Trusted Secure Remote Access

White Paper: How the vKey Solves Remote Workplace Challenges

Executive Summary

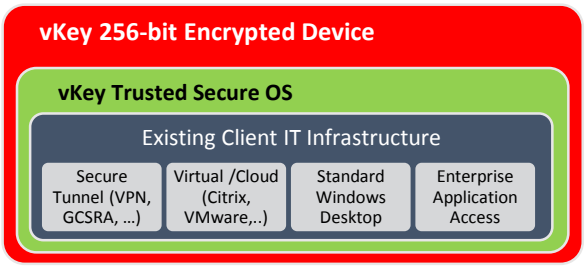
Traditional workstations and laptops can be hard to manage, difficult to secure properly and easy to break.

When remote access is introduced to your corporate infrastructure, to enable employees' access to critical business applications anywhere, the end device is always a potential security threat. The vKey Solution recognizes the following challenges:

- **Enterprises that utilize secure remote access technology, also require a secure, healthy end-point to ensure confidentiality, integrity and availability.**
- **Device management and user accountability are necessary in corporate policy but are difficult to ensure on remote devices.**
- **Business continuity solutions that provide end-users with ready, healthy, end-point devices are often expensive and lack enterprise-level functionality.**

The vKey Device is the solution to address these challenges. An encrypted portable device with vKey software, optionally managed by the vKey Device Manager server.

The vKey Solution



The vKey 4 Device is software on an encrypted, bootable portable storage device that provides a secure operating system environment for use on any modern system (PC or Mac). With a vKey, users can access their workplace resources (applications, desktop, networks, et cetera) without compromising enterprise security.

Zero-Footprint

vKey Devices are bootable in the same way as a computer hard disk. So when you boot (start) from a vKey Device, the vKey appears to temporarily replace the computer's existing computer hard drive with a trusted, encrypted end-point device. vKey doesn't change anything on the computer, nor is there ever any communication between the computer's hard disk(s) and the vKey Device.

Management

DLS offers a remote device management solution – vKey Device Manager (vDM) as a virtual appliance which typically resides in the DMZ of an enterprise network. vDM provides the ability to: link vKey Devices to Active Directory users; create new vKey Devices from regular portable storage media, remotely monitor the connection status of vKey Devices; and, remotely disable or wipe lost or stolen devices.

Lost or Stolen Devices

When an endpoint device is lost or stolen, corporate data and personal information are at risk. The vKey Device mitigates this risk by storing and running everything in an encrypted state using AES-256 algorithm (FIPS 197). Only an authenticated end-user can decrypt the device and its contents.

vKey Solution Use Cases

vKey Devices run on virtually any modern PC or Mac. Simply plug the vKey Device into a host PC or Mac and start the host machine to enable the vKey Solution.

Trusted, Secure Remote Access

vKey 4 Devices come in Standard, Professional and Enterprise editions, all of which are ready to provide secure and trusted thin-client access for end-users with internet or intranet connectivity. Organizations with existing cloud or virtual infrastructure from Citrix, VMware, Microsoft and others can immediately use vKey Devices to provide a portable, trusted and easy to use end-point for cloud or virtual access.

Trusted, Secure and Portable Desktop Virtualization

vKey 4 Professional and Enterprise additions provide secure and trusted cloud or virtual access for end-users with or without internet or intranet connectivity. Where no connectivity exists, these devices can run virtualized copies of the organization's existing Windows desktop. The user simply clicks on an icon to start their own virtualized version of the organization's standard Windows desktop, complete with all of the security, patch updates, VPN connectivity and other capabilities already architected into the organization's Windows desktop.

vKey Devices running virtualized desktops work just like regular laptop computers, and are managed by the end-user, IT tools, and IT personnel as regular laptops also. But unlike a dedicated laptop, the vKey Device is carried in a pocket, can be managed online, and can be wiped remotely if stolen, then replaced in less than 15 minutes for as little as $50.

Asset Life Extension

Most laptop and desktop PC assets must be replaced after 4 years due to advancing OS compatibility requirements. vKey Devices use the extremely hardware-efficient vKey OS. By providing an optimized hardware interface, vKey Devices can deliver vastly improved performance of newer operating systems on aging computer hardware. Asset life can be extended by up to 4 years while also providing instantly, trusted, cloud or virtual access and/or portable desktop virtualization.

Asset Cost Transfer

Many organizations must provide computers to third-party contractors to access their network and infrastructure. Organizations with vKey can transfer the computer asset and management costs to the third-party. By providing access to the organization's standard desktop with a vKey Device, the third-party can bring their own computer and turn it fully into in an organizational computer, simply by booting from the vKey Device. Should a third-party fail to return the device, the vKey Device can simply be remotely disabled or wiped.

Development Testing

vKey Enterprise and Professional devices run virtualized computer images. Developers can replace physical computers with virtual images. One vKey Device can run multiple virtual computer images concurrently.

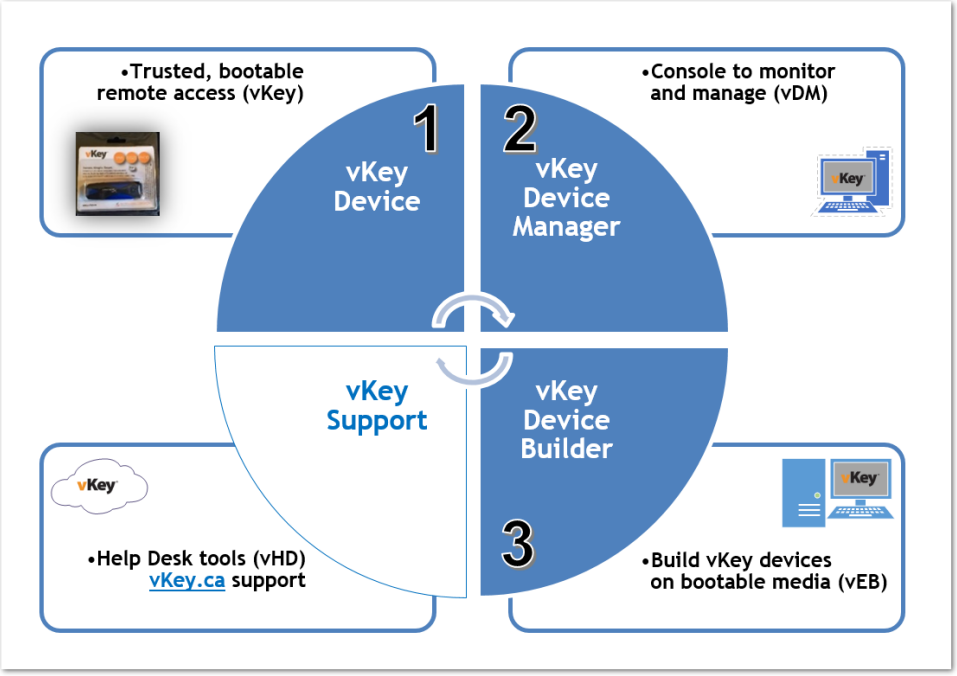
Software Migration Remediation

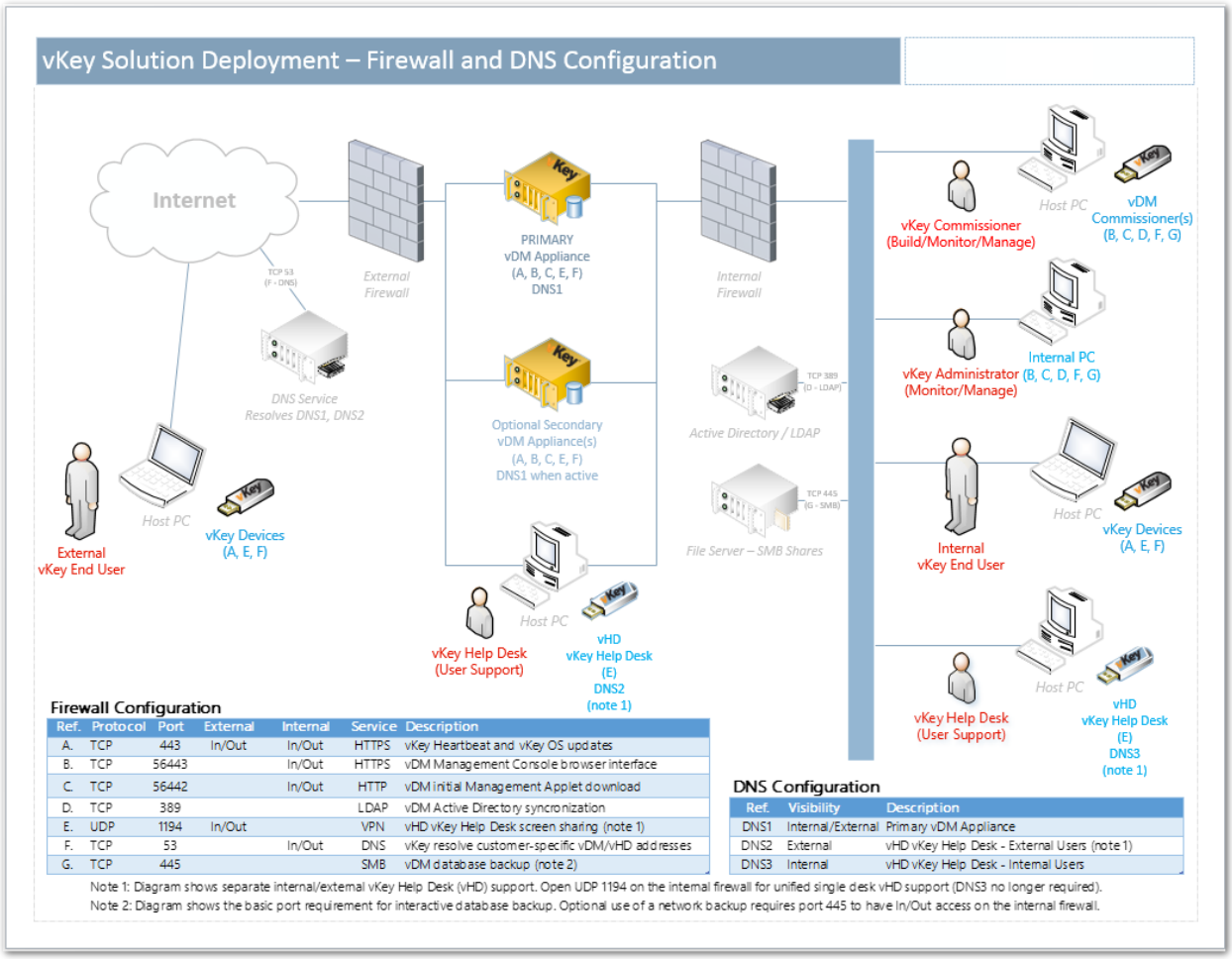
Many organizations found the migration to Windows 7 from XP to be problematic for some XP applications which could not be migrated. vKey Devices have been used to provide Windows 7, 8, and 8.1 functionality for users with no upgrade path XP applications. The Windows XP host machine is used without network access for the problem application, then rebooted with the vKey Device to provide full access to the organization's standard Windows 7, 8, or 8.1 desktop.

Business Continuity

The likelihood of experiencing a disaster is unknown, while the expense of business continuity infrastructure is fixed up front. vKey changes the game by allowing organizations to freely distribute network access and desktop functionality in the form of encrypted virtual laptop computers i.e. vKey Devices. Business continuity actors are given a vKey Device (virtual laptop) to carry or store in a pocket, or on a micro-SD card in their BlackBerry (or similar smart phone). In the case of an event, the user boots the computer from their vKey Device or micro-SD equipped BlackBerry to gain immediate access to the organization's infrastructure or desktop. When sensitivity of the virtual laptop's content or capabilities is paramount, the device password can be withheld until an event takes place, whereupon the password would be shared by phone, text or other means.

The vKey Solution





Firewall Configuration

Ref.	Protocol	Port	External	Internal	Service	Description
A.	TCP	443	In/Out	In/Out	HTTPS	vKey Heartbeat and vKey OS updates
B.	TCP	56443		In/Out	HTTPS	vDM Management Console browser interface
C.	TCP	56442		In/Out	HTTP	vDM initial Management Applet download
D.	TCP	389			LDAP	vDM Active Directory syncronization
E.	UDP	1194	In/Out		VPN	vHD vKey Help Desk screen sharing (note 1)
F.	TCP	53		In/Out	DNS	vKey resolve customer-specific vDM/vHD addresses
G.	TCP	445			SMB	vDM database backup (note 2)

DNS Configuration

Ref.	Visibility	Description
DNS1	Internal/External	Primary vDM Appliance
DNS2	External	vHD vKey Help Desk - External Users (note 1)
DNS3	Internal	vHD vKey Help Desk - Internal Users

Note 1: Diagram shows separate internal/external vKey Help Desk (vHD) support. Open UDP 1194 on the internal firewall for unified single desk vHD support (DNS3 no longer required).
Note 2: Diagram shows the basic port requirement for interactive database backup. Optional use of a network backup requires port 445 to have In/Out access on the internal firewall.

vKey Technology Insights

Device Operating System Management

The system manager in the vKey OS is responsible for starting and shutting down services. User tasks have tightly limited security privileges to protect system security integrity. The Linux systemd system management suite is used by vKey to centralize operating system configuration.

The system manager also provides the following:

- Parallelization capabilities.
- Socket and D-Bus utilization for services initialization.
- On-demand starting of daemons.
- Tracking of processes using Linux cgroups.
- Supports restoration of system state.
- Implementation of transactional, dependency-related, service control logic.

Desktop Environment

In any modern desktop workstation, the primary graphical interface is the desktop.

The vKey OS uses GNOME 3 as a desktop environment (DE), which provides a modern desktop through a sleek, intuitive design that encourages productivity through features like window snapping and a non-intrusive notification system.

Optimized for Virtualization

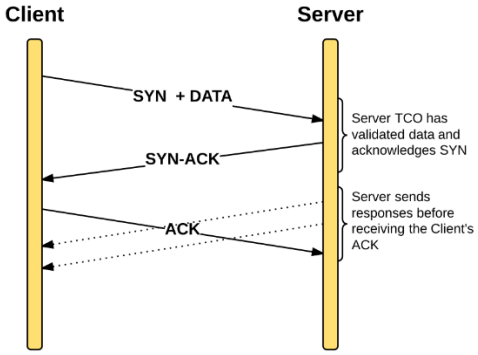
The vKey OS uses XFS as file system, which is a high-performance 64-bit journaling file system that handles large files exceptionally well. Virtual machine containers are a good example of large files that benefit from this.

The vKey processes minutes over hours to reduce frequency error, which useful to virtual machines that have drifting clocks.

Virtualized Windows desktops have been seen to operate more quickly on vKey Devices than in native Windows desktop on the same host PC device.

TCP Enhancements

TCP performance is a key feature of internet and intranet performance in all modern networks. The vKey OS has implemented a number of the most recent TCP protocol improvements including implementation of the fast-open extension for TCP, which is designed to reduce the overhead when establishing a TCP connection.



Utilization of the Tail Loss Probe (TLP) algorithm, as this improves the efficiency of how TCP handles lost packets through a transmission.

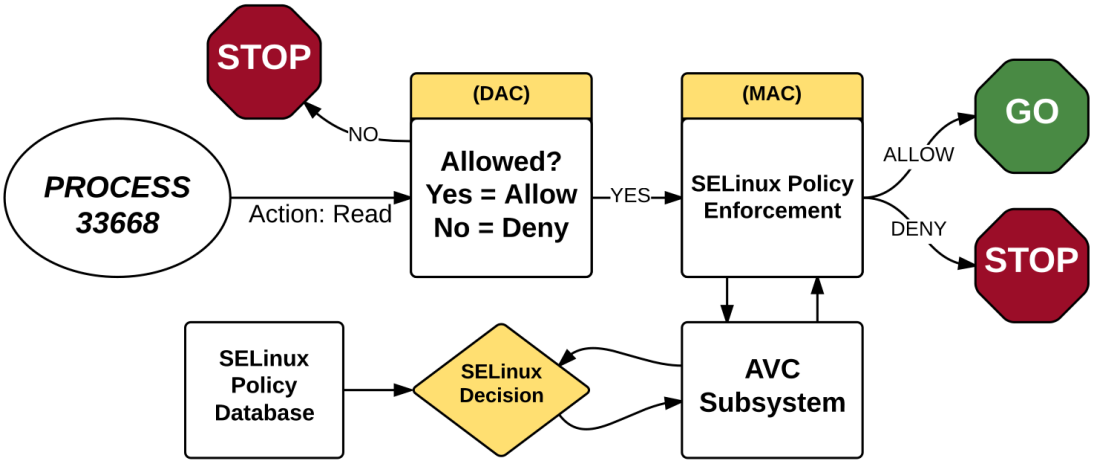
Early retransmission allows the protocol to recover lost segments and reduce overall timeout latency.

Hardened Permissions and Controls

The vKey OS employs two methods to harden permission security in the user environment. First, end-users are logging under the class of 'limited user'. The user is not allowed to execute software requiring root privileges. In contrast to many operating systems, where some processes in the user-space require elevated privileges, the vKey OS uses Discretionary Access Control (DAC) and Mandatory Access Control (MAC) to provide a hardened system with granular policies down to the process access level.

Security-Enhanced Linux (SELinux) is an implementation of the MAC mechanism in the Linux kernel, where ongoing checking and comparing of interactions against a policy database continues even after the traditional DAC has been passed. This model provides the following benefits to the vKey OS:

- Reduced vulnerability to privilege escalation attacks.
- Processes run in domains, which are separated from each other. SELinux policy rules further define how processes may access both files and other processes, such that if a process is compromised, the attacker retains only the limited access to the limited functionality and file sets of the compromised process.



Example: In the figure above, process ID 33668 is requesting to read a file on the system. The Linux kernel's discretionary access control (DAC) will determine if the user has the privilege, if not, it will fail. After passing DAC, it will be processed by SELinux's mandatory access control (MAC) to determine if it there is policy context that supports PID 33668's action. When the AVC subsystem returns a security context that matches the action, it will log the event.