QUANN PROTECT

QUANN ENDPOINT PROTECTION

Be proactive and stop malware before it can execute its payload

Organisations face a huge security challenge today with the sheer number of devices connected to the Internet of Things, the growing number of mobile employees connecting to the corporate network from outside its perimeter, and the widespread use of external devices such as USB drives. It is very difficult for an organisation to ensure that the software on all these devices is updated with the latest patches, and attackers can take advantage of these vulnerabilities to launch zero day attacks.

QUANN ENDPOINT PROTECTION

QUANN Endpoint Protection prevents known and unknown malware-driven attacks and sophisticated vulnerability exploits using a combination of behavioural-based techniques, machine-learning capabilities and real-time analysis of endpoint processes and threats. It moves protection up the attack chain to focus on the core techniques that every attacker must link together in order to execute an attack, thereby stopping malware before it can execute its payload. Backed by a dedicated team of Quann expert security analysts, we ensure that your endpoints are protected 24.7.365.

FEATURES

Continuous real-time monitoring and machine-learning

- All end points are monitored unobtrusively in real time, all the time.
- Vast volumes of data are captured for forensics analysis during attempted attacks to generate actionable intelligence.
- Machine-learning enables the intelligence to be applied proactively to defend other endpoints instead of relying on traditional signature-based approaches to security.
- The endpoints can be locked down to prevent attackers from moving laterally within the network to cause more harm.

Rapid deployment

- The service uses a smart and lightweight agent that can be integrated into existing operations with minimal or no disruption.
- The agent can be deployed within hours (instead of days), is highly scalable and invisible to end users.

Multi-layered approach to stopping malware

- Policy-based restrictions prevent specific execution scenarios such as running a particular file type directly from a USB drive.
- Unknown files are inspected, analysed and submitted to the global threat community for assessment.
- Malware techniques such as thread injection are blocked and systems locked down to prevent access by attackers.

BENEFITS

Protects endpoints against known and unknown threats in real-time

By using a combination of Indicator of Compromise behavioural blocking, advanced malware protection with machine-learning capabilities, and real-time analysis of endpoint processes and threats, we are able to prevent attacks without requiring any prior knowledge of the threat.

Proactively prevents similar attacks on other end points

Security intelligence is generated through detailed forensics of threat data, enabling defences to be applied to other unprotected endpoints, thereby preventing contagion.

Delivers better visibility with holistic approach to endpoint protection

The service can be integrated with existing security appliances and with cloud and network security. This allows threat data to be exchanged in real time to enhance cross-organisation protection.

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**