

Product Name:

PAETEC's Hosted E-mail Security

Availability:

PAETEC's Hosted E-mail Security is available to all PAETEC markets.

Ideal Customer Profile:

Ideal customers include enterprise organizations maintaining their own e-mail server with a minimum of 25 e-mail boxes, often distributed through multiple, remote sites. Successful applications are prevalent in the finance / banking, healthcare, technology / media, and law vertical markets.

CPE Requirements:

There is no additional CPE required.

HOSTED E-MAIL SECURITY | In Brief

Product Description

PAETEC's proactive Hosted E-mail Security uses Internet-level scanning systems to stop e-mail-borne viruses, unsolicited mail, questionable content, and objectionable images before they reach your business network. Hosted E-mail Security services are PAETEC managed / hosted services that do not require any customer-owned hardware or software. PAETEC offers four modules in specified bundles as a complete and flexible solution: Anti-Virus (AV), Anti-Spam (AS), Image Control (IC), and Content Control (CC).

Product Capabilities

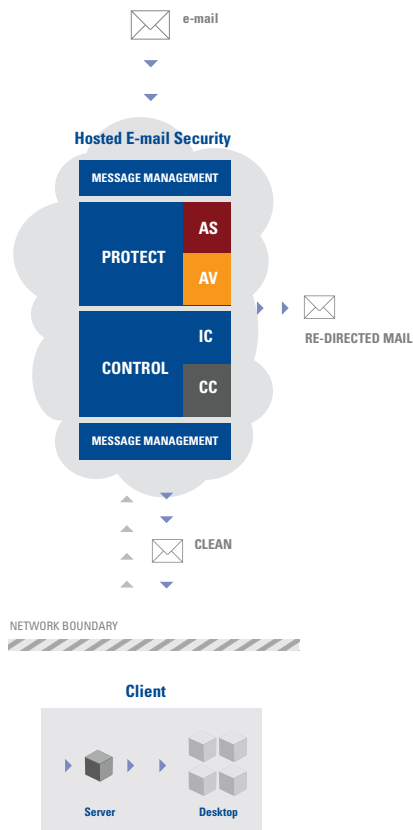
Proactive scanning solutions – Inbound and outbound e-mails are scanned at the Internet- level, which facilitates a cost-effective and architecturally better scanning solution

100% virus detection success rate to date – heuristic-based filters and artificial intelligence proactively detect known and unknown viruses

PAETEC Online – Our customer Web-based management portal enables direct control of AS, IC, and CC filtering criteria for both inbound and outbound e-mails, tracks end-user patterns, and allows customers to review statistical reports

Image Composition Analysis – Objectionable images are recognized through advanced image recognition technology, detecting and stopping suspect content

Tier One Data Centers – Control towers, equipped with mail processing servers, scan e-mail, stopping unwarranted messages prior to being delivered to its final destination; customers are simultaneously provisioned on two towers, in case of an outage



Application One

The United States University employs over 2,000 faculty and staff members on its city campus. In order to effectively prevent spam messages from entering the University's network, it implemented PAETEC's Hosted E-mail Security with Anti-Spam. Anti-Spam combines heuristics, public blacklists, and the University's configurable blacklists and whitelists to handle suspected spam messages according to their policy. Internally assigned University administrators control the filtering criteria for both inbound and outbound e-mails; notifications can be sent to the University's e-mail administrators or detected spam messages can be deleted. The Internet-level Anti-Spam solution saved network bandwidth and e-mail storage space by stopping spam before it reached the University's network. Anti-Spam also increased productivity by 15% because University employees spent less time manually filtering e-mails and more time focusing on business-critical initiatives.

Application Two

Last year, Fairport Financials suffered a network failure induced by an e-mail virus. Costly internal downtime, restoration, and e-mail backup procedures forced IT administrators to review their e-mail scanning solution. Today, Fairport Financials relies on PAETEC's Hosted E-mail Security, with Anti-Virus. Each e-mail message is simultaneously routed through two control towers, each equipped with four mail processing servers. Anti-Virus relies on patented artificial intelligence, which proactively detects both known and unknown viruses, and has a 100% success rate to date. Fairport Financials is protected from server outages because PAETEC's Hosted E-mail Security stops all e-mail viruses before they enter the network.

Application Three

Holley Health Corporation (HHC) recently implemented PAETEC's Hosted E-mail Security to enforce their e-mail Acceptable Use Policy. The policy forbids employees from using company e-mail to send or receive messages containing questionable content or images. PAETEC enforces this policy using patented Image Composition Analysis to identify objectionable images within e-mails, detecting such content as suspect poses, facial tones, clothing, and overall image content. Questionable e-mails are rerouted, tracked, and reported on, based on company policy. Additionally, the Content Control module allows HHC administrators to set criteria by which they can control malicious or inappropriate textual content sent or received by their employees. HHC is protected from objectionable images and questionable content entering or exiting the organization's e-mail server, upholding their business integrity and avoiding potentially embarrassing situations.