Abstract

Enterprises continue to spend more and more of their IT budgets on securing their environment. Indeed, IDC data demonstrates double digit growth for IT security solutions and services in the recent past with accelerating growth forecasted over the next few years. The constant change in the nature of security threats poses a growing challenge to IT staff.

Failures in security can have major impact, particularly when fines are levied for data breach or non-compliance of industry and regulatory controls. Enterprises are also fully aware of the impact of security issues upon brand degradation, customer attrition, and the potential loss of valuable intellectual property. Data loss prevention and endpoint security represent two of the areas in the security landscape that are of greatest concern and that are seeing the largest increases in budgets.

Many organizations are considering Virtual Desktop Infrastructure (VDI), which centralizes the execution of users’ desktops in the data center, in order to address these concerns. But VDI comes with tradeoffs in user experience, productivity, cost, and flexibility that limit its applicability. An alternative approach is to use Intelligent Desktop Virtualization (IDV), which combines the best end point security with no compromises in user experience, productivity, cost, or flexibility.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Introduction</td>
<td>1</td>
</tr>
<tr>
<td>II. Intelligent Desktop Virtualization (IDV)</td>
<td>1</td>
</tr>
<tr>
<td>III. Data Is Not Stolen Even If a PC Is</td>
<td>2</td>
</tr>
<tr>
<td>IV. Lost PC Monitoring, Lockout, &amp; Remote Kill</td>
<td>3</td>
</tr>
<tr>
<td>V. Instant Recovery from Malware &amp; Corruptions</td>
<td>3</td>
</tr>
<tr>
<td>VI. USB Filtering and Policy Controls</td>
<td>4</td>
</tr>
<tr>
<td>VII. Transparent Backup &amp; Recovery</td>
<td>3</td>
</tr>
<tr>
<td>VIII. Isolation and Protection of VMs</td>
<td>4</td>
</tr>
<tr>
<td>IX. The Data-Less End-Point Option</td>
<td>4</td>
</tr>
<tr>
<td>X. Conclusion</td>
<td>5</td>
</tr>
<tr>
<td>XI. The Virtualization Practice</td>
<td>5</td>
</tr>
<tr>
<td>XII. Intel</td>
<td>6</td>
</tr>
<tr>
<td>XIII. Virtual Computer</td>
<td>6</td>
</tr>
</tbody>
</table>
I. Introduction

The focus on security solutions in the enterprise has been growing steadily over the past few years and is expected to increase significantly in the next few years. In fact, according to IDC, the worldwide market for IT security solutions and services is expected to grow at double digit rates — going from $39B in 2011 to over $62B by 2015. This is driven by several factors, including the rapid growth of end user computing devices and the increased mobility of those devices. As an example of increased mobility, in the PC market, laptops have been growing at nearly ten times the rate of desktop computers.

In order to increase end user security, many companies are considering Virtual Desktop Infrastructure, also known as VDI, which replaces PCs with thin clients and moves both the data and the execution of PC workloads into the data center. As a result of major marketing investments by VMware and Citrix, VDI has gained a great deal of attention and interest.

However, VDI suffers from some critical limitations. Users cannot access their computing environment unless they have a connection to the network. In order for their user experience to be acceptable, that network has to have sufficient bandwidth and continuously operate with very low end-to-end latency. It must also offer a high degree of redundancy as employees cannot use their desktops at all during an outage. VDI also comes with significant costs because major investments are required in servers, storage, and network infrastructure to support the desktop workloads running on expensive data center resources.

This gives rise to an important question. How does one give end users an environment that provides them with the best possible user experience and allows IT to meet its mandate to protect corporate data and endpoint computing assets at the same time — and how does one do this at a reasonable cost? Intelligent Desktop Virtualization provides organizations a way to achieve this goal.

II. Intelligent Desktop Virtualization (IDV)

Intelligent Desktop Virtualization (IDV), a phrase coined by Intel, describes an approach to desktop virtualization that, unlike VDI, offers the best of both worlds — great performance for end users and strong security and manageability for IT. IDV leverages client-side hypervisor technology to allow enterprise IT to place a fully managed, backed-up, and secure Virtual Machine (VM) on the end user’s device. IDV also enables companies to put multiple VMs onto a single PC, so a user can have a Corporate VM and a Personal VM, each of which works just like a completely isolated, fully functioning PC. IDV delivers the ultimate in performance to end users because the applications are running locally. Moreover, because IDV uses the compute power on intelligent clients, it does not require the major infrastructure investment that VDI requires. In fact, IDV requires less than 1/20th of the infrastructure investment of VDI.

Advanced IDV solutions use technologies such as type-1 client hypervisors to increase isolation and security. This combined with features like continuous backup ensures that corporate data is always protected and secure. Moreover, if the end user’s device is lost or stolen, the data on the device can be remotely destroyed and a new device can be rapidly provisioned, getting the employee productive again quickly.
How does IDV provide IT with the ability to control and secure desktop images and devices while ensuring users enjoy high performance, mobility, and flexibility? IDV delivers on this promise by stipulating three tenets:

1) **Manage centrally and execute locally** to minimize data center build-out and leverage the processing power of an intelligent client to optimize the user experience.

2) **Deliver layered images intelligently** to enhance updating and patching, streamline storage, and avoid image drift. When IT separates the desktop image into its logical layers, it can manage each layer separately and minimize the number of images. Intelligent delivery requires that the local image running on the PC be synchronized with the central image. This ensures that end users and IT are working with a golden image at all times. The synchronization and storage of these images should be enhanced with de-duplication technology to minimize storage and network bandwidth requirements.

3) **Use device-native management** to provide out-of-band (OOB) access to the device to provide hardened security capabilities and enhanced manageability independent of the OS.

By implementing a solution that adheres to these three principles, IT is able to manage a single central image and deliver it to the user’s device where it best can be executed with the highest level of security.

### III. Data Is Not Stolen Even If a PC Is

IDV solutions use advanced encryption techniques to protect locally stored data. The most advanced IDV solutions use full disk encryption instead of encrypting just the files containing the virtual machines. Full disk encryption provides a higher level of security and is also superior for compliance, because certain regulations requiring encryption specifically mandate full disk encryption. Ensuring that your IDV solution offers full disk encryption provides organizations with a better way to comply with the broadest set of current and future regulations.

The most secure IDV solutions also use a type-1 hypervisor on the client. With a type-1 hypervisor, the hard disk is owned directly by the hypervisor with no underlying operating system intervening. If security and performance of high importance to organizations, they should make sure to purchase a desktop virtualization solution with a true type-1 client hypervisor.

One important benefit that IDV solutions provide is that the data on the end user device is not accessible until the user fully authenticates to unlock the device. If the desktop or laptop is stolen and the hard disk is removed and put into another computer in attempt to access the data, the encrypted data is not accessible.

Companies are legally required to report lost or stolen data. A critical benefit to using full disk AES-256 encryption is that even if the device is lost, there is no data breach as long as this level of encryption is in place. In fact, AES-256 full disk encryption is so strong, it’s used to protect the highest level of government classified top secret information.
IV. **Transparent Backup & Recovery**

Corporate data is automatically and continuously backed up. IDV solutions include management features that automatically detect changes to end user files and transparently and incrementally stream those changes back to the data center where a backup image of the end user’s environment is kept. This means that if the end users’ laptop is lost or stolen, the end user’s computing environment and their data is not lost at the same time. Rather a completely up-to-date replacement image with the most recently backed-up data can be pushed onto a new laptop. With advanced IDV solutions, IT departments can set policies for which items are backed up, how often backups are taken, and how many backup versions are stored. They also provide differential backup and de-duping capabilities to reduce network bandwidth and storage requirements.

V. **Lost PC Monitoring, Lockout, & Remote Kill**

IDV solutions also offer capabilities to continuously monitor end point devices in order to identify and track lost or stolen PCs. Policies can be set to require PCs to check into the central management server on a pre-defined frequency, and if the device fails to check in, the system can be configured so that the virtual machines become inaccessible. With advanced IDV solutions, monitoring frequencies and lockout policies can be set for each individual virtual machine, so that a different policy can be used for a Corporate VM versus a Personal VM.

In the case where a PC is confirmed to be lost or stolen, IDV solutions can issue a self-destruct command to the PC. When the PC next connects to the Internet, that command is received by the PC and all of the data, applications, settings and profiles on that machine are destroyed. The most advanced IDV solutions perform a 7-pass DOD (Department of Defense) compliant wipe of the entire hard drive. Although the data on the machines is already encrypted and therefore cannot be accessed without proper authentication, the ability to lockout VMs and the ability to remotely wipe the hard drive provide additional levels of security.

Note that even if the machine is lost and the drive needs to be wiped, the data will not be lost. This is because the data would have been automatically backed up by the transparent incremental backup features.

VI. **Instant Recovery from Malware & Corruptions**

Capabilities such as “snap back” enable PCs to automatically boot from a pristine golden state every time. So if a virus infects a system, eliminating the virus is as simple as rebooting. This also has the added benefit of keeping computers running quickly. Traditionally, Windows performance tends to degrade over time, reducing the performance of PCs. But with advanced IDV solutions, every time a PC boots, it boots from the clean, golden image ensuring the best performance.

Some IDV solutions also allow IT administrators to setup reboot policies, which can be extremely valuable for large banks of computers used in training centers, libraries, or other areas where shared use computers are deployed. In these use cases, traditional PCs rapidly degrade in performance as different users wreak havoc on the settings, plug-ins, and applications on the PCs. With reboot policies and snap back capabilities, IT
administrators can set these machines to automatically boot to a pristine state every night (or whatever schedule is specified) to make management of these machines virtually maintenance free.

VII. USB Filtering and Policy Controls

IDV solutions also give the IT department granular control over USB device permissions. For example, certain types of devices can be permitted while others are disallowed. And these permissions can be set separately for each VM assigned to the user. So for example, the Corporate VM can have more restrictive policies than the Personal VM.

Using these policies, IT departments can set up permissions so that Corporate VMs are prohibited from using mass storage devices (to prohibit data theft), but are permitted to use devices such as headsets or microphones for unified communications applications. Meanwhile, they can set up policies to allow all USB devices on Personal VMs.

VIII. Isolation and Protection of VMs

Since the type-1 client hypervisor in an IDV solution owns all of the hardware resources on the end user device, including the keyboard and display drivers, viruses which attack the Windows versions of these drivers with the intent of logging keystrokes or scraping screen data are rendered ineffective. This is another example of leveraging the hypervisor to provide a level of security functionality to a guest operating system that is not available natively.

The type-1 hypervisor maintains complete separation between environments (e.g., Corporate and Personal VMs), making it impossible for “bad behavior” in the personal partition to leak over and affect the corporate partition. This is one of the best ways to allow users the freedom to do what they want to do in their personal environments, while keeping the corporate environment locked down and safe, and allow both of these environments to co-exist on the same PC or laptop.

IX. The Data-Less End-Point Option

There are some use cases where data is not permitted to leave the datacenter under any circumstances — typically for compliance reasons. Some IDV solutions provide an option to host all of the data and the VMs centrally while still providing a rich end user experience by running the client hypervisor on the end point device. In this scenario, organizations can use low cost, fan-less PCs with small flash drives to run the client hypervisor while storing the VMs and data on a storage array network. In this model, the screen rendering and graphics are still done locally, providing better end user performance than VDI. And because the local compute power of the PC is used, the total cost is lower than VDI in this model as well.
X. Conclusion

In a recent survey by Intel of over 200 IT professionals, security was selected as one of the top reasons for implementing desktop virtualization:

- Improving client security: 39%
- Lowering desktop management costs: 38%
- Desire to virtualize both server and client environments: 36%
- Improving overall client manageability: 34%
- Part of our overall move to cloud computing: 34%
- Streamlining application deployment and management: 30%
- Simplifying hardware management: 28%
- Simplifying OS management: 18%
- Accommodating user requests for more diverse client endpoints: 16%
- Improving regulatory compliance: 14%
- Implementing a “bring your own computer” policy: 4%

Source: Intel IT Center Peer Research, Desktop Virtualization Insights for IT Strategic Planning, September 2011

While VDI solutions can enhance security, they cannot deliver an excellent user experience across all types of applications (including rich media), and across all connectivity scenarios (including low bandwidth connections, and no available connectivity). They also require massive investments on servers, storage, and networking in order to deliver even moderate user performance.

IDV delivers both the security and manageability required by IT and the end user experience required by the end users. It is the only approach to desktop virtualization that does not involve compromising one of reliability, security or end user experience in order to meet the other goals. Moreover, IDV delivers all of these capabilities at less than 1/20th of the infrastructure cost of VDI. With IDV, organizations are able to meet the needs of both IT and end users, while delivering immediate return on investment.

XI. The Virtualization Practice

The Virtualization Practice provides analysis, commentary, and resources on current Virtualization and Cloud Computing news, events, and community. We break Virtualization into Topics, and feature a world class expert in that topic as the analyst for the topic. Topic Analysts are responsible for writing original, objective, analysis in their area of expertise, and for writing and maintaining a white paper on their market and the vendors that serve that market.

Bernd Harzog

Bernd Harzog is the Analyst at The Virtualization Practice for Virtualization Management. Bernd is also the CEO and founder of APM Experts, a company that provides strategic marketing services to vendors in the
virtualization management markets. Prior to these two companies, Bernd was the CEO of RTO Software, the VP of Products at Netuitive, a General Manager at Xcellenet, and Research Director for Systems Software at Gartner Group. Bernd has an MBA in Marketing from the University of Chicago.

**XII. Intel**

Intel is the leader in microprocessor innovation. By introducing Intel® Virtualization Technology (Intel® VT) to the market, Intel enabled virtualized machines to run at near-native performance levels. Intel continues to innovate with technologies such as Intel® Core™ vPro™ processors that combine CPUs and graphics processing. Intel® Core™ vPro™ processors offer greater levels of manageability and security at the hardware level.

Learn more about Intel® Core™ vPro™ at [www.intel.com/technology/vpro](http://www.intel.com/technology/vpro).

**XIII. Virtual Computer**

Virtual Computer is a market leader in Intelligent Desktop Virtualization, combining client-hosted virtualization with centralized management. The company’s flagship product, Virtual Computer NxTop®, makes managing thousands of desktops and laptops as easy as managing one, while offering new levels of flexibility and productivity to end users. NxTop delivers ultra-fast native PC performance, complete mobility, and better manageability than server-hosted VDI for a fraction of the cost.

Get a free download of NxTop at [www.virtualcomputer.com](http://www.virtualcomputer.com).