StoreNext

Technical Bulletin

Solidcore + Anti-Virus: When to Use Both

S3-TECH-07:07
March 14, 2007

SUMMARY OF SOLIDCORE'S POSITION:

- When using S3 on a POS terminal, standard anti-virus is of no use whatsoever for run-time protection.
- When using S3 on locked "closet" or dedicated workstations where POS, payments and/or store applications run exclusively, standard anti-virus adds no run-time protection.
- Standard anti-virus can protect against "macro" type viruses that attack Word, Excel etc. files that Solidcore does not try to manage. But this is only useful on machines where:
  1. User access is available for non-POS application purposes and
  2. Microsoft Office is loaded and running and
  3. Files that could have macros are copied INTO the machine.

Unless ***all three*** of these conditions apply, A-V will cost money and slow down your machine without adding any run-time protection.

MORE DETAIL

You may have received different answers about this S3-plus-A-V question depending on who you asked, how much they know and exactly how you phrased the question. But knowing the right answer is critical to making sure the customer had the best protection available without wasting A-V license and maintenance/update costs.

- First – we're only talking about anti-virus for "run-time" protection — not using A-V to scan/check a system to make sure it's clean before re-solidifying an end-point after adding new applications. (That is where you ***should*** run an A-V scan, and most dealers have freeware/shareware with which to do this without forcing the customer to buy licensed A-V software for every slice and box in the store.)[1]
- Solidcore does not protect against viruses that inhabit macro routines from Word, Excel, Access etc. These viruses work by getting into a macro attached to (for example) an Excel file. Once opened/run, the macro file spreads by attaching itself to other Excel files, and worst-case corrupt them. The key points are that ***only*** the same type of file (like Excel) can be infected/affected, the system programs are ***not*** affected, and there's nothing in the POS system that's affected. Also, for macro viruses affect the PC, all three of the conditions numbered above need to be at work, including running and using Microsoft Office, copying

[1] The reason to run an A-V scan is to trap any possible malware that could have found its way onto the hard drive since the original installation, even though S3 would have prevented it from installing and running. After scanning the system, ***then*** re-solidify the machine, secure in the knowledge that you didn't solidify and "authorize" any threatening code.

files into that machine — plus ignoring the integrated Windows warnings not to run macros from the file when it's opened.

- Solidcore ***does*** protect against anything else – so these macros are all you really need to think about. No Microsoft Office +no external files = no A-V.

SUMMARY

For A-V could be useful on a box in a solidified store, ***all*** of the following conditions ***must*** be in place or A-V provides no value:

- They have to be running Microsoft Office (Word/Excel/Access etc.)
- They have to be copying external files down ***into*** the machine (note that if ISS45 or ScanMaster is creating Excel extracts for analysis or export, for example, that would wouldn't require A-V).
- So at most there could be one or two machines in a store where these conditions might apply. Again, if they suffer a macro virus, only the ***specific*** file types can be affected. nothing else, including system files or POS data files, will be touched.

That is, a virus in an Excel macro could affect Excel files only, an Access macro virus would affect only Access files and so forth.

Don't forget that if it's not required, adding A-V is "too much of a good thing" since the affected PC will suffer the performance down-side of A-V and of course the customer has to pay its license and the ongoing maintenance.

To Your Success,

Antony van Seventer