

Ensuring a **SECURE** compliant cloud

You've heard of crowd control? Well, now it's time for organizations to exercise cloud control. Your ability to achieve compliance may depend on it.

The fact is, as more and more enterprises embrace virtualization and cloud computing, thereby washing their hands of the equipment and maintenance costs, staffing needs, and IT management responsibilities of a strictly physical IT environment, they're finding that security and compliance issues force them to get their hands dirty all over again. Especially when organizations employ cloud services from third-party vendors, questions arise as to how to retain control of confidential information, particularly in light of the current regulatory climate. It's important to know that even if regulated data is not in your physical possession, you are ultimately responsible for ensuring its security.

In the case of internal clouds, it's just as critical to know who is accessing applications and information—and what users are doing with them—in a virtualized envi-





ronment as it is when those assets are distributed on physical servers and desktops throughout the enterprise.

To the extent that the promise of virtualization and cloud computing may have inadvertently created a laissez-faire attitude among IT professionals and promoted a literal and figurative false sense of security, it's time to right that wrong and understand that control remains essential to ensuring compliance in any kind of IT environment. Fortunately, some of the capabilities of cloud computing can actually make compliance easier if you know how to exploit them.

A DESKTOP-TO-BOTTOM APPROACH TO CONTROL

For IT administrators in the typical enterprise, one area that has heretofore been very uncontrollable is that of employee desktops. According to Eric Baize, senior director of the Secure Infrastructure Group at EMC Corporation, "How employees behave is largely outside the control of administrators: They add software plug-ins to their laptops without permission, change configurations as they please, and are lax about updating security patches. They take their laptops home, to hotel rooms, and on airplanes; they also surf the Internet, shop, chat, and download files onto removable media. Unintention-

ally, they make it very difficult for administrators to effectively manage and protect IT resources."

To ensure security and achieve compliance requirements with respect to employee desktops, IT administrators need to be able to:

- Protect data when an employee device is lost or stolen
- Ensure users are following established use policies
- Enforce strong authentication
- Protect employee devices from malware
- Apply security patches in a timely manner
- Maintain a secure configuration profile

Fortunately, virtualization enables IT administrators to seize control of this often chaotic domain. A "virtual desktop" is a cloud service that actually increases security and makes compliance easier. Administrators can centralize assets in the data center and make them available as a hosted service on demand. A hosted virtual desktop environment gives administrators more control, along with complete visibility into what applications and data are served and to whom and for how long.

Additionally, notes Baize, the virtual desktop reduces the risk of data being stolen or misused. "If a laptop is stolen,

there's no data resident in it that can be compromised," he says. "Administrators can upgrade applications, operating systems, and security patches centrally, globally, and consistently. In addition, virtualization isolation techniques ensure that personal use of the hardware does not interfere with corporate use or impact performance."

FOR EMC, IT'S "CARPE DESKTOP"

EMC Corporation is piloting a virtual desktop initiative internally, looking to achieve not just cost savings but also improved security, compliance, and performance. According to Paul Divittorio, EMC's director of IT Enterprise Systems and Application Hosting Architecture, "Desktop virtualization is one of the company's major priorities. We started the pilot last quarter with 250 desktops, we're going to double that this quarter, and the goal for the year is to virtualize 5,000 employee desktops throughout the organization."

So far, users have accepted the change. "We've been able to reduce application time," says Divittorio. "For example, it's much faster to deliver e-mail server-to-server instead of server-to-desktop. It's easier for employees because they don't have to worry about making updates. And it's easier for me because we have a number of desktops running either XP or Vista, and

"How employees behave is largely outside the control of administrators. Unintentionally, they make it very difficult for administrators to effectively manage and protect IT resources."

ERIC BAIZE, SENIOR DIRECTOR, SECURE INFRASTRUCTURE GROUP, EMC CORPORATION

we can get them all to Windows 7 very efficiently.”

Another benefit is that all software licensing is kept in one place so achieving licensing compliance is simplified. “We can just scan a single server to find all the licenses instead of requiring everyone to keep their computers on so we can search the entire organization,” says Divittorio. “And because there are fewer

storage and processing requirements for employee desktops, we can provision lower-cost devices or allow employees to bring their own machines to work, and still control policy.”

TRUSTING THE CLOUDS OUTSIDE

When cloud services are hosted by a third party, organizations must monitor vendors for security and compliance and

ensure that specific performance metrics for reporting and audit are written into the managed service agreements. Cloud providers should also be able to provide satisfactory answers to the following questions:

How is data protected within your various systems and networks? Do you use two-factor authentication?

What practices do you employ to ensure safe multi-tenancy, authorization, and activity monitoring? Have you implemented fraud-protection technology?

Do you support federated identity management? If not, how are user identities provisioned, validated, managed, and deprovisioned?

May we physically inspect your data centers?

Adds Baize, “Password authentication alone is not sufficient to protect access to external clouds. To be trusted providers, third-party vendors should deploy a cybercrime-aware infrastructure similar to what the financial industry has been doing for years to protect online banking.

“At the same time,” Baize continues, “administrators should insist on the deployment of intelligent cloud storage platforms capable of smart provisioning and data loss protection. If cloud services are multi-tenancy environments, see if your vendor is willing and able to create artificial boundaries around your company’s data.”

Internal or external, servers or desktops, cloud services can free IT administrators from a number of budget issues and day-to-day concerns. Ultimately, though, to ensure security and compliance, administrators must retain control of their IT assets. The good news is that cloud capabilities can help them to do that even better than before.” ■

A portrait of Paul Divittorio, a middle-aged man with short dark hair, wearing a blue button-down shirt. He is smiling slightly and looking directly at the camera. The background is a blurred office interior with vertical lines, possibly from a window or door frame.

“Because there are fewer storage and processing requirements for employee desktops, we can provision lower-cost devices or allow employees to bring their own machines to work, and still control policy.”

PAUL DIVITTORIO, DIRECTOR, IT ENTERPRISE SYSTEMS AND APPLICATION HOSTING ARCHITECTURE, EMC CORPORATION