YesWeHack

Pricing

Continuous Penetration Testing

YesWeHack

Service Description

Our pricing model consists of two categories:

1. **Standard Pricing** – applies when the number of required campaigns is within the limit of the selected asset tier.

   Formula: Asset-Based Fee + Campaign Package Cost = Total Price

2. **Uplift Pricing** – applies only when a customer requires more own-test campaigns than their asset tier includes. An uplift provides the extra CSM capacity needed to safely support the additional tests.

   Formula: Asset-Based Fee + Campaign Package Cost + Uplift Cost = Total Price

This structure ensures pricing is transparent, predictable, and aligned with both the size of the environment and the volume of human-led testing required.

1. Asset-Based Fee (Continuous Testing)
Customers are placed into an asset tier based on the number of in-scope assets. The asset fee covers our ongoing detection service, which combines automated risk-based assessments with manual validation by YesWeHack's in-house pentesters. Testing is powered by our proprietary Security Check engine, a continuously updated library of real-world exploitation scenarios ("checkpoints"). When the automation detects a potential issue, our internal pentesters manually verify, assess, and report the finding. This ensures continuous coverage of the most actively exploited vulnerabilities and misconfigurations, while focusing expert time where risk is highest.

Important note: the asset-based fee is priced to include the proportionate level of Customer Success Manager (CSM) oversight required to manage pen-test **campaigns** (see below).

Therefore, each asset tier is designed with a *maximum number* of pen test campaigns that can be realistically supported within the CSM capacity built into that tier.

2. Pen-Test Campaign Packages (One-Time, In-Depth Human Pentests)
In addition to continuous testing, customers may purchase annual campaign packages up to the maximum permitted per asset tier. Campaigns are fully human-led and managed by a dedicated CSM.

Pentesters are selected from our vetted global community based on experience, skills, and methodology requirements (e.g., OWASP). Every pen-test campaign report undergoes full internal review and retesting before delivery.

Campaign packages are prepaid annually and provide up to the stated number of tests; unused campaigns are not refunded.

Campaign pricing covers the pentester/crowd testing effort only.

This two-part model allows customers to combine continuous, automated-plus-manual detection with optional deep-dive human testing, while maintaining a clear, sustainable, and predictable annual cost structure.

Additional Campaign Capacity

In some cases customers may require more pen-test campaigns than their asset tier allows. To unlock the next campaign tier customers can purchase “additional campaign capacity”.

Each additional campaign creates increased work for your Customer Success Manager - planning, scoping, selecting pentesters, supervising the test, and validating the final report.

The cost for “additional campaign capacity” covers that extra CSM time so we can deliver the extra campaigns properly and maintain service quality.

All prices are in **Pound Sterling (GBP, ex VAT)** and based on an **annual subscription**. Contract terms align with G-Cloud limits.

Pricing Table - Continuous Testing

Asset based fee

Asset Tier	Base Fee	Maximum number of Campaigns per year
A1 (up to 100 assets)	£13,200.00	2
A2 (up to 250 assets)	£22,000.00	5
A3 (up to 500 assets)	£30,800.00	10
A4 (up to 1,000 assets)	£52,800.00	20
A5 (up to 2,500 assets)	£66,000.00	30
A6 (up to 5,000 assets)	£88,000.00	50
A7 (up to 10,000 assets)	£132,000.00	100
A8 (over 10,000 assets)	£176,000.00	Unlimited

Pen-Test Campaigns

Package Name	Campaigns	Cost per Campaign	Total Cost (GBP)
2 Pen-Test Campaigns	2	£6,000.00	£12,000.00
5 Pen-Test Campaigns	5	£5,700.00	£28,500.00
10 Pen-Test Campaigns	10	£5,400.00	£54,000.00
20 Pen-Test Campaigns	20	£5,100.00	£102,000.00
30 Pen-Test Campaigns	30	£4,900.00	£147,000.00
50 Pen-Test Campaigns	50	£4,800.00	£240,000.00
100 Pen-Test Campaigns	100	£4,700.00	£470,000.00

150 Pen-Test Campaigns	150	£4,600.00	£690,000.00
200 Pen-Test Campaigns	200	£4,400.00	£880,000.00

Optional: Fixed Uplift Prices

Unlock Capacity	Additional Pen-Test Campaigns	Uplift Price
2-10	8	£12,000.00
10-30	20	£30,000.00
30-50	20	£30,000.00
50-100	50	£75,000.00
100-150	50	£75,000.00
150-200	50	£75,000.00

Example Costing – No Uplift Required

Customer: 180 in-scope assets
Requirement: 5 pen-test campaigns
Asset Tier: A2 (up to 500 assets)

- Asset-Based Fee: **£22,000**
- 5-Campaign Package: **£28,500**
- Total Annual Cost: **£50,500 (ex VAT)**

Example Costing – Uplift Required

Customer: 180 in-scope assets
Requirement: 25 pen-test campaigns
Asset Tier: A2 (up to 500 assets; includes up to 10 campaigns)

- Asset-Based Fee: **£22,000**
- Additional Campaign Capacity Uplift (10 to 30 campaigns): **£30,000**
- 30-Campaign Package (covers the 25 required): **£147,000**
- Total Annual Cost: **£199,000 (ex VAT)**

One-Time Pen-test Campaigns Definition

These pen-test campaigns are delivered as fully managed, time-bound assessments scheduled in advance.

- Each pen-test campaign is a standalone, in-depth assessment conducted at a predefined date or frequency.
- Pen-test Campaigns are fully managed by the customer's dedicated Customer Success Manager (CSM).

- The CSM selects appropriate pentester(s) based on the customer's requirements, such as the scope, testing methodology, location, and required skillset.
- Pentesters are selected from YesWeHack's vetted Security Researcher community, based on proven expertise demonstrated across multiple bug bounty programs.
- All testing activities are supervised by the CSM, ensuring control, quality, and alignment with customer requirements.
- All vulnerability findings are validated and retested by YesWeHack prior to customer notification.
- Final reports follow the same standard format used by YesWeHack in-house pentesters, with the source of findings clearly noted.

Supported Testing Requirements

- Customers may request recognised methodologies such as OWASP.

Restrictions

- Pen-test Campaigns cannot be used for internal pentesting.
- Pen-test Campaigns cannot be purchased as ad-hoc, punctual pentests. They must be planned in advance.

Additional Pen-Test Campaign Capacity

You *only* pay an uplift when you want more pen-test campaigns than your asset tier includes. As outlined above, the uplift simply covers that extra CSM time so we can deliver the extra campaigns properly and maintain service quality.

Seasonal Discounting

- A seasonal discount of 7.5% is available for purchases made between October 1st and December 31st, each year the framework is live.

Additional Notes

- "Assets" may include web applications, APIs, IPs, domains, cloud accounts, and externally exposed services.
- All subscriptions include ongoing vulnerability management, continuous discovery, alerting, and manual penetration testing.
- On-demand compliance and audit reporting is included, allowing customers to generate downloadable reports at any point during continuous testing or during/after a campaign.
- Individual Prices may increase during the contract as per CCS guidelines at call-off level, where reviews have been agreed by both parties prior to the contract award.

Contract Duration

- Maximum contract term: 36 months, with an optional 12-month extension (total maximum of 48 months).
- Prices listed are per annum and exclude VAT.

Enterprise Style Deals

Enterprise-level commercial arrangements may be considered on a case-by-case basis, subject to G-Cloud framework rules.

Summary

Our pricing model is structured to provide clarity, predictability, and flexibility. Customers first select an asset tier that reflects the size of their environment; this determines the base annual fee for our continuous testing service. This fee covers 24/7 detection of top-exploited vulnerabilities using our proprietary Security Check engine, combined with manual validation by YesWeHack in-house pentesters. This ensures continuous, risk-based coverage that prioritises the vulnerabilities most likely to be exploited in real-world conditions.

Customers may then add annual campaign packages, which provide a set number of fully human-led pentest campaigns. Each campaign is managed by a dedicated CSM and testing is performed by carefully vetted, high-performing researchers from our global community, with all findings internally reviewed before delivery. This combined model enables buyers to tailor the level of human testing they require while retaining a clear, predictable annual cost structure.