LEOSTREAM™

VDI in Healthcare

Managing a Compliant Desktop Infrastructure

Simplifying Desktop Assignments and Login with the Leostream Connection Broker

By Leostream Corporation

Overview

More so than ever before, healthcare institutions are under the gun to deliver high-quality care and ensure compliance with government regulations, all while keeping costs in check. Recent mandates designed to improve accountability of care and administrative efficiency are drivers in shifting the world of medicine from a paper environment to one that is completely digitized – putting IT departments in the center of the action. As doctors and administrative staff become increasingly dependent on IT systems for mobile access to electronic resources, many institutions are turning to desktop virtualization to provide fast and reliable connections, ease systems management, and protect confidential information by keeping it off of end-user terminals.

In healthcare, connection broker technology is critical to deploying a virtual desktop infrastructure (VDI), a solution that separates the desktop environment from physical devices and centrally hosts resources in the data center. A connection broker lies at the heart of any virtual (or hosted) desktop deployment, and is the key component for assigning resources to end users and controlling the end-user experience. It's where all of the data center pieces are tied together, and all of the decisions are made about who can access what and how.

In this whitepaper we explore why healthcare institutions are looking to VDI to maintain a compliant desktop infrastructure while providing secure end-user access point. Secondly, we'll introduce the Leostream Connection Broker, which provides the management console to oversee the entire desktop environment.

Demands for VDI in Healthcare

No matter the industry, there are several draws to implementing VDI, from quick and efficient workstation provisioning, to mobile support for a variety of devices. In healthcare, VDI can specifically address a multitude of demands in order to improve security, mobility, and IT efficiency.

---

1. Increased Demand for Centralized Application Delivery

For most hospitals, virtualization is not uncharted territory. Large-scale rollouts of electronic medical records (EMR) often require application virtualization. EMR systems can run on a central server in the data center and can be accessed by doctors and clinical staff via a remote desktop protocol (RDP) on a thin client or mobile device instead of a fully loaded PC. A centralized approach makes it easier for IT to maintain and standardize the delivery of the application at scale. This concept of centralizing application delivery can also be applied to hosted desktops.

2. The Rise of Health Information Exchange

Interoperability is cornerstone to healthcare's increasingly collaborative care model. In order to stay competitive and to meet new regulations around electronic accessibility, medical institutions are stepping up efforts to improve data sharing. In the health care sector, putting personal health information (PHI) into the wrong hands can have serious consequences. Properly architected VDI solutions can ensure that intellectual property and PHI never leave the data center.

3. Improving Security in a Mobile World

The mobile movement goes hand in hand with health information exchange. Just like everyone else, doctors want to be mobile, and they need access to clinical data and applications at their fingertips. A VDI solution can give IT more control over security no matter where the medical staff roams. By keeping sensitive data off endpoints, information can be accessed from a number of devices and virtually any location. In addition, desktop virtualization offers enhanced security features including single sign-on access and proximity card authentication.

Additional Resource:

Blog: VDI in healthcare – taking the pain out of the desktop login experience

Read Now

4. The Need to Host Legacy Applications

Although huge advances in many areas of healthcare have occurred over the past decade, some corners of the industry have been slow to adopt certain technology. For a variety of reasons, healthcare organizations may be running legacy applications. While the benefits of upgrading to modern browsers, apps, and hardware are numerous, the process is often deemed unnecessary when the pros of redesigning or replacing the application do not outweigh the cons. In this situation, hosted desktops can be used to extend the longevity of a hospital's legacy application.

5. Controlling Hardware Costs

Like most organizations, hospitals and medical groups are on the look-out for ways to reduce costs. However, healthcare groups differ from other businesses in that the government and private insurers primarily fuel profits. Recent reforms that have shifted federal spending have greatly impacted budgets, causing healthcare leaders to use an even more discerning eye when evaluating costs. In some long-term scenarios, VDI has proven to reduce hardware investments and the cost to maintain desktop environments for an overall improved ROI.

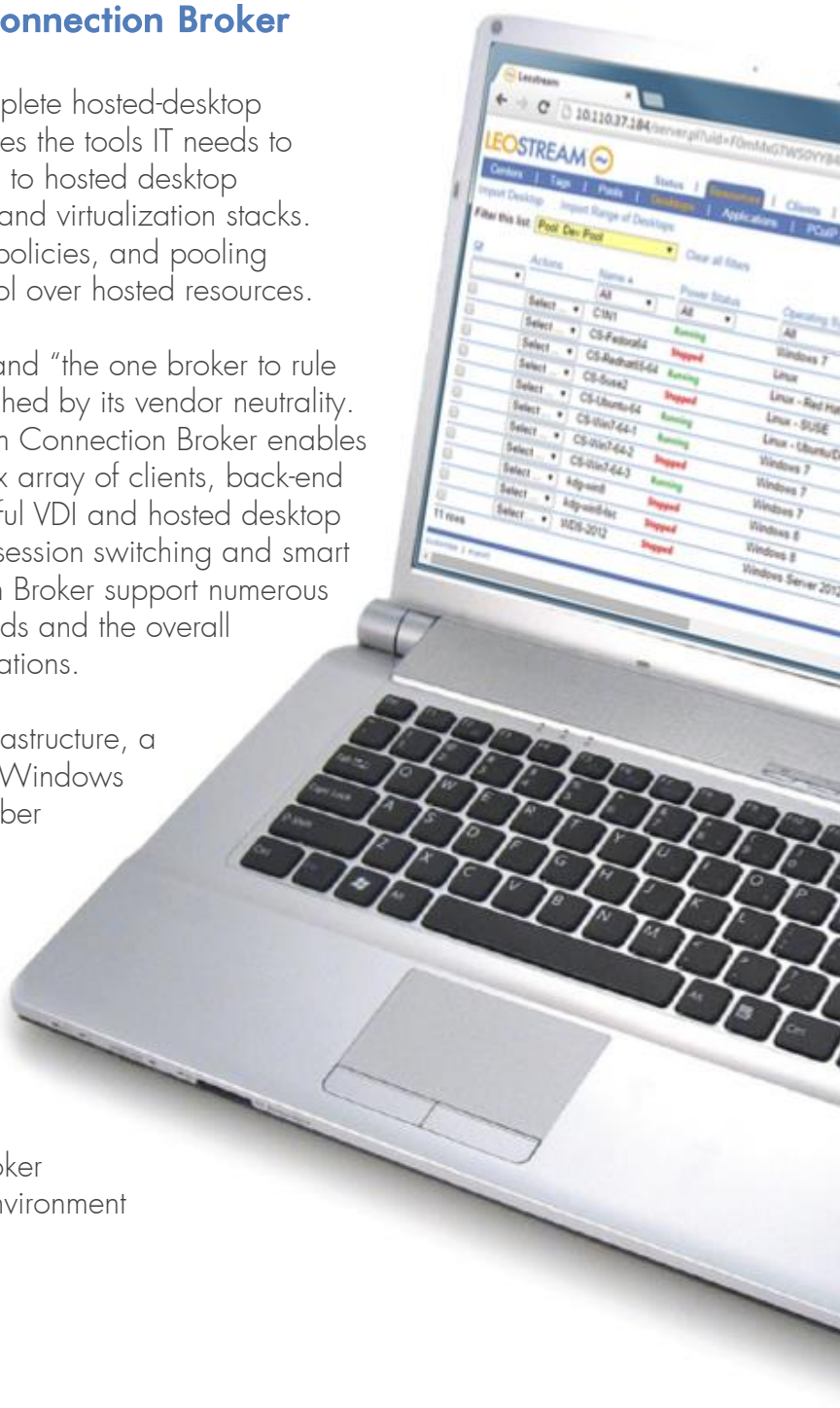
Maintaining a Compliant Desktop Infrastructure and Securing End-User Access Points with the Leostream Connection Broker

Introduction to the Leostream Connection Broker

The Leostream Connection Broker is a complete hosted-desktop connection-management platform. It provides the tools IT needs to manage user assignments and connections to hosted desktop environments across a variety of platforms and virtualization stacks. By offering a comprehensive set of plans, policies, and pooling options, Leostream gives IT complete control over hosted resources.

Coined the "Swiss Army knife of brokers" and "the one broker to rule them all", Leostream's software is distinguished by its vendor neutrality. By minimizing vendor lock-in, the Leostream Connection Broker enables medical institutions to integrate the complex array of clients, back-end systems and protocols required for successful VDI and hosted desktop deployments. Known for its lightening fast session switching and smart card integration, the Leostream Connection Broker support numerous workflows that improve desktop login speeds and the overall physician experience connecting to workstations.

Whether you want a virtual or physical infrastructure, a publicly or privately hosted data center, a Windows or Linux operating system, or any of a number of high-performance display protocols, Leostream offers a single pane of glass to manage it all.



Additional Resource:

eBook: How a Connection Broker Simplifies a Hosted Desktop Environment

Download Now

Why Leostream?

For healthcare institutions, the real benefits of including Leostream in a desktop virtualization initiative include improving security, the end-user experience and IT management.

Advanced Security

- Authentication - With support for two-factor authentication, Leostream integrates with smart cards, biometrics, and proximity cards. Through Leostream's partnership with Ensure Technologies and RF Ideas, hands-free, secure access to desktops in the data center can be achieved.

- Enhanced compliance - Leostream aids with compliance initiatives by providing full system log reports and by keeping HIPAA-governed data "off the edges" of the network, where the risk of loss makes compliance challenging.

End-User Experience

- Anywhere-access: Staff and physicians can access their desktops from any policy-sanctioned location using a PIN or a smart card. Take the example of a nurse that can access her desktops from inside the nursing station or by the patient's bedside.

- Hands-free log-in: By allowing hands-free login for medical staff, the desktop session follows the user. For example, after the initial logon for the day, user desktop sessions can be disconnected and reconnected in a matter of seconds. When a user walks away from a client device, their desktop session locks. When the user moves to a new room, their desktop session follows them.

IT Management

- Optimal Flexibility - The connection broker can plug into the hospital's current infrastructure such as the Active Directory. This type of seamless integration often enables organizations to repurpose or refresh client hardware, resulting in cost savings.

- Fine-grained control - Customized policies provide access to desktops/applications by end-user "role" and "location", and can also control USB device rights..

Connection Broker in Practice

3 Hospital Success Stories

With customers around the globe, the Leostream Connection Broker powers real-world VDI deployments that allow healthcare organizations to integrate nearly any data center element into a robust end-user computing environment. From improving desktop security to streamlining IT administrative tasks, Leostream's software has given hospitals, clinics, and other medical institutions the tools they need to simplify virtual and hosted desktop infrastructures. Below are a few of their success stories.

1 Leostream Connection Broker Makes HIPAA Compliant Anywhere Access Possible for Hospitals

Faced with tight regulation of HIPAA-mandated patient security, the need for failsafe 24/7 system reliability, and manageability concerns, a multi-site clinic turned to a hosted desktop solution managed by the Leostream Connection Broker. IT administrators specifically needed to address the issues outlined in the HIPAA security rules covering access to Electronic Protected Health Information (EPHI), including risks posed by lost passwords, offsite and insecure access, unattended workstations, USB data theft, data interception, and open networks.

The clinic decided to replace standard "fat" desktop PCs with Wyse thin clients equipped with card readers, moved Windows desktops to virtual machines and deployed the Leostream Connection Broker to implement and control secure access to the hosted environment. The Leostream Connection Broker also supports the clinic's need to use smart cards for strong, two-factor authentication, location based access to hosted desktops, and USB lock-down – effectively closing the security gaps that existed with traditional "fat" desktops.

The connection broker gives IT administrators the tools needed to implement the clinic's business rules. Broker policies enabled more granular security, allowing administrators to set location-based settings and USB access rights for groups and individuals.

By moving desktops to the data center, the clinic improved manageability and reduced power consumption. On top of that, adoption of thin clients reduced costs, maintenance, and the "footprint" of the device on medical carts and in space-constrained areas like the clinic's examination rooms.

Download the Full Case Study

2 Leostream Supports Fast Session Switching for Hospital Staff Login

In a fast-paced medical environment, time is always of the essence. Hospitals have shaved precious seconds off session logins using the Leostream Connection Broker. Prior to implementing Leostream, it took one hospital system up to 40 seconds to move sessions between login terminals. By layering the connection broker on top of its Citrix solution, the hospital was able to trim session switching times to under five seconds. In addition, the hospital leveraged Leostream's support for "tap-in" login through its integration with proximity cards. When a user taps the smart card onto the reader, data from the card is validated by the clinic's Active Directory and then sent to the connection broker, which selects the correct hosted desktop to present. The end user types a PIN, providing the second authentication factor, and unlocks the desktop.

Click the video below, to see a preview of the technology in action

3 Large Hospital Improves Security, Compliance and ROI with the Leostream Connection Broker

Across the board, healthcare providers are looking for ways to curb skyrocketing IT costs while addressing security and compliance. The same was true for a 600+ bed New York-based hospital. To achieve these goals, the hospital leadership turned to desktop virtualization design experts to architect a cloud-based VDI solution. With the inclusion of the Leostream Connection Broker, the medical staff now roams freely about the facility while retaining access to their desktop. Patient data remains secure; and the IT staff easily manages desktops and clients.

The urban hospital had a mixed technology environment. In older parts of the facility, staff worked on legacy PCs running either Microsoft Windows XP or Windows 7 operating systems, while in newer areas, staff used Windows-based thin clients and Cloud PCs to work on virtual machines. Over time, all of the PCs were replaced with Cloud PCs and the Leostream Connection Broker was used to provide infrastructure integration, connection management, and policy controls for the virtual desktop infrastructure. Redundant servers and Leostream Connection Broker appliances were deployed, ensuring high availability and uptime.

Critical to a successful deployment was ease-of-use for clinical staff, which was achieved by hands-free authentication. The hospital chose the XyLoc™ proximity solution from Ensure Technologies to provide a secure method of authentication that is virtually hands-free. By utilizing patented technology, the proximity solution provides radio frequency-based (RFID) security that automatically protects PCs when their users step away from them. The RFID credentials are passed to the Leostream Connection Broker, and Leostream policies configured for the hospital ensure that users receive their own desktops and files wherever they use a computer. The Leostream Connection Broker quickly retrieves the same desktop that the staff member used the last time they accessed the system, and is ready to display it by the time they arrive at the client device. That staff member immediately starts working on their desktop in the state they previously left it. No boot up, no login, no fishing for smart cards, and no need to de-glove for a fingerprint scan.

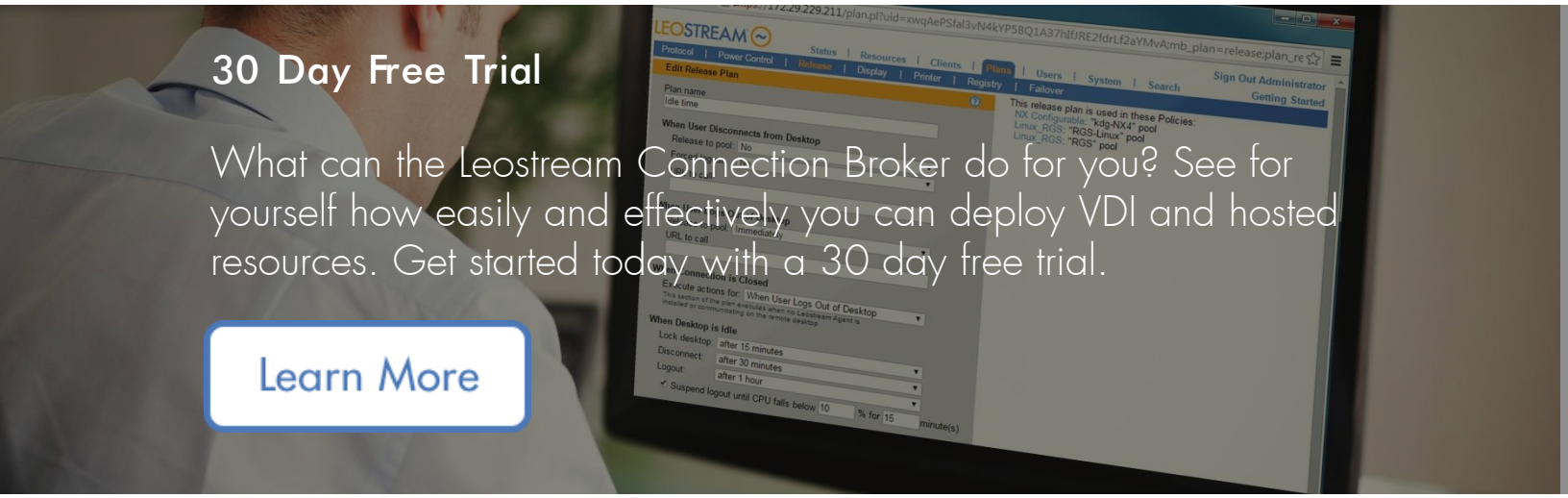
The new VDI solution provides significantly more security and flexibility with fewer resources and made a big impact on the bottom-line. An ROI calculation provided by the hospital determined that after implementation upwards of $471,000 and 1,600 hours of downtime were saved per year.

Download the Full Case Study

Conclusion

When properly implemented, VDI technology can be an ideal solution for healthcare organizations. By facilitating desktop connections and assignments across virtual and hosted desktop environments, the Leostream Connection Broker promotes:

- Protection of confidential patient data
- Centralized IT management
- Hands-free login for medical staff
- Improved desktop connection speeds
- Reduced IT costs and improved ROI
- And more



Suggested Resources

How a Connection Broker Simplifies Hosted Desktop Environments
Download Now

Hosted Desktop Solutions with Pixel-Perfect Graphics
Download Now

Whitepaper: Leostream as a Remote Access Solution
Download Now

Tip sheet: The top 5 considerations to address before deploying a large-scale VDI
Download Now

About Leostream

Leostream provides the critical connection-broker technology required for enterprises to achieve successful large-scale hosted desktop implementations. The Leostream Connection Broker is the industry's most widely deployed vendor-independent connection broker, enabling enterprises to integrate the complex array of clients, back-end systems and protocols required for successful hosted desktop deployments. Hundreds of large enterprises in financial services, healthcare, government and other sectors rely on the Leostream Connection Broker to "make desktop virtualization work" and deliver the best end-user experience. Leostream is based in Waltham, Mass.

To Evaluate or Purchase the Leostream Connection Broker

To evaluate the Leostream Connection Broker, please visit leostream.com and click on the homepage link for a free trial. You can purchase the Leostream Connection Broker by contacting Leostream at +1 781-890-2019 x710 or by contacting sales@leostream.com.

Contact Information


1-781-890-2019 x710


sales@leostream.com


Start a Free Trial