PRODUCT OVERVIEW

WrappingBox

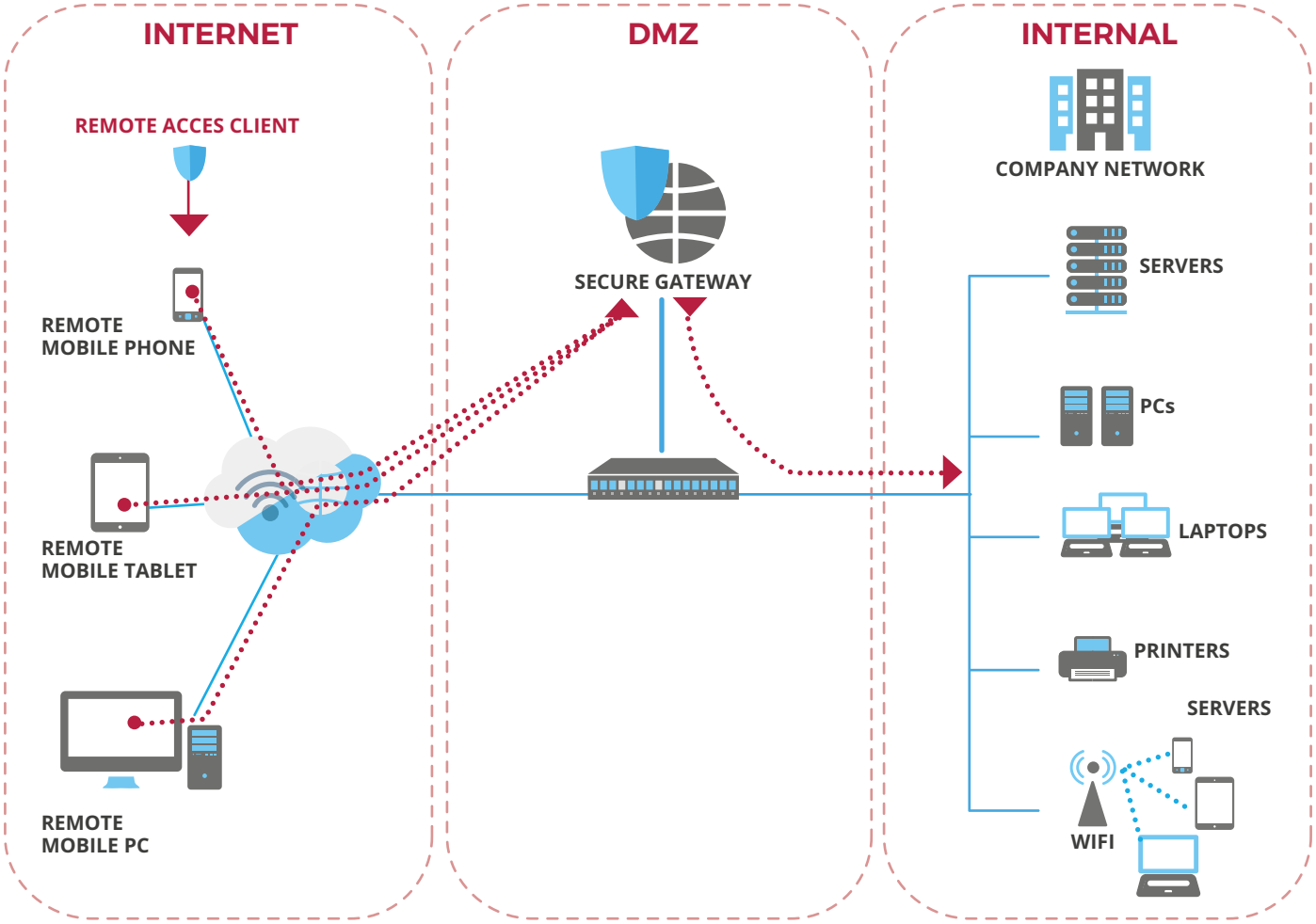
Soliton®

WrappingBox enables secure remote working on Microsoft® Windows® platforms. It does not require Server Based Computing or Virtual Desktop Infrastructures. WrappingBox presents a protected company desktop that is running on the local computer. It launches locally installed applications in a 'wrapped mode'; applications run protected and separated from the resources of the local computer. Data stored on the local computer is automatically encrypted. When closing WrappingBox, it requests to delete, upload the file to the company server or store the file inside the WrappingBox.

Using WrappingBox, companies can now only use the local computer resources and applications without the risk of losing data. Users can download files from the company servers, where they can work with them as usual, both online and offline. The embedded Soliton SecureBrowser Pro allows users to securely access internal company resources.

Soliton®

OUR GENERAL APPROACH IN REMOTE ACCESS SECURITY



All Soliton's remote access security solutions are developed based on the same principles

- Mutual authentication between client and gateway creating a secure connection.
- Gateway protects the servers and the network from cyber-attacks and from unauthorized access.
- Gateway separates the client from the network, the remote device is never part of the network.
- Gateway exchanges information with the network and enables secure access to the network resources.
- Remote access client can be installed by end-user, no special rights required for PCs or Macs.
- User access is based on permission rules or Active Directory group membership; users do not need to remember any URL's.

KEY FEATURES AND BENEFITS

WrappingBox has the following key features:

- Presents a company-workspace to users in the form of a familiar-looking desktop with applications the user already knows from his local computer
- Applications that are launched from the protected workspace are automatically wrapped; applications have no access to the local file system, the registry, the clipboard and the network. Limited access can be defined following any company policy.
- Local disk drives are available to the applications. Files cannot be opened or copied to the WrappingBox. Data that is written to a local drive are stored inside the WrappingBox. All information that is (temporarily) stored inside the WrappingBox is transparently encrypted. This data cannot be accessed from outside the WrappingBox and valuable company information cannot be leaked
- Connects to the company SecureGateway if the user is online. Users can easily download and upload company documents to and from the WrappingBox for temporary local storage and/or editing.
- When closing the WrappingBox, policies define what the user can do with the company data. Documents can be uploaded to a company file server, temporarily stored inside the WrappingBox for offline use, or deleted
- While online, the user can use the embedded SecureBrowser Pro to access internal company web resources. For more details please see chapter 'Embedded Options'.
- Built-in support for two-factor authentication using user certificates or smartcards.
- Price winning and patented technology prevents the data loss through COM (Component Object Model) * patent nr. 6104447
- Application with a small footprint that can be installed and easily removed from a users' pc. Clean install, does not interfere with the local operating system or applications
- Pre-registration of the most widely used applications such as Microsoft® Office and Adobe® Reader®
- Saves on implementing and managing a Server Based Computing platform or Virtual Desktop Infrastructure and any additional licenses that may be required

EMBEDDED OPTIONS

WrappingBox comes with an internal Soliton SecureBrowser implementation, with the following additional benefits:

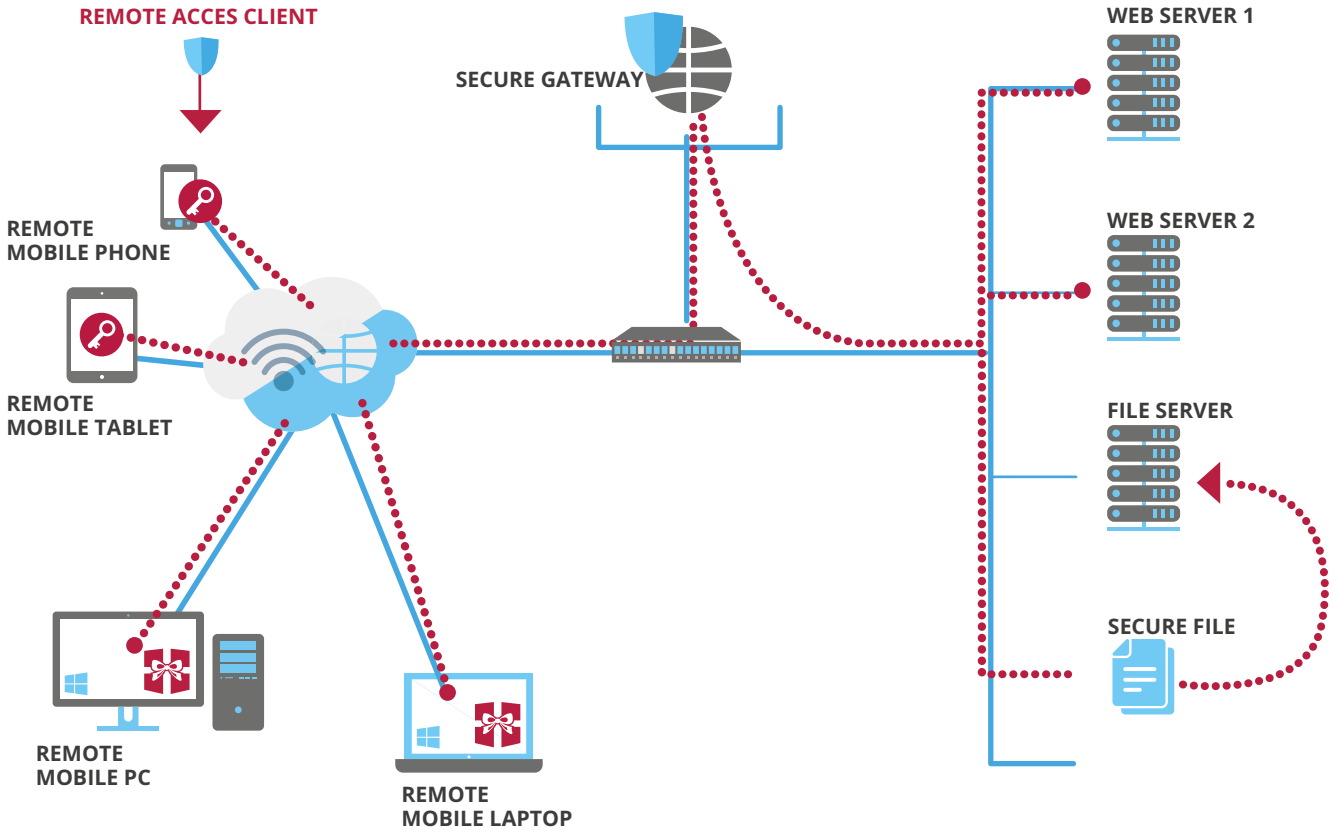
- Sandboxed secure access to internal company web resources, such as Intranet sites, or to the Internet using company access policies. All cached data is automatically deleted after use
- Uses the internal DNS-servers for DNS name resolving without the need for a VPN
- Embedded password manager for Single Sign-On authentication
- Central management portal
- Comprehensive usage logging

A stand-alone Soliton SecureBrowser can be used on macOS, iOS and Android platforms to access documents and company resources.

Related documents:

- Product sheet SecureBrowser

WRAPPINGBOX AND SECUREBROWSER INFRASTRUCTURE



SecureBrowser: available on Android, iOS, macOS and Windows

WrappingBox: includes SecureBrowser

INTEGRATION WITH OTHER SOLITON PRODUCTS

Soliton SecureGateway

WrappingBox is always used in conjunction with Soliton SecureGateway to securely connect to company resources.

The SecureGateway prevents the web servers from having to be Internet-facing. Data in transit between the gateway and the remote client is always encrypted and does not require certificates on each web server. Provides DNS name resolving on the internal network to offer full functionality to the SecureBrowser

Soliton SecureFile

WrappingBox requires Soliton SecureFile to securely transfer files to and from company servers.
It does this by creating a web-based view on internal file repositories, like a Windows-server. SecureFile also enables a private file repository for each user.

Files stored in this area are automatically available on all the users' devices for quick access or reference, without the need for an external cloud service. Using SecureFile, administrators remain in full control over the documents. SecureFile logs all access to files and records which user has downloaded what files and at what time. It can integrate the logging with existing logging and monitoring systems.

Integrating SecureFile does not require any changes to the internal servers, the access rights of the target server will be effective.

SOLITON NETATTEST EPS

WrappingBox can use a client certificate that is installed on the user's device as a second authentication factor, when this is a mandatory requirement from the Secure Gateway. Soliton's NetAttest EPS supports organizations with the creation and safe distribution of client certificates to user devices. An integration with the Soliton NetAttest EPS-series adds an extra layer of security in the form of strong user- and/or device authentication. It provides the possibility to automatically populate the user's logon name from the digital certificate preventing the user from using another identity while logging on.

Related documents:

- Product sheet NetAttest EPS

SPECIFICATIONS

- WrappingBox is a Microsoft® Windows® application with a very small footprint
- Can be easily installed and removed
- Does not interfere with the local installation of applications, just allows them to run in wrapped mode using Microsoft® Component Object Model (COM)
- Embedded Soliton SecureBrowser Pro

VIRTUAL APPLIANCE

	SECUREGATEWAY
Supporting virtual platform	VMware ESXi 6.7 / 6.5 / 6.0
VMware virtual machine version	10
Virtual machine image	OVA
Number of CPU	4
Memory size	8 GB
HDD 1	4 GB
Network adapter	4

	SECUREFILE
Supporting virtual platform	VMware ESXi 6.7 / 6.5 / 6.0
VMware virtual machine version	10
Virtual machine image	OVA
Number of CPU	4
Memory size	8 GB
HDD 1	500 GB
Network adapter	4

ABOUT SOLITON SYSTEMS

Soliton Systems has a strong vision to innovate solutions to logically fulfil the needs of our customers without adding complexity. Soliton support companies with their security management challenges, including network security and remote access to the internal and cloud applications. Soliton's solutions protect the company's resources from unauthorized access and accidental data leakage.

EMEA office

Soliton Systems Europe N.V.

Gustav Mahlerplein 2, 1082 MA Amsterdam, The Netherlands

+31 20 301 2166 | emea@solitonsystems.com | www.solitonsystems.com

SOL19051701v1