Desktop as a Service with VMware and Symantec
Introduction

CIOs are under increasing pressure to reduce desktop and application management costs while providing seamless and secure access to corporate resources across an array of user devices. They also realize that increased regulatory requirements coupled with a rising trend of sophisticated security threats demand new approaches to desktop delivery and management.

This white paper, presented by Symantec™ and VMware®, outlines desktop and application management challenges and ways to address them through a secure, scalable, hosted virtual desktop solution: desktop as a service (DaaS). This paper explains how service providers can deliver a truly differentiated hosted virtual desktop experience through a combination of Symantec and VMware technologies and best practices. It also discusses what drives adoption of DaaS, describes its key elements, and explains how it benefits both IT and end users.

Figure 1. The VMware and Symantec DaaS Stack
Drivers, Challenges and Opportunities

Because of its availability, scalability and usage elasticity, cloud computing is being embraced by organizations of all sizes. Today, business and infrastructure applications such as CRM, email, collaboration, storage and backup are delivered as cloud services. New applications are moving to the cloud every day. But even with this trend toward the cloud, many of today’s business applications will run on Windows-based desktops for the foreseeable future. It will likely be several years before most legacy desktop applications are transformed into cloud offerings.

However, by offering the enterprise desktop from the cloud, organizations are able to extend the advantages of cloud delivery to include legacy desktop applications. DaaS is a combination of industry-leading cloud and virtualization platforms from VMware along with security, compliance, application and desktop management from Symantec. Through DaaS, service providers can serve thousands of desktops securely to enterprise users on multiple device types. The decoupling of the desktop software from end-user computing hardware affords IT the freedom to repurpose existing desktop assets. This also makes “bring your own device” (BYOD) a reality for employees. Since the performance requirements for DaaS endpoints are minimal, the number of capable devices immediately increases—quickly expanding support for the newest phase in end-user computing, i.e. tablet computers—and becomes cheaper. Since the user persona (user profiles and data) is now centralized, upgrading the operating system is much simpler. Users can also access their desktops from any device and still have access to their persona.

In addition to the benefits of security and availability, DaaS provides many new opportunities to augment current desktop management strategies. Much like the datacenter consolidation of servers, DaaS centralizes the desktop assets, which consist of the operating system, applications and user settings. This enables IT to manage the enterprise operating system “gold baseline” as a single image for delivery, patching and troubleshooting. Similarly, IT can now centrally perform backup and recovery tasks. This drives down the total cost of ownership, from a desktop support perspective, while providing the benefits of disaster recovery and business continuity. Confidential data is now easily secured since it is confined to the corporate perimeter instead of being dispersed across far-flung endpoints.

To fully realize the benefits of DaaS, the right mix of solutions, architecture and best practices must be deployed. Centralizing desktops does not eliminate fundamental IT processes. A DaaS desktop needs to be protected, must be well-managed and made compliant with corporate policies. If not done right, security gaps, poor ROI, unacceptable user experience or inability to meet service-level agreements (SLAs) can quickly derail an organization’s DaaS initiative.
DaaS User Personas

There are three main DaaS user personas: the DaaS end user, the DaaS administrator and the DaaS service provider.

DaaS End User

The DaaS end user performs day-to-day work using a physical device to access their desktop in the cloud. This user expects a non-disruptive experience from their physical device, including multimedia capabilities, VoIP, local USB, printer device access and network performance. DaaS end users also expect to be able to access their desktops when there is no network connectivity.

VMware View™ supports all of the DaaS end-user needs—even over bandwidth as low as current 3G networks—by using advanced compression algorithms in the PCoIP protocol. View facilitates offline usage by letting users check out the entire virtual machine from the DaaS datacenter and run it locally. Users can check this offline virtual machine back in to the DaaS datacenter when they finish with their offline activities.

Users are more productive when they have the ability to make self-service requests, which also reduces the load on IT for routine requests (for example, requesting new applications). The DaaS user experience should be consistent, irrespective of the service provider or the type of DaaS deployment—public or private. There should be a common interface and experience for all aspects of DaaS user support and management. For example, some of the applications may be packaged and managed by a DaaS service provider, whereas the rest are sourced, packaged and managed directly by a DaaS administrator. All of these applications should be combined into a common application catalog that the DaaS end user can access through a self-service application portal.

DaaS Administrator

Though the specific roles might differ at each organization, the DaaS administrator is generally responsible for the desktop infrastructure and ongoing support. The DaaS administrator needs the ability to self-provision desktops and assign them to users, and needs to meter and report on application licenses and their usage, and ensure compliance with corporate directives while remediating security incidents. The DaaS administrator also expects to manage the notification of critical incidents. Overall, for DaaS to be successful, DaaS administrators should have the same level of control and flexibility in a DaaS infrastructure that they have in their onsite implementation.

DaaS Service Provider

In order to achieve the control and flexibility of the DaaS infrastructure the DaaS service provider is responsible for enabling the appropriate and agreed upon capabilities for the DaaS administrator. DaaS service providers could include hosting providers or system integrators that offer public, private or hybrid clouds today. If private DaaS is hosted for use within the enterprise, the IT department that hosts and manages the DaaS infrastructure is the DaaS service provider. The operational governance of DaaS, especially when the DaaS service provider and DaaS administrator come from separate legal entities, requires an understanding of the expectations from the DaaS administrator and what he intends to provide for the enterprise. Conversely, having agreed upon procedures and levels of support for the individual DaaS tenants will be on the DaaS service providers’ critical path in their ability to offer an effective DaaS solution in both cost and quality.
Providing DaaS Infrastructure

A DaaS offering can be in the form of a public cloud hosted by service providers or a private cloud hosted by a system integrator or the enterprise itself. Each hosting provider may also customize the offering for specific market segments, ranging from small and medium organizations to large enterprises. There are several factors that determine the type and pricing of DaaS offered—for example, SLAs, privacy, security, compliance, number and types of users, and operating-system licenses. The underlying core infrastructure, however, remains similar for the DaaS hosting provider. This core DaaS infrastructure, consisting of hardware and software, is collectively known as the virtual desktop infrastructure (VDI).

The core infrastructure of DaaS is based on VMware's leading virtual datacenter products, VMware vCenter™ and VMware vCloud™ Director. Using these two products, the hosting provider creates multiple virtual datacenters (VDCs). Each tenant is then hosted within these VDCs and protected at the VDC boundary by VMware vShield™. Individual DaaS desktop virtual machines are protected by Symantec™ Endpoint Protection and managed by Altiris™ Client Management Suite from Symantec. VMware View™ provides the central desktop connection brokering and remote display protocol. Management of the service provider virtual datacenters is performed with vCloud Director and a central VMware vCenter Server that reaches across all tenants and their respective vCenter servers in what is known as Linked Mode. This enables the management of many thousands of virtual machines from a single window while isolating privacy and performance concerns of the vCenter servers to their respective tenants.
Two core facets of DaaS are automation and self-service capability. The automation extends from initial provisioning of tenants and desktops to ongoing management tasks. All DaaS participants, including DaaS end users, DaaS administrators, and DaaS service providers, have their own self-service capabilities. Part of the initial automated provisioning of a DaaS tenant includes (in addition to vCenter Server) the View platform, which serves desktops to DaaS users in an automated fashion, and vShield, which facilitates secure DaaS tenant networking through the vCloud datacenter. Virtual networks can be managed from within their own tenants or at the vCloud datacenter level through tenant-specific vCloud Director logins.

Conceptually, centralizing user desktops is similar to consolidating datacenter servers through virtualization, but there are some significant differences. Unlike server workloads, hosted user desktops dramatically increase the resource requirements because users directly interact with the display. This has implications for storage and network performance and bandwidth, because those infrastructure resources are shared across tenants, although they are logically (and often physically) separated to prevent bottlenecks and potential security breaches from crossing tenant boundaries. A centralized desktop environment can require large amounts of storage and, although datacenter storage costs are decreasing, datacenter storage is still 10 times more expensive than local storage. Proper sizing and optimizing of storage results in significant cost savings as well as ability to meet SLAs. Symantec™ VirtualStore gives the DaaS service provider the flexibility to mix and match storage arrays from various vendors. With VirtualStore, an organization can use low-cost commodity storage for added cost savings while still retaining high levels of performance and reliability.

Hosted desktops also create unique spikes in resource consumption at specific times—for example, “logon storms” that occur when large portions of the DaaS user population initiate their desktops at the beginning of the work day or upon return from the lunch hour. If not managed carefully, even common desktop activities such as virus updates and scanning, inventory and patching can result in unexpected usage spikes. The capabilities of the display protocol, PCoIP by Teradici, play an important role in ensuring acceptable quality of service (QoS) for delivery of the desktop to the endpoint. PCoIP offers 23 counters for the monitoring of sessions, networking, USB and imaging. Once in place and operational, data such as the PCoIP performance counters can be captured with VMware vCenter Operations. Monitoring key metrics drives SLA events for VDI capacity as well as ongoing predictive analysis of cyber threats and remediation of those events. vCenter Operations also performs automated monitoring of the DaaS infrastructure configuration, while automated monitoring of the DaaS desktop configuration is done by Symantec’s Client Management Suite and Symantec™ Control Compliance Suite. This monitoring enforces policy-driven configuration, ensures regulatory compliance and raises alerts when configuration items fall out of compliance.
In today's world of escalating hacker attacks and data breaches, strong security is key to the success of any DaaS deployment. Security considerations should be an integral part of the DaaS design and deployment process. Security policies should be robust and span all aspects of the DaaS infrastructure from the virtual datacenter level and individual tenant boundaries including, network transmissions and devices to individual virtual machines and their combined perimeters. Confidential data should always be encrypted wherever possible, at the datacenter or on user devices. Symantec’s whole disk and folder encryption solutions provide a rich set of policies to protect sensitive data. Organizations should deploy data loss prevention solutions to prevent data breaches on both the network and user devices. The PCoIP protocol used by VMware View secures network transmissions by delivering data in an encrypted tunnel, protecting it from network snooping and similar activities. Symantec™ Network Access Control (SNAC) validates user access to a device before it is allowed to connect to the DaaS virtual machine: SNAC can verify that the accessed device is free of malware, that the security software is running and updated, and that the operating system is at an appropriate patch level. Strong, multifactor authentication for user login should be deployed for an additional layer of security. Solutions from Symantec (Verisign Identity Protection) or RSA (SecurID) can be used for strong authentication.

**DaaS Administration**

The combination of VMware and Symantec tools provides powerful management capabilities for enterprise desktops and applications, as well as a context-appropriate service and support model. From the DaaS administrator’s perspective, these tools and their usage are the same as those used by many enterprises to manage endpoints and virtual infrastructures today. This eases transition to the DaaS model, because there are no new tools or processes to learn or implement. Once the DaaS tenant infrastructure is configured, authorized DaaS end users can begin to use their secure desktop from the cloud.

The initial configuration of the DaaS tenant infrastructure includes VMware vShield Edge, which provides an IPsec VPN that securely connects the DaaS tenant network and the enterprise network. This secure connectivity is needed for accessing enterprise resources from DaaS desktops and includes a replicated (or trusted) Active Directory domain controller that authenticates and authorizes DaaS desktop usage. Also included is DaaS desktop policy management for security and compliance, as well as tools for creating and maintaining desktop operating system templates. VMware ThinApp™ or Symantec™ Workspace Streaming can be used for packaging and deploying centrally managed virtual applications. These solutions enable applications to be streamed from a single, central repository. Symantec’s Client Management Suite offers a central software catalog that is used for aggregating application metadata such as version, vendor, licensing, and support information and renewals. A per-tenant service desk is used to build approval and support workflows. These application management, service desk and workflow solutions are a perfect example of the synergies between VMware and Symantec tools. For example, VMware Service Manager provides a robust, highly configurable Configuration Management Database (CMDB) and IT Infrastructure Library (ITIL)-based management processes for all tenants from a single instance, whereas Symantec™ Service Desk is quickly configured per tenant instance to fulfill DaaS user requests for troubleshooting or adding functionality.

Symantec™ Endpoint Protection (SEP) monitors and protects the guest virtual machines. By leveraging an advanced global insight database and intrusion-detection capabilities SEP provides protection from zero-day threats, automatically remediates malware and can also quarantine the guest virtual machine when necessary. SEP is optimized for virtual environments through a combination of intelligent caching and elimination of redundant scans, enabling SEP to eliminate I/O operations by up to 90 percent. Not only does this greatly improve the DaaS user experience, but it also minimizes the load on the storage system.
The Symantec and VMware solutions provide various tools for the DaaS service provider and administrator to monitor and meet SLAs and QoS requirements. Symantec Endpoint Protection and Client Management Suite include advanced data analytics that provide actionable data on various key performance indicators ranging from security trends to license usage and system resources. With these same methods the DaaS service provider can offer additional value-added services, such as a catalog of cloud-ready applications, for example replacing legacy email with VMware Zimbra®. DaaS service providers can also add value by offering DaaS solutions specific to vertical markets such as health care, manufacturing, retail, finance and government. These same tools also give DaaS service providers the flexibility to offer a variety of service levels that differentiate their offerings and price points.

Conclusion
DaaS puts end users in control in ways they aren’t likely to experience today—for example, the ability to use a device of their choice and the convenience of instant, “anytime” access to their applications and data. At a time when IT budgets are severely constrained, DaaS provides a unique opportunity for organizations of all sizes to move to the cloud with minimal capital costs. It affords IT the flexibility to manage the desktop on a pay-as-you-go model, while keeping the desktop fully secured, managed and compliant. Service providers and system integrators have an opportunity to offer their own differentiated solutions based on proven market-leading solutions from the leaders in virtualization, security, and endpoint management.
Glossary

**Altiris™ Client Management Suite from Symantec** – A systems management solution that provides integrated lifecycle and configuration management for both physical and virtual environments. With a modular approach, Client Management Suite automates time-consuming and redundant tasks to minimize efforts and costs associated with deploying, patching, supporting client systems and software.

**Desktop as a service (DaaS)** – The outsourcing of a hosted Virtual Desktop Infrastructure (VDI) and the agreed-upon services and service levels that constitute the offering. DaaS includes self-service and automation capabilities as well as an approval workflow system to facilitate on-demand additions to services offered and billed.

**PCoIP** – Teradici-patented protocol used by VMware View to compress, encrypt and encode the entire computing experience at the datacenter and transmit it as “pixels only” across any standard IP network to stateless PCoIP zero clients.

**Symantec™ Endpoint Protection (SEP)** – A complete endpoint security solution that provides state-of-the-art defense against all types of attacks for both physical and virtual systems. SEP is powered by Insight, a global cloud-based reputation technology.

**Symantec™ Network Access Control (SNAC)** – A network security solution that controls access to corporate networks. Network Access Control discovers and evaluates endpoint compliance status, provisions the appropriate network access and provides automated remediation capabilities.

**Symantec™ PGP** – An encryption solution that enables organizations to deliver comprehensive data protection with standards-based technology, centralized policy management, accurate compliance-based reporting and true universal management of encryption solutions.

**Symantec™ User Authentication solutions** – Former VeriSign solutions that provide convenient, secure fraud detection, two-factor authentication, and public key infrastructure (PKI) services for protecting online identities and interactions between consumers, business partners and employees.

**Symantec™ Workspace Streaming** – An application delivery solution that enables on-demand application provisioning, offline cache, license recovery and instant application upgrades.

**Symantec™ VirtualStore** – A scale-out NAS solution that addresses the storage challenges of desktop virtualization. Integrated with vCenter, VirtualStore is built on top of commodity servers and storage hardware to provide space-optimized virtual machine provisioning for desktop virtualization environments.

**Thin client** – A computer that depends heavily on some other computer (its server) to fulfill its traditional computational roles. In DaaS a thin client automatically boots its own operating system (Linux available) and load connectivity to the DaaS desktop in the cloud.

**Virtual Desktop Infrastructure (VDI)** – The combination of the hardware (compute, network and storage) and software used to serve virtual desktops from a virtual infrastructure.
**VMware Service Manager** – A 100 percent Web-architected solution that automates IT service management processes in enterprise organizations and is independently verified to the highest level of ITIL compatibility for incident management, problem management, change management, release management, configuration management, service-level management and availability management.

**VMware vCenter™** – Software that provides unified management of all the hosts and virtual machines in your datacenter from a single console with an aggregate performance monitoring of clusters, hosts and virtual machines.

**VMware vCenter (Linked Mode)** – Software that provides a scalable architecture and visibility across multiple vCenter Server instances, with roles, permissions and licenses replicated across the infrastructure so that you can simultaneously log in, view and search the inventories of all vCenter servers.

**VMware vCenter Operations** – A solution that provides proactive administrative monitoring of service levels, optimum resource usage and configuration compliance in dynamic virtual and cloud environments.

**VMware vCloud™ Director** – Software that enables customers to build secure, multitenant hybrid clouds by pooling infrastructure resources into virtual datacenters and enabling those resources to be consumed by users on demand.

**VMware vShield™** – Adaptive and cost-effective security services within a single management framework for securing virtual datacenters and cloud environments at all levels—host, network, application, data and endpoint.

**VMware vSphere™** – A cloud operating system for building shared virtual resources from physical resources. The shared resources perform as dynamic virtual clusters with high availability and business continuity solutions.

**VMware ThinApp™** – Software that packages applications into single executables that are completely isolated from each other and the underlying operating system for conflict-free execution on endpoint devices.

**VMware View™** – Software that modernizes desktops and applications by moving them to the cloud and delivering them as a managed service. View transforms traditional stationary desktops into untethered stateless workspaces available from anywhere and at any time.

**Zero client** – A compact access device that connects a monitor, keyboard, mouse, speakers and USB peripherals to a user’s DaaS desktop. Zero clients have no operating system or disk of their own and initiate connections through firmware.
About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.
Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1 (800) 721 3934
www.symantec.com