Secured crowd testing

VETTED CROWD - TRUSTED COMMUNITY

We understand the importance of protecting your data and systems. That's why we carefully vet our testers at 5 different levels, based on the complexity and the risk of your applications we engage testers from the most suitable levels.

Vetting Level	
Level 0	Not vetted
Level 1	Top ranking testers; Known testers - 1 to 3 years on our platform
Level 2	ID proof, address proof, resume provided, detailed on line profile completed
Level 3	ID proof, address proof, online profile verified & resume screened
Level 4	Interviewed face to face or via skype to verify experience/ qualifications Or cleared IKM online test on software testing/ quality assurance Or software testing qualification such as ISTQB verified
Level 5	Police Verification/ Security Clearance

LEGALLY PROTECTED: NDA | CONFIDENTIALITY AGREEMENTS

We take your information security very seriously and as such, we have legal agreements in place with our testers to protect your IP. Our testers can also sign a direct Non-Disclosure Agreement (NDA) with your organisation, if required.

Level	
Level 1	Agreed to our legal terms and conditions online, including non-disclosure and protection of confidential intellectual property
Level 2	Signed our paper-based non-disclosure/ confidentiality agreement
Level 3	Signed a client/ project specific non-disclosure/ confidentiality agreement

SECURED CONNECTIVITY AND TECHNICAL CONTROLS

Crowdsprint establishes secured private connectivity to your test environments. We can implement 5 levels of technical security controls to establish secured connectivity between your test systems and our testers.

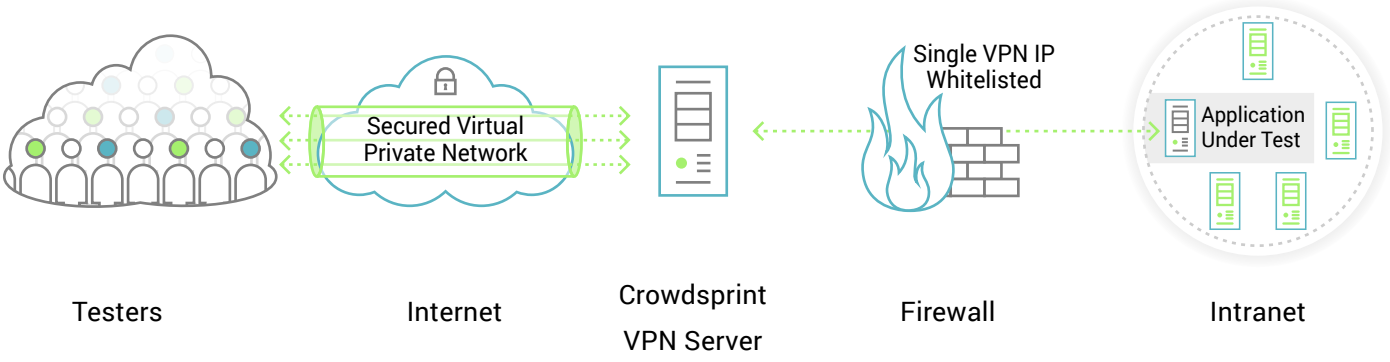
Level	
Level 0	Available on the internet (Pilot/ Prototype; Alpha/ Beta/ PVT)
Level 1	Application level access credentials
Level 2	Additional browser level access credentials (HT access)
Level 3	Crowdsprint VPN Connectivity
Level 4	Crowdsprint VPN Connectivity with security token or logging or IP level access restriction rules
Level 5	Customer specific VPN connectivity and additional security measures or customer authorised local crowd access centre in Melbourne, Sydney, Canberra and Brisbane

SECURED IT INFRASTRUCTURE

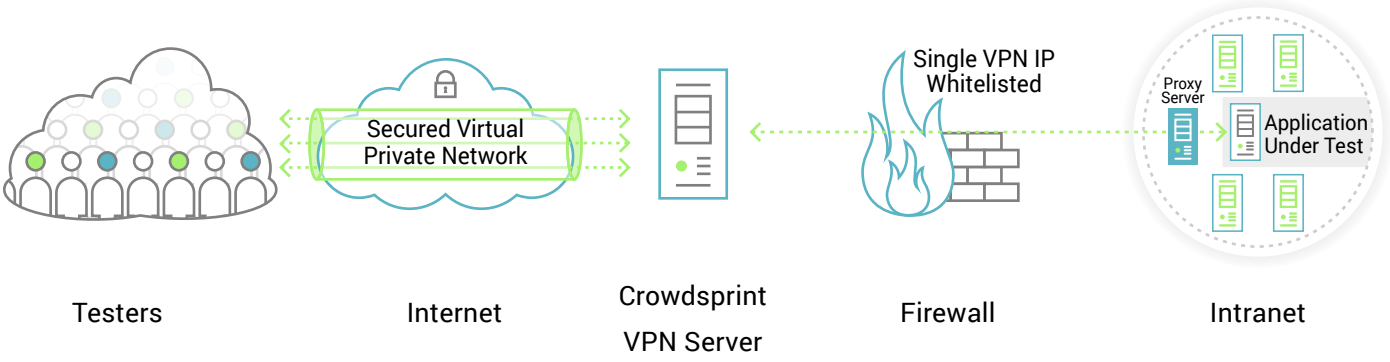
- Our crowd testing platform is built and hosted on ISO 27001 certified MicroSoft Azure data center in Australia.
- Our secured VPN servers are hosted on ISO 27001 certified Amazon Web Services (AWS) data center in Australia.

CROWDSPRINT VPN ARCHITECTURE

Option 1



Option 2



- The client needs to whitelist the VPN server IP address in the firewall. Only one or two IP addresses are whitelisted (Main VPN server, Fall Back VPN server).
- While whitelisting, the client can set-up additional security by setting-up access rules allowing connection from our VPN server's IP address to one or more specific internal IP addresses associated with the application(s) under test. This will restric/deny access to all other IP addresses (systems).