GATEWAY
For organizations that require enhanced program control

SECURE VPN TECHNOLOGY FOR CROWDSOURCED SECURITY

From private financial records and sensitive patient health data to top secret military systems, many security testing use cases require strict transparency and auditability not available in standard crowdsourced programs. Gateway (VPN), part of HackerOne Clear, is designed to meet these requirements.

Gateway allows for all program traffic to be routed through HackerOne’s proprietary VPN technology, capturing all finder traffic data and providing the transparency and controls needed by highly-regulated customers, such as government agencies, insurers, banks, and healthcare organizations.

Frequent customer requirements include:

- The need to satisfy internal legal requirements before starting a crowdsourced security program
- The desire to bring crowdsourced testing to internal, sensitive, or pre-production applications, as well as applications that are not accessible over the internet
- The need for clear-cut visibility into HackerOne finder traffic
- The ability to pause/restart a program or individual finder on-demand

KEY BENEFITS

Bring crowdsourced security to internal attack surfaces:
Test internal or pre-production assets through Gateway with IP whitelisting.

Increase visibility & tracking:
Identify finder traffic and pause/restart a program or a finder.

Scale security testing:
Use Gateway for sensitive applications, and open testing of other apps to the wider community.

TRUSTED GLOBALLY

[Logos of various organizations]
KEY PRODUCT CAPABILITIES

Based on Proven, Easy-to-Configure OpenVPN Technology

- **Easy set-up:** Customers simply whitelist HackerOne-designated IP addresses and update their Web Application Firewall (WAF) / Firewall rules to accept whitelisted, trusted traffic.
- **Traffic isolation:** Gateway offers unique IPs to individual finders, removing the risk that one finder's activity might compromise the performance of other finders.
- **Fast incident response:** Clearly identify & segment H1 ('friendly') traffic to enable incident response teams to quickly respond to suspicious activity caused by non-H1 program traffic.
- **Less noise:** Reduce false alarms triggered by HackerOne-vetted finders testing payloads.
- **Control down to the individual finder:** Pause / restart at the individual finder or program level.

Test Applications That Are Not Publicly Accessible

- **Protected and pre-production assets:** Deploy crowdsourced testing to protected assets such as staging environments, internal applications, applications behind firewalls or a corporate VPN, etc.
- **Regulated data:** Protect privileged systems like PCI Cardholder Data Environments (CDE) and other PCI use cases where infrastructure is not externally accessible.

Capture All Finder Testing Traffic and Data

- **Superior program engagement:** Gateway's split-tunnel design ensures only testing traffic passes through the VPN, protecting the privacy of a finder's personal internet browsing activity, resulting in superior program engagement and trust between the finder and customer.
- **Detailed activity logs:** Customers can request detailed activity logs specifying assets hit on a per finder basis and more.

"The sensitive nature of our assets and hacker participation requirements makes HackerOne's vetting capabilities a critical component of our program's success."

Reina Staley,
Former Chief of Staff, Digital Defense Service

PARTNER WITH HACKERONE

One Platform to Maximize Your Crowdsourced Security Results

Customers can leverage the control and transparency of Gateway for sensitive applications while simultaneously harnessing the larger finder community for less sensitive assets, all on a single platform.

Contact us today and learn more about HackerOne Gateway.

HackerOne is the #1 hacker-powered security platform. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative.