Soliton®

Secure Container DME

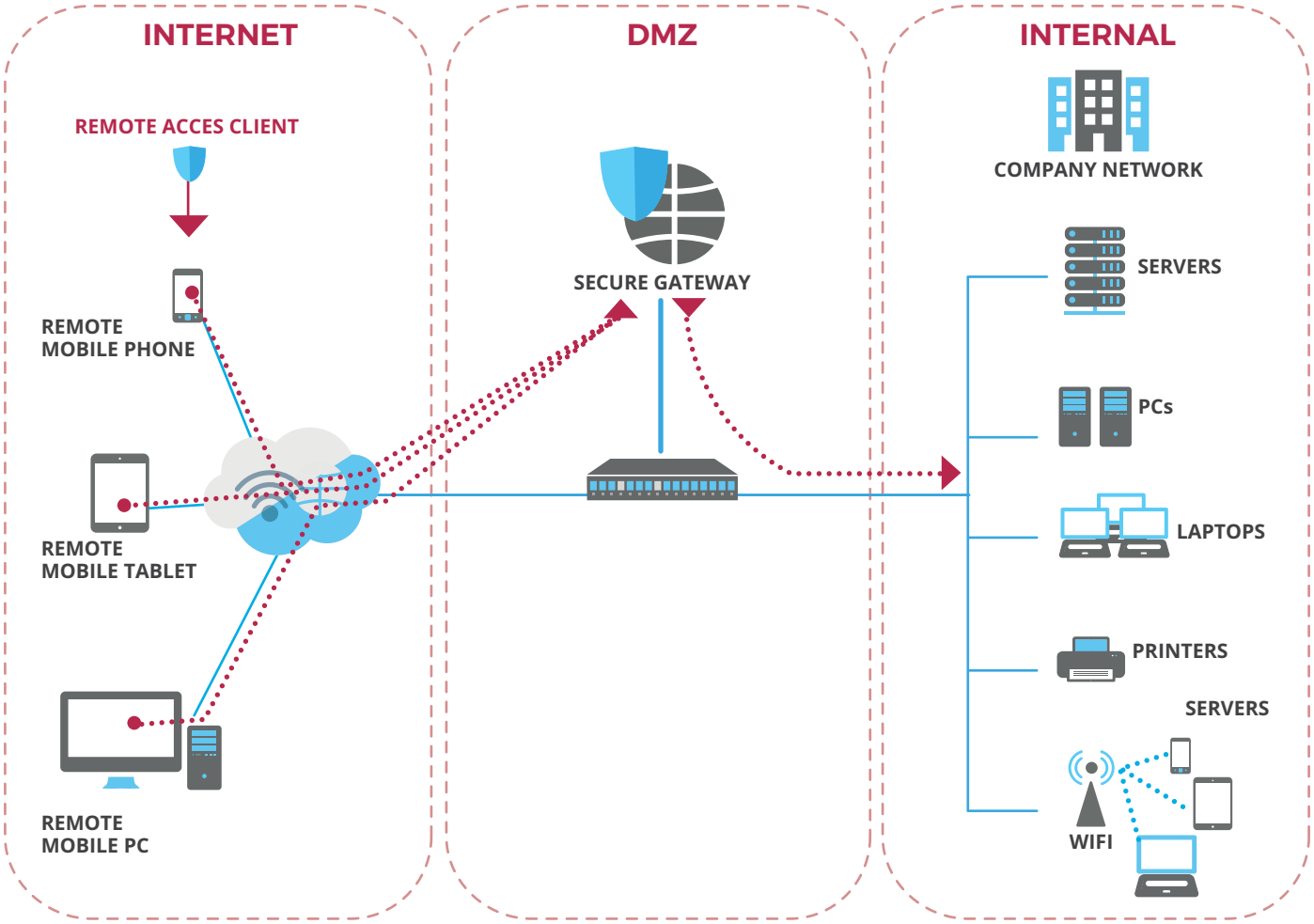
Soliton SecureContainer - DME is a remote access solution enabling employees to securely access corporate data using their mobile devices. Corporate e-mail, calendar, to-do's and other resources are synchronized with the collaboration server. Documents can be downloaded from the company fileservers, temporarily stored, viewed and edited, and uploaded. SecureContainer - DME also enables direct access to company web servers.

All corporate data leaving the organisation is stored inside a secure container on the mobile device. The data inside the container is protected using 128-bits AES-encryption and is accessible via the app. The data can only be accessed by users that can authenticate against the container, even when offline. Administrators are in full control of the secure container and the authentication requirements. Users remain in full control over their (private) device using the local clients and apps for personal use.

The secure gateway separates the remote device from the network, secures the connection and provides all necessary connectivity. One or more connectors make the connection with the internal collaboration servers or Office 365 in the cloud.

SecureContainer - DME is available for iOS and Android.

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 URLs.

SECURECONTAINER DME COMPONENTS

SecureGateway:
Prevents the corporate servers to be Internet-facing. Data in transit between the gateway and the remote client is encrypted using HTTPS. The SecureGateway connects to one or more connectors providing the interaction with the internal Microsoft Exchange or IBM Notes collaboration servers. The gateway and the connectors are available for Microsoft Windows and selected Linux Distributions. Administrators have full control over user- and device access - not over the device itself.

Connectors:
The connector acts as a bridge (connector) between the DME gateway and the collaboration system(s) of choice. By connecting from the internal network to the DMZ only the connectors contribute to additional security.

Client:
Available on iOS and Android. End-users can download the app from the relevant app stores. Users connect the Client to the corporate servers, which requires the user to enter only one URL, an internal directory username and a valid password. After verification, a device certificate is generated for future device authentication. The secure container is created automatically.

SECURECONTAINER DME KEY FEATURES

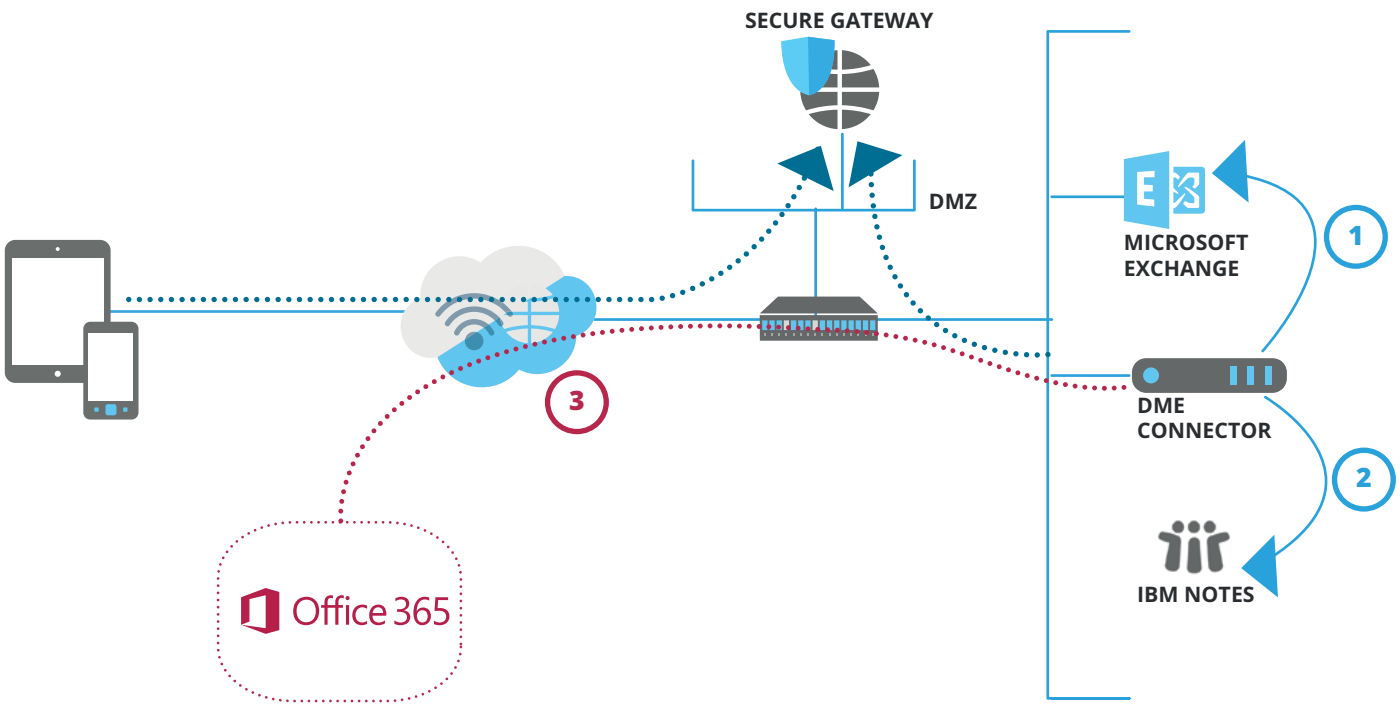
- **Complete separation of business and personal data:** all corporate data is securely stored inside the container on the user's device, all personal data is stored on the device itself. Administrators control the interaction between the two types of data.
- **Data leakage prevention:** The container is encrypted with 128-bit AES-encryption; the corporate data cannot leak to the user's device or the cloud.
- **Remote wipe:** Administrators can remotely wipe the secure container. This operation does not affect the users' personal data on the mobile device.
- **No need to manage the device:** Administrators control the secure container and therefore need not to have full management control over the device (no mobile device management).
- **Single Sign On (SSO):** Single Sign On (SSO): Authentication methods include username and password, swipe gesture, TouchID or FaceID.
- **No use of a Network Operations Centre (NOC):** SecureContainer – DME is an on-premises solution enabling organisations to be in full control. No third-party components are required. All encryption keys are generated within the solution.
- **No need for a VPN:** SecureContainer – DME creates one access route to the internal applications and uses internal DNS servers.
- **Central management console:** Offers IT administrators the possibility of enforcing policies, set user access roles, distribute and manage HTML5 apps, and application blocking.
- **Basic MDM functionalities embedded:** For additional security basic MDM functionalities such as enforcing password controls, remote blocking and detection of rooted or jailbroken devices is included.
- **No dependency on Microsoft ActiveSync:** ActiveSync to synchronize data to and from the remote mobile devices is not required.
- **Fully functional workplace in one app:** contains PIM data (e-mail, calendar, to-do's) document transfer, secure local storage, editing and viewing capabilities and remote access to internal web-based systems.
- **Viewer/Editor:** Users can view and edit attachments sent in e-mails or documents stored in the secure container, on- and offline.
- **AppBox:** The optional AppBox is an HTML5 and JavaScript enabled browser providing direct access to internal web-resources. The AppBox enables IT administrators to control the communication between the secure container on the mobile device and the internal servers.

INTEGRATION WITH OTHER PRODUCTS

SecureBrowser

The SecureBrowser establishes connections between a remote device and web-servers inside an organisation. It delivers secure access to document or website links received in emails.

INFRASTRUCTURE SECURECONTAINER - DME



Want to learn more about our solutions? Contact us at: emea@solitonsystems.com

SPECIFICATIONS

DME GATEWAY AND DME CONNECTOR

PLATFORM	WINDOWS	LINUX
Operating systems version	**Microsoft Windows Server:** 2008 R1 and R2 with all patches applied 2012 in full server mode with all patches applied 2012 R2 2016	Red Hat Enterprise Linux (RHEL) 5 and CentOS5 RHEL or CentOS 6-7 (64 bit only) SuSE Linux Enterprise Server 12 and later
Supported authentication server	LDAP, Open LDAP or Novell eDirectory	

DME CLIENT

PLATFORM	EXCHANGE	MS OFFICE 365	DOMINO
Requirements	MS Exchange 2007 SP I or above MS Exchange 2010 SP I or above MS Exchange 2013 MS Exchange 2016 (requires DME 4.5 SP I or later) MS Active Directory	DME support MS O365 under the following circumstances: O365 runs in a dedicated plan; the customer uses a local AD for user management; Single Sign On (SSO) is enabled between on-premises AD and the Microsoft Cloud	32/64 bit Lotus Domino version 8.5 or later* Domino LDAP Minimum on connector: Notes session mode: Lotus Notes 8.5.x. basic or higher Domino session mode: Domino Server 8.5.3. FP6 or higher

**Restrictions apply when using Domino on the IBM iSeries, pSeries and zSeries platforms. Please contact Soliton or a Soliton partner for more information*

DATABASE

PLATFORM	WINDOWS	LINUX
Requirements	Microsoft SQL server 2008 / 2012 / 2016 / 2017 on a separate or on the DME server	Microsoft SQL server 2008 / 2012 / 2016 / 2017 on a separate and on the DME server MySQL 5.x delivered with Linux 5-7 or MariaDB 10 on a separate or on the DME server

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

SOL1804290301v1