

TrustLayer™

A practical guide using TrustLayer

Cyber Essentials for UK SMBs



Introduction



UK small and medium-sized businesses face a critical cybersecurity challenge. With 43% experiencing cyber-attacks annually and average breach costs of £7,960, robust security frameworks are essential.

Cyber Essentials, the UK government-backed certification scheme, offers a proven solution with 92% reduction in insurance claims and access to lucrative government contracts.



TABLE OF CONTENTS

[The SMB security challenge](#) 02

[Cyber Essentials](#) 04

[Business benefits](#) 05

[TrustLayer One: Built for SMBs](#) 06

[Control your cloud](#) 09

[Train your people](#) 11

[TL;DR:](#) 13

[Cost-benefit analysis](#) 14

[Implementation methodology](#) 16

[Futureproofing and evolution](#) 19

[Your next steps to Cyber Essentials](#) 20

The SMB security challenge

The UK's 5.4 million SMBs represent 99% of all businesses, forming the economic backbone with 16.1 million employees. However, these organisations face unique cybersecurity challenges that make them particularly vulnerable to attack.



Resource & skill constraints

Too few hands on deck

68% of UK SMBs have fewer than three people looking after cybersecurity. That's not a team – it's a vulnerability. And with a third of businesses struggling to hire skilled professionals, that gap isn't closing any time soon.

Zero training, zero chance

Almost 40% of SMBs don't provide any cybersecurity training to staff. That leaves employees wide open to phishing, social engineering, and everyday mistakes. Considering that human error plays a part in 60% of breaches (according to Verizon), it's a costly blind spot.

Not enough budget to budge the needle

Cyber budgets are shrinking, not growing. On average, overall budgets dropped 16% year-on-year, but threats have increased 7%. It's a mismatch: risk is rising, but investment isn't – and attackers know it.



Evolving threat landscape

SMBs are the new sweet spot

SMBs have become the go-to targets for cybercriminals. Why? Weaker defences, fewer resources, and bigger chances of success. 43% of all cyberattacks now hit small businesses – and with automated tools scanning the internet 24/7, it's not a question of if, but when.

Attacks are getting smarter (and cheaper)

AI has changed the game. It's made it easier for even inexperienced attackers to run convincing, damaging campaigns. QR code scams have jumped 1,400% in five years. Deepfakes and impersonation attacks are no longer rare – they're just tools in the modern threat arsenal.

Most SMBs won't recover

The stakes couldn't be higher. 60% of SMBs don't make it past six months after a major cyberattack. Ransomware alone now causes an average of 24 days of downtime. Between rebuilding systems, verifying data, and jumping through compliance hoops, many businesses never fully bounce back.



The challenge is real, and action is overdue

Cyber threats are growing, but most SMBs are working with limited time, stretched teams, and shrinking budgets. That doesn't mean they're ignoring the risks – it means the industry has not made it easy to take action.

Cyber Essentials was designed to change that. It gives businesses a clear, achievable path to stronger security, one step at a time.

Cyber Essentials

Launched in 2014 by the National Cyber Security Centre (NCSC), Cyber Essentials provides a structured approach to cybersecurity through five technical controls designed to prevent approximately 80% of common cyber-attacks.

The Five Core Controls

01 Firewalls & Internet Gateways

Boundary protection preventing unauthorised network access. These systems create barriers between trusted internal networks and potentially hostile external connections.

02 Secure Configuration

Systematic hardening of systems and software to minimise attack surfaces. This includes removing unnecessary software, disabling unused accounts, and implementing strong password policies.

03 User Access Control

Identity management ensuring only authorised personnel access sensitive systems. This encompasses role-based access controls, multi-factor authentication, and regular access reviews.

04 Malware Protection

Comprehensive threat detection and prevention across all systems. Modern solutions must address both signature-based and behavioural threats.

05 Security Update Management

Systematic vulnerability patching and maintenance processes. Critical updates must be applied within 14 days, with automated systems preferred.



Business benefits



Lower insurance costs

Certified organisations are 92% less likely to make a cyber insurance claim. That means lower premiums and better coverage from the start.

Access to government contracts

Certification is a must-have for working with central government, local authorities, and public sector tenders where personal or sensitive data is involved.

Stronger market position

Certification signals credibility. Many organisations now require it from suppliers, and customers are increasingly looking for partners who take security seriously.

Free cyber insurance

UK businesses with under £20 million in turnover receive complimentary cyber liability cover upon certification, giving you added protection without added cost.

TrustLayer One: Built for SMBs

TrustLayer One is a layered security platform designed to help businesses strengthen cyber defences without unnecessary complexity or hidden costs.

It brings together multiple layers of protection—covering email, web access, cloud configurations and user behaviour—into one integrated system. Each layer can be used independently or together, giving organisations the flexibility to scale their protection based on need, risk or compliance objectives.



Architectural Innovation

Layered design

Security needs vary. TrustLayer's modules can be deployed individually or together, allowing businesses to scale protection without unnecessary overhead.

Proxy-free protection

Security should not slow things down. TrustLayer avoids traffic rerouting and keeps performance intact, even as protection scales.

Cloud-native and hybrid-ready

Designed for modern teams working across office, home, and mobile, without the need for complex infrastructure or VPNs.



Each layer plays a specific role in helping SMBs protect their business and improve their Cyber Essentials readiness. Here's how they work in practice.

TrustLayer Mail



Securing email and preventing malware

Email remains the number one attack vector for SMBs, and Cyber Essentials requires organisations to have effective measures in place to prevent malware infections.



Cyber Essentials Control: Malware Protection

This layer helps prevent malware from reaching users via phishing emails, attachments, and malicious links – a core requirement for certification.

TrustLayer Mail delivers layered protection that goes beyond basic filtering to stop sophisticated threats deployed exactly how it works for you – MX mode, M365 connector mode or a mixture of both.

Inline protection

Supports both Microsoft 365 connector integration (no MX record changes) and MX-based routing, ensuring full protection without disrupting mail flow.

Advanced threat detection

Emails are analysed using machine learning models trained on 130+ signals to detect phishing, malware, ransomware, and zero-day exploits.

Impersonation defence

Uses behavioural analysis and executive tracking to identify and stop spear phishing and CEO fraud – a fast-growing threat for small and mid-sized organisations.

Compliance-ready archiving

Tamper-proof email storage with advanced search ensures your records are protected, discoverable, and audit-ready for regulatory and legal requirements.

SecureMail encrypted delivery

Provides end-to-end encrypted messaging via Outlook or a secure web portal, with messages transmitted over TLS to protect sensitive content in transit.



TrustLayer Mail provides detailed threat detection logs and real-time reporting – supporting evidence for Cyber Essentials Plus assessments.

TrustLayer Browse



Controlling access to risky content and cloud applications

Web remains one of the most common attack vectors for SMBs. TrustLayer Browse protects users at point of click by blocking malicious sites, downloads and redirects before they can cause harm.

It also gives IT teams full visibility and control over risky cloud applications, including AI tools, shadow IT and unmanaged SaaS. All without rerouting traffic or slowing down performance.

Real time malware defence

Stops users from accessing known and unknown threats using real-time intelligence, behavioural analysis and SSL inspection.

AI usage protection

Applies policy controls to AI tools, helping prevent sensitive data from being exposed in public prompts.



Cyber Essentials Control: Malware Protection and Secure Configuration

This layer helps stop malware from reaching users through the web and gives IT teams control over which apps can be accessed and how.

Cloud application control

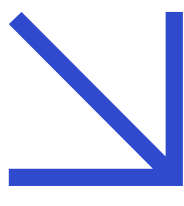
Monitors and restricts use of SaaS apps like Dropbox, ChatGPT and others to reduce risk from shadow IT.

Flexible policy enforcement

Manages browsing rules by user, group or device to support safe access across office, home and remote environments.



TrustLayer Browse supports real world testing of malware protection and browsing controls during Plus assessments, including blocked phishing pages, downloads and AI tools.



Control your cloud. Meet Cyber Essentials.

THE CHALLENGE

Cloud adoption has transformed the way we work – but it's also introduced risk.

Organisations now rely on Microsoft 365, Google Workspace and other SaaS platforms without knowing exactly which apps are in use, or whether approved ones are configured securely.

Under Cyber Essentials, Secure Configuration is critical: all systems and applications must meet defined baselines to reduce attack surfaces and prevent data leakage.

TrustLayer's Cloud Access Security Broker (CASB), as part of TL Browse, gives you complete control over your cloud environment to meet Cyber Essentials' Secure Configuration requirements.

It monitors which cloud apps and services employees are using – from AI tools like ChatGPT and Copilot to file-sharing platforms and other unsanctioned apps – so you can manage adoption, prevent risky usage and protect sensitive data.

With CASB you can:

- Discover and control Shadow IT
- Track and manage access to AI tools and other unsanctioned apps
- Monitor sanctioned apps for misconfigurations
- Enforce policies to block risky or non-compliant applications
- Get instant alerts with clear remediation guidance

THE IMPACT

- ✓ Audit-ready evidence that sanctioned cloud apps meet Cyber Essentials requirements
- ✓ Reduced risk from unsanctioned or insecure applications
- ✓ Greater visibility to identify and address issues before they impact the business
- ✓ Streamlined management with the ability to prioritise and fix issues across all users from one place

THE SOLUTION

TrustLayer Users

↘ **Securing identity and raising awareness**

Cyber attackers often target people, not just systems. Cyber Essentials requires controls that limit unauthorised access and improve user behaviour to reduce risk.



Cyber Essentials Control: Secure Configuration and Access Control

This layer enforces strong user authentication and reduces human error through training and monitoring – core requirements for certification.

TrustLayer Users strengthens the human layer with identity protection and continuous awareness, combining multi-factor authentication, targeted training and behaviour insights.

Integrated MFA

Deploys multi-factor authentication with context-aware checks based on device, behaviour and risk – no infrastructure needed.

Security awareness training

Delivers relevant, engaging training content and phishing simulations delivered to user's inbox on a cadence of your choosing.

User behaviour analytics

Identifies unusual or high-risk behaviour, flagging signs of account compromise or insider threats.

Policy consistency

Applies and enforces security policies across access, training and identity settings to ensure consistent protection.



TrustLayer Users provides audit trails and user-level reporting to support Cyber Essentials Plus evidence requirements.

Train your people. Meet Cyber Essentials.

THE CHALLENGE

Human error remains one of the biggest security risks. Phishing, social engineering and poor security habits can bypass even the most advanced technical defences.

Cyber Essentials' User Access Control requires that users not only have the right access levels but also the awareness to spot and avoid threats.

Without structured, continuous training, organisations struggle to reduce risky behaviour and prove compliance.

TrustLayer's Security Awareness Training (SAT), as part of TL Users, builds a resilient human layer by embedding security knowledge and behaviours into daily routines.

With SAT you can:

- Run targeted phishing simulations to test and educate users
- Deliver bite-sized training content tailored to specific risks
- Track progress and identify high-risk individuals or teams
- Provide evidence of user training for Cyber Essentials audits

THE SOLUTION

THE IMPACT

- ✓ Audit-ready evidence that user training meets Cyber Essentials requirements
- ✓ Reduced risk from phishing, social engineering and unsafe practices
- ✓ Greater visibility to identify and address risky behaviours before they lead to incidents
- ✓ Streamlined delivery and tracking of training across all users from one platform

TrustLayer Posture

↘ Automating secure configuration and patch visibility

Maintaining secure cloud configurations and keeping systems up to date are critical for Cyber Essentials, but manual checks are time-consuming and inconsistent.

TrustLayer Posture gives you continuous visibility across Microsoft 365, Google Workspace and Azure, instantly flagging misconfigurations and missing patches with clear guidance to fix them – all mapped to global standards and frameworks like Cyber Essentials and ISO 27001.

Unified posture visibility

Connects to Microsoft 365, Azure, Google Workspace and others to monitor security settings and configuration drift across your stack.

Update and version monitoring

Identifies unsupported software and missing patches so your team can act quickly and stay compliant.

✓ Cyber Essentials Control: Secure Configuration & Security Update Management

This layer helps enforce secure cloud settings and detect missing updates across SaaS and cloud environments – both key requirements for certification.

Exportable reports for evidence

Downloadable summaries show your configuration and update status at a glance, ready for internal review or external audit.

Secure configuration checks

Surfaces risks like legacy authentication, inactive accounts, excessive permissions and public file sharing.

- + TrustLayer Posture provides real-time evidence of your cloud configuration and patch status, helping you pass device-level and configuration checks during a Cyber Essentials Plus assessment.

TL;DR:

What do I need for Cyber Essentials?

Five key security controls:

1. Firewalls & Internet Gateways
2. Secure configuration
3. User Access Control
4. Malware protection
5. Security update management

These are the baseline for certification – and the foundation of good cybersecurity hygiene.

How does TrustLayer help me achieve it?

Control	Layers involved	Key features
Firewalls	TL Browse TL Posture	• Block risky domains and apps • Detect misconfigured cloud infrastructure (Azure, AWS, Google) • Monitor and control network ingress/egress
Secure Configuration	TL Posture TL Users TL Browse	• M365, Google Workspace and AWS misconfig alerts • Control and monitor Shadow IT usage via CASB • Enforce secure settings and remove unused accounts
User Access Control	TL Users TL Posture	• Adaptive MFA with context-aware authentication • Role-based access control and regular access reviews • Security awareness training and phishing simulations
Malware Protection	TL Mail TL Browse TL Users	• 130+ detection signals in Mail for phishing, malware, ransomware and zero-day exploits • Real-time web threat scanning and blocking • SSL inspection with safe search enforcement • User training to avoid malware threats
Security Update Mgmt	TL Posture TL Browse	• Auto-alerts on patch status for M365, Google Workspace and AWS • Block outdated browsers or device operating systems • Auto-alerts on outdated or insecure settings across TrustLayer One solutions

Cost-benefit analysis



Cutting costs without cutting corners

Cyber Essentials certification is a smart investment—but how you get there matters. Traditional approaches often rely on a patchwork of point solutions, each with their own price tag, integration headaches and maintenance burden. TrustLayer simplifies the journey and slashes the true cost of cyber readiness.

Security Layer	Average traditional vendor		TrustLayer	Monthly Savings
TL Email	Email security	£3.50/user	£2.45/user	£3.55/user
	Archiving	£2.50/user		
TL Users	Security Training	£2.50/user	£2.30/user	£1.20/user
	MFA	£1.00/user		
TL Web	Web Security	£4.20/user	£5.75/user	£10.45/user
	CASB & AI Risk Management	£12.00/user		
TL Posture	CSPM/SSPM	£12.00/user	£500/ connector	£11.00/user
Total monthly costs:		£29.70/user	£11.50/user	£26.20/user

Annual Savings

For a 500-user organisation, TrustLayer delivers over £100,000 in direct cost savings annually. This is without additional discounts included, or the cost of integrating and deploying multiple products.

→ Hidden Cost Elimination

Management complexity

Traditional multi-vendor approaches require coordination between multiple dashboards, APIs, and support teams. TrustLayer's layered platform eliminates these operational overheads.

Integration costs

Point solutions often require expensive custom integrations and ongoing maintenance. TrustLayer's native integration eliminates these hidden expenses.

Compliance overhead

Manual compliance management consumes significant IT resources. TrustLayer's automated compliance monitoring reduces these costs and frees up time

→ Return on Investment

Breach cost avoidance

With average breach costs for SMBs reaching £7,960, TrustLayer delivers rapid return on investment by significantly reducing risk and resource strain.

Customers report a 53% reduction in overall threats, 23% of IT team time reclaimed, and a 33% improvement in end user experience – including fewer security workarounds and support headaches.

Productivity gains

Simplified security management frees IT resources for business-enabling activities rather than reactive security tasks.

Business enablement

Cyber Essentials certification unlocks access to government contracts, potentially worth millions in new revenue.

Implementation methodology



TrustLayer's deployment methodology ensures rapid implementation while minimising business disruption through a phased approach.

01

Phase 1: Assessment and Preparation

Security Posture Assessment

Comprehensive evaluation of current cybersecurity, identifying gaps against Cyber Essentials requirements. This baseline establishes implementation priorities and resource requirements.

Infrastructure Analysis

Review of existing IT infrastructure, cloud services, and user environments to optimise TrustLayer module selection and configuration.

Risk Prioritisation

Classification of identified vulnerabilities by business impact and remediation complexity, ensuring critical issues receive immediate attention.



Phase 2: Core Security Deployment

02



Email security implementation

TL Mail deployment through Microsoft 365 transport connectors, or via MX record changes providing immediate protection against email-borne threats. Policy configuration aligned with organisational requirements and compliance mandates.

Web protection activation

TL Browse implementation using an agent-based deployment. Initial policy setup focuses on malware blocking and enhanced web filtering with out-of-the-box policies.

03

Phase 3: Advanced Capabilities

Posture management integration

TL Posture deployment for continuous compliance monitoring and vulnerability management of your cloud infrastructure. Baseline establishment and automated alerting configuration.

Identity security enhancement

TL Users rollout including MFA deployment and security awareness training program launch. User onboarding with pre-planned training modules.

Policy refinement

Fine-tuning of security policies based on initial deployment experience and user feedback.

04

Phase 4: Certification Achievement

Compliance validation

Automated compliance checking across your cloud infrastructure for the relevant Cyber Essentials controls.

Evidence collection

Report generation to support certification submission, leveraging automated reporting capabilities.



Futureproofing and evolution



Adapts to modern threats

TrustLayer is built to keep pace with how threats evolve. Its cloud-native architecture scales effortlessly as your organisation grows, and its protection stays current without disruption or manual intervention.

Smarter, faster defence

Machine learning models update continuously using global threat intelligence, helping detect new attacks before they cause damage. Behavioural analytics and customer-wide intelligence sharing provide additional layers of insight against unknown threats and insider risks.

Compliance that moves with you

TrustLayer supports multiple compliance frameworks and automatically aligns with changing standards. Audit-ready reporting, automated policy updates and flexible integrations make it easy to stay secure and certification-ready as requirements shift.

- + As new tests and threat vectors are added to Plus assessments, TrustLayer's automated alignment and reporting features help ensure you're ready – without last-minute scrambles or tool changes.

Your next step to Cyber Essentials



Cyber Essentials: done right, done once

Achieving Cyber Essentials is more than a box to tick. It shows customers, partners and regulators that security is built into the way you work. It sets the stage for Cyber Essentials Plus and more advanced frameworks like ISO 27001 or SOC 2, giving you the credibility and technical foundation to reach higher standards. For SMBs, it can be the difference between being considered and being left out.

Everything you need, in one platform

TrustLayer gives you unified coverage across the five Cyber Essentials controls – from stopping malware and securing devices to enforcing MFA and managing cloud access. No stitched-together tools. No conflicting policies. No lost time.

- Save up to £1000s a year versus traditional multi-vendor setups
- Accelerate your timeline for certification and Cyber Essentials Plus
- Reduce overhead with automated compliance monitoring and reporting
- Stay ahead with protection that evolves as threats and standards change

Compliance is just the beginning

Cyber Essentials is a milestone – but the real goal is lasting resilience. TrustLayer helps you go further, embedding security into every layer of your business without slowing you down. It's fast to deploy, simple to run, and ready to grow with you.



Ready to start?

Whether you're preparing for your first Cyber Essentials audit or upgrading to Plus, TrustLayer gives you a direct route – and long-term confidence.

Get in touch to discover more:

