# Comparing Email Management Systems that Protect Against Spam, Viruses, Malware and Phishing Attacks

## An Osterman Research White Paper

*Published December 2006*

## Why You Should Read This White Paper

On several levels, email is the most important application used in business today: email is more important than the telephone for the vast majority of users, about 75% of the critical business content that users need on a daily basis is somehow bound up in their email system, and the typical user spends about 30% of his or her day doing something in their email client. In short, email is absolutely critical to the health and efficiency of just about any organization.

Because email is so critical, managing it properly and protecting it from the growing array of threats that impact it is becoming increasingly important. Systems designed to protect email systems and users from spam, viruses, malware, phishing attacks and other threats must be extremely effective, they must operate with virtually no downtime and they must be easy to manage.

To understand organizations' perceptions about various email management systems, Sunbelt Software engaged Osterman Research to survey organizations that are using five different email management systems. This white paper presents the results of those findings, comparing Sunbelt Software's Messaging Ninja with an average of the other four systems.

It is important to note two things about the research conducted for this white paper:

- As part of its proposal, Osterman Research gave Sunbelt Software the option to end the project after the research phase in the event that the survey results were not favorable. That did not happen.

- All of the products researched for this project had strong points and came out at or near the top in some categories that were researched. The products selected for this analysis are all very capable and in use by millions of customers worldwide. In other words, we did not select second-tier products for this analysis.

*Systems designed to protect email systems and users from spam, viruses, malware, phishing attacks and other threats must be extremely effective, they must operate with virtually no downtime and they must be easy to manage.*

## Methodology

In designing the survey methodology for this white paper, we wanted to obtain 'real world' results from users of various email management systems instead of relying on laboratory testing of these systems. Our thought was that by understanding how various email management systems are used in production environments, we could obtain a solid understanding of the relative pros and cons of each tool. Further, our methodology could obtain results, such as labor investments required to manage these systems, that would not be available via conventional laboratory testing.

A total of 93 Web-based surveys were conducted during September through November 2006 with North American organizations of various sizes. The respondents were drawn primarily from the Osterman Research Survey Panel, although Sunbelt Software also provided some contacts for this research, as well. The products on which we focused in the surveys were:

*We queried survey respondents about the presence of these systems in their organizations and then focused the vast majority of the questions on the system with which respondents were most familiar.*

- Barracuda Spam Firewall
- GFI MailEssentials
- McAfee GroupShield for Microsoft Exchange
- Sunbelt Software Messaging Ninja
- Symantec Brightmail

We queried survey respondents about the use of these tools in their organizations and then focused the vast majority of the questions on the system with which respondents were most familiar. In order to qualify to complete the survey, respondents had to be involved in the management of their organizations' messaging and/or networking systems, and they had to be using at least one of the products above.

Because we obtained results from small, mid-sized and large organizations, for part of this analysis we chose to narrow our review of the survey findings to organizations in the range of 100 to 6,000 email users. Our goal was to provide an 'apples-to-apples' comparison for things like the number of full-time equivalent (FTE) staff members required to manage various email management systems, eliminating both very small and very large organizations. For other data points that were not dependent on organization size, such as ratings for satisfaction with improvements in spam capture efficiency over time, we used the entire data set that we obtained.

Further, because this white paper was sponsored by Sunbelt Software, we chose to compare that company's Messaging Ninja offering – discussed later in this report – with the combined results of the other systems we surveyed instead of comparing Messaging Ninja to the other four products individually.

As an independent research organization that remains vendor agnostic, we wish to report that Messaging Ninja fared very well in our findings, but some of the other products in this analysis also fared quite well, leading some categories.

*Messaging Ninja averaged a very low 4.4% of respondents indicating that various email threat prevention activities were difficult or extremely difficult compared to 16.0% for the average of the other systems.*

## Research Findings

This section reports on the key findings discovered in the survey conducted for this white paper. The first section discusses a comparison of Messaging Ninja vs. the combined group of other products across all of the surveys conducted. The second section discusses the narrower data set of findings for organizations in the range of 100 to 6,000 email users.

### *Difficult in Managing Various Capabilities*

We asked organizations to rate the difficulty they experience in managing various aspects of their email infrastructure on a scale of 1 to 5, where 1 is 'no problem at all' and 5 is 'extremely difficult'. Specifically, we have included in the table below four key aspects of managing an email system focused on specific areas of protection – the results show the percentage of respondents who provided a rating of '4' or '5' for each activity.

**Ratings for Various
Email Protection Activities**

| Activity | % Responding '4' or '5' | |
|---|---|---|
| | **Messaging Ninja** | **Other Systems** |
| Managing anti-spam systems | 10.3% | 19.0% |
| Managing anti-virus systems | 3.4% | 15.9% |
| Managing attachment filtering systems | 4.0% | 15.5% |
| Managing anti-phishing systems | 0.0% | 13.7% |
| **AVERAGE** | **4.4%** | **16.0%** |

It is important to note that Messaging Ninja did not come out
on top in all of these categories – GFI MailEssentials came
out on top in two of them, for example.  However,
Messaging Ninja averaged a very low 4.4% of respondents
indicating that various email threat prevention activities
were difficult or extremely difficult compared to 16.0% for the
average of the other systems.

### Improvements in Spam Capture Efficiency Over Time

We also asked organizations to gauge whether or not their
anti-spam capabilities were a) getting better over time, b)
getting worse, or c) staying about the same.  The results of
our findings are shown in the table below.

**Improvement in Spam Capture
Efficiency Over Time**

| Efficiency Over Time Is: | Messaging Ninja | Other Systems |
| --- | --- | --- |
| Getting better | 55.2% | 39.7% |
| Getting worse | 24.1% | 22.2% |
| Staying about the same | 20.7% | 38.1% |

### Improvements in Anti-Spam False Positives Over Time

We also asked organizations to rate whether or not the false
positive performance of their anti-spam capabilities was
getting better or worse over time, or if it was staying
relatively constant.  Our findings are shown in the following
table.

**Improvements in False Positive
Performance Over Time**

| Performance Over Time Is: | Messaging Ninja | Other Systems |
| --- | --- | --- |
| Getting better | 37.9% | 47.6% |
| Getting worse | 6.9% | 9.5% |
| Staying about the same | 55.2% | 42.9% |

### System Ease of Use

Because email managers are faced with a growing array of
tasks in the context of messaging management, the ease of
use for an email management system is critical.  We asked
organizations to rate the ease of use for their systems on a
scale of 1 to 5, where 1 is ' not easy at all' and 5 is 'extremely
easy to use'.  Our findings are shown in the following table.

*Because
messaging
managers are
faced with a
growing array of
tasks in the
context of
messaging
management,
the ease of use
for an email
management
system is critical.*

**Ratings for System Ease of Use**

| System's Ease of Use Is: | Messaging Ninja | Other Systems |
|---|---|---|
| Not easy at all | 3.4% | 1.6% |
| Not too easy | 3.4% | 4.8% |
| Moderately easy | 6.9% | 28.6% |
| Easy to use | 44.8% | 49.2% |
| Extremely easy to use | 41.4% | 15.9% |

In this category, Messaging Ninja came out decidedly ahead of the other systems we surveyed, with more than twice the percentage of respondents indicating that the system was 'extremely easy to use'.

### System Reliability

Because email systems must operate as close to 24x7 as possible, email security and management systems must be extremely reliable and must operate with virtually no downtime. We asked organizations to rate the reliability of their systems on a scale of 1 to 5, where 1 is ' not reliable at all' and 5 is 'extremely reliable'. Our findings are shown in the following table.

*Because messaging systems must operate as close to 24x7 as possible, email security and management systems must be extremely reliable and must also operate with virtually no downtime.*

**Ratings for System Reliability**

| System's Ease of Use Is: | Messaging Ninja | Other Systems |
|---|---|---|
| 1 - Not reliable at all | 0.0% | 0.0% |
| 2 – Not too reliable | 3.4% | 4.9% |
| 3 – Moderately reliable | 20.7% | 23.0% |
| 4 – Reliable | 48.3% | 60.7% |
| 5 – Extremely reliable | 27.6% | 11.5% |

Here again, Messaging Ninja fared very well in our research, with more than twice the percentage of respondents indicating that the system is 'extremely reliable'. Barracuda Spam Firewall also fared well, with 23% indicating that the system is 'extremely reliable'.

### Data From Organizations of 100 to 6,000 Email Users

This next section examines a subset of the data analyzed above and, as mentioned in the Methodology section, includes only organizations of between 100 and 6,000 email users.

### *Time Spent Deploying Security Capabilities*

We asked organizations about the number of person-hours that went into both the deployment of their email management systems, as well as the amount of time spent during a typical week in managing these systems.  In order to normalize these findings, we calculated the number of person-hours per 1,000 email users.  Our survey findings for the amount of time spent deploying various systems is shown in the following table.

**Person-Hours Spent Deploying Messaging
Management Systems per 1,000 Email Users**

| Activity | Messaging Ninja | Other Systems |
|---|---|---|
| Managing anti-spam systems | 3.0 | 10.0 |
| Managing anti-virus systems | 4.0 | 16.0 |
| Managing attachment filtering systems | 2.0 | 3.0 |
| Managing anti-phishing systems | 0.0 | 0.5 |
| **AVERAGE** | **2.3** | **7.4** |

*Another important aspect of any messaging management system, and one that becomes extremely important for smaller organizations, is the amount of time required to manage it.*

Another important aspect of any email management system, and one that becomes extremely important for smaller organizations, is the amount of time required to manage it.  Our findings for the number of person-hours per 1,000 email users is shown in the following table.

**Person-Hours Spent Managing Messaging Management
Activities per 1,000 Email Users During a Typical Week**

| Activity | Messaging Ninja | Other Systems |
|---|---|---|
| Managing anti-spam systems | 2.0 | 3.0 |
| Managing anti-virus systems | 1.5 | 4.0 |
| Managing attachment filtering systems | 1.0 | 2.0 |
| Managing anti-phishing systems | 0.0 | 0.0 |
| **AVERAGE** | **1.1** | **2.3** |

This finding is significant:  Messaging Ninja requires one-half of the IT time investment during a typical week to manage it compared to an average of the other systems.  Our research found wide variability in the amount of time required for managing these systems.

If we extend the data in the table above to annual time investments and use a fully burdened annual salary for an IT

---

administrator of $80,000 per year, then we find that
Messaging Ninja, for the activities shown above, will have a
labor cost of $2.25 per user per year versus $4.50 per user per
year for the average of the other systems.  Keep in mind that
these costs are only for the labor required to manage email
security activities.

## Sunbelt Software's Messaging Ninja

Sunbelt Messaging Ninja, released in May 2006, is a third
generation, policy-based messaging security framework that
provides system administrators with an easy to use weapon
to enforce email security polces.  Ninja protects
networks against spam, phishing, viruses and other
messaging security threats, and provides unparalleled
flexibility and reliability at the same time.

Ninja gives administrators several security layers for message
inspection, cleaning and management.  By using multiple
scanning engines for both spam and viruses and by
integrating other messaging security rules, all treatment of
messages occurs at the server, not at end-users'
workstations.  Because no client software needed,
administration time is minimized.  Further, because the
modules within Messaging Ninja are designed to work
together, the system provides a powerful combination of
'best-of-breed' and 'all-in-one'.

Unlike legacy security products that filter at the gateway,
Ninja's Suspicious Mail Attachment Removal Technology™
(SMART) is the first policy-based attachment filter that filters
all attachments based on email direction – inbound,
outbound or internally within the organization.  Additionally,
Ninja actually looks inside many types of files to determine
their true identity instead of relying solely on file extensions.
This means that simply renaming a ".exe" file to a ".txt"
extension will not fool the Ninja attachment filter, providing
an important zero-day attack protection capability.

Ninja is policy-based so that administrators can create
different settings for users and groups of users for 100%
detection and removal of possible malicious attachments.
At the same time, Ninja allows policy-level exceptions for
outbound and internal traffic.  The anti-virus and anti-
phishing plug-ins together are highly effective with extremely
low overhead.

*Sunbelt
Messaging Ninja,
released in May
2006, is a third
generation,
policy-based
messaging
security
framework that
provides system
administrators
with an easy to
use weapon to
enforce email
security polces.*

Ninja's plug-in architecture was designed with flexibility and extensibility in mind.  It provides a robust messaging framework that enables administrators to manage all aspects of messaging security, and allows them to create customizable policies utilizing Ninja's integrated plug-in management.

## Summary

Sunbelt Software's Messaging Ninja provides a number of very useful capabilities in an integrated architecture designed to make email security simple and effective.  Our research has demonstrated that Messaging Ninja is rated very highly by users relative to other email management products with which it competes and can be managed at a lower cost per user than other email management systems.

*Sunbelt Software's Messaging Ninja provides a number of very useful capabilities in an integrated architecture designed to make messaging security simple and effective.*