauses and the 25 Recommended Clauses you chose to implement.
→ What's next: Submit evidence for clauses you chose to implement.

- Acceptable Use Policy
Outlines acceptable use of organisational IT resources. [View](#) [Download as PDF](#)
- Access Control Policy
Restricts system access to authorized users only. [View](#) [Download as PDF](#)
- Asset Management Policy
Tracks and secures all hardware and software assets. [View](#) [Download as PDF](#)
- Cybersecurity Awareness Policy
Training staff to recognize and prevent cyber threats. [View](#) [Download as PDF](#)
- Data Backup Policy
Ensures regular backup and recovery of critical data. [View](#) [Download as PDF](#)
- Data Management and Protection Policy
Classifies and protects business-critical data. [View](#) [Download as PDF](#)



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





Gaurav
StrongKeep Cybers...

- Settings
- Domains
- Billing
- Log Out

- Dashboard
- Cyber Posture
- Actions
- Library
- Compliance
- Detection
- Protection
- Training

Suspect an attack?

Activate Help

Contact Us

Cyber Crisis Response Centre

CYBER INCIDENT DIAGNOSTIC TOOL

Use this tool to describe your cybersecurity incident. We will help you identify the issue and provide you a guide on how to recover from it.

What made you suspect something is wrong?

Select an option

Which system or service is affected?

Select an option

How many people are affected?

Select an option

Was sensitive or personal data involved?

Select an option

Is the issue ongoing right now?

Select an option

[Export Guide as PDF](#)

CYBER INSURANCE

Cyber threats can disrupt business operations, impact finances, and erode trust with clients and stakeholders. Cyber insurance serves as a critical part of your cyber resilience strategy, helping you bounce back right after an attack.

Sign up now!

MAKE A REPORT

If your organisation has experienced a cyberattack, you should:

- 1) Submit a detailed [incident report to CSA Singapore](#).
- 2) Make a [police report](#).

GENERATE AN INCIDENT REPORT

Which alert or incident is this related to?

Select an option

Additional notes or observations:

Include additional information.

Download Report 📄

Feedback



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	<i>One-click generation of audit-ready PDF or interactive report: incident timeline, root cause, actions taken, remediation plan and insurer-ready documentation.</i>
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	<i>Built-in notifications alert relevant stakeholders (IT admin, C-suite, insurer) and escalate according to incident type and severity.</i>



Protection: Data (**ROADMAP**)



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



Agentic 24/7 virtual CISO

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



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 **ctrlid** 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Agentic Training System, Agentic Threat Scanning (News & Alerts), Agentic Policy Gap Assessment, Data Loss Protection & Backups
Q3 2025	<ul style="list-style-type: none"> • Agentic & Integrated Protection Tools
Q4 2025	<ul style="list-style-type: none"> • Our cyber knights will be able to vanquish dragons and conquer the world.





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*

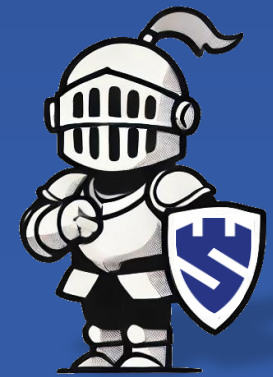
* Includes 5 devices, billed annually, +\$5/mo for each additional device. Promotional pricing.

Insurance

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



**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

