Citrix Secure Remote Access with the SentryBay Armored Client

App virtualization has become central to IT strategy across every vertical, enabling the mobility, flexibility and efficiency needed to succeed in today's competitive markets. In fact, 96 percent of the Fortune 500 trusts Citrix to deliver apps wherever people choose to work, on whatever device they use.

CITRIX® NetScaler

Citrix NetScaler is deployed in thousands of networks around the globe to optimize, secure and control the delivery of all enterprise and cloud services, and to maximize the end user experience across all device types.

XenDesktop provides remote PC access to instantly deliver desktop virtualization benefits without the need to migrate desktops to the data center. Users get a secure, high-definition, direct connection to their office PC.

With remote workers and BYOD becoming more prevalent, Companies are searching for a means of enabling acceptable levels of security for employees that use their own unmanaged devices — also a growing trend, and one that offers significant cost-cutting opportunities for companies.

This paper discusses SentryBay's Armored Client solution for Citrix, which complements Citrix secure desktop environment, by enhancing privacy and security for both remote and unmanaged machines. Also described is the effectiveness of teaming SentryBay's solution with Citrix desktops and applications in providing a remote access security solution for enterprises worldwide.

Business Challenge Summary

The growing remote workforce has created some serious security challenges for companies large and small.

CITRIX® XenDesktop

For thousands of companies worldwide, the purpose of a remote connection is to securely enable access to Company resources through remote-ready solution, such as Citrix XenDesktop. In most remote-work scenarios, the unmanaged endpoint used for remote access is typically a staff member's personal PC or laptop, which the company neither owns nor manages. As a result, the company retains no control as to the de facto security posture or state prior to the employee login and access to the company resources remotely.

This is a scenario that exposes companies' proprietary data and systems to substantial risk, and is duplicated millions of times on a daily basis as remote workers login to perform their jobs.

If the endpoint — the employee's 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, there are three threats in particular that have already proven fearsomely effective in exposing companies' data or systems to bad actors:

1. **Keylogging:** Keyloggers 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.
2. **Screen Scraping:** This activity can deliver every scrap of data displayed on employees' screens directly into the hands of cybercriminals. Virtual desktop users may be particularly vulnerable to screen scraping attacks.
3. **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.

It is important to note that keylogging, screen scraping and browser vulnerabilities are significant security weaknesses that cannot be ignored even if Citrix environments are implemented in accordance with best-practice standards.

Nevertheless, in many industries and regions, compliance auditors demand that organizations properly audit non-corporate machines before allowing access to company resources remotely.

The SentryBay Armored Client provides a full range of protection for companies relying upon Citrix to enable and streamline their remote access needs. SentryBay Armored Client is a solution that protects against zero-day attacks, while also providing independent audit and reporting capabilities on a customer portal.

Top Features to Consider in a Remote Access specific Security Solution

Citrix security solutions give employees and third parties secure access to sensitive business information whether they're at headquarters, a branch office, or offshore locations, and during mergers and acquisitions.

There are a number of features to consider when searching for a Remote Access specific security solution. The following, in particular, should be considered must-have features for any remote access solution undergoing evaluation for deployment in any organization:

1. **Provides Secure Desktop Environment:** The solution must secure the desktop execution environment that is used for remote access, regardless of the security state of the endpoint through which the user accesses the environment.
2. **Provides Compatible & Secure Brower:** The solution must eliminate any potential browser compatibility issues with the browser used to log in to Citrix NetScaler Gateway. It is also essential that the solution protect the integrity of the login process by guarding against threats such as keylogging, screen scraping, man-in-browser, and other malicious attacks.

CITRIX® Receiver

CITRIX®
NetScaler Gateway

3. **Solves Key Support Issues:** In most organizations, quite an amalgam of different browser and receiver versions are likely to be used on unmanaged endpoints. The chosen security solution should eliminate the complex support issues that typically arise as a result.
4. **Updates:** Necessary updates should be provided automatically, and the update process should be seamless and transparent for users.
5. **Deploys Consistent Receiver Version:** The solution should assure that the current Citrix receiver version is deployed upon installation, and always maintained on the client. If a non-current receiver version is detected, the solution should automatically download and install the current version.
6. **Enables Easy Switching:** Users should be able to switch to normal, device-based applications at any time, enabling switching between virtual and local desktops without terminating established connections with Citrix applications.
7. **Provides Secure Customer Portal:** The solution should provide a secure portal for the execution of tasks such as client registration and license management, and should also enhance security by providing comprehensive audit data.

The SentryBay Armored Client is shown to effectively deliver on all these features.

Citrix Ready Secure Remote Access Program Overview

Citrix solutions deliver a complete portfolio of products supporting secure access of apps and data anytime, at any place, on any device and on any network. These include:

1. XenApp and XenDesktop to manage apps and desktops centrally inside the data center

CITRIX® XenApp

CITRIX® XenMobile

2. XenMobile to secure mobile applications and devices while providing a great user experience

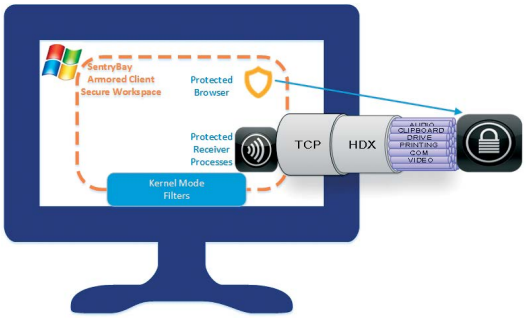
3. ShareFile to provide controlled and audited data access, storage and sharing, both on-premise and in the cloud

4. NetScaler to contextualize and control connectivity with end-to-end system and user visibility

Citrix solutions also integrate with third-party security products to provide advanced levels of system management and identity, along with endpoint and network protection. The Citrix Ready Secure Remote Access program was launched to identify and showcase partner products that are proven to smoothly integrate with Citrix products, and that work to enhance Secure Remote Access by adding extra layers of security. The Citrix Ready Secure Remote Access program serves as an aid to IT executives in quickly and easily finding and sourcing solutions for their Secure Remote Access needs, helping to secure organizations' corporate networks from theft of data, DDoS and other security attacks.

Citrix advises that organizations can best defend against security attacks that might occur through Remote Access by following five best practices — pillars of focus that support enterprise security:

1. **Identity and Access:** Administrators must be able to identify users requesting access to a system and limit the degree of access granted. In comparison to simple password-



based systems, two-factor authentication offers a vast improvement in the ability to properly identify requests for access. The degree of access granted to each individual user should be based on context. The principle of least privilege helps to ensure that users are granted rights that are limited only to those required in the performance of their jobs.

2. **Network Security:** The growing demand for remote access complicates the process of securing a network. Yet the integrity of network security must be maintained while supporting remote access for mobile and third-party users. Network and host segmentation can be useful in shrinking surfaces that are vulnerable to attack. And implementing a multi-layer approach helps to boost network security while ensuring

availability.

3. **Application Security:** All types of applications are potential targets for hackers, but the veritable explosion of apps has created many additional points of vulnerability for most enterprises. Apps on mobile devices are particularly susceptible to exploitation. An important step in reducing risk is enacting centralization and the encrypted delivery of applications. Containerization for mobile apps and inspection of incoming data streams can help to reduce app-related security vulnerabilities.

4. **Data Security:** The security of enterprise data can be enhanced by the centralization and hosted delivery of data by enforcing secure file sharing (to reduce data loss) and by the containerization of data (both in-transit and at rest).

5. **Monitoring and Response:** Vigilance and fast action are required to successfully counter the attacks that most enterprises face on a daily basis. A rapid response to breaches is also critically important, given that even the most secure systems are not completely invulnerable to successful attacks. Rapid detection and response to successful attacks serve to minimize damage and help to limit susceptibility to imminent additional attacks. End-to-end visibility into application traffic supports faster identification of security breaches and system anomalies.

The Benefits and Burdens of Remote Access

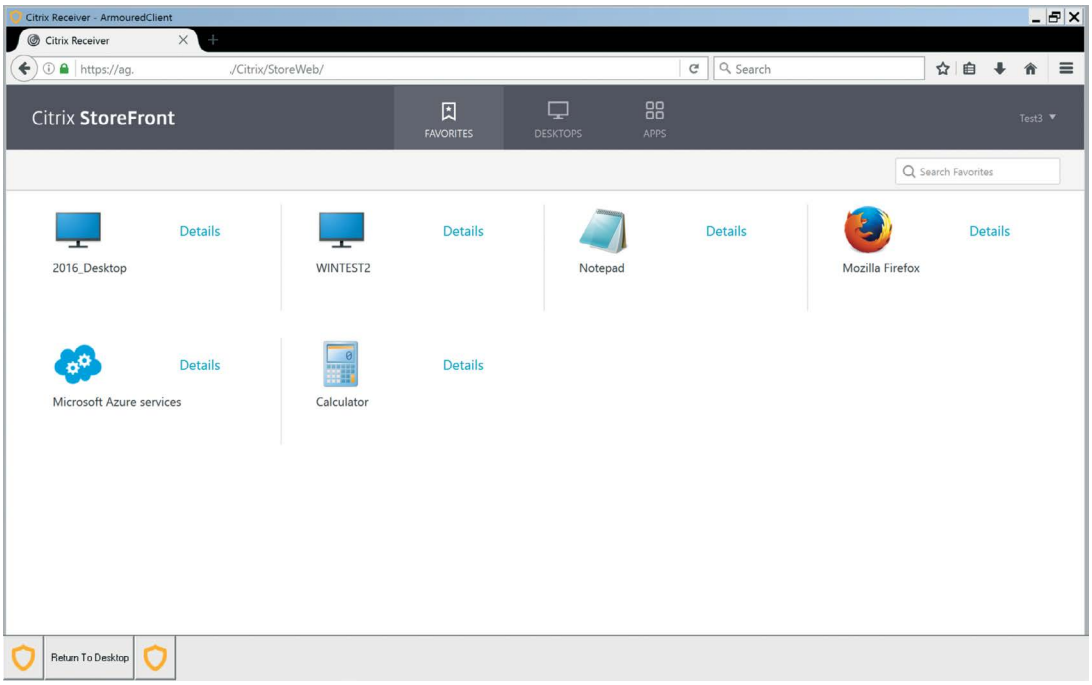
Remote access has enabled an entirely new paradigm of workplace flexibility and productivity. The adoption of mobility enhancing tools such as tablets, smartphones and other devices has transformed many enterprise roles into an any place, any time proposition. Workers have benefited from schedules that offer more flexibility, helping to enhance both work- and home-life. Companies have benefited from the leaps of productivity that remote access enables.

But this ongoing paradigm shift has required that enterprises find ways to balance the protection of sensitive data with the impact of remote access upon user flexibility — the widespread use of virtual public networks (VPNs) over unsecured networks, for example.

While remote access does increase the burden of safeguarding enterprise systems and data, the benefits of remote access justifies the need for an increased focus upon security. The Citrix Ready Secure Remote Access program is designed to help enterprises conform to the five security pillars listed above while meeting the skyrocketing demand for more remote access capabilities.

Armored Client for Citrix

SentryBay's Armored Client for Citrix has been selected to participate in the Citrix Ready Secure Remote Access program. SentryBay's Armored Client solution has demonstrated the ability to consistently conform with and support the five security pillars of the Secure Remote Access



program.

Product Overview

The Armored Client for Citrix wraps the Citrix receiver in a virtual blanket of security, providing key endpoint and browser security for connections to XenDesktop and XenApp installations. The solution defends against existing security threats such as keylogging, screen capture/ session videoing, browser vulnerabilities, DNS poisoning and session hijacking.

Armored Client is extremely cost effective; it enables corporations to quickly and easily deploy corporate Citrix XenDesktop and XenApp applications to any managed and unmanaged PC without security concerns. The solution enhances security of the entire Citrix session from logon authentication to closing down.

Armored Client uses SentryBay's patented technology in providing a lightweight, secure environment that solves today's key security and compatibility issues. The solution boasts an established track record of withstanding the most penetrating scrutiny, particularly from the finance industry sector. This reassures regulatory compliance officers that non-managed PCs may be used to access Company resources remotely without fear of violating any industry governance criteria.

Key Features of Armored Client – and how they meet the key pillars of the Remote Access Program:

- **Identity and Access:** Armored Client strengthens and streamlines the critical process of identifying users, and grants appropriate levels of access based on the user, endpoint,

network, and security profile for each access request — whether originating from within or outside the organization. In particular, Armored Client works with Citrix in four key ways to aid identification and access-granting processes:

1. The NetScaler Gateway can enforce the use of Armored Client. Access to resources can be denied or reduced.
2. The Armored Client's Browser cannot be exploited by common attack vectors, used on the endpoint for the NetScaler login process.
3. Armored Client audits customer portal endpoint each time it is started, providing an additional level of endpoint security.
4. Armored Client enables automated revocation of customer portal based upon designated parameters (such as users that abandon session).

- **App Security:** Armored Client provides additional security to the endpoint to Citrix XenDesktop which allows centralized application, operating system patch management, and configuration management. It provides secure access to organizational resources — even from employee-owned devices — and protects against zero-day attacks.

  The solution also provides and protects a compatible browser used for access, from common threats and zero-day attacks.

- **Data Security:** SentryBay helps protect data that resides in the data center which is displayed on endpoint screens; screen-scrapers and key-loggers can grab that displayed data. Armored Client protects against both of these prevalent risks..

- **Monitoring & Response:** User performance degradation can serve as a coalmine canary of sorts, providing an early indication of security compromises. Armored Client usage is audited and integrated to a SentryBay cloud customer portal. Armored Client also helps to better comply with regulations, reducing the scope and impact of audits while ensuring maximum uptime and performance.

  Importantly, Armored Client for Citrix is based upon core SentryBay-patented technology. This proprietary technology has been closely scrutinized and found to meet the lofty security standards of the finance industry — hence the use of this technology in many financial institutions worldwide. The solution provides audit and reporting capabilities for remote workers' machines while also providing a level of protection that resolves the key security threats highlighted by auditors.

Overview of SentryBay

SentryBay is a real-time data security company developing technology for PCs, mobile, the cloud and the internet of things (IoT). The company provides protection from advanced threats at the key points where data is most vulnerable: at the point of data entry, during transmission, and during exposure to new phishing and malware attacks.

SentryBay's patented technologies have underpinned a cross-platform product range deployed by some of the largest global enterprises, encompassing more than 5 million customers serviced worldwide.

SentryBay offers additional layers of security with its proprietary anti-keylogging and anti-phishing technology. Both technologies are patent protected, with anti-keylogging patents granted in 2012 and 2016, and the anti-phishing patent in 2014.

Solution Detail: Armored Client for Citrix

The Armored Client for Citrix is packaged as a complete security solution for remote access via non-managed PCs. The Armored Client solution contains:

- SentryBay core software
- A self-contained and hardened SentryBay Armored Browser (based on Firefox)
- The Citrix Receiver

Armored Client is deployed and maintained from SentryBay's cloud service, and can be managed using the Citrix NetScaler Gateway. Deployment is quick and easy. To deploy Armored Client, the user simply:

- Clicks a link on a web page hosted by the customer, which downloads the initial installer application (size: 349 kilobytes)
- Runs the Installer, which then downloads the SentryBay software package (size: approximately 300 megabytes) and performs the installation, including the Citrix

Receiver

- Follows a simple three click installation process and restarts the PC. Armored Client is then ready for use

With a secure portal in place, the solution provides integrated client registration and management control. The solution also provides the comprehensive audit data that is crucial in helping organizations maintain and enhance their security posture. Once installed, Armored Client is maintained from SentryBay's cloud-based update service, which also assures that the Citrix Receiver is kept updated to the current version. Support effort is reduced for client compatibility issues such as multiple browsers, Citrix Receiver version and Smart Card configuration.

Armored Client provides an extra layer of security to Citrix Apps and Desktops, providing advanced protection against all common threats (including zero-day attacks) for the Citrix Receiver regardless of the endpoint security state.

Citrix provide secure access to the enterprise apps and data to employees and third parties to get work done, whether they're in the office, at home, or on the go. And offer people the choice to use any corporate or personal mobile device they choose.

SentryBay's Armored client for Citrix complements this by removing remote endpoint security risks, enabling enterprises to worry less about accessing Company resources remotely through unmanaged devices, and eliminating the need to issue expensive corporate laptops.

A Proven Partnership for Remote and Unmanaged Machines

19b43697ecb4e12b06f2772ce1fec914	steve.atkinson@phireserve.com	Microsoft Windows 10 Enterprise	English - United Kingdom	2016-09-18 15:42:21	6.2.0.11151	Windows Defender		TRUE	FALSE	DESKTOP-EV59QBD	172.16.125.130, fe80::83b:6b71:abfe:3bd5
3f8b10b8a8c3cfddaea88b9e1bcfdbb5	steve.atkinson@phireserve.com	Microsoft Windows 10 Pro	English - United Kingdom	2016-09-24 08:30:01	6.2.0.11153	Norton Security	22.8	TRUE	TRUE	DESKTOP-J52LKU4	192.168.0.18, fe80::6ca7:f695:6e46:906a

As the demand for remote access capabilities grows, many companies are scrambling to find a way to maintain or enhance security standards. They are also looking for a means to eliminate the costly practice of supplying each remote employee with a company-supplied machine. The teaming of Citrix and SentryBay provides a solution that fulfills both of those urgent needs.

SentryBay's selection to the Citrix Ready Secure Remote Access program provides enterprises with a proven, reliable, remote access security solution that extends the full range of Citrix benefits to remote users. Armored Client eliminates the security concerns of using unmanaged machines for enterprise operations, helping companies to strengthen security while simultaneously cutting operational costs.

For more information about SentryBay, please visit: http://www.sentrybay.com/

For more information about Citrix NetScaler, please visit: https://www.citrix.com/products/netscaler-adc/

To learn more about the Citrix Ready Program partnership with SentryBay's Armored Client, please visit: https://citrixready.citrix.com/sentrybay/armored-client-for-citrix.html

Appendix

Learn about the enterprise security advantages provided by Citrix NetScaler Unified Gateway at: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/best-practices-for-enterprise-security.pdf

For information on Citrix XenApp and XenDesktop please visit : https://www.citrix.com/products/xenapp-xendesktop/

To learn more about security solutions for business enterprises, contact Citrix and SentryBay.

About Citrix Ready

Citrix Ready identifies recommended solutions that are trusted to enhance the Citrix Delivery Center infrastructure. All products featured in Citrix Ready have completed verification testing, thereby providing confidence in joint solution compatibility. Leveraging its industry-leading alliances and partner ecosystem, Citrix Ready showcases select trusted solutions designed to meet a variety of business needs. Through the online catalog and Citrix Ready branding program, you can easily find and build a trusted infrastructure. Citrix Ready not only demonstrates current mutual product compatibility, but through continued industry relationships also ensures future interoperability. Learn more at citrixready.citrix.com.

About SentryBay

SentryBay Limited (www.sentrybay.com) is a privately held firm headquartered in London with offices in the USA and Australasia and clients and partners globally. SentryBay provides real-time security technologies for PC, Mobile, Cloud and IoT devices. One of their specialist areas is in developing technology that locks down applications and browser connections, providing ultra-secure channels for communications and undertaking web-based transactions. SentryBay's patented technologies include world-leading anti-keylogging and anti-phishing technologies that proactively prevent data loss from both PC-based and mobile devices.