PRODUCT OVERVIEW

SMARTENCRYPT™
by rhipe

WHY ENCRYPTION?

Traditional security strategies are no longer effective in protecting your data in today's landscape.

The new working from home environment has presented several security challenges to businesses including software and hardware vulnerabilities, ransomware, and employee data theft. Traditional security methods can no longer keep up with the exponential growth of external and internal cyber threats.

- Do you have certainty that you have complete ownership and control of your valuable data?
- Do you feel confident that your data is for "your eyes only" and is completely secure?
- Can you prevent employees from taking data when they cease employment with your organisation?

WHY ENCRYPTION?

What is encryption?

Encryption is the process of encoding or scrambling data so that it is unreadable and completely unusable unless a user has the correct decryption key.

Encryption is widely regarded as the most effective way to protect data and has been widely used by the military and enterprise businesses. With the ability to behave, interact and do business remotely extended to most organisation's, there is now also a growing demand for encryption by SMBs.

What is an endpoint encryption product?

Endpoint encryption is an essential software tool for data security, altering the form of data so that is indecipherable to anyone other than the intended recipient across any endpoint device.

This prevents the data from being readable and misused, should that data fall in the wrong hands.

The importance of endpoint encryption

Encryption is an important layer in an organisation's security infrastructure. Security products such as firewalls, intrusion prevention, and role-based access control applications all help protect data within the organisation.

However, breaches and data theft have become increasingly common, and data encryption can protect data even after it leaves an organisation. Encryption is a key defense against data theft and exposure.

> *"... encoding or scrambling data so that it is unreadable and completely unusable..."*

INTRODUCING SMARTENCRYPT

SmartEncrypt is a SaaS encryption solution for SMBs that provides certainty that your company data is protected in the event of a data breach, file access, or data theft.

- Fast and seamless deployment that takes less than 10 minutes
- Cloud based file encryption solution that can be managed, and installed by anyone
- Affordable, low cost monthly investment that protects against major revenue loss and reputational damage
- An automated and invisible solution that has zero impact on productivity
- Protects against unauthorised access to data such as customer lists, high value IP, and protected Personal Identifiable Information (PII).
- Protects all file types

INTRODUCING SMARTENCRYPT

Through adding SmartEncrypt to your existing security stack, it will provide 100% certainty if an unauthorised user accesses a file without an encryption key, it will be impossible to access the data.

Here are just a few of the reasons why traditional approaches to cyber security and compliance will no longer cut it:

1 Traditional cloud based security solutions do not guarantee protection against unauthorised access to data.

2 As companies move all their work to a digital environment, they have less control of the location and movement of their data. Can you name all the apps and clouds your employees are using to store their data?

3 The rise of remote working means that firewalls are only effective if you work in one office.

4 Increased ransomware and phishing puts businesses of all sizes at risk. It only takes one staff member to open a malicious email.

5 Employees have become a driver of incidental and targeted data theft and loss. Accidental deletion and taking customer lists after resignation are just some of the everyday scenarios affecting SMBs.

"... it will be impossible to access the data..."

WHY SMARTENCRYPT?

A solution that provides guaranteed certainty that your data will be protected against all imminent and developing cyber security risks.

Protects against data loss from insider threats - 85% of employees admitted to taking company documents when they left a business. In a survey by Osterman Research, 69% of organisations cite data loss when an employee leaves.

Often, this data is highly sensitive, such as proprietary code, customer and prospect information. In some cases, employees may not intentionally take data out the door, but often, malicious intent is involved. Departing employees, contractors, service providers and temporary workers are all threats to an organisations data security.

WHY SMARTENCRYPT?

Data loss from external threats

Ransomware

Ransomware variants are designed to steal your data and hold it hostage until compensated by the requested amounts. The threat quite often includes data loss or making your company's, and sometimes even employees' or customers', personal data public. This then results in loss of funds or destroying a company's reputation if the requested funds are not paid.

The SmartEncrypt Solution:
Using SmartEncrypt prevents the data from being readable and misused, should that data fall in the wrong hands.

Remote Workers

When employees take their machines home or use their personal devices for work, those machines now sit in a physical and digital space unlike any within the office. Your remote employees are unlikely to have the security protocols more likely found in your office such as a business grade firewall. Especially as shareable assets can most often be accessed by using their personal devices, which for some it is an easier and much more convenient option.

The SmartEncrypt Solution:
Encrypting your valuable company data will protect it and give you ownership and control even at your employee's homes.

BYOD computers

When staff utilise their personal computer for work, IT lacks the control they would normally have over a company issued computer. Risks include a lack of control over the choice of application installed and used, managing security updates and detecting trojans such as ransomware, malware or a virus lurking on the device.

The SmartEncrypt Solution:
SmartEncrypt's folder-level encryption can create peace of mind in use cases such as employees bringing their own devices. There is no need to encrypt the entire device, but rather just make sure the company data is encrypted and safe. If the employee loses the device or leaves the organsation, the access to company files can easily be remotely turned off, keeping the data safe from unwanted eyes even when IT does not have direct access to the device.

> *"The average cost of a ransomware attack on businesses is $133,000"*
>
> *(source: SafeAtLast).*

WHY SMARTENCRYPT?

Compliance

The Privacy Amendment (Notifiable Data Breaches) Bill 2016 established a mandatory data breach notification scheme in Australia.

Security breaches continue to hit the headlines and have highlighted the importance of data security and privacy. In response to the growing risk these threats represent to the community, and our industry, the Australian parliament passed new Mandatory Data Breach notification laws. From February 2018 all Australian organisations who are regulated by the Privacy Act may be liable for large fines for failing to comply with the new rules. Breaches include areas such as attacks on information storage, a loss of documents or data through accident, or the improper disclosure of information.

A data breach happens when personal information is accessed or disclosed without authorization or is lost. If the Privacy Act 1988 covers your organisation or agency, you must notify affected individuals and The Office of the Australian Information Commissioner (OAIC) when a data breach occurs.

The SmartEncrypt Solution: Using SmartEncrypt on your company data allows your organisation to have control of who can access this data. In the event of a breach the data is protected, meaning there is no risk and no damaging consequences from the breach.

When it comes to encryption, many regulations and laws, such as GDPR, PCI-DSS, HIPAA, SOX and GLBA, require that it be implemented. With the increase in cyber-attacks, endpoint encryption is no longer an optional solution for most businesses that handle financial or health information, but rather is becoming more and more a required solution.

Company Directors & The Board

Most Australian company directors know they need to oversee their organisation's cyber risks, but many are not adequately prepared and as a result risk prosecution from the regulator in the event of a breach. The primary legal question for directors is whether they have adequately discharged their duty of care. A company's board and senior Directors may well be exposed to liability for breach of the duty of care if they fail to take the steps that are expected by ASIC in understanding and managing risk.

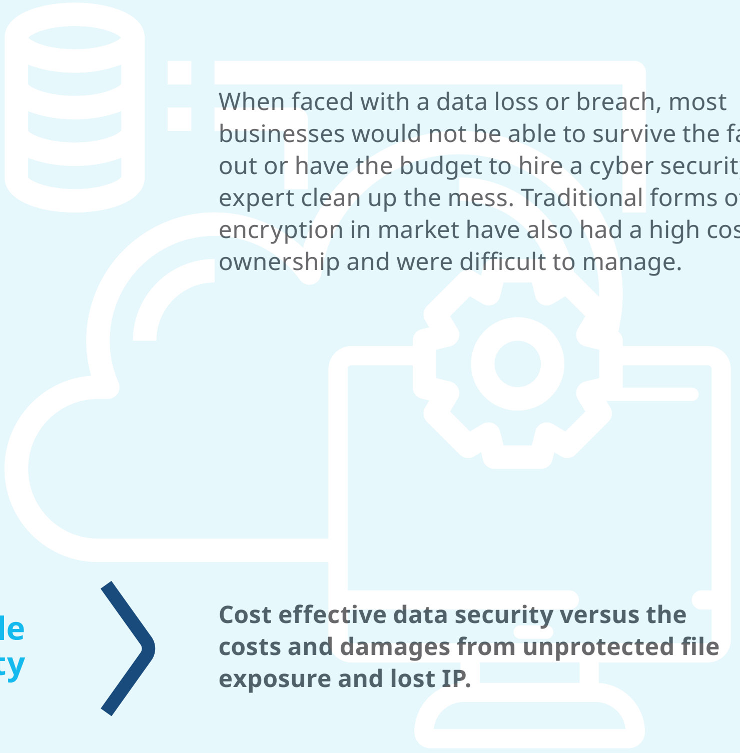
A claim from Directors or the Board that they did not have enough information or didn't understand the requirements, would not be a sufficient defence.

Hacking

Most business owners or directors may think, nobody's going to hack my business, I don't have data worth the effort or I'm not a business that would be worthwhile to target. The reality is that the majority of small to medium businesses hacked, were not actually targeted, they were simply unlucky enough to have a device connected to the internet detected by a scanning tool, leaving them open to the exploitation of a vulnerability .

Many hackers today are using scanning tools and have absolutely no idea who they are hacking until they get into the device. A simple solution is patching all devices, but there is no guarantee that all company devices are always 100% secure. Especially with remote working on the rise there are even more entry points than ever before meaning vulnerabilities are constantly being discovered.

INTRODUCING SMARTENCRYPT



Our mission is to deliver an affordable and accessible encryption solution that delivers cyber resilience for SMBs.

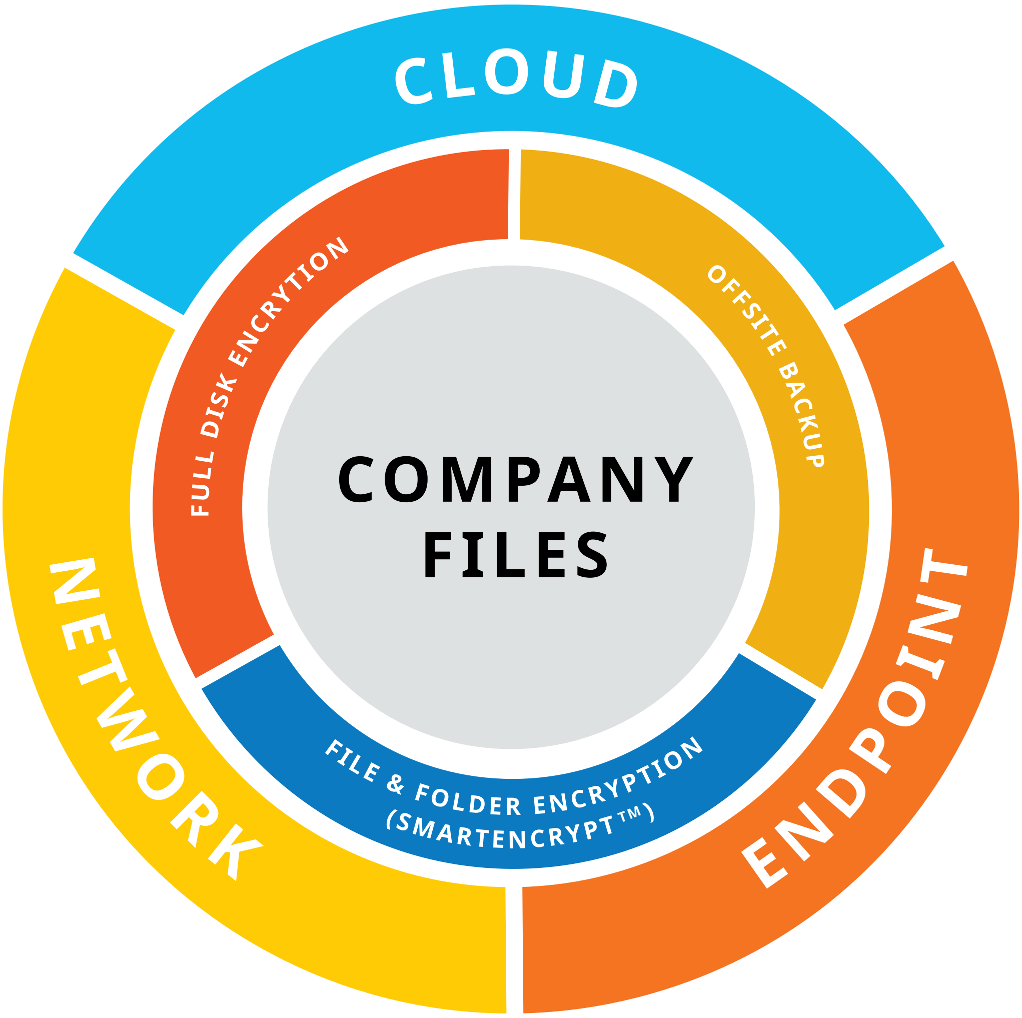
When faced with a data loss or breach, most businesses would not be able to survive the fall out or have the budget to hire a cyber security expert clean up the mess. Traditional forms of encryption in market have also had a high cost of ownership and were difficult to manage.

Key Product Benefits

- **Affordable Security** – Cost effective data security versus the costs and damages from unprotected file exposure and lost IP.
- **File-Level Protection** – File encryption is the last line of defence - encrypted content cannot be decrypted without the encryption key.
- **Protection Certainty** – Always on persistent encryption regardless of data movement; files are not accessible even if stolen or exfiltrated by malware.
- **Secure Remote Working** – Beyond-the-firewall controls enabling use of BYOD computers, cloud storage applications and USBs.
- **Seamless User Experience** – 'Invisible' and seamless encryption/ decryption process with no impact on user workflows.

INTRODUCING SMARTENCRYPT

How SmartEncrypt future proofs your business against unauthorised access



INTRODUCING SMARTENCRYPT

Take the first step to investing in a future of data security and cyber resilience by adding SmartEncrypt to your existing security stack

		BUSINESS BASICS PLAN	BUSINESS PRO PLAN
		For small businesses with simple networks wanting control of who can access files e.g protect payroll and HR data from employees and IT	For business environments requiring granular access controls e.g to restrict highly confidential files to access in the office firewall only, or different teams or departments
		1 to 10 Users 1 Encryption Key	1 to 250 Users 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	Encryption of files stored in OneDrive and SharePoint – also works with OneDrive Files On-Demand	✓	✓
Encrypted External File-Sharing	Allows sharing of PIN-protected files with non-SmartEncrypt Users	✓	✓
Role-based Access	Super or General Administrator, Standard User or Helpdesk role	✓	✓
Two-Factor Authentication (2FA)	One Time PIN code during login for extra identity proof	✓	✓
Offline Access	Allows Users to set a login PIN to access files when no internet connection is available	✓	✓
Auditing and Reporting	Configurable reports for Console, client and login activities	✓	✓
Single-Sign-on	Support for Azure Active Directory		✓
Group Management	Assign Users to groups for granular access control to encryption keys and 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		✓
Geoblocking	Specify countries from where login is prohibited or allowed		✓
IP Address Restrictions	Additional access control to defend IP addresses or ranges		✓
Bulk User Import	Via CSV		✓

ABOUT rhipe

Take the first step to investing in a future of data security and cyber resilience by adding SmartEncrypt to your existing security stack

A global leader in cloud advisory & solutions

rhipe (ASX:RHP) is APAC's leading distributor of cloud solutions and services. rhipe have helped thousands of IT businesses embark on, and accelerate their cloud journey.

rhipe's award winning cloud solutions and advisory services enable cloud businesses and IT services providers to seamlessly deliver cloud services, building profitable solutions, and achieve business growth.

rhipe's multi-disciplinary teams combine business advisory, technical knowledge and deep industry expertise to help IT partners unlock their potential and double their cloud growth. Through a distribution agreement with rhipe, technology businesses gain seamless access to cloud vendor licensing agreements through rhipe's self serve PRISM platform, go to market and business advisory, education and training and professional services.

SMARTENCRYPT™
by rhipe