stratodesk

How Stratodesk Boosts Endpoint Security

Stratodesk Whitepaper

Security is one of the chief concerns facing VDI deployments. In fact, it could be argued that security is the chief reason for virtual desktop infrastructure. It acts as a safety precaution against exploits that target endpoint devices, against natural disasters, theft, and beyond. Additionally, VDI allows IT to manage thousands of devices from one central location. Furthermore, with VDI, no data is stored on the endpoint itself, and yet, end users get the advantage of a full computing environment.

Still, servers, new hardware, IT overhead, Windows licenses and malware/antivirus contracts easily add up to a fortune. IT must deal with the massive demands placed on its own staff resources. In fact, it is estimated that organizations spend upwards of 1,000 hours a week on average updating, maintaining and patching their endpoints alone. Unfortunately, given how busy IT system administrators are today, it is far too difficult for them to manage the endpoint security of each of their devices without the right solution in place.

In order to enable an effective and secure VDI deployment, enterprises and organizations must educate themselves on the many options, challenges, and benefits of securely scaling their network of devices, as well as the alternatives available to reduce IT staff hours and overall costs.

IT leaders that already know the benefit of VDI may see the need to scale their existing environment, but are hesitant to begin the process because of budget restrictions. And they are right in being wary of a complete overhaul of their existing hardware. High performing endpoints can cost a fortune. Amidst the horizon of rapidly growing demands on time and budget, organizations must find a better way to manage and scale their environments, while at the same time cut back strain on staff who are left with more work than they can achieve alone.

With VDI, any given organization's productivity depends greatly on how well system administrators are able to effectively manage their entire network of mixed endpoint devices, and deliver virtual desktops, applications and necessary information to their end users in a convenient and expedient way. For this reason, organizations cannot afford to overlook this important aspect of their business. Endpoint management can, for better or for worse, have a disproportionate impact on the overall well being of day-to-day operations.

This paper seeks to explore effective strategies for enterprises and organizations looking to implement or expand their VDI while cutting costs and increasing security and performance. Also discussed is how NoTouch Desktop can proactively help organizations achieve their goals and better manage their complicated mixed environments of x86 and ARM based devices regardless of make, model or manufacturer.

Summary of Challenges Facing VDI/DaaS Endpoint Security

IT system admins face several obstacles as they struggle to find a balanced approach to endpoint management while also growing the number of seats in their network. Their first obstacle to overcome is the Windows issue. In order to allow for VDI, IT must run Windows installations on each of their endpoint devices. This means extra hours must be spent maintaining these devices. Not to mention IT must also provide antivirus and malware protection for each and every endpoint device. To make things worse, different devices house different versions of Windows, which creates even more complexity.

Along with the Windows problem is the matter of security. As previously mentioned, security is a key concern for VDI deployments – system admins must not only increase and maintain a high security standard while also decreasing login times, they must enable hardened security standards for the safety of confidential data and information. At the same time, they must allow staff to access all of the apps and data they need from any device, wherever they are. This causes great concern for IT managers who now have an equally high demand put not only on budget and security but also on ensuring convenience and flexibility at the same time.

In the case of an endpoint device being lost or stolen, how can IT leaders be assured that no confidential information is then accessible from the endpoint device? What about potential "evil maid" attacks? In reality, too many attack vectors exist that target the endpoint devices themselves.

Reliability is the third great challenge and cannot be stressed enough. Without an endpoint solution in place that is hassle free and one that offers a seamless user experience, workers cannot function at peak performance. If there is any hassle at all on the end user, you can quickly lose the benefit of VDI as IT resources are redirected towards aiding and assisting employees.

And, finally, many enterprises and organizations of all sizes and across multiple industries are facing a growing problem: the trend of faculty and staff bringing personal devices into the office, or using their personal devices to work from home. Employees want and expect to perform integral tasks on personal devices, either at home, in the office, or on the go. But how can this be done without opening up your network to the possibility of a security exploit?

Organizations have virtually zero control over endpoint devices themselves. If they are compromised, lost or stolen, these devices can pose a significant threat to your corporate network if the proper solution is not put in place.

How NoTouch Desktop Solves Security Challenges Facing VDI & DaaS Deployments

As technological innovation and virtualization has grown in adoption, so too has the need for a software solution capable of turning a seemingly mixed collection of new and existing devices into one congruent whole. This solution must be able to solve the challenges facing enterprises in deploying their cutting-edge VDI. It must function at the highest level, delivering the best user experience without breaking the bank.

Amidst the horizon of growlingly complex demands on time, budget, and security, Stratodesk software stands out as a much needed solution for end user computing in an enterprise environment. Capable of repurposing both old and new devices into high performing NoTouch Clients, Stratodesk software seeks to unify, standardize, and enhance the end user experience while delivering unparalleled reliability, faster login times, and protecting confidential data and information.

Stratodesk NoTouch Desktop, comprised of NoTouch OS and NoTouch Center, is the only endpoint OS and management solution able to run and manage both x86 and Raspberry Pi devices in the same environment.

Stratodesk Adds an Important Security Layer to Endpoint Devices

NoTouch is a highly secure software solution. User interaction with the system is limited to (unless otherwise configured) clicking on an icon, entering username & password and then being taken into a full-screen remote desktop. There are not many services running that allow access from the network. The default installation includes several features that may be of interest to some, but are not strictly necessary. If in doubt, go forward and deactivate SSH and RCMD.

Stratodesk NoTouch OS is Linux based, which means that it is impervious to common security threats that target or exploit x86 and ARM based devices. It can be installed via various installation methods like network (PXE) boot or MSI installer, and unlike competitors that require a specific piece of hardware to enable secure BYOD, NoTouch can run on any flash drive to let your end users access NoTouch or their native operating system side by side.

No Personal Data Stored

Devices repurposed and powered by Stratodesk software do not store any personal data on the endpoints themselves. Furthermore, Stratodesk also protects against the possibility of confidential data or information being acquired when a device is lost or stolen. Stratodesk software does this by safeguarding critical, sensitive information by encrypting it and blocking access to it. And while this form of encryption is very effective, some companies will inevitably require further and even more extensive security for certain information deemed by most to be not worthy of protection. For such companies, we offer a Disk Encryption upgrade.

Disk Encryption for Added Protection

Stratodesk's Disk Encryption functionality is an advanced functionality able to transparently encrypt the writable portion of the local storage medium on client devices where NoTouch is deployed. This means that in case of a device being stolen or illegitimately accessed, the data cannot be read. Disk Encryption can easily be switched on or off from NoTouch Center, and can allow for two different key phrases: one from the system, and one inputted by the user.

Even in VDI deployments where most personal information is not stored on the endpoint device itself, with Disk Encryption, any additional data, including URLs or private network certificates, will also be encrypted. Stratodesk protects all vital information from being physically accessed by unauthorized users and offers Disk Encryption to encrypt all data on the writable portion of the disk.

NoTouch Desktop Enables BYOD

Stratodesk's software supports BYOD to meet advanced requirements without opening up potential security threats. Faculty and staff can simply boot NoTouch OS in live mode from a USB stick in order to access important work files wherever they are at. When they are done, they can exit their session and remove the USB stick. Native operating systems won't be affected.

This effectively eliminates the challenges facing BYOD by ensuring that no important data is housed on the endpoint device itself. In the case of a personal device being lost or stolen, that device will not have any confidential or important personal or corporate data stored.

Summary of Security Benefits | Stratodesk

NoTouch repurposes existing devices into NoTouch Clients that require zero maintenance. This removes the Windows licensing obstacle, the need for antivirus/malware contracts, manually updating individual devices, and beyond. Because NoTouch OS is Linux based, it is impervious to common malware and security exploits.

When using Stratodesk software, enterprises can expect these benefits:

- **Cut Your Security Bill:** NoTouch OS installs directly onto all of your endpoint devices bare metal, transforming them into high performing NoTouch Clients. Cancel your malware and antivirus contracts and save your money.
- **Enable BYOD securely** with live boot mode from any USB stick.
- **Stratodesk protects against threats** from devices being lost or stolen. It does this by protecting confidential information and making sure no personal information is stored on the endpoint device itself.
- **Stratodesk offers Disk Encryption** for advanced security use cases.

How Does NoTouch Center Securely Communicate with NoTouch OS?

NoTouch software ensures secure communication between NoTouch Center and NoTouch OS. The overview below offers a complete analysis of these protocols that allow fast and effective management for all NoTouch devices in your VDI environment.

Stratodesk uses TCMP to ensure security between devices and NoTouch Center

- The announcements between the NoTouch Center and NoTouch OS are used for discovery of new clients, checking the runtime status of clients as well as getting new configuration or firmware updates from NoTouch Center.
- The client device connects the NoTouch Center server host by making an HTTP connection
- This protocol has been designed to work with only one-way TCP connection initiation, originating at the client, targeting NoTouch Center
- The frequency of this periodic connect can be adjusted by setting the announce interval parameter in the client's base settings; default is 60 minutes

RCMD: Stratodesk software uses RCMD to perform small actions on the client. RCMD allows NoTouch Center talk to any specific group of machines very quickly. This also allows you to search for new instances. After initial setup, RCMD can be switched off in favor of the even more robust and secure protocols –for example, SSH-based communication.

SSH: NoTouch OS and the Stratodesk Virtual appliance both have SSH access enabled on them. If required, admins can login via SSH and perform maintenance tasks.

VNC: VNC provides the ability to shadow a client from NoTouch Center. NoTouch uses an X11-based VNC server without encryption (x11vnc). A scrambling technique is also used to protect the passwords sent over the wire, but the actual VNC connection is unencrypted. Thus, over the open Internet you can use Teamviewer to enable HTTPS encryption for added security. VNC is primarily used for certificate management and works over HTTPS.

PXE Deployment and Update: PXE boot involves low-level network protocols like DHCP and TFTP that are typically used in LANs only and not over Internet or VPNs. While it is possible to run over WAN links, we strongly suggest using PXE server environments, i.e. instances of the Stratodesk Virtual Appliance or NoTouch OS instances with their built in PXE service capability in each remote location. When deploying Virtual Appliances to other locations, NoTouch Center can be deactivated in the satellite instances as management will be easier when only one instance is used.

SSL/HTTPS Connector: The Admin UI (web-interface) and MSrv module are both accessed via HTTPS.

TCRC: TCRC is a part of the RCMD service used to execute quick actions on the clients.

LDAP Authentication (Active Directory): LDAP allows several system administrators to access NoTouch Center without having to create local accounts. LDAP also allows administrators to define users or groups in the Active Directory and enables an LDAP filter to grant additional users access to NoTouch Center

Security Considerations: When using NoTouch Center in a Stratodesk Virtual Appliance, your clients will automatically use the HTTPS/443 port. You can and should configure Firewall of the VA and leave only port 443 open to ensure maximum security.

Stratodesk NoTouch Desktop Overview

NoTouch Desktop helps boost security with the low footprint NoTouch OS, and saves your system administrators time by automating much of the work involved in endpoint management. Cut costs, eliminate hassle, standardize endpoints, and maximizing security with the #1 solution of choice for organizations looking to scale their VDI.

NoTouch revolutionizes endpoint computing, elevates your workspace, automates management processes, and allows tens of thousands of devices to be managed from one central location. Additionally, NoTouch is the only endpoint management software that can be run on premises or from the cloud, which makes it the perfect solution for both VDI and DaaS.

Instantly deploy NoTouch onto thousands of devices via our various install methods (MSI installer, PXE boot) and enjoy hassle free endpoint computing.

The key benefits of NoTouch Desktop and how NoTouch solves major concerns facing institutions looking to scale are as follows:

NoTouch Desktop Saves On Costs

NoTouch comes with significant savings benefits. NoTouch Desktop provides a solution that easily repurposes PCs, Laptops and Thin Clients in your VDI into NoTouch Clients, operating on NoTouch OS. Not only does NoTouch OS save money by eliminating the need for capital purchases of hardware while eliminating common security threats, our integrated management suite, NoTouch Center, gives complete control over all VDI endpoints across multiple sites from one location. Reduce IT staff hours and hassle with one single endpoint management solution for your entire VDI.

Connects to All VDI Environments

NoTouch OS also has the clients for all major environments prebuilt into the OS. This means that whatever environment you or your solutions provider are using, NoTouch is ready and able to make the connection directly out of the box without any extra effort or expertise needed from your IT staff or workers.

On–Premises or Cloud-Based Administration

NoTouch is the only endpoint management software that can be run either on premises or from the Cloud. With NoTouch Cloud, management updates are applied automatically, appliances are actively managed, and home machines and BYOD are enabled without opening your network up to unnecessary security risks.

About Stratodesk

Stratodesk is the world's leading endpoint OS and management solution. It is used by government and healthcare organizations, banks, SMBs and large enterprises to eliminate cost and scalability obstacles facing their complex network of devices.
By delivering the only management software for mixed environments of x86, ARM and Raspberry Pi devices, Stratodesk is reinventing endpoint computing for enterprise IoT and VDI.
Our cutting edge, linux-based solution, NoTouch, is hardware-agnostic and runs on the Raspberry Pi.

www.stratodesk.com

contact@stratodesk.com

US: +1 (415) 946 4029

EU: +43 (463) 890298