TechTarget

E-Guide

Managing desktops in modern IT environments

Key desktop management tips and tricks for today's mobile, fast-paced workplace

Desktop admins are being forced to rethink their *management strategies due to the challenges presented by mobility trends and the influx of end-user devices in the workplace. Fortunately, the editors at SearchEnterpriseDesktop.com compiled this exclusive desktop guide to help you get started.*

Inside, explore key insights on improving desktop management, identifying and avoiding hidden costs, and minimizing mobile security risks.

Contents

Top 5 enterprise desktop management tips of the year (so far)

SearchEnterpriseDesktop.com Staff

Enterprise desktop management is an ever-prevalent concern for IT administrators. Doing all the tasks and tracking all the components to make sure your organization is running smoothly and safely can be overwhelming. Here’s a look back at the year's top five enterprise desktop management tips so far to help ease your pain going forward.

5. Desktop backup oversights that can get you into a bind

Enterprise policy and regulatory requirements dictate that desktop backups cover data and applications, but many people still save only locally. When that data gets lost, deleted or stolen, it's difficult to restore. Overcome that risky behavior by backing up critical data, updating desktop management backup policies and periodically checking in with users to ensure that proper backups are taking place.

4. Don't ignore mobile security effects on enterprise desktop management

Mobile devices are the new endpoints, so they must be protected as well as -- or better than -- stationary endpoints. A "good enough" approach may not actually be good enough, so IT needs to consider the complexity and array of

endpoints to really boost enterprise mobile security. Don't just let management and users dictate how mobile devices are secured.

Contents

3. Desktop patch management software features: A checklist
Patch management is a critical function, but the amount of patch management software can be overwhelming. Focus on the most important patch software features, such as centralized control, extensibility, reporting and patch removal, to be sure you're choosing the best tools for successful enterprise desktop management.

2. Desktop audit checklist: Five steps to a successful desktop audit
If you didn't perform a desktop audit after the New Year began, worry not -- the next best time to do one is at the end of Q2. So, as you plan for next year, consider conducting a desktop audit to get your IT house in order. A strong desktop audit checklist can help you manage hardware, software and applications better.

1. Using Windows 7 Task Manager features for Windows memory management
To fix your Windows memory management problems, you must first diagnose how memory is allocated. Certain Task Manager features can cure what ails enterprise desktops by monitoring dynamic memory and detecting memory leaks. Memory analysis can also be completed by the Windows 7 Task Manager.

Identifying the hidden costs of desktop management

By Frank Ohlhorst

Most IT managers are well aware of the upfront expenses of deploying and maintaining enterprise desktops. However, there are several costs that they often overlook or ignore. These hidden expenditures lead to a disparity between how much is budgeted and how much is actually needed. Once revealed, they can be a catalyst for upgrades, enhancements and other projects that help improve return on investment and reduce the total cost of ownership.

Contents

To better understand the hidden cost of desktop management, it's important to first define the obvious expenses. These costs include the purchase price of the desktop, the price of deployment, the price of associated service contracts and the cost of the operating system and desktop applications. These expenses are used to determine a basic cost of ownership and create budgets for desktop refreshes and deployments.

But there are many other costs associated with the typical desktop. They include the following:

- Non-energy-efficient desktops
- Unmanaged desktop use
- Help desk and service requests
- Standalone security products
- Extended desktop life cycles
- Locally stored data

Old desktops

Everyone knows that desktops have electrical costs associated with them. Few people, however, realize how much control they have over energy use. What's more, these expenses are usually associated with facilities and not IT operations, so they are often ignored as an element of desktop management.

Today's desktops offer highly efficient power supplies, low-power-usage CPUs and Energy Star-capable chipsets. As a result, although these desktops may cost more initially, they can save an organization a great deal in the long run. When buying new desktops, the power supplies should have an 80 Plus Platinum Energy Star rating.

Unmanaged desktop use

Most organizations use PCs for less than a third of the business day. But these machines are on 24/7 so they can be managed in the off hours or simply because users don't shut them down.

Contents

Employing desktop management systems with energy-saving technologies -- such as automatically shutting down desktops, placing PCs in hibernation or sleep mode when not actively used, or waking PCs up for maintenance -- can save an organization a significant amount of money. What's more, the additional costs of management can be quickly offset by the power savings realized.

Help desk requests

In some cases, help desk and service requests related to faulty components or misuse can be mitigated. On the other hand, an improved management system and more resilient or secure equipment may be a more cost-effective option.

Standalone security products

Many organizations have moved to centrally managed, network-based security, but some still rely on standalone tools that need to be installed on desktops. In these cases, desktop security can be expensive, especially if it entails installation and maintenance by IT. A centralized security product can incorporate additional security features such as data leakage protection and compliance controls. It can also can reduce operational expenses and prevent unforeseen expenses created by security problems.

Extending desktop lifecycles

Most IT departments focus on the perceived savings of delaying a desktop refresh cycle. In the short term, this reduces capital expenditures (no desktop purchases) and operational expenditures (no deployment costs). But when you factor in the costs of replacement parts as warranties expire, extending service contracts, more frequent support requests, traditional software and application maintenance, and lost productivity, the savings is null.

Locally stored data

To maintain desktop integrity and properly support end users, local data must be backed up and be readily available for restoration. This task requires significant resources, including protected storage space, a mechanism for backup and a management element. In addition, users, IT workers and help desk personnel need to know how to back up and restore data, what data is

appropriate to store locally, and how that data should be managed. You may also have to address concerns about regulatory compliance, data leakage and the migration of data to new platforms.

These concerns are often ignored because of the complexities of data backup and integrating technologies. To offset the costs associated with locally stored data, new technologies can be deployed to automate the process, eliminate the capability to store data locally or offer a hybrid approach where data is replicated.

Many problems can arise from the hidden costs of desktop management. But if you consider these often overlooked or ignored expenses, you can come up with a plan to mitigate these costs and hopefully drive up the value of technology -- and the IT department.

Contents

Don't ignore mobile security effects on enterprise desktop management

By Kevin Beaver

Mobile is the new endpoint. But how can IT administrators guarantee mobile security? Many people claim that their workstations are locked down, but that's only half of the battle. From personal firewalls to antivirus to privilege management to data loss prevention -- the technologies are in place, and policies and processes exist to ensure that those endpoints are secure. The problem is that we still seem to be ignoring all of the mobile devices floating around the enterprise.

In any organization, an untold number of mobile endpoints is in use at any given time. These systems represent literally hundreds, if not thousands, of islands of information that likely fall outside of traditional endpoint controls. Asking yourself a few simple questions can help bring the issue to light and, therefore, increase mobile security:

1. **Are employees, contractors and consultants using their phones and tablets for business purposes?** Even if you think they're not,

odds are good that they are -- somehow, some way. Thus, mobile security should be established to protect any enterprise information from being accessed via those mobile endpoints.

2. **What mobile platforms are being used?** It's easy to assume that only Apple or only BlackBerry devices are in use. What about Android-based systems? Symbian? What about others you've never even heard of but that can still access and store sensitive data that your business can't afford to have compromised?

3. **What applications are being used? What data is being accessed from and stored on mobile endpoints?** Odds are good that people are using/accessing email, the virtual private network, intranet portals, customer relationship management systems, PDF files, spreadsheets and the like -- all from their mobile devices. They're sitting on users' desks, in pants pockets and in purses waiting to be exploited.

4. **What endpoint controls are installed across all mobile endpoints?** This is where things get tricky -- and ugly. Some may have passwords. Some may use encryption. Some may be getting backed up. Still, you probably don't have nearly the security controls on your mobile devices that you do on your desktops.

I'd venture to guess that practically any given business has at least a handful of mobile endpoints with a severe lack of security controls that you wouldn't fathom being absent from any given laptop or desktop computer. The data breach headlines and studies confirm this.

For example, the 2011 Ponemon and ID Experts' Second Annual Benchmark Study on Patient Privacy & Data Security found that 81% of health care organizations use mobile devices to collect, store and/or transmit some form of protected health information, while only 51% are actually doing anything to protect these devices. I suspect that of the devices being "protected," many of them can still be exploited because of weak passwords, lack of encryption, mishandled backups and so on.

Contents

Contents

So, why aren't mobile endpoints getting the protection they deserve? Is it because they're so small -- out of sight and out of mind? Maybe it's because they're so pervasive? Perhaps it's because they're personally owned, and management wouldn't dare tell people what they can and can't do with their own devices?

Corporate IT can't afford to ignore the complexity of endpoints and the importance of mobile security. We shouldn't let our guard down with a "good enough" approach -- good enough hardly ever is -- nor can we afford to let management and users continue to dictate how mobile devices will be secured. This is why you must ensure that mobile endpoints get the same level of protection (or better) than traditional workstations.

Mobile devices have redefined IT's responsibilities, not only in how we manage our enterprise desktops but also as they relate to overall compliance and information risk management. The question is: What do you plan to do about your mobile security?

Contents

Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

SearchEnterpriseDesktop

SearchMobileComputing