SMARTENCRYPT
PLAN OVERVIEW

SMARTENCRYPT™ by rhipe

		Business basic plan	Business pro plan
		For businesses with simple networks wanting control of who can access files e.g. protect payroll & HR data from employees & IT	For business environments requiring granular access controls e.g. to restrict highly confidential files for access in the office firewall only, or different teams or departments
		1 to 10 Users and 1 encryption key	1 to 250 users and 10 encryption keys
		30 days audit log retention	1-year audit log retention
Mapped-drive support	Works with NAS/ Mapped drive file systems	✓	✓
OneDrive and SharePoint/Cloud storage support	Encrypt files stored in OneDrive and SharePoint – also works with OneDrive files on-demand	✓	✓
Secure external file-sharing	Allows sharing of passcode protected files to non-SmartEncrypt Users	✓	✓
Role-based access	Super or general administrator, standard user and helpdesk roles	✓	✓
Two-Factor Authentication (2FA)	One time password/ PIN code during login for extra identity proof	✓	✓
Offline access	Allows users to set a login PIN to access files when no internet connection	✓	✓
Client login settings	Auto-disable inactive accounts or lockout for failed attempts	✓	✓
Basic reporting	Console, client, login activities	✓	✓
Single-sign-on	Support for Azure active directory		✓
Advanced rule customisation	Assign rules to groups that can override default settings		✓
Group management	Assign users to groups for granular access control to encryption keys & rules		✓
Device management	Block specific devices from being able to login for any user		✓
Password policy management	Minimum length, strength, and rotation for security maintenance		✓
Geo-blocking	Enables blacklist of countries from where login is prohibited or whitelist where allowed		✓
IP address restrictions	Additional granular access control to define IP addresses or ranges		✓
Bulk user import	Via CSV or active directory import		✓