Proofpoint Security Awareness Enterprise

Take a threat-driven approach to make users resilient

Key Benefits

- See 40% fewer clicks in real-world threat emails in under six months.
- Show your CISO the metrics of successful risk reduction.
- Drive behaviour change with personalised learning experience.
- Automatically analyse user-reported threats without extra IT work.

Proofpoint Security Awareness Enterprise helps you tackle one of the most pressing concerns of every organisation: reducing the security risk that people pose. The 2023 Proofpoint State of the Phish report, our yearly phishing study, shows 98% of all organisations have some form of security awareness education in place. This suggests a widespread recognition of its importance. But training by itself does not always lead to real security outcomes.

For a security programme to be most effective, users must be actively engaged in security learning. They should be able to make safe choices in real-life situations. And their behaviours must have a measurable impact on security outcomes.

Proofpoint Security Awareness Enterprise can help. We address this challenge with the ACE framework, our holistic approach to security awareness. This educational framework is organised into three key steps: assess user vulnerability, change user behaviour and evaluate the programme's effectiveness. Our solution empowers security admins with operational efficiency and the ability to scale globally.

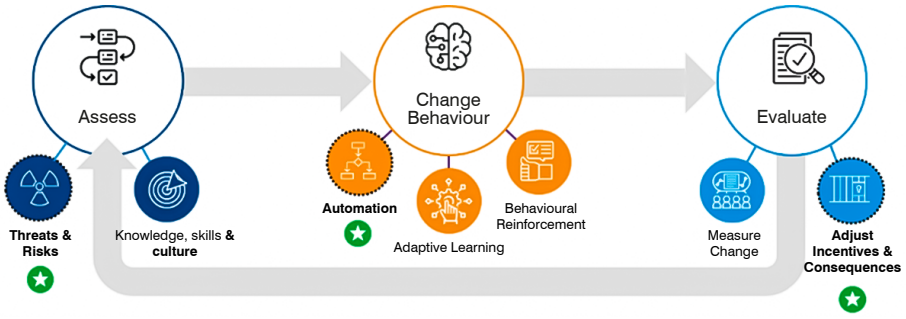

Figure 1: The ACE framework.

Apply Industry-leading Threat Intelligence

Our rich threat intelligence powers Proofpoint Security Awareness Enterprise. We gather this intel from our broad customer footprint. And we use it to help you build an effective training programme. The programme can help you conduct sophisticated phishing simulation campaigns that mimic real-world attacks. You can uncover your Very Attacked People™ (VAPs) and train them on the threats that target them. You can also track how users behave when faced with real-world threats. And you can highlight attack trends in employee newsletters.

Assess User Vulnerability

Proofpoint Security Awareness Enterprise helps you determine your users' level of knowledge, skills and beliefs about cybersecurity. It also indicates how attractive they are as targets. All of this helps you identify highly vulnerable users as well as their ability to behave safely. This way you have a good idea of who needs the most education. And you can then tailor a programme to their knowledge gaps and expected behaviour.

Proofpoint Security Awareness Enterprise helps you:

- Identify knowledge gaps with short, to-the-point quizzes based on our rich threat intel.
- Run phishing tests that incorporate threats we've seen in the wild.
- Analyse vulnerability from participation, performance and the likelihood of being attacked.
- Uncover security beliefs to determine how to impact people's motivation so that they behave safely.
- Reveal VAPs and Top Clickers when integrated with the Proofpoint platform.

Determine what your users know

Our adaptive learning assessments help you determine what your users know and the issues with which they are struggling. The assessments are specific bits of learning that are both concise and precise. You can choose from a variety of quizzes that align to specific learning goals and from microlearning modules that have various levels of difficulty.

Find out what your users will do

Our phishing simulations ensure your users are prepared for real threats. Proofpoint uses threat intelligence derived from more than 2.6 billion emails we see every day. This visibility allows us to offer you thousands of phishing templates that simulate multiple threat types. You can also customise your own templates based on the types of threats in your own environment. And you can auto-enroll into training any user who fails a phishing simulation.

Learn what your users believe

To build a strong security culture, you need to know what your users believe about cybersecurity. Our culture assessments help you to gauge the current state of your security culture. They use short surveys that allow you to explore and measure the three main factors that contribute to this culture: responsibility, importance and empowerment. You can then tailor the programme to impact your people's beliefs and their motivation to take what they learn and put it into practice.

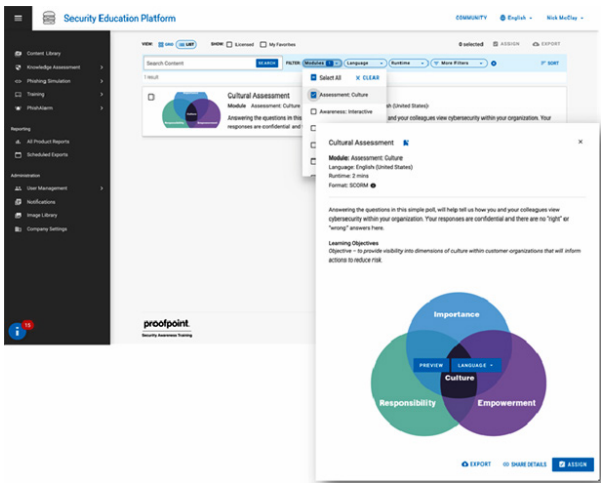

Figure 2: Culture Assessments and enhanced content library and filtering.

Identify your riskiest users

When integrated with the Proofpoint Threat Protection platform, our solution helps you uncover your VAPs and Top Clickers. Armed with this insight, you can provide targeted training to your most-attacked users based on the threats that target them. Our integration with Nexus People Risk Explorer gives you even more insight into your riskiest users. It evaluates their vulnerability, attack index and business privileges. That way, you can focus your programme and resources on the real risks to your organisation.

For more information about the targeted educational content of Proofpoint Security Awareness, see **How Proofpoint Security Awareness Keeps Users Engaged**.

Change User Behaviour

Once you have a baseline of what your users know, do and believe, you can start to change their unsafe behaviour. Proofpoint Security Awareness Enterprise helps you drive behaviour change with tailored education and reinforcement. You can give each person what they need and train them on content that is relevant to them. This helps you maximise the limited time that you have to train them. It can also increase the impact of that training.

Proofpoint Security Awareness Enterprise helps you:

- Motivate users by providing a personalised learning experience.
- Build concise and specific training for each learning objective.
- Deliver engaging content based on the current threat landscape.
- Reinforce learning effectiveness with timely in-the-moment education.

Teach with an adaptive framework and microlearning

Proofpoint Security Awareness Enterprise uses an adaptive learning framework. This is the opposite of a one-size-fits-all approach. The framework delivers security education on a progressive scale. This scale includes four different levels, from the basics to advanced concepts. So, your users can get the training they need with the right level of difficulty.

The adaptive framework is also wrapped into microlearning. These are three-minute modules that have concise and specific learning objectives. Your users receive ongoing training that is easy to digest. And the training is tailored to individual factors such as the person's role, learning style, competency, vulnerability level and language.

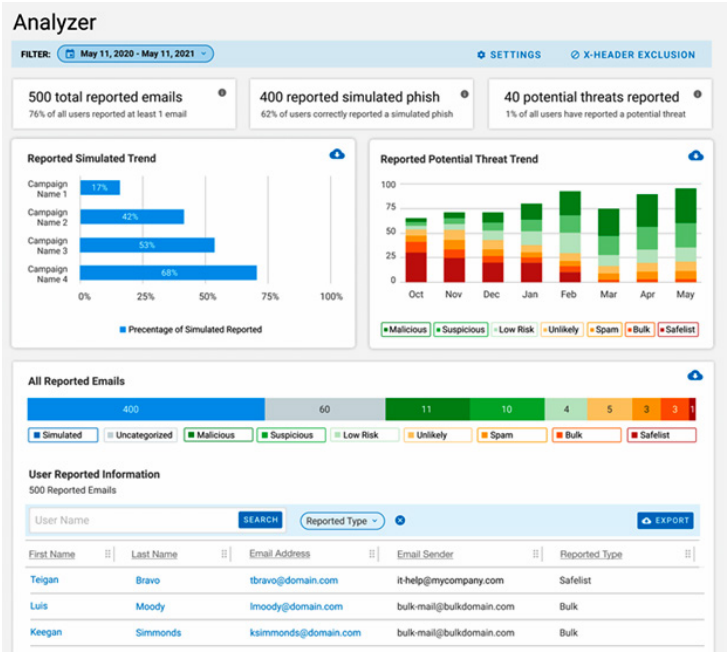

Figure 3: Real-time reporting behaviour for both simulated phishing tests and real-world threats.

Provide threat-driven content and timely training

Trends and tactics in the current threat landscape inform the content of Proofpoint Security Awareness Enterprise. This lets you better prepare your users for current, real-world threats. Our weekly Threat Alerts explain the latest attacks we see across our customer base. And our Attack Spotlights enhances your programme with time-sensitive training.

When Proofpoint Security Awareness Enterprise is integrated with the broader Proofpoint platform, you can provide your users with contextual nudges and positive reinforcement. Teachable Moment popups explain to users why they should not click a phishing simulation link. In-app Email Warning Tag banners alert them to messages that might be malicious. And the Report Suspicious button kicks off our automated Proofpoint Closed-Loop Email Analysis and Response (CLEAR) workflow, which notifies the users with customised feedback about the email they reported.

Evaluate the Programme's Impact

You must be able to evaluate the impact that your security awareness programme has on your security footprint.

Proofpoint Security Awareness Enterprise provides behavioural metrics that show how your people and the programme are performing. And you can clearly benchmark those better security outcomes. For instance, our customers see a drop of 40% in the number of clicks on real-world threats within six months. They also see the number of user-reported emails increase by three times. You can take these risk-reduction metrics to the CISO to showcase the programme's success and get buy-in for further investment and growth.

Proofpoint Security Awareness Enterprise helps you:

- Track user behaviour on reporting of real-world threats.
- Benchmark key metrics against your industry peers.
- Communicate positive change in user behaviour to get C-level support.

Track behaviour for both simulations and real emails

Our unique CISO Dashboard shows the impact of education on your people's behaviour. It tracks user reporting for real-world emails and shows changes over time. This way you can understand how their behaviour has improved. Metrics such as the rate of reporting suspicious emails and the accuracy of that reporting help you measure user performance beyond the training completion rate.

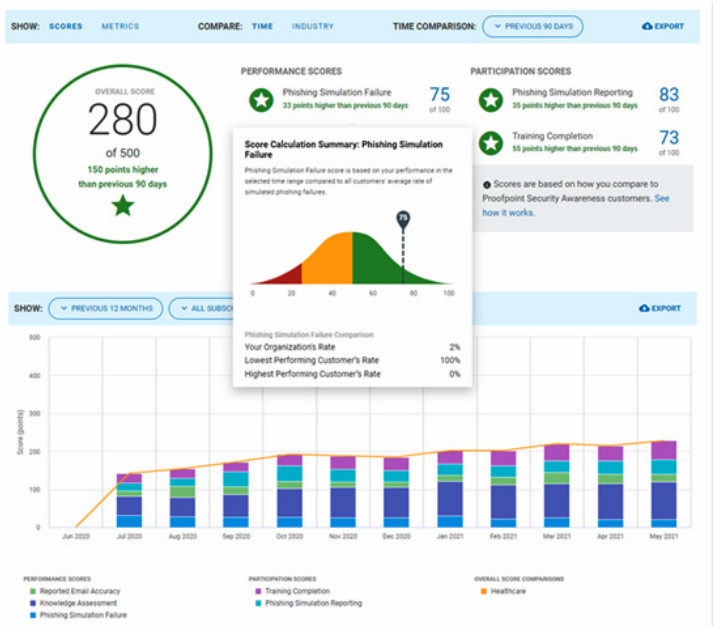

Figure 4: Programme performance tracking in CISO Dashboard Score Summary.

Benchmark against industry peers

The CISO Dashboard also benchmarks the performance of your programme against that of industry peers. It lets you see changes in the real-world behaviour of your users, like, for example, the percentage of users who report suspicious emails. You can then compare their accuracy rate to rates reported in other organisations. This way you can see your programme's impact relative to other companies and share that success story.

Report for Repeat Behaviour

Proofpoint Security Awareness Enterprise gives you daily data about internal tests and external threats. For instance, you can track and report repeat behaviour. Our solution lets you filter and group the users who failed a phishing simulation multiple times within a specified time frame. This ensures that admins are up-to-date and accurate in their escalation plans, such as assigning additional training.

Expand and Scale Your Programme

Proofpoint Security Awareness Enterprise gives you the power of automation and scalability. Automated processes reduce manual work and allow you to be more flexible and efficient with your operations. Our solution also enables a global reach with the ability to scale.

Proofpoint Security Awareness Enterprise helps you:

- Enhance the administrator experience with flexible automated processes.
- Engage your global audience in their preferred language.
- Brand your security awareness programme with expanded language support.
- Follow best practices and get day-to-day help with Proofpoint managed services.
- Make it easy for users to report suspicious email and get positive feedback.
- Automatically investigate and remediate user-reported emails through Proofpoint platform integration.

Support multiple languages

You can engage your global audience in their preferred language. Proofpoint Security Awareness Enterprise offers more than 40 languages across our training modules and Customisation Services. This includes subtitles and voice-overs. And we continue to update with additional languages.

Run flexibly with multitenancy

With multitenant administration, you get an easy streamlined setup that can be rolled out flexibly and configured for your specific use case. Your company-level security team oversees the programme as a whole. It makes group-wide decisions. Individual groups—such as a regional branch or business unit—can tailor the education for their local users and specific requirements. This workflow is ideal for large complex organisations with global or distributed footprints.

Improve productivity with services

Proofpoint helps you augment your security team and apply security best practices. With **managed services**, we can handle the day-to-day work of running and reporting for your security awareness programme. This way, your security team can focus on its primary business activities. With **Proofpoint Security Awareness Customization Services**, you can present a branded programme and further your security culture by customising microlearning modules. These can include assets like corporate logos, colours, imagery, text, voiceover and translation.

Automate user reporting and threat response

When a user reports a suspicious email in their email client, Proofpoint threat detection automatically analyses the email. This reduces your exposure to phishing that might slip through. It also reduces manual work and increases operational efficiency. If our threat detection flags a suspicious email as a threat, when integrated with the broader Proofpoint platform, our automated CLEAR workflow kicks in. It pushes the email into remediation and sends feedback to the users who reported it. This process reinforces positive behaviour for users. And it reduces the remediation workload by as much as 90% for admins.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at www.proofpoint.com.