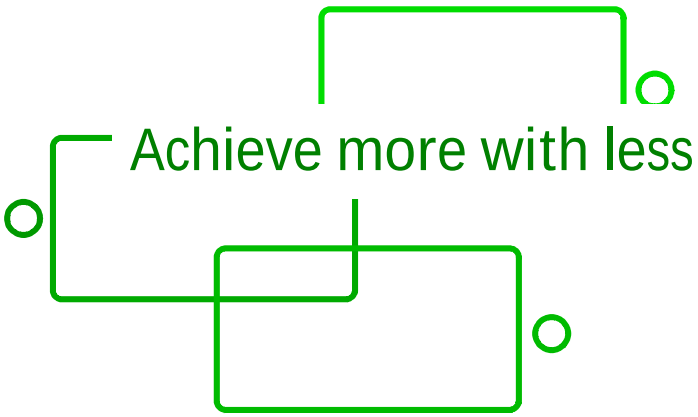
Visendo
Simplifying Messaging

Email Security: a huge challenge for companies

- a practical guide on email threats -

Whitepaper



- ✓ Internet and email security flaws
- ✓ Layered approach while defending
- ✓ Defense technologies
- ✓ SMBs special case
- ✓ About Visendo Mail Server Checker

ppedv AG - HQ – Burghausen, Germany

Tel: +49-8677-9889-110 Fax: +49-8677-9889-44

Info: support@ppedv.de sales: sales@ppedv.de http://www.visendo.com

Introduction

Every business, whether small, medium or corporation has huge threats, every day, coming from the internet: as malware, spyware, Trojans, worms, viruses. For small companies with an average email sending and receiving flow, these threats can be catastrophic (e.g. losing data about an important customer can bring SMBs to bankruptcy). In case of corporations, these threats are a little more complex and require more efficient solutions.

This whitepaper is a practical guide that helps business leaders chooses the right security solution against electronic threats.

The internet and its main threats

Threats

Corporate Threats

These relate principally to loss of IP and confidential information. Think a moment about these possible situations:

- Employees - knowingly or not – emails confidential information to one of your competitors: e.g. date of a new product release, features of a new product
- Your communications department mistakenly announces ahead of time important financial results

In any of these two cases, you can imagine the consequences if the media or your competitors learn of these leaks.

Legal Threats

Two broad categories of threat exist here:

- Offensive messages - mainly sexual harassment and racial abuse – are often spread by email.
- Compliance - companies are now more accountable for how information is stored, used and distributed - so it is imperative that data is managed and controlled correctly.

In the US, the legislation around the privacy of health and medical information (HIPAA rules), the need for financial and accounting compliance to Sarbanes-Oxley and new SEC controls related to share dealing scandals have dramatically raised the cost to business of non-compliance. In Europe, the Data Protection Act, Basel II, FSA regulations and EU94/96 are acting in the same way.

Digital threats

Every organization's IT infrastructure is in danger from malicious code and other harmful inbound content. The principal threats are:

- Spam is unsolicited commercial mass email, often advertising fraudulent schemes or products of dubious quality.
- Worms are a special type of virus that can propel themselves around the internet, without the need to infect a host program or document to act as a carrier.
- Trojans. The term is often used in a broader sense to include any non-viral program that is used to allow backdoor entry into or remote control over a computer system.
- Spyware is any software program that allows remote monitoring of actions and data on a system, without the user's consent or knowledge.
- Proxies are programs that perform action (e.g. relaying mail or caching of web pages) on behalf of a remote user.
- Phishing attacks use 'spoofed' emails and fraudulent websites designed to fool recipients into divulging personal financial data: credit card numbers, account usernames and passwords, social security numbers, etc.
- Denial of service attacks are where the corporate email server or web site are overwhelmed by email volumes forcing them to be shut down temporarily.

What is a layered approach and how a layered approach overcomes all the above described threats

The electronic threats are becoming more and more difficult to to fight against:

- The number of SPAM emails is growing everyday due to the larger number of general sent emails
- Standalone security solutions don't work together making it impossible companies to fight against hybrid threats: e.g viruses correlated with spam.
- New regulations that make weak control both illegal and inefficient.
- Irresponsible service vendors who claim more than what they offer

A layered approach consists of a single, simple comprehensive solution that fills every content security threats: virus, spam, pishing, DoS, spyware and content filtering.

The optimal solution that fights against these threats should fulfill the following conditions

- It should be easy to use - with simple deployment, management and reporting
- It should all the gateway - instead of a patchwork defense
- It should filter both email and web traffic
- It should cover all messaging directions - inbound, outbound and internal
- It should deliver enterprise-class performance - for the highest volumes and most complex traffic.

Fighting against

How threats are addressed

- Anti-virus solutions are one of the key tools in the defense against viruses. However, simply relying on an anti-virus tool alone does not provide organizations with complete protection against complex and hidden content threats.
Virus attacks via email are at a growing rate, but anti-virus solutions are not better than their last update.

- Spam causes a huge drain on system resources, employee productivity and business costs. In addition, spammers are now using viruses to spread emails vice-versa. Spammers are now using Trojans with embedded email engines to relay spam emails through infected computers.
Companies, especially SMBs, need to be able to pass on some of the burden of reviewing potential spam to end-users, which is also a key part of educating companies on how to deal with spam.

Any successful spam solution should offer the following features:
- Bayesian filtering - a statistical inference in which probabilities are interpreted not as frequencies but as degrees of belief.
- Heuristic search - basically analysis guided by rules.
- Auto-whitelisting - the appliance watches your traffic, determines who are the good guys and lets them send you mail.
- Real-time blacklisting - this depends on accessing lists in real-time form the industry bodies that identify dangerous websites
- Sender Policy Framework and Sender ID - Two industry initiatives that put the burden of authenticity on the sender (spammers hate that).
- Integration with Microsoft Office Tools: Exchange Server, Microsoft Outlook

Phishing is the act of sending an email to a user falsely claiming to be a legitimate enterprise in an attempt to scam the user into surrendering private information that can be used for identity theft. Anyone with an email address is at risk of being phished. Phishers send out
millions of these scam emails in the hopes that even a few recipients will act on them and provide their personal and financial information.

Spyware is a broad category of malicious software intended to intercept or take partial control of a computer's operation without the user's consent. Spyware differs from viruses and worms in that it does not usually self-replicate. Typical tactics include delivery of unsolicited pop-up advertisements; theft of personal information (including financial information such as credit card details); monitoring of web-browsing activity for marketing purposes;

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Usually it involves attempts to "flood" a network, preventing legitimate network traffic or an effort to disrupt connections between two machines, thereby preventing access to a service. DoS attacks can disable your computer or your network. Depending on the nature of your enterprise, this can effectively disable your organization

Content filtering stops the things that aren't spam or viruses but can be even more dangerous, like confidential customer data being mailed to a competitor or illegal, immoral or just plain unpleasant material coming in or out. Customers looking for best-in-breed content filtering should look for the following features:
- *Breadth* - to stop spam, viruses, trojans, confidential leaks, hatemail, inappropriate content and malicious code - all from a single management console.
- *Depth* - content engines should have the ability to 'explode' all email content to detect deeply embedded problems and content. Many simple filters may capture common malware data types, but they'll miss the not-so-common, particularly when they're hidden in zipped up attachments.
- *Power* - the performance to handle millions of emails with ease.
- Granularity - Content security is all about creating and enforcing policy and the best results come from the most granular policy management capability. That also requires policy templates and wizards to make it easy to design, deploy and update.
- Management of the application - Look for a solution that requires minimal management time and resource. You should be able to configure and manage all email gateways from a central console, for instance, as well as receive automatic updates and patches.

We will present further the situation of Small and Medium Business. These types of companies have special needs due to low security budgets. However, in their case, misplaced information or damaged information may result in serious problems – sometimes even bankruptcy.

Small and Medium Businesses' Challenges

Small and medium businesses are especially under big challenges in the current economic situation due to the lack of security in their communication, decreased operational efficiency and decreased customer relation retention.

These issues derive from multiple reasons:

- A very simplistic approach to collecting and reading emails from multiple accounts: many small companies use webmail clients for multiple email

accounts instead of receiving all the emails in a single inbox; this yields slower responsiveness to customers, business partners and employees.

- Impossibility to connect to SLA applications to keep track of existing and new customers
- Difficulty in setting up security barriers against cyber-criminals that can drastically affect the company's assets and confidential documents;
- Reduced interest and resources spent for email and document recovery systems in case disasters
- Difficulty in setting up email archiving and storing processes that comply to industry and regulatory retention requirements
- Reduced budgets for software solutions that could solve all these problems.

The current economic situation can be an outstanding chance for small and medium companies to cover the market gap between them and the big players due to the small player's flexibility. However, in order to sustain all the marketing, sales and production efforts, SMB's need efficient and secure electronic applications to cover and protect their assets.

The investment in such solutions is, however, a difficult process that involves testing, evaluating and budgeting. And for SMB's the ratio between quality and price is always the critical factor.

The most important factor should be the flexibility of the selected product, just like in the case of SMBs business models. Electronic messaging is mission critical, but remains vulnerable to a growing array of threats. Viruses, worms, denial-of-service attacks, spam, legal e-discovery and the need to satisfy a growing set of regulations all make effective message management increasingly difficult.

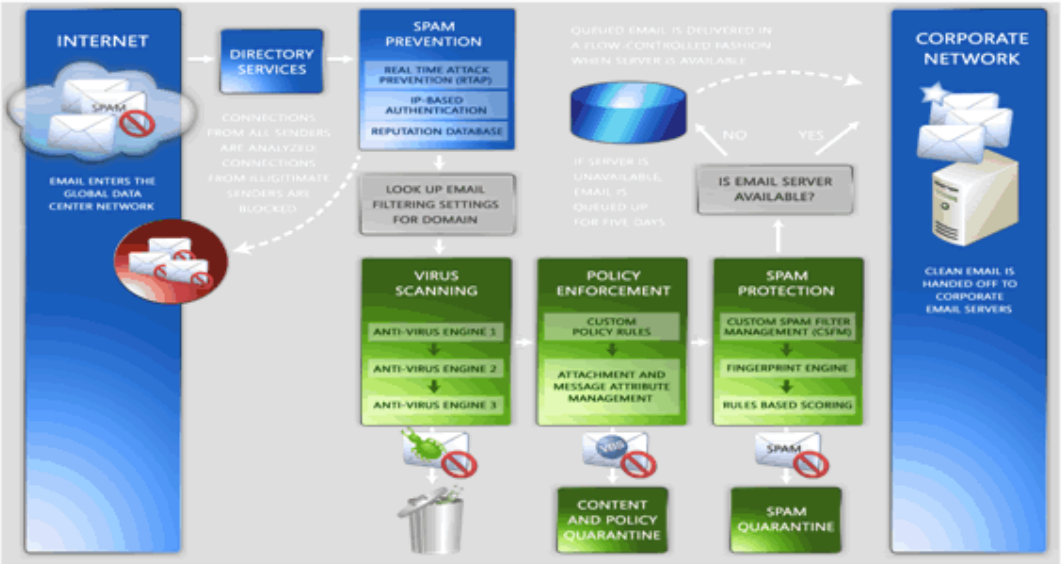
Visendo Email Solutions Overview

Visendo offers a bundle of email solutions to assist companies in meeting complex e-mail requirements, including services for e-mail filtering, distribution, archiving and continuity assurance that help businesses communicate with confidence. Visendo Mail Checker Server provide enterprise-class reliability for messaging security and management and can assist organizations by protecting itself from spam and malware, satisfying complex retention requirements for e-Discovery and compliance,

encrypting data to help preserve confidentiality and maintaining access to e-mail during and after emergency situations.

Visendo Mail Solutions simplify the administration of the messaging environments with services that are easy to deploy, manage, and maintain. The hosted online services model requires no hardware or software installation, minimizes the up-front investment and provides a predictable payment schedule through a subscription-based service.

As a comprehensive messaging and collaboration solution providing secure, standards-compliant features for small-to-medium-sized businesses Mail Checker Server uses a layer of protection features deployed across network of secure Internet connections. The services create a security-enhanced message stream to and from your on-premises, hosted or online messaging environment.



Visendo Mail Checker Server includes a powerful spam blocker, spam filter, grey list processing, and other new features; it uses a wide variety of local and network tests to identify and intelligently learn spam signatures.

It supports mailing lists, remote access and administration, spam-blocking, content filtering, mobile email, and multiple domain support; Visendo MCS uses all current email authentication techniques to minimize email fraud and security threats.

Just like an email gateway, it delivers full email server functionality, it can be installed in minutes, and requires minimal support and administration.

There are a few issues that any technical director from any company should bear in mind before deciding for an Email Solution:

1. define the company's electronic assets (contracts, offers) that need to remain confidential and should be securely stored
2. define the number of email accounts/user used in relation with customers, business partners or company colleagues
3. make a statistic with the regular security issues the company encountered in the last 6 months: spasm/ day, pishing attempts, viruses encountered in the email server etc
4. calculate the approximate space needed for email storage
5. define other issues like: out-of-the office situations
6. if there is any need to integrate the email system with existing applications used by the company: specific SLA's, document collaboration and sharing etc

After having answered all these issues, a decision can be made bearing in mind the importance of the price/quality ratio.

Based on the above described needs, the IT director should make a lis of the key capabilities for the optimum solution.

Visendo Email key features:

Enterprise Class Reliability

- Scales to meet the needs of virtually any enterprise
- SLA-supported uptime and performance
- Tried and tested backup e-mail system for rapid disaster recovery
- Secure, strategically located, as OutOfBox Solution

Active Protection

- Layered real-time anti-spam and anti-malware defenses
- Eliminate threads before they reach the corporate firewall

Simplified Management

- Simplifies IT environment by minimizing the need to deploy, configure, monitor, and update in-house e-mail security servers and applications
- Helps free network and server resources
- Eliminates up-front capital investment
- Offers a predictable, subscription-based payment
- Lower total cost of ownership when compared with on-premises solutions
- Allows you to respond quickly to e-Discovery requests
- Helps free up administrator time to focus

Conclusion:

Electronic messaging is mission critical, but remains vulnerable to a growing array of threats. Viruses, worms, denial-of-service attacks, spam, legal e-discovery and the need to satisfy a growing set of regulations all make effective message management increasingly difficult.
While choosing the right electronic solution for a SMB can be a complex and difficult process, any technical director has to bear in mind both technical issues and business needs of the company.

Visendo Email Suite offers multiple benefits for small and medium companies that consist in e-mail filtering, distribution, archiving, continuity assurance and server security while helping businesses communicate with confidence bearing in mind the optimal price/quality ration.

About Visendo

We are an Independent Software Vendor (ISV) specialized in internet systems integration on Microsoft technologies. We have always been one of the top 3 companies on the markets we entered. We were one of the first three Microsoft gold partners in e-commerce on the German market: this is the highest level for a Microsoft partner. Hence, you, as a potential customer, will benefit on our experience and quality of services that guarantees your investment.

For further information, please visit us on:website:
http://www.visendo.com, Product downloads

Blog: http://www.blog.visendo.com

Linkedin, Twitter , Facebook

Did you find this paper useful? Give us feedback NOW!

ppedv AG - HQ – Burghausen, Germany

Tel: +49-8677-9889-110 Fax: +49-8677-9889-44

Info: support@ppedv.de sales: sales@ppedv.de http://www.visendo.com