# WATCHGUARD FULL ENCRYPTION

**The first line of defense to protect data simply and effectively**

According to Gartner,[1] a laptop is stolen every 53 seconds. The growing amount of data stored on endpoints has clearly increased interest in this data, along with the risk of suffering a data breach through the loss, theft or unauthorized access to information.

This has led regulations such as the GDPR[2] in the European Union and the CCPA[3] in the United States to become more demanding in an effort to reduce the increasing likelihood of loss, theft or unauthorized access to data and the serious economic impact this entails.

## CENTRALLY STRENGTHEN SECURITY AGAINST UNAUTHORIZED ACCESS

One of the most effective ways of minimizing data exposure is to automatically encrypt the hard drives on desktops, laptops and servers. This way, access to data is secure and complies with established authentication mechanisms. Establishing encryption policies provides an additional layer of security and control for organizations, although it may also lead to data control and recovery issues if the key is lost.

**WatchGuard Full Encryption** leverages BitLocker, a proven and stable Microsoft technology, to encrypt and decrypt disks without impacting end users. It provides organizations with the added value of centrally controlling and managing the recovery keys stored on WatchGuard Cloud-based management platform.
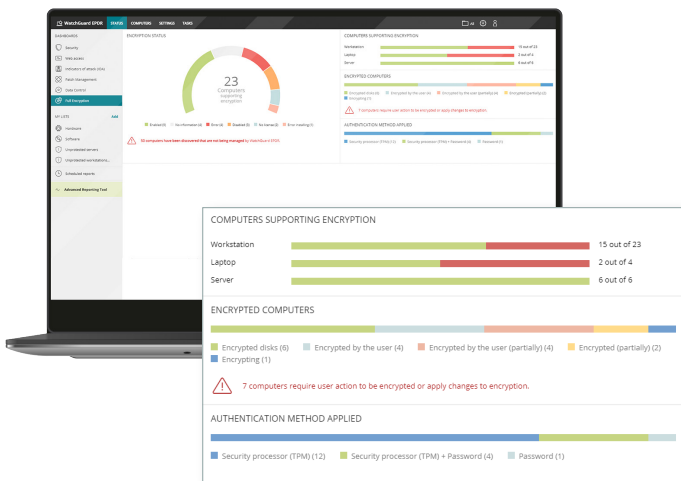


*WatchGuard Full Encryption dashboard in WatchGuardr's web management console with key indicators of the encryption status of endpoints across the organization.*

## BENEFITS

### Prevent loss, theft and unauthorized access to data without impacting users

- Encrypt your disks and protect their content against theft, accidental loss and malicious insiders. Data encryption, decryption and access are automatic, immediate, and seamless to users.

- For your convenience, recovery keys are stored and recovered securely from the Cloud platform and its web console.

### No deployment or installation. No servers or additional costs Zero problems.

- **WatchGuard Full Encryption** centrally manages BitLocker, a proven and widely used Windows technology.

- BitLocker is included out of the box in most Windows operating systems, and with WatchGuard's Cloud platform web console you'll have a single centralized place to manage your devices.

- You won't need to deploy or install another agent. All WatchGuard Endpoint Security solutions share the same lightweight agent.

- The ability to centrally manage recovery keys from the Cloud means you don't have to install or maintain servers to manage them.

- **WatchGuard Full Encryption** can be enabled immediately and is easily managed through WatchGuard Cloud's user-friendly interface.

### Regulatory compliance, reports and central management

- **WatchGuard Full Encryption** aids and simplifies compliance with data protection regulations by monitoring and enforcing BitLocker activation on Windows devices.

- All WatchGuard Endpoint Security solutions provide intuitive dashboards, detailed reports and change audits.

- Additionally, its role-based management allows administrators to implement different authorization levels and different policies for groups and devices from a single centralized web console.
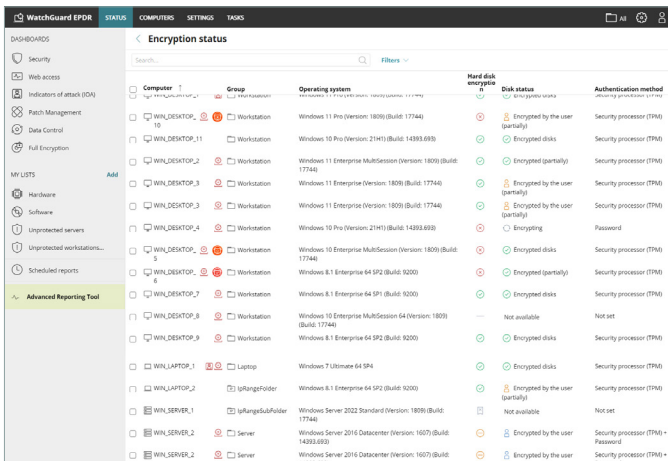
## SECURE USB FLASH DRIVES

Over the past year, worldwide pen drive use has grown, especially in industrial organizations, increasing by 30%. Cyberattackers noticed this trend and use USB drives as a point of entry to gain access to a system and infect all or part of your network.

As a result, organizations are more likely to suffer data breaches or unauthorized access to sensitive information. According to a study by Forrester, [4] the loss or theft of assets like laptops or USB drives involved 20% of data breaches reported by global security decision-makers in 2020.

The first step to minimizing the risk of threats is to have a strict policy with guidelines for USB drive use in the organization, role levels, and permissions based on staff profiles, only using devices provided and verified by the organization's IT team or MSP.

However, these guidelines may not be sufficient in the face of growing cyber threats. **WatchGuard Full Encryption** provides maximum data protection on all encrypted endpoints by enabling pre-boot authentication that verifies the user's identity before the operating system loads, preventing laptops from loss, theft, and unauthorized access to data this way.



*Computer list showing encryption status, the groups they belong to, their operating system and the authentication method used.*

## KEY FEATURES

The trend towards hybrid work models, either working remotely or from the office, makes full-disk encryption a crucial first line of defense for devices like laptops and USB drives.

**WatchGuard Full Encryption** is an additional module for WatchGuard Endpoint Security solutions, designed to centrally manage full disk encryption that enables the following features:

### Full Drive Encryption and Decryption

**WatchGuard Full Encryption** leverages BitLocker to fully encrypt the drives of your Windows laptops, desktops, servers, and removable storage drives. **WatchGuard Full Encryption** dashboard provides global visibility into compatible network endpoints, their encryption status and the authentication method used, and enables administrators to assign encryption settings and restrict encryption permissions.

### Centralized Management of Recovery Keys

If the access key is forgotten, or there are changes in the boot sequence, BitLocker will ask for a recovery key to start up the affected system. If required, the network administrator can get the recovery key through the management console and send it to the user.

### Lists, Reports, Centralized Policy Application

The computer list in the console allows administrators to apply multiple filters based on encryption status. These lists can be exported for data analysis with external tools.

Define encryption policies from the console and view policy changes through audit reports you can present to regulatory bodies and institutions if required.

---

[1] TechSpective

[2] GDPR - General Data Protection Regulation: Forces organizations to ensure the personal information they process is protected. Failure to comply with it can result in severe fines and indirect damages.

[3] CCPA - California Consumer Privacy Act of 2018: This is the first United States law following in the footsteps of the European Union's GDPR. It applies to businesses based in California and businesses based outside the state.

[4] The State Of Privacy And Data Protection, 2021 - Forrester

**Supported platforms and systems requirements of WatchGuard Full Encryption**

**Compatible with WatchGuard EPDR, WatchGuard EDR and WatchGuard EPP Supported operating systems:** Windows.

**List of compatible browsers:** Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge and Opera.

---