

cymplify

Active Cyber Risk Management Platform
Overview



If Cybercrime were a country, it would have the worlds **3rd largest economy.**

As the number of Attackers dramatically increases, and the focus of those Attackers continues to shift away from large Enterprise Organisations toward less secure and more exposed Small and Mid Sized (SME) Organisations that make up over 95% of all businesses across the globe, Cyber is now the **#1 Risk** to global business
(* Allianz Risk Barometer 2022)

Accelerated by the CoVid 19 Pandemic, threats such as Ransomware, Fraud, Extortion and Data Theft all form part of a global Cybercrime Pandemic generating an estimated \$6 Trillion per year in 2021, increasing to over \$11 Trillion by 2025.

SME Boards and Business Leaders **urgently need** a powerful, practical, affordable, easy to use and continuous solution for Cyber Risk Management - built for today's threats , using the same tools and techniques as today's attackers - to confidently address the growing Cyber Threat.

Welcome to Cymplify...

We Help Stop Attacks on Your Business

What is it?


Our cloud native platform is purpose built from the ground up to meet the specific needs of SME businesses.

The Cymplify platform provides any business with the tools they need to confidently and continuously address Cyber Risk - all in one place.

Using a holistic and proactive approach, your licence provide access to a powerful yet easy to use suite of solutions that bring together the all important **Three Pillars of Cyber Security:**

A teal double-line icon consisting of two parallel diagonal lines.

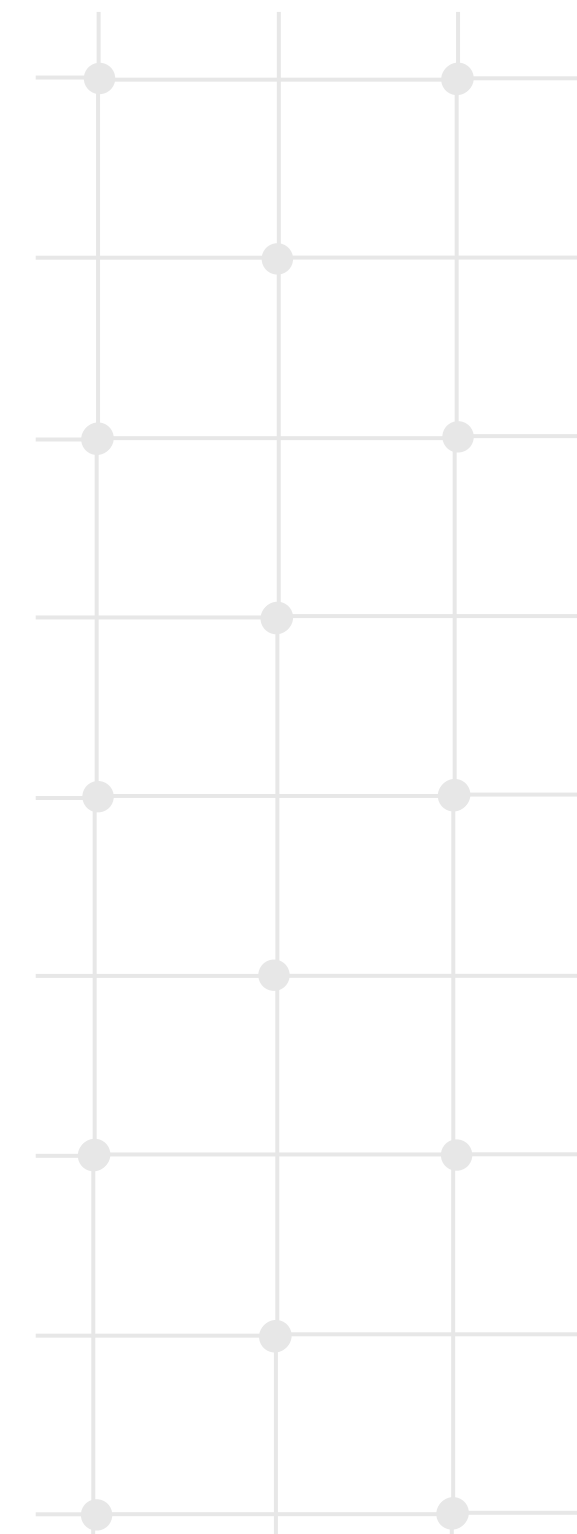
Technology

A magenta double-line icon consisting of two parallel diagonal lines.

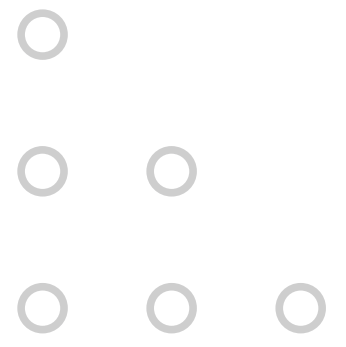
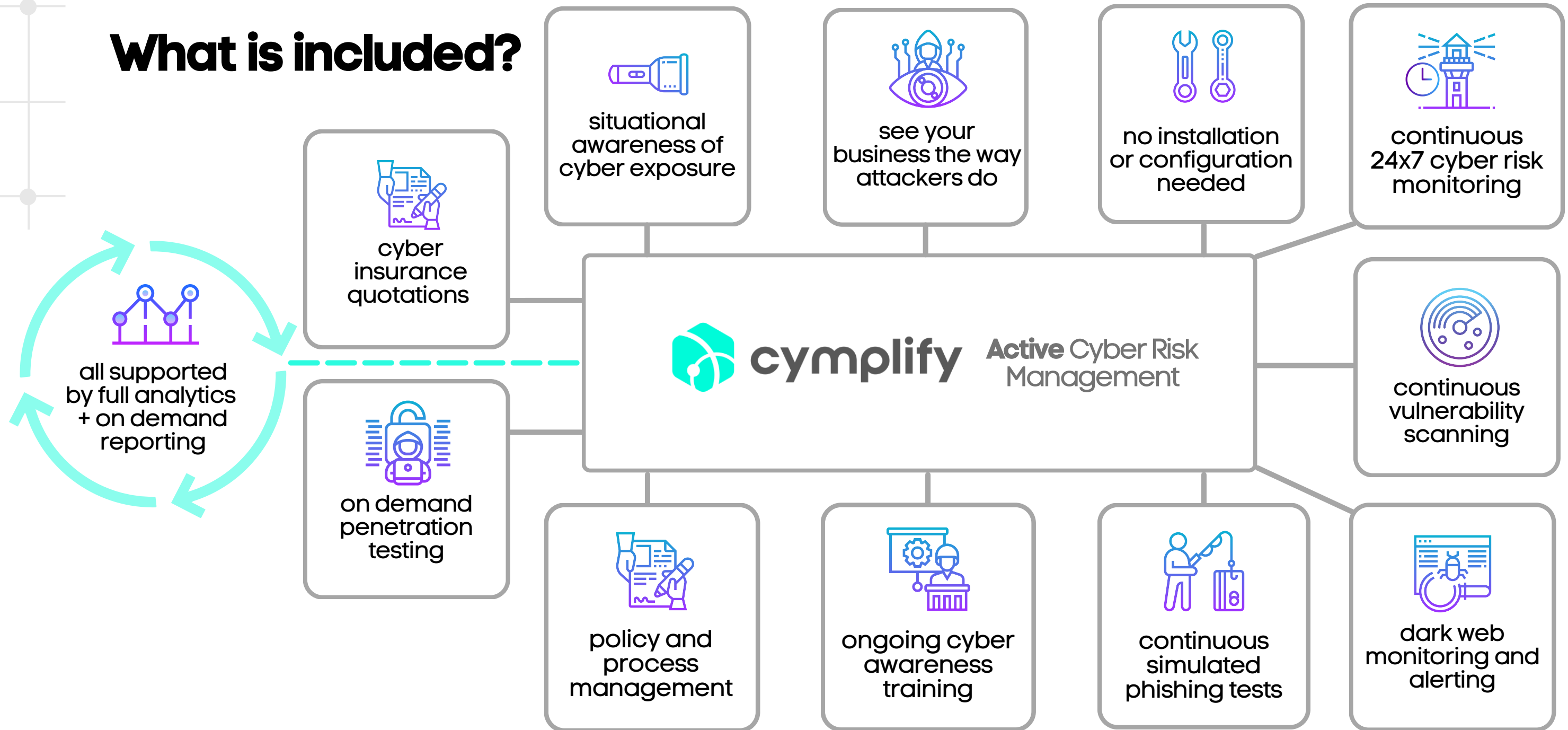
People

A grey double-line icon consisting of two parallel diagonal lines.

Process



What is included?



Example Dashboards

Active Cyber Risk Management Platform



cymplify

- Home
- Cyber Risk
- Dark Web
- Penetration Testing
- Cyber Training
- Phishing Simulator
- Policy Hub
- Cyber Insurance
- Report Generator

Cyber Risk Exposure

Top 3 Critical Risks

- 1 Close public TeamViewer access to your organisation
- 2 Close public access to database services
- 3 Close all developer access on external services

Dark Web Exposure

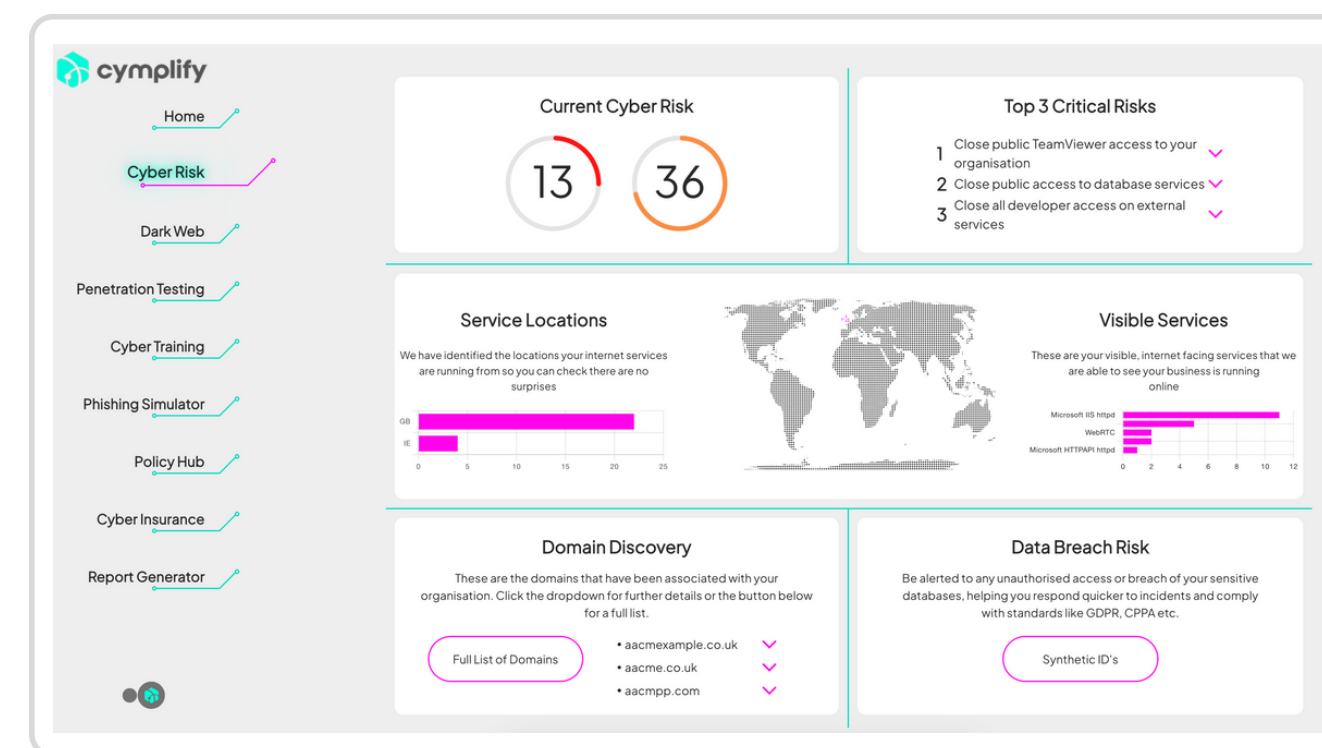
Penetration Test Data

Access Test Report

Cyber Awareness

Compliance Hub

Unviewed %
Viewed %
Signed %



cymplify

- Home
- Cyber Risk
- Dark Web
- Penetration Testing
- Cyber Training
- Phishing Simulator
- Policy Hub
- Cyber Insurance
- Report Generator

Current Cyber Risk

13 36

Top 3 Critical Risks

- 1 Close public TeamViewer access to your organisation
- 2 Close public access to database services
- 3 Close all developer access on external services

Service Locations

We have identified the locations your internet services are running from so you can check there are no surprises

Visible Services

These are your visible, internet facing services that we are able to see your business is running online

Microsoft 365 Intpd
WebRTC
Microsoft HTTPAPI Intpd

Domain Discovery

These are the domains that have been associated with your organisation. Click the dropdown for further details or the button below for a full list.

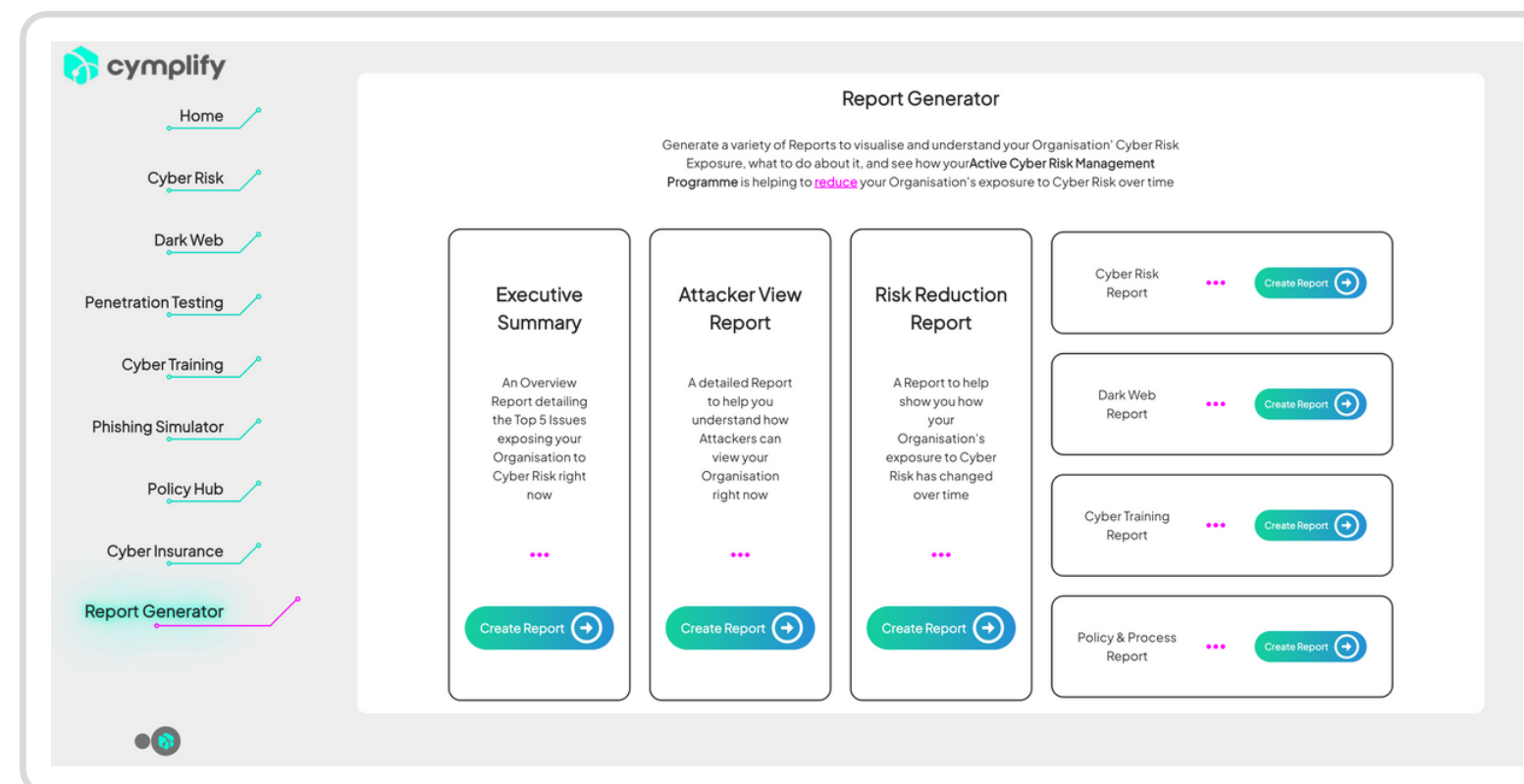
Full List of Domains

- aacmexample.co.uk
- aacme.co.uk
- aacmcp.com

Data Breach Risk

Be alerted to any unauthorised access or breach of your sensitive databases, helping you respond quicker to incidents and comply with standards like GDPR, CPPA etc.

Synthetic ID's



cymplify

- Home
- Cyber Risk
- Dark Web
- Penetration Testing
- Cyber Training
- Phishing Simulator
- Policy Hub
- Cyber Insurance
- Report Generator

Report Generator

Generate a variety of Reports to visualise and understand your Organisation's Cyber Risk Exposure, what to do about it, and see how your Active Cyber Risk Management Programme is helping to reduce your Organisation's exposure to Cyber Risk over time

Executive Summary

An Overview Report detailing the Top 5 Issues exposing your Organisation to Cyber Risk right now

Create Report

Attacker View Report

A detailed Report to help you understand how Attackers can view your Organisation right now

Create Report

Risk Reduction Report

A Report to help show you how your Organisation's exposure to Cyber Risk has changed over time

Create Report

Cyber Risk Report

Create Report

Dark Web Report

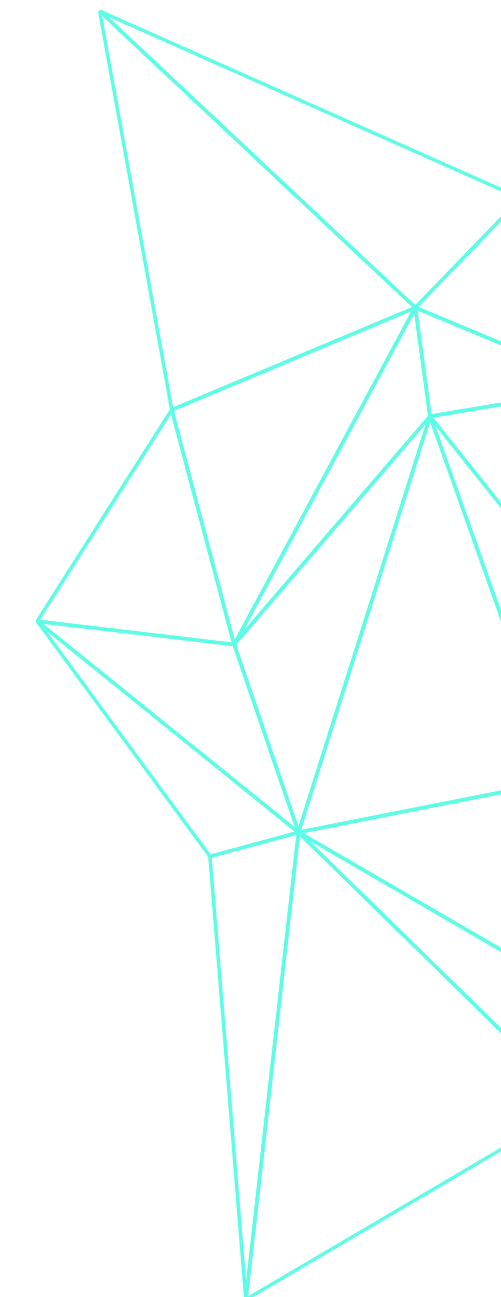
Create Report

Cyber Training Report

Create Report

Policy & Process Report

Create Report



Real Time Cyber Risk Exposure Visibility and Control



Immediate visibility of a wide range of Cyber Risk Insights

The dashboard shows a 'Current Cyber Risk' section with two gauges: one at 13 (red) and one at 36 (orange). Below this are 'Service Locations' with a world map and 'Visible Services' with a bar chart. A 'Domain Discovery' section lists domains like aacmexample.co.uk and aacmcp.com. A 'Data Breach Risk' section has a 'Synthetic ID's' button.

Uncover and understand High Risk Issues - what they are, where they are and what to do

A grid of risk issues, each with a red warning icon and a 'READ MORE' link. Issues include 'Vulnerable services', 'Email spoofing policy', and 'Email sender protection'.

Drill down into each specific issue for full details, description of potential impacts and advice on how to fix it

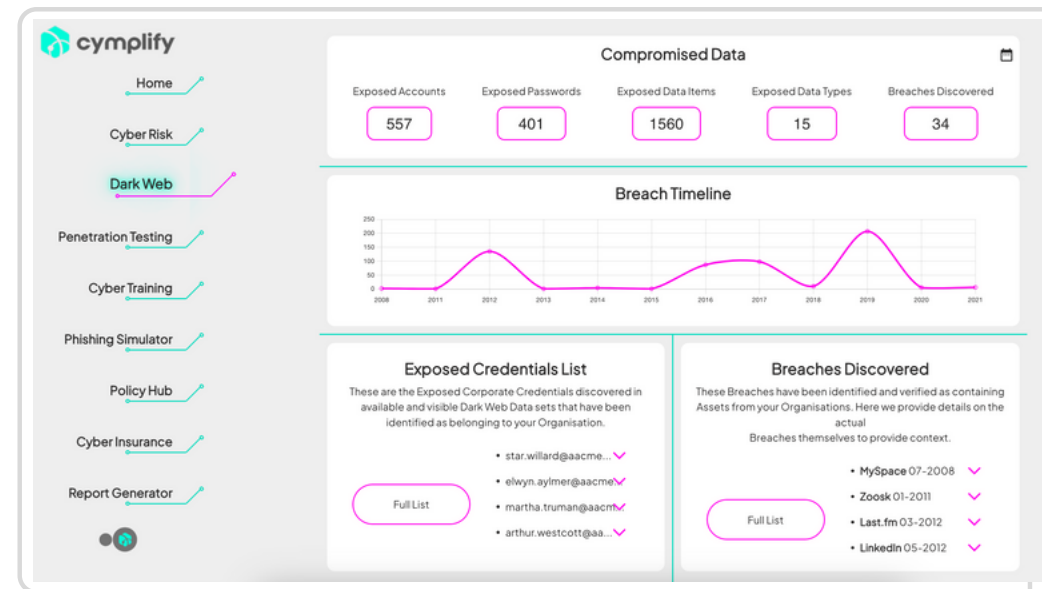
A detailed view of a 'Vulnerable services' issue. It describes an OpenSSH 8.2p1 Ubuntu-4ubuntu0.3 vulnerability and provides instructions on how to resolve it by updating the software.

+ Email Alerts when new Exposures are detected

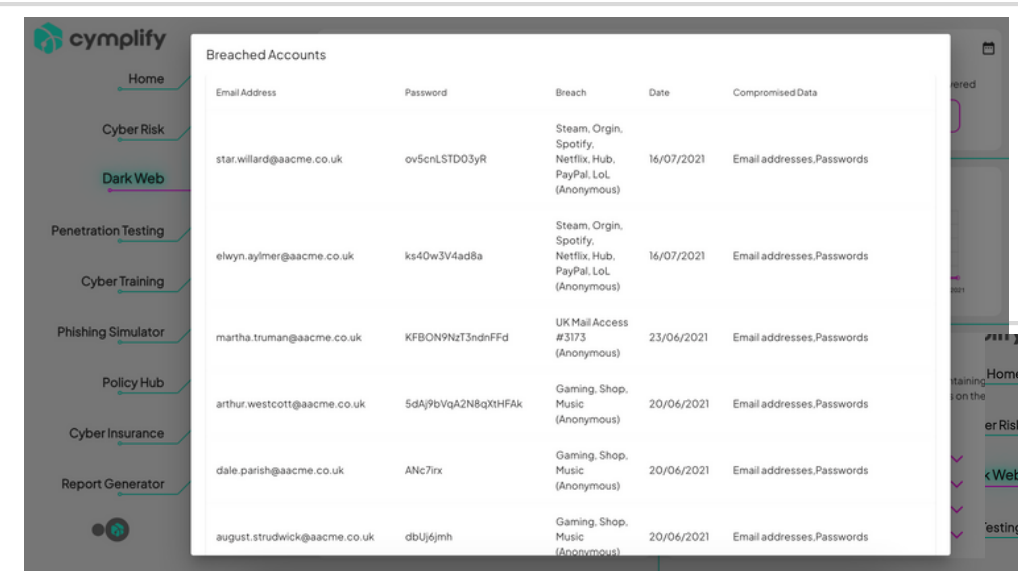
An email alert with the subject 'New Cyber Risk Discovered'. It features the Cymplify logo and a red 'Alert!' button. The main text states: 'Cymplify has detected the following new Cyber Risk: Out of date software. Microsoft IIS httpd 10.0 is an older version of this product. This service is using port 80 on IP address 52.97.202.120. Newer versions of products become available to ensure any bugs or vulnerabilities are fixed to maintain maximum security. The older the version, the more vulnerabilities it is likely to have. Older versions of services are less well-supported by the developer, making an organisation more vulnerable to cyber attacks and service failure. What should you do? To maintain optimum security and prevent cyber attacks, a more recent version of this product may be preferable. Refer to the Microsoft IIS httpd website for more detail. Additionally, we're always happy to have a chat to explain any additional queries you have, or to walk you through the required steps. Please log in to the Cymplify platform for more information.'

Dark Web Breach Exposure Visibility and Insight

Immediate visibility of all Corporate Credentials exposed in existing Breach Data on the Dark Web

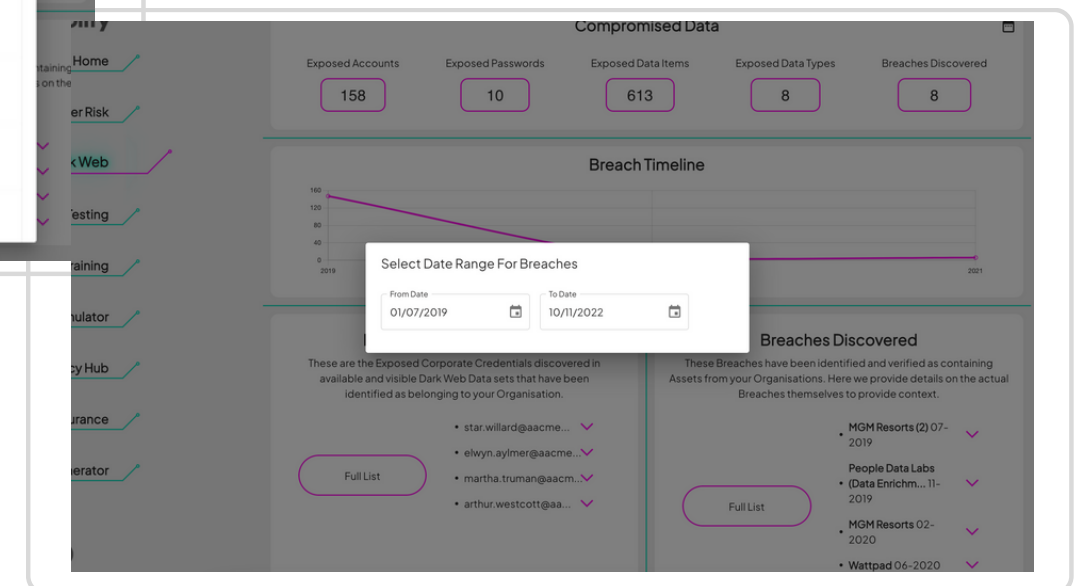


Drill down into your exposure in Dark Web Breach Data - including exposed credentials, passwords, the specific breaches you have been involved in and details of over 100 different Data types

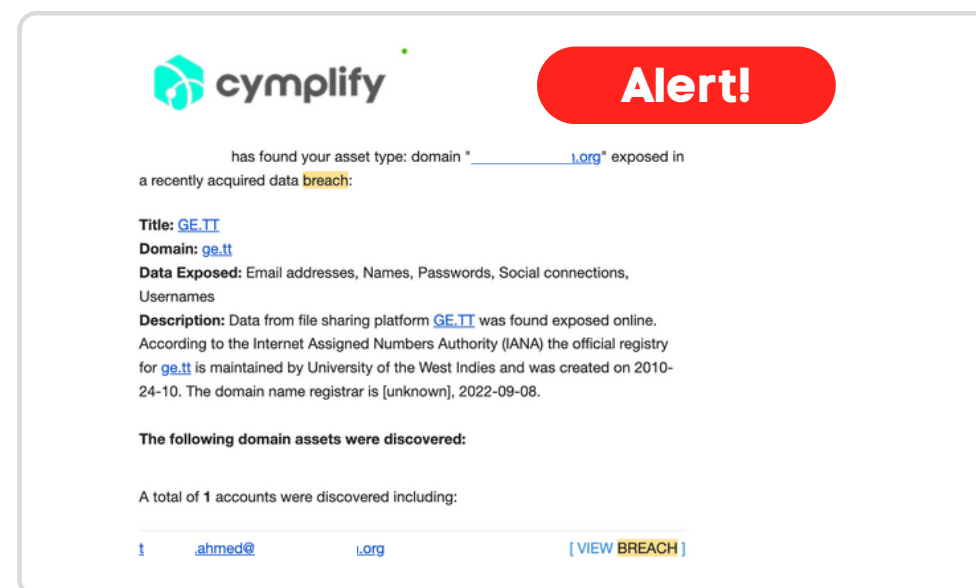


Email Address	Password	Breach	Date	Compromised Data
star.willard@aacme.co.uk	ov5cnLSTD03yR	Steam, Origin, Spotify, Netflix, Hub, PayPal, LOL, (Anonymous)	16/07/2021	Email addresses, Passwords
elwyn.aymer@aacme.co.uk	ks40w3V4ad8a	Steam, Origin, Spotify, Netflix, Hub, PayPal, LOL, (Anonymous)	16/07/2021	Email addresses, Passwords
martha.truman@aacme.co.uk	KFBON9NzT3dnrFfd	UK Mail Access #3173 (Anonymous)	23/06/2021	Email addresses, Passwords
arthur.westcott@aacme.co.uk	SdA9bvQ42N8qXHfAK	Gaming, Shop, Music (Anonymous)	20/06/2021	Email addresses, Passwords
dale.parish@aacme.co.uk	ANc7ix	Gaming, Shop, Music (Anonymous)	20/06/2021	Email addresses, Passwords
august.studwick@aacme.co.uk	dbUj6jmh	Gaming, Shop, Music (Anonymous)	20/06/2021	Email addresses, Passwords

Refine date range on Breach Exposure information - to see all, some or most recent exposure - or exposure during a specific time period



+ Email Alerts when new Breach Exposure is detected



Alert!

has found your asset type: domain "* .l.org" exposed in a recently acquired data breach:

Title: [GE.TI](#)
Domain: [ge.tt](#)
Data Exposed: Email addresses, Names, Passwords, Social connections, Usernames
Description: Data from file sharing platform [GE.TI](#) was found exposed online. According to the Internet Assigned Numbers Authority (IANA) the official registry for [ge.tt](#) is maintained by University of the West Indies and was created on 2010-24-10. The domain name registrar is [unknown], 2022-09-08.

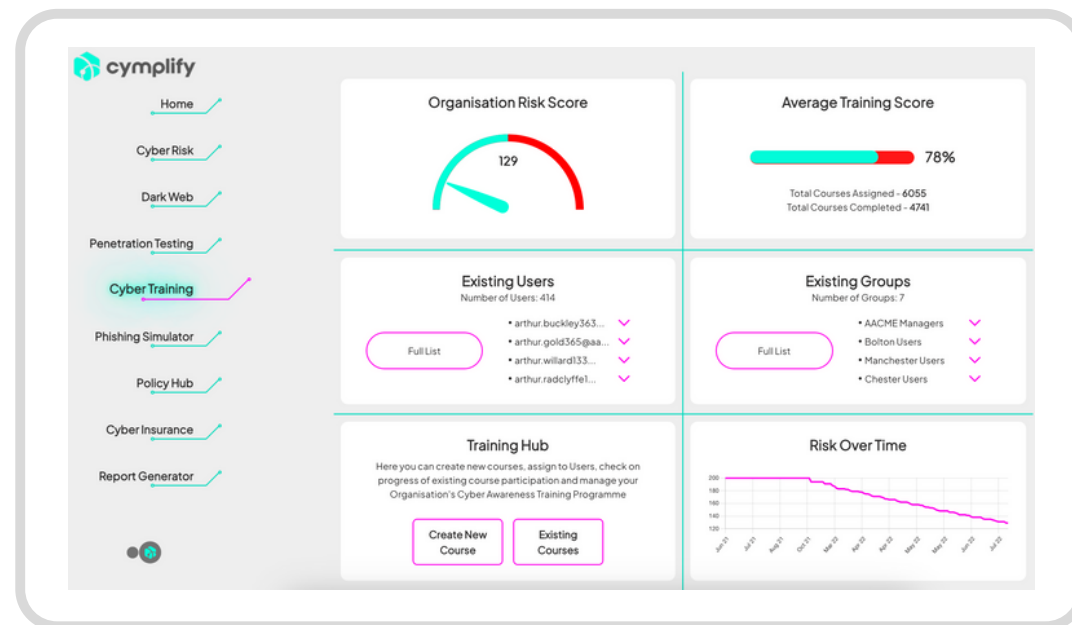
The following domain assets were discovered:

A total of 1 accounts were discovered including:

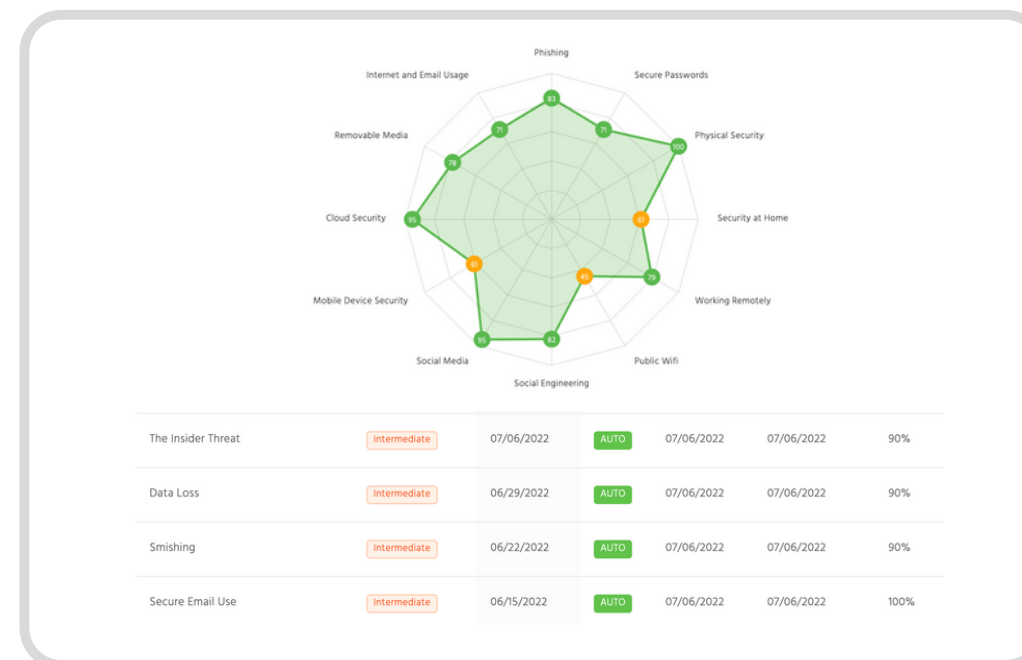
1 [ahmed@ .l.org](#) [\[VIEW BREACH\]](#)

Ongoing Cyber Awareness Training & Simulated Phishing Programmes

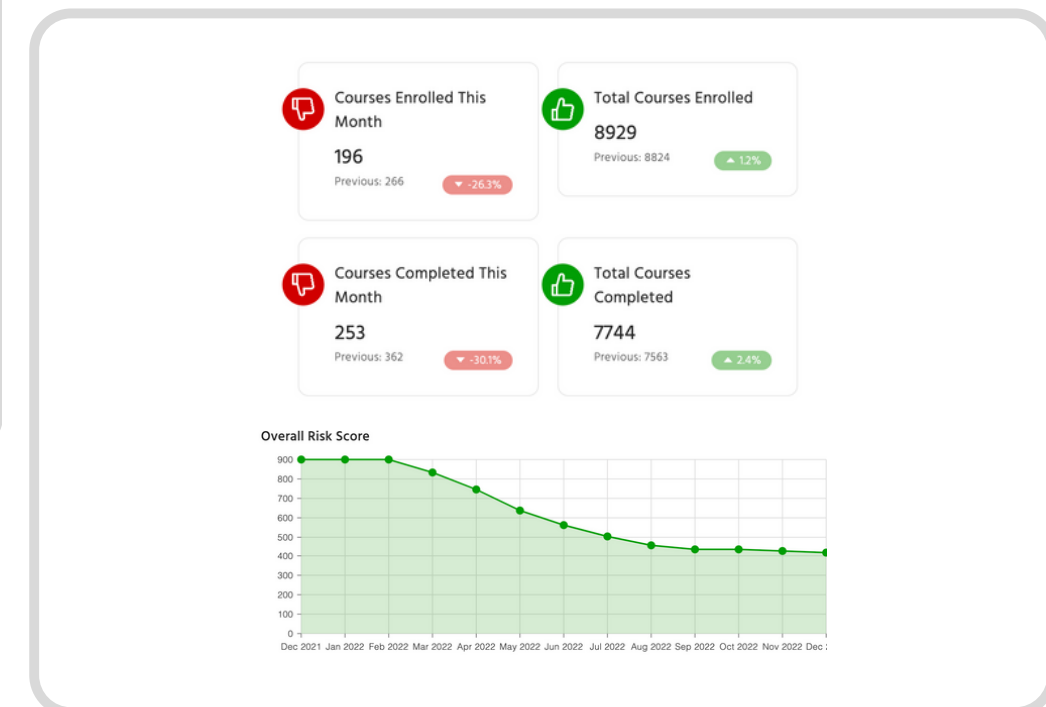
Centralised control of Cyber Awareness Training Programme



All Users receive initial Gap Analysis questionnaire, with subsequent training auto delivered based on individual training needs analysis

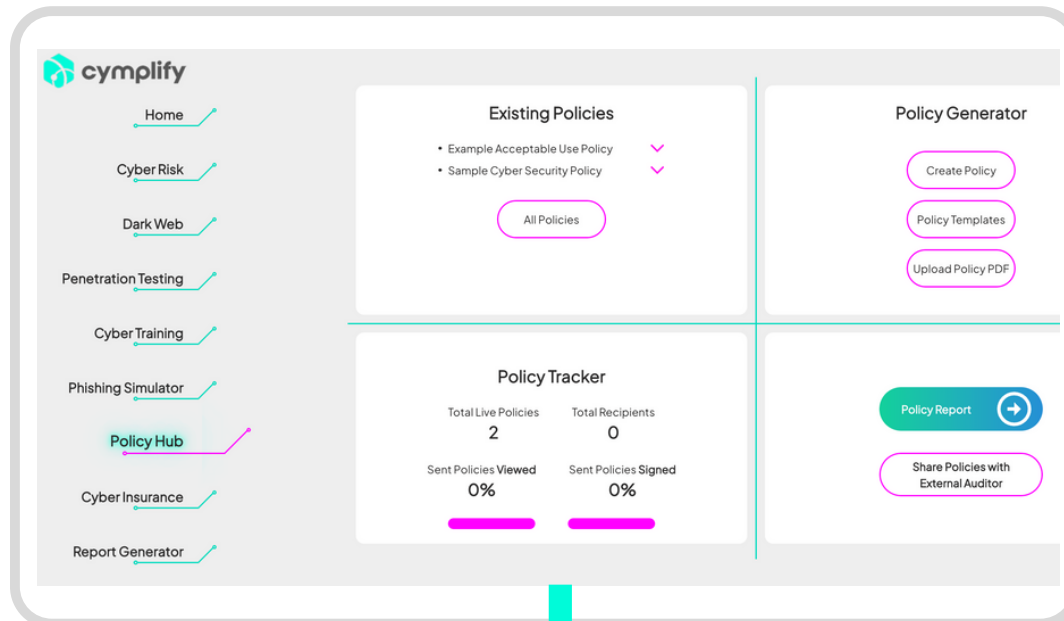


Drill down into Group or Individual User performance in specific scenarios or over time



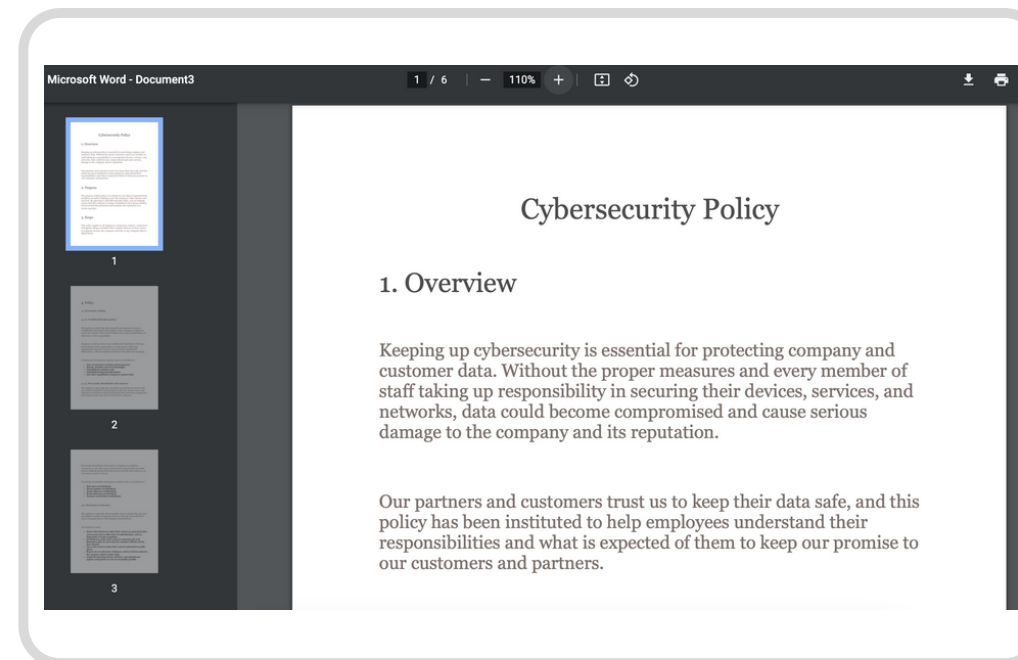
Centralised Policy and Process Management Hub

Centralised Policy Management, Policy creation, send and track views and acceptance across the organisation



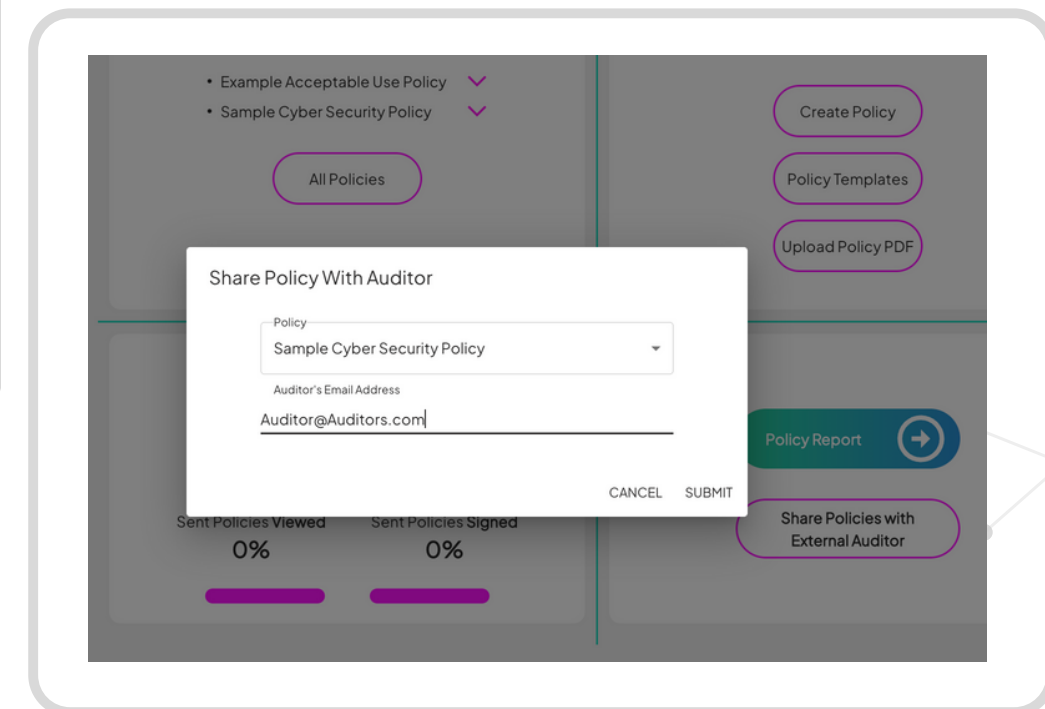
The dashboard shows a sidebar with navigation links: Home, Cyber Risk, Dark Web, Penetration Testing, Cyber Training, Phishing Simulator, Policy Hub (highlighted), Cyber Insurance, and Report Generator. The main content area is divided into three sections: 'Existing Policies' with a list of 'Example Acceptable Use Policy' and 'Sample Cyber Security Policy' and an 'All Policies' button; 'Policy Tracker' with a table showing 'Total Live Policies: 2', 'Total Recipients: 0', 'Sent Policies Viewed: 0%', and 'Sent Policies Signed: 0%'; and 'Policy Generator' with buttons for 'Create Policy', 'Policy Templates', 'Upload Policy PDF', 'Policy Report', and 'Share Policies with External Auditor'.

Access a range of Boilerplate Cyber Policies, pre built and approved templates to help create your own



The document shows the 'Overview' section of a 'Cybersecurity Policy'. The text reads: 'Keeping up cybersecurity is essential for protecting company and customer data. Without the proper measures and every member of staff taking up responsibility in securing their devices, services, and networks, data could become compromised and cause serious damage to the company and its reputation. Our partners and customers trust us to keep their data safe, and this policy has been instituted to help employees understand their responsibilities and what is expected of them to keep our promise to our customers and partners.'

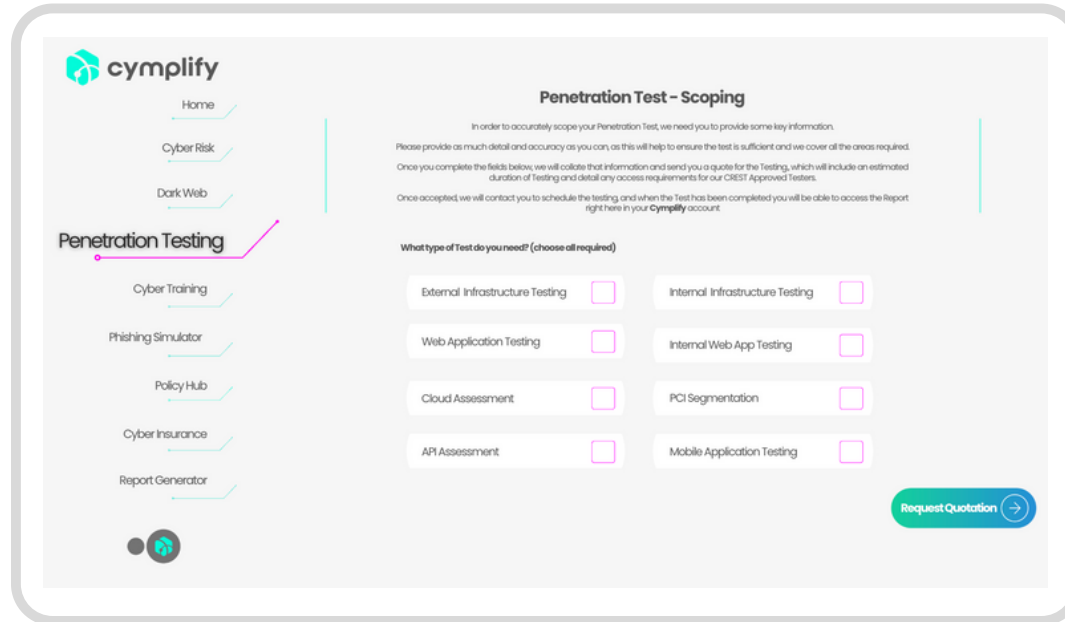
Share your policies directly with a Third Party Auditor for them to review and provide feedback



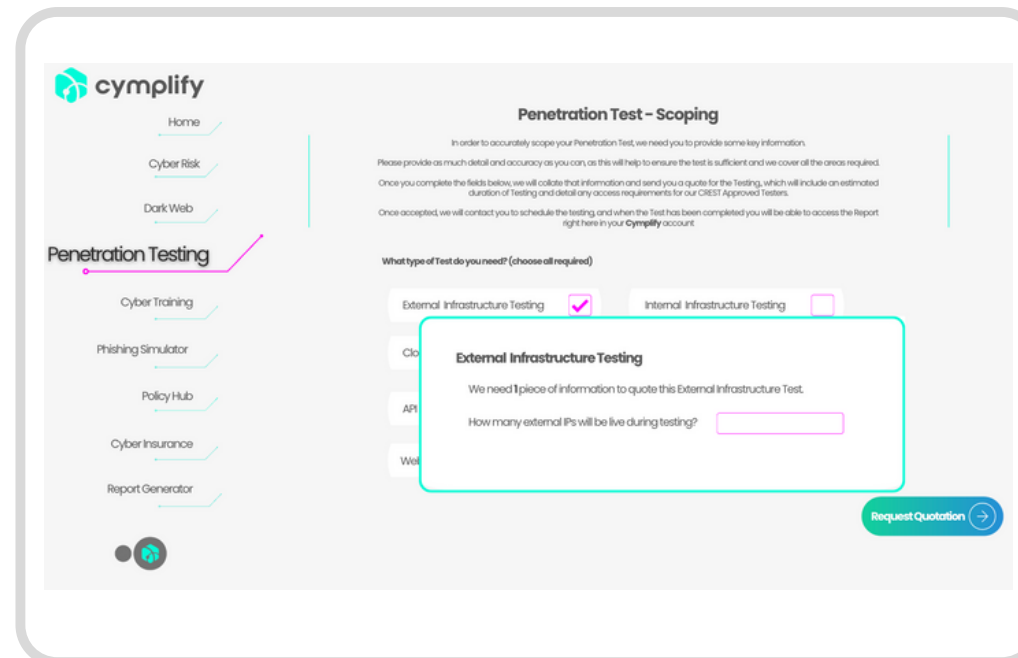
The dashboard is shown with a modal window titled 'Share Policy With Auditor'. The modal contains a dropdown menu for 'Policy' with 'Sample Cyber Security Policy' selected, and a text input field for 'Auditor's Email Address' containing 'Auditor@Auditors.com'. There are 'CANCEL' and 'SUBMIT' buttons at the bottom of the modal.

Centralised Penetration Testing Scoping, Quoting and Scheduling

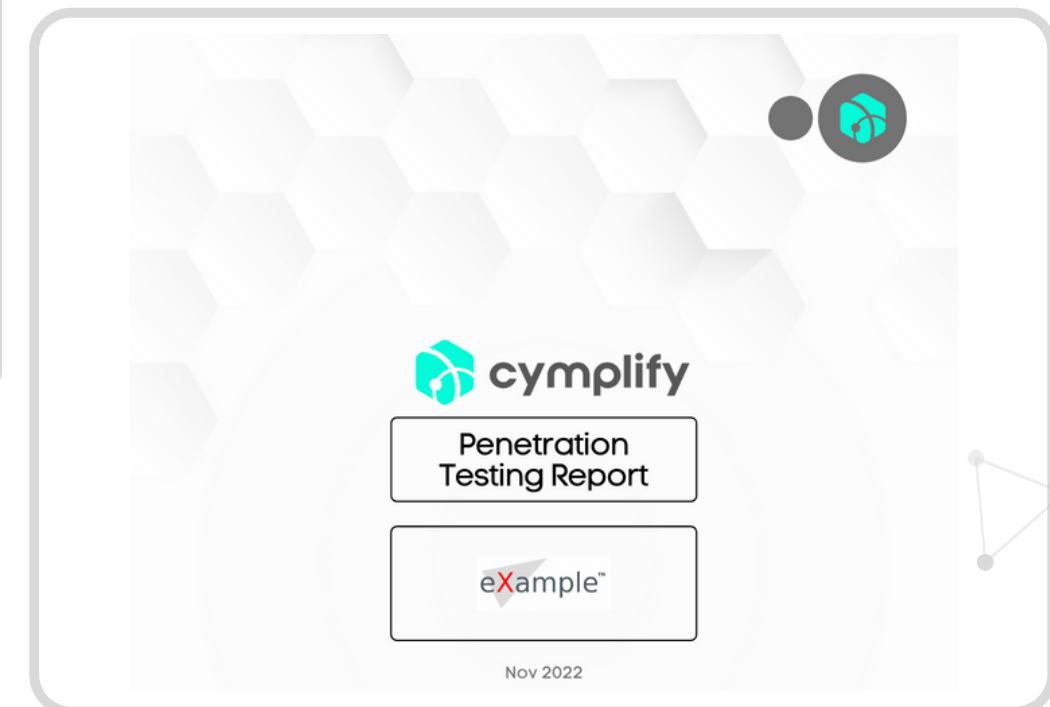
Choose, scope and schedule a wide variety of Penetration Testing in app



Schedule and engage CREST Accredited Ethical Hackers to carry out the required Testing



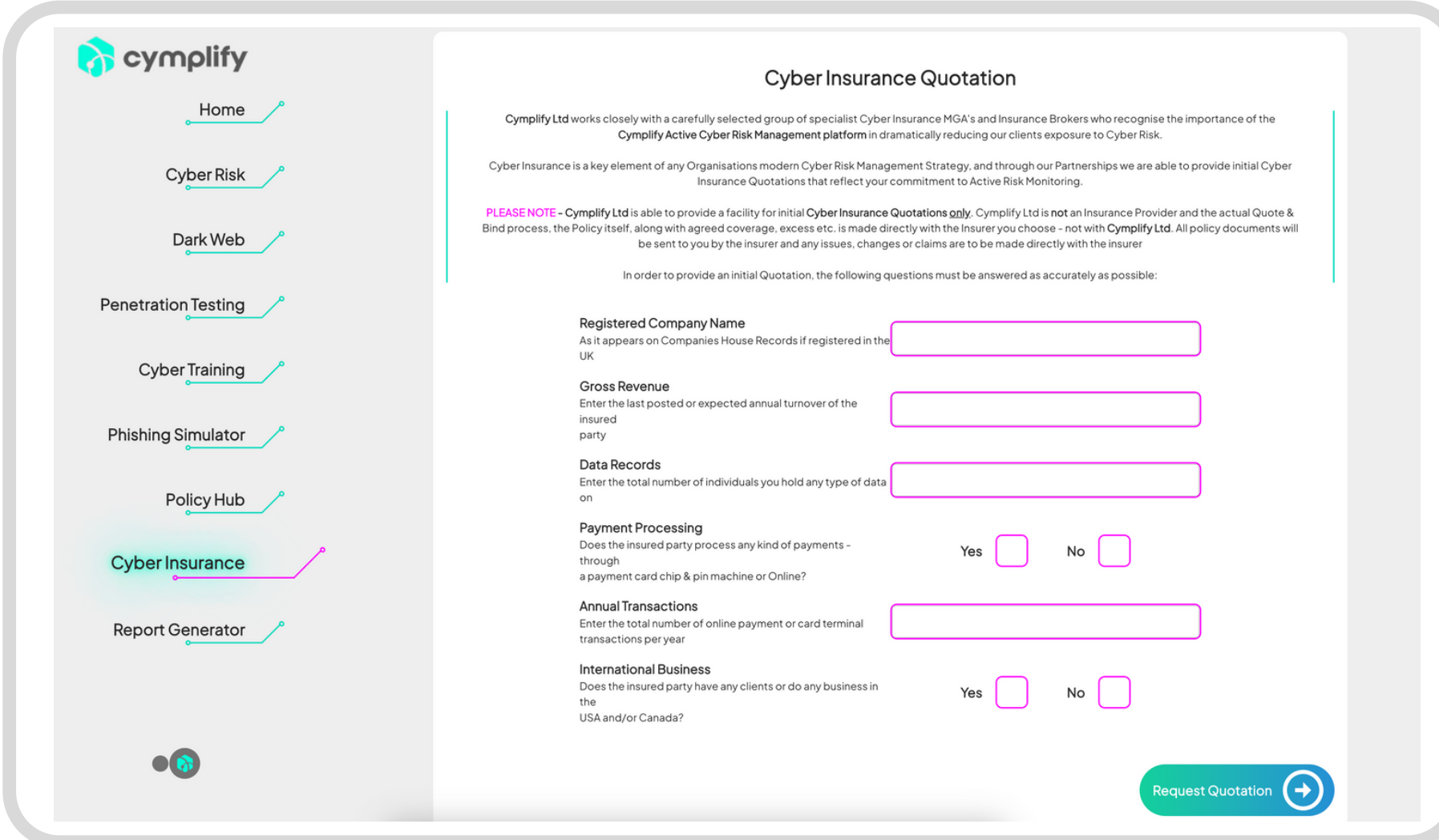
Access Penetration Test results and full Report in app



Integrated **Cyber Insurance** module - direct access to specialist Cyber Insurers and Brokers

Cyber Insurance is now an integral part of both a Cyber Resilience Strategy, and increasingly to Commercial Partnerships and Supplier requirements. However, at the same time as gaining prevalence, actually getting Cover is rapidly becoming much more difficult due to the pace at which the Cyber Threat changes, and the Insurance industry's complexity which leads to an inability to adapt quickly.

Your Cymplify subscription comes complete with direct access to carefully selected, specialist Cyber Insurers and Brokers who recognise and understand the value of the Active Cyber Risk Management platform you are using - and this is reflected in the Policy Documents and Cover Quotes you will receive directly inside the Cymplify app itself



cymplify

- Home
- Cyber Risk
- Dark Web
- Penetration Testing
- Cyber Training
- Phishing Simulator
- Policy Hub
- Cyber Insurance**
- Report Generator

Cyber Insurance Quotation

Cymplify Ltd works closely with a carefully selected group of specialist Cyber Insurance MGA's and Insurance Brokers who recognise the importance of the Cymplify Active Cyber Risk Management platform in dramatically reducing our clients exposure to Cyber Risk.

Cyber Insurance is a key element of any Organisations modern Cyber Risk Management Strategy, and through our Partnerships we are able to provide initial Cyber Insurance Quotations that reflect your commitment to Active Risk Monitoring.

PLEASE NOTE - Cymplify Ltd is able to provide a facility for initial Cyber Insurance Quotations only. Cymplify Ltd is not an Insurance Provider and the actual Quote & Bind process, the Policy itself, along with agreed coverage, excess etc. is made directly with the Insurer you choose - not with Cymplify Ltd. All policy documents will be sent to you by the insurer and any issues, changes or claims are to be made directly with the insurer

In order to provide an initial Quotation, the following questions must be answered as accurately as possible:

Registered Company Name
As it appears on Companies House Records if registered in the UK

Gross Revenue
Enter the last posted or expected annual turnover of the insured party

Data Records
Enter the total number of individuals you hold any type of data on

Payment Processing
Does the insured party process any kind of payments - through a payment card chip & pin machine or Online? Yes No

Annual Transactions
Enter the total number of online payment or card terminal transactions per year

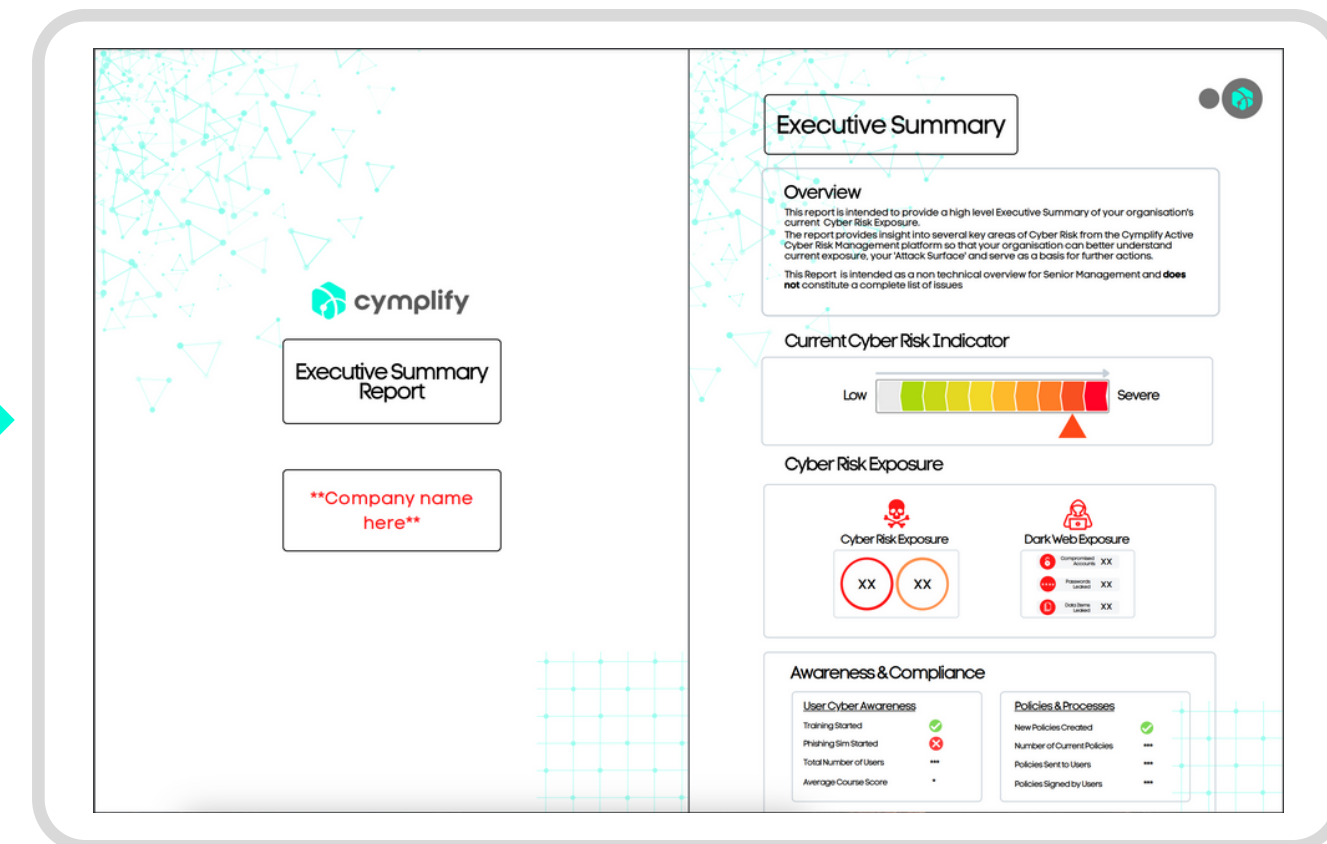
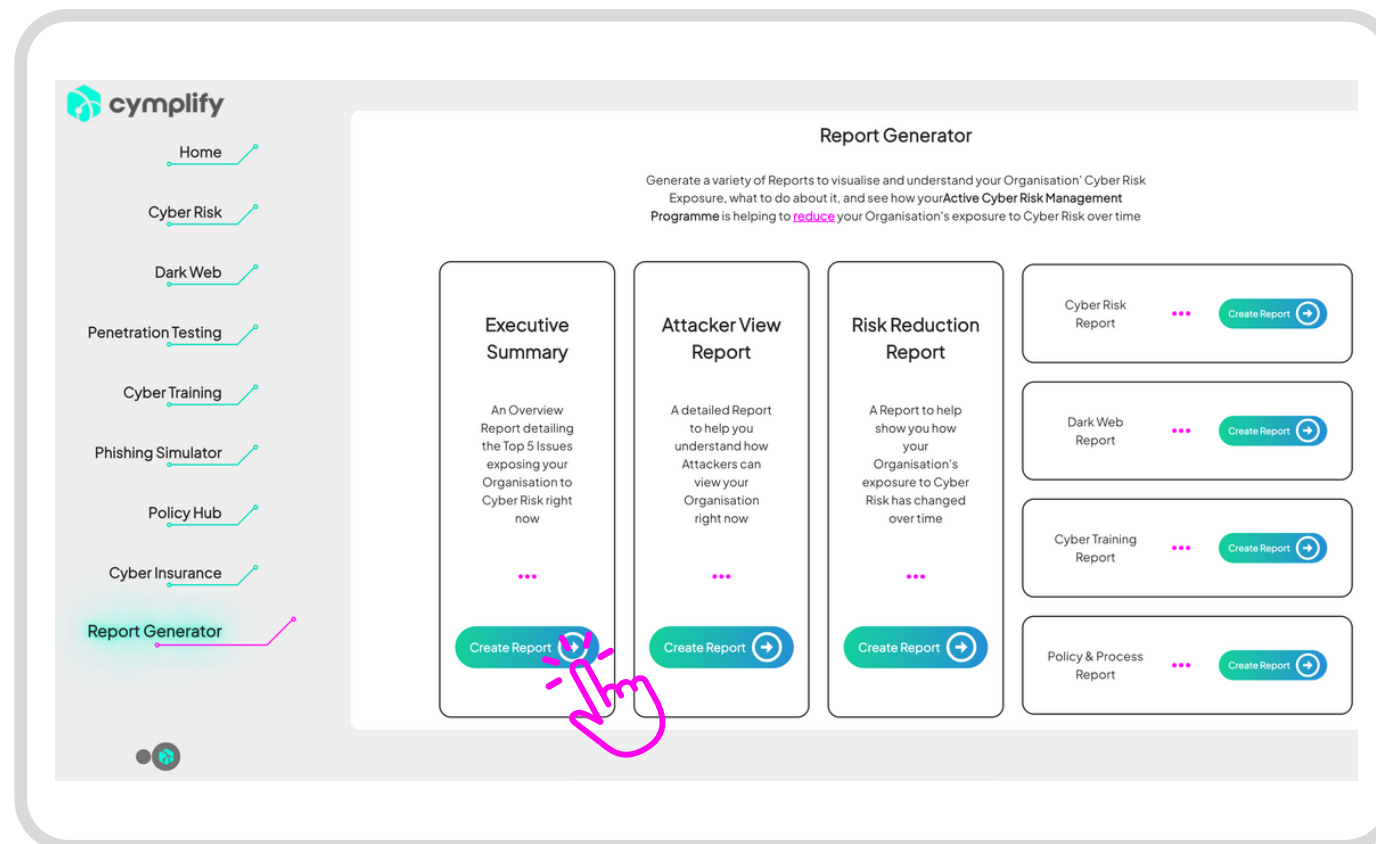
International Business
Does the insured party have any clients or do any business in the USA and/or Canada? Yes No

[Request Quotation](#)

Centralised Report Generator - visualise Risk exposure, evidence Cyber risk reduction over time and demonstrate ROI across the business

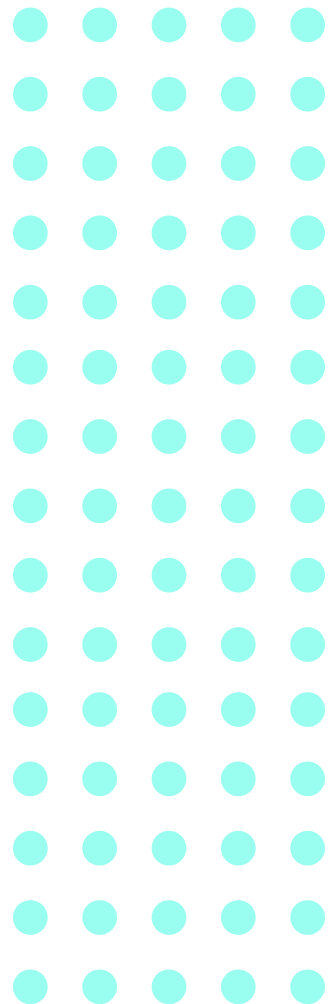
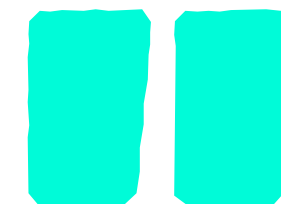
Choose from a variety of Board Level or Risk Specific Reports across all elements of the platform

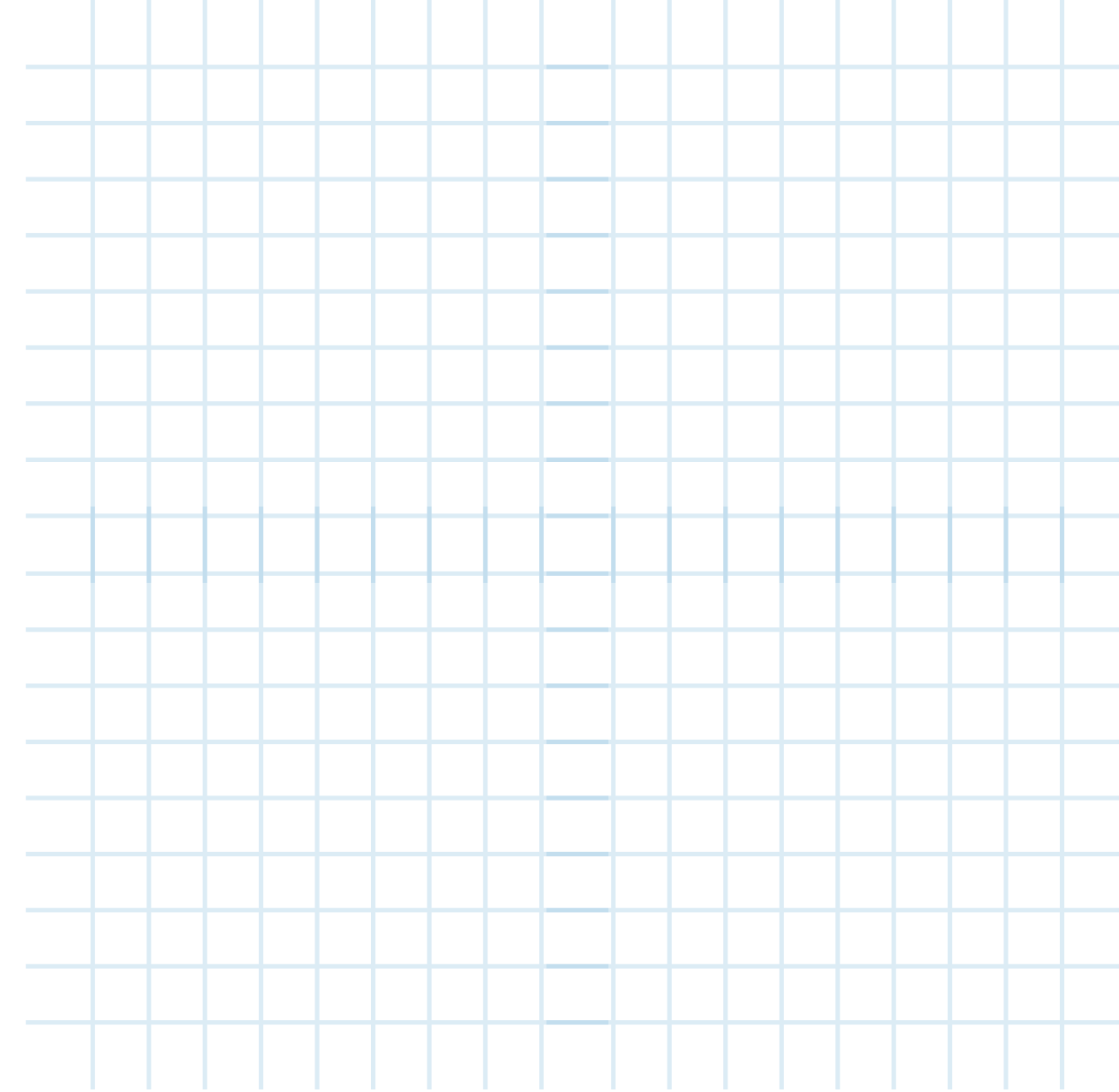
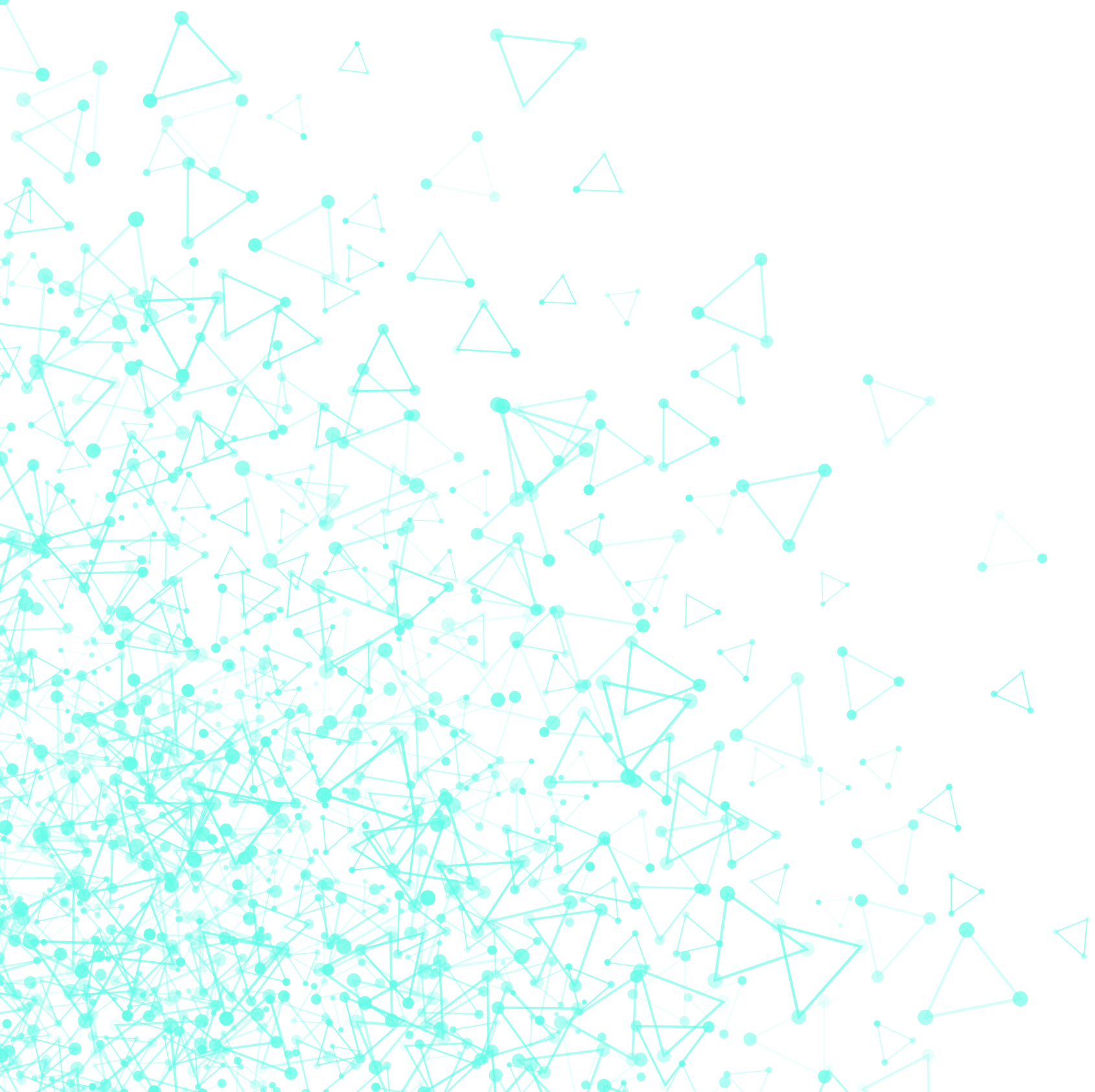
Access reports instantly - one click download for Excel or PDF to share with Key Stakeholders





The Cymplify Active Cyber Risk Management Platform brings powerful, simple, affordable and continuous Cyber Risk Management within the reach of every business. Cutting edge tools, 'Always On' monitoring, real time Alerting and detailed analytics enable any business to **dramatically** reduce their Cyber Risk exposure, promote a culture of Security, and compete effectively in the digital first, globally connected world





w: www.cymplify.co.uk

e: hello@cymplify.co.uk

t: +44 (0)7801899016

a: 71 Shelton St, London, WC2H 9JQ