Business

ENDPOINT ENCRYPTION

ENDPOINT ENCRYPTION · POWERED BY SOPHOS

If the laptop walks, the data stays safe

Protect your critical corporate data on lost or stolen devices without slowing down your workforce.

- Disk encryption & data tracking
- Granular compliance tracking
- Self-service recovery
- Automatic recovery key rotation
- Secure file sharing
- Centralised Cloud management

THE CHALLENGE

A Lost Laptop Is A Data Breach

Devices go missing every day. On an unencrypted drive, every file is readable by whoever finds it. Under POPIA, that can also become a reportable incident.

THE SOLUTION

Encryption That Runs Itself

Endpoint Encryption manages the encryption already built into Windows (BitLocker) and macOS (FileVault) from one console. Protection switches on silently — no new servers, no drop in performance.

Enterprise-grade encryption, without the enterprise overhead.

BUILT ON TRUSTED FOUNDATIONS

Microsoft BitLocker and Apple FileVault, managed centrally through the Sophos Central platform.

AT A GLANCE

What's Included With Every Encryption Licence

The Encryption Platform
Full-disk encryption for every Windows and macOS device, plus AES-256 secure file sharing.

The Management Console
One Sophos Central dashboard for policy, live device status and exportable reports.

Six Reasons You Need It

>> Your data stays secure 01

Data on a missing laptop stays unreadable and an inconvenience to replace, not a reportable POPIA incident.

>> Nothing new to run 02

It switches on encryption your operating systems already have. No new infrastructure to buy or maintain.

>> One standard across devices 03

Windows and Mac are protected to the same level, so no device is left as the weak link.

>> IT stops being the bottleneck 04

Locked-out users get themselves back to work, freeing your team from routine recovery tickets.

>> Compliance you can prove 05

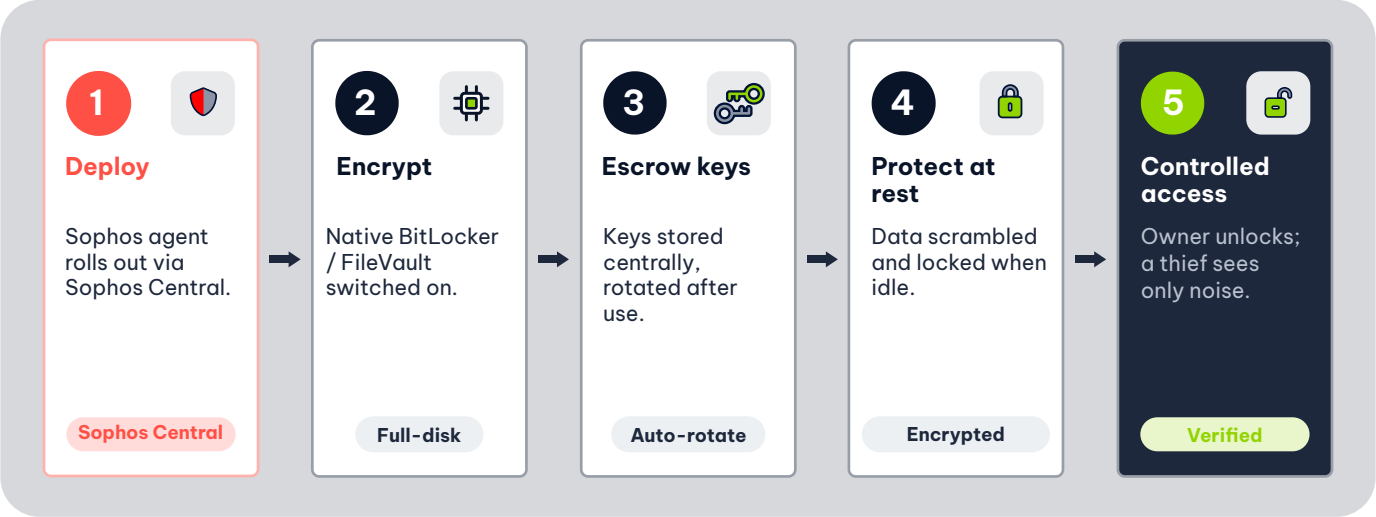
When an auditor asks which devices are encrypted, the evidence is minutes away and not a fire drill.

>> One less silo to manage 06

Encryption lives in the same platform as your other Sophos Security, not in yet another tool.

Five Steps, One Encrypted Fleet

From rollout to recovery, every device follows the same protected path.



PROTECT your critical corporate data

KEY FEATURES

The Full Feature Set

	FEATURE	WHAT IT DOES FOR YOU
01	**Full-Disk Encryption**	Manages native BitLocker (Windows) and FileVault (macOS) to encrypt the entire drive.
02	**Secure File Sharing**	Password-protected, AES-256 encrypted files up to 50MB, for internal and external recipients.
03	**Compliance Reporting**	Real-time exportable reports of encryption status across every managed device.
04	**Self-Service Recovery Portal**	Locked-out users retrieve their own recovery key from a secure, web-based portal.
05	**Automatic Key Rotation**	Recovery keys are single-use and rotate automatically after each use.
06	**Sophos Central Management**	Encryption policy, device status and key recovery, all from the unified console.

REAL-WORLD USE CASES

Built For How You Work

USE CASE 01
Financial & Professional Services

Client data on partner laptops stays protected off-site, and encryption reports are produced on demand for auditors.

USE CASE 02
Healthcare

Patient records on mobile workstations stay unreadable if a device goes missing, supporting POPIA obligations.

USE CASE 03
Field & Remote Teams

Laptops travel constantly. Self-service key recovery keeps remote staff working without waiting on IT.

USE CASE 04
Multi-Site SME

Head-office IT sees and manages encryption across every branch remotely, without visiting sites.

For more information on complementary or alternative products, visit us at vox.co.za

Business Support : +27 (0) 87 805 0500
Email: info@voxtelecom.co.za

Vox® Business