SentryBay®

Armored Client for Citrix | White Paper

PhireServe

Author: Steve Atkinson
April 2016

Citrix Secure by Design

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

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

But there has always been a concern if the endpoint used to access Citrix 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.

It must be stressed that keylogging, screen scraping and browser vulnerabilities are the only security weakness when accessing Citrix environments that are implemented to best practices. However endpoint security for unmanaged PC's is a concern for many companies in most sectors, particularly those bound by regulatory compliance - which either prevents the use of non-managed endpoints for remote access or is high on the security risk register today.

Corporate remote access to Citrix normally requires:

1. An endpoint device connected to the Internet
2. A browser (for the gateway logon process)
3. Citrix Receiver Installed or Citrix environment with HTML5 Receiver option configured
4. User credentials (Username & Password)
5. Multi-factor authentication (Security Token, Pin, Smartcard etc.)

Unmanaged Endpoints

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 Citrix.

One cannot mandate operating system levels or application versions (including browsers). Even once a user installs the Citrix Receiver the version used is difficult to control. This, as well as being a security concern, is a major headache as browser types / configurations and Receiver 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 do not rely solely on signature based detection and also use other protection techniques such as Threat Intelligence and behavioural analytics, but these are often still fallible and. due to management and privacy issues, often cannot be properly deployed and maintained on non-corporate devices.

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 very expensive (particularly if they are only used to allow access via Citrix) 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.

Citrix End Point Agent (EPA)

Citrix provides the EPA solution which enforces the use of an agent delivered and configured by the NetScaler Gateway. 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 EPA certainly adds value, the current issues with this solution are:

- EPA does NOT guarantee the endpoint has not been compromised - thus does not satisfy compliance regulation audits in some industry sectors
- EPA is difficult to deploy, maintain and generates a lot of support overhead
- Additional licencing is required (if not on Platinum)
- Citrix NetScaler Gateway must be used

Bootable Thin OS Solutions

Bootable USB devices which use a “thin” operating system (together with a locked down browser and Citrix Receiver) provide a secure environment to access Citrix. 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 has to be issued to each user
- The user has to 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 Citrix and 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.

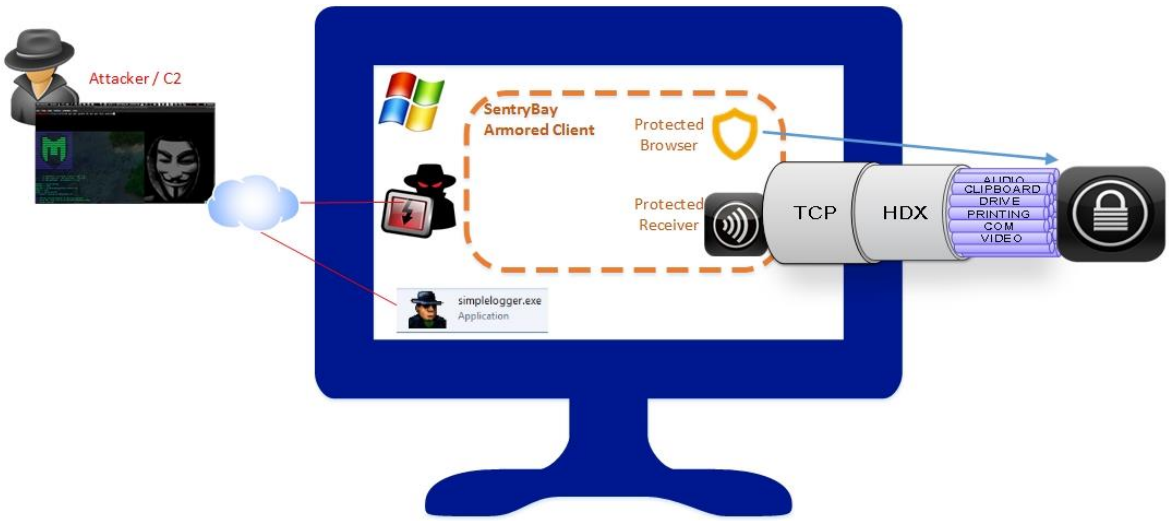
SentryBay Armored Client for Citrix

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:

1. Protect the browser and logon process from keylogging & other malicious attacks
2. Protect Citrix session from Keylogging
3. Solve browser compatibility issues
4. Enforce and deploy a consistent installed Citrix Receiver version
5. Works with older (supported) Citrix environments, not just the latest 7.x releases
6. Enable the ICA / HDX virtual channels to function normally, where possible
7. Allow the user to switch to their normal applications at any time without disconnecting from Citrix applications

Armored Client 2.0

SentryBay has recently released the full Receiver version of the Armored Client for Citrix. The solution uses SentryBay's core patented anti-Keylogging technology which protects access and operations when using Citrix on Windows endpoints, regardless of the security state of the client operating system.



Armored Client Security

When launched, The Armored Client creates a separate secure desktop session and one-time user account that has an ACL set which cannot be accessed by any other accounts on the PC (including system accounts).

There are two applications which will run inside the secure desktop session using the one-time user account context:

1. An Armored browser for the user to log onto the Citrix Gateway (NetScaler or F5) which is protected from key logging and screen scraping. The browser is a lightweight and locked down version of Firefox. This does not allow any plugins to be installed except the Citrix receiver plugin, which is enabled by default. This also provides anti-phishing, anti-spoofing and man-in-the-browser type attacks.
2. When the Citrix Receiver is launched within the secure desktop session, it is also fully protected from key logging and screen scraping.
3. All virtual channels are controlled by the Citrix administrator using HDX policies in the normal way.

Armored Client Deployment & Enforcement

Each customer gets a unique download URL whereby staff can download the Armored Client package. The Citrix NetScaler can be configured to detect a custom "User-Agent" string presented by the browser, which, if not present after authenticating the user, could be redirected to an internal web page with instructions and download link etc. Although not a 100% effective security control, it is an effective first pass and an easy way of deploying the client to unmanaged PC's whilst enforcing day-to-day usage by staff.

In future releases it will also be possible for each customer to set their own custom User-Agent string value.

For absolute trust it is possible to embed a unique client certificate (supplied by the individual customer) and pin this to the Armored Brower. This can then be detected by the Gateway using a certificate-based authentication policy, in addition to existing authentication methods.

Management

A customer portal can be provided so that basic self-service audit and management functions can be performed. This is under development today and will be available soon.

Armored Client Package

The Armored client for Citrix solution contains:

1. SentryBay core software
2. A self-contained and hardened Armored browser (Firefox)*
3. Citrix Receiver**

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

- Clicks a link which downloads the initial installer application which is 349k in size.
- Runs the Installer which then pulls down the SentryBay software package (approx. 244MB) and install including the Citrix Receiver**.
- 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 (Citrix NetScaler or F5 Big-IP), and logs into their Citrix session as normal.

*The version of Firefox deployed as part of the Armored Client package does not interfere nor use any existing Firefox or other browser installations already present on the endpoint.

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

As Citrix releases newer Receiver 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 intention is to update the Receiver shortly after Citrix releases their updates (subject to QA testing).

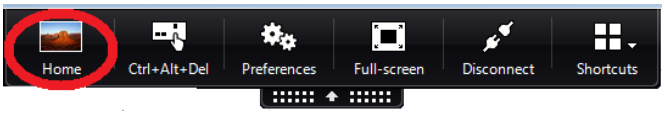
Functionality

The Armored client allows the Receiver tool bar and virtual channels to work in the normal way, which can be controlled by the Citrix administrator using HDX/ICA policies.

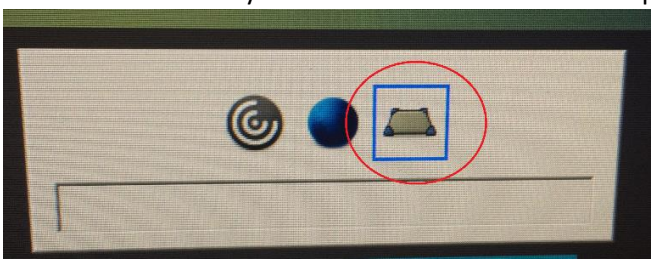
This includes screen printing and copy / paste from the secure to standard desktop sessions using the "Ctrl + Print-Screen" keys (providing the Citrix HDX policy allows this). However even when this functionality is enabled no Malware / Hackers can capture keystrokes or screens.

The only difference to the normal user experience is:

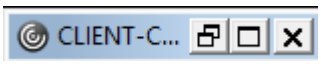
1. User must launch the Armored Client to access the corporate Citrix system
2. Receiver Toolbar functions in the normal way and supports multiple monitors. However, if multiple monitors are in use, even if only one is actively used for the Citrix session, the other/s cannot be used by the standard desktop session. The user must switch back to the normal desktop session using the process below:
    a. Use the Home button in toolbar to minimise the session



    b. Then use Alt+Tab keys to switch to the normal desktop



    c. At this point all the monitors can be used by the standard desktop as normal
    d. To switch back to the Secure desktop session, click the Armored Client icon active in the task bar
    e. To go back to the Citrix session maximise / restore or just right click the minimised window bar (bottom left corner or screen) or use Alt+Tab



Screen Sharing with the Armored Client

By design, remote assistance screen sharing software and other video capture software will not work when the Secure Desktop session is active, although it will work as usual when the Normal Desktop session is active. This includes RDP, Remote assistance, WebEX / GoToMeeting screen sharing type solutions as well as VNC etc.

Citrix Session Sharing does work allowing the remote operator to see the active session as normal, even though it is running in the Secure Desktop session.

It is possible to white-list software such as Citrix GoTo Assist, LogMeIn etc. and dependant on customer requirements this may be allowed as standard in the future.

OS support

The initial version of Armored Client for Citrix supports the following Windows desktop operating systems (32 & 64bit):

- Windows Vista – SP3
- Windows 7 – SP2
- Windows 8
- Windows 8.1
- Windows 10

A MAC version is in development and will be available later in 2016.

Citrix Compatibility

The Armored Client will work with any Citrix XenApp, XenDesktop, NetScaler environment which is currently supported by Citrix for use with the Receiver 4.x.

Note: F5 Big-IP appliances can act as an ICA Proxy for Citrix could be used instead of NetScaler Gateway.

Conclusion

The Armored Client for Citrix solves the key security challenges, protecting against key-logging and screen capture using SentryBay's patented technology, regardless of the security status of the endpoint where the Citrix Receiver 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 ICA/HDX policies as desired.

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

As well as solving security risk, both browser and Receiver compatibility issues are solved, as the Armored Client keeps both updated (seamlessly) to the latest versions. Browser compatibility and out-of-date Receivers 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 Browser can be managed using the NetScaler Gateway, with additional basic audit and management functions available via the customer portal.

The Armored Browser for Citrix should be viewed as an additional level of security on the endpoint when using Citrix, SentryBay still recommends the use of Anti-virus, Windows/Personal Firewall and Operating System patching etc.

For further information on SentryBay's Armored Client for Citrix please contact PhireServe (details below).

PhireServe

Phireserve is the Global Distributer of Armored Browser & Client for Citrix product range.

189 Lynchford Road
Farnborough
Hampshire
United Kingdom
GU14 6HD
+44 (0)1252 757660
Email : Info@PhireServe.com
Web: Http://Phireserve.com

SentryBay

3 Manchester Square
Marylebone
London
W1U 3PB
+44 (0)203 219 3060
Email : Info@Sentrybay.com
Web: Http://Sentrybay.com