How and Why is Open-AudIT "more secure"?

Introduction

Recently we have been asked the question - why do you consider Open-AudIT more secure than other similar programs? As with most things, the answer is "it depends".

Open-AudIT can be operated in such a way as to be *extremely* secure. But as usual with computer-based security, the more secure you wish to make something, the more inconvenient it becomes to use. The old phrase *"the most secure computer is one that is turned off and in the cupboard"* comes to mind.

Below we will outline some options that can be used with Open-AudIT that will increase security. Like most items within Open-AudIT, these are *options* and not mandatory. How far you take security is up to you.

On-Premise, Not Cloud

Open-AudIT can be run on **your** server in **your** data center. It does not *need* access to the internet *at all*. Even the installation on Linux where we use the distribution package manager for our prerequisites can be negated by you using an in-house and security team-approved package repository.

Open-AudIT does not store any of your data in the cloud. Even licensing information can be provided without having to access the internet from the Open-AudIT server.

Sure, it is easier to allow it to access the internet to download packages (including security fixes) for your distribution, but that's up to you and your security policies. Open-AudIT does not *need* the internet.

Open Source

Open-AudIT Community source code is available on GitHub. You are encouraged to inspect any code you have concerns about, and because it is open source - you are also encouraged to ask us about any issues you have or report any findings. We are always more than happy to accept code contributions, vulnerability reports, or even simple questions. We're here to help.

The audit scripts themselves (Windows, Linux, MacOS, et al) are deliberately written in readable native shell script (VBScript for Windows, Bash for *nix). You can see exactly what commands are run. You can remove any commands you feel you don't need. You can ask a third party to inspect the code for you and (if you want to) report any findings.

Open-AudIT Enterprise uses Open-AudIT Community as its engine. Enterprise instructs Community what to do (in most, but not all cases). So you can read exactly what happens when a discovery is run (for example). In the cases where Enterprise itself does the heavy lifting, if you are concerned with any issues Firstwave is happy to work through them with you - just ask! Try that with another commercial software vendor!

Agent? Discovery? Credentials?

So you have an issue providing Open-AudIT credentials to discover your devices. I have an answer - don't then! Sure, I mean, discovery is the best thing since sliced bread. You don't need to know ahead of time "What's On Your Network". But how can you extract data from devices without providing credentials?

In the case of computers, an easy option is to copy the appropriate audit script to the target machines and set it to execute on a schedule. More details on the wiki. The machines will send their data to Open-AudIT on that schedule, almost as if you were running discovery. There is no "agent" that asks Open-AudIT what to do (although we do have plans for that - stay tuned). The device simply runs the audit script on a schedule (again, you can *read* the audit script) as the user you tell it to and sends the output to the server. No credentials are involved at all.

What about other "network devices"? Think switches, routers, printers, etc. Obviously, it is best if you can provide some SNMP credentials for these devices. They only need "read-only" access. But if you don't want to do even that, there's nothing stopping you from running discovery, finding the devices, and making a rule or two to identify them. You won't have much information, but you'll know they're on the network, what they are, and when the last time they were seen was. You will also see if anything new appears on the network.

And if something goes wrong?

The audit scripts all accept a debugging argument. You can run the script utilizing that and see in more detail what the issue is. And if you can't figure it out - that's what we're here for! Open a support case and we'll get things running in no time.

Open Data

And lastly, not so much a security issue - more peace of mind. The data structures are **open** and **documented**. You can even view them inside the application. Your data is **your** data. You can extract it any time you like. We even helpfully provide exports to CSV, JSON and XML. And we have a JSON API. And you can write custom reports and have those output in CSV, XML, and JSON! Again, it is **your** data - not anyone else's. You can be confident that the security of your data is in your hands.

Wrap Up

I hope this post has alleviated any concerns you have about Open-AudIT and Security. If you have any questions at all, please don't hesitate to reach out to us here at FirstWave. We're always happy to discuss your concerns and needs. And maybe if your question isn't something I've addressed here, I can add it here for future users 🙂