MailInspector

Corporate Antispam and Email Gateway

Your company safe from targeted attacks, ransomware, virus, phishing, and unwanted emails.

Emails are the main tool for communication between companies all over the world, but for this same reason they are also the main source of attacks by people and criminal organizations that aim to steal money, data, and practice crimes against organizations of all types. What is even more concerning is that, as technology advances, virtual attacks also evolve and become more difficult to be detected at the same time their consequences are more devastating to organizations

On the same pace that virtual attacks are becoming more and more sophisticated, protection systems also need to evolve in order to prevent those new types of threats.

The HSC MailInspector is a complete email protection solution **that can detect security risks to organizations with precision rates above 99.8%.** For it uses more than 28 layers of protection that go through the connection layer to the message and attachments.

In addition to the local filtering layers that run in the local MailInspector appliance, the solution also uses a secure connection to HSC's global protection cloud: the Smart Defender.

There are **two antivirus engines** running simultaneously being one from HSC and the other from **BitDefender** – evaluated with the highest score by AVTEST.

Main protection technologies

APT - Advanced Persistent Threat

Protects against targeted and persistent attacks.

Zero-Hour Protection

Online verification of files, URLs and IPs reputation;

Compliance

Data Loss Prevention (DLP), cryptography, and audit.

Timeline

Dashboard showing all users' actions related to URLs and files.

Collaborative Analysis System

Analyzes URLs in a way that users can see a preview of the content of website pages and report security risks.

Online Sandbox

Simulates users' activities with the use of artificial intelligence, machine learning, among other technologies that analyze files and URLs and classify potential threats.

CDR - Content Disarm and Reconstruction

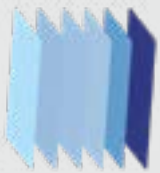
Removes potentially dangerous content from inside files, documents, and infected HTML, thus protecting users from zero-day attacks.

HSC MailInspector relies on its own technology for fighting targeted attacks, integrated to our security cloud which is able to eliminate threats in real time through machine learning, artificial intelligence, and sandbox technologies.

Smart Defender is a powerful threat detection engine that runs in HSC cloud. It uses behavior analysis technology to simulate users' possible actions when opening files or clicking on links received by email. This way, Smart Defender opens files and tests web pages, acting as a sandbox from our cloud and detecting security risks before they reach our customers' network.

Smart Defender engine inside MailInspector

MailInspector intercepts the messages before they get to the mail server so it can analyze them through its protection engines. The same way, it filters e-mails sent out of your company's domain, applying compliance rules.



When someone sends an email to a domain protected by MailInspector, it goes through 28 layers of filtering that analyze it from the connection layer to the message content – header, message body, IPs, links, and attachments – on the search for possible threats.

MailInspector sends IP addresses, URLs and attachments potentially dangerous to Smart Defender analysis. Which uses machine learning, sandbox, and URL crawler among other techniques to simulate users actions and find out the real intention of a website, IP, URL or attachment, blocking possible threats in real time even before they reach to the user inbox.

Through its exclusive engines, Smart Defender can detect threats in real time and block possible attacks by virus, phishing, ransomwares, and other threats. At the same time, it updates its global knowledge base so when a new threat is detected, all the users globally connected to its cloud get protected in less than 60 seconds.

Multiple Platforms and Installation Options

MailInspector Cloud

- It's the best option to protect email in the cloud. Protects on premise mail servers and cloud systems such as GSuite and Office 365.

- It's the only offer in the market that includes a protection module against Advanced Persistent Threat (APT).

- Daily delivery by email of personal quarantine summary.

- Users can mark messages as safe or block them, and manage senders and domains in their whitelist and blacklist – reducing the workload of infrastructure administrators.

- High availability and continuity of emails. Guaranteed message guarding at no additional cost in the event of a 24-hour failure on the local mail server.

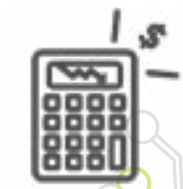
On Premise and Virtual Appliance

- HSC MailInspector can be implemented bare metal, in virtual servers as XenServer, VMware and Hyper-V, besides having a vendor certified physical appliance.

- With the on premise distribution, licensing is based on number of mail boxes so it's possible to configure high availability clusters without the need to hire additional servers.

- Besides the cloud version functionalities, the on premise version still permits more costumized spam and threats filtering configurations.

- The native load balance garantees better performance and security for the organizations filtering and delivering of emails.



Best cost benefit and BRL prices.

Double protection: HSC + BitDefender.

Administration and reports in one single interface.

Protection against APT and other threats.

Real time protection with Smart Defender

MailInspector is the leader solution in the Brazilian market for protecting and securing corporate emails. Among our customers are the most respected private and public organizations in Brazil and the South America.

For more informations, enter our website and get to know the E-mail Gateway MailInspector:

hscbrasil.com.br