



Avalon Email Threat Protection

Avalon's Email Threat Protection service provides the most effective blocking of spam, viruses and phishing exploits, while restoring end-user confidence in email. With Avalon, email users enjoy unparalleled proactive and granular control over access to their inbox -- access is denied to unwanted senders and content, while access is assured for the mail they want to receive. Powerful end-user controls are matched by exceptional configurability for solution providers, enabling them to meet the widest range of customer requirements and address the toughest spam problems. Standard configuration options simplify deployment.

Avalon Defenses

Users have access to a broad range of blended email defenses and can modify the deployment options to create custom defaults for new users. These configurations can be made available to the end-user, or reserved for use by Solution Providers on behalf of their clients. As a result, Avalon provides an effective method for every user's needs and preferences.

Whitelisting	Users often get started by using Avalon's automated Outlook Whitelister to build a whitelist of their legitimate correspondents. This is accomplished by running an automated utility that harvests Outlook contacts and addresses from messages in one's Sent folder. Automated "whitelist on first outbound" and "whitelist on reply" features then keep building one's whitelist over time. Whitelisting can be done on an address or domain basis.
Content Filtering	Users are generally deployed utilizing content filtering to screen messages from unknown senders. Filtering provides simple set-and-forget protection, although users must recognize that filtering is a fallible technology that requires routine inspection of a quarantine folder to identify erroneously blocked messages. Avalon provides a simple means for the user to tailor the sensitivity of the filter for their specific preferences.
Challenge-Response	When users receive a message from a sender who is not on their whitelist and that fails the content filter, they may choose to send an automated reply asking the other party to resend their message or click a link to add themselves to the whitelist and resend the original message. While legitimate correspondents will typically comply, spammers often do not monitor or respond to such messages, and hence their messages aren't cleared for delivery.
Protective Addresses / Address-on-the-Fly™ (AOTF)	Avalon makes it easy for users to employ multiple addresses for a single inbox. We refer to these addresses as Protective Addresses because they provide both a means of protecting the integrity of one's primary email address and of protecting access to one's inbox. Avalon's Address-on-the-Fly™ feature enables one to spontaneously declare a purpose-specific address for disclosure on a web site, in a discussion forum, in print or conversation, etc. These addresses take the form of a root name plus a suffix of the user's own choosing. For example, when registering on eBay, Jane Doe might use the address jdoe.ebay@herdomain.com , where the ".ebay" suffix serves as an "email PIN" that assures delivery of email sent to this address. Addresses are independently controllable by policy, so that legitimate users of the address can be "locked down" in the event the address is ever harvested and abused by a spammer.

Avalon Permitted Languages	This capability augments traditional content filtering by blocking messages in any language other than those specifically approved for delivery at the enterprise and individual user levels.
Avalon Permitted Countries	Based upon enterprise and user level settings, this capability makes delivery decisions based on a message's country of origin. Many domestic businesses, for example, may not ever want to receive email that can be determined to have originated outside the home country. This feature also includes the capability to map an organization's incoming email by country of origin.
Total Control	Total Control leverages the full power of Protective Address to provide maximum control over access to one's inbox. In this mode, Avalon utilizes an automatic challenge-response for every new inbound correspondent, asking them to resend their message to a Protective Address with a suffix automatically assigned by Avalon. By establishing correspondent-specific To – From address pairs, each controllable by policy, Avalon deprives spammers of their primary technique – if they spoof the From address, they must associate it with the proper To address in order to reach the user's inbox; the chances of this are negligible. Hence the name Total Control.
Anti-Virus	Avalon scans both incoming and outgoing mail for viruses, worms, and other malware. Virus scanning occurs after other
Blended Defenses	Avalon enables users to mix-and-match various defenses to suit their specific preferences. Our experience shows that blending Protective Addresses with traditional methods produces a stronger defense that also avoids the pitfalls of traditional defenses used independently.
Outbound Mail Auditing	Avalon also blocks outbound email that contains spam and viruses, and provides a means of rate-limiting outbound email volumes. We use these features to identify and alert on open relay conditions and potential compromised, "zombie" PCs, in order to prevent our customers from inadvertently spamming their contacts and to avoid blacklisting, with the business disruption that accompanies that unpleasant outcome.

Spam Handling Options

After configuring the preferred defenses, the next step is to specify the manner in which Avalon should handle spam. Again, a variety of options exist to respond to individual or organizational preferences.

Flag and Deliver	A user who doesn't have a serious spam problem may elect to have spam delivered to their inbox with a spam tag in the subject line. This avoids the need to examine the daily digest or inspect the quarantine, and enables the recipient to identify a false-positive immediately.
Quarantine	Spam can be delivered to a quarantine folder for periodic inspection by the intended recipient.
Daily Spam Digest	Users may elect to receive a daily summary of the new mail diverted to their quarantine folder. The summary includes the sender, subject line, date and time, and links to either release a message to one's inbox, or release the message and whitelist the sender, so that future mail from the sender will be delivered directly to the recipient's inbox.

Delegated Spam Folder	Spam may also be diverted to a folder managed by someone other than the recipient. For example, an administrative assistant might manage the DSF for an entire department, or someone in IT might do it for the entire company.
Vaporize	After becoming comfortable with the accuracy of their protection, some users elect to vaporize spam rather than quarantine it. Alternatively, one may elect to vaporize only those messages with a score that exceeds a pre-specified threshold – everything else goes into the quarantine.
Challenge-Response	A user can also choose to Quarantine spam or senders that are not on their whitelist, and opt to send a notification back to the sender providing the ability to whitelist themselves, or send the original email to a new Protective Address.

Other Features

Avalon includes a number of other features that enhance the overall email experience.	
Granular Security States	Avalon's granular inbox access control flows in part from the range of security states that can be applied to a specific sender and address. For example, if an Address-on-the-Fly starts to attract spam, users have a variety of choices – they can (a) block the specific abusing sender, (b) lock down the address, reserving its future use solely for the existing community of legitimate senders, (c) restrict future use just to senders at the domain of the sender to which it was initially disclosed, (d) restrict use even further to just the party to which it was initially disclosed, or (e) disable the address, in which case all future incoming mail on the address will be blocked, flagged or challenged.
User Control Panel	As an option, Avalon automatically inserts a control panel at the bottom of incoming messages, and removes it on Forward or Reply. This control panel provides a means of communicating with the user, for example, to inform them when one correspondent appears to have shared their address with a third party. It also provides a simple means for the user to update their access preferences for a specific sender and address, by clicking on the intuitive in-message links that are provided. Avalon's control panel has been translated into Spanish, French, German, Brazilian Portuguese, Dutch, Italian and Chinese, with Russian and Hebrew on the way.

Administration

Avalon includes a range of tools to help solution providers and ISPs manage the email environment and troubleshoot issues.

LDAP Integration	Avalon's LDAP Exporter is run on the LDAP server to synchronize users and domains up to the Avalon server for automated deployment.
Unified Log	The unified log consolidates information from various sources to simplify the process of diagnosing a potential delivery issue.
Usability Features	The Avalon portal provides an extensive history system, pages are searchable and sortable to identify sharing events or enforce policies on who can use a particular Protective Address, or who is part of a community whitelist able to send email to a specific address.
SMTP Enforcement / Protection Against DoS and	Avalon uses its LDAP sync capabilities to maintain a database of known users at each customer domain. This database enables the system to deny delivery

DHA	of mail to unknown users after receiving the "To:" address from the header. This approach provides protection against directory harvest and denial of service attacks, and can save considerable bandwidth.
Open Relay Detection	Avalon's outbound mail auditing capability enables the system to block mail to and from the same user, which is indicative of an open relay condition.
Graphs and Statistics	The Avalon portal provides a capability to graph various email statistics over time, such as the volumes of mail sent to unknown users, spam, and legitimate outgoing mail.

Other Email Services

Over time Avalon will include a growing number of email services not directly related to security.

Email Continuity	When a customer's local email server experiences an outage, Avalon automatically queues all incoming mail until the server comes back on line, at which point it resumes delivery.
Large File Handling	Avalon handles attachments up to 25 MB in size. Special arrangements can be made in advance if a customer needs to send a larger attachment.