

WatchGuard Full Encryption



DATASHEET

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.

2 WatchGuard D/DR 104	COMPLETING SUTTING TANS		□~ ◎ 8	
Extrements O Security	BIONTON STATUS		COMPLETES SUPPORTING INCOMPONY Victorian Victo	
VHO AGANE VHO AGANE VHO AGANE VHO AGANE VHO AGANE VHO AGANE VHO AGANE			Severe Gaude	
Oute Control	23 Compu- terry	iters	E forsystel des 15 III. Servystel fyrhe vervill III. Servystel ty the verville PI III. E forsystel participation (201	
orien AA	I Dabelji - Norferenceji - Gravji - S	natad () = balanas() = bro readry()		
Sobers C Sobers	🛆 13 surguines have been decouved that are not being the	nggal by WatchDarry (1958).	🖩 Security processer (1965) / 2) 📲 Security processer (1965 + Nacoured J) 👘 Intersered (1)	
 Unprosense workshore. Scheskulet reports 				
$\sim~$ Advanced Reporting Tesl	_			
	cc	MPUTERS SUPPORTI	NG ENCRYPTION	
	Wo	irkstation		15 out of
		otop		2 out of 4
		ver 🗾		2 out of 4 6 out of 6
	Ser		15	
	Ser	Ver		6 out of 6
	EN	Ver	IS Encrypted by the user (4) Encrypted by the user (partially) (4)	6 out of 6
	EN	ICRYPTED COMPUTER		6 out of 6
	Ser EN EN	ICRYPTED COMPUTER	Encrypted by the user (4) Encrypted by the user (partially) (4) re user action to be encrypted or apply changes to encryption.	6 out of 6

8

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.

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

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.

WatchGuard EPDR STATU	<i>к</i> (COMPUTERS SETTINGS	TASIIS				⊡⊴ © 2	
DASHBOARDS	<	Encryption sta	tus					
Security		Search Q Filters ~						
Web access		Computer 1	Group	Operating system	Hard disk encryptio n	Disk status	Authentication method	
			I THURSDOOL	TELEVISTIC PERMIT	U	C Dicyprecions	accurry processor (17m)	
Patch Management Data Control	0	WIN_DESKTOP_ 🧕	🧿 🗀 Workstation	Windows 11 Pro (Version: 1809) (Build: 17744)	۲	Encrypted by the user (partially)	Security processor (TPM)	
Full Encryption	Π	WIN_DESKTOP_11	UWrkstation	Windows 10 Pro (Version: 21H1) (Build: 14393.693)	\odot	 Encrypted disks 	Security processor (TPM)	
MY LISTS Add		WIN_DESKTOP_2	Workstation	Windows 11 Enterprise MultiSession (Version: 1809) (Build: 17744)	Ø	 Encrypted (partially) 	Security processor (TPM)	
Hardware	0	WIN_DESKTOP_3	O 🗋 Workstation	Windows 11 Enterprise (Version: 1809) (Build: 17744)	0	Encrypted by the user (partially)	Security processor (TPM)	
G Software		WIN_DESKTOP_3	🧟 📋 Workstation	Windows 11 Enterprise (Version: 1809) (Build: 17744)	Ø	Encrypted by the user (partially)	Security processor (TPM	
Unprotected servers	Π	WIN_DESKTOP_4	🙆 🗋 Workstation	Windows 10 Pro (Version: 21H1) (Build: 14393.693)	۲	 Encrypting 	Password	
Unprotected workstations	0	WIN_DESKTOP_ 🧕	Workstation	Windows 10 Enterprise MultiSession (Version: 1809) (Build: 17744)	۲	 Encrypted disks 	Security processor (TPM)	
Scheduled reports	0	WIN_DESKTOP_ 🧕 6	Workstation	Windows 8.1 Enterprise 64 SP2 (Build: 9200)	۲	 Encrypted (partially) 	Security processor (TPM	
Advanced Reporting Tool	0	WIN_DESKTOP_7	Workstation	Windows 8.1 Enterprise 64 SP1 (Build: 9200)	0	 Encrypted disks 	Security processor (TPM	
		WIN_DESKTOP_8	Q 🗋 Workstation	Windows 10 Enterprise MultiSession 64 (Version: 1809) (Build: 17744)		Not available	Not set	
	0	WIN_DESKTOP_9	🧕 🗋 Workstation	Windows 8.1 Enterprise 64 SP2 (Build: 9200)	0	 Encrypted disks 	Security processor (TPM	
	0	WIN_LAPTOP_1	🧿 🖿 Laptop	Windows 7 Ultimate 64 SP4	0	 Encrypted disks 	Security processor (TPM	
	п	WINJLAPTOP_2	DipRangeFolder	Windows 8.1 Enterprise 64 SP2 (Build: 9200)	0	8 Encrypted by the user (partially)	Security processor (TPM	
	0	WIN_SERVER_1	IpRangeSubFolder	Windows Server 2022 Standard (Version: 1809) (Build: 17744)	E	Not available	Not set	
	0	WIN_SERVER_2	🧕 🗋 Server	Windows Server 2016 Datacenter (Version: 1607) (Build: 14393.693)		Encrypted by the user	Security processor (TPM Password	
	0	WIN_SERVER_2	🧕 🗀 Server	Windows Server 2016 Datacenter (Version: 1607) (Build: 14293-693)		8 Encrypted by the user	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.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. © 2023 WatchGuard Technologies, Inc. All rights reserved. Watch-Guard, the WatchGuard logo are trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE67519_112923