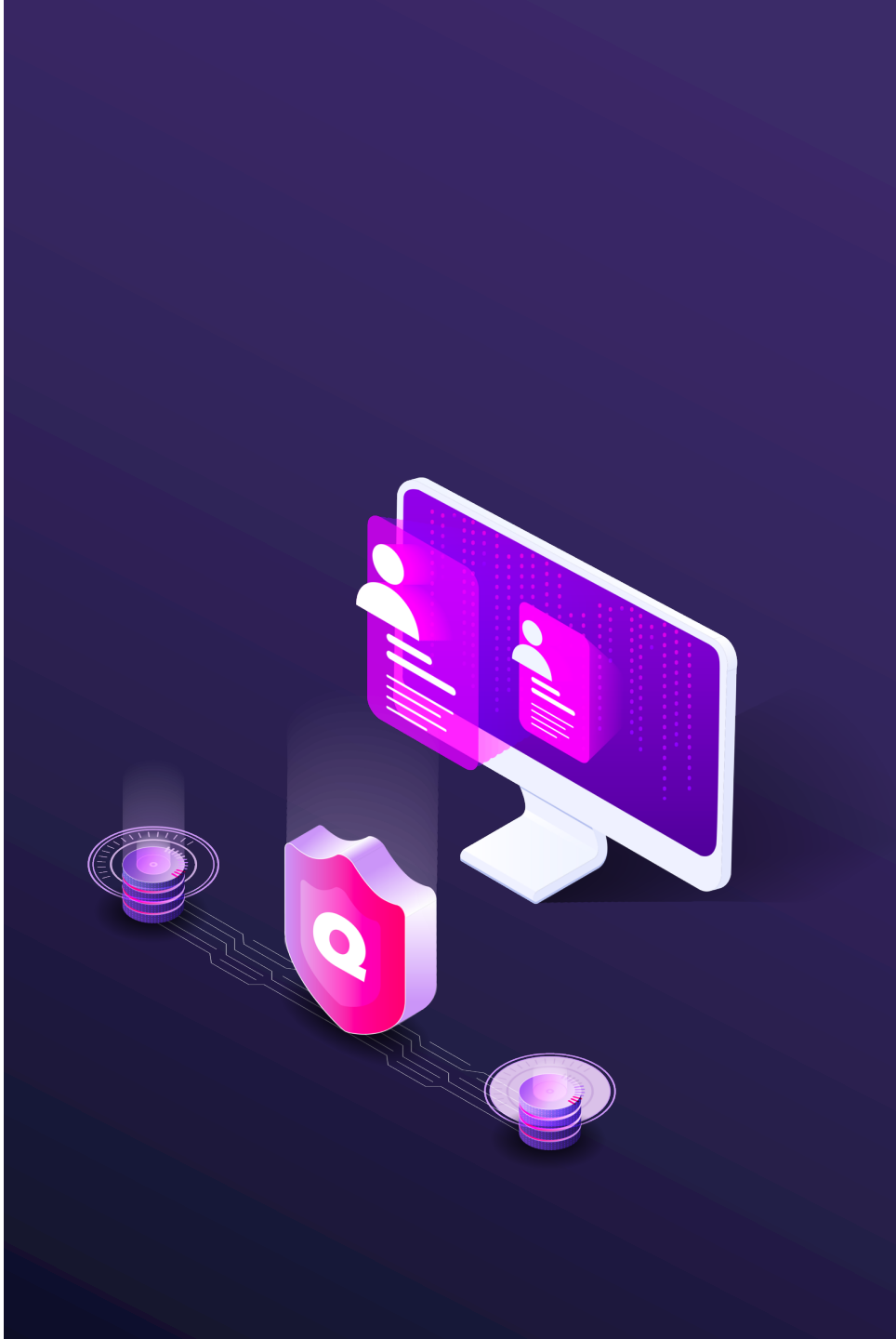
Feature Overview

# Sign-up & Lead Protection

Eliminate fake leads, sign-ups and registrations that pollute your systems, pipeline, and waste your resources.



CHEQ paradome

# Online sign-ups and lead-gen are at the core of the organization's GTM strategy

Whether you're a SaaS company, online retailer, Higher Education Institution, or publisher, online sign-ups and lead generation are at top priority in your GTM strategy. User acquisition is the fuel that helps any business grow and thrive, and focusing on good leads while eliminating the junk is key for efficiency.

Being a top priority for marketers, they invest heavily in developing websites and landing pages, creating content, creative and experiences to attract and convert audiences. The smarter they are with the invested resources, the more quality leads come in, and in turn better conversion rates and ROI.

## Common scenarios

- Signing up for services and events
- Creation of new accounts
- Contact forms
- Booking services, meetings or demos
- Downloading gated content

CHEQ paradome

**But it's not always the users you wished for...**

# Bad actors take advantage of frictionless landing pages and form-fill flows

Data suggests that bots, fake users, and other bad actors with no intention to convert, can account for up to 40% of your overall website traffic, engaging with your site assets in a multitude of harmful ways, including generating new accounts, leads and sign-ups.

The fact that sign-up flows are typically designed to be frictionless makes it easier for them to create new accounts. Sometimes these are automation tools, but more often it's mal-intent humans using fake credentials. Sign-ups are often used to abuse marketing promotions, validate stolen credit card information, make fraudulent transactions, or sell them to other cybercriminals.

CHEQ paradome

### *Carding Attacks*

*Fake accounts can be used to test stolen credit card information to see if the card still works.*

### *Promotion Abuse*

*Fake accounts created to take advantage of welcome offers, promotions, or incentives for resale or financial gain.*

### *Selling Access/Credentials*

*Fraudsters will also create new accounts to sell to other cybercriminals interested in accessing your platform*

### *Affiliate Lead Fraud*

*Affiliate partners fill out forms and generate fake leads using stolen data in order to increase commissions*

### *Data Exploit*

*Attackers submit fake leads to collect company data and email addresses, setting up malware attacks and phishing schemes*

### *Pipeline Flooding*

*Businesses use bots to flood their competitors' pipelines with fake leads harming their sales team's performance*

### *Creating Legitimate Online Presence*

*Cyber criminals create fake online accounts for various services to for a seemingly legitimate online identity*

# Fake leads and sign-ups entering your funnel are detrimental to the GTM organization

**Skewed Data**

Fake leads skew your metrics and seriously damage your forecasting and planning

**Wasted resources**

Fake users inflate your marketing tech stack bills and waste your sales team's time.

**Damaged Reputation**

Fake leads portray you as a business with security issues or as a spammer sending unsolicited emails.

**Lost Reveunues**

Fraudsters create fake accounts to abuse your marketing promotions.

CHEQ paradome

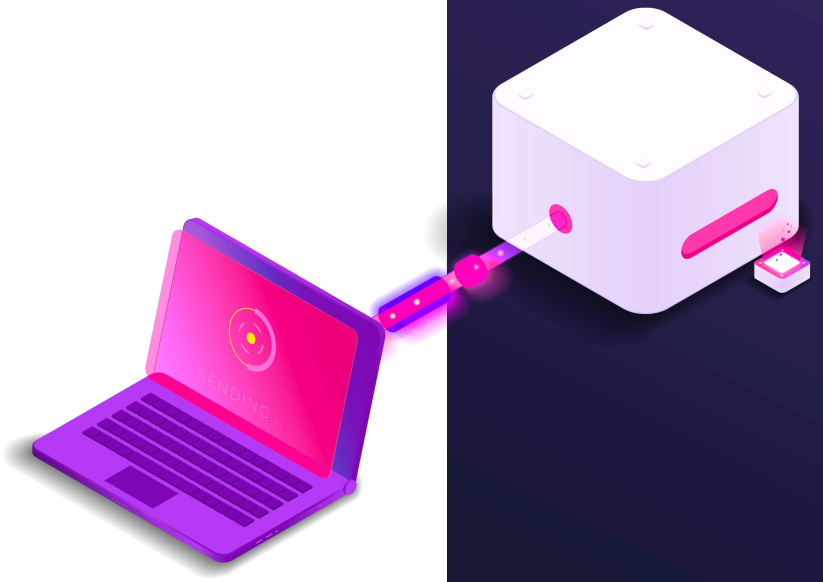
Introducing

# CHEQ Sign-up & Lead Protection (SLP).

## Protecting your funnel from bad actors

CHEQ Sign-up & Lead Protection (SLP) is a comprehensive solution designed to protect against automated and malicious human actors from abusing your website's form fill flows. Part of CHEQ's On-Site Security solution, SLP uses sophisticated methods to validate the authenticity of users filling out forms, signing up, or creating new accounts.

The solution can be activated in two modes: blocking or data enrichment, allowing you to either block the user in real-time, or allow them in your funnel while adding CHEQ's analysis data to their profile.




CHEQ paradome

Go beyond bot-mitigation.

# Protect your sign-ups and leads from bad actors.

## Protect your resources

Prevent bad actors from straining your infrastructure, abusing your promotions and using up your teams' precious time.

## Maintain efficiency

Prevent fake leads from contaminating your CRM and sales pipeline, and maintain your teams' focus on real potential customers.

## Keep the fraudsters out

Prevent fraudsters from using your site to validate stolen credentials and abusing it for nefarious activities.

## Protect your brand

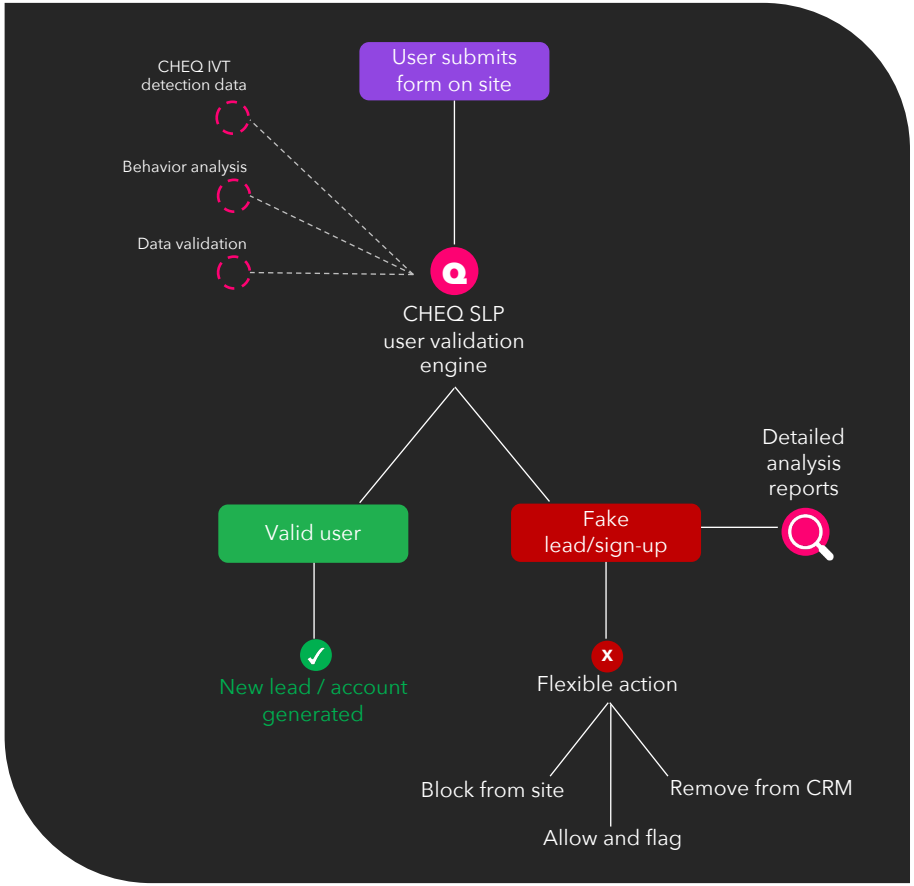
Protect criminals from creating fake accounts and false registrations that can damage your business's reputation.

CHEQ paradome

# How it works

A user on your site submits a form. CHEQ's SLP feature deploys a series of tests to validate the user, analyzing input data such as email and phone number as well as behavioral patterns and data collected from CHEQ's IVT detection engine. SLP can be deployed on any page that allows users to submit information.

When a submitted form is deemed invalid, it can either be blocked immediately or allowed in the funnel along with the detection data, threat type, risk score and CHEQ's recommendation for action.




## The setup

1. CHEQ tag is placed on site
2. Define protected assets: form, sign-up, new account
3. Your dev team works with CHEQ's technical success team to integrate the solution on your digital assets, and apply your preferred protection policies

CHEQ paradome

# Reach out and start securing your forms, leads and sign-ups.

Contact your rep or visit www.cheq.ai

CHEQ paradome