QUANN PROTECT

QUANN SECURITY DEVICE MANAGEMENT

Keep your security devices patched and working effectively without the need for in-house specialist skills

The proper management of security devices is critical in meeting the cybersecurity needs of a dynamic business environment and protecting the organisation's assets. As cyber threats evolve, the devices have to be maintained and upgraded on a continual basis to ensure that vulnerabilities are not exploited. This involves intensive effort and highly specialised skills, which organisations may not have or may find costly to maintain.

QUANN SECURITY DEVICE MANAGEMENT

QUANN Security Device Management provides organisations with a full suite of services to help manage your security devices without having to build up the capabilities in-house. Delivered by QUANN's highly-skilled and experienced team of security experts, it encompasses device maintenance, configuration, backups, software upgrades and patching, and 24x7 monitoring through QUANN next-generation Security Operations Centres.

FEATURES

Network security device management

- Security devices such as Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), Security Information and Event Management (SIEM) systems, United Threat Management (UTM) systems, Virtual Private Networks (VPN) and Web Application Firewalls are updated and patched to protect them against internal and external threats.
- We ensure that the perimeter defence is properly configured and regularly maintained, and work closely with your organisation to reduce the attack surface of your network.

Content security device management

- We centralise management and reporting functions across multiple email and web security appliances.
- We simplify administration and planning, improve compliance monitoring, help enable consistent enforcement of policy and enhance threat protection.
- Enterprise content is also protected across common hosting services such as the cloud.

Endpoint device management

- We provide real-time protection against malware and other threats on devices such as remote or removable drives, mobile devices and other advanced endpoints.
- The devices are scanned for dormant threats and a series of health audits is carried out to provide them with proactive protection.

BENEFITS

Reduces operational costs

By leveraging security expertise from QUANN, organisations do not have to worry about training in-house security personnel or dealing with the overheads involved in round-the-clock security device monitoring and maintenance.

Minimises business risk

We ensure that all security devices are regularly maintained and patched, and that they are securely deployed and configured. This prevents vulnerabilities from being exploited and helps organisations reduce business risk arising from cyber threats.

Delivers peace of mind with 24x7 in-country support

QUANN's regional network of Security Operations Centres provides in-country monitoring 24.7.365 to ensure vigilance and protection against threats.

QUANN
THE ART AND SCIENCE OF BEING CYBER SECURE

For more information, please contact us at **info@quannsecurity.com**
or visit our website at **quannsecurity.com**