SANS

WHAT WORKS™

Increasing Security and Reducing Costs by Managing Administrator Rights with Process-based Privilege Management

with

VIEWFINITY

WhatWorks is a user-to-user program in which security managers who have implemented effective internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know more about? Let us know. www.sans.org/whatworks

About the User
The user interviewed for this case study has requested anonymity to maintain confidentiality. The WhatWorks program can help more users make more informed decisions if we allow seasoned professionals from major user organizations to share their stories without revealing the name of the organization.

The user in this case study served as the Workstation Architect for his company. In his role, he was responsible for all aspects of the project to migrate the company from Windows XP to Windows 7. This included leading the teams that gathered requirements, designed solutions and implemented the project corporate wide. Other responsibilities included oversight of the solutions for software packaging and delivery and the Citrix environment.

SANS Summary
Taking advantage of major technology transitions to increase security is a very effective strategy. In this case, migrating to a Windows 7 environment from XP meant that a legacy tool that allowed users one of three levels of administrative rights to their workstations would need to be replaced. The Workstation Architect spearheaded a search for a Privilege Management product to reduce help desk calls when users installed software (both legitimate software and malware) that impacted the performance of their PCs. The Viewfinity solution he found allowed him to implement a process-based whitelist that supports a variety of more than 3,000 applications installed for business use and significantly decreased the manpower required to support user installation requests.

~~~~~~

Interview

Q: What caused you to look for a solution like Viewfinity?
A: In our Windows XP environment, we had a custom written tool that gave users 24 hour administrative rights to their machines. Going into Windows 7, we knew that tool wasn't compatible with Windows 7. About 1,000 of our 6,000 end users had local administrative rights on their PCs and it had gotten out of hand. We had three different models for the XP environment: regular users who were given complete local admin rights, users with extra accounts without Internet access who had local admin rights and users utilizing the custom written tool for temporary access. Going into Windows 7, we had to come up with a solution to handle administrative rights and that's what set us down the path of looking at the different tools and options out there.

Q: Was it out of the question to use only Windows native features and allow people to be standard users?
A: Granting users only standard rights wasn't going to be an option. When we looked at our Windows 7 project, we had about 1,000 applications that were packaged and available for delivery through our own application store, so we wanted to use that as our main source for application installs. When we looked at all the applications that were installed on our XP machines, we had more than 70,000 instances of software that was manually installed on machines over an eight to ten year period. When we took a look at the applications that were installed that were actually required for business use, it filtered down to about 3,000. A lot of them were applications that shouldn't have been on there
~~~~~~

in the first place, like personal tax software. Looking at that, we were able to reduce that number to relevant applications that were going to need to be installed manually. Rather than having our local rollout team conduct every instance of those installs, we wanted to give the business and the end users an option to be able to do that themselves, which led us to evaluating products in the market.

Q: Tax software so they could print their returns?
A: Exactly. This is not a business application. We took care of what we could before the rollout and then handled separate requests for anything that was not required for business use.

"Overall, Viewfinity has exceeded my expectations."

Q: How did you convince management to pay for this?
A: I was new to the role, but in our requirements gathering it was identified that we needed a solution. We knew we had an issue with our standard users who had Internet access and local admin rights. We knew we needed a solution, so it wasn't a hard sell and the budget was included in the original Windows 7 project. We did a separate RFP process to look at different tools and options, but getting management buy in wasn't that hard because we had a history of dealing with issues that could be traced back to local administrative rights on machines.

Q: Can you walk me through the process you used to find the best solution?
A: The process was conducted a few years ago, so I don't have all of the details. As the Workstation Architect over the Windows 7 project, I worked with our Security team and project stakeholders to develop a list of requirements. Once we had a requirements list, we researched our options based on knowledge of companies in the space. The leading recommendation was BeyondTrust, which led me to look at their competitors and that's when we identified the companies to include in the RFP process. We evaluated Viewfinity, BeyondTrust, AppSense and Quest. During the RFP process, we had several presentations with each vendor and evaluated their responses against our requirements. Based on our scorecard criteria, we selected Viewfinity as our Privilege Management solution.

Q: What were your top criteria when you compared the products?
A: The primary driver for Viewfinity was to meet business needs and retain control. Viewfinity met our needs and allowed for an on-premise solution that could be managed outside of the Group Policy Objects/Active Directory team. The ease of use in setting policies was also a big plus.

Q: With what you saw of Viewfinity, are you using their privilege management product or have you upgraded your environment so you may also utilize their application control capabilities?
A: Currently we're on an older version of their privilege management tool, but we will work with them to upgrade to the latest version in the near future. We have not done a full evaluation of the new version, so I am not sure about the full feature set. We have approximately 500 policies for application installs, MSIs or executables, being able to run scripts as an administrator, installing ActiveX controls and doing some of the Windows tasks. My philosophy was to allow everything that we're comfortable with across the board. Now if the end user wants to install a local printer, they no longer need to wait for local support to set it up; they have the rights to do this themselves. We implement on an

as needed basis and are trying to whitelist items companywide. We have on demand access as an option that replaces directly adding users to the local admin group. Essentially, they are able to run applications and tasks that require local admin rights, but now they're doing it on a per process basis rather than having blanket rights to that machine.

> **"I look forward to working with Viewfinity as we prepare to upgrade to the latest version."**

Q: What about the ones that don't fit into those categories for allowed privilege escalation? Does the ops team have to allow or disallow?
A: We've got two processes in place today: one for on demand access that is essentially replacing local admin rights and another one in which the request goes through a set of approvals. We look at the criteria to see if we should handle it locally or if we should put a policy into Viewfinity to cover that specific need. For example, if a developer needs frequent access to uninstall, reinstall, or update software, we allow on demand access. If a user is trying to install an application or run it with administrative rights, that is a workflow in which a Viewfinity window pops up and prompts them to put in a ticket to our workstation team. If it is for a business need and there are no security risks, it will be approved globally so that other users with the same need can double click the file and install it without any other interaction.

Q: This is the area where I've seen deployments of these kinds of products hit the wall in the past. What is the workload like for responding to this?
A: I was running it during the Windows 7 project and I will tell you it wasn't full time, but initially it was a significant effort – probably five policies a day during the heart of the rollout or around an hour a day. Today we're only at 500 policies. Now that we're in an operational state, we get less than 5 ad hoc requests per week for our 6,000 machines.

Q: You got approval, the product showed up, how long did it take you to become operational?
A: I introduced the tool with Windows 7 prior to the rollout, so getting it set up and installed was completed in a week.

Q: When you rolled out the Windows 7 image, the Viewfinity side came with it?
A: Exactly. So for us, it was very quick. The support team was on-site helping us with the install and it was completed in a day. We spent a day training and then it was ready to be included in the Windows 7 image. It really wasn't that difficult to get set up and rolled out. It's a big change for the end user because of the pop up box and not just having local admin rights. Educating the end user population was probably the toughest part in getting that adopted. We didn't do the GPO option; I wanted to stay away from that because I don't control our AD group. This way we were able to hit the ground running with Viewfinity at the time of the Windows 7 rollout.

Q: How long did it take for the number of policy requests to stabilize?
A: After the rollout it was just a few weeks. For those applications requiring admin rights that we knew about prior to the rollout, we got policies in there beforehand. For example, we have a graphics group that installs a certain application that's not packaged. Before

we rolled out, we worked with our IT representative to get that policy in Viewfinity so that when we did roll them out, they could just double click and install the application they needed.

Q: Earlier, you mentioned the tax software installation as an example. What approach did you take for telling users about authorized and unauthorized software installation?
A: Our approach is that they are still standard users without on-demand rights. If they are going to require something going forward they would have to put in a separate request. This has been the case for our environment for the last 10 years, so there wasn't a lot of education effort around unauthorized software discussions though Viewfinity brought more visibility to the process.

Q: If someone really wanted to still do that they would have to request the ability to load TurboTax?
A: Correct. And they would probably get denied unless there was a specific business reason. But having a system in place helps cut down on those personal requests significantly.

Q: What would you say were the top two reasons why you ended up going with Viewfinity?
A: I would say the number one reason was being able to have my own console where I didn't have to go through our GPO team. Also, the flexibility of the tool itself and the different options for on demand and individual applications – and then some of those Windows tasks that we could deploy to all users. Those were the main reasons why we ended up going with Viewfinity.

> **"Viewfinity has been quick to respond to any inquiries or support issues and has made our jobs easier in providing a working solution for rights management in our environment."**

Q: You had to spend some money to buy the product and you obviously had to fight through some user impact. Are there some metrics you report upwards about its value?
A: No. For the most part, having a tool in place was the requirement. We have inquiries from our Compliance and Security teams into reporting, but we don't report to management on any specific metrics.

Q: Many people try to install copies of things the company didn't purchase and preventing that is important to IT for their desktop management environment.
A: Correct, but from the Workstation perspective, it is not our job to handle license management. We have an Asset Management team that relies on SCCM data to report on license use.

Q: How long have you been operational?
A: Our first production roll out began in July 2013, but initial pilots began in October 2012.

Q: Based on what you know now is there something you'd do differently, some lessons learned you'd like to pass on to other people who will be following your path?
A: Yes, the biggest thing is that user education is crucial. We focused our education efforts on the IT community rather reaching out to the overall business and all end users; including some of that up front education would certainly have helped. Other than that, I think the tool helped save us quite a bit of end user frustration. I've known other companies that just rolled something out, took the hard stance about standard users and it ended up causing more work in the end.

Q: Are there some features or requirements you'd like to see added to Viewfinity?
A: Yes. I'd say the biggest frustration is that pop up box that comes up and says "you don't have rights to this" and it includes a message box. This message box causes confusion because the users think it automatically puts in a request to the Service Desk. Users think that if they put in a justification, someone's going to automatically act on it. We could set up an email or notification to create a ticket, but it would cause a lot of tickets. We've asked to have more control over end user messaging. This has been updated in a future version based on customer feedback and we plan on working with Viewfinity in the near future to update our version to address this issue.

> **"The main reasons we chose Viewfinity were being able to have a console separate from the GPO team, the flexibility of the tool itself, and the different options for on demand and individual applications."**

Q: You mentioned that Viewfinity came in when you were doing the initial set up. How has the support been overall?
A: Very good. We've only had to put in a couple of cases where we saw some weird interaction. Most of it ended up being something on our side, but they've been very responsive. We put in a ticket at viewfinity.com/support and within the day they'll have a reply and then they'll work with us on anything that we need to implement. Viewfinity got in the way of our group policy that allowed ActiveX installs so I had to work with them to figure out how to get around that. They helped come up with a solution that required just a few edits of policy.

Q: I know you're on the end user computing side, but do you know if you are using Viewfinity on the server side as well?
A: No. There have been discussions from the security server team, but we aren't doing anything on the server side.

Q: How do you feel about Viewfinity overall?
A: Overall, Viewfinity has exceeded my expectations. They came on site to help us with the installation and initially performed training for support staff. In the days since implementation, they have been quick to respond to any inquiries or support issues and have made our jobs easier in providing a working solution for rights management in our environment. I look forward to working with them as we prepare to upgrade to the latest version.

SANS Bottom Line on Viewfinity Privilege Management solution:

1. The Workstation Architect took advantage of major technology transitions to both reduce operations costs and make advances in security;
2. Prior to removing admin rights, Viewfinity provides the capability to do a thorough inventory of what business applications and tasks are required for both formal and informal business processes;
3. After removing admin rights, Viewfinity permits two processes: one for on demand access, and another in which the request goes through a set of approvals;
4. Significantly reduces manpower needed to support user install requests;
5. Supports a process-based whitelist capability;
6. Good tech support and overall high marks for responsiveness.

VIEWFINITY

For more information:
Visit www.viewfinity.com;
Call 800-455-2010 or
Email info@viewfinity.com