CORPORATE VIRUS PROTECTION

Today's Product Selection Criteria

At Trend Micro, we are talking to corporate information security experts every day. Through these conversations, we get a pretty good picture of what's important to them in selecting virus protection software — and what's not important.

Here's a summary of how Trend's customers value the different aspects of anti-virus software functionality:

Functionality	**Importance to the Customer**
Virus detection performance	Provided the vendor has ICSA or CheckMark certification, very few customers spend time conducting their own detection tests as part of the evaluation process.
Detection capability for other malicious code threats (Trojans, droppers, ActiveX and Java)	Customers do worry about threats that are coming over the horizon. But if those threats are not yet 'in the wild', a contractual commitment from the vendor to provide detection when it's needed is usually sufficient.
Responsiveness to new threats	If those new threats — whether they're new 'traditional' viruses or new types of malicious code — become reality, customers need to know they can rely on their vendor's research team to deliver a solution fast.
Service and support	In the constantly changing landscape of virus and malicious code detection, commitment to ongoing service and support is vital. What is provided as part of the base price, what is available as an optional extra and the type of year-on-year maintenance agreements available are key selection criteria.
A comprehensive range of integrated protection products	Virus and malicious code threats can come from many sources. Customers need to be sure they're not leaving any potential entry point unprotected. And product integration and effective management tools mean that maintenance tasks like updating need to be undertaken only once.
Manageability	META Group says: "If you can't centrally manage your virus protection software, then you don't have virus protection." Our customers agree with this 100% - they know they can't rely on end users to keep their anti-virus activated and updated.
Remote user management	With the rapid growth of telecommuting, 'hot-desking' and home-based satellite offices, out of sight must not equal out of mind when it comes to virus protection. Remote users are connecting to the network, opening up yet more virus entry points, so administrators have to be able to ensure those remote systems have the same level of protection as locally-connected machines.
Central reporting	As with the manageability issue, customers recognize that if they can't pull together a single picture of the vulnerabilities of their networks, they are going to miss potential — even actual — virus outbreaks.
System performance	If virus protection interferes with system performance, mail delivery, or other key aspects of today's business communication processes, end users are going to try to disable it or otherwise get around it. Another red flag.
Remote (browser-based) administration	And if the administrators themselves are remote, a browser interface means they can manage enterprise-wide anti-virus issues wherever they are.
Automatic deployment and	Administrators today can be responsible for thousands of individual

updating	desktops at dozens of different sites. There's no way they can visit every individual desktop to ensure that it's updated and correctly configured. Quite rightly, they demand that the anti-virus software automates this process.

*Both ICSA and CheckMark certification marks are awarded to products that detect 100% of 'in the wild' viruses and 90% of 'zoo' viruses. Further information on the web at http://www.icsa.net and http://www.westcoast.com.