

RE: [SPAM] – RE: recommendations for centrally managed corporate antivirus solution – Bayesian Filter detected spam

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-02/msg00354.html>

- *From:* "Hopke, Greg" <GHopke@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 19 Feb 2008 12:22:49 -0500
-

You can point any pc in EPO to use the McAfee http site for DAT updates as a failover if the pc is not on your LAN for updates. This is great for laptops.

Greg

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx>]

On Behalf Of Albert Gonzalez

Sent: Friday, February 15, 2008 9:49 PM

To: Secure This; illuminaeti@xxxxxxxxxx

Cc: security-basics@xxxxxxxxxxxxxxxxxxxxx

Subject: [SPAM] – RE: recommendations for centrally managed corporate antivirus solution – Bayesian Filter detected spam

We currently use McAfee and their ePo server. We manage roughly 12000~ clients. The reporting makes the higher ups happy and is generally fast and smooth with custom granular control. Unfortunately it does not allow updates via the internet, only via our corp mgmt server(s). We just rolled out their HIPS solution, and all it took was a flick of the switch and as clients check in (often right? :) the agent was deployed. I am happy with the implementation, although this and symantec are the only ones I have seen (corp deployments) I have not had the chance to do any bakeoffs as these are existing infrastructures.

Opinions and experiences help, but every environment is different and highly depends on what you want to report on. It all boils down to reporting and that "warm fuzzy" feeling.

Thanks,
– Albert

— Sent from my HTC8600.

Success comes to the person who does today, what you're thinking of doing tomorrow.

RE: [SPAM] – RE: recommendations for centrally managed corporate antivirus solution – Bayesian Filter detected spam

-----Original Message-----

From: Secure This <lists@xxxxxxxxxxxxxxxx>

Sent: Friday, February 15, 2008 8:43 AM

To: illuminaeti@xxxxxxxx

Cc: security-basics@xxxxxxxxxxxxxxxx

Subject: Re: recommendations for centrally managed corporate antivirus solution

McAfee EPO is the main player in the large corporate sector in the Europe from my experience of around 50 large companies. Most seem happy enough with it and renew their contracts. Works well across multi office

companies.

Hi list

On the different networks I manage, I've been using Symantec corporate since version 7. I've never had any major issues with it until now.

Version 11, now called "Symantec endpoint Protection" requires IIS and

either MS SQL or the symantec embedded database. I installed a copy on a test server and it just about crippled it. Network access from clients was incredibly slow and processor use was hitting %100. I've heard the same comments from a colleague who installed it on a new server at the customer's request. The file server was virtually unusable even before the client was installed on the workstation. Also the new GUI is just plain awful.

I don't have the time or resources to tweak settings to get better performance out of the AV.

I've heard good things about NOD32, Sophos and Kaspersky. I've started looking around and of course, every website I visit tells me the software they sell is the best in the universe.

So, looking for real answers from real users, I thought I'd ask you all about your experience, positive or negative, with various corporate antivirus software.

Thanks in advance.

RE: [SPAM] – RE: recommendations for centrally managed corporate antivirus solution – Bayesian Filter detected spam