Unpacking VDI in the Finance Industry

Financial institutions have complex needs. They are often large organizations with numerous users and systems spread across many locations. They typically have a proprietary line of business applications and need to support special peripherals, such as card readers. In many cases, systems are shared by users. And these institutions must adhere to strict regulatory guidelines that require the highest level of data protection and auditing.

VDI technology can address these issues while making it easier for IT to provision and manage systems throughout the IT environment.

What is VDI?

A virtual desktop infrastructure, or VDI, refers to an architecture in which virtual systems are hosted in a data center. Full systems consisting of the desktop operating system, business applications, storage, and user-specific settings are hosted as virtual machines, or VMs, on a server. When a user runs an application or performs a task, this application or task is not running on the local computer. Instead, the person is accessing their virtual desktop remotely, using a PC, thin client, or mobile device.

A number of vendors offer robust VDI solutions for hosting virtual desktop environments. Three leading vendors are VMware, Microsoft, and Citrix. They offer a broad range of tools for creating and updating virtual desktop images, securing end-points with threat protection, managing storage and cloud resources, monitoring user activity, and more.

The Virtual Advantage

An architecture that combines VDI and thin clients offers some key advantages for highly regulated industries, such as healthcare and financial services.

Rather than working on a local system, users access data and run workloads on the remote system. This system and its workloads are stored and managed on a secure, centralized server that offers enhanced logging and auditing capabilities.

There are a variety of options for how an organization can configure its VDI environment, ranging from environments that are extremely locked down to environments that give users extensive control over their personal environment. Virtual desktops can be configured with your choice of operating system (typically Windows or Linux), they can include line of business apps, and they can support (or limit) various user permissions. When VDI is combined with a thin client solution, institutions enjoy the security, flexibility, and cost efficiency that come with thin clients, and can offer employees a clean, clutter-free workspace with room for upgrades that can boost productivity, such as larger and better monitors like the LG 38-inch UltraWide Curved thin client monitor, which provides enough real estate for the most ambitious multi-tasker.

One key option that will define your overall strategy is whether your virtual desktops are persistent or non-persistent. Non-persistent, or stateless, virtual desktops prevent users from customizing the individual environment. These stateless virtual desktops provide a generic, base environment that is essentially static from one session to the next.

Persistent virtual desktops, on the other hand, offer much more flexibility. Each user has their own virtual desktop on which they can install apps, save files, and make changes that will appear from one session to another. A persistent virtual desktop functions more like a local OS.

Each approach has its own advantages and which strategy an organization implements should depend on the company's business needs.

Provisioning VDI at scale

VDI boasts many benefits for IT departments that need to provision and manage large numbers of systems across different locations. Virtual environments can be configured to a strict standard, providing all the necessary applications and security settings. These baseline environments, which remain in the data center, are quickly provisioned to users as necessary. In roles where users frequently share systems, thin clients can be deployed, allowing users to log into any system to access their profile and desktop environment.

When new users need to be added to the network, they are simply given access to the baseline environment for their role. And this is done remotely by IT from a centralized location.

Securing the financial sector

Because the actual working environment remains in the data center, many common attack vectors are removed. Data remains stored in a secure data center and the workloads accessing the data are also housed on secure servers.

The centralized nature of VDI also ensures that each user is working on an up-to-date system. When a new patch or security update becomes available, IT can apply these changes to the baseline image. All users running virtual desktop environments receive the updated image. There is no need to push updates and wait for systems throughout the entire IT infrastructure to receive the latest security settings. And there’s not a risk that mobile devices outside the network might not receive critical updates in a timely fashion. Mobile devices connecting remotely, like clients within the corporate environment, are accessing the virtual environment hosted in the data center.

A locked-down, stateless VDI machine will prevent viruses and ransomware from being accidentally unleashed in the environment. Workstations carry certain vulnerabilities—such as physical theft, direct access to system resources, and the potential for malware to be installed. In a VDI architecture, the client system is essentially a remote control. Changes to the client system will not reach critical processes. Application workloads and sensitive data are abstracted from the client layer and remain securely removed, protected by firewalls and other security protocols in the data center.

To further protect data from misuse, virtualized environments can be segmented into various "trust zones." This controls the flow of data throughout the network, allowing IT to limit how data is shared across hosts or even physical NICs. A large bank, for instance, can organize applications and data into zones so information relevant to one division is not exposed to other divisions. By limiting a group's access to only the particular resources it requires, an organization can further reduce the potential for breaches and misuse of data.

Compliance and auditing

Current regulations, such as the Sarbanes-Oxley Act and the General Data Protection Regulation, define strict rules around data protection and compliance auditing. When an organization relies on traditional workstations it can be difficult for the IT department to monitor exactly how local applications and sensitive data are used. With VDI systems, IT gains complete insight into user activity. Individual transactions can be monitored, and IT can track exactly what data is accessed by which users.

Full data protection is maintained with data remaining in the data center on secure, encrypted drives. There is no risk of a rogue user copying data to a USB drive or sensitive data being exposed on a lost or stolen device.

Conclusion

VDI is a good solution for most modern IT environments. However, it is particularly well-suited to highly-regulated industries, such as financial businesses, where data protection and strict auditing policies are mandated. Combined with streamlined deployment and centralized systems management capabilities, VDI is a strategy financial institutions can bank on.