WHITEPAPER

Next-Level Endpoint Security

An Overview of NComputing's Offerings

This paper examines efficient approaches enterprises, and organizations can adopt to implement or expand their Virtual Desktop Infrastructure (VDI) or Desktop as a Service (Daas) while simultaneously reducing expenses and enhancing security and performance. It demonstrates how NComputing can actively assist organizations in accomplishing their objectives and efficiently managing their complex mixed environments, comprising Raspberry Pi-based and x86-64-based devices from different makes, models, and manufacturers.

Benefits of VDI & DaaS over traditional PCs/laptops

VDI and DaaS are more secure than conventional Windows PCs and laptops for a few reasons:

- **Central management of applications & data:** VDI allows IT administrators to centrally manage and control virtual desktops in the data center locations, which can help ensure that all security policies, software updates, and patches are applied uniformly across all virtual desktops. End-users no longer patch or install anything and can't introduce unauthorized software to their system.
- **Reduced risk of data loss due to theft or disaster recovery:** It's much easier for IT to secure the applications and data stored in the data center locations versus hundreds or thousands of traditional PCs or laptops. Because data is only stored centrally on VDI servers, it is easier to back up and recover data in case of a disaster or system failure, minimizing downtime and data loss.
- **Improved user delivery:** With VDI, any organization's productivity depends significantly on how effectively the system administrators can manage their entire network of mixed endpoints and deliver virtual desktops, applications, and necessary information to their end users.
- **Access control:** VDI enables IT administrators to implement granular access controls to virtual desktops, which can help prevent unauthorized access to sensitive data.

Challenges in endpoint security for VDI and DaaS

- **VDI and DaaS Endpoints are still vulnerable and require constant updates & management:** Enabling VDI or DaaS requires IT to run Windows installations on each endpoint device, equating to additional maintenance time. Moreover, IT must ensure each endpoint device has current antivirus and malware protection. Complicating matters further is that devices may be running different versions of Windows.
- **BYOD initiatives:** The trend of faculty and staff bringing personal devices into the office or using them to work from home. BYOD presents several security risks including accidentally or intentionally leaking sensitive data outside the organization, corporate data breaches due to device loss or theft, malware infections, lack of software updates or patches, and weak authentication on personal devices which attackers can easily bypass. BYOD devices are not company assets and cannot be centrally managed.

Boosting Endpoint Security and Cost-Effectiveness

NComputing LEAF OS is an advanced Linux software endpoint solution that enables organizations to deploy virtual desktops and applications securely and efficiently. With LEAF OS, organizations can establish a unified VDI and DaaS endpoint environment that standardizes and enhances the end-user experience while delivering unparalleled reliability, faster login times, and robust data protection. LEAF OS runs on x86-64 and Raspberry Pi platforms, offering a seamless and consistent experience across different devices. Organizations can leverage existing hardware investments and quickly scale their virtualization infrastructure.

Security is built from the ground up

NComputing's endpoint solution features LEAF OS and PMC Endpoint Manager. There are several key areas where NComputing boosts endpoint security:

"Chain of Trust" Secure Boot

UEFI Secure Boot is a security mechanism implemented in modern computer systems that ensures only trusted software can run during the boot process. The benefits include:

- **Protection against malware:** Secure Boot prevents malware from infecting the boot process, ensuring the system is free of malicious software from the moment it starts.
- **Protection against unauthorized access:** Secure Boot ensures that only authenticated operating systems and boot loaders are allowed to run, preventing unauthorized access to the system.
- **Compliance with security standards:** Secure Boot must comply with specific security standards, such as the UEFI Secure Boot specification for the x86-64 platforms.

Fully locked-down Linux OS

LEAF OS is a locked-down Linux operating system leveraging a read-only system image impervious to common security threats that target or exploit x86 and ARM-based devices. All changes made to the system during runtime are kept in memory only and deleted on reboot. System reboot always reverts the endpoint device to the original state based on the read-only image, further improving security posture and reducing the risk of successful cyber-attacks. This approach cuts down common security threats and renders device antivirus software unnecessary.

No personal data stored on devices

LEAF OS has a smaller attack surface than a traditional PC and eliminates user data leakage as LEAF OS does not store user data locally. Malware and other cyber threats that attack local storage devices have no target.

Encrypted communications

All LEAF OS communication to VDI environments and NComputing's PMC Endpoint Manager are encrypted using TLS (Transport Layer Security) protocols to establish a secure connection between the endpoint and the server components.

Exposing systems hosting sensitive data to the public Internet is not required. LEAF OS offers a variety of VPN options providing secure connections to the organizations' premises. Branch office or home users can safely access the hosted data on remote systems through encrypted VPN tunnels. LEAF OS includes the following VPN clients:

- IPsec/IKEv2
- IPsec/L2TP
- OpenVPN
- OpenConnect (Cisco AnyConnect)
- Fortinet SSL VPN
- PPTP

Granular access control

A locked-down VDI environment, as defined by the IT admin, means no other local processes or services are allowed. User access is restricted to specific applications and VDI environments, preventing unauthorized access to sensitive data and systems. Administrators can toggle on or off individual features or even platforms per endpoint.

Kiosk login for public access. Kiosk mode is a feature that restricts the endpoint to run only a specific application, further limiting the attack surface.

The admin can manage what local device settings are available to end users, providing granular control.

USB peripheral lock-down & management

Effective USB peripheral management is essential in protecting against potential security risks, as bad actors can hijack USB devices to steal sensitive data or execute unauthorized software. Admins can deactivate USB ports to reduce the attack surface or configure rules to block unwanted USB devices. LEAF OS provides granular access control over USB peripheral devices, including mass storage, audio, printers, video & image devices, smart card readers, and serial ports. Ethernet, WiFi, and Bluetooth connectivity access are also subject to management.

Centralized management

NComputing's PMC Endpoint Manager can remotely provision and manage LEAF OS endpoints, enforce security policies, apply software updates and patches, and monitor user activity. This centralized management reduces the risk of security breaches and helps IT administrators maintain a secure computing environment.

Manage devices in local and wide area networks, including devices behind firewalls and NAT routers. Working-from-home and hybrid workforce deployments are fully supported.

Onboarding new devices to PMC is easy and secure:

- Zero-touch onboarding based on predefined MAC addresses – new devices must connect online and are provisioned automatically without end-user interaction.
- Automatic discovery & onboarding of new devices in LAN environments.
- Optionally require a security passcode for new client onboarding in a WAN environment.
- Secure VNC shadowing for remote support. Password protection & secure remote shadow from PMC.
- Mark a device as 'Lost' (i.e., stolen) - PMC can mark the device as 'lost' to perform a remote factory reset to wipe all device configurations, lock the UI and block the device operability. Subsequently, PMC can mark the device as 'found' to unlock functionality and restore regular operation.
- PMC supports role-based access control (RBAC) to manage permissions and privileges of functions available to IT administrators. If an admin account is compromised, exposure is limited to only the features & functions authorized for that user.
- Detailed PMC event logging with filtering capability for tracking & auditing purposes.
- LEAF OS cannot be spoofed - Each LEAF OS device identifies itself with a unique and unalterable "serial number" obtained directly from the system hardware. This key is required for activation by *NComputing*'s PMC Endpoint Manager. This approach prevents bad actors from spoofing or impersonating a LEAF OS device.

Revitalize old computers running outdated Windows systems into high-performance, secure endpoints with zero maintenance

Install LEAF OS directly on the old computer's hard drive, converting the system into a powerful, secure, locked-down Linux thin client remotely provisioned and managed by PMC Endpoint Manager. Get more service from old computers and remove the need for antivirus/malware contracts and vulnerabilities related to outdated Windows patches. Deep integration into each supported VDI environment delivers a PC-like performance to end users, even on obsolete computers.

Enable BYOD and provide an isolated, secure computing environment

Run LEAF OS from a USB pen drive. USB booting leaves the user's existing operating system, files, and hard drive untouched while providing an ideal, isolated, and secure environment for work-from-home use cases. When users finish their work, a simple reboot to their native OS returns their device to personal use. Neither the BYOD nor USB devices house any data. PMC can remotely manage the USB pen drive to provision, configure and apply software updates. This isolated environment helps protect against malware, viruses, and data loss.

Summary

VDI and DaaS offer many benefits, including secure central management of applications and data, reduced risk of data loss due to theft or disaster recovery, improved user delivery, and granular access control. However, using VDI and DaaS endpoints requires constant updates and management, which can be time-consuming, resource intensive, and present potential roadblocks for wider adoption or deployment. Additionally, implementing BYOD (Bring Your Own Device) initiatives can present several security risks, including the possibility of compromised endpoint devices and unauthorized access to corporate resources.

NComputing improves endpoint security and economics by:

- Eliminating the need to upgrade hardware or run device antivirus software.
- Reduce maintenance costs and IT staff hours with centralized device management, software updates, and provisioning from a web browser.
- Strengthen endpoint security from device boot with our read-only, fully locked-down Linux OS providing secure & encrypted VDI sessions.
- Enable BYOD with an isolated, secure, and virus-free computing environment while preventing data leakage.

By incorporating these measures, organizations can enhance endpoint security, safeguard sensitive data, and reduce the risk of data breaches or unauthorized access while saving costs.

400 Concar Drive, 4th Floor | San Mateo, CA 94402 | 1.650.409.5959 | *info@ncomputing.com* | *www.ncomputing.com*

359067_V2