REDITE.

Cyber & Data Security

AUTHORISED DISTRIBUTOR SentryBay® ASIA PACIFIC

Armored Client for VDI Remote Access

White Paper

Author: Adam Gurney

Updated: July 2020

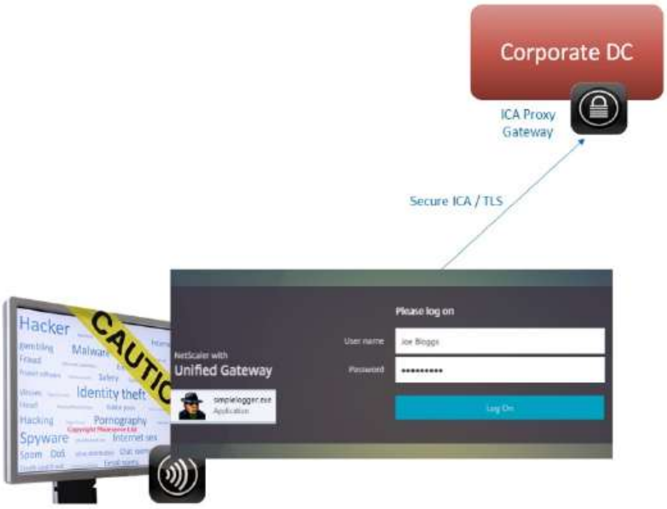
Table of Contents

VDI Secure by Design

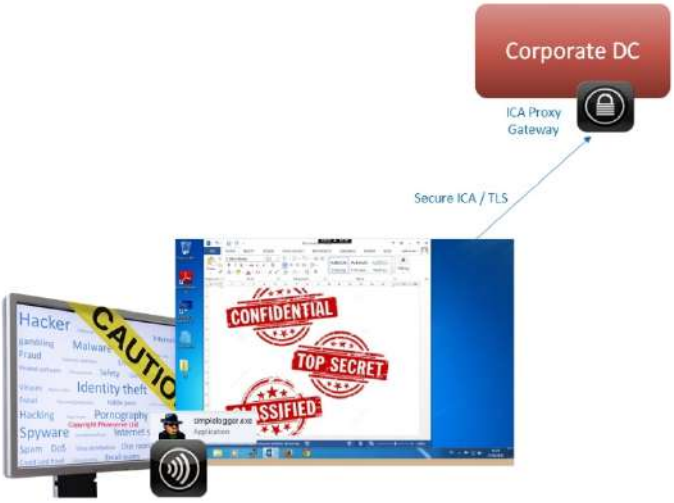
VDI technology has been a preferred method for providing secure remote access to internal corporate applications and data for many years. By design VDI solutions provided by Citrix, VMware and others are very secure, as in effect staff or partners are using a high performance and secure remoting protocol to use desktops, applications, and data. Granular controls can be applied when the user is accessing virtual desktops, applications and data from outside of the corporate perimeter, preventing the user from local drive access, screen printing, printing etc.

By utilising a secure gateway (such as Citrix NetScaler, VMware UAG or F5), which provides multi-factor authentication and proxies the session traffic to the backend systems, one could be forgiven for thinking there are no risks in using it today.

But there has always been a concern if the endpoint used to access the VDI platform is unmanaged. If the endpoint is compromised by threat actors such as malware or hackers, there is a very real risk of keylogging or screen scraping capturing confidential data. In today's heightened security threat landscape, there are also risks of malware (such as Zeus variants) using browser attacks which actively try to exploit the logon process of remote access systems.



User name: Joe Bloggs



Citrix, VMware and AWS Workspaces remote access environments are not disproportionately vulnerable to risk. It is important to note that keylogging, screen scraping, and browser vulnerabilities are the most significant security weaknesses faced when accessing these environments. Nevertheless, compliance auditors are now increasingly demanding that organizations properly audit and take reasonable measures to protect non-corporate machines before allowing remote access to corporate systems.

Corporate remote access into VDI normally requires:

1. An endpoint device connected to the Internet
2. A browser (for the gateway logon process)
3. The VDI client to be installed on the endpoint (Citrix Workspace App, VMware Horizon app etc)
4. User credentials (Username & Password)
5. Multi-factor authentication (Security Token, Pin, Smartcard etc.)

Unmanaged Endpoint Risk

The unmanaged endpoint used for remote working is typically a staff member's personal PC or laptop which the company does not own or manage. This means there is no actual control as to the security posture or state prior to it being used to access the VDI platform with increased risk. In most cases on Windows, the owner will have Local Administration Privileges, making it relatively easy for a threat actor / malware to compromise the machine.

One cannot mandate operating system levels or application versions (including browsers). Even once a user installs the VDI client of choice, the version used ongoing is difficult to control. This, as well as being a security concern, is a major headache as browser types / configurations and VDI client versions cause a very high percentage of support issues related to remote access.

Whilst Cyber awareness training is often conducted for staff members, if they use their home PC for remote access then this is often used by other family members, who may not be as security-savvy, so the risk of compromise is far greater.

Providing 3rd party remote access is also a concern as it may operate to different standards. There have been some very high profile cases in the past few years where breaches have occurred via partners – who were compromised in the first instance.

Most security professionals will agree that running standard Anti-Virus software alone is no longer enough to properly protect a PC. Advanced endpoint security solutions that do not rely solely on signature based detection are emerging but these can still be fallible. Due to management as well as privacy issues these often do not support, or cannot be properly deployed nor maintained on non-corporate devices.

Remote Access – Endpoint Risks Today

If the employee's endpoint device, over which the company exercises no control, is compromised in any way by threats such as hackers or malware, there is a real risk that data or systems access will be exposed. In today's heightened security threat landscape, the following threats should be addressed:

- Keylogging: Key-loggers covertly record every keystroke. Keylogging can result in a treasure trove of data for cybercriminals, including passwords, credit card numbers, bank PIN codes and much more.
- Screen Scraping: This activity can deliver every scrap of data displayed on employees' screens directly into the hands of cybercriminals. Virtual desktop and Remote Access users may be particularly vulnerable to screen scraping attacks.
- Browser-Based Attacks: Workers browsing the internet expose themselves and their employers to a host of additional threats that target the browser software as a gateway. With a wide variety of browsers in use and no lockdown policies in place.
- ICA File Interception (Citrix): ICA files can be intercepted either in flight or from the endpoint's file system and re-used in a timely fashion elsewhere.
- RDP Double-hop or VNC Attacks: Common ways for malicious threat actors to compromise confidentiality on endpoints is by use of RDP & VNC attacks.
- Printing: The Windows printing sub-system can be exploited by common malware, at the point a print job is passed to the Print Spooler (from any application) it can be copied and content displayed by a malicious threat actor.

General Endpoint Risks

- Elevated User Privileges: Being a non-managed machine it should be assumed that most users will have local Administrator privileges on their own machines which increases risks of compromise greatly.
- Security Posture of Device: Ensuring that the device is patched and running Anti-Virus as well as a personal firewall is in use, should be a minimal requirement. This however does not guarantee the host is not already or cannot be compromised.
- Shared Device: It is entirely feasible that the device may be used by other family members who may have no security awareness training.
- Phishing Attacks: The most common way of distributing malware is by use of email. It should be assumed that email systems that do not have enhanced anti-phishing protections are used regularly which greatly increases the risk of infection.
- Counterfeit / Malicious Software: Often software is installed from dubious sources, so there is a high risk of Malware infection.
- Device used on High Risk Wireless Networks: Entirely feasible that the device could be used for remote access whilst on un-secured public Wi-Fi-networks. Heightened risk of network snooping and other malicious attacks.

How is the non-managed endpoint risk addressed today?

Apart from accepting the risk and doing nothing, the following types of solution are seen in the field today to try to address the problem:

Corporate Laptops

Many companies simply provide corporate laptops to staff for remote access. This is expensive (particularly if they are only used to allow access via the corporate environment via a VDI client) and certainly is not flexible. Where home workers are remote most of the time this also proves difficult to manage, as they are operating outside of the corporate perimeter and the various management systems.

Endpoint Compliance Checks

These are solutions which enforce the use of an agent delivered and configured by the gateway being connected to by the VDI client. Pre & post authentication access policies can be used to check for minimum system/application levels/versions and other criteria, which then provides a level of assurance before granting access.

Although these compliance check solutions certainly add value, the current issues with these solutions are:

- They do NOT guarantee the endpoint has not been compromised – thus does not satisfy compliance regulation audits in some industry sectors
- They are typically difficult to deploy, maintain and generates a lot of support overhead
- Additional licencing is required
-

Bootable Thin OS Solutions

Bootable USB devices which use a “thin” operating system (together with a locked down browser and the VDI client of choice) provide a secure environment to access the virtual environments. These have been around for some years now and there are numerous vendors providing these in various form factors.

While these devices do provide a secure environment there are some limitations and challenges:

- A physical device must be issued to each user
- The user must boot the OS from a USB device from their own PC which can prove difficult as there is no control how the BIOS is configured
- This system can be time-consuming for users
- The user cannot use their own PC until they disconnect from the VDI environment, shutdown the bootable device, which is even more of an issue if you want to provide 3rd parties / partners remote access

It should be noted that there are a few solutions around that run, in effect, as Type2 hypervisors on top of the underlying OS, but these will not prevent keylogging nor screen capture.

SentryBay Armored Client

The design objectives for SentryBay set out to use their core patented technology to provide a lightweight, secure environment to solve the key security and compatibility issues today on both Windows and MacOS endpoints:

1. Protect the browser and logon process from keylogging, screen-scrapping & other malicious attacks
2. Protect the VDI client from keylogging, screen-scrapping & other malicious attacks
3. Integrate with the solutions gateway platform
4. Solve browser compatibility issues
5. Enforce and deploy a consistent VDI client version
6. Enable the relevant virtual channels to function normally (where possible)
7. Allow the user to switch to their normal applications at any time without disconnecting from their VDI published desktops and applications.

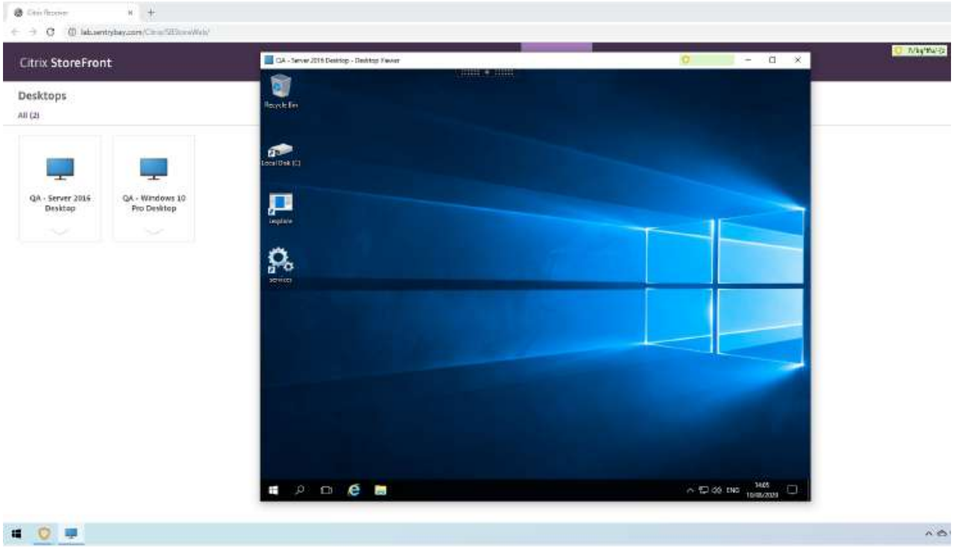
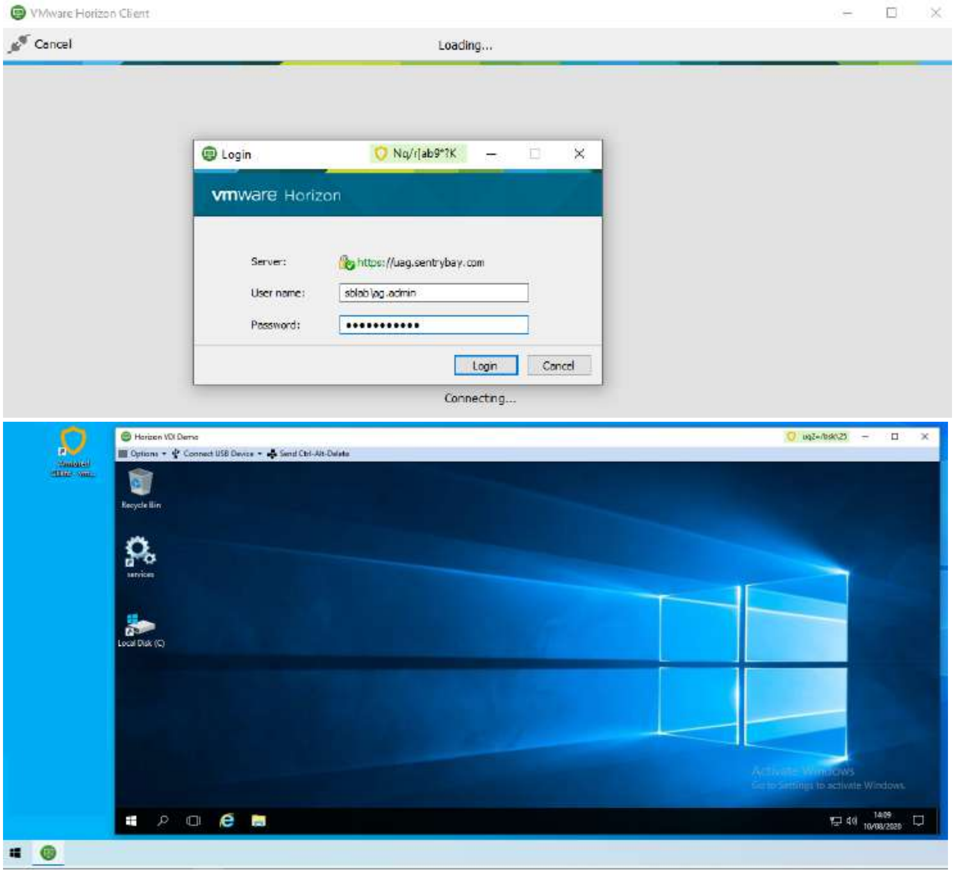

lab.sentrybay.com/Citrix/SBStoreWeb/
Citrix StoreFront
Desktops
All (2)
QA - Server 2016 Desktop
QA - Windows 10 Pro Desktop
QA - Server 2016 Desktop - Desktop Viewer
Recycle Bin
Local Disk (C:)
ENG

Image 1

Image 1 above shows the Armored Client running on a PC with the Armored Client secure browser logged into Storefront and a launched Citrix desktop in a Window. The Citrix sessions work in the normal way and can be used in Window or full screen / multi-screen modes as usual within the secure workspace.

Image 2 below shows the Armored Client protecting the VMware Horizon client



Server: https://uag.sentrybay.com

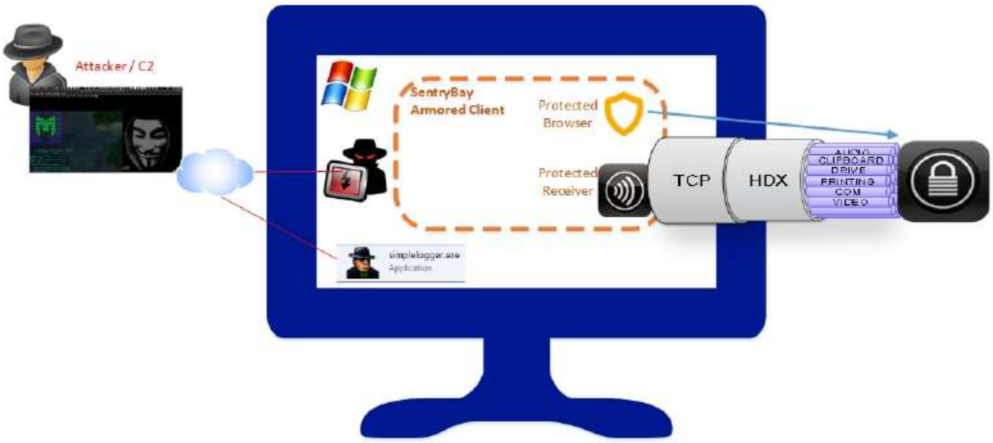
User name: sblab\ag.admin

Password: ●●●●●●●●●●●●

Image 2

Windows Armored Client

The Windows version of the Armored Client has been architected to provide a very high degree of security features to protect against common Malware and threats. Because of this a separate desktop session is created which makes it possible to provide the necessary security controls whilst imposing little performance overhead.



Windows Supported Operating Systems:

- Windows 7 SP1 onwards (32 & 64bit versions)

Windows Armored Client Security Features

The claimed security features have undergone rigorous testing, over two separate third party audits lasting a total of 6 weeks which successfully validated these. The Security features provided by the Armored Client include:

Security Feature	Comments	Security Feature	Comments
Dedicated Secure Browser for Armored Client	Locked Down HTTPS enforced Configurable	DLL Injection & Process Hooking Protection	
Key-Logging Protection		Gateway Integration for enforcements	
Screen Scrapping Protection		ICA File Interception & Hi-Jacking Protection	
Protect target processes used by VDI clients		Admin Portal Integration (Optional)	Logging audit data to portal License Management
RDP Double-hop Prevention		VNC Attack Prevention	
Anti-Decompiling / Debugging & Code Obfuscation		Managed VDI Client Version	

Note: Certain security features have not been disclosed, further details may be shared under mutual Non-Disclosure Agreement with our customers.

MAC Armored Client

The MAC version of the Armored Client, due to the macOS operating system allows the required security features to be implemented in a more seamless way than the Windows version.

MAC Supported Operating Systems:

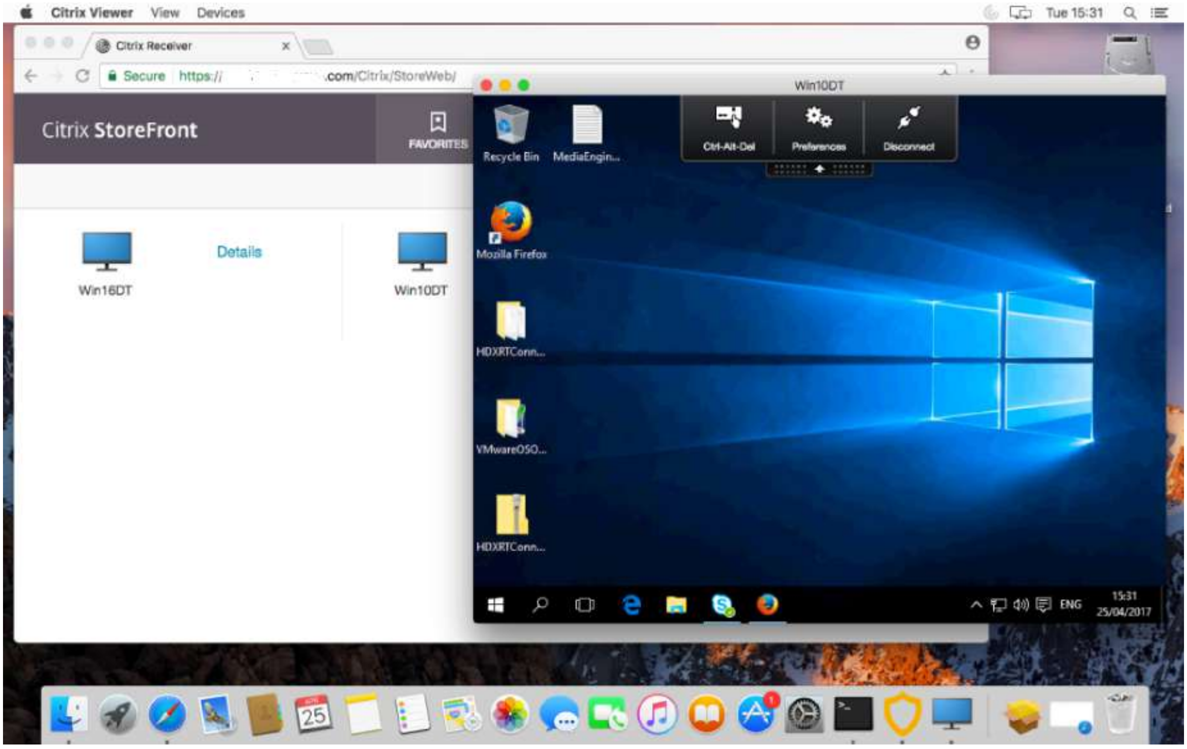
- macOS (High Sierra) & above

MAC Armored Client Security Features

The MAC edition of the Armored Client provides near security feature parity as the Windows version, including:

Security Feature	Comments	Security Feature	Comments
Dedicated Secure Browser for Armored Client	Locked Down HTTPS enforced Other	**NetScaler Integration**	
Key-Logging Protection	Citrix Receiver Browser All other apps whilst active	**ICA File Interception & Hi-Jacking Protection**	
Screen Scrapping Protection	Citrix Receiver Browser	**Admin Portal Integration** (Optional)	Logging audit data to portal License Management
Protected Receiver **Processes**		**Managed Receiver Version**	
Anti-debugging / Code Obfuscation		**Other (non-Disclosed)**	

Note: Certain security features have not been disclosed, further details may be shared under mutual Non-Disclosure Agreement with our customers.



The image above shows the Armored Client running on a MAC with Secure browser logged onto Storefront and a launched Citrix desktop in a Window. The Citrix sessions work in the normal way and can be used in Window or full screen modes as usual.

Armored Client Deployment & Portal

The SentryBay Armored Client solution provides cloud based software distribution, license management and an administration portal which also collects client audit data (optional). Each customer gets a unique download URL whereby staff can enter their details then download and install the Armored Client package

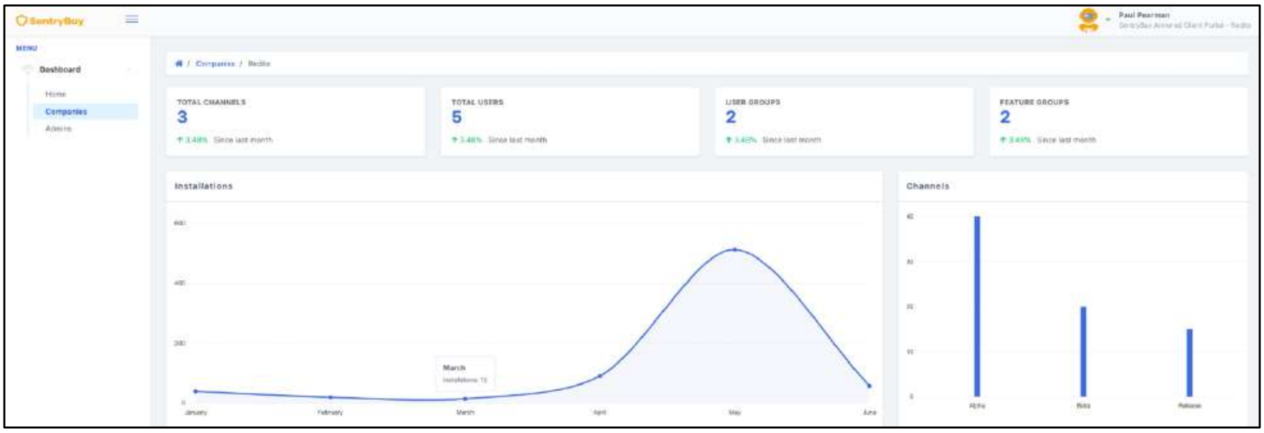
Cloud Delivered and Managed

The Armored Client is cloud delivered and managed, providing the following features for both Windows & MAC editions:

- The Armored Client, VDI Client of choice and browser are wrapped as one package
- Unique URL Download Page per customer
    - Restricted / Authorised Downloads
    - API / Enterprise Connector
- The software auto-updates
- Release Management
    - Controlled / Targeted by defined Groups
- Centrally Licensed
    - License / Device Revocation
- End-Point Audit data logged to Portal
    - Audit Data Logging (Optional)

Management - Client Administration Portal

A secure integrated SentryBay portal is available to provide additional Enterprise management capabilities for the Armored Client. The portal provides an integrated client registration and licensing process as well as providing audit data, client revocation and other administration functions.



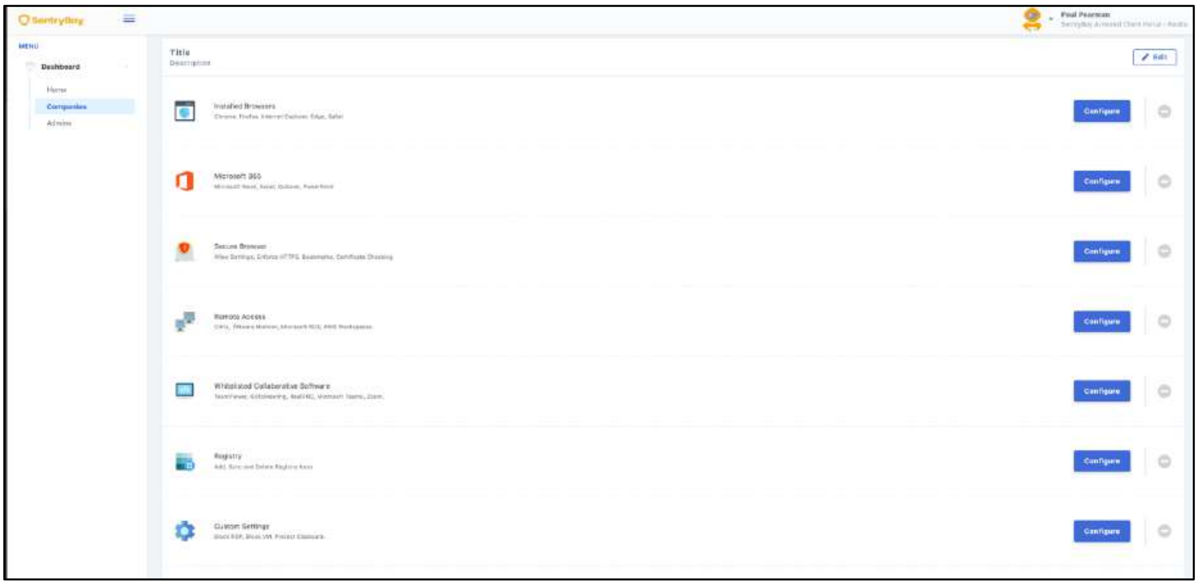
TOTAL CHANNELS
3
↑ 3.48% Since last month

TOTAL USERS
5
↑ 3.48% Since last month

USER GROUPS
2
↑ 3.48% Since last month

FEATURE GROUPS
2
↑ 3.48% Since last month

Through the Armored Client portal, the Administrator can define what applications need to be protected and configure the secure browser component:



Title
Description

Installed Browsers
Chrome, Firefox, Internet Explorer, Edge, Safari

Microsoft 365
Microsoft Word, Excel, Outlook, PowerPoint

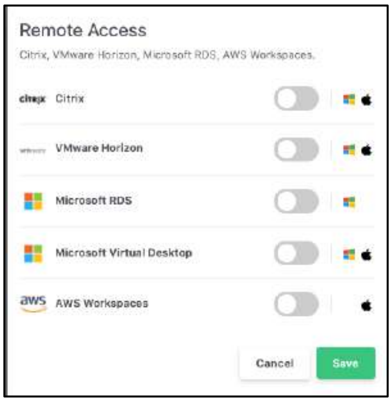
Secure Browser
Allow Settings, Enforce HTTPS, Bookmarks, Certificate Checking

Remote Access
Citrix, VMware Horizon, Microsoft RDS, AWS Workspaces

Whitelisted Collaborative Software
TeamViewer, GoToMeeting, RealVNC, Microsoft Teams, Zoom.

Registry
Add, Sync and Delete Registry Keys

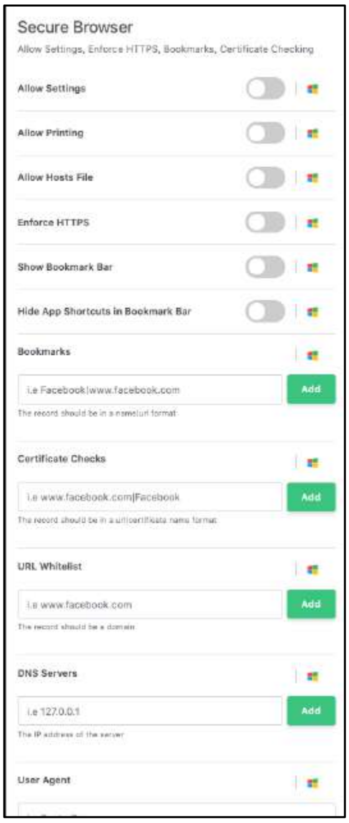
Custom Settings
Block RDP, Block VM, Protect Clipboards



Remote Access

Citrix, VMware Horizon, Microsoft RDS, AWS Workspaces.

- Citrix
- VMware Horizon
- Microsoft RDS
- Microsoft Virtual Desktop
- AWS Workspaces



Secure Browser

Allow Settings, Enforce HTTPS, Bookmarks, Certificate Checking

- Allow Settings
- Allow Printing
- Allow Hosts File
- Enforce HTTPS
- Show Bookmark Bar
- Hide App Shortcuts in Bookmark Bar

Bookmarks

i.e Facebook|www.facebook.com

The record should be in a name|url format

Certificate Checks

i.e www.facebook.com|Facebook

The record should be in a url|certificate name format

URL Whitelist

i.e www.facebook.com

The record should be a domain

DNS Servers

i.e 127.0.0.1

The IP address of the server

User Agent

A secure API can also be provided the customer wish to pull the audit data into their own data lake to use for Configuration Management Databases (CMDB) and ITIL Asset Control.

With every launch of Armored Client the following data is captured and sent to the customer portal:

- HW ID
- OS information
- Geo location information
- Installation date
- Installed Armored Client version
- AV vendor & version
- Firewall & Windows update checking – patches / hotfixes

Armored Client Package

The Armored Client solution contains:

1. SentryBay core software
2. A self-contained and hardened Armored browser (based on Chromium technology) *
3. Citrix Receiver, VMware Horizon, AWS WorkSpaces or Windows Virtual Desktop client **

The Armored client is deployed and maintained from SentryBay's cloud service. The user:

- Clicks a link which downloads the initial installer application.
- Runs the Installer which then pulls down the SentryBay software package and install including the VDI Client**.
- Follows a simple 3-click installation process and restarts the PC, at which point the Armored Client is ready to use.

The user then launches the Armored Client whenever they require access to the Gateway, and logs into their VDI session as normal.

*The browser deployed as part of the Armored Client package does not interfere nor use any existing browser installations already present on the endpoint, including Google Chrome or Edge which use the Chromium codebase

**If a Citrix Receiver or Citrix Workspace App (CWA) is already installed at the current or newer version used in the Armored Client then the Receiver/CWA will not be downloaded; the existing version will be used. If either no Receiver/CWA is installed, or an older version is detected, then the Receiver/CWA will be downloaded and installed or upgraded on the endpoint by the SentryBay updater service.

VMware Horizon Client will also be installed and updated should an existing version not be detected.

Client Management

Once installed the Armored Client will be maintained including specific VDI client from Redite's cloud-based Sydney updater service. It should be noted though that the updates are delivered in the background and applied the next time the PC restarts (Windows, MAC does not require reboot) and do not interfere with the normal operation. An indicator that updates are available and will be applied on next restart will be shown in the Armored Client's control panel.

The VDI client installed is also maintained by the client updater service. As Citrix, VMware, Amazon and Microsoft release newer client versions these will be tested by SentryBay and validated. Once released, updates will be pulled by existing clients from the cloud updater service which runs each time the application is launched.

The updater service provides reassurance that the latest client is in place on the device whether the device is managed or unmanaged. This reduces the complexity of supporting multiple versions of the VDI client and removes browser compatibility issues.

Update Release Control

Client Administrators will be able to run Armored Client builds on a pre-release channel so they can test and validate future updates in advance. Production users are defined in additional (n number) of deployment wave groups where new versions can be deployed in distinct phases, to ensure good release management practices.

VDI Compatibility

The Armored Client will work with any Citrix XenApp, XenDesktop, NetScaler environment which is currently supported by Citrix. VMware supported covers all Horizon and UAG environments, whilst Windows Virtual Desktop and AWS WorkSpaces support is across the most recent releases.

Conclusion

The Armored Client solves the key security challenges on both **Windows** and **MAC** endpoints. Protecting against key-logging and screen capture using SentryBay's patented technology, regardless of the security status of the endpoint where the VDI session is running. Thus this solution provides uncompromising confidentiality, allows the Receiver to function in the normal way, and provides flexibility for individual organisations to retain control and configure VDI specific session policies as desired.

The user can continue to use their normal desktop by switching desktops - without having to close their VDI session - providing a seamless experience.

As well as solving security risk, both browser and VDI client compatibility issues are solved, as the Armored Client keeps both updated (seamlessly) to the latest versions. Browser compatibility and out-of-date VDI clients cause organisations a tremendous amount of support effort today, which will be removed by using SentryBay's solution, which has been designed to solve these key challenges.

Distribution and enforcement of the Armored Client can be managed by integrating the solution with the VDI gateway in operation.

With the availability of a secure portal the solution provides integrated client registration, management control as well as providing comprehensive audit data, further enhances the security posture.

The Armored Client should be viewed as an additional level of security on the endpoint when using VDI for remote access, SentryBay still recommends the use of Anti-virus, Windows/Personal Firewall and Operating System patching etc. (each audited each time the Armored client is started and logged to the portal).

Further Information & Contact Details

REDITE.
Cyber & Data Security
AUTHORISED DISTRIBUTOR OF SentryBay

Paul Pearman
New Business Development Manager

Phone	0429 877 623
Email	paul@redite.co
Web	www.redite.co