Email Protection: Assessing the costs

When considering the purchase of an email security solution (antivirus, antispam, antiphishing), it is easy to be overwhelmed by choices. The email security market is getting more and more crowded, and the offer is as varied as confusing, ranging from state-of-theart to frivolous. How can you make sense of the market's noise and hype? How can you measure the real value of the offered products and services?

Some vendors claim outrageous catch rates, and listed prices sometimes omit yearly subscriptions or hide required hardware or maintenance costs.

Initial estimates will compare solutions' claimed efficiency with their price. This quick comparison is often misleading: Some vendors claim outrageous catch rates, and listed prices sometimes omit yearly subscriptions or hide required hardware or maintenance costs. But even with accurate information, this estimation has its limit: pricing stands only for a fraction of the total email security cost.

Assessing the costs

Recognized industry analysts have evaluated the yearly Total Cost of Ownership of an email security solution within a range of $65 to $100 per mailbox (depending on the study). With product prices rarely exceeding $30 per mailbox, there is definitively something more to be looked at than just pricing.

When assessing the cost, consider the following:
1. Product costs
2. System administration costs
3. Productivity losses
4. Hidden costs

When assessing the cost of an email security solution, corporations should consider the following main cost areas:
1. Product Costs
2. System Administration Costs
3. Productivity Losses (another way to look at efficiency)
4. Hidden Costs

Let us review those in more details.

The product cost should include the cost of the solution (with the needed subscriptions and maintenance costs), the cost of required additional hardware and software if any, and the installation costs (including initial configuration). You can disregard server and installation costs for email scanning services.

While required, an easy to use administration console is not sufficient to reduce administration costs. Let us point out aspects that can badly influence the cost of the three major administration tasks:

- **Threat protection updates**: Most solutions include automated updates of their antivirus, antispam and antiphishing engines. This being said, several solutions still entail administrators or users to feed a self-learning system with messages announced as spam or non-spam. This may soon represent a non-negligible cost.
- **Quarantine Administration**: Several elements will influence these costs, like: i) does the system allow both system and user quarantines, ii) does the system send scheduled quarantine digests to end users, iii) does the system allow web quarantine access and how is this access granted (password management), and finally iv) does the system automatically clean aged quarantine items.

The product cost should include:
- the cost of the solution
- the cost of required additional hardware and software
- the installation costs

- **User Administration**: Most companies will want differentiated settings for their users, like user-defined trusted lists for instance. Creating these users and their aliases can become very time consuming if not automated through LDAP/AD integration or other alias-aware populating processes. To reduce further administration hurdles, companies should favour solutions that ease the definition of user settings through user delegation and by configuring exceptions only.

Productivity losses are mainly influenced by the spam let through rate (spam still getting to the inbox – also called false negative rate), the false positive rate and the impact of user delegation.

Productivity losses are mainly influenced by
- the spam let through rate
- the false positive rate
- the impact of user delegation

- **Let-through rate**: The market offers lots of tools to calculate the cost of spam. You can use the same tools to calculate the cost of left through spam. A 5% difference in catch rate may quickly represent a difference of several thousands of dollars in productivity loss.
- **False positives**: The cost of false-positives is highly dependent on the quality of the quarantine administration. In some cases the average cost can be as high as $50 per item.
- **User delegation**: Delegating settings to users is valuable overall. It is often a must. However it will influence users' productivity. Analyse the different methods provided to users to customize their environment and assess their easiness and efficiency. Distinguish between experienced and average users.

Beware that some implementations promote or require the installation of plug-ins on each client.

Finally, beware that some implementations promote or require the installation of plug-ins on each client. This has a serious cost impact (installation costs and more importantly productivity losses for all end users).

Hidden costs are mostly infrastructure related. Administrators experience them when their system performance is hindered by hacker attacks (dictionary harvesting, open relay or denial of service attacks), when their system is unavailable (due to maintenance or disaster), or when new threats appear and new features are needed. The better the product underlying architecture is structured the less it will suffer from those situations. While hidden costs are difficult to measure (but can often count for half of the total cost), here are some architectural bases that can reduce them:
- Exhaustive and efficient perimeter defence
- Database support (for easier data recovery)
- Clustering support (for higher performance and redundancy)
- Inbound/Outbound filtering (for mail compliance)
- Flexibility to catch new threats (like the latest "Image Spam").

Efficiency and effectiveness should be the key drivers in any cost assessment.

Conclusion

Several years with email security experience has guided Norman in considering all cost aspects – over the years – of email security. We know that pricing remains a key decision factor (our competitive pricing reflects that). For email security however, efficiency and effectiveness should be the key drivers in any cost assessment.

Vircom is one of Normans technology partners, and develops the Modus™ technology, which Norman Email Protection is based upon.