Endpoint Privilege Management: Identifying, Justifying, and Deploying Your Best Solution

By:

Brett Wyer
Senior Solution Architect
Set Solutions

July 8, 2019

Prepared by:
Set Solutions, Inc.
1800 West Loop South
Houston, TX 77027
Phone: (713) 956-6600
Setsolutions.com
SECTION 1 - AN INTRODUCTION

A question CISOs bring to us frequently is, “how can I revoke local administrator rights from my users without severely impacting their job?” If your organization is struggling with this challenge, please be assured that you are not alone. There are ways to lock down end-user workstations without them lining up outside your office with pitchforks and torches.

Before digging into the topic, though, let’s go through a quick level set.

What is “administrative access” and why is it a problem for Information Security teams?
All operating systems, be it Windows, Linux or Mac OS X, have the concept of administrative access. Depending on the operating system, users with this level of access may have different names such as Administrator, Super-User or Root. In short, this allows the user to bypass and/or disable most if not all security mechanisms in the operating system, granting them the “keys to the kingdom”. This is a prime target for malware and other attacks.

If administrative access is so dangerous, why shouldn’t I just revoke it?
While the nuclear option is certainly attractive, there are legitimate business needs for “admin rights” (poorly-written applications, help desk staff needing to install software, a server administrator troubleshooting an issue, a VIP installing iTunes, etc.). Taking away admin privileges without considering the repercussions will lead to ineffective users, upset VIPs, stressed out help desk staff, and hamstrung desktop/server administrators. Essentially, the quickest way to get the masses lined up outside your office is to get between what they need to do and what they can do.

Fine, so how do I address this problem without taking a long walk off a short plank?
There are several Endpoint Privilege Management (EPM) solutions, both commercial and built-in, to provide more granular control than just a blatant “no more admin access” edict. These products by their very nature are highly complex and have very deep hooks into the operating system they’re tied to. They are designed to only grant administrative rights to a user under very specific circumstances and only for as long as they’re necessary.

It should be emphasized that implementation of an EPM solution is not just a “run setup and click through the installation wizard” deployment. Considerable up-front research along with cooperation from IT administrative staff and executive buy-in are all mandatory parts of a successful implementation. Leveraging a commercial product over OS built-in controls will mitigate some of the legwork but at the end of the day, an EPM solution is no substitute for good administrative control.

Okay, so where do I go from here?
That’s a great question! In the next section, these three questions will be covered:
• How do Endpoint Privilege Management solutions work?
• What do I need to know about my environment to deploy one?
• What are some of the capabilities of solutions designed to address this challenge?

SECTION 2 – GETTING INTO THE WEEDS

How does an EPM solution work?
Probably one of the biggest frustrations a Solutions Architect deals with on an almost daily basis is cutting through vendor marketing fluff and getting to the real question: “what does your product really do, and how does it work?” Well, you can save a few hours of your life by reading this (relatively) simple explanation of EPM:

An Endpoint Privilege Management solution hooks deeply into the operating system and intercepts the execution of commands, scripts and programs. Execution is allowed and privilege escalation is potentially performed based on a set of rules.

To anthropomorphize a bit, think of an EPM solution like Big Brother. Every action of every user is watched and assessed; some solutions can even record user actions. When an attempt is made to perform a function such as opening a Word document or installing a driver, it is intercepted and evaluated against The Rules. If the attempt passes muster, the action is allowed and if necessary, privileges are temporarily elevated to allow execution. If not, the action can be stopped or a prompt for further permission can be presented.

What do I need to know before I roll out EPM?
An EPM solution is by no means a “push it and forget it” installation. While deployment will provide unprecedented control over what an end user can do, with great power comes great responsibility. Due to the depth of the OS integration and the potential for disruption, considerable research and planning must be done up front to prevent a career-adjusting event. Here are some points to consider:

• Is there an executive sponsor that owns locking down the environment?
  Cultural change is disruptive, and implementation of a security product with this level of control will impact all levels of the organization. Air cover from one or more executives is not just a luxury; especially when a VIP loses the ability to install iTunes on their corporate laptop.

• Is the current environment well-understood and reasonably secure?
  Do controls around administrative access exist today that users are accustomed to dealing with, or is the Domain Admin password posted on a sticky note on the 3rd floor printer? An EPM solution is not a substitute for good security practices, nor is it a good way to implement them from scratch.
• Are there sufficient personnel, and is there buy-in from the staff to support an EPM deployment?
With the significant benefits gained from an EPM solution come considerable administrative load; platform and rules maintenance, help desk tickets, and event monitoring are all critical parts of ongoing support in an EPM solution. Consider the impact on the End-User Support Team during the deployment process for example—packaging, testing, installation and troubleshooting. This is a non-trivial effort.

Rolling out a new tool represents a “spend” of political capital; selling the tool and its benefits to the impacted teams can reduce that “cost”. Be creative and look at EPM from the other teams’ perspectives, determining ways it can help them once they deploy it. For example, a big pain-point for desktop support teams is users installing software or drivers that render machines unusable. Configured correctly, EPM can reduce or even eliminate this issue. Couched in these terms, pushback can be turned into enthusiasm.

• Are there products in my environment an EPM solution would need to integrate with?
Users are going to be stymied in their attempts to install the latest version of their favorite tool that they simply can’t do their job without and will want to request an exception. One of the features of a good EPM solution is a mechanism to assist the help desk in determining whether a request should be approved or denied. Integration with a detonation technology such as FireEye AX or Palo Alto WildFire, or a hash lookup service such as VirusTotal can provide this insight at the click of a button.

Understanding the tool and its integration points can help streamline support once it’s been deployed. This will ultimately reduce the impact on affected groups, meaning it’s easier to get their buy-in.

Why would I want this headache?
That’s an excellent question. Remember, this entire conversation started with three questions:
• What is “administrative access”?
• Why is it a problem for Information Security teams?
• If administrative access is so dangerous, why shouldn’t I just revoke it?

There is no getting away from the fact that users will occasionally need administrative access to their system. The easy route of giving users Local Admin rights simply isn’t secure; however, not doing so creates its own headaches. This doesn’t have to be a black-and-white conversation though; EPM creates a grey area between those two extremes. Here are some sample use-cases:

• Just-in-time privilege escalation for sanctioned software installations
A developer attempts to install a JDBC driver on their machine. The installer hash is recognized, the user is asked if they wish to perform the action, then Local Administrator rights are automatically granted to the installer process for the life of the installation.
• **Application whitelisting based on source**
  A network architect attempts to install Google Chrome on their laptop from the on-premise software server. The package has been executed from a sanctioned source, so appropriate rights are invisibly granted to the installer for the life of the installation.

• **One-off or offline privilege escalation for VIPs or IT architects**
  A trusted user attempts to install an unknown software package that is requesting administrative rights. They are prompted with a challenge code and instructions to call the help desk. The help desk validates the individual in question is who they say they are, keys the challenge code into their system and receives a response code they provide the user. The user keys in the code and administrative rights are granted for the life of the installation.

• **Automatic privilege escalation based on publisher certificate**
  A remote user is shipped a DVD with custom-written and signed software provided by their organization. Installation requires administrative rights and they are automatically granted by the EPM agent upon recognition that the software is properly signed by a trusted entity.

Hopefully, these examples give you an idea of the level of flexibility offered by a good EPM solution. Understand, too, that there are other capabilities such as time-of-day, specific machine, computer attributes (WMI query) and more.

**Okay, this looks like something I need in my environment, what’s next?**
This is where the rubber meets the road. In the next and final section, the following points will be covered:

• Some common requirements and the features they map to
• Deployment and maintenance efforts
• What’s involved in a Proof-of-Concept and how to work with a vendor to do one

*Section 3 on next page*
SECTION 3 – A DEEP DIVE

EPM customization
It’s rare that a product will map to business requirements with a “Setup > Next > Next >” installation approach. As EPM has the potential to impact much of the interaction between a user and their system it cannot be approached that way either. A well-designed product should provide flexibility to meet the unique challenges created by your environment and your user’s needs.

Here are some examples to get you thinking about requirements:

• OS Support
  Windows may be installed on 90%+ of desktops in the world but that’s rarely the only operating system version running in a corporate environment. Marketing or artistic departments frequently prefer OSX and developers tend to lean toward Linux. Don’t forget server OSes and OS version variants. Do you still have Windows XP or Windows Server 2003? Does your deployment need to consider all of these platforms?

• Delegation of administrative rights
  In a large organization it’s unlikely that the team sponsoring the EPM deployment will be able to provide all the end-user support. More likely, the Security, Help Desk and End-User Support teams (at a minimum) will be involved in the day-to-day management. Given this, does the product provide granular control over who can do what (role-based access control)? Is it appropriate for a Level I Help Desk tech to have the ability to create and delete execution policies?

• Logging, monitoring and policy update
  If a user attempts to install a printer driver and fails due to lack of administrative rights, does the product monitor for and log this attempt as well as providing an easy way for the Help Desk to update a policy to allow this activity? Of course, that policy update should be logged in a separate audit log as well.

• Language support, localization and branding
  There are likely going to be dialog boxes presented to the user, prompting them to take an action or warning them that an attempt was blocked. In an international organization, these may need to be customized for two or more languages. Does the product detect the OS localization and prompt with the correct language as well as adding languages that might not be supported? Does the product allow for branding with corporate logos?

• Policy flexibility
  Policies are the core of any EPM product. They are the rules that drive the decision to grant (or deny) rights to run an application. Think through the circumstances that may need to be considered when deciding whether to grant permission or not. Some common examples:
- Time of day (working hours vs. otherwise)
- AD group membership or specific user accounts
- Computer name where request is originating (kiosk for example)
- Policy lifetime
- Where the software is being run from (software share for example)
- Whether the software has been signed and by whom

**Privilege escalation flexibility**
A good product should support both invisible and prompted privilege escalation (of course, it should notify the user when their request has been denied as well). It should also have a mechanism for disconnected users to escalate privilege as well; the last thing you want is an executive without VPN access to not be able to do something they need to be able to do.

This is just a smattering of the possible scenarios. Others might include decisions based on compliance requirements, remote vs. local users, computer attributes, OS version, network connection, etc. When considering a product, go to the vendor’s web site and download the administrative documentation. Familiarize yourself with the policy administration section for ideas on how the product might fit your unique requirements.

**Deployment and maintenance**
You’ve determined you need an EPM product and defined the general requirements related to policies. The next question is how to operationalize it. Of course, the first step is how to deploy it—both the back-end server component as well as the client end of it. Some things to consider:

- **Is the server component going to be on-premises or in the cloud?**
  If the deployment will be on-prem, what are the infrastructure and connectivity requirements? If it’s cloud-based, what data will be stored there and are there any compliance implications? What are the client connectivity requirements? Don’t forget firewall changes for both servers and clients!

- **How will the client component (agent) be deployed and maintained long-term?**
  The client agent component will have to be pushed out to all target machines. Are the end-user and server teams (if applicable) on-board with this and do they have a tool to do it? Once the agent has been deployed, how will it be updated? Does the EPM solution provide a mechanism to manage and maintain the agent or is it a “bring your own solution” situation?

- **Does the agent installation and do subsequent upgrades require a reboot?**
  One of the biggest pet peeves of an End-User Support team is having to reboot a machine to install new software. Is this a requirement?

- **What are the product SLAs to the business?**
  As the agent is likely going to be in constant communication with the server component, what are the uptime requirements? Does the product provide for this? How must it be architected to respond to server-side outages without impacting the
user base? This not only encompasses high availability and disaster recovery but also backups.

- **How will this be rolled out?**
  The quickest way to generate a career-impacting event would be to push an EPM product out to all your users in the default configuration; I can guarantee this will fail in a spectacular and memorable fashion. Instead, a staged rollout perhaps focusing on IT power users first, then gradually moving out to the rest of the company in logical groups. I cannot emphasize enough the importance of starting in monitoring mode then moving to enforcement mode later.

Of course, there are plenty of other considerations beyond the scope of this short blog post; it is critical that all impacted teams sit down together and get an understanding of not only what the product does but also how it works and how it will impact the infrastructure. Only then can the full scope of effort be defined for both deployment and operationalization in your environment.

**Okay, I need EPM. I have my requirements, I have buy-in and I’m prepared to put the work into it. What do I do now?**

Well, here is some great news for you: If you’re still reading this paper and have done your homework, you have pretty much everything you need to do a proof-of-concept. The next steps would be:

- Identify and gather stakeholders to be involved in the POC. This includes not only administrative personnel (Help Desk, End-User Support, Operations, etc.) but also a few of your internal customers that are savvy and willing to provide useful feedback.
- Get a lab together. This should be a handful of machines that represent the various types of systems the solution would be running on. A “Golden Image” on them is helpful as that becomes the baseline for testing policies to allow for further software installation.
- Remember that list of requirements you came up with? Work up a scorecard and assign a weight to each one based on its importance to you.
- Build a short-list of EPM solutions you want to test. Probably not more than three as testing is time-consuming and can be complex.
- Either engage the solutions vendors directly or identify a reseller like Set Solutions you can work through to coordinate with the individual vendors on your behalf. A reseller should be able to help you with the POC effort and bring their own expertise to bear as well.
- Share your requirements with your partners. This will not only help them focus on what’s important to you but also impress upon them that you’re serious about the effort and not just kicking tires.
- Test each product against your list of requirements and rank its ability to meet them on your scorecard. Once the POC is complete, if done correctly, the scorecard should paint a clear picture of each product’s ability (or lack thereof) to meet your needs.

That’s pretty much it. Hopefully you have have found this Endpoint Privilege Management whitepaper useful. If you would like assistance with EPM or other cybersecurity solution integration needs, please reach out to us at [https://www.setsolutions.com/contact/](https://www.setsolutions.com/contact/), or call us at 713-956-6600.