AdminOnDemand
... a part of CapaOne

WHY USE PRIVILEGED ACCESS MANAGEMENT (PAM)

LIVING ON THE EDGE...

Imagine this nightmare scenario: Every user in your organization is a local administrator on their computer! I don't have to explain the constant danger that lurks behind every click the user makes when they check their email or browse the internet. You probably already know that local administrator rights should be avoided or kept to an absolute minimum, but to keep the users happy they get to keep their rights.

Why would any IT department want that? "Because that's the easiest way to install software or printers – and we don't have time to package everything". What else could you do to minimize the threat from the big bad internet?

The easiest way to do this would be to cut the internet connection and turn off every computer in the company. This, of cause, would have implications on productivity, and the employees would probably think your decision was rather stupid.
Implement User Account Control and removing the employee's ability to be local administrators are a little less drastic changes, and probably easier to digest than the alternative above.
Unfortunately, every company has a group of users or a certain employee type that requires local administrator rights to perform their jobs. As an example, I could mention the developer-type employee, who constantly is updating or adding features to their development tools.
These sorts of users can become quite a burden for the software packaging team in your IT department, and what usually happens, is that the developers become permanent local admins on their computers.

The developers are probably not the users you should fear the most – what about a stressed-out customer service employee or the CEO secretary who opens a spear-phishing mail and clicks on a malware-infected URL. That's where things get out of control very fast if the user is a local administrator.

THE SOLUTION

Introducing AdminOnDemand – a Privileged Access Management (PAM) tool and a part of CapaSystems CapaOne solution.

With AdminOnDemand you can easily assign local administrator rights based on different methods, such as Active Directory group membership or local group membership, or assign a user local administrator rights on a single computer.

CapaSystems
...because time matters

CapaSystems A/S
Roskildevej 342C
DK-2630 Taastrup

(+45) 70 10 70 55
sales@capasystems.com

There is even an option to assign a global local administrator.
For a computer to be able to receive an AdminOnDemand configuration, it needs to be tagged. A computer can be tagged with as many tags as you wish.

Tags are applied in the devices list, where filters can be applied to the devices list to single out exactly the computers you need to tag. The filters can be based on many different criteria, such as computer name, hardware information, and software installed on the computer.

The search filters are an extremely powerful tool, you can even create a list of computers with batteries that have a poor maximum capacity.
When the computer is tagged and a configuration is applied to that tag, the user can start elevating MSI or EXE files.

HOW DOES IT WORK

To use the AdminOnDemand privileged access management solution to run or install a program, the user must right-click on the file and select “Run as AdminOnDemand”. At this moment the user is authorized through either Active Directory group or local group membership or via the relationship to the computer or whether the user has global administrator rights. This makes changes to the configurations work instantly because the user is authenticated on their elevation request.
The user is presented with a warning that actions are logged when a program or installer is elevated.

The user is now presented with a User Account Control prompt, here they must type in their credentials and password.
Logging of user actions is instantly sent to the CapaOne Portal, and a dashboard shows you which programs have been installed, and how many times. The dashboard also displays which applications are elevated and a list of the users who requests local administrator rights.

Every graph in the dashboard is clickable – this means that you can do a deep dive into the information very fast.

If you click on an application in the graph, you will be able to see who has installed the application and on what computer, and when it happened. If you want to analyze what the most active users are doing when elevated that is also possible – just click on the graph with their name next to it. If a user is elevating a Command prompt, the actions done inside the prompt are also logged.

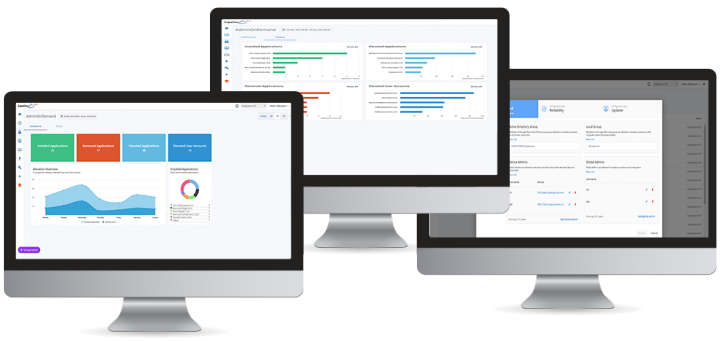
A CHANGE FOR THE BETTER

Going from being a local administrator, to not having any rights on the computer might be a big change for the users in your organization, and you might get a few complaints about your decision. To make the transmission easier on the users, why not assign everyone in the organization local administrators rights through the privileged access management tool AdminOnDemand? The users would have the same rights as before, but they might think twice before installing non work-related software.

And as a bonus, you get to see what the users are installing through our extensive logging methods.

You can use all this logging information to your advantage in your software packaging team. It might be a good idea to package the most installed programs.

With privileged access management solution AdminOnDemand you’ve got the perfect tool to help your users and keep the client platform secure at the same time.



CapaSystems
...because time matters

CapaSystems A/S
Roskildevej 342C
DK-2630 Taastrup

(+45) 70 10 70 55
sales@capasystems.com