



Email Defense

Superior Email Filtering

LuxSci provides one of the most comprehensive email filtering solutions currently available. Whether you are looking for protection from spam, viruses, attachments, HTML, malicious content, or email attacks, Email Defense is there to protect you.



- All email that you receive for your domain will be filtered for the best protection — even email that is sent from other people in your domain outbound through LuxSci.
- You can protect a large number of addresses and aliases at different domains without having to purchase protection one license at a time. Instead, licenses are purchased on a domain wide basis.
- Setup takes only minutes — even for domains with thousands of users.

What Features Does Email Defense Have?

Email Defense Portal

Email Defense users and account administrators will be provided with access to the Email Defense portal where they can configure their email filtering policies, view detailed reports, see their quarantined messages and optionally release them for delivery.

High Availability and Zero Latency Message Delivery

Email Defense will not slow the speed of delivery of your email. Offering redundant, load-balanced server architecture, Email Defense provides carrier-class availability of filtering and delivery components. Sub-second processing provides for almost no delay as messages are “proxy-streamed” to their ultimate destinations.

Recipient Shield

Email Defense also allows administrators to add recipients to a Deny list, where incoming mail sent to specific email addresses (such as the address of a former employee) is denied, accepted and bounced, or accepted and discarded. These actions can be set to vary by whether the email address is found on the Deny list or is merely invalid in your domain.



Quarantine Reports

Protected users can get regular reports of messages that have been quarantined due to their anti-Spam, anti-Virus, or content filtering policies. Users can easily delete or release messages from the quarantine, as well as manage their allow and deny lists, from within their email program such as Outlook, Thunderbird or Entourage. Reports are also available at any time through the Email Defense portal.

Control Console

Email Defense's customizable and easy-to-use Control Console is a centralized management platform that provides you with one interface for managing all corporate-wide email threats, protection and security. Use the Control Console to:



- [Obtain cross-browser support](#) for both Internet Explorer and Firefox.
- [Establish numerous policies](#) that instruct the Email Defense Service on how to handle viruses, spam, unwanted attachments, unwanted content and unwanted HTML in messages intended for recipients on your network.
- [Reduce the IT department spam-management burden](#) by determining whether the quarantine process for spam and unwanted email will be managed by your IT department, your end users, or both.
- [Automatically quarantine suspect messages](#) by safely isolating unwanted messages outside of your network, where they can be reviewed and deleted, or released according to the policies you set.
- [Create customized message rules lists](#), including "Allow" and "Deny" lists (for message senders), as well as an "Exempt Users" list (for users and recipients). Filter emails by content, attachment type, and more.
- [Customize policy control and enforcement](#) to be able to implement and enforce email policy for your entire organization, whether your organization has one office or multiple offices located around the world.
- [Reduce corporate liability and risk](#) by only allowing safe emails into your network.

How does the Quarantine feature work?

Email Defense consistently achieves industry-leading low false positive rates using "intelligent," customizable spam filtering technology. Simply blocking or allowing email according to default rules isn't an effective method for optimizing filtering. With easy and personalized conditioning, Email Defense offers superior protection against spam and false positives.

Setting rules around legitimate messages

Allowing end-user control, where employees are allowed to "condition" their own quarantine, helps reduce the amount of time IT managers spend dealing with spam, and also further ensures that the appropriate messages are quarantined.



Sophisticated end-user conditioning

If you opt for end-user management, your employees will be sent a periodic Quarantine Report. Employees then review the messages identified as spam to further define the quarantine rules by deleting, forwarding, always allowing, or always denying the messages.

Spam and Virus Filtering

Email Defense empowers businesses to protect their networks from the damaging effects of spam, including IT resource drain, reduced employee productivity, increased legal liabilities, decreased network bandwidth, and costly downtime.

Protecting Your Network at the Perimeter

Virus and Worm Scanning provides organizations with an additional layer of virus protection at the network perimeter. Through sophisticated technology and content behavior analysis, Email Defense detects quarantines, blocks and strips viruses and worms before they can enter or leave the network. Email Defense's virus scanning feature is updated every five minutes with new virus and signature patterns to ensure continuous proactive virus protection.

Teaming with Anti-Virus Leaders

The Email Defense package provides complementary protection to on-premise anti-virus products, and is powered by industry-leading virus-scanning engines McAfee, Authentium and Sophos. With the Email Defense triple virus and worm solution, you get:

- Our proprietary worm detection technology, which identifies and intercepts zero-day mass mailing worms before they enter your corporate network.
- Protection from three leading third-party engines, McAfee, Authentium and Sophos.
- Sophisticated security to complement your current on-premise solution.
- Up-to-the-minute defense against the latest threats with virus definition updates every five minutes.

Zero-Day Worm Threat Protection

Email Defense's Virus and Worm Scanning feature protects customers from the dangers of mass mailing worms and viruses, often hours before anti-virus services can distribute signature updates to their customers. The Threat Center quickly identifies sudden surges of suspicious messages, which are then intercepted before they can reach customers' email networks.



Email Security Results

Using a multi-layered spam filtering approach, Email Defense can dynamically calculate the spam probability of each spam message and:

- Instantly block 99% of spam
- Complete safe, external scanning to block spam before it reaches your network
- Accurately filter content to ensure industry-leading low false positive rates
- Provide up-to-the-minute defense against the latest blended email threats
- Effectively quarantine spam for seven days
- Generate custom quarantine management reports



Sophisticated Filtering

Unlike some competitor spam filtering solutions which use only a single spam classification technique, Email Defense leverages several of the industry's most effective spam detection techniques to separately analyze the same message, including:

- **Premium Anti-Spam Multi-Language Filter** – Utilizing Cloudmark AntiSpam filtering, this level of security protects you from Spam on a global scale. It is continually updated based on real-time feedback provided by a worldwide network of users. The software used for this filter is constantly being reevaluated to ensure that the very best programs are being used for our filters.
- **Sender Policy Framework (SPF)/Sender ID** – For inbound messages, LuxSci can check if the message has an associated SPF/Sender ID record. If there is, it can help determine if the email sender's domain is from a list of IP addresses authorized to send email from that domain. LuxSci can also protect your domain from being used in forged email messages.
- **Statistical Filtering** – Our filtering methods utilize a statistical Bayesian algorithm to determine the probability that an email message is spam based on how often elements in that message have appeared in other spam emails.
- **Industry Heuristics** – Email Defense incorporates thousands of successful industry-wide spam-fighting rules into its filtering layers.
- **Proprietary Heuristics** – Email Defense experts write and update thousands of proprietary rules to block spam using real-time data from the Threat Center.
- **URL filtering** – URL filtering works by comparing embedded links found in email messages with URLs associated with identified spam.
- **Reputation Analysis** – Like black and white lists, reputation analysis blocks spam based on comprehensive information about the source of the message – rating the reputation of the sender based upon the percentage of spam messages sent from that IP address in the past.
- **Reputation-based RBL filtering** – Email Defense assigns a level of trust to key real-time blackhole lists (RBL), which rates the reputation of the RBL based on its accuracy at blocking spam.

Fraud Protection and Anti-Phishing Features

Phishing attacks use spam techniques to distribute large volumes of fraudulent, yet official-looking, emails



designed to deceive consumers into disclosing sensitive information. By disguising the messages to appear from well-known banks, online retailers and credit card companies, phishers have been able to convince up to five percent of email users to give up sensitive personal information.

Phishing emails, like spam, can be identified and filtered out of inbound email to stop employees from receiving them. The Email Defense Service anti-spam rules automatically protect businesses from anti-fraud and phishing scams before they can enter your network. The Email Defense Threat Center monitors the global state of email communication, 24 hours a day, seven days a week, to stay ahead of the latest spam and phishing attacks and keep your network safe from unwanted mail.

Content and Attack Guards

Now, more than ever, individuals and enterprises need sophisticated tools to protect themselves and their end users against the increasingly advanced tactics of spammers. While spam poses some very real productivity problems for organizations, inappropriate content in email attachments also increase corporate risk and liability.

Stop SMTP Attacks

Significant threats to the enterprise come in the form of Denial-of-Service (DoS) attacks, Dictionary Harvest Attacks (DHA), mail bombs, email flooding, and other attacks designed to interrupt service or collect corporate or personal email addresses. Because email utilizes the Simple Mail Transport Protocol (SMTP), an open-recipient system that allows anyone to send messages to anyone else without the recipient's permission, your email server is always at risk for these attacks. Email Defense is here to help.

Shield Your Network

Our Email Defense Service removes the threat of network probes and completely shields your network from vulnerability and attack. You can now conceal your Internet-facing mail servers and gateways, and remove the threat of anonymous connections without hassle. By pointing your Mail Exchange (MX) record to Email Defense, a real-time filtering process:

- Conceal your critical messaging gateways and shieldgroupware email servers from attack
- Protect your email infrastructure at your network gateway, providing real-time monitoring and analysis of incoming messaging traffic
- Instantly block Denial of Service and other SMTP-based attacks, including dictionary attacks, email bombs and email flooding



Keyword Filtering

Content and Attachment Filtering is standard in the Email Defense Service and provides organizations with a layer of protection at the network perimeter. This filtering enables Email Defense to identify, quarantine and block unwanted and malicious content in body copy and in attachments before they can enter your internal network.

Keep Out Bugs

Web bugs are intrusive and nearly imperceptible tags embedded in HTML that give spammers the ability to monitor end-user activity and obtain their information. Our Content and Attachment Filtering includes an HTML shield that blocks web bugs as well as spam beacons.

Click Protection

What used to be a harmless click on an embedded email link to an unknown web site is now a security risk. Today, linking to suspect web sites can open up enterprises and their users to email attacks and other security risks that can drain valuable resources. To combat this, Email Defense can warn users before they link to suspect Web sites—further increasing corporate control and security.



Email Defense also provides enterprises with insight into their users' email and Web behavior by enabling them to track URL click-throughs from email to the Web. In addition, they can monitor if users are clicking on Web sites that would have negative consequences that could expose your infrastructure to hackers and continuous attacks.

How does Click Protection work?

Email Defense enables administrators to build URL white lists using full URL descriptors, straight IP addresses, and entire domains—all while leveraging wildcard (*) characters to maximize coverage.

Enterprises can choose to enable and disable URL click-throughs from email, or display a warning message before allowing or denying the click. Once clicked, the link is temporarily redirected to a pre-customized warning message for the user. Depending on the policy settings for that particular URL, the user will either be denied or allowed access to it.

Administrators can also generate reports on any URL links that have been clicked by a user and obtain other statistics for tracking URL trends. Reports can be configured per user or for the entire domain.

For more options, see our documentation [Email Defense: Optional Features](#).