

## EXECUTIVE OVERVIEW

# VIRTUALLY SECURE

### How Virtualization and Security Interact

*Virtualization changes IT infrastructure, and in doing so, changes the existing security posture of the organization. This report examines the uses of virtualization for security, how to make virtual infrastructure more secure, and the products now on the market at the intersection of virtualization and security.*

## ICE | INFRASTRUCTURE COMPUTING FOR THE ENTERPRISE

### 4 FINDINGS

- As virtualization becomes ubiquitous, people are getting worried. Virtualization adds a new wrinkle to IT infrastructure, and may introduce new vulnerabilities. **PAGE 4**

- To date there has been no successful malicious attack on a bare-metal hypervisor. That makes right now a great time to think about securing virtual infrastructure — ahead of need. **PAGE 4**

- Live migration across insecure subnets poses obvious risks. Less obvious are the risks posed by virtual appliances. **PAGE 4**

- Some advocates for virtualization have argued that encapsulating operating systems inside virtual machines can, counter-intuitively, make them more secure. We are skeptical. **PAGE 7**

### 5 IMPLICATIONS

- Virtualization improves isolation, but better isolation is not necessarily better security. **PAGE 7**

- A compromised VMM or hypervisor layer is the worst-case scenario, but it is not the only threat. **PAGE 7**

- Special features of virtualization add new vulnerabilities to IT infrastructure. Without modification, physical-world security tools are poorly equipped to handle these threats. **PAGE 11**

- VMsafe aims to give third-party security products the same visibility into the operation of VM guests as the hypervisor itself. The Xen community has similar plans. **PAGE 11**

- Security is a tiny portion of the virtualization market. Two events could change that: the release of products based on VMsafe APIs, or a major virtualization security breach. **PAGE 15**

### 1 BOTTOM LINE

- Virtualization is neither a huge departure from earlier methods of organizing IT resources nor a silver bullet. To secure virtual infrastructure, the usual security principles must be applied: defense in depth, network design and segmentation, and unified security management.

DECEMBER 2008

## Executive Summary

Perhaps the most challenging problem facing enterprise architects, chief information security officers and chief information officers is a fundamental confusion – abetted by the security industry – over what exactly is ‘virtualization security.’ Executives, hearing claims of economic advantages in virtualization of resources, are pressing hard to make decisions about a technology that is entering the mainstream at a furious pace.

In the meantime, vendors are promoting several classes of products under the generic banner of ‘virtualization security.’ These classes include products that essentially provide situational awareness of virtualized assets and environments. They also include products that protect against more traditional threats that have become harder to track within virtual network segments – for example, by tracking network hosts or providing virtual network firewalling, intrusion detection and prevention, and so on. And finally, these products include offerings from vendors that have simply substituted a virtualized appliance – to be run on commodity hardware – for a hardware appliance.

To the C-level executives with a less-than-encyclopedic knowledge of the technology deployed in their organizations, this is extremely confusing. We believe that marketing hype is slowing adoption as these C-level types grapple with the big picture in an attempt to make reasoned and informed decisions about virtualization deployments. In this report, we have grouped these product classes into three main buckets:

- Using virtualization for security
- Securing virtual infrastructure
- Virtual security products.

# TABLE OF CONTENTS

<b>SECTION 1: EXECUTIVE SUMMARY</b>	<b>1</b>
1.1 KEY FINDINGS . . . . .	1
1.2 METHODOLOGY . . . . .	3
1.3 THE STORY SO FAR . . . . .	4
<b>SECTION 2: USING VIRTUALIZATION FOR SECURITY</b>	<b>7</b>
2.1 ON THE SERVER . . . . .	8
2.2 ON THE CLIENT . . . . .	9
<b>SECTION 3: SECURING VIRTUAL INFRASTRUCTURE</b>	<b>11</b>
3.1 SECURITY AT THE HYPERVISOR LAYER . . . . .	11
3.2 SECURITY WITHIN VIRTUAL NETWORKS . . . . .	13
3.3 SECURITY FOR LIVE MIGRATION . . . . .	14
<b>SECTION 4: VIRTUAL SECURITY PRODUCTS</b>	<b>15</b>
4.1 MARKET SIZE . . . . .	15
4.2 VIRTUALIZATION SECURITY FROM WITHIN THE PHYSICAL SERVER . . . . .	17
4.3 VIRTUALIZATION SECURITY FROM OUTSIDE THE PHYSICAL SERVER . . . . .	21
4.4 PHYSICAL-WORLD VENDORS WITH VIRTUALIZATION STRATEGIES . . . . .	22
<b>COMPANY INDEX</b>	<b>31</b>
<b>TERMS OF USE</b>	<b>34</b>