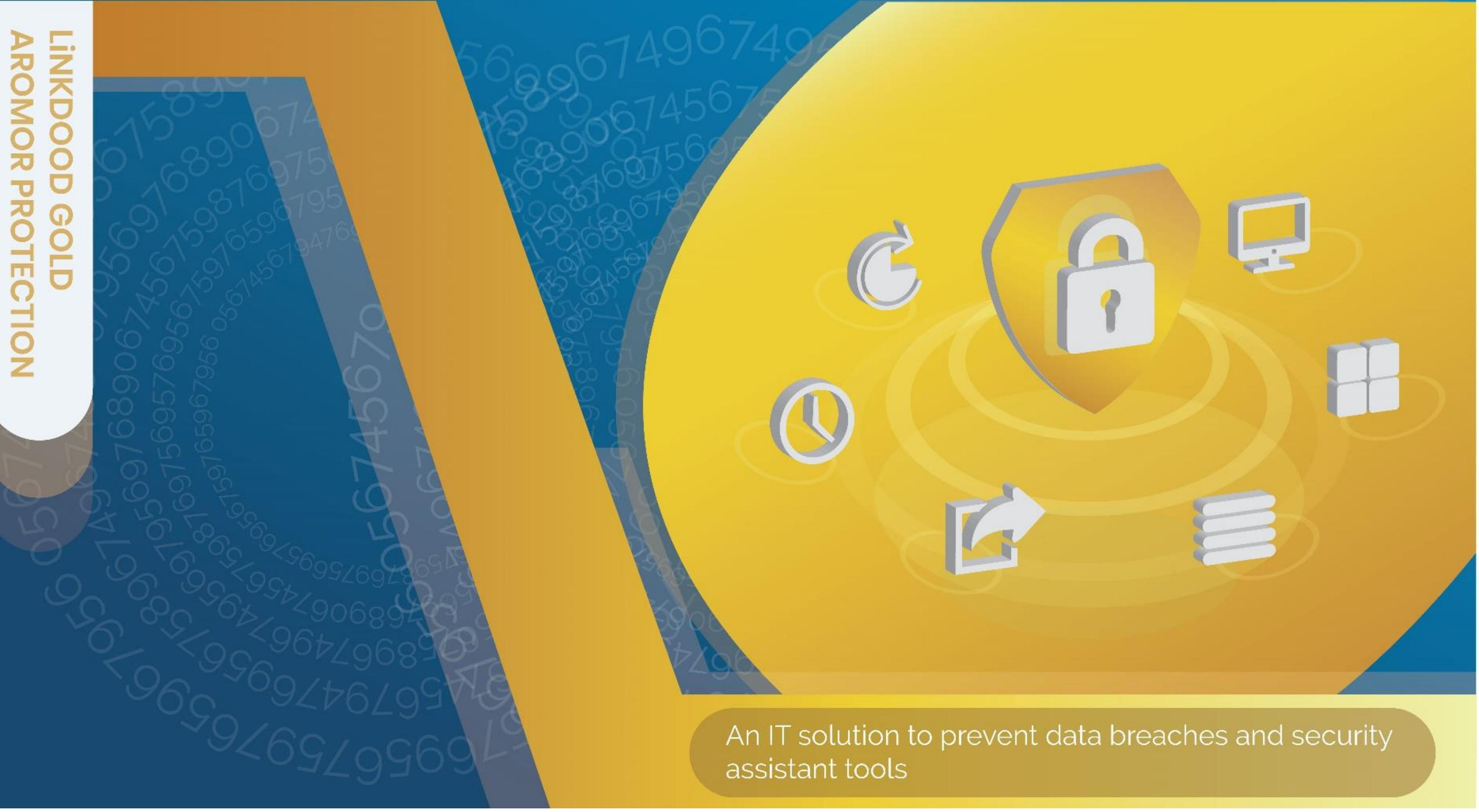


An IT solution to prevent data breaches and security assistant tools

Powerful Shield On-Guard for Your Data

Who is the targeted user?

Enterprise who need to secure their sensitive and important data may use this document to understand how LiNKDOOD Gold Armor Protection protects the important data with special storage space which can access by authorized user only. Other than that, this paper also describe how to overcome the issues while transferring important data from one place to another with encryption technology only in LiNKDOOD Gold Armor Protection.

BEYOND SECURITY LINKDOOD

Table of Content

Introduction

Data theft and breaches happened all around the world which threatens many companies and organizations. Important and sensitive data which stored in computer hard drives are flows seamlessly throughout organizations and out to employees across the globe. This can wind up in the hands of unintended recipients, who can misuse the data for malicious purposes. Data breaches occurs due to poorly planned business processes that use insecure procedures as well as employee inappropriate way of handling data. Employees may transfer sensitive data to external media devices such as USB storage drives, smartphones or send the data via email to an unauthorized person. Conduct a training to educate the employees able to minimize the risk of data breaches which cause by careless data management. Being aware of most risks related to data transmission media devices helps to keep data in safer manner.

Nowadays, Windows vulnerability makes it possible to allow attackers to completely take control over computers with an easy hack. Computer systems running unsupported software are often exposed to cyber security threats, such as increased risks of malicious attacks or electronic data loss. These vulnerabilities could allow an attacker to run malicious codes on the endpoint, which would also let the attacker execute programs, delete data and other unauthorized actions.

How Does the Solution Works?

Linkdood Gold Armor Protection (LGP) aims to protect important data, handle vulnerability issues, malware attacks as well as to provide user with ease of use. The following section will describe on 'Data Breaches Prevention System', 'Baseline Security Assistant Tools' and 'General Assistant Tools' functions available in LGP.

Data Breaches Prevention Tools

Data Breaches Prevention Tools, available in LGP consists of functionalities such as 'Personal Space', 'Private Space', 'Secure File' and 'Data Lock'. These tools are used to protect confidential and critical data to prevent unauthorized end users accidentally or maliciously leak the data to unknown third parties. The tools are briefly explained as below:

- **Personal Space**

‘Personal Space’ functions as a secure storage to store confidential data which is located in “My Computer / This-PC”. To access ‘Personal Space’, login to LGP with valid login credentials. A ‘Personal Space’ storage created, allowed user to manage the important files added and remove the files once the files no longer required. Folders can be created to group the files into different categories based on user’s requirement. Setup and install LGP in a shared endpoint located inside an organization’s department allowed other users to safely use the shared endpoint without the risk of data exposure to unauthorized party.

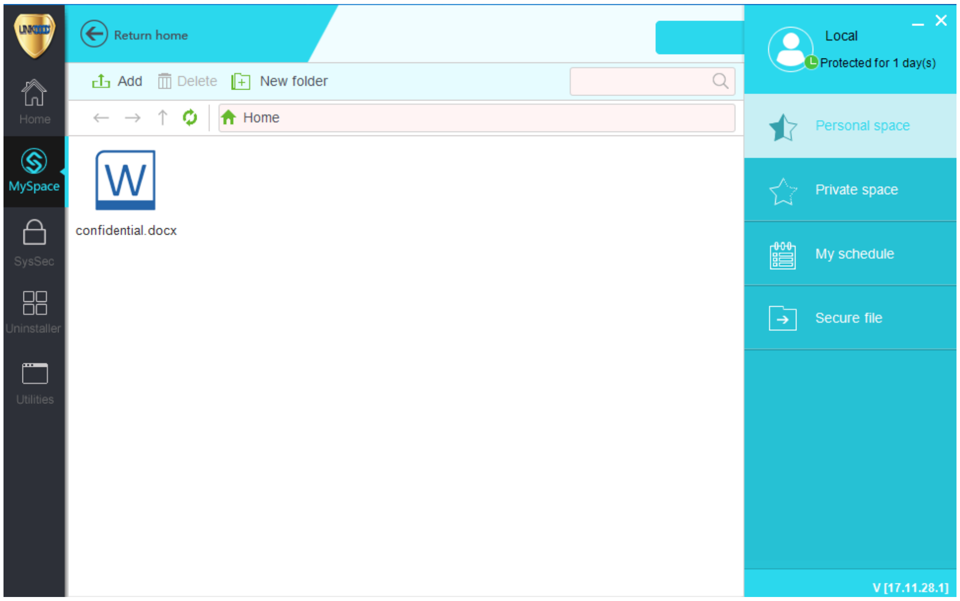


Figure 1 MySpace – Personal Space

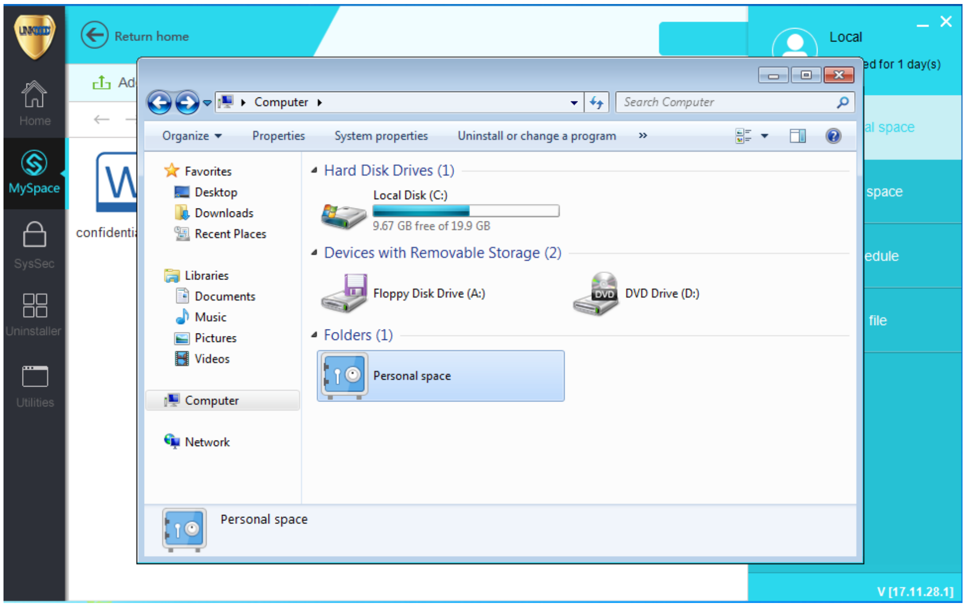
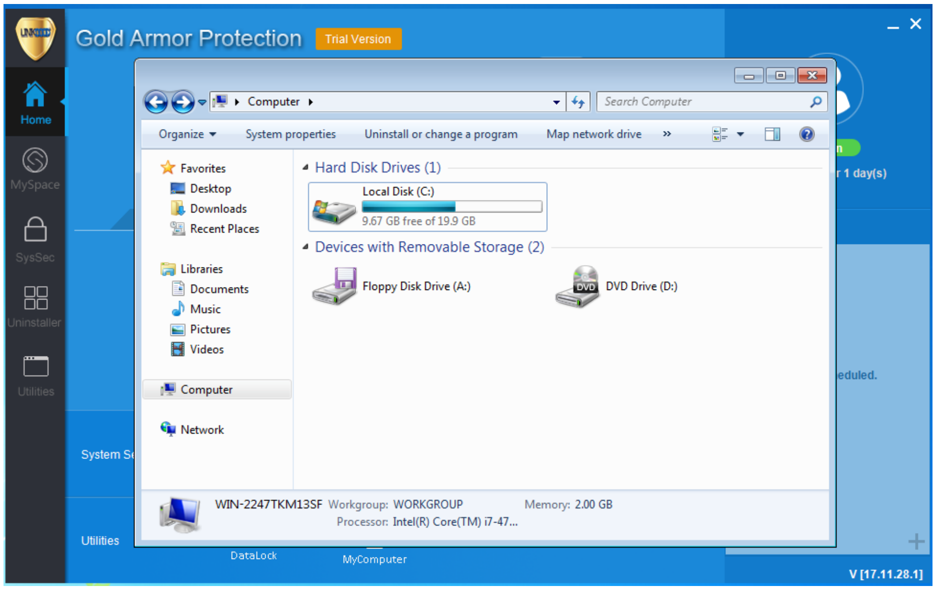


Figure 2 MySpace – Login LGA



9.67 GB free of 19.9 GB

WIN-2247TKM13SF Workgroup: WORKGROUP Memory: 2.00 GB
Processor: Intel(R) Core(TM) i7-47...

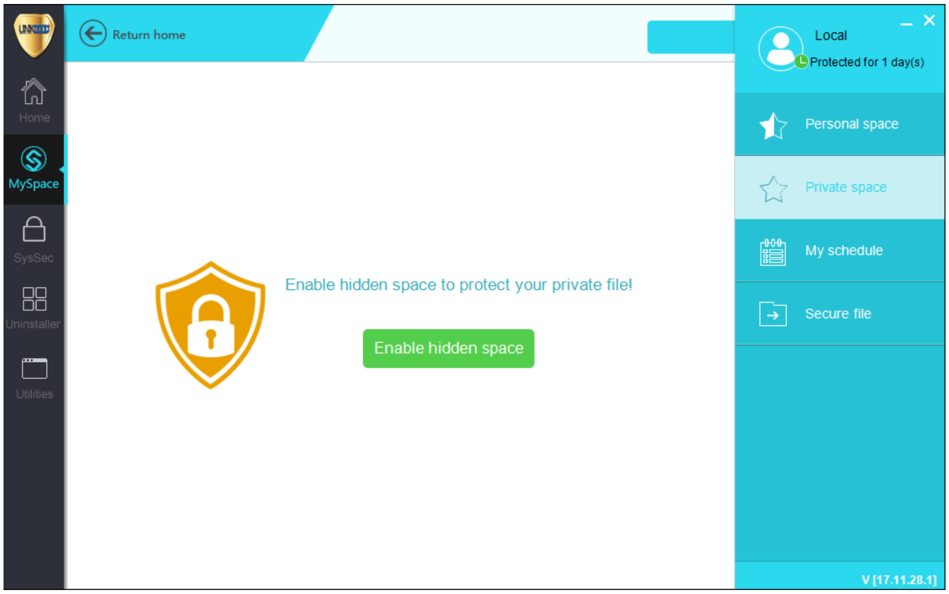
Figure 3 MySpace – Logout from LGA

- **Personal Space Figure Description**

Figure 1 show the ‘Personal Space’ storage content. When user login to LGA, the previously stored files will show in ‘Personal Space’. At ‘Computer / This-PC’ page, when LGA user login, the ‘Personal Space’ will display in the ‘Folders’ section. When logout from LGA, the ‘Personal Space’ hidden from display.

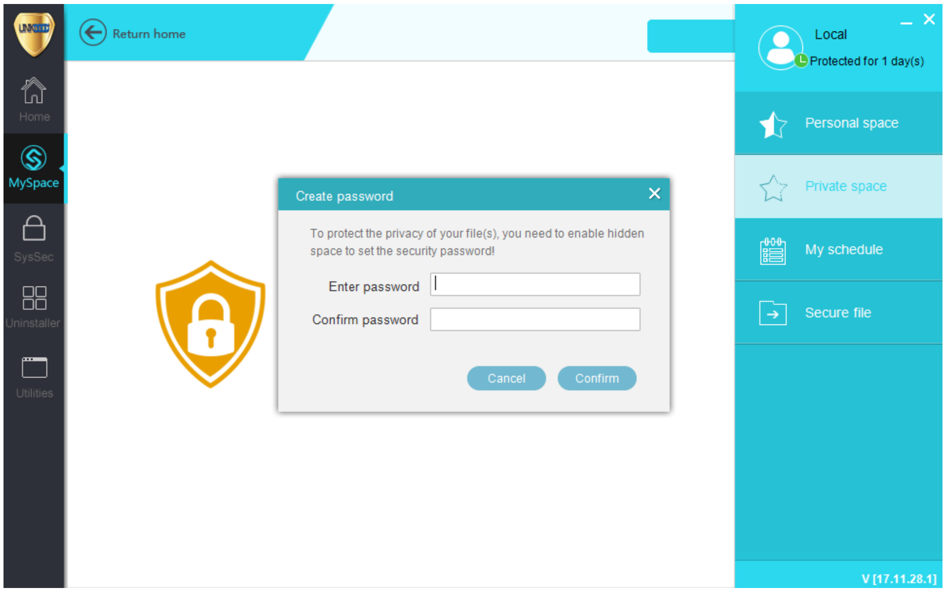
- **Private Space**

'Private Space' functions similar to ‘Personal Space’ but come with extra security layer protection on login credentials which provide a two factor authentication before access to the ‘Private Space’ contents. A new password is required at the first setup of ‘Private Space’ storage. After finish password setup, the ‘Private Space’ storage created, allowed user to manage the important files added and remove the files once the files no longer required. . Folders can be created to group the files into different categories based on user’s requirement. ‘Private Space’ is a storage where allow user to store higher level of confidential and sensitive files which can be viewed by higher level staffs only.



Enable hidden space to protect your private file!

Figure 4 MySpace – Private Space 1st Access



Create password

To protect the privacy of your file(s), you need to enable hidden space to set the security password!

Enter password

Confirm password

Figure 5 MySpace – Create Password

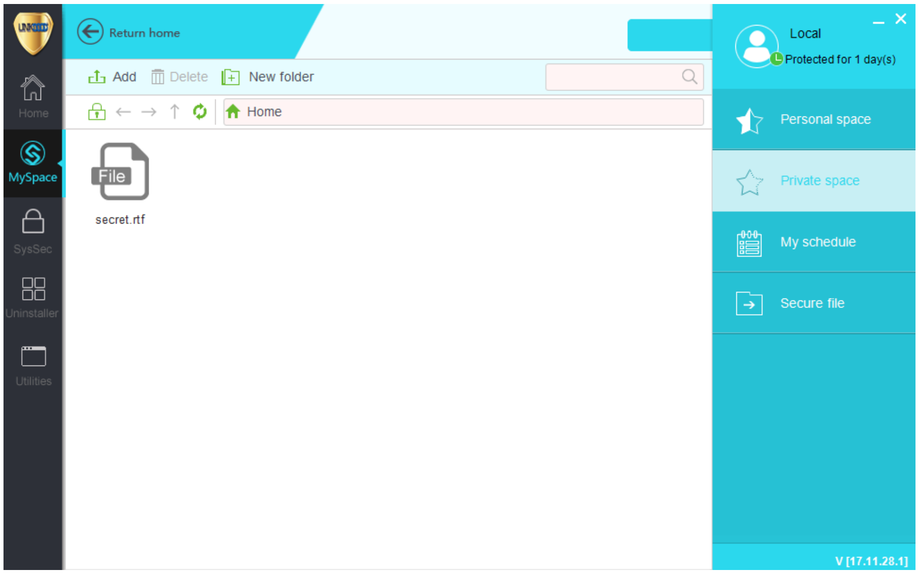


Figure 6 MySpace - Enabled Private Space

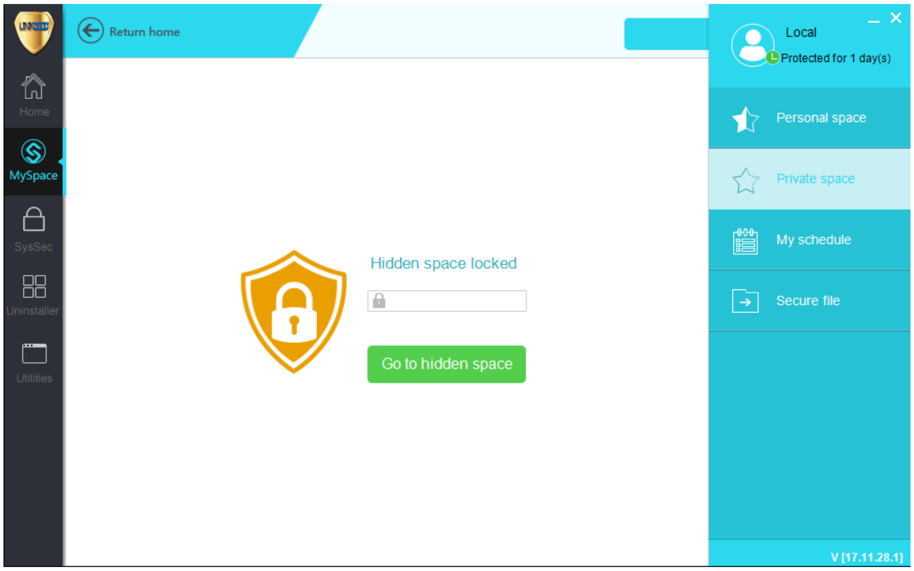


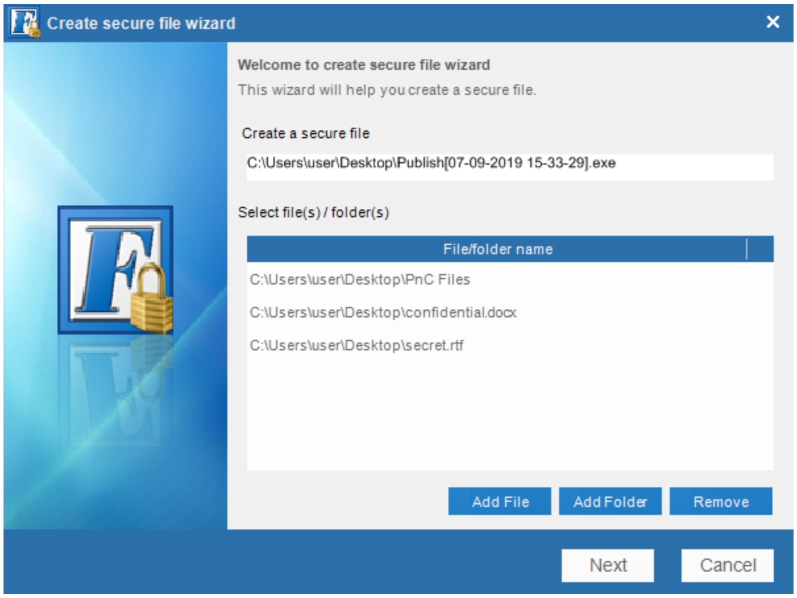
Figure 7 MySpace - Private Space 2nd Access

- **Private Space Figure Description**

Figure 4 show the ‘Private Space’ storage 1st access. When click “Enable”, a “Create Password” window prompt. After set the password, it grants access to “Private Space’. When re-login to LGA and access to ‘Private Space’, user have to key-in the correct password in order to access ‘Private Space’ storage.

- **Secure File**

To secure a document and transfer to other party, ZIP and secure it with a password is what commonly done for the senders. However, attackers who successfully steals the ZIP document are able to see the contents if they are able to obtain the password. LGA ‘Secure File’ solved this issue by applying certain conditions to the files or folders. Other than applying conditions, ‘Secure File’ can secure the files or folders by applying a dual layer security to the files or folders which is password lock for the files and folders, and use LGA unique authentication code generator to perform the authentication step.



Welcome to create secure file wizard

This wizard will help you create a secure file.

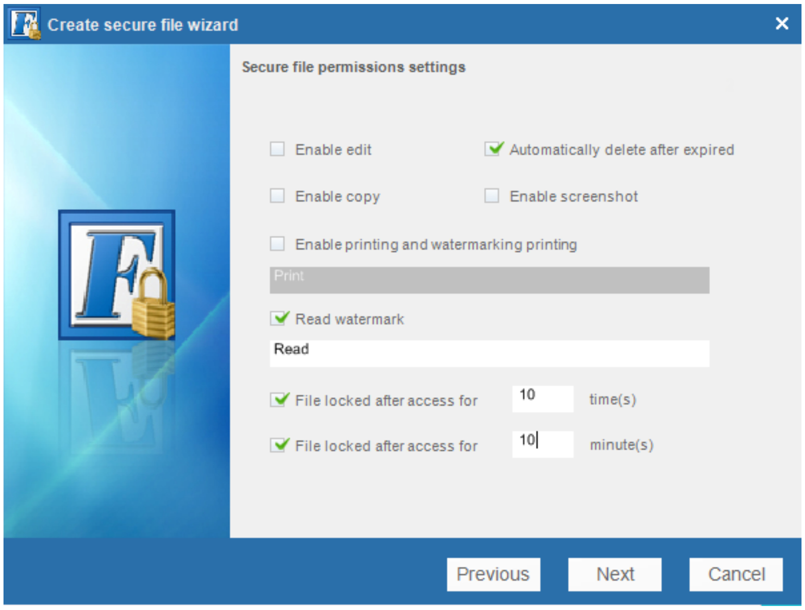
Create a secure file

C:\Users\user\Desktop\Publish[07-09-2019 15-33-29].exe

Select file(s) / folder(s)

File/folder name
C:\Users\user\Desktop\PnC Files
C:\Users\user\Desktop\confidential.docx
C:\Users\user\Desktop\secret.rtf

Figure 8 Secure File – Add Files/Folder



Secure file permissions settings

□ Enable edit ☑ Automatically delete after expired

□ Enable copy □ Enable screenshot

□ Enable printing and watermarking printing

Print

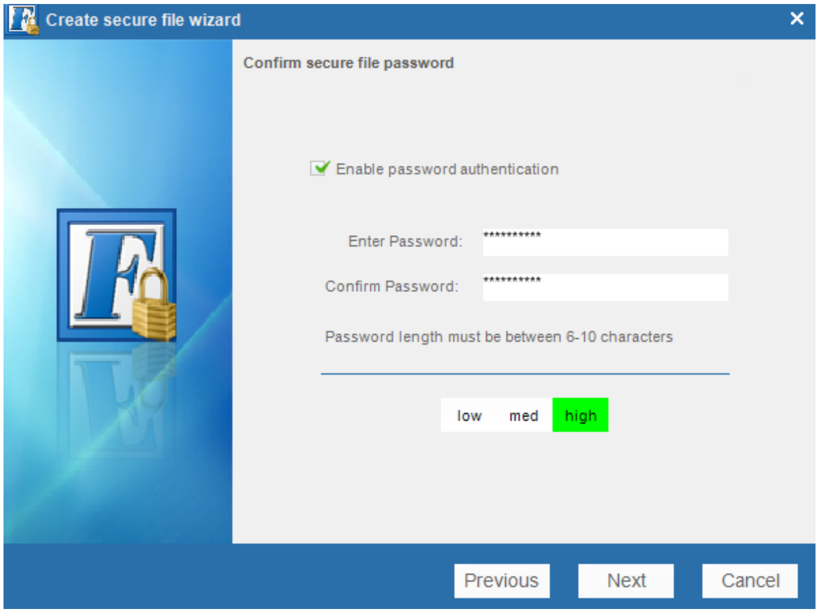
☑ Read watermark

Read

☑ File locked after access for 10 time(s)

☑ File locked after access for 10 minute(s)

Figure 9 Secure File – File Conditions



Confirm secure file password

☑ Enable password authentication

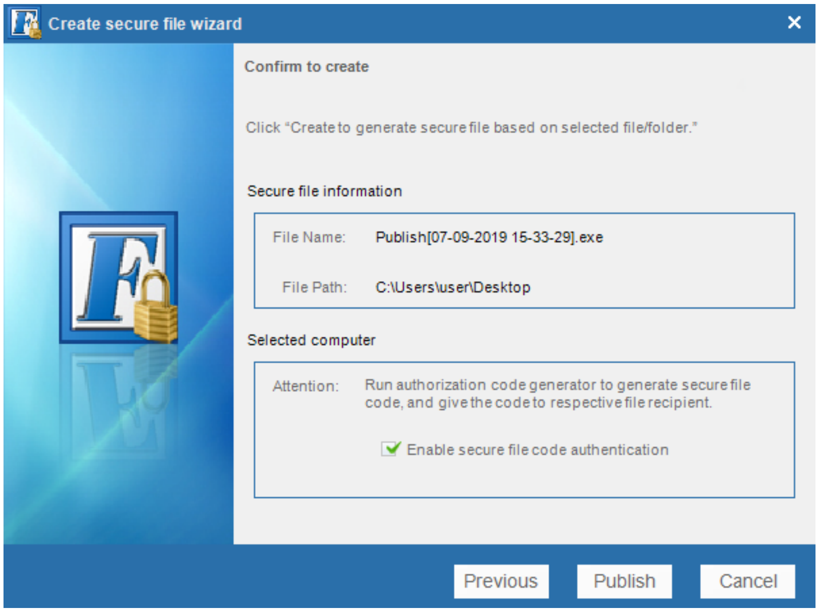
Enter Password: **********

Confirm Password: **********

Password length must be between 6-10 characters

low med high

Figure 10 Secure File – Password Authentication



Confirm to create

Click "Create to generate secure file based on selected file/folder."

Secure file information

File Name: Publish[07-09-2019 15-33-29].exe

File Path: C:\Users\user\Desktop

Selected computer

Attention: Run authorization code generator to generate secure file code, and give the code to respective file recipient.

☑ Enable secure file code authentication

Figure 11 Secure File – Enable Secure Code Authentication

- **Secure File Figure Description**

Figure 8 shows the 'Secure File' wizard. User can add confidential files or folders which need to be transfer to other parties. Click 'Next' and proceed for file permission settings. The settings include:

Enable Edit: Permission to edit the content of the files.

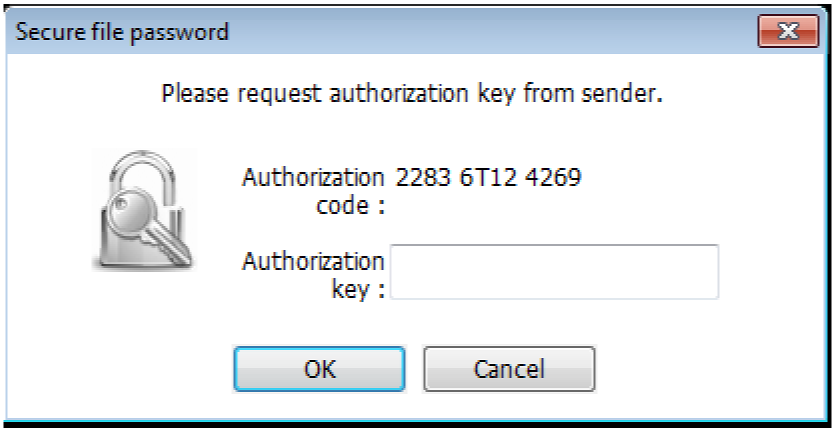
Enable Copy: Permission to copy the content to other locations.

Enable Printing and Watermarking Printing: Enable file printing come with watermarks (watermark text can be set)

Read Watermark: Come with watermarks when access and view through the file contents (watermark text can be set)

Automatically Delete After Expired: File will be deleted after expired. The expired settings come with the condition below:

- File locked after access for XX times: The archive files/folders will be locked/expired after number of times access.
- File locked after access for XX minutes: The archive files/folders will be locked/expired after certain period of time.



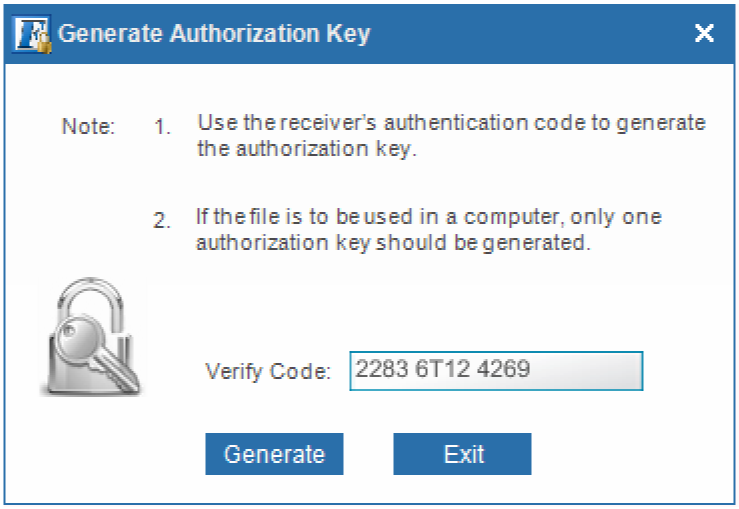
Secure file password

Please request authorization key from sender.

Authorization code : 2283 6T12 4269

Authorization key :

Figure 12 Secure File – Authorization Key



Generate Authorization Key

Note: 1. Use the receiver's authentication code to generate the authorization key.

2. If the file is to be used in a computer, only one authorization key should be generated.

Verify Code: 2283 6T12 4269

Figure 13 Secure File – Key Generator

- **Secure File Authentication Key Generator**

After create an archive file with LGA 'Secure File' system, to access the contents of archive file, recipient has to send the authorization to the sender for key generate purpose. Once the sender receive the authorization key, make sure the recipient is the correct person then only proceed to generate authorization key.

- **Data Lock**

Data 'Lock' able to either lock or hide files or folders from being visible to others. A 'Lock' file required LGA login password to grant access into the file.

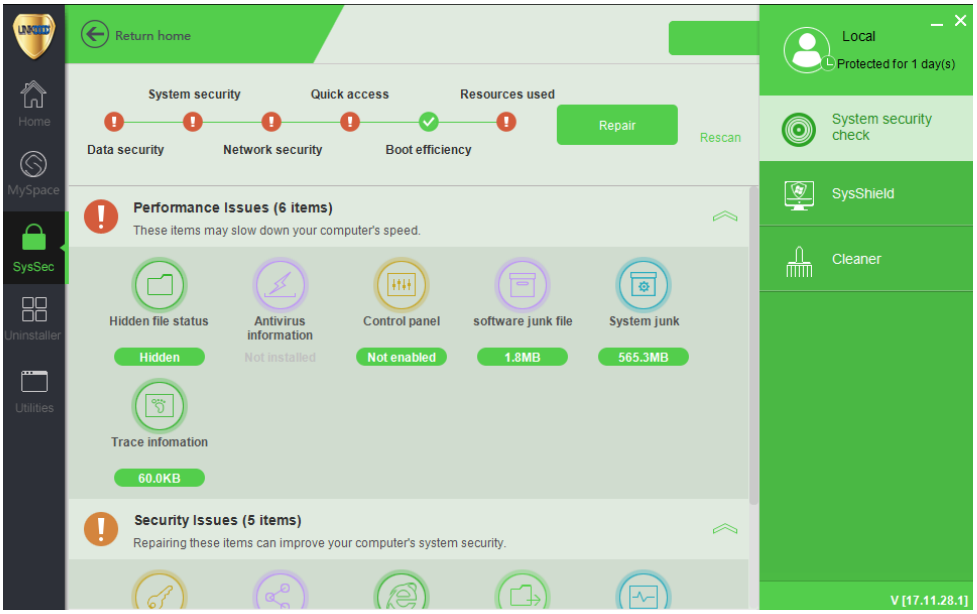
'Hide' file cannot be viewed by others once the LGA user logout from LGA. Valid LGA user has to login in order to make the hidden file shown up.

Baseline Security Assistant Tools

Baseline Security Assistant Tool functions to assist the user to understand the overall performance issues and security issues that currently exist as well as to optionally perform preventive measures to protect against vulnerabilities.

- **System Security Check**

'System Security Check' performs a security scanning to check the current Microsoft Windows performance and security issues. Full 'System Security Check' includes 'Data Security', 'System Security', 'Network Security', 'Quick Access', 'Boot Efficiency' and 'Resources Used'. Click on 'Repair' will resolve most of the issues without any further actions.



Performance Issues (6 items)

These items may slow down your computer's speed.

Hidden file status: Hidden
Antivirus information: Not installed
Control panel: Not enabled
software junk file: 1.8MB
System junk: 565.3MB
Trace infomation: 60.0KB

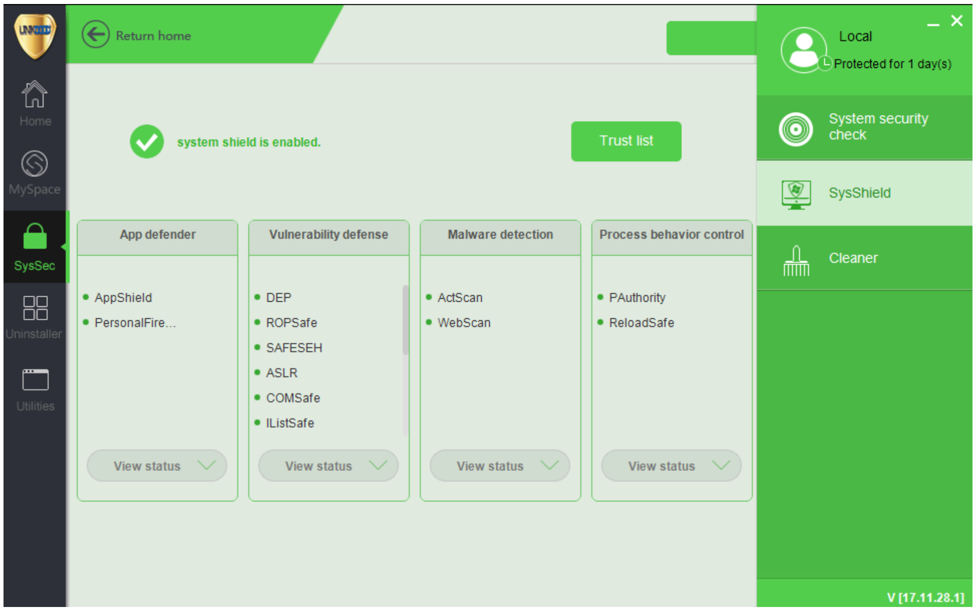
Security Issues (5 items)

Repairing these items can improve your computer's system security.

Figure 14 System Security Check

- **System Shield**

'System Shield' provides protection by implementing 4 key functionalities; 'Application defender', 'Vulnerability defense', 'Malware detection' and 'Process behavior control'. 'Application defender' able to isolate untrusted applications and prevents it from executing. 'Vulnerability defense' prevents any risks caused by system vulnerabilities. 'Malware detection' performs checking on web content before parsing the content on the browser. 'Process behavior control' detects and prevents the process from reloading the module on the attacker's server.



system shield is enabled.

App defender	Vulnerability defense	Malware detection	Process behavior control
AppShield	DEP	ActScan	PAuthority
PersonalFire...	ROPSafe	WebScan	ReloadSafe
	SAFESEH		
	ASLR		
	COMSafe		
	IListSafe		

Figure 15 System Shield

General Assistant Tools

General assistant tools include tools such as 'My schedule', 'Cleaner', 'Uninstaller', 'System Doctor', and 'Shortcut Operation'. These tools provide the user with other functions such as a task reminder and troubleshooting in case of facing any common issues.

- **My Schedule**

‘My Schedule’ allows the user to create schedule task lists or reminder. 'My Schedule' allows user have a more systematic way to monitor daily and future tasks.

- **Cleaner**

‘Cleaner’ helps to clear all unnecessary Windows junk files that remains in the computer system. This allows the computer to operate more efficient and rapid. There are two types of cleanup as shown below:

- **Default Cleanup:** Choose the section user needs to scan and clean for junk files. After perform scanning, all the unused and junk files will be listed out, and request user to select and complete the cleanup steps.
- **Custom Cleanup:** Choose / drag the files needed to be wiped out completely into this section. Shredder is to perform a complete delete and destroy the files and documents. Normal delete files can be restore using recovery tools but for the Shredder function, the files would be completely destroyed after delete process.

- **Uninstaller**

'Uninstaller’ helps the user to completely uninstall and remove applications. Using ‘Uninstaller’ to perform uninstalling of application, ensures that all unused files and folders related to that application will be deleted. Hence, it provides a clean and complete method in removing software.

- **System Doctor**

‘System Doctor’ scans and troubleshoots most of the common issues related to the Windows system, network and devices. ‘System Doctor’ will perform an update at the system registry and may require a system restart to take effect.

- **Shortcut Operation**

‘Shortcut operation’ provides an easy way for users to access commonly used tools.

Conclusion

Linkdood Gold Armor Protection (LGP) helps to protect Microsoft Windows based desktops, laptops, and file servers by providing data leakage prevention, baseline security as well as some other tools that may be useful to the user. It helps to protect all data regardless of whether the data is only distributed within a network or data that are sent over the Internet. LGP is capable of providing active defense against any vulnerability attacks, perform malware detection and monitor the behavior of processes running on the endpoint. LGP comes with bundled with other useful tools such as ‘System Doctor’ which assists the user to troubleshoot commonly faced problems.