Endpoint Security (EPP Solution)

Perfect for small business

Secure your devices from malware and ransomware

In the ongoing battle to defend your business, the endpoint is a favorite target for cyber criminals. This means that it is more important than ever to protect and monitor all endpoints that handle sensitive information and connect to systems both inside and outside the business network.

CyberCision Endpoint Security is an effective Cloud-native security solution that centralizes next-generation antivirus for all your Windows, macOS and Linux desktops, laptops, and servers, in addition to the leading virtualization systems and Android devices. This complete protection covers all vectors: network (firewall), email, web, and external devices.

Multiple Platforms

High performance and minimal device impact

Simple to set up and manage

A simple, affordable and effective solution to secure computers, smart phones and servers from advanced malware and ransomware attacks

Powered by world's leading solutions for small business

WatchGuard

CyberCision

Endpoint Security (EPP Solution)

Perfect for small business

Features

Centralized Device Security
Centralized management of security and product updates for all workstations and servers on the corporate network. Manage the protection of Windows, Linux, macOS and Android devices from a single web-based administration console.

Malware and Ransomware Protection
WatchGuard EPP analyzes behaviors and hacking techniques to detect and block both known and unknown malware, as well as ransomware, trojans and phishing.

Advanced Disinfection
In the event of a security breach, WatchGuard EPP allows enterprises to quickly restore affected computers to the state they were in before the infection with advanced disinfection tools and quarantine, which stores suspicious and deleted items. It also allows administrators to remotely restart workstations and servers to ensure they have the latest product updates installed.

Real-Time Monitoring and Reports
Detailed, real-time security monitoring is delivered via comprehensive dashboards and easy-to-interpret graphs. Reports are automatically generated and delivered on protection status, detections and improper use of devices.

Granular Configuration of Profiles
Assign specific protection policies by user profiles, guaranteeing the application of the most appropriate policy for every group of users.

Centralized Device Control
Stop malware and information leaks by blocking entire device categories (flash drives, USB modems, webcams, DVD/CD, etc), allow listing devices or configuring read-only, write-only, and read-and-write access permissions.

Fast, Flexible Installation
Deploy the protection via email with a download URL, or silently deploy to selected endpoints via the solution's distribution tool. MSI installer is compatible with third-party tools (Active Directory, Tivoli, SMS, etc).

Malware Freezer
Malware Freezer quarantines detected malware for seven days and, in the event of a false positive, automatically restores the affected file to the system.

ISO 27001 and SAS 70 Compliance Guaranteed 24/7
The solution is hosted on WatchGuard Cloud with complete data protection guaranteed. Our data centers are ISO 27001 and SAS 70 certified, allowing customers to avoid costly service outages and malware infections. Contact your authorized WatchGuard reseller or visit www.watchguard.com to learn more.

The Watchguard Unified Security Platform™
Supported platforms and systems requirements of Watchguard EPP Supported operating systems: Windows (Intel & ARM), macOS (Intel & ARM), Linux and Android. List of compatible browsers: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge and Opera.

Benefits

Multiplatform Security
- Security against unknown advanced threats: detects and blocks malware, trojans, phishing and ransomware.
- Security for all attack vectors: browsers, email, file systems, and external devices connected to endpoints.
- Automatic analysis and disinfection of computers.
- Behavioral analysis to detect known and unknown malware. Cross-platform security: Windows systems, Linux, macOS, Android and virtual environments (VMware, Virtual PC. MS Hyper-V, Citrix). Management of licenses belonging to both persistent and non-persistent virtualization infrastructure (VDI).

Simplify Management
- Easy to maintain: no specific infrastructure required to host the solution; the IT department can focus on more important tasks.
- Easy to protect remote users: each computer protected with WatchGuard EPP communicates with the Cloud; remote offices and users are protected quickly and easily, with no additional installations.
- Easy to deploy: multiple deployment methods, with automatic uninstallers for competitors' products to facilitate rapid migration from third-party solutions.
- Smooth learning curve: intuitive, simple web-based management interface, with most-frequently used options one click away.

Lower Impact on Performance
- The agent has minimal network, memory and CPU usage, since all operations are performed in the Cloud.
- WatchGuard EPP requires no installation, management or maintenance of new hardware resources in the organization's infrastructure.