Dual Scanning Virus Protection

The Excedent virus scanning solution scans all inbound and outbound emails using a unique three-stage, dual scanner process.

Stage 1: The Pre-scan
The first stage serves two functions. First, it searches for email vulnerabilities. It then searches for MIME segments that have the potential to carry a virus.

By searching for email vulnerabilities, the scanner is able to block emails that are dangerously formatted and which could execute code without user intervention. This includes protection against all known Microsoft Outlook security threats such as MIME headers exploits, fragmented message segments and file extension obscuring. This most notably provides protection against worm viruses that can replicate themselves by using the Microsoft Outlook address book.

If vulnerabilities are found, the email is quarantined and the sender is notified (see Virus Notifications).

The system then checks for any portion of the email that could possibly contain a virus. If all MIME segments are guaranteed to be safe, then scanning stops at Stage 1. However, if any MIME segment is found that is not guaranteed to be safe, the email continues to Stage 2. This eliminates unnecessary scanning of plain-text emails and safe attachments such as images, keeping email delivery ultra-efficient without compromising email security.

Stage 2: The Dual Virus Scan
Any portion of an email that has the possibility to contain a virus is scanned during Stage 2. This includes almost every type of file attachment as well as HTML messages and embedded scripts. Redundant, industry leading virus scanners are put to use, rooting out malicious worms, Trojan horses, and macros before they have a chance to do any harm.

Each portion of an email is passed through two, independent virus scanners to ensure maximum protection against new email born viruses. Clam AntiVirus (www.clamav.net) and F-Prot (www.frisk-software.com) are the current scanners of choice. Both companies maintain 24-hour dedicated virus researchers who respond to new and emerging threats, doubling the chances of blocking new virus outbreaks. Updated virus definitions are automatically installed hourly and can be manually updated at the push-of-a-button when emergency virus alerts are made public.

The Excedent system was built from the ground up with the ability to “plug-in” virtually any virus scanner on the market. This protects Stage 2 of the Excedent system from depending on any one company, and allows for seamless upgrades to the latest “best-of-breed” virus protection as the market evolves.

If a virus is found, the email is quarantined and the sender is notified (see Virus Notifications).

Stage 3: Restricted Attachments
A final level of protection prevents the sending of certain types of attachments, which could contain dangerous code and are often used by malicious hackers to spread viruses. These files either contain executable code themselves or may contain links to other files that contain executable code. Restricted file types include, but are not limited to program files (.exe, .com), script modules and files (.bas, .vbs, .js), Internet links (.url, .ins), and shortcuts to files (.lnk, .pif).

When an email is sent that contains a restricted file attachment, the sender receives a "bounced" email notification informing them of the restriction.

Virus Notifications
When a virus or email vulnerability is found, the email is quarantined within the network and the sender receives a detailed email notification about the virus. A notification is also sent to the intended recipient only if the message was sent to a local user on the same domain. This protects companies from the embarrassment of inadvertently attempting to send a virus to one of their customers or to another company.

Some viruses are known to forge the sender's "From" address, such as the recent Klez virus. These forgeries are recognized by the system, and only the appropriate party receives the virus notification.

Zero Added Points of Failure
Redundancy and fail-over support are built into every aspect of the Excedent system. Should any portion of this three-stage process fail, safeguards are in place to ensure that the remaining stages execute and email traffic continues without interruption.

Effectiveness
Thousands of virus-infected emails arrive at the Excedent system each day. To date, not a single infected email is known to have made it through successfully. Even newborn viruses that have not yet been added to the virus definitions are stopped at the door.

About Webmail.us
Webmail.us provides small businesses with email hosting solutions based on proven, open-source software applications. The company eliminates the need for customers to purchase and manage email-related software, hardware or security services. All email hosting packages include domain-based email with secure POP3, IMAP4, spam and virus protection, large mailboxes and an Outlook style webmail interface. Webmail.us is a TRUSTe privacy seal holder and a wholly owned subsidiary of Excedent Technologies. For more information, please visit us at www.webmail.us.