



Separation of Duties

in Virtual Environments

White Paper

Introduction

Sensitive data disclosure remains one of the top information security risks in IT. For instance, at least 382 data leaks happened during Q1-Q2 2010, compromising a huge total of 539 million records (according to InfoWatch report.)

While companies keep investing in IDSs, DLPs and other technical solutions, the toughest incidents tend to have mostly social, not technical background. Unauthorized access through an attack can be monitored, but improper access through misconfiguration or privilege abuse is very hard to discover, as it results from regular, legitimate activity. Going virtual makes the information security task somewhat more complicated.

Virtualization solutions by VMware provide a solid ground for building information security-aware infrastructure. For example, virtualization makes it possible isolate applications and/or entire machines that process business-sensitive data. On the other hand, virtualization brings in its specific information security risks. These should be addressed before you can leverage the new technology, especially when specific external regulations (such as PCI DSS) apply.

Why Superusers Matter

Imagine a physical server processing business-sensitive data. In well-administered networks, there's a known list of user accounts that have administrative privileges on the server and can potentially gain access to the data it hosts. You can basically do nothing about it, because there will always be someone who has administrative privileges on a particular machine. Is this a security vulnerability? With adequate permissioning and audit policy in place, it is not. Proper employees presumably have proper access level, and all access attempts outside the normal pattern are logged and reported respectively.

So, do virtual environments make a difference? From a bird's eye view, virtualization is all about consolidating hardware, saving power and other operational expenses. Inside the virtual environment – and that's a huge benefit – you still have the same servers, the same permissions and audit, and, probably, the same IT personnel in charge.

The difference is outside the virtual environment. As your virtualized production servers are now hosted on a virtualization server (hypervisor), the latter needs maintenance and supervision by system administrators. So, a new IT role – virtualization administrator – appears. Primarily due to workload consolidation, a “virtual” administrator is much more of a superuser than his “physical” peer. Outside the box your virtual machine is just a set of files hosted somewhere in the virtualization infrastructure. Virtualization administrators can access your virtual machine’s data even when it’s powered off. To put it simple, there are several ways to **access the sensitive data beyond traditional communication channels and audit mechanisms**. Let’s examine some of these ways:

- ▶ First of all, a virtual machine’s files can be simply copied to a removable media – almost any USB-powered gadget (MP3 players included) is enough. To do that, one can log on to an ESX server, or use the VMware vSphere Client to **download a virtual machine disk** to his/her computer (**Datastore Browser | Download a file from this datastore to your local machine** option).

Once you have the .vmdk at your disposal, it’s just a matter of several minutes before one can access the data on it. The disk can be mounted to another virtual machine, or to the host OS (e.g. using freely available VMware DiskMount utility.) Alternatively, one can log on to the ESX server and **mount a virtual machine disk directly** from the console.

- ▶ A more sophisticated way of gaining access to data inside a virtual machine involves third-party tools based on VIX API. The latter provides for quite powerful mechanisms of automating virtual machine-related operations, including file and application management beyond the host OS. A video that demonstrates access to virtual machines via VMware Guest Console (based on VIX API) can be found at <http://www.youtube.com/watch?v=IURuCCMHvp>.

To put long story short, virtual environments can provide too much power to privileged users, at least out of the box.

The Solution

Information security challenges are not a novel for many other IT systems. Deploying infrastructures involves proper configuration, both performance- and security-wise. The question is – what should be done to address these challenges.

At a first glance, the solution looks pretty simple. All you have to do is delegate virtualization administrators just enough privileges they need to maintain the environment, and restrict them from accessing the sensitive data inside VMs. To achieve that, you also have to prevent self-escalation.

Apparently, there should be a dedicated person (or persons) in charge of privilege management – security officer. By internal policy or for compliance, security officers in return should be restricted from accessing the virtual environment.

VMware Native Tools

Can you enforce separation of duties using the native management tools?

The VMware vSphere security model doesn't consider the security officer role out of the box. So, you will have to allocate necessary privileges one-by-one, from over a hundred of available permissions. Not going into detail, a security officer should be granted the following privileges:

- Access management (Virtual machine | Provision | Allow disk access, or Allow read-only disk access),
- Audit management (Global | Log events),
- Security policy management (Distributed Virtual Switch | Policy operation, or Distributed Virtual Port Group | Policy operation),
- Permission management (all objects).

The latter privilege leaves the door open for self-sanctioning. That is, a security officer will be able to assign whatever privilege to whatever account, including his/her own.

Yet another consideration is that authentication in VMware vSphere Client is performed via Microsoft Windows user accounts. In particular, any member of the built-in Administrators group on the VMware vCenter machine gains the Administrator role in the virtual environment. Administrators are true superusers, as they can both create other roles and manage privileges.

This quick review reveals the fact that native management tools don't provide for reliable privilege delegation and separation of duties.

Security Code vGate

Security Code, Inc has recently introduced an unparalleled information security solution for virtual environments powered by VMware Infrastructure and VMware vSphere.

Security Code vGate builds an authentication layer featuring access control and separation of duties – on top of the standard VMware security model. System administrators that maintain virtual environments can be granted only the privileges they require to perform their assigned tasks. In return, personnel in charge of privilege management and security auditing can be restricted from accessing the virtual environment.

To ensure that all actions are legitimate and tracked in line with corporate policies, vGate controls the communication and management activities throughout the entire virtual environment:

- Granular privileges are granted according to the administrator role and workload trust level.
- Risky operations, e.g. downloading and snapshotting virtual machines can be restricted.
- All management traffic is locked within the secured subnet. Network traffic between authorized personnel and infrastructure elements is signed, eliminating the possibility of “man-in-the-middle” attacks.
- Local and network logons to infrastructure servers (ESX included) can be restricted and reported.
- “Secret” virtual machines are stored and run only on designated trusted workloads.
- Alternate communication channels, including VIX API calls, VMCI traffic, etc. are disabled.
- Rich auditing adds up to the native VMware audit trails.

Each and every setting related to information security is configured via flexible security policies that can be tailored to the company’s internal policies and/or compliance regulations as the case may be. Once instructed, vGate proactively maintains the specified security level to ensure compliance with specific standards.

This paper only provides a brief overview of some virtualization-specific security risks and solutions. For a complete picture, visit www.vgate.info.

Please note that the content in this document is protected under copyright law even if it is not distributed with software that includes an end user license agreement. No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Security Code.

The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Security Code. Security Code assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this document. IN NO EVENT SHALL SECURITY CODE, ITS EMPLOYEES, PARTNERS OR SUPPLIERS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT.

Any references to company names in artwork or screenshots are for demonstration purposes only and are not intended to refer to any actual organization.

About the Company

Security Code, Inc. is the leading Russian provider of hardware and software solutions for compliance and security of corporate IT systems.

Company's core expertise area is sensitive data protection at banking & other financial institutions, healthcare organizations, government agencies, telecommunications, and beyond.

Security Code, Inc. is a technology partner of world's leading software and hardware vendors: VMware, Microsoft, Citrix, IBM, Oracle, and Cisco.

Contact Information

Security Code, Inc.

PO Box 55
Moscow 127018
Russia
Tel: +7 495 980 2345
Fax: +7 495 980 2345
Email: info@securitycode.ru
<http://www.vgate.info>

Security Code Sales Office Europe

PO Box 40
3632 ZR Loenen a/d Vecht
The Netherlands
Tel: +31 (0) 29 423 4374
Email: info@securitycode.ru
<http://www.vgate.info>

© 2011 Security Code, Inc. All rights reserved.

All trademarks and registered trademarks used are property of their respective owners.