The New Windows Security

Achieving PC Lockdown without User Backlash in Five Easy Steps

Written by Dell Software

Abstract

Users are accustomed to being in control of their PCs, laptops and mobile devices at home, and they often demand similar flexibility at work. But users with too much power sometimes get themselves, and their organizations, into trouble. All too often, without meaning to, they introduce security risks by falling prey to phishing schemes, risk fiscal exposure by violating software licenses and generate help desk calls by misconfiguring applications.

The key to success is achieving the right level of control. This white paper explains five key steps that will enable you to ensure that users get the most benefit from today's information technologies, while also safeguarding the content and configuration of their systems.

Introduction

Remember the good old days, when an anti-malware solution was "good enough" PC security? Life was easier back then. IT problems were simpler, and PCs seemed easier to maintain: Grant administrator privileges to a troublesome user, and his or her issues just melted away.

Those days are over now. Managing that same network in today's world requires greater effort and smarter solutions. Throwing administrator privileges at a user issue is no longer the everyday practice; it's a resume-producing event.

Today's Windows security requires locking down PCs and their installed applications in new and unexpected places. Unapproved apps must be blocked from execution, and administrator privileges must be removed—all without impacting users.

Makes you miss the old days, doesn't it?

Figure 1. Blocking illegitimate applications is critical to reducing help desk calls, damage from malware and costly license violations.

Block unapproved applications from ever executing.

Thankfully, new approaches are evolving to meet IT's new demands. One can't simply lock down a PC by eliminating administrator rights and blocking applications—not impacting users means treading lightly. You'll need intelligent tools, a gentle touch and just the right amount of communication to achieve modern-day PC lockdown with user satisfaction.

Concerned about how to get there? Consider these five steps as your guide for PC lockdown success:

Step 1: Targeted approval

Poke around any uncontrolled PC environment, and you'll find a nightmare of legitimate, illegitimate and quasi-legitimate applications. That menagerie of known and unknown is a big contributor to excessive help desk calls, unexpected malware intrusion and costly license violations.

The solution is to get rid of the software. But with desktops and laptops spread across all manner of places, merely finding those apps is no trivial task. Getting an accurate view of all the applications and then uninstalling the dozens or hundreds of individual apps on individual devices could take weeks of weekends and late nights.

Here's a better idea: Block unapproved applications from ever executing.

An application is little more than a set of files that get executed by a PC's processor. Prevent those files from executing, and they devolve from dangerous application to mere wasted disk space.

A smartly designed management solution will help you inventory every application—legitimate or not— to create a heads-up display of your environment. Check off items in the list to approve the apps your business deems appropriate, and everything else becomes no longer a problem.

Step 2: Configuration lockdown

Even legitimate applications can have illegitimate configurations. Client apps need server connections. Line of business apps require complex settings. A problematic app includes that one checkbox that explodes everything every time it gets enabled.

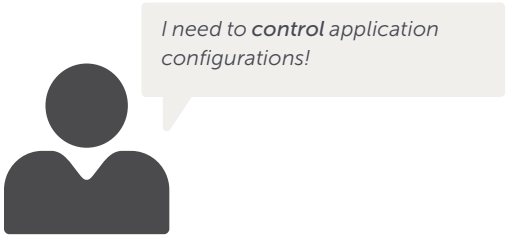

Figure 2. Relying on users to correctly configure applications—even if you provide instructions—is rarely a winning approach.

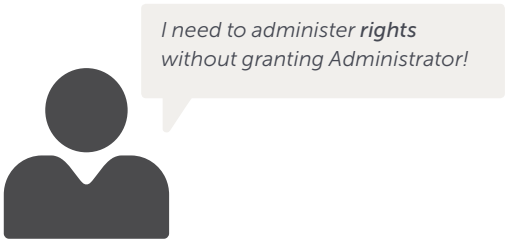

Figure 3. Some applications require administrative rights to run, but granting full Administrator rights to their users creates serious problems.

In the past, IT has given users instruction manuals to guide them toward correct configurations. We've also burned countless hours picking up the pieces when users can't follow them. An incorrectly configured application is no better than one that's broken or missing, but relying on users is rarely a winning approach.

Here's a better idea: Centrally control app configurations for the user.

Smart IT pros know that application configurations are easily found if you look in the right places. Checking a box changes a 0 to a 1 in a specific registry location. An app's server connection string is actually stored in some file on disk. The right solution lets you turn a written instruction guide into an enforceable policy that guarantees every app always works.

Step 3: Selective elevation

Administrator privileges are Windows' necessary evil. In the right places, its privileges allow trusted people to solve problems, install software and maintain a healthy Windows experience. In the wrong places, Administrator becomes the source of an ever-growing problem. Users with administrative rights install software they shouldn't. They turn off firewalls and disable anti-malware. They misconfigure network settings so badly they'll never find their home drive again.

Administrator's even bigger concern are the applications that require its presence. Unfortunately, you likely have some poorly written or ancient—but somehow necessary—applications that mandate administrative rights to run. In the past, the only option was to grant full Administrator rights to that application's user. Doing so solved a small problem by creating a much larger one.

Here's a better idea: Grant administrative rights to the application, not the user.

Windows by itself has but a single throttle for administrative rights: You either have them, or you don't. However, administrative rights needn't be binary when they're applied not to users but to their applications. Doing so creates a granularly controllable environment of selective elevation, where problem apps get the administrative access they need. And users don't.

The right privilege management solution will incorporate selective elevation into its inventory and approval functions. With it, if you can inventory and approve an app, you can elevate it.

Grant administrative rights to the application, not the user.

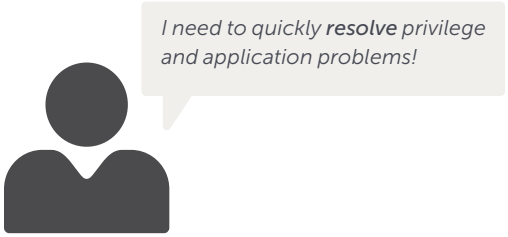

Figure 4. A good lockdown solution not only alerts users when they violate a policy, but also enables them to easily file a service request that can be quickly resolved.

Give users installation freedom that's tightly controlled.

Step 4: Integrated service desk

In a perfect world, every PC lockdown activity succeeds with zero user impact. Application access is perfectly scoped to user roles, and elevations are accurately deployed to needy apps. In all but the tiniest of Windows environments, that mapping is nearly impossible to predict on the first try.

Windows environments are also changing environments. New business ventures create new users and roles, which themselves require new accesses on a seemingly constant basis.

The traditional approach to managing IT change usually starts with a service desk call. A user communicates his or her issue with a service desk person, who translates it into a work order, which gets interpreted by a field technician, who usually needs to contact the user directly to resolve the request.

Here's a better idea: Integrate service requests into the lockdown solution.

A lockdown solution will at some point alert users that it has taken action. That alert can be a one-way notification that a policy has been enforced. A smartly designed solution, on the other hand, can make better use of the experience. Such a solution might alert the user that he or she has broken a policy, while at the same time offering the opportunity to file a service request. Those service requests can be fulfilled from the same console, unifying the experience and eliminating the multiple steps that prolong resolution and reduce user satisfaction.

Step 5: User self-service

Many IT administrators fear self-service; it conjures up the same nightmares that PC lockdown attempts to confront. Yet many IT pros forget that user self-service has been around since Windows' earliest days. Peek through early Windows versions and you'll find a Control Panel icon titled Add/Remove Programs. For a generation we've used that icon for removing applications—but nearly never for adding them.

Here's a better idea: Give users installation freedom that's tightly controlled.

Figure 5. Once applications are white-listed, configurations are controlled and elevations are appropriately targeted, the only step left is to let users do the work of installing software.

The addition of self-service works best as a final step in the PC lockdown activity. Once applications are white-listed, configurations are controlled and elevations are appropriately targeted, the only step left is to let users do the work. With smartly designed installation packages and the selective elevation that a good privilege management solution facilitates, installing software becomes just another daily activity—with no need for constant attention from IT.

Tools for a holistic approach to PC and user lockdown

Smart IT shops realize that Windows alone can't accomplish these steps. They know they need additional tools that facilitate PC lockdown and privilege management activities. A good solution must seamlessly slipstream into a running production environment, monitor activities as it builds its inventory, support flexible policies and expose an easy-to-implement interface that assures minimal user impact. Equally important is an integrated systems management infrastructure: tools designed to support an integrated, collaborative approach to security and systems management can help IT departments manage security effectively.

A complete solution: Dell KACE plus Desktop Authority Management Suite

PC lockdown capabilities such as those included in Dell KACE™ K1000 Management Appliance can play a critical role, and coupled with tools that control user privileges on a granular level, like Dell™ Desktop Authority™ Management Suite, extends PC lockdown to user lockdown. Together, the K1000 and Desktop Authority Management Suite offer a range of security options to help you control access and maintain endpoint security, and they are easy for administrators of all skill levels to learn and use.

The K1000 provides comprehensive and easy-to-use configuration policy management and enforcement for Windows, Mac and Linux systems. The K1000 can create and enforce reliable configurations, and it provides a complete audit trail by tracking edits to endpoint configurations, including the who, what and when of each addition, deletion or change. These capabilities are essential for satisfying regulatory compliance requirements and for determining when configurations are exposing your organization.

As outlined above, the basis of any good configuration and lockdown strategy is to know what is on your network—legitimate or not. Utilizing a cloud-based software catalog of more than 110 million unique executable files (that is updated nightly), the K1000 provides deep interrogation of all endpoints for an accurate view of all software installed across a network. Moreover, it enables the administrator to remotely remove all unapproved installations quickly and easily from a central location.

The appliance's integrated self-service user portal enables organizations to publish approved applications, license keys, files and scripts so users can install software or configure their systems—regardless of whether they have local administration rights on their PC.

In addition, the K1000 offers service desk functionality that merges seamlessly with the systems management console, enabling IT staff to view and address user requests for privileges, all from a single location.

Desktop Authority Management Suite extends K1000 configuration management with deep configuration capabilities for Windows systems. By providing administrators with granular control over system settings, Desktop Authority Management Suite enables IT administrators to easily create a customized, secure and efficient Windows environment tailored to each user and machine.

The basis of any good configuration strategy is to know what is on your network - legitimate or not.

With Desktop Authority Management Suite, users can customize their computers the way they want, but administrators retain centralized control over key settings. The solution enables administrators to selectively elevate user rights, thereby eliminating the need for local admin rights that allow users to install malware or unapproved software, copy data to flash drives, and leave computers unlocked and unattended. This approach reduces risk to computers and data without impacting user productivity.

Conclusion

PC lockdown is a balancing act: organizations need to give users the tools and flexibility they need to do their jobs while avoiding the security, compliance and other risks that local administrative rights introduce. Implementing the best practices explored in this white paper requires the right tools. With the K1000 Management Appliance and Desktop Authority Management Suite, enterprises can maximize user productivity while also maintaining centralized control over security policies.

With the K1000 Management Appliance and Desktop Authority Management Suite, enterprises can maximize user productivity while also maintaining centralized control over security policies.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.