SOPHOS

Security made simple.

Sophos SafeGuard Enterprise

Proactive Data Protection with Synchronized Encryption

Sophos SafeGuard encrypts content as soon as it is created. The encryption is always on, allowing for seamless and secure collaboration. Synchronized Encryption proactively protects your data by continuously validating the user, application, and security integrity of a device before allowing access to encrypted data. This method of always-on protection goes everywhere your data goes, making it the most comprehensive data security solution on the market.

Highlights

- Application-aware encryption that's always on
- Synchronized Encryption proactively protects data against threats
- Comprehensive encryption across platforms and devices
- Transparent encryption process for secure collaboration
- Proof-of-compliance reporting
- Centralized key management
- Manages device encryption including BitLocker and FileVault 2
- Supports Windows, Mac, iOS, Android, and cloud-based file sharing
- Synchronizes encryption keys with Sophos Mobile Control

Always-on encryption protects data everywhere

Sophos SafeGuard Enterprise is data-centric, automatically securing content upon creation. Once encrypted, files remain secured when shared across platforms and devices, or if they are emailed or uploaded to cloud-based file sharing programs such as Box, Dropbox, or OneDrive. This method promotes secure collaboration everywhere, working across device and platforms without compromising security and preventing accidental data leakage.

Transparent encryption ensures user productivity

Encrypting, decrypting, and accessing information is automatic and transparent to the end user. Your users can open an encrypted file, edit it, or share it internally as they normally would. For externally sharing, decryption or creating password protected files takes only one click.

Proactively protects data against data theft

SafeGuard Encryption has the ability to intelligently protect your data against theft. It automatically encrypts your content, and the content stays encrypted even when it's shared or uploaded to a cloud-based, file-sharing system.

Synchronized Encryption continuously validates the user, application, and device integrity. If your data ever ends up in the wrong hands, SafeGuard renders the information unusable; the files remain encrypted and unreadable.

Real-time threat protection

SafeGuard Enterprise offers Synchronized Encryption by connecting to Sophos Endpoint Protection. The SafeGuard local agent listens to an endpoint's Security Heartbeat™ and enables automated, proactive protection. For example, in the event of an active infection, the SafeGuard agent can temporarily revoke the encryption keys, proactively protecting your data against threats. As soon as the security health of the device is restored, the SafeGuard Management Center pushes the encryption keys back to that device, restoring access to encrypted data.

Secure external sharing with password-protected files

With SafeGuard it's simple to share content with people outside of your organization. Users can create a password-protected file with a single click of a mouse. The file is securely wrapped in an HTML 5 format, so it doesn't require the recipient to install any software. All they need is a web browser and the password to access the encrypted content.

Mindful, one-click decryption

Users can also decrypt files to make them publicly available with one simple click. And because decryption is a logged event, you can record each instance and alert your administrator when someone attempts to decrypt a large number of files. While decryption is simple, it remains a conscious action. This inverted logic helps prevent accidental data leakage and helps to educate end users.

Lost devices, protected data

Full-disk encryption is an essential first line of defense to protect your data in the event of a lost or stolen device. SafeGuard gives you the ability to managed Windows BitLocker and OS X FileVault 2 encryption from the SafeGuard Management Center.

Synchronized for secure content collaboration on mobile devices

Sophos SafeGuard synchronizes your encryption keys with Sophos Mobile Control*, giving you seamless and secure access to encrypted files on iOS and Android devices. Using Sophos Mobile Control's Secure Workspace app on a trusted device, users can view, access, and share encrypted data securely.

Secure key recovery on Mobile Devices

Key synchronization between SafeGuard and Sophos Mobile Control* lets users retrieve their FileVault or BitLocker full-disk encryption recovery keys directly in the Sophos Secure Workspace app on thier mobile device. This helps users get back to work faster without having to contact the help desk, saving both time and IT resources.

SafeGuard Management Center

Manage your encryption policies and keys for all of your devices using this centralized console. From the SafeGuard Management Center, you can set data security policy for groups and devices, secure, store, exchange, and recover keys. You can also generate compliance and audit reports, all from within the console.

SafeGuard Licenses

Modules	SafeGuard Disk Encryption	SafeGuard File Encryption	SafeGuard Enterprise
Full Disk Encryption	✓	-	✓
Centrally Manage BitLocker and FileVault 2	✓	-	✓
File/Folder Encryption	-	✓	✓
Encryption for File Shares	-	✓	✓
Encryption for Cloud	-	✓	✓
Removable Media Encryption	-	✓	✓
Synchronized Encryption	-	✓	✓
Management Console	✓	✓	✓

Try it now for free

Register for a free 30-day evaluation at sophos.com/data.

* Requires Sophos Mobile Control Advanced

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

16-06-29 DSNA (DD-2378)

SOPHOS