BeyondTrust Report

Legacy Applications and Least Privilege Access Management

~ Legacy applications reveal desktop security "Wild West"

January 2011

Abstract

In an enterprise Windows' desktop environment, whether a company has 100 or 10,000 seats, the challenge of managing access is fraught with difficulty.

In a study conducted by BeyondTrust, this report details the results of a survey of 185 IT Administrators and Help Desk Operatives who are collectively responsible for over 250,000 individual Windows' desktops, in EMEA and North America. This report details their experiences with legacy applications in relation to their ability to effectively elevate access to the networks they manage.

beyondtrust®
privilege. made simple

www.beyondtrust.com

BeyondTrust – Corporate Headquarters
2173 Salk Avenue
Carlsbad, California 92008
Phone: +1 800-234-9072

Table of Contents

Executive Summary

Whenever we hear the phrase "Wild West", the first words that come to mind are old, unsecure, and vulnerable. Any old western featuring Clint Eastwood or John Wayne depicts all of these descriptions. And coincidentally "Wild West" provides the perfect analogy for the way an enterprise's remaining legacy infrastructure interfaces with a Windows desktops environment.

Though often overlooked, every IT Administrator must face the challenge of managing legacy applications that simply will not run unless individual desktops are configured for administrator access. Indeed, in an enterprise Windows' desktop environment, whether a company has 100 or 10,000 seats, the challenge of managing access is fraught with difficulty.

Currently, there are two options available to administrators:

Option 1: **Adopt best practice of removing administrative rights.**
Result: Overwhelms help desk with support calls and hampers productivity.

Option 2: **Grant users administrative privileges.**
Result: Can provide access points for malware, hackers, insider threats; and, the less reported though still equally damaging, 'fat fingered' unintentional error.

What has not been clear until now is that IT Administrators and Helpdesk Operatives that choose option 2 for the sake of productivity, and thus leave their desktop environment unnecessarily exposed, are not being cavalier or necessarily neglectful. The fact is they are left with no other choice because without their legacy applications running efficiently, productivity would come to a halt.

Legacy applications return administrators to the "Wild West".

Increasingly difficult to thwart, attacks by people with legitimate access to an organization's computers, devices and networks represent a growing problem across the globe. These insider threats frustrate Admins, auditors and managers who lack the resources to properly identify them, oversee their behavior and protect mission-critical information technology (IT) assets from the misuse of privilege.

In a study conducted by BeyondTrust, this report details the results of a survey of 185 IT Administrators and Help Desk Operatives who are collectively responsible for over 250,000 individual Windows' desktops, in EMEA and North America.

This report details their experiences with legacy applications in relation to their ability to effectively elevate access to the networks they manage.

About the Data Collection and Analysis

To compile this report, we first consulted over 30 sales representatives from our reseller network. They each indicated how often legacy applications were cited as a desktop 'management headache' by the IT managers and Network operatives with whom they spoke.

This was interesting because it underlined that poor privileged access management on the desktop, and the inherent risks to network security this poses, is not always the result of neglect or lack of foresight.

Instead it suggested that those charged with managing desktop access are forced to act in the way they do – either giving everyone full access to the network regardless of job description, or locking the network and productivity down - because the company relies on one or more essential legacy applications which only run on Windows if users are given full administrator, or super user status.

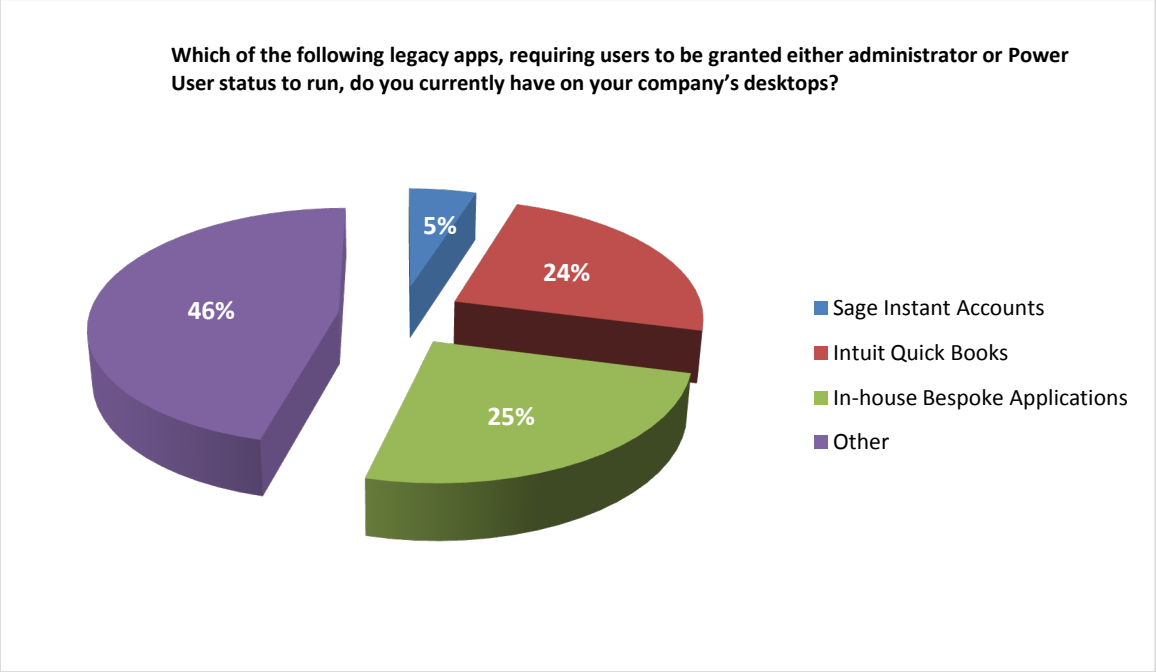
To establish whether this anecdotal evidence was uniform across organizations of different sizes, BeyondTrust polled 185 IT administrators and Helpdesk operatives across the UK and North America.

Our questions sought to establish what kind of legacy application was responsible for forcing the enterprise to elevate user privileges on the desktop, as well as how much time they spent solving problems caused by the impact of over privileging users.

Then, we also polled 40 IT analysts and consultants as a control group.

Our rationale here was that, given their position within an organization or as a sub contractor, they would provide an alternative and independent viewpoint which would either verify our initial findings or provide an alternative viewpoint.

Analysis of IT Administrator & Help Desk Operative Data



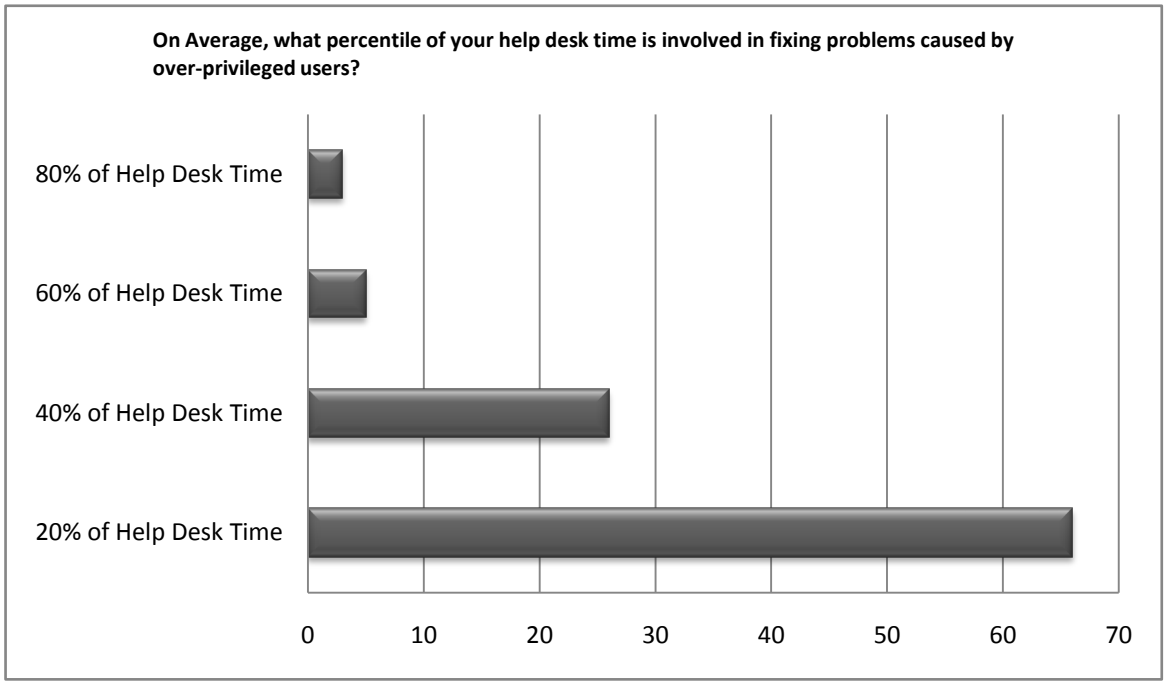
Key Findings

1. In organizations with more than 2500 desktops, it was in-house bespoke applications (51% of respondents), and a range of 'other legacy apps' (40%) which force IT Admins to elevate privileges to Administrator or Super User status.

2. In enterprises with fewer than 2500 desktops it was Intuit QuickBooks (33% of respondents), and again 'other legacy apps' (50%) which most often forced IT Administrators to elevate network access privileges to the more risky Administrator or Super User status.

   Survey respondents were invited to name which legacy app they were nominating when selecting 'Other,' revealing over 50 different apps that were nominated, with a number citing 'too many to mention.'

   This offers a revealing insight into the state of desktops today – i.e. they are littered with applications, each requiring different configuration settings for different users, making effective access management practically impossible.



Key Findings

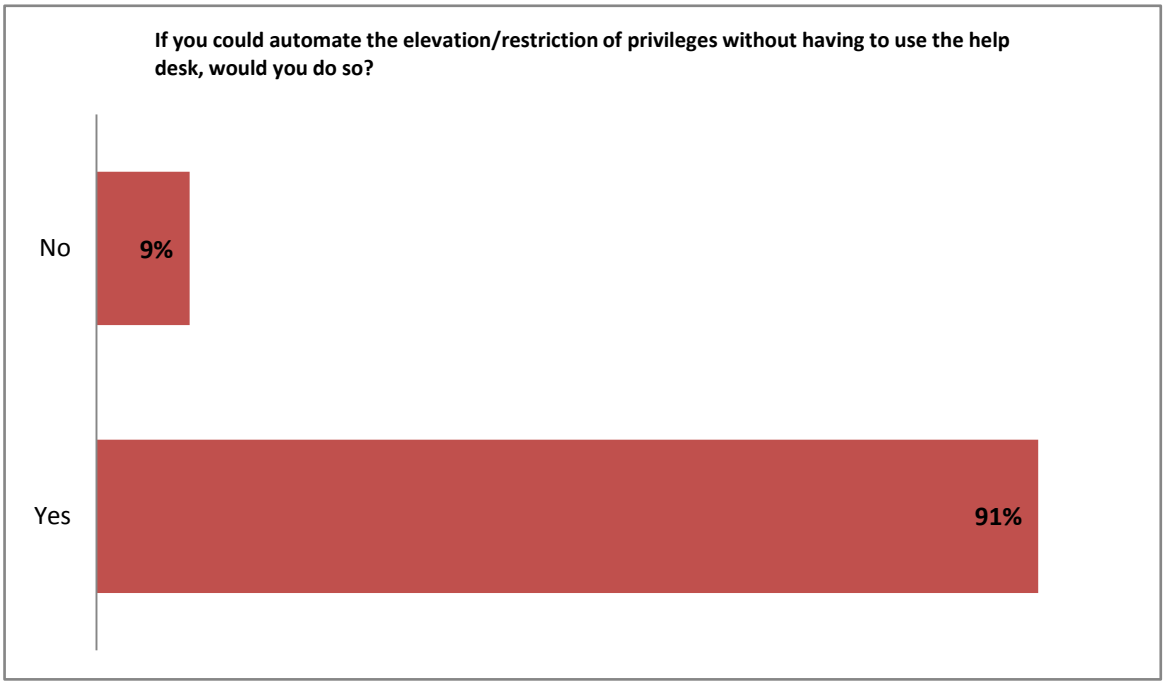
1. IT Admins and Help Desk personnel say they spend more than 1/4 of their time fixing problems caused by over-privileged users.

2. The average amount of time spent fixing these problems was 29% (the vast majority reported spending about 20% of their time).

3. The same results show that 1/3 of IT Admins and Help Desk personnel spend at least 40% of their time fixing these problems... some (a small handful) spend 80% of their time fixing these problems.

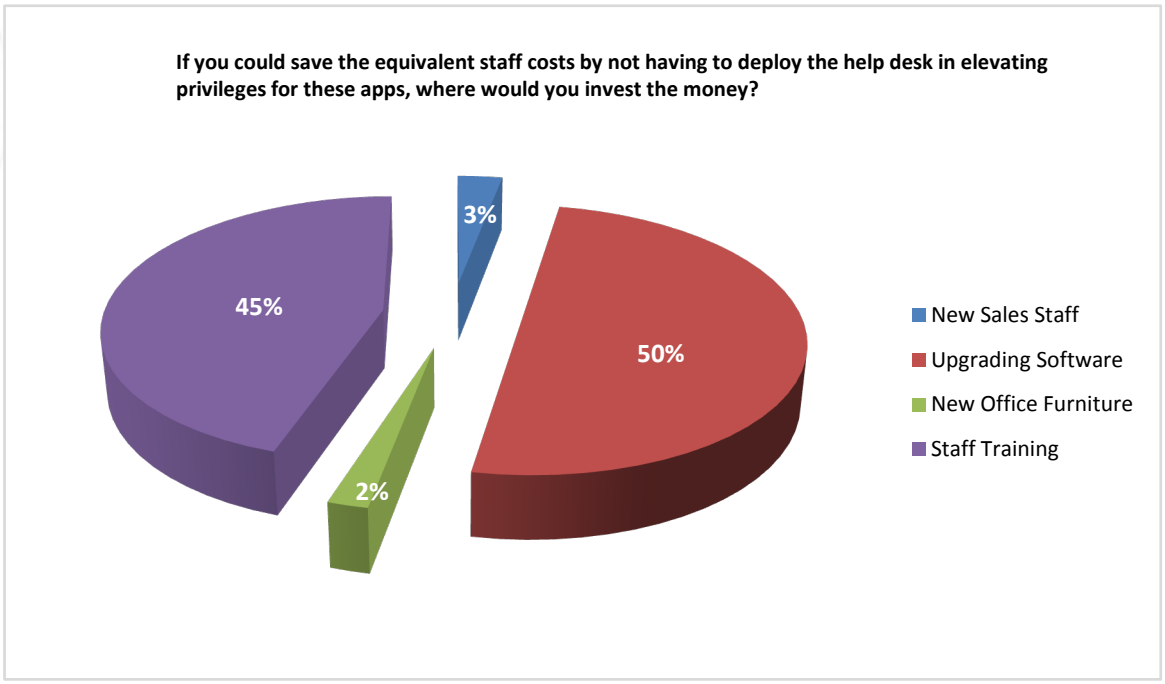
Gartner's recent report, ***Organizations That Unlock PCs Unnecessarily Will Face High Costs,*** shows that when a user is standard user, the amount of IT labor needed for technical support is 24% or $1200 pa per desktop less than when a desktop user is an administrator.[1]

[1] Gartner, Inc Michael A. Silver, Ronni J. Colville, Dec.19, 2008.



Key Findings

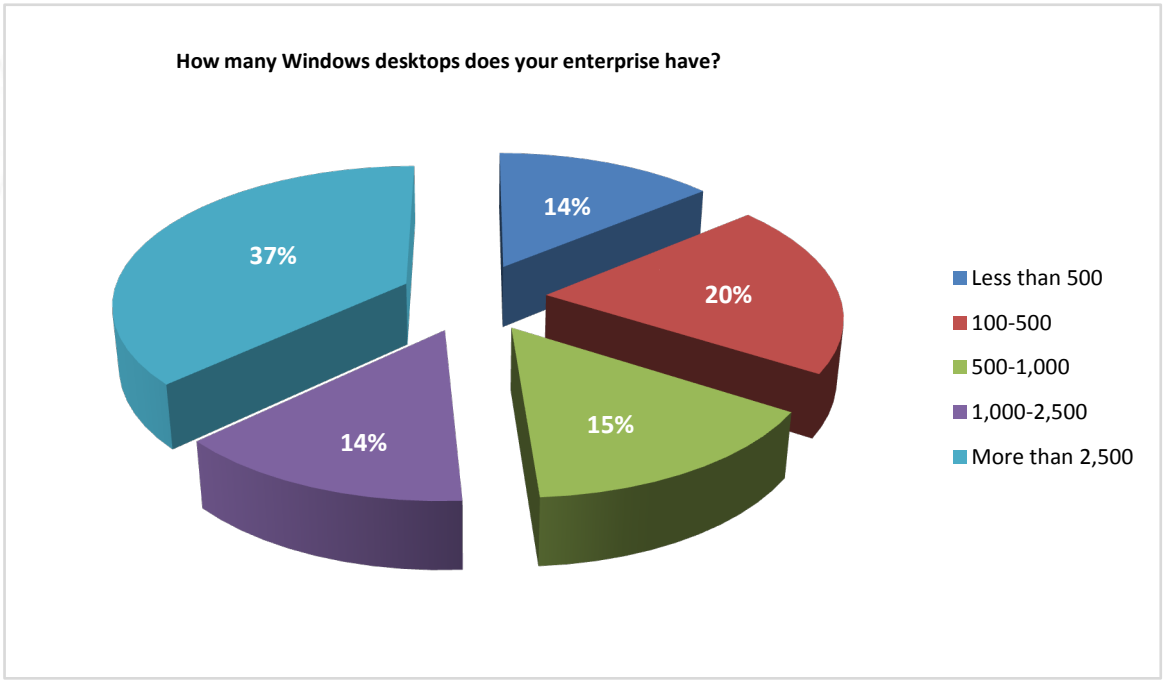
1. 90% of IT Admins and Help Desk personnel who admit to experiencing the headache of managing the impact of legacy apps would welcome help with automating the process of dealing with over-privileged users.



Key Findings

1. Their choice of what to do with the money they would save on help desk costs is revealing. Overwhelmingly, they would invest the savings on either training staff or upgrading software.

   In essence, the experience of IT Administrators and Help Desk operatives are legion; they want to spend more time improving user experience, with better training and software, and less time fighting fires.



Key Findings

1. What is revealing here is that with the exception of the use of Intuit QuickBooks as the prime suspect legacy application, in organizations with more than 2500 desktops the experience of all IT Administrators and Help Desk Operatives is uniform.

2. Legacy applications make their lives difficult and consume a disproportionate amount of their time, regardless of the size of the organization.

3. This points to the ubiquity of Windows and its inherent problems in elevating privileged access based on company policy rather than the requirements of individual applications.

Independent IT Analysts and Consultant Control Group

We established this control group to provide a check and balance to the data provided by the IT Administrators and Help Desk Operatives.

While the latter are arguably closer to the 'coal face,' the former has a potentially more objective view given the number of organizations they encounter in their work. The group comprised both general IT and security analysts or consultants.

The results provided by this control group were surprisingly consistent with the main group of respondents, and in particular the breakdown of legacy app type (question 1) was almost identical.

The marginal differences in their responses were as follows:

- Question 2: 80% of analysts and consultants suggested that 20% of help desk time was devoted to managing user privileges caused by legacy apps, compared with 66% of IT Administrators and Help Desk operatives.

- Question 3: Only 80% of analysts and consultants said they would automate the elevation of privileges if they could. Presumably, those that viewed this solution with caution might want to provide a solution of their own.

Why Administrators View the Desktop as the "Network Wild West"

As cited above, survey respondents were invited to name which legacy applications they were nominating when selecting 'Other.' Revealing over 50 different applications, notable selections include:

- A number of respondents cited 'too many to mention.'
- Old Mainframe applications.
- Software used for running an office (printer drivers) or the desktop itself (defragmenter).
- Third party point of sale software provided to retailers.
- Adobe and Flash software.
- Respondents from industries such as oil, automotive, and chemical cited technical applications which, although used by a handful of employees, still enforce the entire desktop to be set to administrator or super user status.
- Applications downloaded by individual employees from the web to help them do their job better: for example, financial trading software.
- Applications downloaded and installed by employees for their own entertainment, including: iPhone applications, and in one instance, a Golf Course Game Application - many of which could violate security and compliance regulations.

This paints a revealing picture of enterprise desktop environments today: they are littered with applications, each of which requires different configuration settings for different users, and makes effective access management practically impossible.

Indeed, is it any wonder that today IT Admins consider desktops the "Wild West," not just because of the overwhelm of managing access to multiple applications, but also because they never know what they were going to encounter on a user's workstation.

One desktop manager, reported: "We have limited control on what the end user can install and change on a desktop, and in many cases we have limited awareness of changes being made. In most cases it's too late if a user installs malware and adware, leaving our desktop resources left fire-fighting problems."

Summary

Far too often, it's been the assumption that that IT Administrators and Helpdesk Operatives are being cavalier or unnecessarily neglectful, when they set desktops to run on administrator status, - 'the choice for productivity' - thus leaving their desktop environment unnecessarily exposed.

As this report shows, the experience is quite the contrary. They are not neglectful. They have an impossible task. One that leaves them consistently on the back foot and unable to either finance or execute a desire to make the desktop environments they manage a more efficient place.

It is true that more recent editions of both Sage and Intuit, two of the programs cited here, will run on Power User status, but in terms of securing the desktop from either accidental or intentional harm caused by over privileged users, is like trying to shut the door and instead deciding to leave it ajar slightly.

It is important to realize the fact that insiders are not just employees.

Today, insiders also include contractors, business partners, auditors, customers... And, it is important to recognize that not all insider attacks are done intentionally. The misuse of privilege in an organization can result in accidental and indirect harm as well as intentional.

Start 2011 off by understanding best practices for privilege identity management and formulating plans to implement a least privilege solution:

Secure Windows, legacy applications and eliminate Admin rights:

PowerBroker Desktops enables organizations to remove administrator rights and allow end-users to run all required Windows applications, processes and ActiveX controls. By eliminating the need to grant admin rights to end-users, IT departments can extend Group Policy to create a more secure, compliant and productive environment.

About BeyondTrust

BeyondTrust is the global leader in privilege authorization management, access control and security solutions for virtualization and cloud computing environments. BeyondTrust empowers IT governance to strengthen security, improve productivity, drive compliance and reduce expense. The company's products eliminate the risk of intentional, accidental and indirect misuse of privileges on desktops and servers in heterogeneous IT systems.

With more than 25 years of global success, BeyondTrust is the pioneer of Privileged Identity Management (PIM) solutions for heterogeneous IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises.

Customers include eight of the world's 10 largest banks, seven of the world's 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities.

The company is privately held, and headquartered in Carlsbad, California with offices in Los Angeles, the Greater Boston area, Washington DC, as well as EMEA offices in London, UK.

