PEN PROTECT

YOUR CYBER PROTECTION PLATFORM

Pen underwriting

penunderwriting.co.uk

WELCOME TO
PEN PROTECT

Pen Protect is a cyber protection platform available to Pen cyber policyholders. It's included as standard with all Pen Underwriting cyber insurance policies.

Through Pen Protect, you'll have access to sophisticated yet user-friendly cyber risk management through a variety of cybersecurity tools and services all in one place.

Real cyber risk insights in real time

Pen Protect provides real-time insights into your cyber risks, detecting vulnerabilities and actionable steps for effective remediation. The platform also includes advanced phishing simulation technology and an inbox defender, addressing the top cyber exposure risk — the human element.

This guide explains the tools and services offered by Pen Protect that can help your organisation bolster its cyber defences in today's challenging cyber risk landscape.

127 The average number of **new vulnerabilities** Pen Protect detects **every day**.

Source: Internal data collected between 01 Jan 2025-03 Mar 2025.

PEN PROTECT TOOLS AND SERVICES

1 Vulnerability scanning
Daily boundary scanning, identifying cyber vulnerabilities as they are released, with remediation steps.

2 Threat intelligence
Integrating with threat intelligence feeds, Pen Protect can provide context about emerging threats and how they might impact your organisation.

3 Personalised training
Engaging, multi-format cyber educational content, including micro-trainings, flashcards, videos and quizzes.

4 Inbox defender
An email plugin instantly helps to identify red flags and stop upcoming email attacks.

5 Phishing simulations
Simulated attacks across multiple channels — not just email — including SMS, Slack, Teams, WhatsApp and phone calls.

6 Always on support
An AI-powered tool offering support to manage cybersecurity strategies, backed by the expertise of a team of specialist humans.

CONTINUOUS VULNERABILITY SCANNING

Stay ahead of the cyber risks to your organisation

Pen Protect's continuous vulnerability scan primarily focuses on external-facing systems and networks. It evaluates your organisation's internet-facing assets to identify potential vulnerabilities and security weaknesses that could be exploited by attackers.

Common Vulnerabilities and Exposures (CVE)

- A standardised system for identifying and cataloguing publicly known cybersecurity vulnerabilities.
- Each vulnerability is assigned a unique identifier to facilitate information sharing and management.

Common Vulnerability Scoring System (CVSS)

- A framework used to assess the severity of security vulnerabilities.
- Provides a numerical score reflecting the potential impact and exploitability of a vulnerability.
- Helps your organisation prioritise your response efforts.

Exploit Prediction Scoring System (EPSS)

- A model designed to estimate the likelihood of a vulnerability being exploited in the wild.
- Offers additional context to CVSS scores by focusing on the probability of real-world exploitation.
- Aids in more effective risk management and prioritisation.

Our seven-step process to identify your systems' vulnerabilities

1 **Asset discovery:** The continuous vulnerability scanner first identifies all the systems and applications within the external network that need to be assessed.

2 **Vulnerability database update:** The continuous vulnerability scanner updates its database with the latest CVEs. CVEs are publicly disclosed security vulnerabilities, each with a unique identifier.

3 **Scanning:** The continuous vulnerability scanner probes the identified assets to detect vulnerabilities. It does this by sending requests to systems and analysing responses to identify potential weaknesses. The scanner looks for specific patterns or signatures that match known CVEs.

4 **Analysis:** The scanner compares the gathered data against its database of CVEs. It checks for known vulnerabilities based on software versions, configurations and other indicators.

5 **Reporting:** Once the scan is complete, the tool generates a report detailing the vulnerabilities found. This report includes the CVE identifiers, descriptions of the vulnerabilities, their severity levels and recommendations for remediation. The scans will be sent to you via email.

6 **Remediation:** Based on the vulnerabilities, the platform provides a remediation script (if it is available).

7 **Continuous rescanning:** Follow-up scans are conducted at a frequency you decide. It's essential to scan frequently to ensure that vulnerabilities have been effectively addressed and no new issues have arisen.

ACTIVATE PEN PROTECT >

ONGOING DEFENCE AND LIVE THREAT INTELLIGENCE

Identify emerging threats in real-time

Pen Protect is continually monitoring threat intelligence to stay ahead of new and evolving cyber risks to help stop threats in their tracks.

Threat intelligence integration

By integrating with threat intelligence feeds, Pen Protect can provide context about emerging threats and how they might impact your organisations. This helps you understand the likelihood and potential impact of different cyberthreats.

Risk scoring

Pen Protect assigns a risk score to each insured based on the findings from the assessments. This score reflects the overall cybersecurity health of your organisation and helps Pen Underwriting understand the level of risk.

Regular threat information

Pen Protect ensures that all our cyber policyholders are informed about the latest cyber claims information through newsletters and online portals. We think it's important to stay vigilant against cyberthreats by sharing insights on emerging risks and trends in cybersecurity. You'll receive guidance on best practices to enhance your cyber defences, such as implementing strong passwords and regular software updates.

ACTIVATE PEN PROTECT >

PERSONALISED AND ENGAGING CYBERSECURITY TRAINING

Equip your people to become threat barriers

The human factor is the biggest cyber risk organisations face, with threat actors waiting to take advantage of employee errors and behaviours. Pen Protect adds a new level to your employee cybersecurity training through a personalised and consistent approach.

Simplify compliance

Effortlessly meet regulatory requirements with 200-plus pre-built training modules and automated compliance reporting.

Personalised training paths

AI generates tailored, adaptive learning experiences for every employee based on their risk profile, role, industry and behaviour patterns.

Training variety

Deliver engaging, multiformat content, including micro-trainings, flashcards, videos and quizzes.

Gamified learning and engagement

Motivate employees with points, badges and rewards that turn training into an engaging, interactive experience, fostering long-term behavioural change.

Empower with Cyber Defence Centre's AI Assistant

Boost participation and retention with real-time behavioural nudges directly in Teams and Slack.

Behavioural insights and nudges

Leverage AI-driven analytics to detect risk patterns and deliver targeted nudges, ensuring employees continuously improve their security behaviours.

ACTIVATE PEN PROTECT ❯

INBOX DEFENDER AND PHISHING SIMULATIONS

Prevent social engineering attacks through early intervention

Make sure your employees can detect threat signals to avoid social engineering attacks. From suspicious domains to data leaks, Pen Protect's email plugin instantly helps to identify red flags and stop upcoming attacks across Gmail and Outlook.

Phishing reporting

Allows your employees to report suspicious emails directly from Outlook or Gmail with just one click.

Email analysis and red flag detection

AI scans your reported emails for phishing indicators and highlights the risks.

Automated user feedback

Provides instant explanations as to why an email is identified as safe or dangerous.

Phishing simulation integration

Tracks your users interactions with simulated attacks to reinforce their training.

Multi-channel simulations

Simulate attacks across multiple channels — not just email — including SMS, Slack, Teams, WhatsApp and phone calls.

Diverse and sophisticated attack types

Test resilience with AI-powered attacks like phishing pages, deepfakes, QR code phishing, BEC, malware, spoofing and more.

Hyper-realistic scenarios

Build resilience with lifelike attack scenarios tailored to industry-specific threats and the latest phishing trends.

ACTIVATE PEN PROTECT >

ALWAYS-ON SUPPORT

Real-time AI guidance backed by expert humans

Pen Protect includes Virtual Chief Information Security Officer (VCISO) support. An AI-powered tool helps you manage your cybersecurity strategies, providing guidance and recommending best practices. The chatbot VCISO gives real-time support and advice backed by a team of human cybersecurity experts.

AI Assistant for employees

A 24/7 security copilot integrated into Microsoft Teams and Slack, delivering tailored training, answering questions and providing compliance guidance aligned with your organisation's policies and procedures.

ACTIVATE PEN PROTECT ❯

ACTIVATE PEN PROTECT

Access to Pen Protect is included as standard with all Pen Underwriting cyber insurance policies.

To give you a sense of the value it offers — beyond the ongoing cyber protection it provides — take a look at the table below to see what your organisation might pay per employee for the equivalent cyber protection tools and services.

Security tools £/employee (annual)	Market pricing
Vulnerability monitoring	**£17**
Threat intelligence	**£12**
Inbox defender (email security)	**£34**
Security training & phishing sims	**£32**
Always on support (ask the expert)	**£12**
Typical cost per employee	**£107**

Estimated savings by company size	
10-employee organisation	**£1,070** per year
25-employee organisation	**£2,675** per year
100-employee organisation	**£10,700** per year
250-employee organisation	**£26,750** per year

You can activate Pen Protect and your cyber protection tools by scanning the QR code, clicking the link below or visiting penprotect.ai.

ACTIVATE PEN PROTECT >

Pen
underwriting

www.penunderwriting.co.uk