schools broadband™

Endpoint Protection

Protect your school's devices from cyber attacks everywhere

Malware and ransomware form some of the most prevalent threats to schools and MATs, with Endpoints (devices) being the primary target for most cyberattacks. And as technology infrastructures grow in complexity, schools and MATs struggle to find the expertise and resources necessary to manage security risks.

Using real-time threat intelligence and the latest machine-learning algorithms, our core Anti-Virus service (EPP), is a new approach to protection. For even greater protection, our Endpoint Protection Detection and Response (EPDR), automates the prevention, detection, containment and response to advanced threat, zero day malware, ransomware, phishing, in-memory exploits, fileless and malwareless attacks, inside and outside your school network.

WatchGuard®

The iSPAs
6 x ISPA Award
WINNER

Easy to Use and Manage

Endpoint Security portfolio handles all needs of your endpoint protection in a remarkably simple way from a single web console

Easy to set up

Cross-platform endpoint management from a single pane of glass

Clean, user-friendly interface design that can be quickly mastered

Simplifies and Maximises Security

Automated services reduce costs of expert personnel

No false alerts to manage, no time wasted on manual settings

No management infrastructure to install, configure or maintain

Endpoint performance is not impacted since it is based on a lightweight agent and Cloud-native architecture

Supported Platforms and Systems

Supported operating systems: Windows (Intel & ARM), macOS (Intel & ARM), Linux and Android. Compatible browsers: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge and Opera.

EPP & EPDR

WatchGuard EPDR integrates traditional endpoint technologies with innovative, adaptive protection and EDR technologies in one single solution. Unlike other solutions, it combines the widest range of endpoint protection technologies (EPP) with automated detection and response (EDR) capabilities. It also has two services, managed by WatchGuard experts, that are delivered as a feature of the solution:

Zero-Trust Application Service: 100% classification of the applications

Threat Hunting Service: detecting hackers and insiders

Features	EPP	EPDR
Device Control	✓	✓
Automatic updates	✓	✓
Automatic discovery of unprotected endpoints	✓	✓
Patch Management for OS and third-party applications	✓	✓
Security for VPN connections (requires Firebox)	✓	✓
Centralised Cloud-based console	✓	✓
Ability to configure and apply settings on both group and endpoint basis	✓	✓
Ability to assign preconfigured roles to console users	✓	✓
Ability to assign custom permissions to console users	✓	✓
Ability to customise local alerts	✓	✓
User activity auditing	✓	✓
On-demand and scheduled reports at different levels and with multiple granularity options	✓	✓
Threat Hunting Service (indicators of attack)		✓
Incident graphs and lifecycle information available from the web console		✓
Ability to export lifecycle information for local analysis		✓
Advanced Visualization Tool (add-on)		✓
Discovery and monitoring of unstructured personal data across endpoints (add-on)		✓
Advanced attack investigation (Jupyter Notebooks)		✓
Lock mode in the Advanced Protection		✓
Anti-exploit technology		✓
Block programs by hash or name (pe.: PowerShell)		✓