

## Re: Betr.: Re: MS Patches Management software: SUS vs 3rd party

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-11/0207.html>

---

**From:** Neil Fryer ([nfryer\\_at\\_marimba.com](mailto:nfryer_at_marimba.com))

**Date:** 11/11/03

Date: Tue, 11 Nov 2003 18:28:55 +0000

To: "Philip Wagenaar" <[p.wagenaar@accon.nl](mailto:p.wagenaar@accon.nl)>

Hi Philip,

I know that this may be a bit late, and this is not an excuse to get the company that I work at more money either. As even if that was the case I wouldn't directly see any of it.

If you are looking at Patch Management solutions, have a look at us if nothing else.

<http://www.marimba.com>

I hope that if nothing else it gives you another avenue to explore.

Kind Regards,

Neil Fryer

On Wednesday, Oct 29, 2003, at 08:11 Europe/London, Philip Wagenaar wrote:

- > *We are also currently looking at a solution for updating our clients*
- > *and servers.*
- >
- > *We have tested SUS server (free from Microsoft) as disucced before.*
- > *The major drawback is that if a new unpatched client connects to it,*
- > *it retrieves all patches at once. There is no management in SUS,*
- > *except approving new updates.*
- >
- > *Currently Microsoft is holding a betaprogram for the next version of*
- > *SUS <http://www.betanews.com/article.php3?sid=1060982281> where you can*
- > *find out more about it (or just go directly to*
- > *<http://www.betaplace.com> (Microsoft's betaprogram's website) and log*
- > *in using the Guest ID MSUSCustNom*
- >
- > *Another program we are going to test is Service Pack Manager from*
- > *[www.raxco.nl](http://www.raxco.nl). This program has much better management options and*
- > *supports NT 4.*

>  
> *Met vriendelijke groet,*  
>  
> *Philip Wagenaar*  
>  
> *AccoN Accountants & Adviseurs*  
> *ICT Project Bureau*  
> *Postbus 5090*  
> *6802 EB Arnhem*  
> *The Netherlands*  
>  
> *tel. +31 (0)26-3842384*  
> *fax. +31 (0)26-3630222*  
> *mobile: +31 (0)6-25388935*  
> *MSN/E-mail: p.wagenaar@accon.nl*  
> *<http://www.accon.nl>*  
>  
>  
>>>> *Charles Otstot <charles.otstot@ncmail.net> 28-10-03 14:05 >>>*  
> *Andres,*  
>  
> *If they are planning to include the Windows NT 4.0 servers for the*  
> *period they are in use, SUS is out. SUS only works on 2000 and above.*  
> *Shavlik make a couple of products, HFNETCHK Pro (paid version) and*  
> *HFNETCHK LT (free version). LT was limited in it's abilities at one*  
> *point, I've not really kept up with it, but it is suitable for some*  
> *locations.*  
> *As to other commercial products, ST Bernard and Shavlik both do a solid*  
> *job for MS patches.*  
> *If you want more than Microsoft patches, about the only product*  
> *available is PatchLink ([patchlink.com](http://patchlink.com)). PatchLink does a reasonably*  
> *good*  
> *job for MS patches, but also provides the ability to patch other OSes*  
> *and*  
> *application vendor products.*  
> *The other primary players in this market are Service Pack Manager (I*  
> *tested this product and was not overly impressed.) and a fairly new*  
> *product by Ecora which I have not tested (I completed my testing before*  
> *the product was introduced.)*  
>  
> *I would note that, given the tone of your posting, it is highly*  
> *unlikely*  
> *that the servers have reached a consistent patch level. You may find*  
> *that patching with any of the patch distribution tools in this scenario*  
> *will not be totally successful initially. You may want to consider*  
> *recommending (or creating for them) batch files for an initial rollout*  
> *to bring the servers to a consistent patch level \*before\* using any of*  
> *the patch tools. Most of the products will allow you to set mandatory*  
> *patch levels, but they will also be patching \*immediately\* if you*  
> *place a server into a group with mandatory patches (no ability to*  
> *schedule=reboots at bad times). The rationale (as best as I can figure)*

- > *is that a server should not be in use if it is non-compliant, and if a*
- > *server already in use \*becomes\* non-compliant with your mandatory*
- > *configuration, immediate action is required. This may help you avoid an*
- > *easy trap to fall into (i.e. setting your mandatory patches and placing*
- > *all your servers into the group at initial setup). Once you have*
- > *patched*
- > *to the necessary level, you can place servers into mandatory groups if*
- > *you desire. Again, don't put new patches into the mandatory until*
- > *they've been rolled out. At this point, you can schedule new patches to*
- > *be rolled out individually (and where required) with installation and*
- > *reboot at any time the server owner requires.*
- > *I would also recommend that they centralize antivirus services with one*
- > *or more master servers passing out updates to client servers.*
- > *Symantec's Corporate Edition is fairly easy and straightforward to*
- > *configure and with the System Center Console installed, is easy to*
- > *manage.*
- >
- > *The major issue I see with either of these two pieces is the*
- > *(apparently) total decentralization of server management. All of the*
- > *patch distribution mechanisms and Symantec CE assume/depend on at least*
- > *some level of centralized management. Obviously, the more important*
- > *and*
- > *difficult issues you face (e.g. lack of policies) are completely*
- > *dependent upon at least some level of centralized management/authority.*
- > *It really seems to me that your first and foremost recommendation has*
- > *to be that the client develop some sort of centralized control,*
- > *otherwise they have no real hope of resolving their issues (if they*
- > *consider the things you've listed issues at all).*
- >
- > *Charlie*
- >
- >
- > *Andres Martinez wrote:*
- >
- >> *I'm looking the best solution for one of our customers to deal with*
- >> *the administration and deployment of security patches, if somebody*
- >> *can make a recommendation based on real experience I'll appreciate.*
- >> *Customer server environment:*
- >>
- >> *125 servers: 80% Windows 2000 – 20 % Windows NT 4.0 (They are*
- >> *planning to get rid of NT servers soon)*
- >> *All servers on same physical location.*
- >> *There is no central administration of servers: Server managment*
- >> *provided for different people with different Technical skills. Hard*
- >> *to get control. Few IT resources.*
- >> *By default Windows installations = High risk of security problems.*
- >> *Lack of security policies for server management and security.*
- >> *Very reactive to solve problems.*
- >> *Lack of software or scripts to automatize processes like patches*
- >> *deployment.*
- >> *They already have had serious problems due to virus like welchia and*

SecurityFocus BASICS: Re: Betr.: Re: MS Patches Management software: SUS vs 3rd party

>> *blaster who exploit know security vulnerabilities.*  
>> *Corporate Symantec antivirus used for virus protection, but not*  
>> *installed on all servers, problems with antivirus updates on some*  
>> *servers.*  
>> *It is hard to obtain approval for reboot servers due to mission*  
>> *critical role and business nature (healthcare industry), so minimum*  
>> *downtime is required.*  
>> *What would you use ?*  
>>  
>> *MS Software Update Services (SUS) which is free*  
>>  
>> *or Third party software like Hfnetchk Pro or St Bernard Update expert*  
>> *(<http://www.mcpmag.com/Features/print.asp?EditorialsID=354>)*  
>>  
>>  
>>  
>> *Waiting for your comments*  
>>  
>>  
>>  
>> *Thanks*  
>>  
>>  
>>  
>> *Andres*  
>>  
>>  
>>  
>>

---

>> -----  
>> *Forum Systems PRESIDIO: PGP / XML GATEWAY APPLIANCE*  
>> *The Presidio integrates PGP data encryption and XML Web Services*  
>> *security to*  
>> *simplify the management and deployment of PGP and reduce overall PGP*  
>> *costs*  
>> *by up to 80%.*  
>> *FREE WHITEPAPER & 30 Day Trial –*  
>> *[http://www.securityfocus.com/sponsor/ForumSystems\\_security-](http://www.securityfocus.com/sponsor/ForumSystems_security-basics_031027)*  
>> *basics\_031027*  
>>

---

>> -----  
>>  
>>  
>>  
>  
>  
>  
>  
>

---

Re: Betr.: Re: MS Patches Management software: SUS vs 3rd party

> -----  
> *Forum Systems PRESIDIO: PGP / XML GATEWAY APPLIANCE*  
> *The Presidio integrates PGP data encryption and XML Web Services*  
> *security to*  
> *simplify the management and deployment of PGP and reduce overall PGP*  
> *costs*  
> *by up to 80%.*  
> *FREE WHITEPAPER & 30 Day Trial –*  
> *[http://www.securityfocus.com/sponsor/ForumSystems\\_security-](http://www.securityfocus.com/sponsor/ForumSystems_security-basics_031027)*  
> *basics\_031027*

> -----  
>  
> #####  
>  
> *Dit e-mailbericht is uitsluitend bestemd voor de geadresseerde.*  
> *De informatie hierin is vertrouwelijk, zodat het derden niet is*  
> *toegestaan om daarvan kennis te nemen of dit te verstrekken aan*  
> *andere derden. Indien u dit e-mail bericht ontvangt terwijl het*  
> *niet voor u bestemd is, verzoeken wij u contact op te nemen met*  
> *de afzender en de informatie te verwijderen van iedere computer.*  
> *Bij voorbaat dank.*

> -----  
>  
> *The information transmitted in this e-mail is intended only for*  
> *the person or entity to which it is addressed and contains*  
> *confidential information. Any review, retransmission or other*  
> *use by persons or entities other than the intended recipient is*  
> *prohibited. If you received this in error, please contact the*  
> *sender and delete the material from any computer. Thank you.*  
>  
> #####  
>  
> #####  
> #####  
> *This e-mail message has been scanned for Viruses and Content and*  
> *cleared*  
> *by MailMarshal*  
> #####  
> #####

> -----  
> *Forum Systems PRESIDIO: PGP / XML GATEWAY APPLIANCE*  
> *The Presidio integrates PGP data encryption and XML Web Services*  
> *security to*  
> *simplify the management and deployment of PGP and reduce overall PGP*

SecurityFocus BASICS: Re: Betr.: Re: MS Patches Management software: SUS vs 3rd party

- > *costs*
- > *by up to 80%.*
- > *FREE WHITEPAPER & 30 Day Trial –*
- > *[http://www.securityfocus.com/sponsor/ForumSystems\\_security–](http://www.securityfocus.com/sponsor/ForumSystems_security-basics_031027)*
- > *basics\_031027*

>

> -----

---

Forum Systems PRESIDIO: PGP / XML GATEWAY APPLIANCE

The Presidio integrates PGP data encryption and XML Web Services security to simplify the management and deployment of PGP and reduce overall PGP costs by up to 80%.

FREE WHITEPAPER & 30 Day Trial –

[http://www.securityfocus.com/sponsor/ForumSystems\\_security–basics\\_031027](http://www.securityfocus.com/sponsor/ForumSystems_security-basics_031027)

---