DATASHEET

WATCHGUARD EPP

Strong Endpoint Protection Platform

CYBERSECURITY CHALLENGES

In the ongoing battle to defend your organization, 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 corporate network.

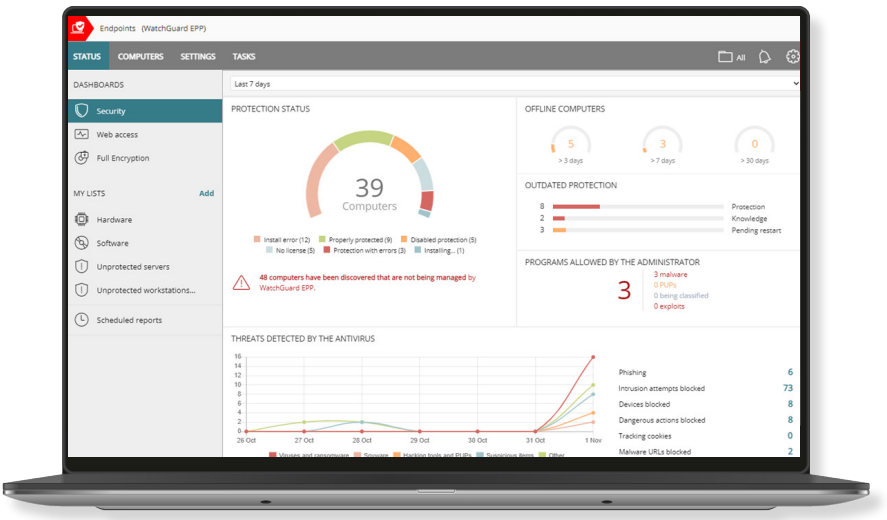
In fact, last year over 350,000 new malicious programs were being registered every day. Hackers are targeting vulnerable endpoints, where enterprises store their most valuable assets. The reason? As is so often the case, for economic gain. Malware and ransomware have become some of the most prevalent threats, although paradoxically, the direct costs are not the main problem – rather, it is the downtime they cause. This is forcing enterprises to adopt measures to improve their security posture.

PROTECT YOUR COMPANY AGAINST MALWARE AND RANSOMWARE

The increasing exposure of companies to new types of malware and threats endangers their security posture, requiring new approaches to help reduce the impact of possible attacks.

WatchGuard EPP 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.

It includes a set of EPP technologies to prevent malware, ransomware and the latest threats. One of these technologies checks in real time the WatchGuard Threat Intelligence, a huge repository being fed by the latest machine-learning algorithms, to detect malicious attacks faster.



BENEFITS

Multiplatform Security

- Security against unknown advanced threats: detects and blocks malware, trojans, phishing and ransomware.
- Automatic analysis and disinfection of computers. Behavioral analysis to detect known and unknown malware.
- Cross-platform security: Windows systems, Linux, macOS, iOS, 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 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, its lightweight agent has no impact on endpoint performance, simplifying security management and increasing operational efficiency.

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, iOS 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.), allowlisting 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.

ENDPOINT RISK MONITORING

Manage and monitor unprotected endpoints, indicators of attack, security misconfigurations, OS and third-party software vulnerabilities, and missing patches to proactively safeguard your network before a breach occurs.

VULNERABILITY ASSESSMENT

Vulnerability assessment is a critical process that helps IT teams identify, evaluate, and prioritize security weaknesses and vulnerabilities in applications and systems. Understand and identify potential threats and take proactive measures to mitigate them before being exploited by attackers.

RANSOMWARE REMEDIATION & RECOVERY

To prevent the recovery of a corrupted system, apart from encrypting files, adversaries try to delete backup and VSS files created by admins and turn off services designed to help recovery.

The shadow copies feature leverages the operating system technology, and it will protect these files using our anti-tampering technology so users will be able to recover the information after a ransomware attack.

IT professionals use shadow copies to recover files from critical system failures, but it is also an excellent technology for recovering files encrypted by ransomware.

Supported platforms and systems requirements of Watchguard EPP

Supported operating systems: Windows (Intel & ARM), macOS (Intel & ARM), Linux, iOS and Android.

List of compatible browsers:
Google Chrome, Mozilla Firefox, Safari and Microsoft Edge

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com WatchGuard Technologies, Inc.

Part No. WGCE67474_050523