White Paper

Does your VDI have a gap in its armour?

How you can use Armored Client to secure VDI remote access

Author: **Tim Jenkins**

Updated: **March 2021**

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, Microsoft, Amazon and others, provide security for staff or partners to use a high performance and secure remoting protocol for access to desktops, applications and data. Granular controls can be applied when the user is accessing virtual desktops, applications and data from outside 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.

However 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.

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 devices 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
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 implies there is no control as to the security posture or state prior to it being used to access the VDI platform. In most cases on Windows, the owner will have Local Administration Privileges, making it relatively easy for a threat actor / malware to compromise the device.

It is difficult for the organization to mandate aspects such as operating system levels or application versions (including browsers) remotely. Even the VDI client version installed is difficult for the organization to control. This, as well as being a security concern, is a major headache as browser types / configurations and VDI client versions cause many 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 device can be used by other family members, who may not be as security-savvy, increasing the risk of compromise.

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

Most security professionals realize that running standard anti-virus software alone is no longer sufficient to properly protect a PC. Advanced endpoint security solutions that do not rely solely on signature-based detection are emerging, but these too 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 an unmanaged device is compromised in any way, there is a real risk that data or systems access could 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, sensitive corporate data, and much more.

- **Screen Scraping:** This activity can deliver every item of data displayed on the unmanaged device 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 as a gateway.

- **File Interception:** Files can be intercepted either in flight or from the endpoint’s file system and re-used 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 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 device, it should be assumed that most users will have local Administrator privileges which increases risks of compromise.
- **Security Posture of Device:** Ensuring that the device is patched and running anti-virus and that 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 people, such as family members with little or no security awareness training.
- **Phishing Attacks:** A common way of distributing malware is via email. It should be assumed that email systems that do not have enhanced anti-phishing protections are used regularly, increasing the risk of infection.
- **Counterfeit / Malicious Software:** Often software is installed from dubious sources, increasing the risk of malware infection.
- **Device used on High Risk Wireless Networks:** The device could be used for remote access whilst on un-secured public Wi-Fi-networks, producing a 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 solutions are sometimes used 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 is not flexible. Where home workers are remote most of the time this also proves difficult to manage, as they are operating outside 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, they can Introduce challenges:

- They do not guarantee the endpoint has not been compromised - thus do not satisfy compliance regulation audits in some industry sectors
- They are typically difficult to deploy and maintain, and generate a lot of support overhead

- Additional licencing is required

Bootable Thin Operating System 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, however there are 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 over 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, and shutdown the bootable device, which is even more of an issue if there is a need to provide 3rd parties / partners remote access
- They can still be subject to attacks.

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

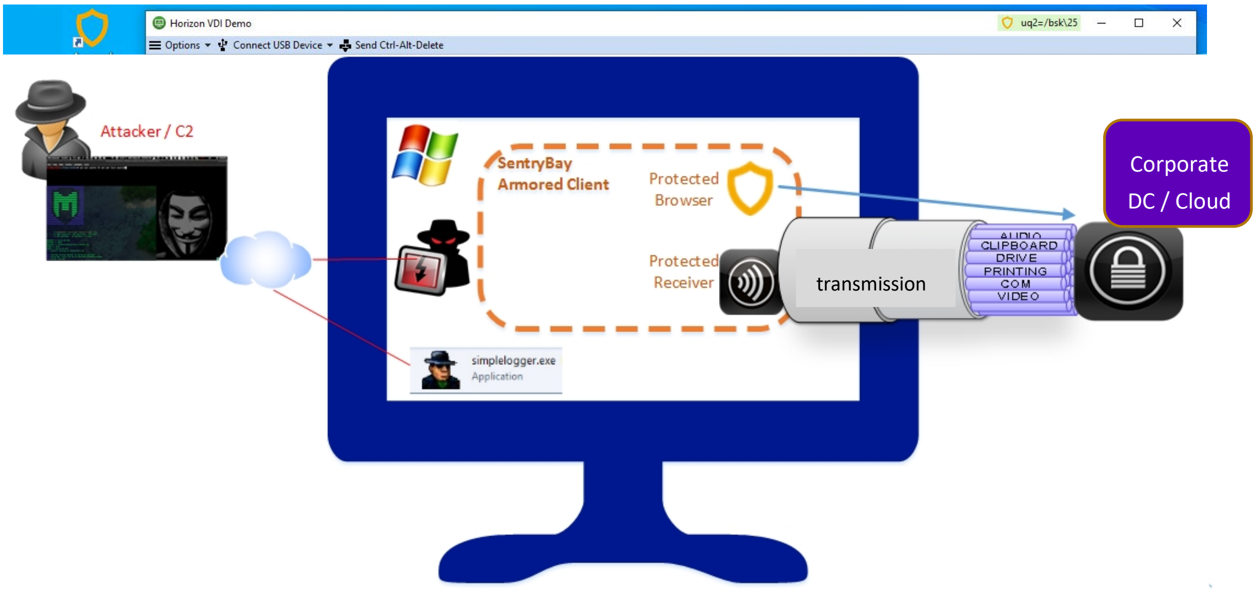
SentryBay Armored Client

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 on Windows, MacOS, iOS, Android and Thin client endpoints:

1. Protect the browser and logon process from keylogging, screen-scrapping & other malicious attacks
2. Protect the VDI client from keylogging, screen-scraping & other malicious attacks
3. Integrate with the solutions gateway platform
4. Solve browser compatibility issues
5. Enforce and deploy a consistent VDI client version (If required)
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

SentryBay Armored Client - Windows version

The Windows version of the SentryBay Armored Client has been architected to provide a high degree of security features which protect against common malware and threats. A separate desktop session is created to provide the necessary security controls whilst imposing little performance overhead.



Windows Supported Operating Systems:

- Windows 8.1 onwards (32 & 64bit versions)

Windows Armored Client Security Features

The security features have undergone rigorous testing, validated by two separate third-party audits lasting a total of 6 weeks. 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**	Protects against a wide range of malware attacks, eg. TrickBot,

			Emotet, or Dridex.
Key-Logging Protection	Kernel level protection	**Gateway Integration for enforcements**	Ensures endpoints connection have compliant security
Screen Scraping Protection	Prevention of screen data from being exfiltrated	**File Interception & Hijacking Protection**	
Protect target processes used by VDI clients	Prevention of illegitimate code from being injected into running processes	**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**	Deployment of the corporate sported VDI client and the necessary plugins

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

SentryBay Armored Client - MAC version

The MacOS version of the Armored Client provides keylogging and screen scraping protection as well as other protections.

MAC Supported Operating Systems:

- macOS (Mojave) & 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	VDI client Browser All other apps whilst active	**File Interception & Hijacking Protection**	
Screen Scraping Protection	VDI client Browser	**Admin Portal Integration** (Optional)	Logging audit data to portal License Management
Protected Application Processes		**Managed VDI Client deployment**	
Anti-debugging / Code Obfuscation	Guaranteed protection	**Other** (non-Disclosed)	

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

SentryBay Armored Client Deployment & Portal

The SentryBay Armored Client solution provides cloud-based software distribution, license management and an administration portal. Each customer receives a unique download URL whereby staff can enter their details to download and install the Armored Client package.

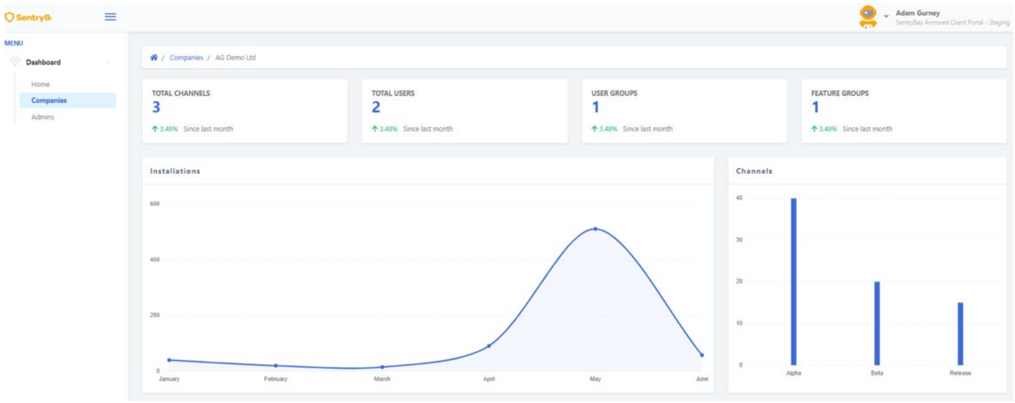
Cloud Delivered and Managed

The Armored Client deployment portal provides:

- The Armored Client, VDI Client of choice and browser wrapped as one package
- Unique URL Download Page per customer
  - Restricted / Authorised Downloads
  - API / Enterprise Connector
- Software auto-updates
- Third-party software download
- Release Management
  - Controlled / Targeted by defined Groups
- SAML Integration
- Centrally Licensed
  - License / Device Revocation

Management – Client Administration Portal

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

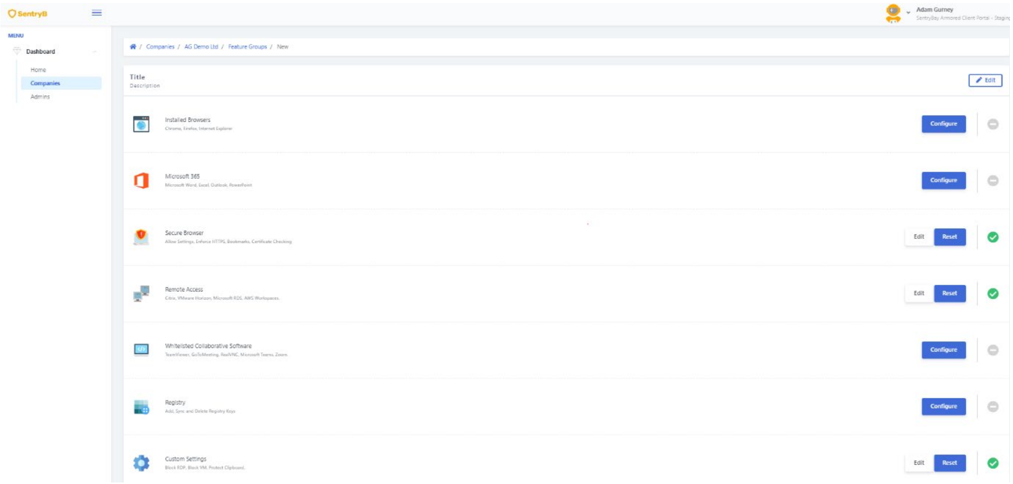


TOTAL CHANNELS 3 ↑3.48% Since last month

TOTAL USERS 2 ↑3.48% Since last month

USER GROUPS 1 ↑3.48% Since last month

FEATURE GROUPS 1 ↑3.48% Since last month

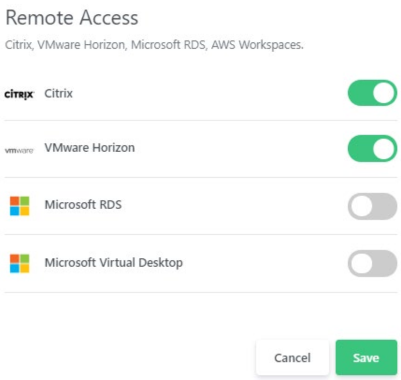


Companies / AG Demo Ltd / Feature Groups / New

Title
Description

Installed Browsers Chrome, Firefox, Internet Explorer	Configure	⊖
Microsoft 365 Microsoft Word, Excel, Outlook, PowerPoint	Configure	⊖
Secure Browser Allow Settings, Enforce HTTPS, Bookmarks, Certificate Checking	Edit Reset	✓
Remote Access Citrix, VMware Horizon, Microsoft RDS, AWS Workspaces.	Edit Reset	✓
Whitelisted Collaborative Software TeamViewer, GoToMeeting, RealVNC, Microsoft Teams, Zoom	Configure	⊖
Registry Add, Sync and Delete Registry Keys	Configure	⊖
Custom Settings Block RDP, Block VM, Protect Clipboard.	Edit Reset	✓

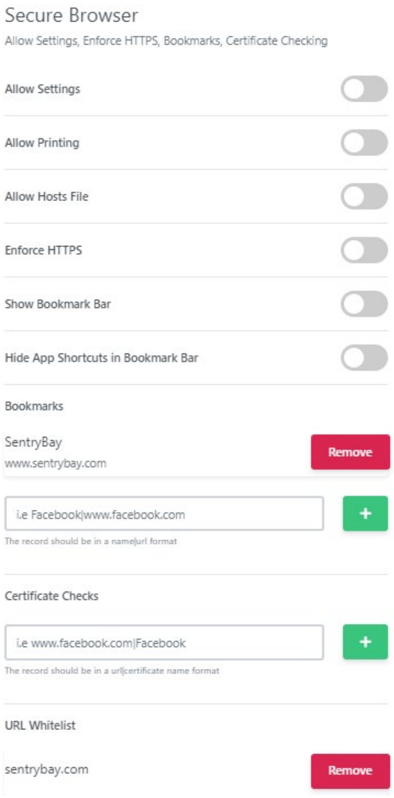
Through the Armored Client portal, the Administrator can define what applications need to be protected and configure the Secure Browser component:



Remote Access

Citrix, VMware Horizon, Microsoft RDS, AWS Workspaces.

- citrix Citrix ☑
- vmware VMware Horizon ☑
- Microsoft RDS ☐
- Microsoft Virtual Desktop ☐



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

SentryBay
www.sentrybay.com

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

sentrybay.com

Armored Client Package

The Armored Client solution contains:

1. SentryBay core software
2. A self-contained and hardened Armored Browser (based on Chromium technology) *

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 installs it.
- 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.

Client Management

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

Update Release Control

Client Administrators are 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 deployment groups where new versions are deployed in distinct phases, to ensure good release management practices.

VDI Compatibility

The Armored Client will work with any Citrix Virtual Apps & Desktops, NetScaler environment which is currently supported by Citrix. VMware support 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 Windows, MAC, iOS, Android and Thin client endpoints. It protects against keylogging and screen capture using SentryBay's patented technology, regardless of the security status of the endpoint. Thus, this solution provides uncompromising confidentiality, allows the client 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 risks, both browser and VDI client compatibility issues are solved, as the Armored Client keeps both versions controlled. 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.

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 and management control.

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 software, Windows/Personal Firewall and Operating System patching etc.

For further information on SentryBay's Armored Client please contact us using the forms on our website.