



WatchGuard Full Encryption

The first line of defense to protect data simply and effectively

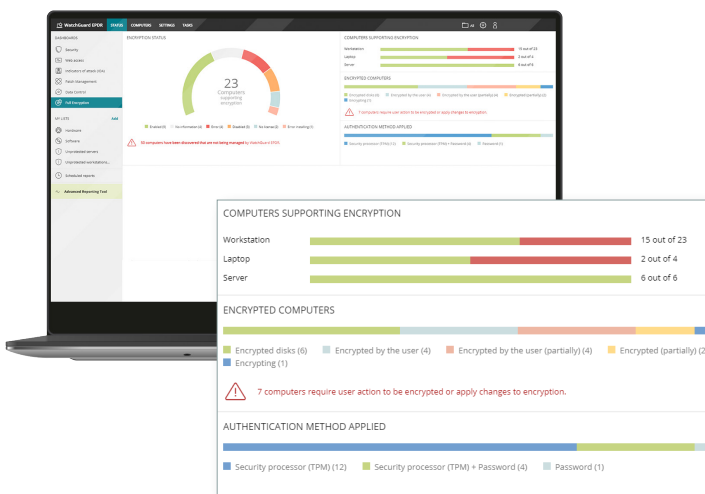
According to Gartner,¹ a laptop is stolen every 53 seconds. The growing amount of data stored on endpoints has clearly increased interest in this data, along with the risk of suffering a data breach through the loss, theft or unauthorized access to information.

This has led regulations such as the GDPR² in the European Union and the CCPA³ 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 protects Windows and macOS devices with full disk encryption against potential data breaches and unauthorized access. It leverages BitLocker on Windows operating systems or FileVault on macOS systems to encrypt and decrypt disks without impacting end users, providing organizations with the added value of centrally controlling and managing the recovery keys stored on WatchGuard Cloud management platform.



WatchGuard Full Encryption dashboard in WatchGuard'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.

- BitLocker comes pre-installed in most Windows operating systems, while FileVault is included in most macOS devices. With WatchGuard's Cloud platform web console, you will have a single centralized location to manage all your devices.
- You won't need to deploy or install another agent. All WatchGuard Endpoint Security solutions share the same lightweight agent.
- **WatchGuard Full Encryption** can be enabled immediately and is easily managed from the Cloud console.

Regulatory compliance, reports and central management

- **WatchGuard Full Encryption** aids and simplifies compliance with data protection regulations by monitoring and enforcing data encryption.
- **WatchGuard Full Encryption** leverages BitLocker or FileVault allowing admins to set up encryption policies and centrally manage recovery keys from the Cloud.
- All WatchGuard Endpoint Security solutions provide intuitive dashboards, detailed reports, and user activity logs for audits.

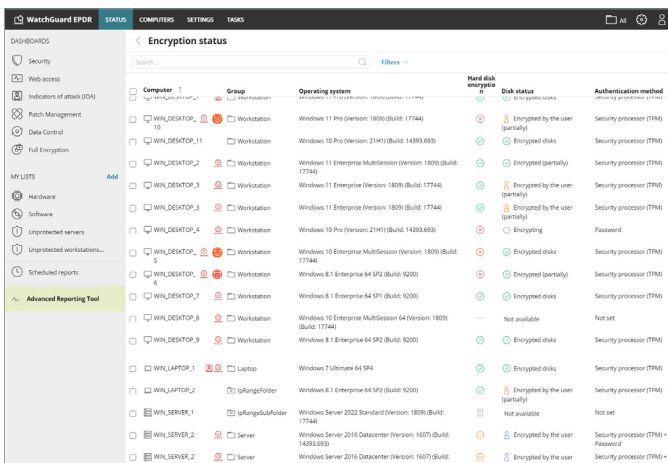
Secure USB Fash Drives*

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 the network.

As a result, organizations are more likely to suffer data breaches or unauthorized access to sensitive information. According to a study conducted by Forrester,⁴ the loss or theft of assets like laptops or USB drives involved 17% of data breaches reported in 2023.

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	Group	Operating system	Hard disk encryption	Disk status	Authentication method
WIN_DESKTOP_1	Workstation	Windows 11 Pro (Version: 1809) (Build: 17744)	Encrypted by the user (partially)	Security processor (TPM)	Security processor (TPM)
WIN_DESKTOP_10	Workstation	Windows 10 Pro (Version: 21H1) (Build: 14393.688)	Encrypted disks	Security processor (TPM)	Security processor (TPM)
WIN_DESKTOP_11	Workstation	Windows 10 Pro (Version: 21H1) (Build: 14393.688)	Encrypted disks	Security processor (TPM)	Security processor (TPM)
WIN_DESKTOP_2	Workstation	Windows 11 Enterprise MultiSession (Version: 1809) (Build: 17744)	Encrypted (partially)	Security processor (TPM)	Security processor (TPM)
WIN_DESKTOP_3	Workstation	Windows 11 Enterprise (Version: 1809) (Build: 17744)	Encrypted by the user (partially)	Security processor (TPM)	Security processor (TPM)
WIN_DESKTOP_3	Workstation	Windows 11 Enterprise (Version: 1809) (Build: 17744)	Encrypted by the user (partially)	Security processor (TPM)	Security processor (TPM)
WIN_DESKTOP_4	Workstation	Windows 10 Pro (Version: 21H1) (Build: 14393.688)	Encrypting	Password	Password
WIN_DESKTOP_5	Workstation	Windows 10 Enterprise MultiSession (Version: 1809) (Build: 17744)	Encrypted disks	Security processor (TPM)	Security processor (TPM)
WIN_DESKTOP_6	Workstation	Windows 8.1 Enterprise (Version: 1809) (Build: 9200)	Encrypted (partially)	Security processor (TPM)	Security processor (TPM)
WIN_DESKTOP_7	Workstation	Windows 8.1 Enterprise 64 SP1 (Build: 9200)	Encrypted disks	Security processor (TPM)	Security processor (TPM)
WIN_DESKTOP_8	Workstation	Windows 10 Enterprise MultiSession (Version: 1809) (Build: 17744)	Not available	Not set	Not set
WIN_DESKTOP_9	Workstation	Windows 8.1 Enterprise 64 SP2 (Build: 9200)	Encrypted disks	Security processor (TPM)	Security processor (TPM)
WIN_LAPTOP_1	Laptop	Windows 7 Ultimate 64 SP4	Encrypted disks	Security processor (TPM)	Security processor (TPM)
WIN_LAPTOP_2	UplungFolder	Windows 8.1 Enterprise 64 SP2 (Build: 9200)	Encrypted by the user (partially)	Security processor (TPM)	Security processor (TPM)
WIN_SERVER_1	UplungSubFolder	Windows Server 2022 Standard (Version: 1809) (Build: 17744)	Not available	Not set	Not set
WIN_SERVER_2	Server	Windows Server 2016 Datacenter (Version: 1607) (Build: 14393.688)	Encrypted by the user	Security processor (TPM) + Password	Security processor (TPM) + Password
WIN_SERVER_2	Server	Windows Server 2016 Datacenter (Version: 1607) (Build: 14393.688)	Encrypted by the user	Security processor (TPM) + Password	Security processor (TPM) + Password

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 encrypts the drives of your Windows and macOS laptops, desktops, servers, and removable storage drives (Windows only). **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. For macOS, if the user password is forgotten, FileVault will also ask for a recovery key to start up the system. In both cases, if required, the network administrator can get the recovery keys through the management console and send them 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 Security, 2023 - Forrester

* External and USB flash drives encryption and decryption are supported in Windows operating systems only.

Supported platforms and systems requirements of WatchGuard Full Encryption

Compatible with WatchGuard Advanced EPDR, WatchGuard EPDR, WatchGuard EDR and WatchGuard EPP Supported operating systems:

[Windows and macOS.](#)

List of compatible browsers: [Google Chrome](#), [Mozilla Firefox](#), [Safari](#), and [Microsoft Edge](#).