



Hosting and Installation Security

The QSI Inc. Hosting Facility is protected by a security system and is not open to the public.

Power to the climate controlled server room is conditioned through a redundant battery backup/power supply system, which is in turn connected to an automatic transfer switch. The automatic transfer switch is connected to both the local power grid and to a commercial grade Cummins Owens natural gas powered generator. The generator system is under service contract, is automatically exercised weekly, and is professionally checked every three months.

The redundant compressor air conditioning system is also under service contract.

The hosting facility is connected directly to the fiber optic network of Level 3 Communications. Level 3 is one of the largest Tier 1 backbone providers in the world, and it recently merged with another Tier 1 provider, Global Crossing.

The router is configured to block certain ports to protect the network from unwanted traffic and intruders. In addition, security updates are applied to its servers on a regular basis, and all of the web servers are configured to evaluate every URL request and block requests that match known patterns of exploits.

Virus protection is Symantec Endpoint protection, which is under contract.

Other Notes on Security

TCP/IP port filtering is the practice of selectively enabling or disabling Transmission Control Protocol (TCP) ports and User Datagram Protocol (UDP) ports on computers or network devices. When used in conjunction with other security practices, such as deploying firewall software at your Internet access point, applying port filters to intranet and Internet servers insulates those servers from many TCP/IP-based security attacks, including internal attacks by malicious users. An Internet or intranet host, such as a computer or network device on a TCP/IP-based network, uses a combination of an IP address and port number to communicate with an application or service running on another Internet or intranet host. Together, an IP address and port number make up a *socket*. Because TCP/IP hosts are assigned a unique IP address, and standard TCP/IP-based applications and services typically use a specific TCP or UDP port number, sockets can direct communications between specific applications or services running on specific hosts.