



WYSE THINLINUX WITH SUSE LINUX OFFERS SECURITY, MANAGEABILITY

Wyse thin clients minimize malware with a smaller attack surface, protecting user data and delivering a lower TCO



EXECUTIVE SUMMARY

Given the uptick in high-profile malware attacks, IT security has become everyone's concern. Indeed, the devastating nature of modern malware requires all IT professionals to learn more about datacenter and endpoint options that enhance datacenter and user security. Dell's ThinLinux, based on SUSE Linux Enterprise Server, is an operating system that works with Wyse thin client endpoints to create one of the most secure environments available.

Wyse Thin Clients, with their minimal attack surface, provide peace of mind and a compelling feature set at a significantly lower TCO. Together these technologies create a canopy that can keep your users safe in an increasingly uncertain online environment. Among several enhancements, we are proud to offer superior ease of management with streamlined infrastructure to support your thin client footprint, once deployed. Our linear structure makes it far easier for your IT department to add applications as needed, presenting what feels like an open architecture, while still maintaining the elevated security enhancements of the SUSE Linux Enterprise distribution.

WYSE THINLINUX WITH SUSE LINUX: A MODERN ANTIDOTE TO UNCERTAINTY

There are many situations where endpoint security cannot hinge on a "maybe," a "could be," or a "possibly." This is especially important in an era when each week seems to bring word of a new breach or incursion. In a recent incident in March 2017, the Milwaukee-based Metropolitan Urology Group notified nearly 18,000 patients, that a malware attack may have exposed their names, medical data, account numbers, and medical procedures.¹

In such highly-critical environments, little can be left to chance or to a lack of imagination. IT departments need to limit the number of attack surfaces by deploying locked-down endpoints and safeguard user documents by keeping them in the datacenter where they are less prone to malware or hacker incursions than if stored locally. For customers looking for solutions that are both secure and affordable, Dell offers a range of Wyse thin clients based on the Wyse ThinLinux operating system.

ThinLinux also protects crucial data and potentially sensitive intellectual property (IP) by preventing hackers (or users) from using the local OS to take screenshots, another key security feature. This enterprise-grade Dell solution is based on SUSE

Linux Enterprise Server, which offers improved security over previous offerings based on the SUSE Linux Enterprise Desktop software iteration. Wyse Thin Clients minimize the malware attack surface, providing security and peace of mind at a significantly lower TCO.

While other Linux permutations or "definitions" are defined by their limitations, Wyse ThinLinux is a 64-bit OS that delivers striking performance improvement over the previous generations supplemented with a new, aesthetically pleasing user experience. It continues to build on its legacy features like management with Wyse Device Manager (WDM) and the https INI configurations server, and supports a broad range of peripherals and I/O elements that users have come to expect in a modern operating system.



The new layered structure allows upgrades and new applications to be added with ease. Early adopters have appreciated many of its enhanced features and consistent uptime. Its new flexibility adds the ability to connect to latest VMware, Citrix, and RDP clients, the ability to incorporate unified communications applications that use webcams such as Skype for Business, terminal emulation, and support for multi-monitor 4K displays.

In the past, there have been trade-offs between peripheral support and security. ThinLinux offers the right balance between the two. Without compromising on security, ThinLinux offers the ability to assign local printers, smart cards, CAC cards, SIPR cards, user proximity cards, fingerprint readers. Users (if approved by your IT department) can also access external storage platforms such as USB drives or traditional external hard drives along with an extensive list of standard

¹ *Healthcare IT News*, "Ransomware Attack Exposes Data of Nearly 18,000 Metropolitan Urology Patients," by Jessica Davis, March 2017.

peripherals. Wyse ThinLinux also provides the ability to use different-sized monitors, including those with touch capability.

With the advent of Wyse ThinLinux in 2016, enterprise IT departments started to evaluate its new user interface, simplified workflows, and enhanced security. Today Dell offers the peripheral drivers and a full feature set that place it among the most effective virtualized desktop environments. Our updates and additions include using version 4.4 of the Linux kernel with the latest libraries and features, as well as a simplified UX and modern UI. ThinLinux sets new benchmark in the user experience by offering support for multiple languages as well as multi-byte input package support. Additionally, we allow your IT department to choose Google's Chrome browser, and include rebranding customizations that can display your company logo at boot and shutdown.

A unique feature of ThinLinux is your ability to prevent users from downloading files from browsers. This prevents the unauthorized installation of new files while still allowing the ability to run native applications directly from web links. Over the past year, malware has become increasingly sophisticated, in some cases attacking traditional endpoints when users either unknowingly install fake browser extensions, when they click on malicious spam links, or when they attempt to view spoofed YouTube videos that include malicious JavaScript.²

While some may argue that "Linux is Linux," and that many distributions use the same binaries and minor enhancements, incorporating slight improvements that only long-time users would notice. But sophisticated, technically-minded IT managers will appreciate the fact that Dell has leveraged SUSE Linux Enterprise Server OS to deliver a Linux-based solution that is significantly more secure and more extensible. This allows you to add far more enhancements, as needed. When it comes to the network profile, only the most essential ports are open while also offering the flexibility to make port changes depending on which VDI brokerage your IT team chooses, and enabling VPN connections for secure remote access.

By default, ThinLinux only allows incoming TCP connections to its ICMP (ping) services and the WDM management agent service. It can also be configured to allow connections to its VNC and SSH services however these are typically disallowed by default to maximize the security of the thin client. Additionally, ThinLinux includes a full suite of standard Linux network tools including IP, Netstat, and Ethtool that can be used locally or remotely via WDM to monitor the thin clients' network activity.

Passionate Linux IT professionals may want to know more about what makes our SUSE-based option better than other manufacturers' thin clients running Linux. Indeed, they may be slightly skeptical and want to know why they should choose a Dell-architected Linux solution among the many software distributions and hardware endpoints on the market. The answer is clear from our mature Linux and Dell solution architecture backed by Dell Support. Among several enhancements, we are proud to offer superior ease of management with streamlined infrastructure to support your thin client footprint, once deployed. Our linear structure makes it far easier for your IT department to add applications as needed, presenting what feels like an open architecture, while still maintaining the elevated security enhancements of the SUSE Linux Enterprise distribution.

Our Wyse endpoints extend your TCO benefit by performing longer than a traditional PC, in some cases as long as five to seven years. Because our Wyse thin and zero clients have no moving parts, there is very little to break down, even with constant use. An Ethernet connection is all that is required to deliver a user's desktop from your datacenter. However, because the only elements that move from the datacenter to the edge are the pixels that present the user with a compelling and seamless computing experience, you know your data remains secure.

Additionally, Dell offers on-premises or remote cloud-based options to configure, monitor, and manage your Wyse endpoints and user security settings. Wyse ThinLinux minimizes the need for malware definitions and OS and application patching, thereby effectively reduces your IT support and maintenance costs. With its simplified OS packaging, imaging and deployment, your endpoint deployment times can be significantly reduced – along with IT travel and administration costs – across your user base.

In conclusion, Wyse ThinLinux is easy to deploy, configure, and manage given its rock-solid foundation built on SUSE Linux Enterprise Server. It delivers a better user experience by supporting a wide range of monitor sizes and screen resolutions and providing a familiar experience that will enhance productivity. It offers a full, traditional PC experience to your users by enabling broad peripheral support and allowing (if approved by your IT department) touch interface controls and other now-standard endpoint functionality. Please contact your Dell Sales Representative for a test drive of our Wyse thin and zero clients today.

Reed Martin is a Technical Marketing Senior Advisor in the Cloud Client-Computing division at Dell.

² eSecurity Planet, "Understanding Ransomware Vectors Key to Preventing Attack," by Paul Rubens, March 20, 2017