

VIRTUALIZED DESKTOPS GROW UP

Mapping the Intersection of Management and Security

Desktop virtualization is booming – but not for the reasons we anticipated as recently as 18 months ago. Rather than replacing physical PCs, desktop virtualization offers to transcend existing methods of managing and securing desktops.

ICE | INFRASTRUCTURE
COMPUTING FOR
THE ENTERPRISE

4 FINDINGS

- By providing a centralized point of control and enforcing a consistent execution environment, desktop virtualization can improve security. **PAGE 1**
- Securing VDI is part of a broader management challenge that brings together disparate IT groups and buying centers in security, desktop architecture and systems management. **PAGE 25**
- VDI and desktop virtualization present new models for endpoint security, but also heighten the need for securing and managing access by privileged users to the hypervisor, and tying authentication to provisioning. **PAGE 8**
- The link between desktop virtualization platforms and identity access management logic (as well as log management and data protection) is still loose, with plenty of scope to more tightly align provisioning and policy. **PAGE 18**

5 IMPLICATIONS

- Better endpoint security through virtualization will appeal to enterprises and facilitate operational improvements for those struggling to maintain a set of 'golden images.' **PAGE 15**
- Management of user profiles, configuration and data is performed in relative isolation from other policy stores. Desktop virtualization must be tied to broader management frameworks. **PAGE 39**
- No single desktop virtualization model will prevail. Implementations are still largely driven by specific use cases. This implies the need for higher-level management. **PAGE 28**
- Despite alliances between AV and desktop virtualization vendors to migrate agents off the guest OS, desktop virtualization adoption will amplify debates on the diminishing value of AV. **PAGE 8**
- The 'desktop in the cloud' may remain aspirational for some time – especially as storage costs stand in the way of adoption. **PAGE 35**

1 BOTTOM LINE

- Desktop virtualization's appeal is unlikely to be based on economics relative to a physical PC. Additional storage may, in fact, make it more costly. The technology sells on its ability to efficiently manage, define and update a workspace image, whether hosted on the server or the client, as well as the resulting security benefits. By centrally managing user configurations, the scope now exists to define specific correlations between users and applications. However, desktop virtualization can compound the challenge of virtualization management, especially at the hypervisor layer. Change brings risks. Tighter integration with other policy stores and granular entitlement provisioning will further extend desktop virtualization's value.

JULY 2010

REPORT SNAPSHOT

TITLE	Virtualized Desktops Grow Up: Mapping the Intersection of Management and Security
ANALYST	Steve Coplan, Senior Analyst, Enterprise Security Practice Rachel Chalmers, Research Director, ICE William Fellows, Principal Analyst
RELEASE DATE	July 2010
LENGTH	41 pages

ABOUT THIS REPORT

Desktop virtualization is booming – but not for the reasons we anticipated as recently as 18 months ago. Rather than replacing physical PCs, desktop virtualization offers to transcend existing methods of managing and securing desktops. Its appeal is unlikely to be based on economics relative to a physical PC – additional storage may, in fact, make it more costly. The technology sells on its ability to efficiently manage, define and update a workspace image, whether hosted on the server or the client, as well as the resulting security benefits. By providing a centralized point of control and enforcing a consistent execution environment, desktop virtualization can improve security.

Through the central management of user configurations, the scope now exists to define specific correlations between users and applications. However, desktop virtualization can compound the challenge of virtualization management, especially at the hypervisor layer. Change brings risks. Tighter integration with other policy stores and granular entitlement provisioning will further extend desktop virtualization's value. This report examines the intersection of management and security for virtualized desktops, including end-user perspectives, current and future use cases, and an in-depth user deployment study, as well a discussion of partnership and M&A opportunities.

TABLE OF CONTENTS

SECTION 1: EXECUTIVE SUMMARY	1
1.1 INTRODUCTION	1
1.2 KEY FINDINGS	3
1.3 METHODOLOGY	5
SECTION 2: SCOPING SECURITY FOR DESKTOP VIRTUALIZATION	6
2.1 DESKTOP VIRTUALIZATION SECURITY OVERVIEW	6
<i>Figure 1: Virtual desktop security should contain infection and prevent it from propagating through the infrastructure</i>	<i>7</i>
2.2 SECURITY FOR VIRTUALIZED ENDPOINTS	8
<i>Figure 2: Virtualization exists in layers between the hardware, OS, applications and user environment. Security must address each layer.</i>	<i>11</i>
2.3 USER AND ADMINISTRATOR AUTHENTICATION	13
2.3.1 User Authentication – Strong Authentication and SSO Converge	13
2.3.2 Desktop Virtualization Amplifies the Need for Privileged Identity Management	15
2.4 ACCESS CONTROL	17
2.4.1 The Intersection of User Virtualization and Identity Management	18
2.5 APPLICATION VIRTUALIZATION SECURITY	20
2.6 VIRTUALIZATION INFRASTRUCTURE AND MANAGEMENT	22
2.6.1 Configuration Management	23
2.6.2 Virtualized Visibility?	25
2.6.3 The Convergence of Desktop Management and Endpoint Security?	27
2.7 PROVISIONING AND GOVERNANCE	28
SECTION 3: END-USER PERSPECTIVES	30
3.1 CURRENT AND FUTURE USE CASES	30
3.2 USER VIRTUALIZATION DEPLOYMENT USE CASE: KAWEAH DELTA	31
3.3 DESKTOP VIRTUALIZATION AND THE NEW BUYING CENTER	35

SECTION 4: IMPLICATIONS AND REPERCUSSIONS	36
4.1 SECURITY AS A DIFFERENTIATOR	36
4.2 ALLIANCES AND M&A.	37
4.3 VIRTUALIZATION SECURITY OR SECURITY FOR VIRTUALIZATION?	39
INDEX OF COMPANIES	42

ABOUT THE 451 GROUP

The 451 Group is a technology analyst company. We publish market analysis focused on innovation in enterprise IT, and support our clients through a range of syndicated research and advisory services. Clients of the company — at vendor, investor, service-provider and end-user organizations — rely on 451 insights to do business better.

ABOUT TIER1 RESEARCH

Tier1 Research covers consumer, enterprise and carrier IT services, particularly hosting, colocation, content delivery, Internet services, software-as-a-service and enterprise services. Tier1's focus is on the movement of services to the Internet — what they are, how they are delivered and where they are going.

© 2010 The 451 Group, Tier1 Research and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication, in whole or in part, in any form without prior written permission is forbidden. The terms of use regarding distribution, both internally and externally, shall be governed by the terms laid out in your Service Agreement with The 451 Group, Tier1 Research and/or its Affiliates. The information contained herein has been obtained from sources believed to be reliable. The 451 Group and Tier1 Research disclaim all warranties as to the accuracy, completeness or adequacy of such information. Although The 451 Group and Tier1 Research may discuss legal issues related to the information technology business, The 451 Group and Tier1 Research do not provide legal advice or services and their research should not be construed or used as such. The 451 Group and Tier1 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.



*Analyzing the Business
of Enterprise IT Innovation*



Better perspective from the top in independent tech research