White Paper

Windows Endpoint Security is Least Privilege and Data Loss Prevention

by Derek Melber (MCSE, MVP)

Abstract

The networks that we manage and work in today is much different from the networks we worked with even 10 years ago. Mainly because technology, hardware, and software have become more advanced. Unfortunately, so have viruses, malware, spyware, and end-users. With the influx of successful attacks on corporate networks, not to mention the theft and publication of intellectual property, the need for endpoint security is now at an all time high. What is important to note is that the old school philosophy of protecting the endpoint with a perimeter firewall and written security policy is no longer valid. This white paper discusses the sophistication of strategy and approach that enterprises must take to protect endpoints for a standard corporate network.

beyondtrust
securing the perimeter within

www.beyondtrust.com

BeyondTrust
2173 Salk Avenue
Carlsbad, California 92008

Phone: +1 818-575-4000

Table of Contents

Executive Summary

The networks that we manage and work in today is much different from the networks we worked with even 10 years ago. Mainly because technology, hardware, and software have become more advanced. Unfortunately, so have viruses, malware, spyware, and end-users. With the influx of successful attacks on corporate networks, not to mention the theft and publication of intellectual property, the need for endpoint security is now at an all time high. It is important to note that the old school philosophy of protecting the endpoint with a perimeter firewall and written security policy is no longer valid. To protect endpoints for the typical corporate network today you need to have a more sophisticated approach.

First, your endpoint security must begin with a least privilege approach. Least privilege will help your users protect themselves by removing their local administrative privileges. When a user is configured to run as a local administrator, there are too many errant and malicious actions that can be performed on the endpoint. In this scenario, IT loses full control of endpoints where the user is a local administrator, not to mention the damage that can be done to the network when a virus or other malicious code infiltrates other desktops and servers through an endpoint where the user is running with local administrative privileges. The most difficult aspect of least privilege is still allowing users to run and install all approved applications and OS features while running with least privilege.

Second, all endpoints must be managed to control their access to data. For most organizations today, nearly all intellectual property, financials, human resources, credit card information, social security numbers, etc. are stored as data on some server in the organization. If any of this data is compromised by becoming public, being sent to competitors, emailed outside of the organization illegally, or accessed from a lost or stolen laptop or tablet, the company will lose millions, if not billions, of dollars. All company critical data needs to be monitored, tracked, and protected from any possible leaks outside of the organization.

Finally, it is important to understand that least privilege does not protect data against leaks, and protecting data against leaks does not solve least privilege. If either of these solutions for your endpoint security is left out, you are exposing the entire network to potential infiltration of malicious software or exposure of intellectual property to a Wiki site.

Least Privilege Defined

The concept and term “least privilege” is not new, nor is the ideal solution for solving it. However, with the heightened need to secure endpoints, more and more organizations are looking to solve least privilege to protect the enterprise. The term least privilege is important, as it defines a very special situation that many people are trying to solve, yet do not understand. If we look at the true definition, as defined by the United States Department of Defense (DOD), we can decrypt the intent of the definition.

"[The Principle of Least Privilege] requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use."

Department of Defense (DOD-5200.28-STD), also known as the orange book

If we break down what is included in this definition, we can clearly see it is not nearly as complicated as it seems. The following are key aspects of the definition of least privilege:

1. Access should be the most restrictive set of privilege, which in most cases is standard user. There are some installations, applications, OS features, etc which require local administrative privileges, but most do not require this level of privilege.
2. There is nothing that states that the user cannot run an authorized task with elevated privileges, only that the privilege be most restrictive.
3. Authorized tasks can be confusing in this context, but the intention is that only authorized and required tasks can be run at all. When run, those tasks need to be run with the most restrictive privileges.

You can clearly see that the definition is not very restrictive with what can be run and what level it can be run at. This is good, due to the situation that many software vendors have left corporations to deal with applications that are poorly built and require local administrative privileges.

The definition also begs the question: "What would an authorized task include?" From my perspective for endpoint security, that is a very important question. It should also be an important question for you, as you try to develop a least privilege and endpoint security strategy. There are four main areas that authorized tasks fall into for endpoints:

Installing applications

Installing applications would encompass installing nearly any application locally or via the network. For your static users, this means from a CD/DVD, network, download then install, etc. For your mobile users, it would mean they might need to install an application from the customer network or remoting back into the corporate network. I tend to have customers force testing and approval for any Internet based installations, as these can contain viruses or worms.

Running applications

Running applications would include both off-the-shelf and homegrown applications. In essence, it does not matter where you got the application, if it is an approved task (application), then it should be included in the list. For most companies the criteria are "if the application makes the company money, then it is required and approved."

Installing ActiveX Controls

This includes installing any ActiveX Control from the Internet or an Intranet. The only privileges that are allowed to install most ActiveX Controls are local administrators. With the continued use of Corporate Intranets and many companies moving to the "cloud", ActiveX Controls are a vital part of nearly every company.

Running OS Features

OS features includes any OS feature that is required for the productivity of a user, to improve computer performance, monitor of the computer, to maintenance maintain of the computer, etc. Users are often told to defragment their hard drive, alter Control Panel settings when mobile, etc. If running as a mobile user on Windows XP and a mobile user, installing a local printer at a remote location is nearly essential. If it is an authorized OS feature, then it needs to be run successfully by a standard user running with least privileges.

The Need for Least Privilege

Every administrator understands the need for least privilege for endpoints. Even if the administrator runs with local administrative privileges, that admin is fully aware of the possible consequences that can arise from such a decision. Therefore, the need for least privilege is relevant, known, and indisputable.

There are others who are not convinced that the need for least privilege is so apparent and consider it unimportant. Many who feel this way are typically living their lives with the thought of "I have not experienced any problems, so there is obviously no risk," or worse yet they feel "we don't have the budget for solving a problem that is not causing any issues." These mindsets have cost more than a few Fortune 100 companies millions of dollars in IT hours and loss of reputation.

It is clear that least privilege is needed and required for even the smallest of companies. Without least privilege, users can cause significant problems for their desktop, as well as for the entire enterprise. To get a small glimpse of what can occur when users are granted local administrative privileges; the following gives you an idea.

Complete Inability to Control Endpoint

When a user is granted local administrative privileges, that user can perform any task they desire on the desktop. Even with the most sophisticated and complex array of Group Policy and other management settings being delivered from Active Directory and the network, the local user can subvert the settings with ease. The easiest way the user can undermine the network administrator's attempts at control is to simply remove the endpoint from the domain. In essence, the endpoint now becomes a rogue desktop in the environment, with little to no management over this device. Registry modifications, installations of malicious software, reduction of security settings, poor Internet Explorer configurations can all lead to large problems for the entire network.

Infestation of Viruses, Malware, and Spyware

Nearly every computer and endpoint in the world has been attacked by a virus, malware, or spyware at some time in its life. In most cases, the infection is neutral and goes on without any issues. However, there are some malicious applications that cause complete destruction of the endpoint and can even distribute itself to other computers on the network.

There are many reasons that malicious applications enter the enterprise, but one of the easiest ways to eliminate more than 90 percent of all malicious applications from infecting endpoints is to not have the user running as a local administrator.

The majority of all viruses, malware, and spyware require local administrative privileges to install and run. Without this level of access, they instantly become insignificant.

Increased Help Desk and ROI Costs

There has been a direct link to the cost of corporate helpdesks to that of users being local administrators on their desktop. (Gartner, Inc., "Organizations That Unlock PCs Unnecessarily Will Face High Costs," Michael A. Silver, Ronni J. Colville, Dec.19, 2008.) This comes as no surprise to anyone in the IT industry that has been responsible for supporting end point desktops in any capacity. When a user is given the ability to perform actions they are not authorized to perform, they will perform these tasks regularly. Most cases are errant mistakes, but others can be malicious in nature and can be eliminated by removing the user from being a local administrator. Once users on end points are reduced to least privilege users, the helpdesk calls will reduce immediately and the overall ROI for each end point will increase.

License Management

The Internet has made access to pirated and illegal software all too convenient. When a user has access to the Internet, at work and at home, illegal applications and software will be downloaded. Once the user realizes that these applications and software can be installed on their corporate desktop, either directly from the corporate network or from home via a USB thumb drive, because they are local administrators, the software will be installed.

Requirements for Least Privilege for Endpoints

In order to meet the requirements for least privilege for endpoints, there are certain events that must occur and specific environments that must be achieved in order for success. There are some that will claim that not all of these requirements need to be met, but if any of these are left out, it makes it extremely difficult to implement a full least privilege solution into an existing Active Directory environment.

Standard User Privileges at the Endpoint

Every user in the environment should be running without local administrative privileges. This means that the user should not have credentials for any account that has membership in the local Administrators group on the endpoint. This also means that the user cannot have any credentials that can be used with a RunAs or Windows Vista/7 User Account Control scenario to elevate tasks with alternate

credentials. PowerBroker Desktops Windows Edition provides the ideal solution for users to run with standard user privileges at the endpoint. PowerBroker Desktops Windows Edition provides the following benefits:

- All tasks are run under the logged on user context
- No user is ever given administrator credentials
- Alternate credentials are never used for the elevation of a task
- Seamless integration with Windows Vista/7 User Account Control

All Approved Elevated Tasks Must be Determined

To solve least privilege problems, all approved tasks must be discovered and then configured to be allowed to run. This can be very difficult without a seamless integration within your least privilege solution. Manually discovering approved tasks that must be elevated can be a daunting assignment even for the smallest of companies having very few endpoints. Manual attempts also cause significant loss of productivity for the user being used to discover the tasks, as well as for the IT staff that is documenting the tasks that need to be elevated.

The final step for a manual approach is most likely the most time consuming, which is to find the task executable and all required switches in order to elevate it in a rule or policy. Instead, there needs to be an automated solution to discover the approved tasks and also generate a policy, which can then be copy and pasted into the final least privilege solution you are deploying. PowerBroker Desktops Windows Edition provides an integrated solution within its reporting console that allows for quick and easy automatic rule creation for the elevation of approved tasks. Automatic rule generation provides the following benefits:

- Integrated in the PowerBroker Desktops Windows Edition interface
- Works in the background to discover approved elevated tasks on every endpoint
- Generates policies for every elevated task
- Policies can be copy and pasted into Group Policy Objects easily
- Filters can be placed on discovered tasks to reduce false positives

Design Needs to Integrate Seamlessly into Existing Environment

All Active Directory administrators know the complexity that goes into designing, deploying, and managing the Active Directory structure. With Active Directory already in place and solidified, there is little chance that it can be redesigned to support a least privilege implementation. However, there must be some way to work with the existing Active Directory structure to implement the least privilege solution to the variety of users, computers, departments, etc within the corporation. Ideally, a solution needs to work with the existing Active Directory

and Group Policy management tools to make the overall efficiency of managing the least privilege deployment and solution optimal. The solution also needs to provide a method to isolate users, computers, groups, IP address ranges, operating systems, etc. This is needed to negate the existing Active Directory structure and target tasks on endpoints with extreme precision. PowerBroker Desktops Windows Edition provides a solution to this problem with Collections and Item Level Targeting to integrate seamlessly into the existing Active Directory structure. Collections and Item Level Targeting provide the following benefits:

- The least privilege solution is not dependent on the existing Active Directory structure
- Collections can be created to deploy least privilege to users, desktops, departments, etc.
- They can be nested to provide easy management and deployment of least privilege policies
- Item Level Targeting can be set at the Collection level to optimize the analysis of the policies in the Collection
- Item Level Targeting has over 25 filters which can isolate the endpoint with precise accuracy
- Item Level Targeting uses direct API calls to optimize the deployment of the least privilege policies

All Approved Tasks Can be Executed

The term "task" in this context is not only an application. Here, task needs to be anything that the endpoint can perform, which is approved by the enterprise. Examples might be to install a local printer when the user is at a branch office, install an ActiveX control when accessing the new Cloud application, or installing a new application that is required to perform end of month financials. Just ensure that your least privilege solution can provide elevation for all approved tasks on the endpoints. PowerBroker Desktops provides a solution to allow all approved tasks to be elevated. PowerBroker Desktops provides the following benefits:

- All applications, developed internally or purchased, can be elevated
- ActiveX control installations can be elevated
- Installations of applications and services can be elevated
- Built-in operating system features and applications can be elevated
- CD and DVD access can be elevated
- All elevated tasks can require justification and/or credentials
- Users can optionally self-elevate tasks if a rule does not exist for the task

Least Privilege with Whitelisting

Another possible addition to your least privilege solution is to incorporate whitelisting. Whitelisting is the concept that an approved list of applications is developed and enforced on each endpoint. If an approved application is not on the whitelist, it must be added to the whitelist in order for the endpoint to run the application. Since most endpoints require different approved tasks and applications, management of the whitelist can become cumbersome and overwhelming.

Gartner defines whitelisting (AKA application control) as "…technologies on the endpoint use an enforcement agent component to ensure that only "known good" software can run. When the user (or a program on the endpoint) tries to run or install an application (e.g., executable, script, or other type of software component), the agent checks the application against policy. It either allows the application to run or not. Related security policy usually expresses some form of a "deny all but the known good" rule or "only allow certain applications to run in certain circumstances."" (Gartner, Inc., "Application Control and Whitelisting for Endpoints," Dan Blum, Mar.10, 2011.)

Whitelisting solutions are built directly into Windows XP, Windows Vista, and Windows 7. In Windows XP, whitelisting is implemented through Software Restriction Policy (SRP) and in Windows Vista/7, whitelisting is implemented using AppLocker. Both technologies provide a way to allow a specified list of applications, as well as a list of applications by using wildcards, paths, publishers, hashes, etc.

Whitelisting Requirements

In order for whitelisting to be successful, there are, of course, specific aspects of the endpoint environment that must be known and the overall whitelisting technology in place. Whitelisting technology requirements include:

- A known list of all allowed tasks (including all OS features, installations, etc)
- On-going management and policy generation of approved tasks
- Process for generating approved tasks onto the whitelist which are not discovered automatically
- Integration into the existing Active Directory environment
- Granular control over each whitelist for targeting to users, computers, groups, departments, etc.

Whitelisting Limitations

Although whitelisting is an excellent method to control which applications are allowed to run and which applications are denied from running on each endpoint, it is not a solution to least privilege. A whitelisting solution without least privilege still requires the user to have local administrator privileges to run the applications approved by the whitelist, which require elevation. However, the flip side of this is not as limiting. Least privilege solutions without whitelisting protect all elevated applications, just not the applications that do not require elevation. If the application does not require elevation, it is being run as a standard user and the risk associated with this application is almost negligible compared to those applications that are elevated to run with administrator privileges.

What Least Privilege Is Not

Least privilege solutions have been around for years and have provided a solution to allow standard users to run all approved tasks at each endpoint. Companies like BeyondTrust have been solving least privilege for the longest time, since early 2005. Like any great solution, the breadth of the solution needs to expand as the technologies around it become more complex and sophisticated. In this case, the technologies around least privilege that need to be addressed are in the area of data access. Yes, the need to access data is not new data access not new, but the unwanted and illegal exposure of data is becoming more prevalent.

Currently, access to data is not solved by least privilege due to the current running of the tasks, as well as the controls over the data. If a user has access to data, there is nothing that restricts the user from copying and pasting the data into an email, nor sending the data file in an email to a Wiki site.

Least privilege is a needed and all encompassing solution. However, least privilege alone does not solve the need to control data leaks. IT security needs to understand and develop solutions that also address how data is accessed, copied, and transferred.

Data Leak Protection Defined

There is an every growing interest in data leak protection, as can be observed by recent articles written by well-known analysts like Gartner and Burton Group. For most security professionals the attention is long overdue, as other security professionals have been concerned about data leaks for years.

A data leak is a malicious (sometimes errant) sharing or transfer of data from within the corporation to somewhere outside the corporation. The leak can occur by someone with local administrator privileges or even local standard user

privileges. The key aspect of the data leak scenario is that there is little control or monitoring over what users can do with data once they have legitimate access to the data. Least privilege is not a solution to data leak protection, as this only restricts the user's privilege at the endpoint.

Data leak prevention provides data control and monitoring solutions to solve the issue of data privacy and confidentiality for any IT infrastructure. A state-of-the-art data leak protection solution should provide content-aware data leak protection, device control, e-mail control, Web control, and access control to data, at a minimum.

The Need for Data Leak Prevention

The need for data leak prevention (DLP) is clearer now more than ever. With the abundance of data leaks in the past 18 to 24 months, companies are scrambling to get a handle on their data to ensure there are no more embarrassment or litigation issues in the future. Again, security professionals have known for years that a data leak is possible and eminent, due to the nature of traditional data storage, access, and protection.

All HR, finance, credit card, intellectual property, etc., is stored as some form of data on the network. This data can be in a document, spreadsheet, database, or any other form of file type. Data is typically stored on servers, but with storage area networks (SANs), cloud storage, USB thumb drives, laptops, tablets, etc, data can literally be anywhere in the corporation.

Traditional data storage security is done two different ways. First, there is the well-known access control list (ACL). The ACL is a list of users and groups, "who", can access the data, listing the specific permissions and "what", and the user can do with the data. As long as the user has at least "Read" access to the data, the user can leak the data outside of the company walls. The second way to secure data is to encrypt the data. Data encryption is supported within Windows, as well as by some other well-known security companies. If the user trying to access the data does not have the correct encryption key to decrypt the data, the user will be denied access. However, as soon as the user can decrypt the data, it is the same scenario as the traditional ACL; the user can now leak the data outside the company.

The following are examples of companies that have had data leaks in the recent months, giving you insight into how easy data leaks can be executed.
Sony Corporation - Sony's PlayStation Network was down for a week, which the company admitted that an unauthorized person had stolen personal information belonging to 77 million account holders.

RSA Security - The RSA was breached recently with the thief stealing information related to the RSA's SecurID tokens. This RSA two-factor authentication solution is used by millions of users, including government and private sector organizations.

WikiLeaks - The United States Government has tens of thousands of documents leaked out by Pfc. Bradley Manning, who served as an intelligence analyst in Iraq.

HSBC - HSBC had data from over 130,000 clients stolen from the HSBC Holdings Plc's private bank in Geneva, Switzerland.

Requirements for DLP

When looking at a DLP solution, you need to ensure that the solution will meet and exceed all of the known issues that have come to light with data leaks. Using the historical data leak data over the past few years, it is obvious where the leaks are occurring, so addressing these areas is essential in your DLP solution. At a minimum, you need to ensure your DLP solution addresses the following five areas:

- Preventing WikiLeaks Incidents
- Preventing Access to Data on Stolen or Lost Computers
- Controlling Removable Devices
- Restricting Data Access to Specific Applications
- Preventing Data from Being Transferred Outside of the Organization

In order to understand each of these areas of protection that are required to prevent data leaks, the following sections describe each of these in more detail.

Preventing WikiLeaks Incidents

Most of the WikiLeaks incidents that have occurred are due to massive information transfer to the site. This type of behavior was out of the ordinary for the user that sent this information, as the user has never transferred this much information in this format before. What a DLP solution should do is profile for this behavior and creates an alert of the activity. Data should have the ability to be classified or not, but event without classification, when activity outside of the norm is detected, someone should be notified. If the US Army had a data leak protection solution in place, The Bradley Manning incident with WikiLeaks could have been prevented. PowerBroker DLP Edition provides this level of monitoring and alerting.

Preventing Access to Data on Stolen or Lost Computers

Every corporation has a mobile work force and mobile devices. It is a common occurrence for these devices to be lost or stolen. With the technologies that are available, criminals can access data on a hard drive, even when they do not have the local administrator password. DLP solutions should include encrypting technologies to automatically encrypt sensitive or confidential data on mobile devices. This would make the data inaccessible to criminals when devices are lost or stolen. PowerBroker DLP Edition provides this level of encryption on mobile devices.

Device Control

Mass storage devices have come a long way from the time we had floppy drives. USB thumb drives, USB hard drives, and other portable devices are commonplace and now can store enormous amounts of data. Users do not require local administrative privileges to use the devices and can copy data to these devices with ease. DLP solutions make control of these devices easy and protected from data theft. A quality DLP solution should have very granular control over these devices, down to the manufacturer, model, and device ID level. PowerBroker DLP Edition provides this level of granular control over devices.

Restricting Data Access to Specific Applications

Data stored on a network or server must be stored using a specified file type. Common file types include .docx, .xls, .db, etc. Each file type is typically associated with an application or list of applications. For example, .xls files are associated with Microsoft Excel and .docx files are associated with Microsoft Word. However, there is nothing in the system to restrict a file from being opened using a different application, which can cause significant data access issues. The point is that if a user has permissions to a file, the data within the file can still be accessed even if the user does not have the appropriate or desired application to open the file type. DLP solutions can prohibit this access by forcing specified file types to only be accessible by specific applications. PowerBroker DLP Edition provides this level of control over data and applications.

Preventing Data from Being Transferred Outside of the Organization

The reality is that many users have access to confidential data in any organization. The fact that these users are responsible for over 70 percent of data thefts should not come as any surprise. Controlling how a user can work with data is a critical piece to any organizations security posture. DLP solutions can prevent users from unauthorized copy and transfer of data. This can be control over placement of

unauthorized text into emails, social media sites, or to other files. PowerBroker DLP Edition provides this level of data control.

Summary

Endpoint security is essential for every organization. With hundreds, thousands, or 10's of thousands of endpoints, every instance becomes a potential threat or risk. First and foremost, endpoint protection starts with least privilege. Ensuring that all users are standard users, and not having local administrator privileges, is paramount for the overall security of your endpoints and entire network.

However, providing access to the users of these endpoints with the ability to run all applications, perform installations, and authorized operating system functions is also required. Whitelisting of applications can help secure the endpoint, but this alone is not a solution to least privilege. A least privilege solution alone is not enough to protect the endpoint though, due to the ever-growing data leak issues that are occurring.

DLP is just as important as least privilege to secure the endpoints. DLP has specific requirements such as control over devices, transferring data, accessing data with specified applications, and more. If corporations can obtain a least privilege solution along with a DLP solution, such as those provided by PowerBroker from BeyondTrust, their overall security of endpoints will be second to none.

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 the greater Los Angeles area, greater Boston area, Washington DC, as well as EMEA offices in London, UK.

PowerBroker DLP Edition is a powerful data control and monitoring solution to the problem of data privacy and confidentiality in IT infrastructure. PowerBroker DLP Edition effectively replaces individual security tools, such as content-aware DLP, device control, e-mail control, web control, access control to files and more, combining them into unified data control policy, delivered through Microsoft's Group Policy infrastructure.

For more information, visit www.beyondtrust.com.

About the Author – Derek Melber (MCSE, MVP)

Derek Melber (MCSE, MVP), President and CEO of BrainCore.net Derek Melber, MCSE, MVP, is an independent consultant, speaker, author, and trainer. Derek's latest book, The Group Policy Resource Kit by Microsoft Press, is his latest best-selling book covering all of the new Group Policy features and settings in Windows Server 2008 and Vista. Derek educates and evangelizes Microsoft technology, focusing on Active Directory, Group Policy, Security, and desktop management. Derek speaks and trains for MISTI, TechMentor, Windows Connections, and TechEd.