

Espion Interceptor Solution Comparison

So, how does the Interceptor based solution differ from what you currently have?
Here's how - take a look at the three scenarios below:

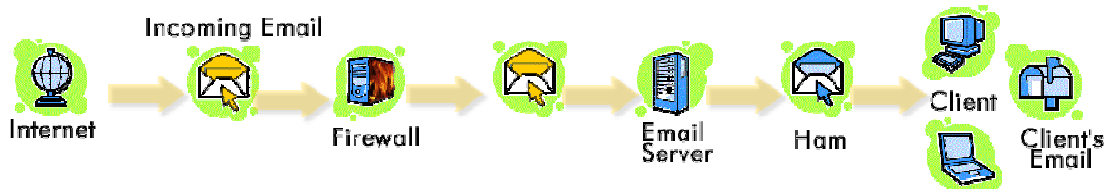
- SCENARIO 1 - typical client based spam and virus protection
- SCENARIO 2 - typical email server based spam and virus protection

NOTE: if you don't do either scenario 1 or 2, then maybe you should immediately give us a call ☺

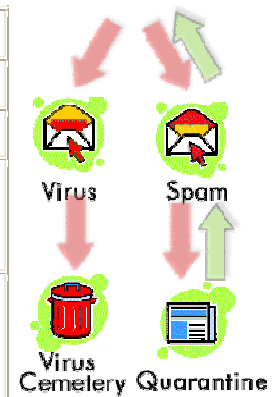
- INTERCEPTOR SCENARIO - typical "moat" approach

SCENARIO 1:

This is typical of a small to medium organisation that relies on virus and spam protection being installed, and maintained current on each PC workstation.



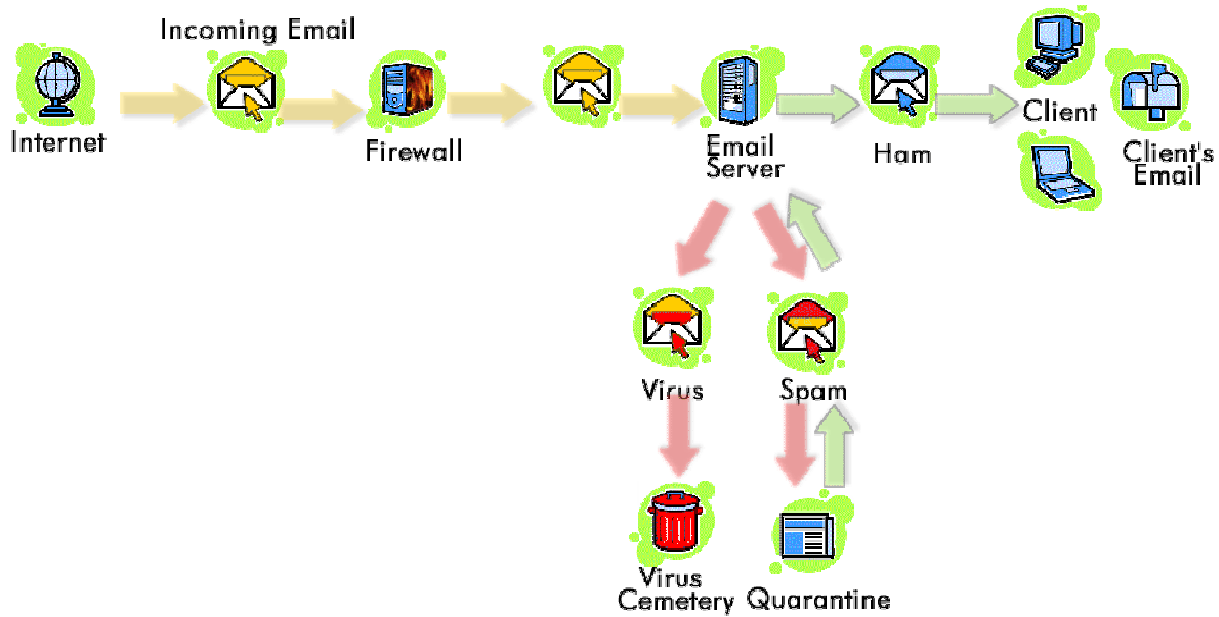
SCENARIO 1		
Characteristic	Exposure	Description
Security Risk	HIGH	All viruses reach the client PC
Maintenance	HIGH	Each client PC needs to be constantly maintained (OS, virus and spam software - ie Windows, McAfee, Symantec, etc.)
Cost	MEDIUM- >HIGH	Each client PC needs to be licensed (virus and spam software - ie. Symantec, McAfee). Also client maintenance cost is significant (either system administrator or each employee)
Scalability	HIGH	Horizontal scalability model ensures no limits other than network bandwidth and depth of your pockets.
Economies of scale	LOW	The more you grow the more it costs - each new employee workstation increases the overall solution cost and management complexity.



Espion Interceptor Solution Comparison

SCENARIO 2:

This is typical of a medium to large organisation that relies on virus and spam protection being installed, and maintained current on their mail server.

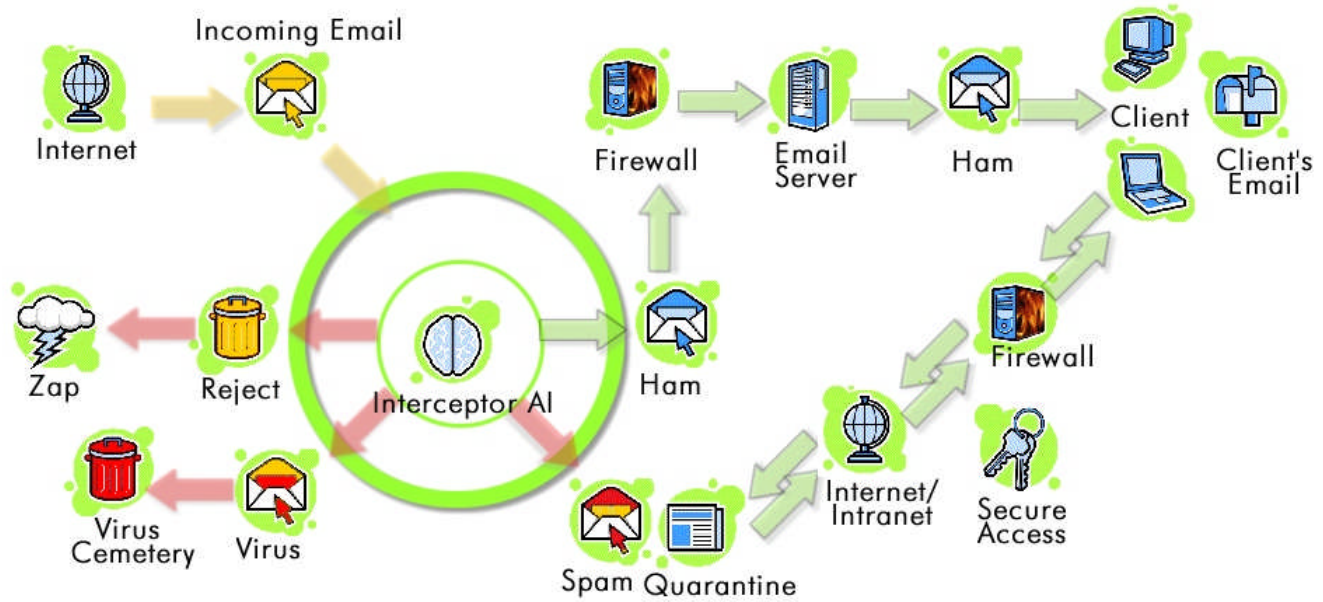


SCENARIO 2		
Characteristic	Exposure	Description
Security Risk	HIGH	All viruses reach the corporate email server
Maintenance	MEDIUM	Only email server needs to be constantly maintained (virus and spam software)
Cost	MEDIUM->HIGH	Each new email client needs to be licensed (virus and spam software on the email server - ie Symantec, McAfee, SurfControl, etc. all based their licensing on the number of email boxes)
Scalability	LOW	Very limited vertical scalability as it directly depends on the email server hardware. Also as an added nuisance, the performance of the email server directly depends on the amount of overhead that it has to do in order to process viruses and spam load.
Economies of scale	LOW	The more you grow the more it costs - each new employee workstation increases the overall solution cost.

Espion Interceptor Solution Comparison

INTERCEPTOR SCENARIO:

This is how Interceptor shields your organisation from spam and viruses.



INTERCEPTOR SCENARIO		
Characteristic	Exposure	Description
Security Risk	LOW	All viruses and spam are stopped before they even enter your network, let alone your email server or even worse, your email client.
Maintenance	NEAR ZERO	Interceptor updates itself - virus, spam, web attack and IDS signatures - you may want to do the reporting either yourself or we can do even that for you.
Cost	LOW	Interceptor is an appliance - hence costs the same regardless of how many email accounts it handles.
Scalability	HIGH	Interceptor scales from a few hundred email accounts to 20,000 email accounts with the same hardware and software stack - the only difference between the solutions lies in the hardware speeds and feeds - CPU, memory and disk speed.
Economies of scale	HIGH	The more you grow the cheaper it gets - each new employee workstation decreases the cost per email account - since Interceptor costs the same.

BackGround Software

Espion Interceptor Solution Comparison

4

For more information, please contact:
BackGround (BGD) Software Inc.
7398 Yonge St., Suite 118
Thornhill, ON L4J 8J2 CANADA
Tel: (416) 917-0130
Toll-Free: (888) 230-8320
EMail: sales@bgdsoftware.com
WWW: <http://www.bgdsoftware.com>

BackGround Software
(BGD Software Inc.)

7398 Yonge Street, Suite 118 Thornhill, ON L4J 8J2, CANADA
Phone: 416-917-0130 Toll-free: 888-230-8320 Email: info@bgdsoftware.com Web: <http://www.bgdsoftware.com>