

# Achieving Endpoint Security

## With VMware ACE

### The Challenges of Unmanaged PCs

It's an IT department's worst nightmare: mobile employees or contractors connect to the corporate network and viruses or other malicious programs running on their PCs transfer to the network. Home users or telecommuters also pose a threat: they can expose the network to vulnerabilities as soon as they remotely access the corporate network via a VPN.

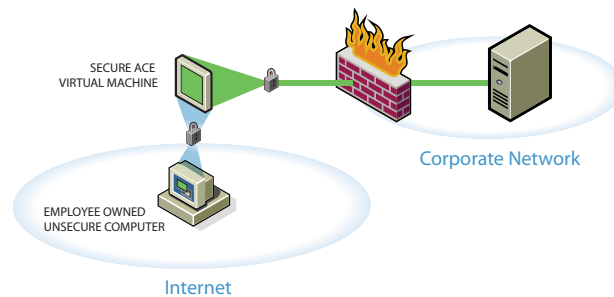
What's more, unmanaged PCs that access the corporate network can put sensitive corporate data and intellectual property at risk. Corporate data can be copied via remote hard drives, flash drives, CD/DVD media, or printers. The rising problem of laptop theft adds to the risk of sensitive corporate information getting into the wrong hands.

Traditionally there's been no sure-fire way to eliminate network vulnerabilities and secure these devices, while letting end users run the applications they use today. IT organizations have pursued the full range of options, from procuring separate dedicated PCs for end users and investing in scan and block technology to denying access to the network altogether, and still their endpoints are vulnerable. Still, IT departments are troubled by managing the systems and updating endpoint PCs with patches, especially because many of these systems are not owned by the IT organization.

### VMware® ACE Provides Control Over Desktop Endpoints Like Never Before

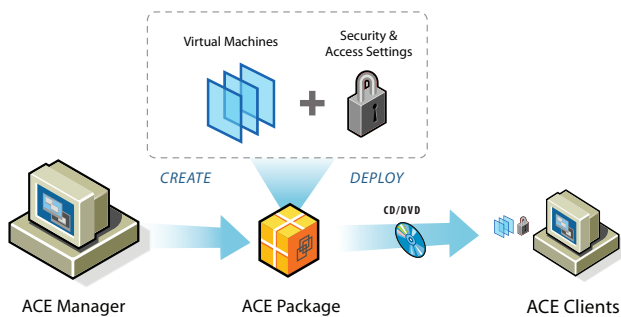
VMware ACE makes it possible for IT departments to manage a remote desktop PC or laptop as they would any normal PC in their network, creating a "virtual laptop" that meets corporate security standards. How? Administrators use ACE Manager to set security policies that control encryption, expiration, network and device access for each virtual machine running on an unmanaged PC. Telecommuters, consultants, and mobile workers use their corporate applications and tools in a virtual machine, effectively allowing them to run a PC on top of a PC, on any desktop system.

### VMware ACE Endpoint Security



VMware ACE creates a secure endpoint on an unmanaged PC and blocks the host from accessing the corporate network

### VMware ACE Solution



Administrators use ACE Manager to create a "package" containing a secure virtual machine for deployment to end users running the ACE client

## Summary

Desktop virtualization with VMware ACE gives enterprise organizations unprecedented control over the unmanaged PCs of contractors, telecommuters and mobile workers. There's no better way for administrators to help secure an unmanaged PC and prevent host PC access to the corporate network, while still letting end users run their preferred applications.

To learn more about VMware solutions, visit our Web site at <http://www.vmware.com/solutions> or contact your VMware representative.

### VMware ACE Solution

**IT Administrator:**

- VMware ACE Manager enables IT administrators to create a VMware ACE package for deployment to end users. The package contains an image of a complete desktop environment (virtual machine) along with access and security policies for how it will be used.

**End User:**

- VMware ACE client software allows end users to run the secure environment (virtual machine)—specified by the IT department—on their desktops.

## ACE Capabilities and Uses

Capabilities	How It Works	How and Why It's Used
Virtual Machines	VMware ACE Manager enables administrators to encapsulate an image of a complete PC (the operating system, applications, security configurations, and data) into a set of files. This set of files, called a virtual machine, can be deployed to any PC, including VMware ACE desktops.	<ul style="list-style-type: none"> <li>• Create secure endpoints. VMware ACE clients make it possible to isolate virtual machines from anything running on the host unmanaged PC. End users can install additional applications outside of the virtual machine that do not affect the secure environment.</li> <li>• Reduce costs. VMware ACE clients become IT managed assets, enabling administrators to take advantage of existing infrastructure and security tools. Telecommuters or contractors can also use their own equipment because virtual machines are hardware independent, saving IT organizations the expense of procuring additional PCs.</li> <li>• Achieve endpoint compliance with regulatory agencies such as HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley. Every VMware ACE environment deployed regardless of hardware type can be configured according to IT guidelines.</li> </ul>
Data Encryption	VMware ACE clients run an encapsulated image or virtual machine that is password protected and offers AES-128 encryption.	<ul style="list-style-type: none"> <li>• Protect confidential information on unmanaged PCs and the corporate network. VMware ACE ensures that no one without a password can access anything inside of a virtual machine. Administrators can impose password requirements on the virtual machine. VMware ACE virtual machines can also be joined to an Active Directory domain.</li> </ul>
Network Quarantine	VMware ACE Manager allows administrators to set policies for host and virtual machine access. VMware ACE clients can be restricted from accessing the Internet from inside their virtual machines.	<ul style="list-style-type: none"> <li>• Control the spread of viruses and malware. VMware ACE clients block the host PC from accessing the corporate network. Only VMware ACE virtual machines can access or communicate with the enterprise network.</li> </ul>
Device Access	Virtual machines can be created in VMware ACE Manager with device policies. End users can be denied access to host PC peripherals such as printers, USB memory keys, and DVD/CD writers.	<ul style="list-style-type: none"> <li>• Lock data on unmanaged PCs into a secure virtual machine. VMware ACE lets administrators control sensitive data inside a virtual machine from accessing host PC devices such as USB storage drives and CD-ROM burners.</li> </ul>
Hardware Independence	The set of files that comprise a virtual machine do not tie directly to devices or other hardware configurations.	<ul style="list-style-type: none"> <li>• Deploy Everywhere. There's no need to create separate images for every desktop hardware configuration supported in the field. Virtual machines can be deployed on any x86 PC.</li> </ul>
Deployment Using Existing Tools	VMware ACE Manager enables administrators to wrap up a virtual machine with security and access controls into an MSI-compliant package for deployment using CD/DVD media, direct download, etc. Machines can then be patched or updated using standard tools.	<ul style="list-style-type: none"> <li>• Keep unmanaged PCs current with the latest software and security patches. VMware ACE is compatible with existing installation and upgrade tools for distributing patches and keeping endpoint PCs up-to-date.</li> </ul>
Simple End-user Experience	End users running VMware ACE virtual machines run the same applications they are running today. They can work connected or disconnected from the network.	<ul style="list-style-type: none"> <li>• No retraining. There's no new software to learn and use. The VMware ACE client and virtual machine install like any software package. Users boot their PCs, log in, and their virtual PC runs like a normal desktop.</li> </ul>

VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com)

©1998-2007 VMware, Inc. All rights reserved. Protected by one or more U.S. Patents Nos. 6,397,242; 6,496,847; 6,704,925; 6,711,672; 6,725,289; 6,735,601; 6,785,886; 6,789,156; 6,795,966; 6,880,022; 6,944,699; 6,961,806; 6,961,941; 7,069,413; 7,082,598; 7,089,377; 7,111,086; 7,111,145; 7,117,481; 7,149,843 and 7,155,558; patents pending. VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 07Q3\_VM\_ACHIEVING\_ENDPOINT\_SECURITY\_SB\_EN\_R1

