squire technologies
the signalling specialists to the telecoms industry

Product Security Policy

Squire Technologies Ltd – Product Security Policy

Squire Technologies products are specialised ‘black box’ Telecommunications systems intended for use within secure networks with suitable firewall protection and access control. Suitable access control and security protection should be put in place by the customer who is using the Squire product.
Squire products are hardened with particular minimal install Linux OS and kernel versions which are installed either by Squire Technologies or by the customer using Squire Technologies installation instructions. The Linux OS and kernel versions should not be changed. Squire Technologies do not recommend installing Linux updates or patches. If there is a particular security concern or vulnerability then Squire Technologies may issue a security advisory or provide specific advice but this will be on a case by case basis.
For Session Border Controller (SBC) product installations, Squire Technologies will assist the customer with the implementation of security hardening through IP tables configuration, user account password changes and installation of Fail2ban intrusion protection however the customer is ultimately responsible for the security of the Squire product in their network and Squire Technologies cannot be held responsible in any way for security breaches.

Squire Technologies are not responsible for Operating System administration.
If there is a specific need for security hardening on a purchased product then this requirement should be discussed with the Squire Technologies commercial and technical teams.