Working on Thin Clients? Here's How to Keep Your Data Safe

by Guest Contributor | Jun 22, 2016 | TechPro Essentials | 0 comments

Thin clients certainly aren't going to make headlines for being a sexy technology. However, they do present significant benefits in a number of environments, including factories, colleges, healthcare, and call centers, where users have tasks that require limited resources in terms of hardware and storage.

Earlier this year, The Register conducted a survey on the topic and found that there is a notable acknowledgement of the role thin clients play in meeting the needs of employees with relatively undemanding application requirements.

For users who spend most of their time accessing server- or cloud-based business applications, like on Chromebooks, or performing lightweight tasks with Microsoft Office, organizations can make a pretty good case for virtualizing and centralizing their Windows environment.

Guest article by *Roman Foeckl, CEO and Founder, CoSoSys*

According to IDC, by 2018, thin clients are expected to reach 7.8 million units shipped worldwide. Even with the recent dip in demand due to economic factors, the approach to data security in the thin client environment needs to be discussed.

For those vaguely familiar: A thin client is a light machine, with no hard disk and limited power compared to classic computers or so-called "fat" clients. They can run on Remote Desktop Protocol (RDP), Virtual Desktop Infrastructure (VDI) or other protocols. The IT infrastructure in these environments is simplified, with a terminal server that fulfills tasks like data processing and storage, acting like a host to the thin clients.

This technology presents benefits that include reduced total cost of ownership, simplified security, and increased

productivity. Moreover, the ease of replacing an old or damaged thin client is mutually beneficial to both the IT administrator and the user.

While the advantages of thin clients are clear for IT professionals, let's focus on the less obvious factors that could represent a threat — even in this type of environment.

How to ensure thin clients remain secure

In general, security professionals consider thin clients more secure because they do not have storage capacity. This means that everything users access and store resides on terminal servers, and that they have limited administrative privileges and limitations on installed applications. However, here's a few things to note:

- **USB Ports**: Thin clients with USB ports and Internet access make data transfers possible on the terminal server. As a result, it is very possible for a user to send confidential files to the cloud. Due to the lack of local storage, the chances of employees copying data on USB sticks are often even greater than on traditional computers. In the current mobile and digital context, users need flexibility and access to information to do their job, so even in a thin client environment, completely blocking access to USB ports and to the Internet would diminish productivity.
- **Internet Access**: Even organizations that offer as little as basic access to email are at risk for a data breach due to potential unauthorized file attachments, e-mails mistakenly sent to the incorrect recipients, or sensitive data sent to personal e-mail addresses. In the case of full access to the Internet, environments were observed where users uploaded confidential information to cloud file sharing applications, compensating for the thin clients' lack of storage and making them as vulnerable as classic desktops.
- **Central Server Storage**: While it is also a strong advantage, data saved and accessed from a centralized server could be very appealing for external attackers, even though it is considered an advantage compared to traditional environments where data is spread across users' computers and various drives.

Four tips to keep your company data safe

Security precautions in thin client environments should mirror those in traditional environments. IT administrators must enforce control on the use of portable storage devices and filter data that is copied or uploaded to cloud storage and other online applications. As thin clients continue to make their way into the workplace, think about the following tips to keep your company data safe.

Educate employees

According to a recent survey by CoSoSys, 35% of enterprise employees think that data security is not their responsibility. Add to this that 70% have access to and use confidential files, but 60% do not know which ones are actually confidential. When implementing DLP policies, IT departments need to properly train employees on how to use the technology, or face the consequences.

Data Loss Prevention (DLP)

DLP enables organizations to manage and control what USB and peripheral ports can connect to the endpoint, as well as what and how information leaves the safety of the network – something very useful for thin clients. The technology can notify the IT team of any situation where internal policy is violated.

USB encryption

Lost unencrypted USB devices still represent a major source of data breaches. If the best course of action for an organization is to allow access to USB thumb drives, then they should authorize only encrypted devices, ensuring that no third party can access stored data.

Embrace innovation

Beyond all else, each device and way of connecting to the Internet presents a unique opportunity to change the mindset within the organization that harbors fear of new or different technologies. By adopting a proactive approach to embrace new employee technologies, organizations can experience an increase in employee productivity and a reduction in insider and malicious threats to the corporate information security structure.

Roman Foeckl is the Founder and CEO of CoSoSys. Roman's vision is to offer an easy-to-use and implement Data Loss Prevention Solution that covers all popular platforms, from Mac OS to Windows and Linux, so large and small businesses can protect their data against accidental loss or intentional data theft.