e-Jan

CACHATTO®
SecureContainer

Remote access solution

*As of January 2022

What is CACHATTO?

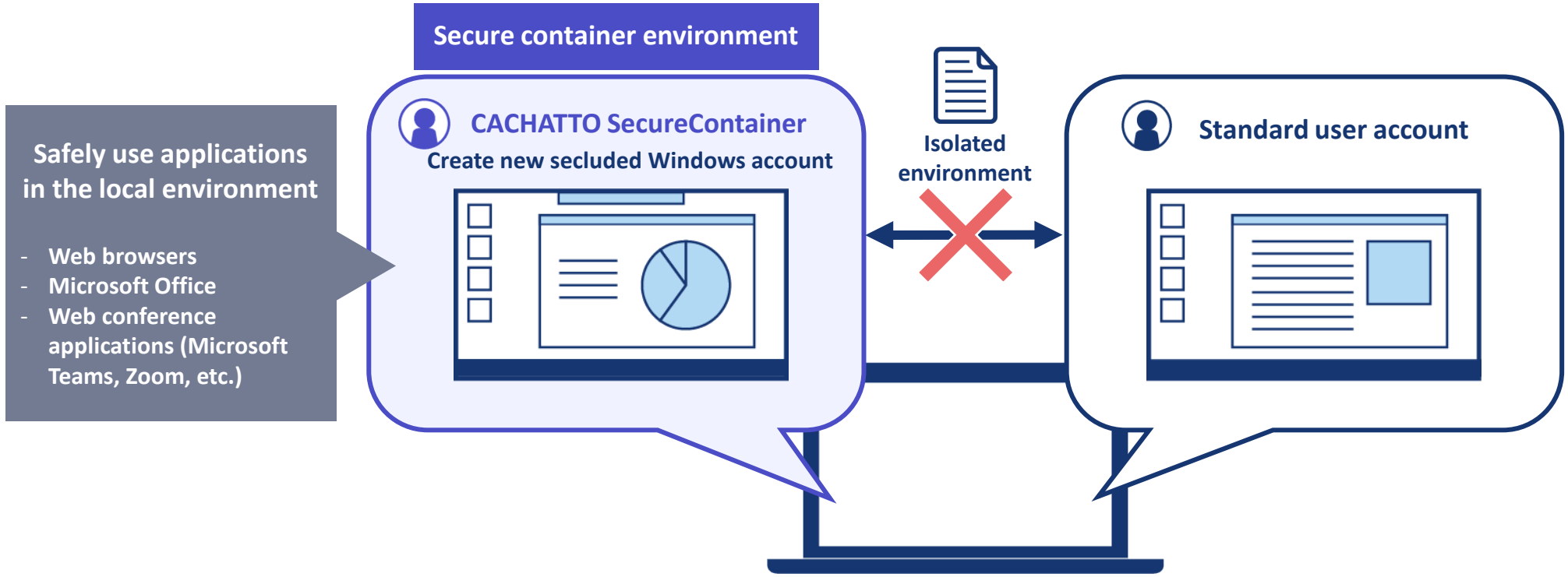
Provides a secure resource access environment

CACHATTO is a remote access service that enables users to conveniently access to the intra/cloud business system in a single secure platform from a variety of devices.
It ensures a high-level of access security and delivery of the right applications and resources to the right users, and keeping accessed data stay within the secure environment.

What is CACHATTO SecureContainer?

Secure workspace utilizing native applications

CACHATTO SecureContainer provides secure workspace (secure container area) generated on an access Windows PC, a secure and comfortable telework environment is provided while utilizing the local resources of the PC.



What is CACHATTO SecureContainer?

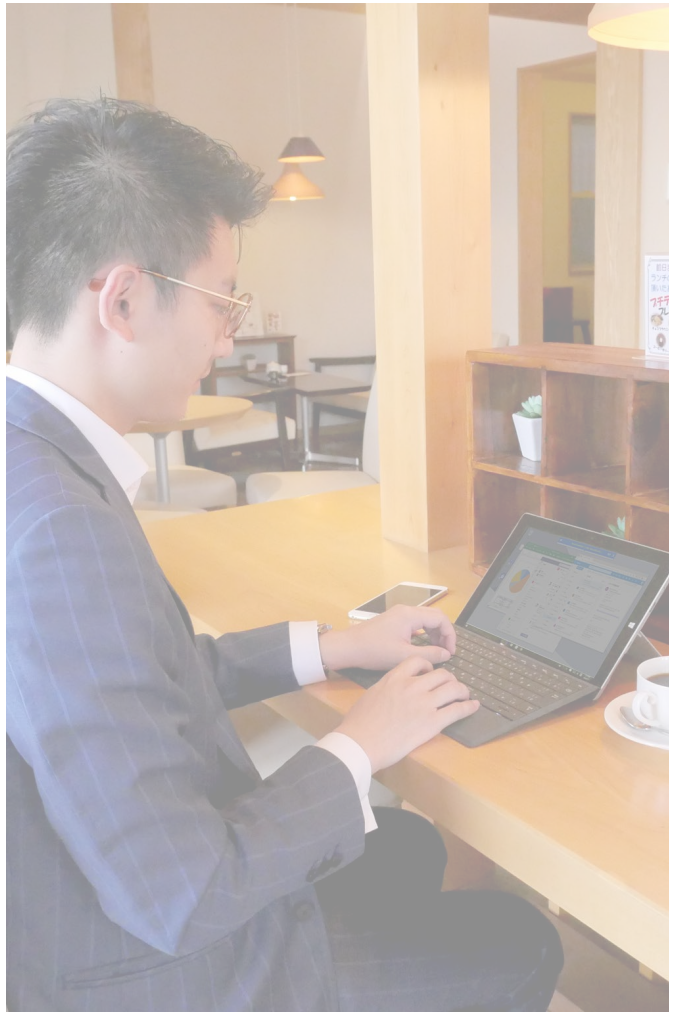
Access authorized files within a secure environment via unmanaged PC

Objective

- Provide a safe environment to access on-prem and cloud-based resources, and a way to use native applications to create or edit files
- Have an ample management and a way to enforce security policies even if user is using a personal or unmanaged computer

Solution

- Create an isolated secured container that can utilize natively installed applications, while keeping all accessed and saved data secure only within the environment
- Link with IDaaS (Authentication Provider Service), to access cloud-based resources that can be restricted only from secure container application
- CACHATTO SecureBrowser may also be used to access on-prem and cloud-based resources



What is CACHATTO SecureContainer?

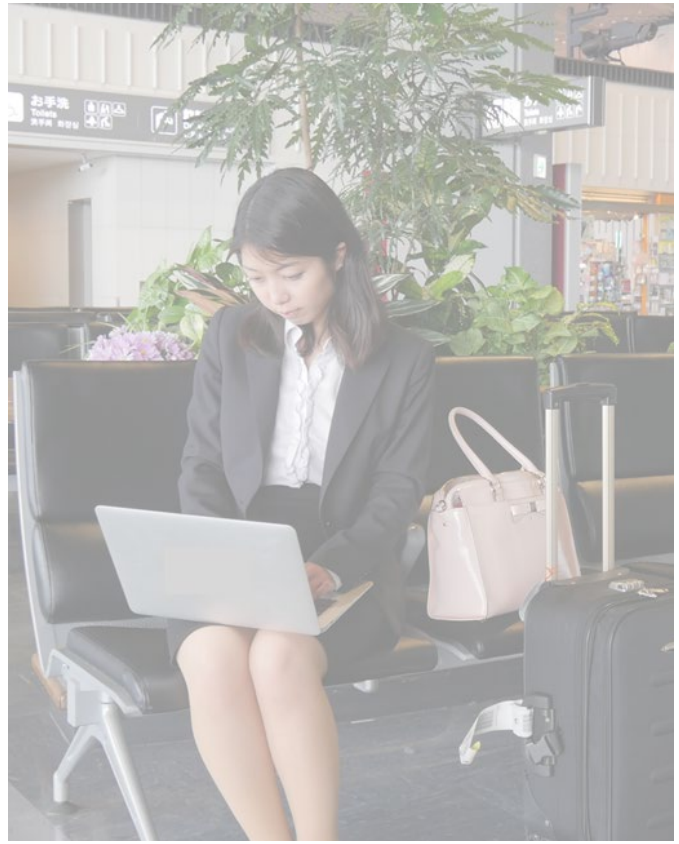
Network connectivity independency

Objective

- Work remotely without the use of remote desktop connection due to its dependency on network environment
- Reduce the operational load on the connected PC

Solution

- On-prem resources are made available thru a SecureBrowser and cloud-based services can be directly accessed from a secure environment
- There is no need to setup a streamer connection, like remote desktop or Virtual desktop (VDI), to access resources



What is CACHATTO SecureContainer?

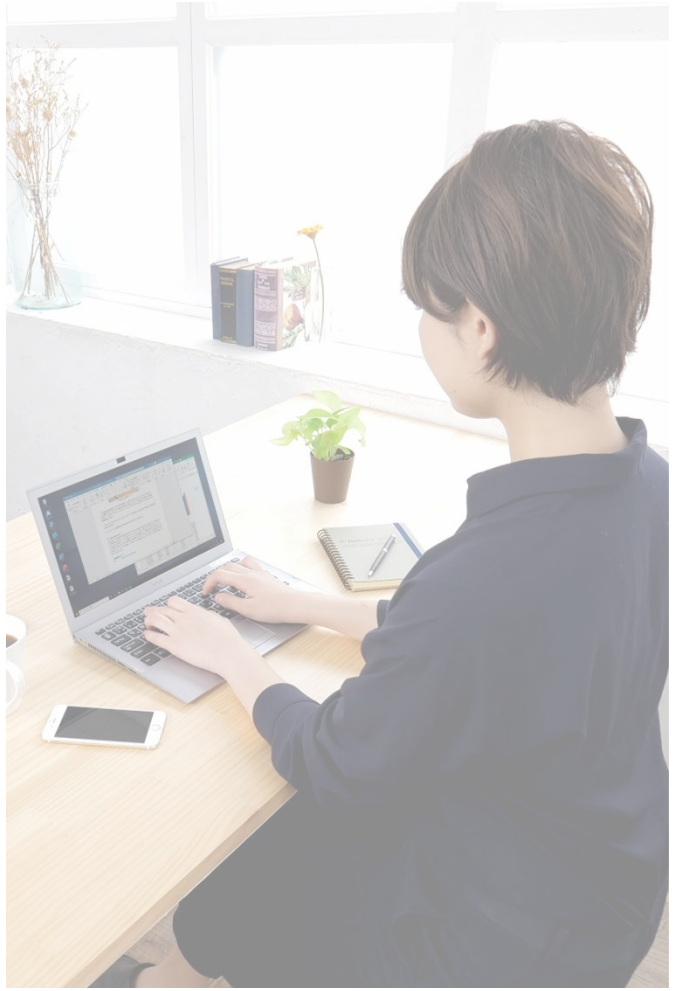
Use of native applications and web conferencing applications

Objective

- Use of natively installed applications, including communication tools
- Ensuring that data are kept within a secure environment to prevent data from leaking

Solution

- Web conferencing applications, including Microsoft Teams, can be safely and directly be used within a secure area. Microphone and web cams can also be utilized.
- The applications installed locally on the PC can be also utilized in the secure workspace
- Administrators can configure the settings to allow data to be kept within the SecureContainer to be accessed on next login, or clear all data upon closing of the environment



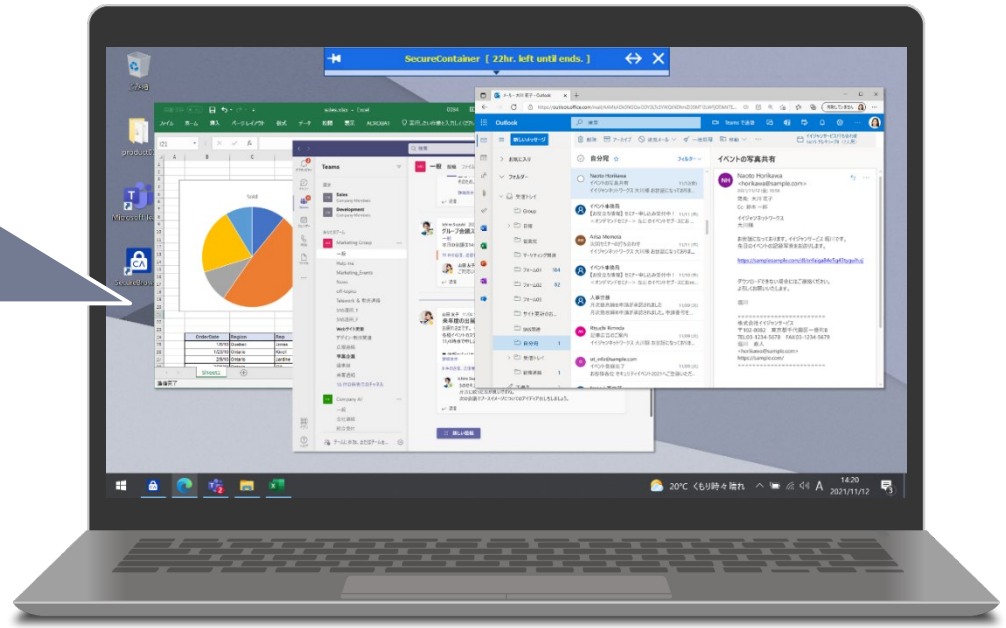
CACHATTO SecureContainer

Isolated workspace

The system creates a new Windows user account isolated from the local set account, dedicated to create a secure contained workspace. The SecureContainer environment is a dedicated Windows user account that is generated separately from the standard user account. It is completely isolated, restricting any file sharing and transfer between accounts.

Secure isolated workspace

- **Use locally installed applications**
- **Web camera and microphone in the local PC can be utilized**
- **Accessed or created files are securely stored within the workspace**
- **On-prem and cloud-based resources can be accessed and edited/created files can be uploaded via CACHATTO SecureBrowser***



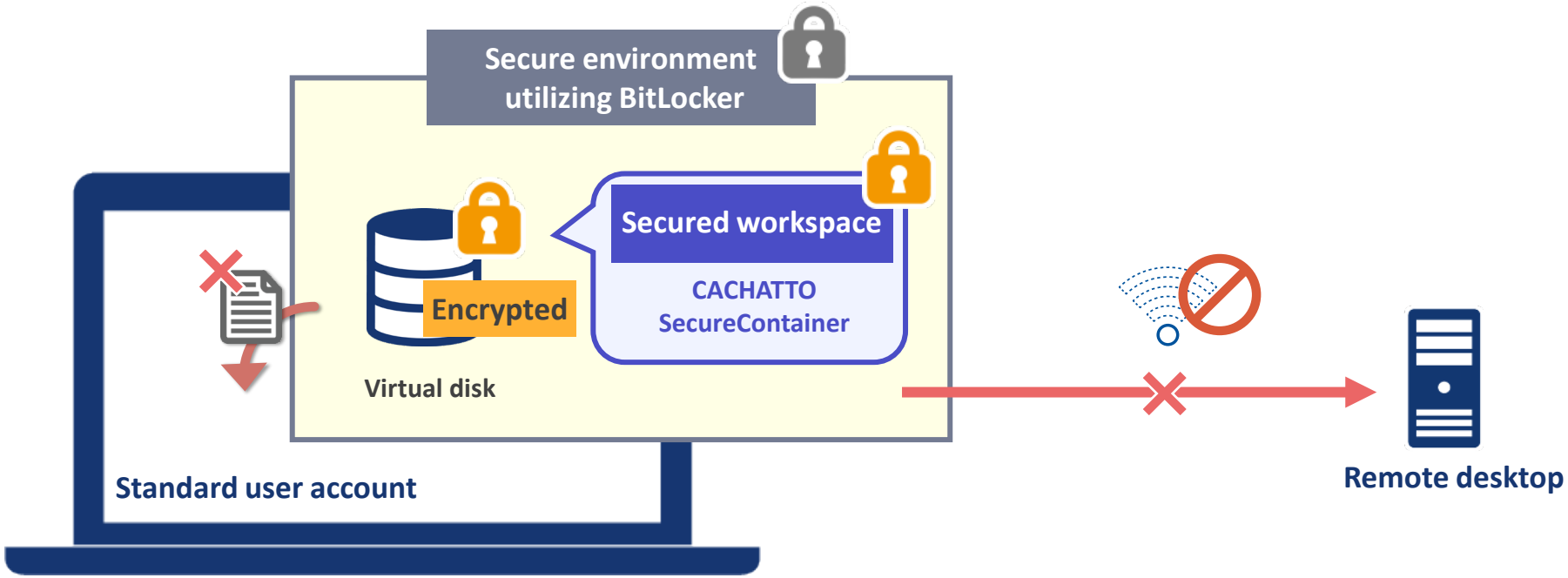
*File upload/download limitations may apply

CACHATTO SecureContainer

Keep data within a secure workspace without the need to connect to a remote desktop

By utilizing Windows BitLocker, CACHATTO SecureContainer is set within an encrypted virtual disk, which is completely inaccessible locally. This reduces the risk of information leakages when the device is stolen, lost or used by unauthorized user.

CACHATTO SecureContainer provides a workspace which users can use to complete work-related tasks without the dependency of internet connectivity stability, while making sure files are kept locally isolated and secure.

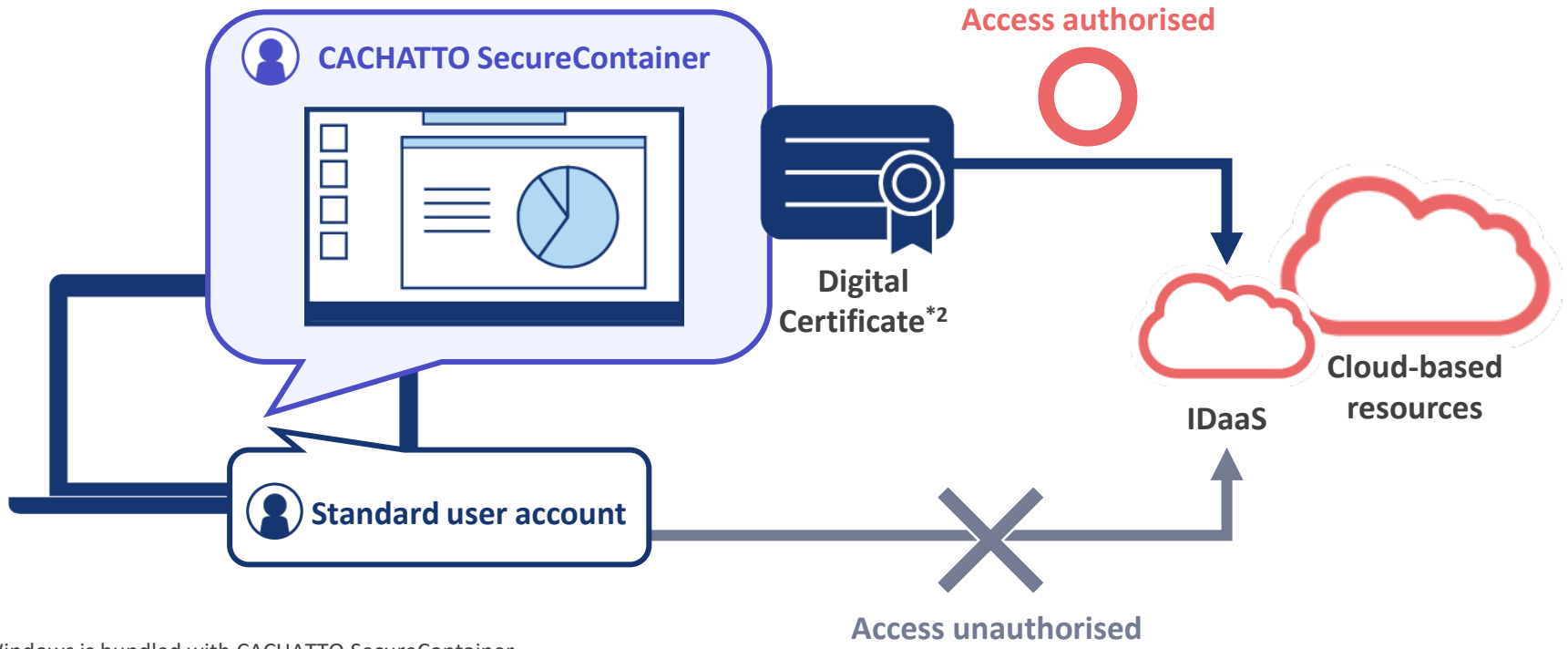


CACHATTO SecureContainer

Accessing on-prem and cloud-based resources

On-prem and cloud-based resources can be accessed through CACHATTO SecureBrowser*1.

However, cloud-based services can also be accessed by linking with IDaaS (Authentication Provider Service) that has client certificate issuance/authentication functions, allowing access within the SecureContainer while restricting it for the local account.

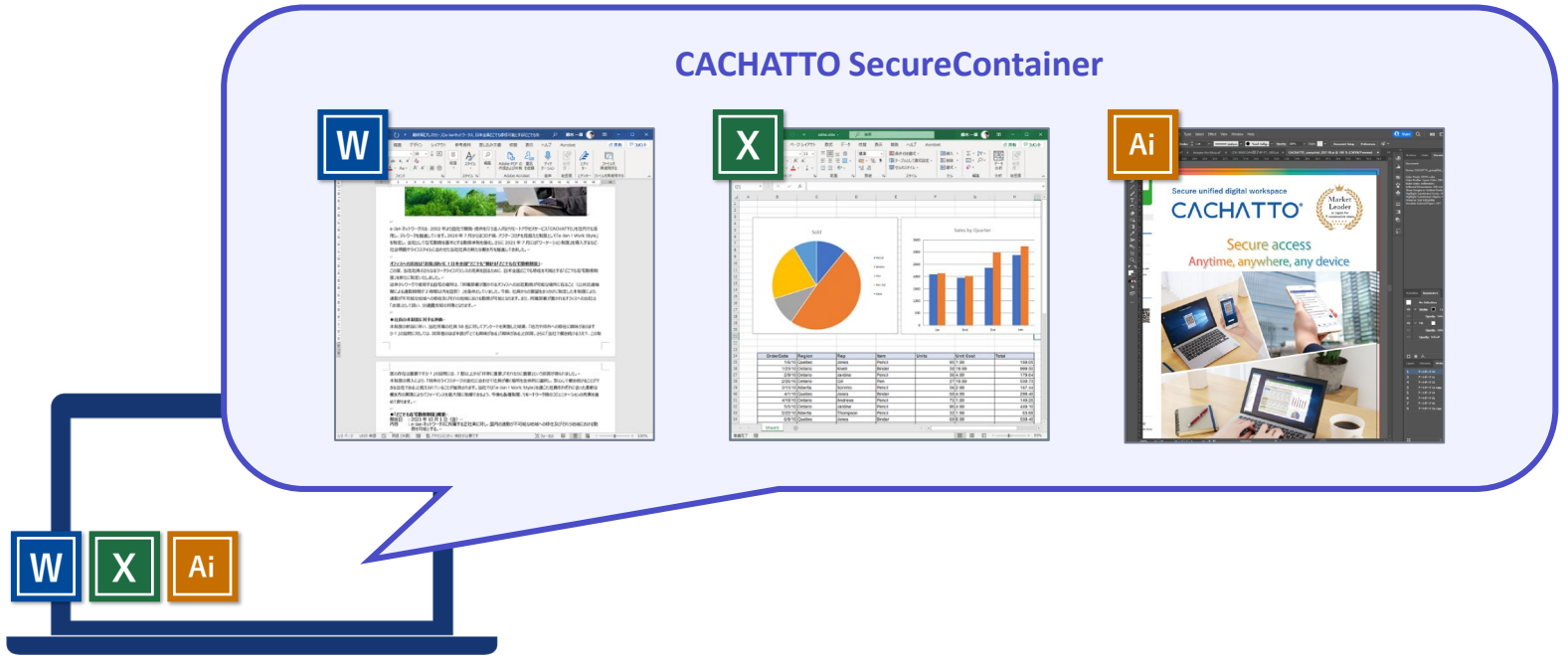


*1 CACHATTO SecureBrowser for Windows is bundled with CACHATTO SecureContainer
*2 Client certificate not included in CACHATTO SecureContainter solution

CACHATTO SecureContainer

Utilising locally installed application

Users can view and edit files using Microsoft Office or any of the locally installed applications. CACHATTO SecureContainer uses local resources such as the local applications, memory and CPU, so you users work lightly.



* Microsoft Office and/or other applications must be set prior to use with the SecureContainer.
* Adobe applications are not officially supported.
* Some applications may not be supported.

CACHATTO SecureContainer

Functions and features

Building telework environment

There is no need to set a physical PC or virtual desktop to connect to. No VPN required. The solution is equipped with various management tools, while providing a way to reduce the cost of building a remote-work environment.

Reduce risk of information leakage

Since the export of data to local user accounts is restricted and the data is also encrypted, the risk of information leakage is minimized. Data are kept safe even when accessed using personal or unmanaged PCs.

Authorised-based access

Only users who were provided with digital certificates via IDaaS are given cloud access within the secure environment. Also, access via CACHATTO SecureBrowser is also available to access on-prem or cloud-based resources.

Utilize locally installed applications

Locally installed applications can be used to open, edit or create files. Files within the environment may be uploaded later to a respective portal, file server or sent via email.

Use of web conferencing applications

Web communication applications can be used within the SecureContainer. Also, applications, like Zoom or Microsoft Teams may utilize camera and microphone.

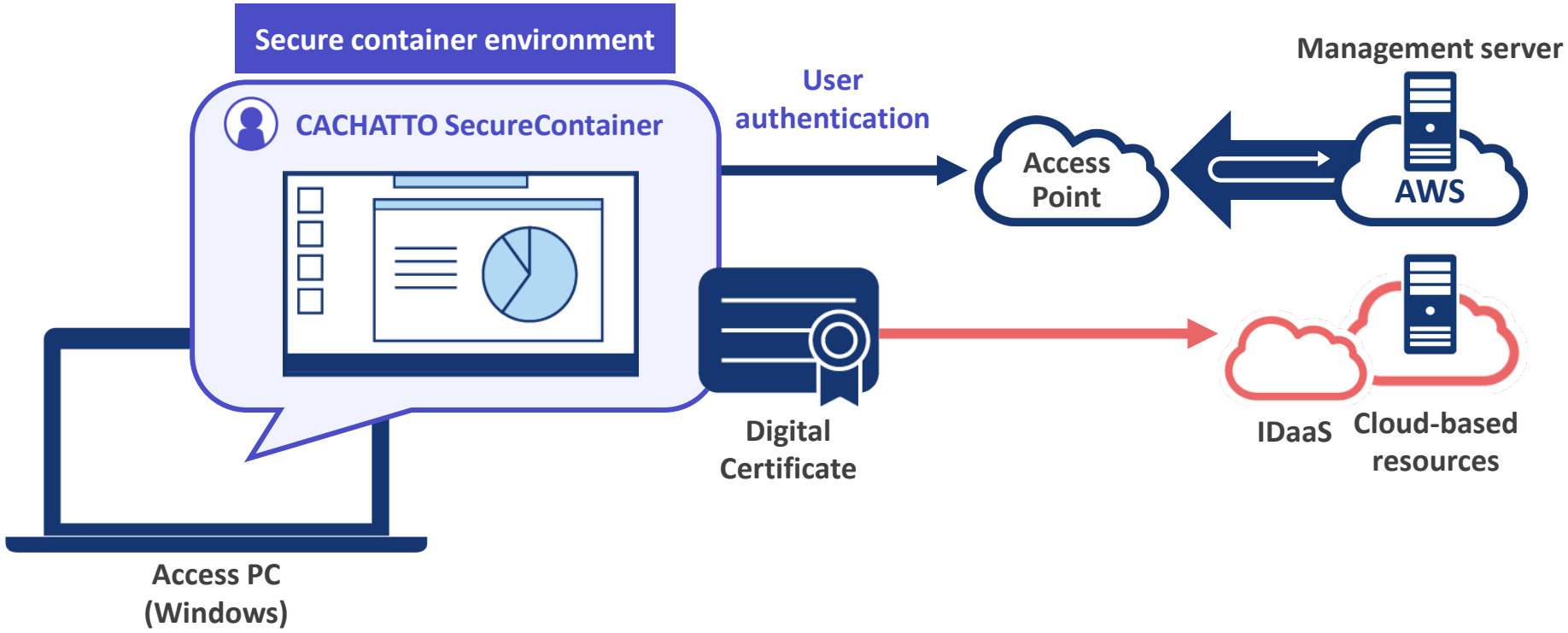
Minimize impact of network connection environment

The solution has offline capacities that help minimize the impact of being dependent on network connection environment for working, unlike remote desktop solutions. Thus, minimizing business inefficiency due to network stability.

CACHATTO SecureContainer Cloud

Management server on the cloud

e-Jan Networks may provide a built management server on the cloud, packaged with (AWS) hosting. This provides a quick and easy deployment without the need of adding equipment such as servers to the company.



*Communication through the customer's internet connection, such as VPN, would be necessary to access on-premise resources

CACHATTO SecureContainer

Recommended usage environment	
Supported OS	Windows 10
CPU	Above or equal to Intel Core i5-8265U
RAM	8 GB

* Verification on Windows 10 is done via "Semi-Annual Channel" from the latest to 3 generations at the time of release.
* Supports Windows 10 Home, Windows 10 Enterprise and Windows 10 Pro.
  Windows 10 Long-Term Servicing Branch (LTSB) and Windows 10 IoT are not supported.
* Please contact us for the minimum operating environment.

CACHATTO

Product and contact information

Product website

CACHATTO product information site	https://www.cachatto.com/en/
CACHATTO SecureContainer page	https://www.cachatto.com/en/csc

CACHATTO free trial

Contact and send an application for a 2 weeks free trial for 5 users by contacting out sales department or partner vendors