NComputing

WHITE PAPER verde

# How to Secure Your Data with the VERDE VDI™ Private Cloud Solution.

## The Most Secure VDI For Your Data.

## Table of Contents

## Delivering Three Security Benefits

With BYOD and the popularity of mobile devices on the rise, data is becoming increasingly vulnerable. As a result, organizations worldwide, including those in need of government-level security, are under pressure to find new ways to connect users to their applications, data and missions, while increasing operational control and reducing security risks.

From its inception, a Virtual Desktop Infrastructure (VDI) has held an inherent advantage when it comes to security. In virtualized desktop environments, all data remains exclusively and entirely within the data center. Although users of virtualized desktops experience the same interaction with data that they always have, and can even enjoy the flexibility of using their preferred devices, such as personal tablets and laptops, no data actually flows across the network and no data resides on end-user systems in virtualized desktop environments. The scope of securing the environment therefore narrows to securing the data center – a more manageable exercise for data and network managers and information security professionals.

By moving to a virtual desktop infrastructure, organizations can greatly reduce risk in key areas that present challenges, including BYOD, multi-level security and business continuity. The *NComputing* **VERDE VDI** (Virtual Enterprise Remote Desktop Environment) private cloud solution allows IT professionals to easily deploy, configure and manage the entire end user computing experience, whether Windows or Linux-based, while ensuring tight security across the enterprise.

### Security Benefit #1: Securing Data at Rest

#### Solving the challenge of data at rest - keep it in the data center and off the desktop

Inactive data, such as a document stored on a user's desktop and not currently in use, presents a challenge to information security professionals. Regardless of how long it has been since someone last accessed the document, the document must remain secure, with appropriate encryption and backup, and it must remain readily available to the user.

One way to secure data at rest is to keep it in the data center, where it is physically secure and managed within a server-based computing solution. In virtualized desktop environments such as those created by *NComputing*, users edit data via remote sessions. During the sessions, users see a visual representation of what they are working on as they use the applications and operating systems they are accustomed to using. However, the visual representation consists entirely of pixels – the data itself does not move over the network and is never stored on the endpoint device. All data, including data at rest, remains securely within the data center.

### Security Benefit #2: Authentication, Authorization and Accounting

#### Desktop virtualization addresses three critical criteria in securing the environment

Authentication, authorization and accounting, known as AAA, are critical criteria for securely controlling and monitoring access to a network and its resources. Desktop virtualization addresses each of these, providing network and security professionals with the ability to:

- Verify identity before allowing any access at all (authentication)
- Determine exactly which desktops, applications or networks any user can access (authorization)
- Track and record a user's activity on the network at a level that ensures non-repudiation (accounting)

### Authentication

Just like a personal computer, **VERDE VDI** desktop virtualization controls user access down to the desktop level. However, before a user can access data, applications or even the desktop itself, **VERDE VDI** requires data center or desktop authentication. That means that upon connection, the user must authenticate via a directory (**VERDE VDI** supports Active Directory, eDirectory, and Oracle Internet Directory, or your choice of any other LDAP-based directory service) and receive authorization before proceeding.

This level of authentication is superior to PC-level security methods, in which a user who cannot successfully authenticate when attempting to connect to a network presumably already has access to the physical PC and its contents.

### Authorization

Authorization determines which desktops, applications or networks any user can access. With **VERDE VDI** desktop virtualization, network authorization is required even before a user reaches the desktop. **VERDE VDI** utilizes a two-factor authentication process that includes standard user/password login requirements and optionally layers in an extra level of security through MAC address filtering.

Even through a BYOD device, absolutely no information is viewable until the user has received access to the network.

### Accounting

Once authentication and authorization complete, accounting tracks and records the user's interaction with the network and the desktop cloud infrastructure at a granular level. Administrators can audit this information, filtering by specific users, events, networks from the system console when needed.

## Security Benefit #3: Application and Regulatory Compliance

### VERDE VDI desktop virtualization addresses both licensing and regulatory compliance

Compliance – both application compliance (licensing) and regulatory compliance (control of data) – is an essential security consideration.

**VERDE VDI** desktop virtualization makes compliance with application licensing easy because IT provisions all user applications in a single desktop container per user. Network administrators can monitor and control which applications are in use and by what user, and whether the user has proper authorization and licenses for the applications.

In addition to auditing application use, **VERDE VDI** can also track and control data flow itself. That ensures that when users access network data, they are doing so within the compliance policies and parameters set forth by the network manager. It is important to note that **VERDE VDI** controls both the data and the data paths themselves. With a PC, giving a user access to a network share on a physical PC results in data moving across the network to the endpoint PC, whether through a VPN or the public Internet. With a desktop virtualization container, by contrast, data never leaves the data center. The data moves from the data store to the application that is using it, but all movement takes place within the data center. This ensures a completely isolated and secure environment that the network administrator can physically control.

That sort of complete control of the desktop, applications, data and networks is particularly critical in instances in which data and data flow require tight control to meet regulatory compliance laws such as HIPAA.

An additional security benefit of the **VERDE VDI** solution is the ability to separate auditing data, user data and system data throughout the data's lifecycle. IT can keep audit logs and backup media separated per security regulations, allowing different backups to different targets – an important part of the compliance lifecycle. Backup and control is simpler because everything remains under the system administrator's control, and in one physical location. Without control over physical links, security and network managers must wrestle to bring compliance under control.

## VERDE VDI Solves Three Key Security Challenges

**VERDE VDI** desktop virtualization specifically addresses three challenging areas for network security professionals:

- **BYOD:** Bring Your Own Device means users now introduce their own iPads, smart phones and other devices to the network, expecting access anywhere and at any time. Desktop virtualization locks down BYOD issues with granular control.
- **Multi-level security:** The US Department of Defense accepted multi-level security from *NComputing* allows network security experts to differentiate user missions on the server side and physically segregate the data flow between them. Read the Case Study.
- **Disaster recovery:** Often thought of as a business issue, disaster recovery is also a security concern. VERDE VDI desktop virtualization solves business continuity issues with its unique infrastructure design, including: stateless servers, single-volume backup and restore, and high availability within clusters.

### Security Challenge #1: BYOD

#### VERDE VDI, in effect, locks down user devices with access control, architecture and governance and risk management

BYOD, or bring-your-own-device, has proven popular with users because it offers great flexibility, allowing users to access the network at home or on the road using user devices such as iPads and smart phones. However, that flexibility also introduces huge security challenges. IT still needs user management, as well as tools to implement and enforce security policies for each user.

**VERDE VDI** desktop virtualization addresses three security domains relating to BYOD: access control, security architecture and design, and data flow control.

#### BYOD: Access Control

Desktop virtualization gives IT control over access to all data residing within the data center for all users. Because this access control takes place at the gateway, only authorized users can receive content. At the gateway, authentication, authorization and access control take place – all before giving users access to their desktops.

Specific to BYOD, **VERDE VDI** desktop virtualization enables IT to control access to peripheral devices at a granular level. Policies can be set to control exactly what, if any, peripheral devices a user is allowed to connect to virtual desktops, as well as which networks each device can access.

As always with desktop virtualization, once a user has access to a container, he still cannot use the endpoint device to remove data from the network, since the user is simply seeing a real-time view of the desktop, rather than actual data. Access control policies can lock down the use of clipboards, USB storage and even printers.

While this level of control does not eliminate the importance of endpoint security, it helps minimize its scope and complexity.

### BYOD: Security Architecture and Design

From both data compliance and data at rest aspects, security concerns dictate that data not leave the data center. Users must be able to access documents within a secure virtual container that allows them to view documents but not download them. Data control with desktop virtualization allows this while preserving data integrity. Data authored during a desktop virtualization session originated in a secure environment following network policies, so authorship is never an issue.

*NComputing* maintains a leadership position in security architecture and design. Out of the box, **VERDE VDI** includes the ability to remove malicious software upon image reboot. Malware protection resides on the server rather than on individual devices, so device security in a BYOD environment is easier to maintain and monitor.

A user attacked by a virus can log out and reconnect, bringing up a pristine desktop based on the original gold image delivered from the secure data center, while preserving the user's personal data. With **VERDE VDI**, malware and unauthorized changes cannot persist between sessions, and users return to the gold image without losing data.

**VERDE VDI** also has the native capability to allow quotas and limits to be set on both sessions and organizations using the system. Since the system is multi-tenant, it supports different companies, missions, organizations and groups within the same infrastructure. The system administrator controls how much storage and how much network capacity each user – or group of users – can consume. This is extremely effective in preventing denial of service attacks, since a user or group of users can never take over the system.

**VERDE VDI** provides native controls with which to set data, network and processing quotas without requiring third-party storage products or firewalls from outside vendors.

### BYOD: Information Security Governance and Risk Management

BYOD also raises security issues around governance and risk management. **VERDE VDI** has received government accreditation and has been validated using DISA (Defense Information Systems Agency) security scans and Secure Technical Implementation Guides (STIG).

With **VERDE VDI** desktop virtualization, IT can track any action occurring on the network via an unauthorized device, even without access to the actual device. Moreover, pre-established policies dictate administrator and end user assignments during account creation. Meeting specifications of the Department of Defense (DOD), **VERDE VDI** desktop virtualization tracks network assignment by user. The system can monitor every occurrence on the network, beginning with the network address assigned to the user upon connection. That includes the capability to monitor not just IP addresses, but also the most fundamental aspects of the network, including hardware addresses – a granular level of tracking that ensures non-repudiation.

## Security Challenge #2: Multi-level Security

### Desktop virtualization from NComputing simplifies multi-level security with a DOD- accepted solution allowing mission segregation on the server side

Although BYOD is perhaps the biggest security concern in today's enterprise, there are other issues, including the need to provide multi-level security.

**VERDE VDI** enables DOD-accepted multi-level security segregation on the server side, making desktop security far more efficient for network managers. With **VERDE VDI**, IT can comply with a security policy calling for three separate, physical desktops for a user within the same client desktop environment. Each desktop has different policies and communicates

with separate physical networks, but all three implementations exist within a single infrastructure. That avoids the difficult-to-manage silos of applications created when this problem is addressed using other methods

**VERDE VDI** enables centralized management, avoiding the need for redundant infrastructure to ensure physical separation. That makes providing desktops to end users very efficient – even with users assigned to different missions and security levels. When missions change and IT must reassign resources, it is easy to repurpose the hardware and software. Changing access to data and applications based on role or device is as simple as changing central authentication policies, with no need to "wipe," or even touch, end user devices. Missions can execute on separate physical networks within the same management umbrella, unifying all control under one console.

### Access Control

Part of ensuring tight multi-level security is access control. **VERDE VDI** requires users to pass through access control even before accessing the system gateway. In addition, a gateway checks user access before allowing connection to an enclave. Gateways are physically separate and on different networks, giving the user access to separate networks and enclaves as needed.

The **VERDE VDI** single-infrastructure design includes gateways with built-in firewall controls, eliminating the need for a separate, third-party firewall between the gateway(s) and the infrastructure. IT can share management functions while separating computing, networks and data by policy.

For less stringent compliance requirements such as application licensing scenarios, sessions can run on their own dedicated nodes on a secure network, with data paths allowed to cross.

### Telecommunications and Network Security

Cloud computing offers many benefits, including enabling remote users and providing high network throughput over distance. There is an additional and significant cloud benefit: security. **VERDE VDI** Cloud Branch technology allows network managers to isolate networks, processing and data within the same infrastructure or mission, while retaining centralized management. Its desktop cloud system extends beyond desktop virtualization capabilities to enable virtual desktops within the native **VERDE VDI** infrastructure. That level of scalability ensures that adding additional capacity horizontally will not require that you modify your data center.

With Cloud Branch technology, there is no requirement to manage a separate instance of an operating system such as Microsoft Windows 7 or 8 for each user. Instead, IT can manage a single operating system push changes out to users as needed via policy settings, even if those users are running virtual desktops on isolated networks. This makes use of **VERDE VDI** cascading management system, which ensures that when the user consumes the image, the consumption takes place on a separate node with appropriate access controls to the network. Cloud Branch technology can extend centralized management to physically isolated nodes within the same data center, or over vast geographic distances, with the same ease.

**VERDE VDI** desktop virtualization also uses dedicated network ports for different tasks. An end user's desktop might display remotely over one port, while image synchronization across servers occurs on a different port, and the management platform resides on yet another dedicated, discrete port. This permits greater control over data flow.

### Multi-tenancy

Multi-tenancy is a key element of cloud computing. The **VERDE VDI** technology is multi-tenant by default, allowing for confidentiality, isolation and compliance within a single infrastructure. Using native multi-tenancy, **VERDE VDI** enables a set group of servers to be dedicated to one mission, enclave, organization, team or company. **VERDE VDI** software ensures that anyone who authenticates from that organization runs workloads and accesses data only within those servers. The number of servers assigned to that organization can easily be resized, repurposed or horizontally scaled.

## Security Challenge #3: Business Continuity and Disaster Recovery

### NComputing makes securing an often-overlooked area easy and straightforward

Business continuity and disaster recovery are an important security concern as well as a business issue. Based on its infrastructure design, **VERDE VDI** desktop virtualization provides a solid, secure, easily manageable business continuity and disaster recovery solution.

### Single Volume Backup / Restore

Because **VERDE VDI** allows use of a single volume for backup and restore purposes, the entire state of a system can be stored on a single storage device or logical storage system. This allows the network administrator to centralize all data on a single device or volume, if desired, making backup simple and straightforward. Backing up or restoring system data, configuration policies and user data involves a single process.

### Stateless Servers

Stateless servers translate to high availability in a cluster. All **VERDE VDI** servers are stateless; each has a unique address assigned to it but is otherwise identical to every other server. There is no physical server affinity for workloads or data by default. The unexpected loss of a number of servers simultaneously may slow the network, but the cluster continues to operate. When servers are back online, they begin working automatically after automated deployment, without human intervention or an extensive setup process.

### High Availability within Distributed Clusters

High availability within clusters is critical for business continuity. For disaster recovery, **VERDE VDI** Cloud Branch technology allows geographic dispersal of clustered computer resources. If a data center in one location goes down, Cloud Branch can continue to run other data centers since Cloud Branch can run even when disconnected from the network. During repair, Cloud Branch uses cached information from the most recent synchronization to continue operating without interruption.

A retail model serves as an excellent use case illustrating the power of **VERDE VDI** Cloud Branch in guaranteeing high availability. Imagine a master data center storing all images, policies and management systems in a central location, connected to a number of branch servers in different locations (retail stores) – a federated model. Each store's on-premise servers connect to user terminals at the store location. Users need limited, controlled access to the central data center based on policies, and continual access to the system. With Cloud Branch, a caching proxy allows offline work to continue. Updating the operating system image for all stores, for example, can happen automatically, in parallel to users based on their last node image. If connectivity with the data center is lost, branches can continue operating based on their most recent image.

## Summary: VERDE VDI, Desktop Virtualization and Security

Fast-moving technology and business challenges such as BYOD, multi-level security and disaster recovery drive the need for better security across today's enterprise networks.

**VERDE VDI** desktop virtualization, including its Cloud Branch technology, brings high levels of security to multiple aspects of the virtualized user environment. Because applications and data remain within the data center at all times throughout every user session, **VERDE VDI** is a natural solution that puts the security perimeter back in the data center.

## Additional Resources

### Articles

- Understanding Successful VDI Implementation
- How Government Entitites Can Deploy Linux and Windows Virtual Desktops
- Managing User Profiles within Traditional or Virtual Desktop Settings

### Case Studies

- **U.S. Department of Defense:** The solution for the mixed world of Windows and Linux
- **Chuo University:** A Desktop Cloud Environment for Anywhere, Anytime Learning
- **Gruppo api:** Reducing Operating Costs by 30% with VDI
- **LMU Munich:** Streamlines IT operations and improves service to students

### Documentation

- VERDE VDI Datasheet

### Whitepapers

- How VDI Secures Your Data
- Cut your Storage Costs in Half



1900 S. Norfolk Street, Suite 245 | San Mateo, CA 94403 | 1.650.409.5959 | *info@ncomputing.com* | *www.ncomputing.com*





662762_V2