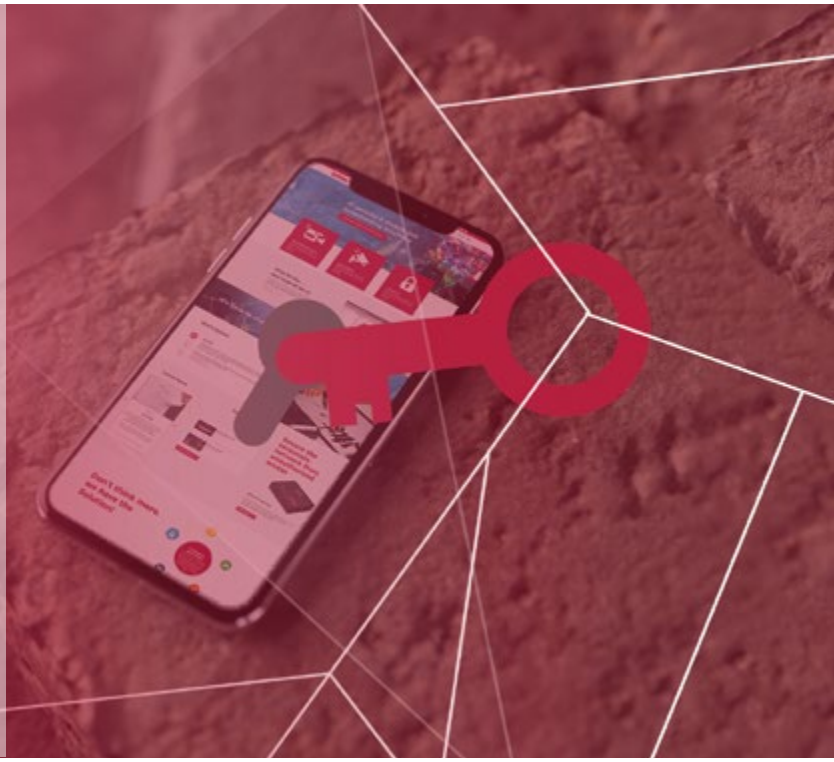
Soliton®

Secure Browser

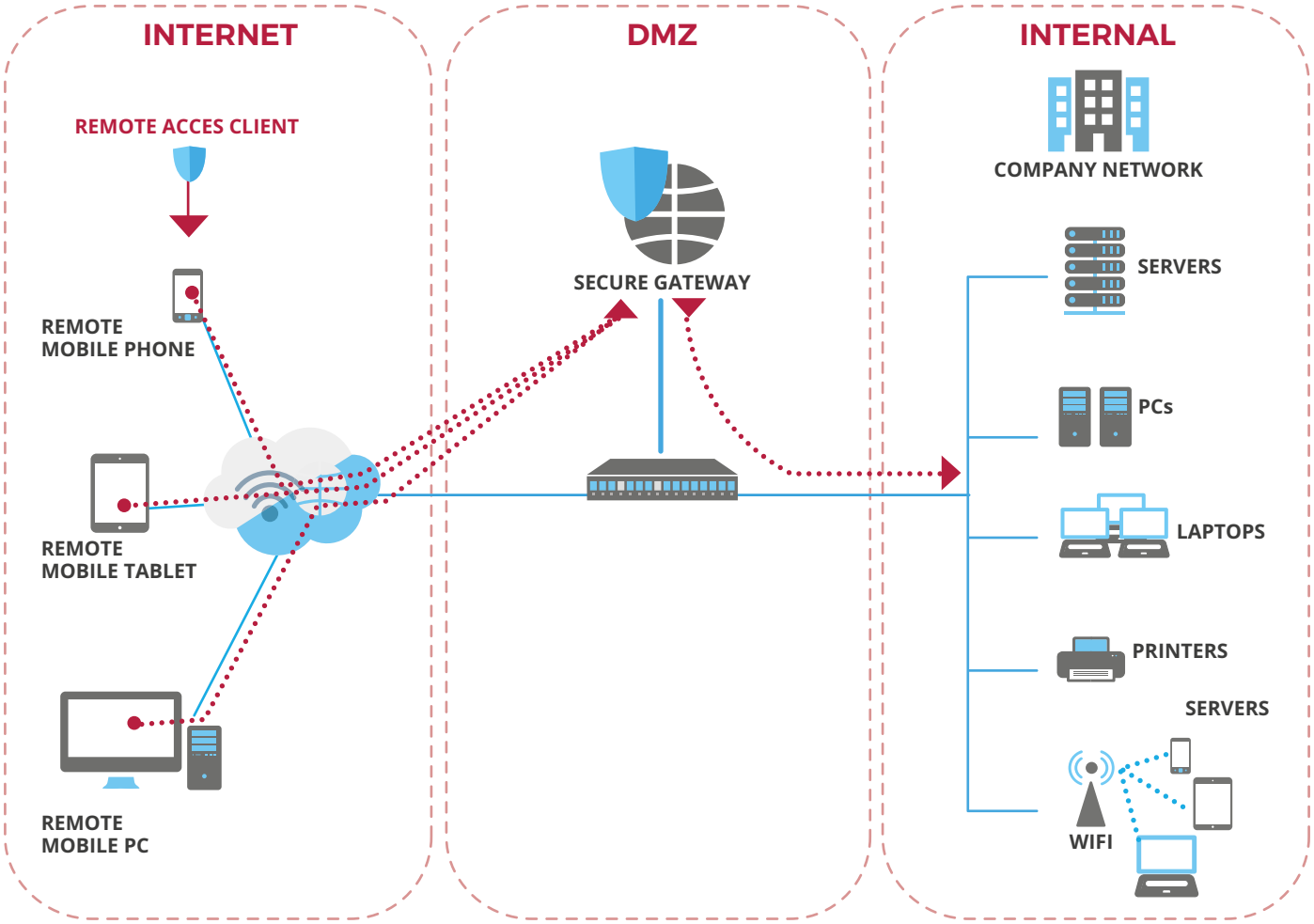


Soliton SecureBrowser is a remote access solution that establishes connections between a remote device and web servers inside an organisations' network. A secure gateway is used to separate the remote device from the network, secure the connection and provide all necessary connectivity. The internal web servers do not have to be Internet-facing, while at the same time offering full functionality.

On the client-side, users use a dedicated SecureBrowser that is used to connect to the internal web servers and as well to the external cloud services. While securely working with company data, users can still use any other browser to connect to Internet-resources. In SecureBrowser, users get access based on permission rules or Active Directory group membership. The URL's are automatically provided, users do not need to remember them. The SecureBrowser contains a document reader, allowing documents to be opened on the client without the risk of data leakage. The SecureBrowser will delete all browsing data after the session is terminated. If required, SecureBrowser can enforce strong user and device authentication and even bind a user identity to a device.

SecureBrowser is available for Windows, Mac, Android and iOS

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.

SECUREBROWSER COMPONENTS

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.

SecureBrowser: Available on all platforms. End-users can download the app from the relevant app stores. The SecureBrowser client automatically provides the links to the web servers that the user is authorized to use, users do not have to remember the URL. It also provides Single Sign On (SSO) to applications for user convenience. SecureBrowser prevents the user from installing plugins and purges all cached data automatically after the termination of the connection.

KEY FEATURES AND BENEFITS

The SecureBrowser supports a number of key features, including:

- **Internet access with sandboxed browsing:** When users shut down the browser, all browser data is deleted. Automatically erasing of cache is also possible after a pre-set period.
- **No need for VPN:** The SecureBrowser creates one access route to the internal applications and uses internal DNS servers. Users can still use their personal browser for private reasons.
- **Usage log:** The SecureGateway logs all access attempts, such as user information, what time the user logged in and the resources that were accessed. The SecureBrowser can integrate the logging with existing logging and monitoring systems.
- **Central management console:** Provides IT full control on settings, users and usage. IT administrators can control the access to other applications, prevent copy/paste/download of files or allow the download of files in a dedicated secure environment.
- **Built-in document viewer:** On Windows, iOS and Android devices, Microsoft Office-documents, PDF files, images and a selection of other files are displayed in a secure area and automatically deleted after shutting down the browser.
- **Comfortable browsing:** Including tab browsing for using multiple web pages, searching on the address bar, corporate common/ personal bookmark, copy/paste only possible inside the Secure Browser, full screen and gesture control (iOS/Android).
- **Complementary to Mobile Device Management (MDM):** Companies using MDM solutions can push the SecureBrowser as the default mobile browser on devices for an extra layer of security.

OPTION SECUREFILE

SecureFile enables the secure access, download and upload of files from a PC, mobile device or tablet to the internal file server via the SecureBrowser. 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.

INTEGRATION WITH OTHER SOLITON PRODUCTS

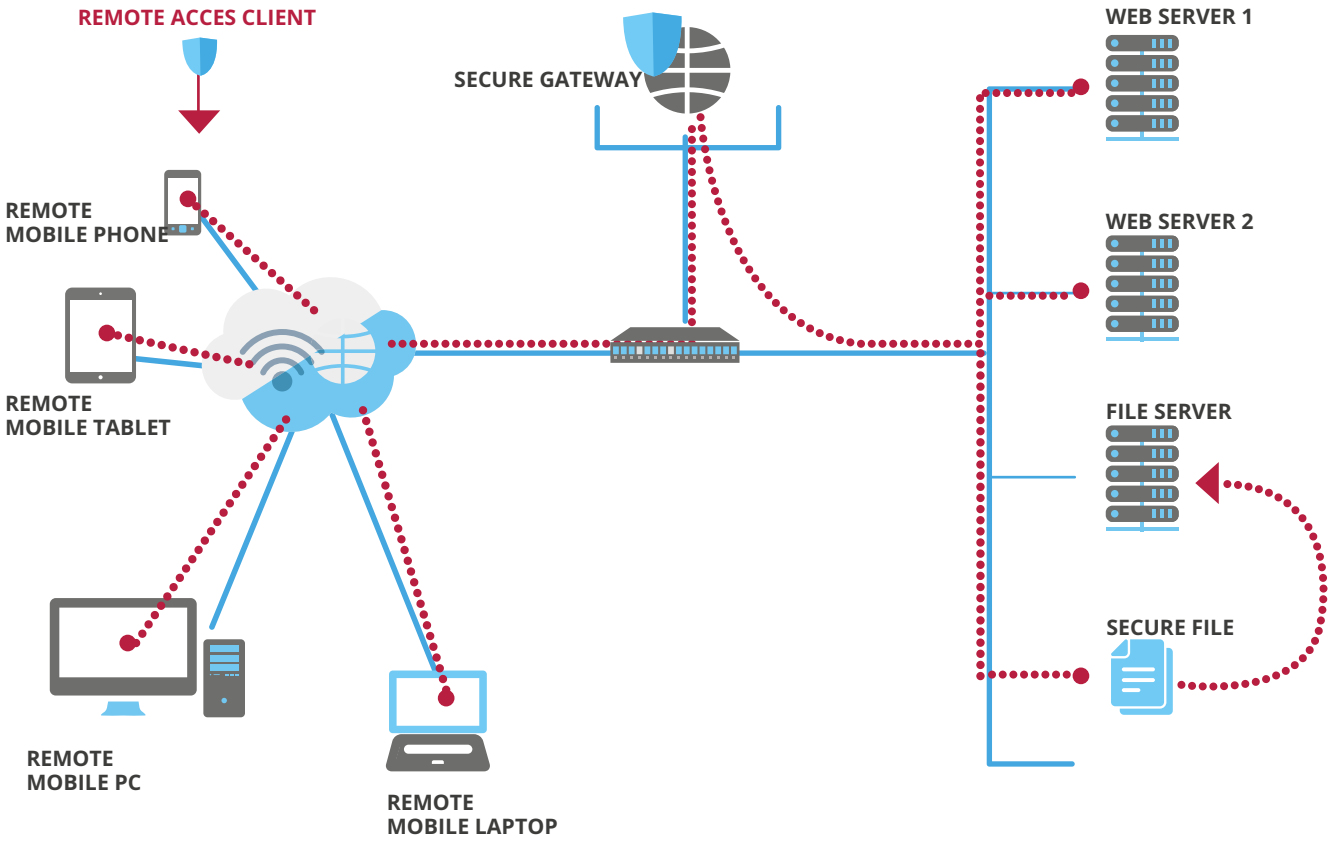
SecureContainer – DME

The SecureBrowser integrates with Secure-Container – DME to deliver secure access to document or website links received in emails.

NetAttest EPS-series

SecureBrowser can use digital certificates for strong authentication purposes. 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.

SECUREBROWSER INFRASTRUCTURE



SPECIFICATIONS SECUREBROWSER

SPECIFICATIONS

Platform	Windows, Mac OS, iOS, Android
Operating systems version	Windows 10 / Windows 8.1 (except RT) / Windows 7SP1 Mac OS 10.13x / 10.12x iOS 12.0 / 11.4-11.0 / 10.3-10.0 Android 9.0 / 8.1-8.0 / 7.1-7.0 / 6.0 / 5.1-5.0
Number of users	100 / 500 ~ 20,000
Supported authentication server	RADIUS (PAP, CHAP), LDAP, CRL obtaining HTTP)
Log output destination	Local, Syslog

PHYSICAL APPLIANCE

Form factor	EIA19 inch (incl. rack mount kit)
Dimensions (W x D x H)	443 x 44 x 386 mm
Network interface	Auto-MDI-X x 4 ports
Weight	7.1 kg
Power supply	90 ~ 264VAC / 47 ~ 63Hz (90 ~ 135Vac)
Max. power consumption	107 VA
Calorific value	409.2BTU/h / 103.1kcal / 120W
Operating environment	Temperature 0 ~ 40°C / Humidity 20 ~ 90% RH non-condensing
Certifications	VCCI (Class A), FCC (Class A), CE (Class A), UL, RoHS, PSE (power cable)

VIRTUAL APPLIANCE

Supported 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	8,192 MB
HDD 1	4 GB
Network adapter	4

SPECIFICATIONS SECUREFILE

SPECIFICATIONS

Supported file protocol	CIFS / SMB
Supported authentication server	Local (CSV importable) LDAP
Log output destination	Local, Syslog (UDP)
Operating confirmation browser	SecureBrowser
Other functions	SNMP (agent), NTP time synchronisation, UPS compliant

PHYSICAL APPLIANCE

Form factor	EIA19 inch (incl. rack mount kit)
Dimensions (W x D x H)	443 x 44 x 386 mm
Network interface	Auto-MDI-X x 4 ports
Weight	7.3 kg
Power supply	90 ~ 264VAC / 47 ~ 63Hz (90 ~ 135Vac)
Max. power consumption	120 VA
Calorific value	409.2BTU/h / 103.1kcal / 120W
Operating environment	Temperature 0 ~ 40°C / Humidity 20 ~ 90% RH non-condensing
Certifications	VCCI (Class A), FCC (Class A), CE (Class A), UL, RoHS, PSE (power cable)

VIRTUAL APPLIANCE

Supported 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	8,192 MB
HDD 1	4 GB
HDD 2	500 GB
Network adapter	4

ABOUT SOLITON

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

SOL1902201v1