LEARNING MADE EASY

VMware® Special Edition

Modern and Secure Hybrid Cloud Platform

for dummies®
A Wiley Brand

Secure apps and infrastructure

Run all apps on one platform

Build a true hybrid cloud

Brought to you by

vmware®

Himanshu Singh

About VMware, Inc.

VMware, a global leader in cloud infrastructure and business mobility, accelerates the digital transformation journey by enabling enterprises to master a software-defined approach to business and IT. With VMware solutions, organizations are improving business agility by modernizing data centers, driving innovation with modern data and apps, creating exceptional experiences by mobilizing everything, and safeguarding customer trust with a defense-in-depth approach to cyber-security. VMware is a member of the Dell Technologies family of businesses.

Modern and Secure Hybrid Cloud Platform

VMware Special Edition

by Himanshu Singh

for dummies®
A Wiley Brand

Modern and Secure Hybrid Cloud Platform For Dummies®, VMware Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

ISBN 978-1-119-61170-7 (pbk); ISBN 978-1-119-61169-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor: Rebecca Senninger

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Siddique Shaik

Introduction

Why do you need a modern and secure hybrid cloud platform? Basically, because the world is changing before our eyes. Digital transformation is sweeping across all industries, and you need the right technology to capitalize on this wave and stay competitive.

To compete in the new digital economy, your business needs a modern data center that is highly scalable, available, and secure. A modern data center enables your organization to move quickly and confidently into the new digitally driven world and adopt the hybrid cloud. I'm talking about a data center that gives you the ability to not only run apps in a reliable and secure manner, but also to connect apps across clouds and devices while maintaining rock-solid security.

You can't make this leap forward with yesterday's approaches to IT infrastructure. You need a modernized data center that is fully virtualized, software defined, intrinsically secure, and highly automated, with a consistent approach to infrastructure, application, and security delivery across a hybrid cloud environment.

In the age of the digital economy, this sort of modernized data center is no longer a nice-to-have. It's a must-have. It's a strategic priority.

About This Book

This book is your guide to a modernized, more secure hybrid cloud platform. So, how do you get there? The first step is to get intimately acquainted with the concepts explored in this book. In the pages that follow, I provide tips, insights, and advice for building a modern and secure hybrid cloud platform to drive your digital transformation forward and create a clear route to the next-gen hybrid cloud.

Don't let the small size fool you. This book is loaded with information that can help you understand and capitalize on virtualization technologies to build your modern and secure hybrid cloud platform. In plain and simple language, the book explains the inner workings of a next-generation platform, why you need it, and what capabilities to look for.

Icons Used in This Book

To make it even easier to navigate to the most useful information, these icons highlight key text:

EXAMPLE

Enrich your understanding with these real-life examples.

REMEMBER

Take careful note of these key takeaway points.

TIP

These tips can save you time and effort.

TECHNICAL STUFF

Read these optional passages if you crave a more technical explanation.

Where to Go from Here

I wrote this book as a reference guide, so you can read it from cover to cover or jump straight to the topics you're most interested in. Whichever way you choose, you can't go wrong. Both paths lead to the same outcome — a better understanding of the characteristics of a modern, secure hybrid cloud platform and the steps and best practice to consider as you move forward.

For more information on the characteristics of a modern and secure hybrid cloud platform, head to `vmware.com/products/vsphere`.

IN THIS CHAPTER

- » Highlighting data center security issues
- » Calling out key challenges for IT
- » Pointing to the path forward

Chapter 1 The Case for a New, More Secure Approach to the Data Center

To compete and succeed in the digital economy, all businesses require a modern data center built around a highly secure hybrid cloud platform. It's the key to supporting a dynamic, digitally driven business that can ward off rapidly evolving security threats.

This chapter highlights the scope of today's hybrid cloud security challenges and the need for a modern and secure hybrid cloud platform that creates the foundation for digital business transformation.

Understanding the Big Picture

With the adoption of digital transformation, today's enterprises are leaning more on digital assets, digital identities, and digital channels to drive revenues. This new reality makes comprehensive security across infrastructure and applications of paramount importance. To protect the business, IT teams need to protect digital assets from ever-more-sophisticated security threats.

Those threats are rising in terms of number and severity, and they can be devastating to a business. Research from the University of Maryland's Clark School reveals that a hacker strikes every 39 seconds and the cost of breaches is rising. According to the Ponemon Institute, the average financial loss from a cyber-attack, now estimated at $3.6 million, is up 62 percent in the last five years, largely due to the number of days intrusions take to resolve. And for many companies, this number can be drastically higher, reaching hundreds of millions of dollars in losses stemming from decreased revenues, remediation costs, the impact of regulatory infractions, and a decline in customer trust.

In addition to managing the financial downside of breaches, businesses must invest time and funds to reassure customers that their data is secure. With threats continuing to increase in number and severity globally, the onus is on organizations to ensure comprehensive protection across their IT infrastructure and applications.

In this new era of ever-more sophisticated cyber-security threats, comprehensive built-in security across infrastructure and applications is essential.

Addressing New Hybrid Cloud Challenges

As security threats increase in number and scope, traditional security models and antivirus products can be both ineffective and inefficient. They can protect only against known threats and pre-identified virus signatures, leaving your applications vulnerable against new threats and attack vectors. Moreover, they can consume a significant amount of system resources while failing to stop attacks. And by the time an attack is detected, it's often too late to stop the damage.

We need to do better. Security now must be enabled at the foundation of the IT architecture and across the entire hybrid environment, not just in select components or layers. IT organizations now need to comprehensively secure applications, data, infrastructure, and access. And security needs to be easy to operationalize in a seamless and transparent manner.

Looking at the Path Forward

So, how do you get to where you need to be? The path forward begins with a comprehensive modern and secure hybrid cloud platform that increases IT agility and creates a seamless foundation for the management of private and public cloud services alongside traditional data center infrastructure.

You can find more detailed information about the characteristics of a fully featured, modern and secure hybrid cloud platform in Chapter 2. For now, keep this thought in mind: In its work to drive the digital transformation, your IT organization is taking on a leadership role — and positioning the business for success in the digital economy.

REMEMBER

To stay competitive and protect the business, all enterprises need to get on the path to a modern and secure hybrid cloud platform that spans from the traditional data center to private and public clouds.

IN THIS CHAPTER

- **Building security into your IT environment**
- **Enabling efficient management at scale**
- **Leveraging a universal application platform**
- **Supporting hybrid cloud**

Chapter 2 Modernizing and Securing the Hybrid Cloud Environment

In this chapter, you start with the basics. A software-defined data center (SDDC) model changes the ground rules for IT operations by virtualizing compute, networking, and storage, with integrated management. Organizations that implement an SDDC model create a digital foundation that provides the ultimate flexibility in how and where workloads run — which is one of the keys to accelerating digital transformation.

At the same time, the SDDC provides an opportunity to create a zero-trust security model with comprehensive application visibility and consistent security controls across clouds. This model fully protects existing and new workloads in ways never before possible.

A modern and secure hybrid cloud platform enables this comprehensive approach to the SDDC with built-in security. In particular, a fully featured next-gen platform delivers on four key requirements for the modern, hybrid IT environment:

- Provide comprehensive built-in security.
- Enable simple, efficient management at scale.

- Deliver a universal application platform.
- Enable a seamless hybrid cloud experience.

Providing Comprehensive Built-In Security

In a time when security threats are increasing and attacks are coming from all directions, security has emerged as a top IT and business priority. Security must now be enabled at the foundation of the IT architecture and across the entire environment, not just in one component or layer. IT professionals need to comprehensively secure applications, data, infrastructure, and access. This security needs to be easy to operationalize in a seamless and transparent manner.

In this new era, your next-gen data center security platform should offer comprehensive security that starts at the core, reaches to the network edge, and encompasses the hybrid cloud. Your platform should secure applications, data, infrastructure, and access at scale via an operationally simple, policy-driven model. Protecting all four of these areas is essential for digital transformation and the evolution of your business.

To enable this comprehensive approach to security, your next-gen platform should allow you to:

- Use VM-level encryption to protect against unauthorized data access. Your platform should also include capabilities to safeguard data at-rest and data in-motion.
- Secure infrastructure via a secure boot model that protects both the hypervisor and the guest operating system. This approach helps prevent images from being tampered with and wards off the loading of unauthorized components.
- Leverage enhanced audit-quality logging capabilities that provide more forensic information about user actions. With these capabilities, your IT team can better understand who did what, when, and where if an investigation into anomalies or security threats requires this understanding.

- Defend applications in virtualized environments by watching for and responding to changes to the state of the application that indicate threats.

Ultimately, the goal is to provide a complete security model for the infrastructure in your software-defined data center.

Enabling Simple, Efficient Management at Scale

More than ever before, we have complex applications coming online. This complexity effectively increases the frequency of infrastructure security patches and the amount of IT admin time spent on constant software updates. A modern and secure hybrid cloud platform should help you handle these challenges with capabilities for simple and efficient management at scale.

This management at scale is enabled by a virtual server appliance that reduces operational complexity by embedding key functionality into a single location. This virtual appliance should include capabilities such as one-click patching, backup and recovery, native high availability, and much more. With this virtual appliance in place, your IT team should no longer need to interface with multiple components to get lot of things done.

Delivering a Universal Application Platform

In a modern and secure hybrid cloud, IT must support next-generation, cloud-native apps alongside traditional business-critical apps. This is easier said than done. Next-gen apps often have substantially different characteristics from legacy applications, and they are often built with new and evolving technologies, like containers (for example, Kubernetes) or specialized hardware, such as GPUs, persistent memory, and non-volatile memory.

These new next-gen applications include workloads like artificial intelligence, machine learning, and big data, which are increasingly being deployed in all types of businesses. This increasing diversity of applications, workloads, and use cases puts additional demands on IT infrastructure. To meet these demands, infrastructure must evolve — now, not years from now.

These challenges are best met with a universal application platform that is built to run any application, onsite or in a hybrid cloud. A universal application platform supports your existing mission-critical applications as well as new workloads, from 3D graphics, big data, and high-performance computing to machine learning, in-memory, and cloud-native. This platform also supports and leverages the latest and greatest hardware innovations, including graphics processing units (GPUs), to help your IT team deliver exceptional performance for your new and emerging workloads.

Enabling a Seamless Hybrid Cloud Experience

The increasing adoption of hybrid clouds creates the need to connect applications and migrate workloads from on-premises systems to the cloud and back. In this new, very cloudy era, your IT team needs a stable on-premises platform along with the ability to quickly adopt new capabilities in the public cloud. And across the hybrid environment, you need comprehensive visibility and ease of management for your resources, whether they are on-premises or in a public cloud.

Your next-gen data center modernization and security platform should arm you with the capabilities you need to support and secure this true hybrid cloud experience in a seamless manner.

EXAMPLE

For example, a next-gen data center platform should support cross-cloud hot and cold migration, to enable a seamless and non-disruptive hybrid cloud experience for users.

In Chapter 3, I dive into the specific capabilities in the VMware vSphere environment that enable a modern and secure hybrid cloud platform.

IN THIS CHAPTER

- **Securing applications**
- **Securing infrastructure**
- **Securing data**
- **Securing access**

Chapter 3 Essential Capabilities for Next-Gen Security

A next-gen data center virtualization and security platform incorporates advanced capabilities for securing applications, infrastructure, data, and access. In a VMware environment, these capabilities are delivered via the vSphere Platinum platform.

Understanding vSphere Platinum

VMware vSphere Platinum is a new edition of vSphere that delivers advanced security capabilities fully integrated into the hypervisor. This purpose-built virtualization and security solution is designed to protect enterprise applications, infrastructure, data, and access.

VMware vSphere Platinum combines two proven products:

- **VMware vSphere:** The industry-leading, efficient, and secure hybrid cloud platform for all workloads
- **VMware AppDefense:** Data center endpoint security powered by machine learning and embedding threat detection and response into the virtualization layer, to reduce security risk

While being operationally simple, vSphere Platinum helps your organization ensure that your applications and virtual machines are running in their known-good states, with minimal overhead and performance impact.

The rest of this chapter takes a closer look at how vSphere Platinum helps your team secure applications, infrastructure, data, and access.

Securing Applications with Purpose-Built VMs

Innovative organizations use vSphere Platinum to safeguard their hybrid cloud environments powering digital transformation. They address in-guest threats by protecting the integrity of applications running on vSphere with AppDefense.

Instead of chasing threats, AppDefense enables enterprises to:

- Understand an application's intended state and behavior, or what it's supposed to do, and then monitor for changes to that intended state
- Respond fast to any change from the known-good state, indicating a threat
- Ensure that all VMs and applications run in known-good states, removing the burden of detecting threats that may not fit a known signature

AppDefense locks down the guest operating system for all applications, the VMware application stack, and third-party applications. It gathers inventory data on VMs and applications from the VMware centralized management application, development tools, and automation frameworks. Machine learning algorithms are applied to discover the intended state, establish the known-good behaviors for the application and VM, detect anomalies, and prevent further deviation. These capabilities help you ensure the integrity of your applications, infrastructure, and guest OS.

AppDefense also provides a rich set of automated or orchestrated incident response mechanisms to address attacks. Detailed visibility improves change management and compliance reporting processes while machine learning simplifies and automates auditing and application reviews.

Securing Data with Encryption

Enterprise stores of valuable personally identifiable information (PII) and intellectual property (IP) entice attackers seeking to wreak havoc and enjoy ransomware paydays. vSphere Platinum protects against unauthorized data access, both when data is in-motion and at-rest, across the hybrid cloud.

TECHNICAL STUFF

vSphere Platinum features FIPS 140-2 Validated VM encryption and encrypted vMotion to enable the live migration of running VMs from one physical server to another with zero downtime. These capabilities help ensure continuous service availability and complete transaction integrity.

Securing Infrastructure through Validation and Attestation

vSphere Platinum delivers comprehensive built-in security at the foundation of a secure SDDC. Its features and capabilities include Secure Boot for ESXi, which ensures that only VMware and partner-signed code is running in the hypervisor, and Secure Boot for Virtual Machines, which helps to prevent image tampering and unauthorized component loading.

TECHNICAL STUFF

The dictionary defines attestation as the evidence or the act of showing that something is true. For vSphere Platinum, attestation is the act of proving that your computer's firmware, ESXi boot loader, VMKernel, and core ESXi processes have not been tampered with by bad actors, and are installed exactly as they were built and delivered by VMware. With support for TPM 2.0 for ESXi, vSphere Platinum enables hypervisor integrity by validating the Secure Boot for ESXi process and enabling remote host attestation.

In vSphere Platinum, Virtual TPM 2.0 provides the necessary support for guest OS security features while being operationally simple. vSphere Platinum also supports Microsoft Virtualization-based

Security (VBS) for enterprises running Windows 10 and Windows Server 2016 security features, such as Windows Defender Credential Guard, on vSphere.

Securing Access with Greater Visibility

Audit quality logging in vSphere Platinum helps ensure authorized administration and control by providing high-fidelity visibility to user activity. vSphere Platinum maximizes the efficiency and effectiveness of virtualization and security operations while streamlining the application security readiness review process. It enables a simple and powerful way to maintain existing workflows while continuously monitoring for threats.

Enabling Collaboration across the Data Center

vSphere Platinum fosters unprecedented collaboration among vSphere administrators and security, compliance, and application teams. vSphere Platinum empowers your vSphere administrators to help shrink the attack surface and reduce the risk of security compromise in the enterprise. It provides your IT administrators with visibility into the intent of VMs and a detailed inventory of apps while increasing their understanding of application behaviors and providing alerts about potential issues and deviations.

Administrators using vSphere Platinum gain the benefits of a simple, lightweight, and scalable security solution with better protection — without agents to manage and with minimal overhead and performance impact. vSphere Platinum makes it easy to leverage existing technology and knowledge of what is already running in the data center with the hypervisor's unique visibility, automation, and isolation qualities to improve security across the enterprise.

At the same time, your security, compliance, and application teams using vSphere Platinum can better support IT security and compliance efforts. They improve visibility into application behaviors and VM purpose while more quickly detecting, analyzing, and responding to threats. Behavioral analytics and machine learning in vSphere Platinum increase the accuracy of threat detection while big data correlation improves identification and context in a cloud SaaS model. Your security, compliance, and application teams working in conjunction with your vSphere administrators using vSphere Platinum deliver greater protection while increasing business agility.

TIP

Thanks to deep integrations, vSphere Platinum works seamlessly with other VMware solutions, including VMware vSAN, VMware NSX, and VMware vRealize Suite. The result is a complete security model for your data center and extension to hybrid cloud.

A platform with these essential capabilities for next-gen security enables a rich set of benefits for IT administrators and security teams — which I explore in Chapter 4.

IN THIS CHAPTER

- » **Highlighting benefits for IT administrators**
- » **Highlighting benefits for security teams**
- » **Enabling a single view of the truth**

Chapter 4 Realizing the Benefits of a Modern and Secure Hybrid Cloud Platform

A comprehensive approach to managing and securing applications, data, infrastructure, and access helps your IT and security teams conquer today's complex challenges across your hybrid cloud, including new and emerging security threats.

In this chapter, I discuss the benefits for your IT administrators, security teams, and the broader range of your organization.

Benefits for IT Administrators

For your IT administrators, vSphere Platinum, being a modern and secure hybrid cloud platform, changes the ground rules for managing a hybrid IT environment.

For starters, the vSphere Platinum platform gives your IT administrators visibility into the intent of each virtual machine, and a detailed inventory of application assets and context. This view helps your administrators understand how your different applications behave — and know when they aren't acting right. When application issues arise, the platform alerts your admins to potential issues and deviations.

To dig a little deeper, this modern and secure hybrid cloud platform enhances security across your data centers. With the capabilities I cover in Chapter 3, vSphere Platinum shrinks potential attack surfaces and reduces the risk of security compromise. For example, this full-featured cloud platform embeds threat detection and response capabilities into the virtualization layer, while using machine learning to ensure that virtual machines and applications are running in a known-good state.

Want to make your day-to-day life easier? This modern cloud platform establishes a simple and powerful way to enable collaboration among your security, compliance, and application teams. The platform provides a shared view that gives everyone better visibility into application behaviors and the purpose of VMs while helping people more quickly detect, analyze, and respond to threats. Behavioral analytics and machine learning capabilities increase the accuracy of threat detection, while big data correlation improves identification and context in a cloud SaaS model.

Okay, now you can make life ever easier for your IT team. vSphere Platinum enables better visibility and protection with a simple, lightweight, and scalable security solution — with no agents to manage and with minimal overhead and performance impact. If you're a vSphere shop, you can now use a common virtualization platform that you already own, understand, and run in your data center, and upgrade to vSphere Platinum to gain all the benefits of unique visibility, automation, and isolation qualities.

While I'm talking about visibility and protection, you'll be glad to know that vSphere Health works to identify and resolve potential issues before they have an impact on your environment. Telemetry data is collected from vSphere, and then used to analyze preconditions within your environment. Discovered findings can be related to stability as well as incorrect configurations in vSphere.

When you put it all together, you've created a new playing field. Your IT administrators can now play a larger and more critical role in the security of your entire IT environment — and become security heroes!

Benefits for Security Teams

While changing the ground rules for managing your hybrid IT environment, a modern and secure hybrid cloud platform simultaneously delivers an uncommon set of benefits for your security teams.

These benefits begin with much better visibility and situational awareness of application behaviors and virtual machine purpose. Apps and VMs no longer do their thing in a black box. You now have the visibility you need, along with alerts into application communications and deviations, to enable faster detection, analysis, and time to response. You have the information and insights you need to quickly understand attacks and make fast decisions that take application context and scope into account.

In contrast to bolted-on, point security tools and reactive antivirus solutions, the vSphere Platinum hybrid cloud platform embeds security everywhere. Along the way, it enhances collaboration between your IT and virtualization administrators and your security, compliance, and application teams. This close collaboration is one of the keys to improving threat response and time to remediation.

In another important benefit for security team, this modern hybrid cloud platform can reduce false positives, so people aren't spending all their time chasing down nonexistent issues and threats. This benefit is enabled by integrated behavioral analytics and machine learning that correlate big data for better identification and context to provide a more precise method to identify and respond to threats.

Ultimately, as a modern and secure hybrid cloud platform, vSphere Platinum brings people together. Your security and compliance teams can now easily coordinate their work with that of your IT admins and application teams to enhance the security of your hybrid cloud environment — while enabling DevOps processes, respecting existing workflows, maintaining separation of duties, and increasing business agility.

Benefits for Everyone

As a next-gen hybrid cloud platform, vSphere Platinum fosters unprecedented collaboration among IT administrators and security, compliance, and application teams. IT admin teams see issues from an infrastructure perspective, security teams see issues from an app perspective, and everyone has a single view of the truth.

This unified view helps shrink the attack surface and reduce the risk of security compromise while providing visibility into the intent of VMs. It enables a detailed inventory of apps while increasing everyone's understanding of application behaviors and providing alerts about potential issues and deviations.

Ultimately, when your security, compliance, and application teams are working in close collaboration with your IT administrators, your organization is poised to deliver greater protection while increasing business agility.

All these benefits are enabled by the foundational components of a modern data center — which I cover in Chapter 5.

IN THIS CHAPTER

- » Virtualizing storage and networking
- » Managing private clouds
- » Supporting hybrid cloud environments

Chapter 5
The Fundamentals of the Modern Data Center

A comprehensive modern and secure hybrid cloud platform builds on the fundamental capabilities of the modern data center. These include storage virtualization, network virtualization, cloud management, and support for hybrid cloud environments. These are all foundational capabilities for a software-defined data center (SDDC).

Virtualizing Storage

Software-defined storage (SDS) is one of the key building blocks for hyper-converged infrastructure (HCI) and the SDDC. Software-defined storage abstracts physical storage constructs to enable flexible and precise consumption according to application requirements. This capability is made possible by the hypervisor, which acts as a broker that balances the needs of a virtual machine and the applications it runs.

HCI collapses compute, storage (including storage networking), and management onto virtualized, industry-standard hardware, enabling a building-block approach to infrastructure with scale-out capabilities. In HCI, all key data center functions run as software on the hypervisor in a tightly integrated software layer.

In an HCI environment built on SDS, where an x86 Intel-based server platform runs a hypervisor and includes virtualized storage devices, the storage software runs either in the hypervisor or in a VM. The storage components are typically a mix of solid-state drives (SSDs) or hard-disk drives (HDDs). Newer all-flash HCI solutions are built from SSDs (such as Intel SSD Data Center Series), PCIe devices, or other flash technologies.

HCI implements shared storage by pooling the storage resources distributed across multiple server nodes. You essentially end up with a storage-area network (SAN) inside an x86 server system. So, in the simplest terms, HCI extends the server virtualization technology you already know by abstracting and pooling storage attached to the x86 servers, and incorporating them as part of the virtualized environment.

In an HCI environment, compute, storage, and management resources are delivered through an x86 server platform. The server platform runs a hypervisor and pools direct-attached storage devices together from across multiple servers in the cluster to create shared storage, which acts like that provided by traditional SAN or network-attached storage (NAS) devices.

The VMware HCI offerings combines the power of vSphere with VMware vSAN, powering industry-leading solutions with vSphere-native, flash optimized storage for private and public cloud deployments.

Virtualizing Networking

In this section, I dive into the concept of network virtualization — how it works, how it differs from other approaches to the network, and why the time is right for this new approach.

Network virtualization makes it possible to programmatically create, provision, and manage networks in software, using the underlying physical network as a simple packet-forwarding backplane.

Here's how it works:

- Network and security services in software are distributed to hypervisors and "attached" to individual virtual machines, based on networking and security policies defined for each connected application.
- When a VM is moved to another host, its networking and security services move with it.
- When new VMs are created to scale an application, the necessary policies are dynamically applied to those VMs as well.

TECHNICAL STUFF

Similar to the way a virtual machine is a software container that presents logical compute services to an application, a virtual network is a software container that presents logical network services — logical switching, logical routing, logical firewalls, logical load balancing, logical VPNs, and more — to connected workloads. These network and security services are delivered in software and require only IP packet forwarding from the underlying physical network. The workloads themselves are connected via a software representation of a physical network "wire." This allows for the entire network to be created in software.

VMware NSX is designed to serve as a network virtualization and security platform for the SDDC. NSX reproduces the entire network model in software. This end-to-end model enables any network topology — from simple to complex multitier networks — to be created and provisioned in seconds.

Managing Cloud Environments

A robust cloud management platform (CMP) is a fundamental enabler of the modern data center. A fully featured CMP provides a dynamic, consistent digital foundation to deliver applications across multi-cloud environments, powering business innovation. It makes operating a private cloud and consuming private cloud resources as easy as if they were in a public cloud.

Capabilities of a complete CMP include automated life-cycle management and self-driving operations that deliver high availability and support service-level agreements (SLAs) with a minimal amount of errors. For your developers, the CMP supports multiple sandbox models for requesting services. This gives them the freedom to use the tools of their choice, increasing their productivity.

In a VMware environment, these capabilities are delivered via the vRealize Suite cloud management platform. This enterprise-ready, hybrid CMP enables your developers to quickly build applications in any cloud with secure and consistent operations. It provides developer-friendly infrastructure (supporting VMs and containers) and a common approach to hybrid and multi-cloud, supporting major public clouds, such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform.

Supporting Hybrid Cloud Infrastructure

Public clouds offer a way to gain the flexibility and speed necessary to respond to changing business needs, accelerate innovation, and align costs to business requirements. But reaping the benefits of public cloud is easier said than done. After you decide to make the move to public cloud, complexity abounds. Many companies struggle to adapt and migrate applications to run in a cloud environment.

So how do you move forward with confidence? For many organizations, the answer is VMware Cloud on AWS. VMware Cloud on AWS is an integrated cloud offering jointly developed by VMware and AWS. It is sold, delivered, managed, and supported by VMware. It delivers a highly scalable, secure, and innovative service that allows your organization to seamlessly migrate and extend your on-premises VMware vSphere-based environments to the AWS Cloud running on next-generation Amazon Elastic Compute Cloud (Amazon EC2) bare metal infrastructure.

VMware Cloud on AWS brings the broad, diverse, and rich innovations of AWS services natively to the enterprise applications running on VMware compute, storage, and network virtualization platforms. This allows your organization to easily and rapidly add new innovations to your enterprise applications by natively integrating AWS infrastructure and platform capabilities.

TIP

With VMware Cloud on AWS, you can simplify your hybrid cloud operations by using the same VMware Cloud Foundation technologies — for example, vSphere (including vCenter Server), vSAN, and NSX — across your on-premises data centers and on the AWS Cloud. There's no need to purchase any new or custom hardware, rewrite applications, or modify your operating models.

Now that you've spent a good deal of time understanding the need for and benefits of modernizing and securing your entire IT environment, I want to make sure I also cover some basics when it comes to adopting virtualization in the first place, and setting up your core environment.

At the most basic level, these foundational capabilities for a modern and secure data center begin with the migration to next-generation virtualization — a topic I cover in Chapter 6.

IN THIS CHAPTER

- **Getting started with your modern virtualization and cloud platform**
- **Adding operations management**

Chapter 6

Next-Gen Virtualization Preflight

When a virtual environment is firing on all cylinders, it drives down costs and minimizes downtime while increasing productivity. Unfortunately, many businesses undercut those gains before deployment by incurring costs and causing downtime in the earliest stages of the shift from physical to virtual.

This is a case where a little planning goes a long way. This chapter discusses some things to consider before you begin your migration. Know what to expect and you can plan accordingly.

Preparing to Move from Physical to Virtual

Preparation is key in ensuring the success of an important project such as implementing next-gen virtualization. In the following sections, I make sure you've covered all the bases.

Assembling your team

Before you move your physical server workloads into virtual machines, enlist a cross-discipline team that includes IT admins, application owners, finance personnel, and other stakeholders. It's important to have a range of perspectives to make sure your virtualization strategy aligns with business priorities. As you move forward, this team will also help you demonstrate how cost savings and improved service levels in the data center affect the rest of the organization.

Assemble a detailed plan that outlines the full scope of the project and its phases. Work with your finance team members to determine total cost of ownership (TCO) and your projected return on investment (ROI). If you need new hardware such as servers, storage arrays, or networking gear, put it in the budget.

REMEMBER

The cost of new hardware might be offset by savings in other areas, such as maintenance or operating expenses.

Next, decide which workloads will be your highest priority for the physical-to-virtual (P2V) migration. For example, you might start with test and development workloads; and then virtualize your Tier 2 applications; and finally virtualize your Tier 1, mission-critical applications.

TIP

Before you roll out the new virtual environment, allow time to test it thoroughly. Record baseline performance on your current servers and applications. It's important to have this data before migration begins so you can benchmark VM performance gains against native performance levels. This helps justify the project for management buy-in.

REMEMBER

Be sure to carefully schedule the migration and expected downtime for the workloads you're migrating. Using a proven P2V conversion tool such as VMware vCenter Converter can help you minimize downtime and maximize automation during your migration process. vCenter Converter converts both Windows and Linux physical machines to a VMware virtual machine format and brings them into your VMware environment, automating the migration process semi-transparently for your users.

Using traditional versus virtual storage

Shared storage improves availability and allows hypervisors to leverage capabilities (such as VMware vMotion) to migrate running VMs across hosts for zero-downtime maintenance. Today, there are multiple options for shared storage:

- **Traditional external storage-area network (SAN) or network-attached storage (NAS) array:** Compared to virtual storage, a SAN or NAS solution can be more expensive and can require more technical expertise because it needs specialized hardware and IT staff. For organizations with available capital and larger IT environments, traditional arrays provide deduplication, array-based replication, and unified storage offerings (for example, NFS, iSCSI, Fiber Channel).
- **Virtual storage:** This option is simpler than SAN and NAS because you don't need to purchase, configure, or maintain an external hardware array. For businesses that need shared storage but do not need all the features of an enterprise storage solution, a solution such as VMware vSAN can save capital expenses and ongoing management costs.

Sizing and managing shared storage

Virtualization allows you to pool your storage infrastructure, which gives you flexibility for optimal workload placement. You can place high I/O-intensive workloads — such as Tier 1, mission-critical database applications — on Tier 1 back-end storage, which might be on high-speed SSDs or enterprise-grade SAS disks. At the same time, you can move test and development environments or rarely accessed data to slower and lower-cost storage to reduce expenses over the long run.

When sizing and managing your shared storage, you should:

- Monitor how much space is used on your existing physical volumes, and also the number of I/O operations per second (IOPS) your workloads use. This information can help you choose the right type and size of disks for your new environment.

- Calculate your storage needs, in both raw capacity and IOPS, on current and future workloads. What's the best way to meet those needs? Do you need the array-based replication or extreme amounts of capacity that a traditional storage array can provide? Or could your needs be met by a more cost-effective vSAN solution that allows you to scale storage capacity and performance as you add physical host servers?
- Take advantage of the storage efficiencies of virtualization. For example, on a traditional physical server, adding or reconfiguring disk drives is difficult, time consuming, constrained by available drive bays, and can sometimes result in downtime or data loss. In a virtual environment, physical storage devices are abstracted — separated — from the virtual machine, so storage capacity can be added without affecting the VM in any way. Virtual disks, by the same token, can be easily expanded without requiring complex reconfiguration of physical storage devices.
- Choose thin or thick provisioning of virtual disks for individual VMs. Thick provisioning allocates all the space for a virtual disk the moment you create it; thin provisioning allocates space as necessary throughout the virtual disk's life. If you have a dedicated storage solution from a third party, thin provisioning may be available at the array hardware level as well.

TIP

Using VMware vSphere, you can configure Storage I/O Controls to guarantee a certain amount of I/O resources for each virtual disk, or you can enable Storage I/O Controls to provide equitable access to storage resources for all VMs. This ensures that no particular workload will dominate the resources of any physical array.

Addressing basic security and compliance

REMEMBER

Just like physical servers, VMs need to have appropriate security and compliance policies in place. Remember the following:

- If your business must comply with any government regulations, consider any audit rules that apply. For example, will it be acceptable for each workload to share physical networks or virtual switches? Must the data itself be on separate physical storage?

- As you set up policies and provisioning, keep in mind the challenge of managing sensitive data from different applications. Do the rules allow that data to reside with the data from other applications at the compute, networking, and storage layers?
- Make sure you have a working management network with all management interfaces of physical hosts, switches, and other data center infrastructure in the environment. Isolated management networks provide higher security while preventing VM traffic from interfering with management traffic.
- You need to balance VM protection with performance by scheduling security scans and other checks for off hours.

Using Operations Management to Meet Business Objectives

Server virtualization allows physical resources to be shared among many virtual servers, improving resource utilization. But this isn't just about utilization. It's also about performance and security. It's important to make sure your mission-critical applications have the resources they need to perform well while ensuring they meet your company's compliance and security policies.

Here are some things to consider:

- Define affinity rules for your VMs. For example, you can define host affinity rules to keep VMs together, so a web server VM and its associated app and database VM are kept on the same physical server for high-speed virtual network connectivity. You can also define anti-affinity rules. For example, you can keep multiple database servers on separate hosts so if a physical host fails, other database VMs will keep running.
- Determine whether your applications must reside on specific hardware for compliance or process reasons.

- Make sure you determine the recovery time objective (RTO) and recovery point objective (RPO) for each workload. That way, when you're creating your business continuity and disaster recovery plans, your backup and recovery policies are aligned with your business priorities.

TIP

As the saying goes, those who ignore history are doomed to repeat it. By monitoring performance issues, resource shortfalls, and other historical data on your VMs, you can anticipate future spikes in memory and CPU usage, and plan accordingly so critical applications do not hit capacity limits. The tools of a modern virtualization platform make it easy to monitor and analyze workloads and diagnose problems, so you can keep your business-critical applications and VMs operating at peak performance.

Before you deploy, you need to know several things:

- Prepare carefully to optimize resource utilization. Early planning will help improve consolidation and ROI down the road. So before you install, find the guardrails with vRealize Operations. How many hosts, VMs, storage systems, and clusters will you be monitoring? You'll need this baseline information before you start.
- Consider the appropriate permissions for different user types. Using vRealize Operations, you can configure permissions and security, and then assign privileges so authorized users have access to the right assets in the management console. For example, admins should be able to touch everything. Help desk staff should have the permissions they need to fix day-to-day problems without inadvertently changing policies or settings. Consider the best way to set up multiple user permission levels to maintain the security of the environment while giving all staff members the ability to fix day-to-day problems as they arise, so your business keeps moving.
- Model your virtual environment on your business structure. Structure your operations views with intelligent groups that make sense for your business. Group objects based on specific business needs, departments, locations, and more to create a simplified view of your environment from the vRealize Operations dashboard. Tailoring groups to your

specific business needs helps simplify IT tasks, so IT staff is better equipped to manage more systems, lowering administrator overhead and freeing up staff for innovation elsewhere.

- Create policies for efficient resource management. Use vRealize Operations to assign policies to certain groups of resources, geographic locations, or business units to customize alerts and capacity management settings. Take advantage of the out-of-the-box policies that will meet most of your business needs (for example, production or test environments, batch or interactive workloads) or create your own personalized policies.
- Identify the needs of workgroups to configure capacity settings. Every workgroup has different needs at different times. A production team working on a product launch might need to be over-provisioned for a few months with extra CPU and storage. A development and test environment might be fine with high-density, over-committed VMs and resources. With accurate capacity analysis, you can account for varying business needs and tap your massive pool of resources so every workgroup has what it needs.
- Choose how you want to be alerted. Smart alerts let you choose how you want to be notified by your management platform when a problem is developing. vRealize Operations learns typical behavior in your environment, so it provides fewer, more meaningful alerts that let you know when there really is a problem — for example, when a dynamic threshold is exceeded or an anomaly is detected. Similar to capacity settings, alerts are configured based on policies that you define. Alerts also provide actionable recommendations so you can find and fix problems fast, before they cause downtime.
- Set up email notifications for administrative alerts. To monitor data center health and capacity from anywhere, configure an optional SMTP server to activate email service for notification messages when problems occur. You can set email notifications for all types of alerts, so you can address problems as they happen in real time, minimizing downtime.

  For administrators, it's especially important to set up email notifications for administrative alerts to ensure vRealize Operations is always running properly.

- Schedule reports to help address bottlenecks before they occur. Use reports in vRealize Operations to monitor capacity and performance in the vSphere environment and to help avoid bottlenecks. It's a good idea to schedule reports for regular intervals — weekly, monthly, quarterly, whatever makes sense for your business. You can also pull reports on demand for a real-time snapshot of the IT environment, and use historical reports to track growth patterns and anticipate future capacity needs. Detailed reporting is one of the most underappreciated aspects of a virtual environment, and one of the best tools to continuously improve performance and efficiency.
- Unify your view of the virtual environment. Use the dashboard to quickly recognize areas that need attention and look deeper into individual components of the environment when necessary. The consolidated dashboard helps you ensure that resources are being used efficiently and that all systems are performing and available, all from a single view that allows you to spend less time monitoring and more time optimizing. With this dashboard, you get a holistic view and deep insights into the status of infrastructure and applications to help ensure quality of service and early detection of performance, capacity, and configuration issues.

IN THIS CHAPTER

- » Highlighting tips, techniques, and insights
- » Getting the best from your secure hybrid cloud platform

Chapter 7
Ten Best Practices for Securing Your Hybrid Cloud Environment

Best practices for a modern hybrid IT environment build on a robust virtualization and security platform. Given the rising importance of security in today's hybrid environments, these best practices begin with the implementation of five core principles of cyber hygiene, which equate to the first five best practices listed in this chapter. These principles are among the most important and basic steps that any organization should take to build security into the data center.

TIP

One additional bit of advice: While these five principles of cyber hygiene apply across the board to your critical as well as non-critical systems, you might want to focus on your most critical systems first, and then expand your cyber-hygiene program to the rest of your systems.

The last five best practices give you a broader look at securing your hybrid cloud.

Establish a Least-Privilege Guideline

The least-privilege principle is pretty simple: Users should be allowed only the minimum necessary access needed to perform their jobs, and nothing more. The same holds true for system components. They should be allowed only the minimum necessary functions needed to perform their purposes, and nothing more.

Implement Micro-Segmentation

Your hybrid IT environment should be divided into small parts to make it more manageable in terms of security. This micro-segmentation is one of the keys to protecting applications and systems and containing the damage if any one part gets compromised. Micro-segmentation protects your overall IT environment by breaking it up into these smaller parts. It's similar to the use of compartments on a ship. It makes the ship easier to protect. If the ship is damaged in one area, the damage is contained to that area.

Encrypt All Data

For critical business processes, all data should be encrypted, while stored or transmitted. In the event of a data breach, stolen critical files should leave hackers and thieves with nothing but unreadable data. This core principle of cyber hygiene is like an insurance policy for protecting your data from any threats that might come your way.

Use Multi-Factor Authentication

The identity of users and system components should be verified using multiple factors, not just simple passwords. Moreover, the strength of your multi-factor authentication of users and system components should be commensurate with the risk of the requested access or function. In other words: The greater the risk, the stronger the security.

Make Patching a Priority

While this principle of cyber hygiene may sound like something out of a Systems Management 101 textbook, it's worth repeating because of its importance: All systems should be kept up to date with the latest patches and consistently maintained. Any critical or non-critical system that is out of date is a meaningful security risk.

When you do these five things well and consistently, you're making cyberattacks much more difficult to carry out and far less damaging to your enterprise. In even the most devastating data breaches over the last few years, the effective use of all of these principles could have made a big difference in the outcome.

Establish a Security Education Program

To propagate the principles of cyber hygiene, put a mandatory education process in place for everyone — from your IT professionals and business leaders to your employees and third-party contractors.

When everyone is on board:

- IT professionals should be committed to designing security into systems.
- Developers should learn a minimum amount of code-security skills.
- System architects should sign for security outcomes.
- Foundational security knowledge should be as familiar as knowledge of computing, networking, or storage.
- End users should be aware of the risks and their responsibilities in protecting information.
- Throughout your organization, security basics should be as well understood as going to a website or checking email.

Focus on Protecting Critical Individual Applications

Focusing on critical individual applications puts the focus where it should be: on the crown jewels — your mission-critical business applications and the data within them. I'm talking about applications like:

- An enterprise application that processes sensitive data in creating your company's financial statements
- An ordering application that fulfills customer orders and stores personal information and credit card data
- An HR application that contains confidential employee data
- An R&D application that contains trade secrets

The application is the mechanism for accessing and interacting with the data. Even though the goal of information security is to protect these crown jewels, current approaches are focused on protecting the IT infrastructure: for example, routers or servers. Protecting the IT infrastructure is certainly necessary, but that's doesn't go far enough. That's like trying to protect all the houses in a community by putting a fence around them with a locked gate. It would be more effective if you focused on protecting each individual house.

With current approaches, it's hard to effectively achieve security goals, such as ensuring only minimum necessary access. For example, a firewall is often set up at the perimeter of the whole enterprise to control access to a group of applications, which can often be thousands of applications. Instead, there should be a firewall set up to control access to each individual critical application, allowing only access by the users and system components that absolutely need access to that one application.

TIP

You can build these granular firewalls with the micro-segmentation capabilities of VMware NSX, and the AppDefense capabilities included in vSphere Platinum.

Automate Network and Security Provisioning

Automation is one of the keys to maintaining a secure, modern data center. Automate network and security provisioning so that as new compute resources are created, they're secured by default. When using policy-based security automation and micro-segmentation, your IT team can help prevent intrusion and secure network traffic inside your enterprise, such that malware cannot move laterally.

Micro-segmentation limits a threat's ability to propagate across the environment by enforcing network security policies at the most granular level of an application, the individual data center endpoint. You can then segment workloads residing on the same physical host without hair-pinning traffic out through an external physical or virtual firewall. And if you use VMware NSX to automate network and security provisioning, you can enforce a least-privilege model that limits access by user or role and prevents system components from interacting unnecessarily.

Leverage the Power of Adaptive Micro-Segmentation

You can leverage VMware NSX to provide zero trust networks through micro-segmentation. vSphere Platinum now integrates with NSX to provide Adaptive Micro-segmentation — a comprehensive, built-in zero-trust model to secure internal network traffic generated by applications deployed across private or public cloud environments.

By adopting Adaptive Micro-Segmentation, your IT team can save time while building confidence in your internal network defenses. vSphere Platinum provides a holistic picture of an application's topology without the need for lengthy application security reviews. The integration with NSX enables your information security and IT teams to use that understanding of application topology to dynamically create network security policies. As the application's topology changes over time, the network security policies automatically adapt to help ensure a continuous zero-trust posture.

Only IT teams deploying NSX with vSphere Platinum (and built-in AppDefense) gain this level of visibility and control because of the technologies' integration into the hypervisor and other native control points within deployed applications.

Always Keep Security Top of Mind

Think of security as an intrinsic component of your day-to-day IT charter. While SecOps and InfoSec teams absolutely do focus on security, intrusion prevention, firewalls, and more, it's clear that IT now has to play a central role in protecting the business, given the increased frequency and sophistication of cyberattacks.

With this goal in mind, take steps to ensure that security is enabled in all layers of your hybrid IT stack, and is not just a bolt-on solution. When security is ingrained in your data center, you're in a position to comprehensively secure your IT environment from the ground up — including infrastructure, data, access, and applications.

This isn't just about IT. When you take all the steps outlined here, you're helping your business compete and succeed in the digital economy. In this new era, the foundation for business success is a modern IT environment built around a highly secure hybrid cloud platform. That's what it takes to support a dynamic, digitally driven business that can ward off rapidly evolving security threats.

IN THIS APPENDIX

- Highlighting resources
- Linking to research reports, blogs, and product information

Appendix Resources

Ready for a deeper dive into the concepts and technologies embodied in a modern and secure cloud platform? Immerse yourself in these recommendations for resources that will enrich your understanding of the concepts, technologies, and tools for taking IT to a new level.

Explore Top Resources to Learn More

Here are some videos and resources that will help explain next-gen virtualization and security and save you from having to read a bunch of detailed technical papers:

vSphere Platinum overview: Learn about the newest edition of vSphere, with enhanced application security: `https://www.youtube.com/watch?v=TI4Zdn_7QBw`.

vSphere 6.7 overview: Check out a brief video to get informed about what vSphere offers, and how it can help you build a modern and secure hybrid cloud platform: `https://www.youtube.com/watch?v=DtCG8rU0F7g`.

vSphere Use Cases: Check out the core use cases supported by vSphere:

- *Use-case menu:* `https://www.vmware.com/products/vsphere.html#usecases`
- *Data Center Consolidation and Business Continuity:* `https://www.vmware.com/products/vsphere/data-center-consolidation.html`
- *Enhanced Application Performance and Availability:* `https://www.vmware.com/products/vsphere/enhanced-app-performance.html`
- *Application and Infrastructure Security:* `https://www.vmware.com/products/vsphere/secure-applications-and-infrastructure.html`
- *Virtualized Big Data:* `https://www.vmware.com/products/vsphere/virtualize-big-data.html`
- *Legacy Unix to Virtual Linux Migration:* `https://www.vmware.com/products/vsphere/unix-to-virtual-linux.html`
- *Containerized Modern Apps:* `https://www.vmware.com/products/vsphere/integrated-containers.html`
- *Support for Remote Offices and Branch Offices:* `https://www.vmware.com/products/vsphere/remote-office-branch-office.html`

vSphere Customer Feedback and Testimonials: See what others are saying about vSphere, and how you can benefit from their experiences of using the latest and greatest technologies:

- *vSphere Customer Feedback Videos:* `https://www.youtube.com/playlist?list=PLymLY4xJSThqgiSjyJBDBVCrVg-bz8o57`
- *vSphere Customer Reviews:* `https://www.itcentralstation.com/products/vsphere-reviews`
- *vSphere Customer Research Survey Results:* `https://www.techvalidate.com/portals/vsphere-6-7`

vSphere Capabilities: Learn how the capabilities of vSphere come together to provide an ideal foundation for your applications, your cloud, and your business: `www.vmware.com/products/vsphere`.

vSphere YouTube Channel: Get a close-up look at the latest from vSphere, and listen to testimonials from customers: http://vmw.re/vsphereonyoutube.

vSphere Customer Stories: Hear the inside stories from IT professionals and business leaders talking about why they chose the vSphere platform and the benefits they're realizing: www.vmware.com/products/vsphere.html#resources.

Join the Online discussion

One of the great things about the Internet is that it provides the opportunity to connect with people who are experts or who have encountered the same problems you may be facing. Here are some places where you can connect with other next-gen virtualization users:

vSphere Blog: Get fresh insights into the latest with the platform, its capabilities, and its ongoing enhancements from people who work with the software every day: https://blogs.vmware.com/vsphere.

vSphere Community: Tap into the vast vSphere ecosystem. Access how-to documents, ask technical questions, and get direct insights from the user community: https://communities.vmware.com/community/vmtn/vsphere.

VROOM! Performance Blog: Rev up your virtualization engine with these insights from VMware's performance team: https://blogs.vmware.com/performance.

Dive into the Product Details

Here are some resources I've found that can help you get the information you need to make your next-gen hybrid cloud project a great success:

vSphere Website: Get key details on vSphere and vSphere Platinum, including information on use cases, pricing, and the features in different product editions: www.vmware.com/products/vsphere.html.

vSphere Platinum Solution Brief: Learn more about how to secure applications, infrastructure, data, and access with the capabilities of VMware vSphere Platinum: `https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/vsphere/vmw-vsphere-platinum-solution-brief.pdf`.

vSphere Data Sheet: Learn how vSphere delivers simple and efficient management at scale and comprehensive built-in security while providing a universal application platform and a seamless hybrid cloud experience: `https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/vsphere/vmw-vsphere-datasheet.pdf`.

What's New in vSphere white paper: Get a close-up look at capabilities that help IT organizations respond effectively to trends that are putting new demands on IT infrastructure: `https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vsphere/vmware-whats-new-in-vsphere-whitepaper.pdf`.

Customer Reviews on vSphere: Hear firsthand from IT leaders who are capitalizing on the capabilities of a modern and secure hybrid cloud platform: `https://www.itcentralstation.com/products/vsphere-reviews`.

Hands-on labs: Test-drive the full technical capabilities of VMware products in these free evaluations that are up and running on your browser in minutes — with no requirement for installation: `https://www.vmware.com/try-vmware/try-hands-on-labs.html`.

vSphere Evaluation: Start your 60-day trial of vSphere. Evaluate the software in your own environment: `www.vmware.com/go/evaluate-vsphere-en`.

vSphere Upgrade Center: Learn why and how to upgrade to the latest version of vSphere. Access technical resources on the details of vSphere upgrade and installation processes: `www.vmware.com/products/vsphere/upgrade-center.html`.

About the Author

Himanshu Singh is Group Manager of Product Marketing for VMware's Cloud Platform business, and runs the core product marketing team for VMware vSphere. His extensive past experience in the technology industry includes driving cloud management solutions at VMware, growing the public cloud business at Microsoft Azure, as well as delivering and managing private clouds at IBM. He holds a B.Eng. (Hons.) degree from Nanyang Technological University, Singapore, and an MBA from Tuck School of Business at Dartmouth College. Follow him on Twitter at @himanshuks.

Author's Acknowledgments

The author extends his thanks to the subject matter experts on the VMware Cloud Platform team for their help in pulling together and reviewing the content in this book. The author also sends thanks to the writers and editors at the Wire Stone agency and John Wiley & Sons, Inc., for their assistance with the development and refinement of the content. In addition, this book leverages content from the earlier VMware-sponsored *Virtualization 2.0 For Dummies, Hyper-Converged Infrastructure For Dummies,* and *Network Virtualization For Dummies,* as well as several of the assets listed in the appendix.

You need a modern and secure virtualization and cloud platform

To protect and grow your business in the new digital economy, your company needs a modern cloud platform that is highly secure, scalable, and performant. You need to build an efficient IT environment for hybrid clouds that intrinsically secures applications, infrastructure, data, and access. Other essential components are simple and efficient management at scale, a universal application platform, and a truly seamless hybrid cloud experience. You can also take advantage of all the benefits of virtualization — the ability to run, manage, connect, and secure applications in a common operating environment across hybrid clouds.

Inside…

- Why your business needs to run on a modern and secure hybrid cloud platform
- How to secure applications, infrastructure, data, and access
- How storage and network virtualization fit into the picture
- How you can get on the path to seamless adoption of hybrid cloud

vmware®

Himanshu Singh is Group Manager of Product Marketing for VMware's Cloud Platform business, and runs the core product marketing team for VMware vSphere. He has vast experience with both private and public clouds and is a regular speaker at key technology conferences. Follow him on Twitter at @himanshuks.

ISBN: 978-1-119-61170-7
Not For Resale

for dummies®
A Wiley Brand