Remote Desktop Access for the Mobile Workforce

Security White Paper

May 2013

Table of Contents

1. Situation Analysis

The Mobile/BYOD revolution is here to stay. Each day, as new devices are released to the market, they are brought into your company and onto the corporate network by employees who use them to access everything from corporate email to line of business applications locked inside highly customized IE browsers.

But if you are like most CIOs, CSOs and IT managers responsible for network security, you're spending countless nights worrying about the security ramifications. One of the biggest challenges most companies face is how to allow mobile devices to access applications and desktops in a secure manner that doesn't impact the user experience to the point that they simply bypass the network and data security measures in place.

Splashtop Enterprise with SplashApp technology solves this challenge. Based on the popular Splashtop Remote Desktop app that has been downloaded by more than 14 million users and one of the Apple App Store's top 25 best-selling iPad apps of all time, Splashtop Enterprise is used by professionals at 60% of Fortune 100 companies. By replacing poor performing and cumbersome legacy VDI, VPN and RDP solutions, users can now access their applications and data that reside on physical or virtual desktops within the corporate network – from their own mobile devices—quickly, easily, and securely.

This white paper provides server, desktop, network and security personnel with an architectural overview and description of the specific security controls implemented by Splashtop Enterprise. The Appendix addresses how it can help organizations to meet HIPAA guidelines for the privacy and security of healthcare information.

2. Architecture

Before describing the specific security mechanisms implemented in the Splashtop Enterprise solution, it is important to understand the underlying architecture as seen in Figure 1.

The solution is comprised of three components, each residing on different systems within an enterprise network. Together, they provide a secure, end-to-end remote desktop experience.

Figure 1: High Level Architecture

2.1. Splashtop Enterprise App

The Splashtop Enterprise App is a lightweight remote client that is downloaded and installed from the appstore available from the user's mobile device. Supported devices include Apple iPad or iPhone and Google Android phone or tablet. Macs and Windows-based PCs download the software directly from Splashtop. Users initiate secure remote access requests from their mobile device to their desktop (running Splashtop Streamer for Business software) by entering their credentials into the Splashtop Enterprise App.

2.2. Splashtop Streamer for Business

The Splashtop Streamer for Business software must be installed on each Windows PC or Mac desktop that the user will want to access from their mobile device. IT administrators can either install the software onto the employee's desktop computer directly using the management tools already in place, or allow users to download the streamer from the Splashtop Center server. IT can use the email templates provided in the Splashtop Center to distribute activation instructions with links to automate the download process. To enable mobile users to access more than one specific desktop computer, streamers must be installed onto those other systems as well. The streamer software can automatically login using the users' AD credentials and enable people to optionally join a group (or groups) as defined by the IT admin in Splashtop Center.

2.3. Splashtop Center

Splashtop Center is installed behind the enterprise firewall (or in the DMZ) on an existing Windows server. Its primary role is to authenticate and securely broker connections between the user's mobile device (running the Splashtop Enterprise app) and the user's desktop (running Splashtop Streamer for Business software). It also offers a management console allowing IT administrators to:

- **Set user, device, security & access policies including MAC address filtering**
- **Activate and deactivate users and devices**
- **Generate or import SSL certificates**
- **Group a pool of computers to be shared by users**
- **View real-time connections and audit trails**

Seamless integration with existing Active Directory (AD) domains helps to simplify the process of user authentication to ensure that only authorized users can establish remote sessions.

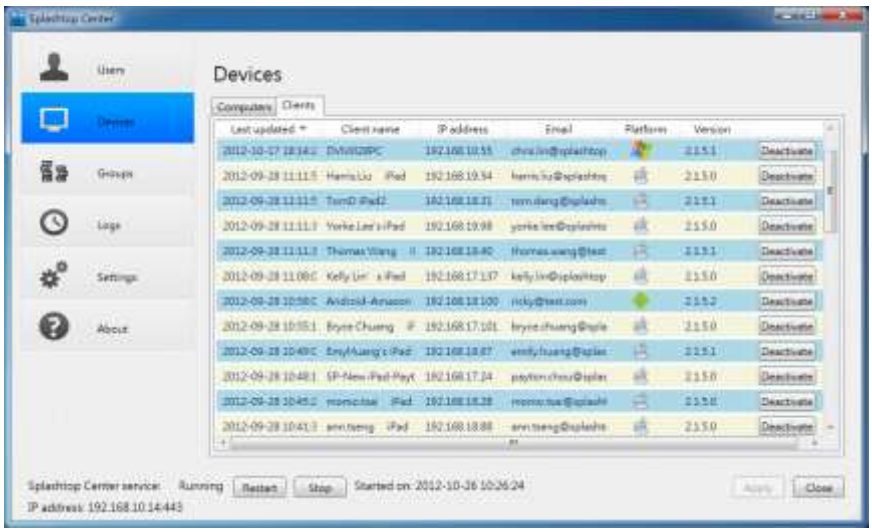

Figure 2: Splashtop Center Console

When the mobile device running the Splashtop Enterprise app is outside the local network, the Splashtop Center software provides secure relay services to enable cross-firewall connections between the mobile device and the desktop running the Splashtop Streamer for Business. All cross-firewall connections are encrypted using Secure Socket Layer (SSL) AES 256 – eliminating the headache of setting up VPNs, creating per-user firewall policies, configuring mobile VPN clients or supporting multiple RDP apps. For more information please read the whitepaper 'Splashtop Enterprise - Removing VPN-RDP Complexity'.

Splashtop Center's security controls ensure the protection of sensitive data and so helps improve regulatory compliance. For organizations specifically concerned with HIPAA compliance, please see the Appendix.

3. IT Security Controls

3.1. End-to-End-Data-Security

All communications within the Splashtop Enterprise solution – from the app through Splashtop Center and to the Splashtop Streamer for Business and back again – are secured over Splashtop's patent-pending streaming technology using the IETF-standard Transport Layer Security (TLS) protocol, ensuring the confidentiality, integrity and availability of data.

Splashtop Enterprise also prevents eavesdropping on and modification or replay of communications by restricting the cipher suite to 2048 bit ECDHE-RSA with 256-bit AES-CBC and SHA1.

In addition to the secured end-to-end session, Splashtop Enterprise leaves the data on the desktop, locked behind the corporate firewall. By streaming only the desktop display and sound, Splashtop Enterprise allows the user to access sensitive data remotely without actually transferring the source data to the mobile device where it may be easily stolen or copied. This not only prevents data from being stolen 'in flight' outside the organization but also secures the data from being stolen when accessed internally.

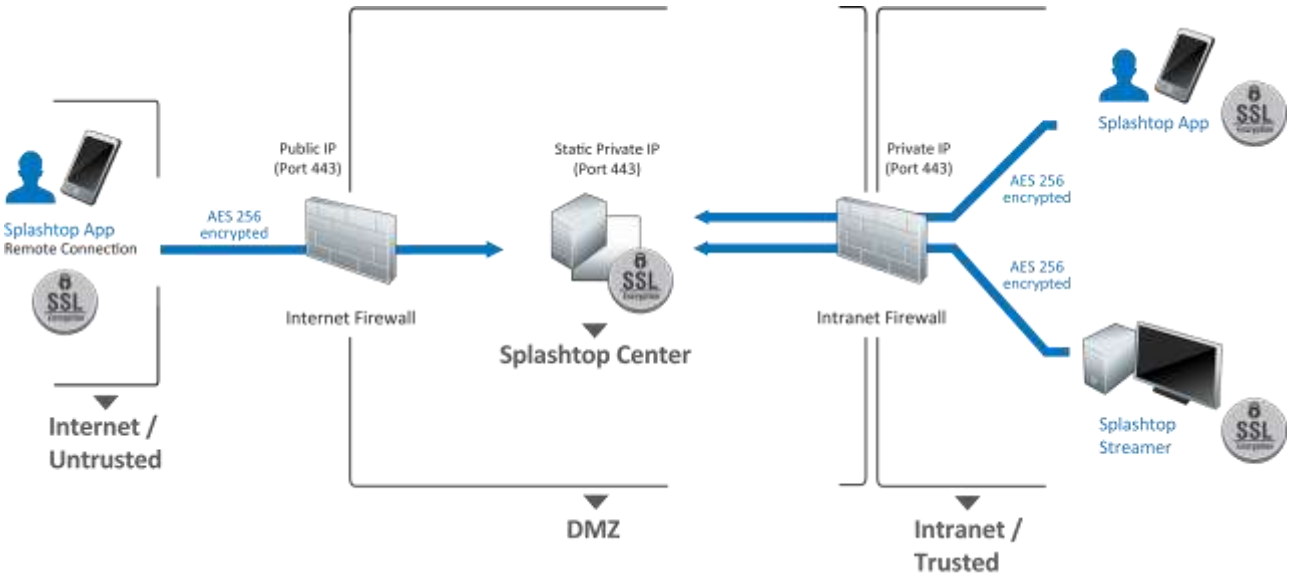

Figure 3: Splashtop Center Deployment in DMZ

3.2. Firewall Configurations

Based on the usage patterns and the location of desktops within the enterprise, changes to the firewall configuration file may be necessary in order to enable Splashtop for Business to function appropriately:

- For Intranet-only use of Splashtop Enterprise (e.g., both the mobile device and the desktop are behind the corporate firewall), no changes to the firewall are required.

- If the Splashtop Center is located in the DMZ and the mobile devices are behind the DMZ, then port 443 needs to be opened in each firewall.
- For internet usage where the external mobile device access and the Splashtop Center is located behind the corporate firewall, port 443 must be opened and port forwarding for Splashtop Center must be configured on the firewall. If port 443 is being used by another service, it can be changed to another port.

3.3. User Authentication

Seamless integration with existing Active Directory domains helps IT administrators simplify the process of user authentication and ensure that only authorized users can establish remote sessions.

Authorized Splashtop administrators can enable user access either manually, by entering the user's email address, or automatically, through seamless integration with Active Directory. In the latter option, Splashtop Center checks the user's username and password used during windows login against the Active Directory domain for each remote access session initiated by the user. Because Splashtop Center accesses the corporate Active Directory using read-only permissions, the data in the Active Directory remains safe from any rogue attempts to change its contents.

Gateway Users (local Splashtop Center users) passwords are stored in a salted hash. Domain User (AD users) passwords are never stored in Splashtop Center (and optionally never stored on the mobile device).

3.4. Digitally signed Applications

All software shipped by Splashtop is digitally signed so nothing can be altered or updated by any individual without the private key, ensuring the integrity of the Splashtop software reducing security risks.

3.5. Encryption

Splashtop Enterprise encrypts all data end-to-end using 256-bit Advanced Encryption Standard (AES). AES is the NIST-approved (National Institute of Standards and Technology) successor to DES.

3.6. Device Authentication

Only approved devices that have been specifically added by the Splashtop administrator can access the Splashtop Enterprise solution. Within Splashtop Center, administrators can allow/deny remote access by mobile devices individually using MAC addresses, lock or disable access by device, disable auto-logon (forcing users to enter passwords to connect), and de-activate a mobile device entirely.

3.7. SSL Security Certificate Administration

For additional security, both the Splashtop Center administrator and Splashtop mobile users themselves can import existing SSL certificates signed by a Certificate Authority (CA) or generate new, self-signed certificates. This additional layer of protection ensures that only the authorized user can initiate Splashtop remote sessions, even if his/her password is compromised. Only PFX format certificates are supported.

On local LAN connections, Splashtop apps and streamers will attempt to connect peer-to-peer to improve performance. The Splashtop Center administrator can optionally force additional security by prompting users to add an existing, or to generate a new, self-signed SSL certificate.

3.8. Additional Security Features

- **Blank screen:** Automatically blank the screen while a remote session is active, ensuring that an individual near the PC being accessed cannot see the remote user's actions. The admin can optionally force the blank screen for each session.
- **Screen auto-lock:** Automatically lock PC after the remote session ends to ensure the PC is not left logged in after a remote session terminates.
- **OS-level Access Control:** Splashtop Enterprise can optionally enforce controls already in place on the corporate LAN. In order to select this option, the user must supply his computer credentials in addition to his Splashtop credentials, thereby making it impossible for anyone other than the owner of the system to get access to that computer.
- **Session idle timeout:** Logout users when session has no activity for a specified time.
- **Remote connection notification:** Notify users on the desktop systems when a remote user connects to the PC with an on-screen message, eliminating "stealth connections".
- **Copy/paste prohibited:** Prohibit remote user from copying/pasting information to/from the desktop
- **File transfer prohibited:** Prohibit remote user from transferring files to/from the desktop.
- **Disable remote auto-login:** Force password re-entry for every remote connection.
- **Hide streamer configuration:** Non-admin users are unable to view/change configuration options.
- **Invalid SSL certificate warning:** Warning displayed to the Splashtop Enterprise app mobile user if the SSL certificate on Splashtop Center is invalid.
- **Proxy Server authentication:** The Splashtop streamer supports Basic and NTLM authentication with a proxy server using HTTPS to help prevent password capture, replay attacks and spoofing.

4. Conclusion

Splashtop Enterprise with SplashApp technology was designed and created by a team of security and networking experts, leveraging cutting-edge encryption and authentication technologies. This on-premise product is specifically built to give IT teams full control over securing the data while, at the same time, giving employees the flexibility to access it from anywhere. It is particularly applicable to organizations operating in industries with stringent legislative and compliance regulations where controls for data privacy and systems security are mandated.

Splashtop aspires to touch people's lives by delivering the best-in-class remote desktop experience – bridging tablets, phones, computers and TVs. Splashtop technology empowers consumer and business users with high-performance, secure, interactive access to their favorite applications, media content and files anytime, anywhere.

Prior to Splashtop Enterprise, the team at Splashtop developed the Splashtop Operating System (OS), an Instant ON OS that is pre-installed on more than 100 million desktops and laptops manufactured by HP, Lenovo, Dell, Acer, Sony, Asus, Toshiba, Intel and others. Splashtop Inc's headquarters are in San Jose, California.

4.1. Contact Information: Office Locations, Telephone Numbers

For further details and to start a free trial, please visit www.splashtop.com/enterprise

Silicon Valley Headquarters

1054 S. De Anza Blvd, Suite 200

San Jose, CA 95129

U.S.A

+1.408.861.1088

Taipei Office

10th Floor, No. 222,

Fuxing South Road, Section 1,

Taipei, Taiwan, 10666

+886.2.2778.0706

Tokyo Office

Level 20 Marunouchi Trust Tower - Main

1-8-3 Marunouchi, Chiyoda-Ku

Tokyo 100-0005 Japan

5. Appendix

5.1. HIPAA Compliance

Every business that is part of the U.S. healthcare industry must comply with Federal standards regulating sensitive and private patient information. In addition to protecting worker health insurance coverage, HIPAA sets forth standards for protecting the integrity, confidentiality and availability of electronic health information.

While no single product or solution can make an organization HIPAA-compliant, Splashtop® Enterprise is a solution that can help organizations meet HIPAA guidelines for the privacy and security of remote access to healthcare information and can be used within a larger system to support HIPAA compliance.

Although HIPAA compliance per se is applicable only to entities covered by HIPAA regulations (e.g., healthcare organizations), the technical security controls employed in the Splashtop Enterprise solution and associated host and client software meet HIPAA technical standards. Furthermore, the administrative configuration and control features provided by Splashtop Enterprise support healthcare organization compliance with the Administrative and Physical Safeguards sections of the final HIPAA Security Rules.

The following table is based upon the HIPAA Security Standards rule published in the Federal Register on February 20, 2003 (45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule). All implementation standards or specifications marked with a capital “(R)“ are required, while those marked with a capital “(A)” are considered “addressable”, essentially meaning that the entity is allowed some flexibility in taking “reasonable” steps to comply with the standard or specification to which it refers.

NIST Special Publication 800-66[1]. Descriptions. HIPAA Safeguard R=Required / A=Addressable	
Security Requirements	**Splashtop Enterprise Security Features**
Unique User Identification (R): Assign a unique name and/or number for Identifying and tracking user identity. [164.312(a)(2)(i)]	Allows the administrator to assign a unique user id/password (ID) to individual users. IDs can be edited or de-activated/deleted.
Access Control (R): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4). [164.312(a)(1)]	The Splashtop Center Server authenticates and verifies IDs against Active Directory. Grouping allows users access to groups of physical or virtual desktops on a per user and group basis. Device authentication ensures compromised ID credentials cannot be used from non-authenticated devices.
Person or Entity Authentication (R): Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. [164.312(d)]	Restrict access from remote locations by limiting access to the local network only. Restrict access using MAC address filtering on desktops and mobile devices
Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. [164.312(a)(2)(iii)]	Force password entry for every session by removing automatic login option from remote device. Non-admin users are unable to override configuration options. Authenticating with proxy servers helps prevent password capture, replay attacks and spoofing. Idle timeout ensures sessions are not left logged in.

Security Requirements	Splashtop Enterprise Security Features
Audit Controls (R): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronically protected health information. [164.312(b)]	Maintains an audit trail of all connections including the devices connecting from/to, session duration, date and time of session. A real-time view of sessions is also displayed.
Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information. [164.312(a)(2)(iv)] Transmission Security (R): Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. [164.312(e)(1)] Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. [164.312(e)(2)(ii)]	Uses SSL/AES-256 bit encryption for the end to end communication so customer health information is protected during transmission. Restricts cipher suite to 2048 bit ECDHE-RSA with 256-bit AES-CBC and SHA1. Code signed components of the software eliminate the possibility of tampering. Option to upload company SSL certificates for additional security.