

Re: Norton vs McAfee

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-02/2181.html>

From: Richard Perry (newsgroups_at_perrysonline.net.no.spam)

Date: 02/24/04

Date: Tue, 24 Feb 2004 09:34:00 -0800

Dave-

Thank you so much for your information. I really do appreciate the details in which you described your setup. And these ramblings I do appreciate. The other ramblings I was referring to were the ones about the inaccuracy of information I received from one of my users.

However, after reading all of your post, I come to one conclusion. If I wanted to find out what version of software, what dat file is installed, and the number of viruses on computer ABC, I would have to scan thru an ASCII text file to find that information, correct?

Richard

"David H. Lipman" <DLipman~nospam~@Verizon.Net> wrote in message news:uChTCoo%23DHA.3808@TK2MSFTNGP09.phx.gbl...

> *Replies are inline.*

> *"Richard Perry" <newsgroups@perrysonline.net.nospam> wrote in message*

> *news:%23Rz\$uJo%23DHA.2524@tk2msftngp13.phx.gbl...*

> */ Dave-*

> */ I am replying to this message as I do not wish to propagate your other*

> */ response to my other post. I am looking for helpful information, not*

> */ ramblings.*

> */*

> */ However, this post contains a lot of beneficial information and I would like*

> */ to get more details from you with how you use this product. Your stated use*

> */ of McAfee is identical to the current implementation that I am working in*

> */ with one exception. We are deploying v7 on all Windows 2000 workstations.*

> */ However, we are not "pushing" anything to any workstation or server. We are*

> */ manually installing the software on all workstations, and setting the*

> */ software to do an autoupdate on system startup. For the most part, this is*

> */ covering all of our antivirus needs.*

>

- >
- > *Having all the platforms perform an auto-update means more bandwidth use to the Internet. I*
- > *pull the files from the McAfee FTP server and post the files to the Server's replication*
- > *source directory and let the NT Replication Service push the files to all NT Domain*
- > *controllers. This way our satelite office users don't get updates over a T1 line but get it*
- > *from a local BDC server. When PCs are updated, the traffic stays on the LAN and never hits*
- > *the MAN and WAN.*
- >
- > *By pushing updates I get two results. Guarantees that as users logon to the Domain, they*
- > *will get the updates. The second is Configuration Management. I can push changes to the*
- > *configuration such as new files extensions, EXTRA.DAT files, patches or software updates.*
- >
- >
- > */ I have one major complaint about our current setup. I have no way at the*
- > */ present time to load a central console and see how many machines are*
- > */ currently running any version of software, the latest dat file installed,*
- > */ the current engine installed, or the number of viruses caught on any*
- > */ workstation. Any or all of this information is critical in my mind as it*
- > */ would help me to identify machines that might be vulnerable, users that have*
- > */ a high number of viruses and can therefore be considered a risk, and justify*
- > */ the latest upgrade to the latest version if necessary (future use).*
- >
- >
- > *I override the default log files which are store on the local PC. Stupid idea ! I created*
- > *a hidden share and I have all the clients report to the centralized log files.. I also use*
- > *the Centralized Alerter. If a PC gets a hit. All the administrators get a NetBIOS Pop-Up*
- > *on their PC. It indicates the name of the infector, what has been found to be infected and*
- > *the action as well as DAT and ENGINE version.*
- >
- >
- > */ I have not found that the current version of McAfee Enterprise contains the*
- > */ tools that would allow me to do this. Since you are not only a fan of*
- > */ McAfee, but also a current user of the software, you are in a good position*
- > */ to point out how I can use the software. Just keep in mind that it is*

not

> / enough for me to simply deploy the software. I want to report on where that

> / software is and how well it is working.

> /

> / Richard

>

>

> By maintaining full control over the clients I guarantee updates, force Configuration

> Control, force centralized reporting and take advantage of centralized alerting. Besides

> events being logged into the the Alert Manager Server's application log, I get a ASCII log.

> I keep a master text file log on a per week basis. For example if a get a "hit", I'll create

> a file called 02-27-2004.log which will contain that weeks logged events I also keep a

> spreadsheet of all hits. Each row is a different infector. Each column is a year. So at

> the start of the year, the row "JS/IEStart" and all other previously noted viruses are set to

> zero and the total is zero. If I get a hit of the "JS/IEStart" I note the number of hits.

> By the end of the year I can see the total number of hits and what viruses were prevalent

> that year. the spreadsheet goes back several years. If you were to ask me "how many hits

> of the "JS/IEStart" I had in 2003" I can tell you as well as the total hits of this

> infector over the years.

>

> As to the hidden share I mentioned. Lets assume that collating server is called SERVER1. I

> create a hidden share \\server1>alert\$ { when we used to have Win98 platforms, the share

> "alert\$" was set to be a "Null Session Share" such that a client could write to the log

> files even if there was no authenticated user. As of 12/31/03, no Win9x/ME platforms were

> allowed to exist on our MAN so that Null Session Share capability was removed }

>

> I have TXT files called...

>

> \\server1>alert\$\Webdownload.TXT

> \\server1>alert\$\Emailevent.TXT

> \\server1>alert\$\Vshield.TXT

>

> for servers...

>

- > `\\server1>alert$\server1_netshield.txt`
- > `\\server1>alert$\server2_netshield.txt`
- > `\\server1>alert$\server3_netshield.txt`
- >
- > *I also create a JOB file that is dropped into the MS tasker. It is given a specified user*
- > *account (called 1145scan) so it can perform the JOB and log the even. At 1145am (when the*
- > *majority of users go to lunch) the workstation performs a mandated scan of the platform.*
- > *This too goes to a log files such as \\server1>alert\$\Vshield.TXT*
- >
- > *My organization "requires" maticulous logging, reporting and a daily scan of the desktops.*
- >
- > *By pushing updates to the workstations, I can over ride McAfees default settings t*
- > *accomplish these task.*
- >
- > *The solution is simple. I keep a file on the PC whose extension is the latest McAfee DAT*
- > *revision. When I go in tomorrow, I will set a counter in the Kixtart script to "327". When*
- > *my users logon to the PC, the script looks for a file called "mcafee_.327". If it exists,*
- > *the PC has already been updated. If it doesn't, the file "mcafee_.326" is erased and the NT*
- > *Service is stopped. I then copy the SuperDAT (renamed to setup.exe) to a local directory.*
- > *I then execute the SETUP.EXE with the force switch paramenter (setup.exe /F). I then import*
- > *a REG file that is the Configuration Mnagement file. I then restart the NT Service and then*
- > *write the file "mcafee_.327".*
- >
- > *Advantages, of the above. If I delete the mcafee_.xxx file, I can force and update by*
- > *relogging onto the domain. If I want to change the bahaviour of the client, I edit the REG*
- > *file.*
- >
- > *In summation, I can't and don't leave things to chance. I force the configuration and*
- > *updating guaranteeing protection and equality of McAfee AV software on ALL my workstations.*
- > *I over ride the local reporting with Cetralized Reporting and I take advantage of*
- > *Centralized Alerting. I get ASCII log files with which I use to maintain historical log*
- > *records in case of a security audit.*
- >

microsoft.public.security.virus: Re: Norton vs McAfee

> *I hope you enjoyed the above "ramblings" :-)*

>

> *Dave*

>

>