

# You've got spam! Now what?

[www.novell.com](http://www.novell.com)

---

EXECUTIVE GUIDE

# N

**Novell.**



[www.novell.com](http://www.novell.com)

[www.gwava.com](http://www.gwava.com)

# Table of Contents

You've got spam!  
Now what?

---

2 — INTRODUCTION

2 — EXECUTIVE SUMMARY

2 — E-MAIL IS UNDER ATTACK

3 — WHAT IS SPAM?

4 — HOW MUCH DOES SPAM COST  
A COMPANY?

5 — WHAT CAN YOU DO ABOUT SPAM?

6 — DESKTOP PROTECTION

6 — SPAMMER LISTS

6 — ANTI-SPAM SERVICE PROVIDERS

7 — ANTI-SPAM GATEWAYS

8 — INTEGRATED SOLUTIONS

9 — ALL-IN-ONE PRODUCTS

9 — CONCLUSION

# Every Company Needs an Anti-spam Strategy

# N

Spam is a perplexing topic. Most people find it annoying, but few agree on anything past that starting point. What is spam? How much does spam cost a company? And, most importantly, what can we do about it? Each of these questions leads to heated discussions, as each speaker is sure they have the one true answer.

In this paper, we'll take a look at what Spam is, the direct and indirect costs of spam, and what can be done about spam.

## EXECUTIVE SUMMARY

### 1. Spam is a problem that cannot be ignored.

It has to be dealt with, or it will continue to consume valuable corporate resources.

### 2. Spam is a slow cancer on your system. Every

year, we see more spam, and every year it costs more to deal with it. As with a slow growing cancer, it's easy, but foolish, to try to ignore it

### 3. There is no simple cure for spam. Because it

is so cheap to send spam, as long as spammers get one reply to thousands of sent spams, they will continue to spam. Given the international nature of the Internet, local, state, and national laws will have no effect on spam. Effectively dealing with spam means you need centralized and ongoing efforts to manage and prevent spam.

### 4. Internal spam has the potential to be the most costly and damaging your company faces. Companies have faced—and lost—

very expensive lawsuits when their employees have sent offensive e-mail to co-workers.

Corporate policies that prohibit these e-mails have not been an effective legal defense.

Even winning a lawsuit can be expensive in today's litigious society. It's better to avoid the problem.

### 5. Spam is only part of the e-mail hygiene problem. When looking at spam issues,

remember there are related e-mail issues. An integrated solution can save money compared to implementing a range of products to address the e-mail hygiene issues.

**Every company should implement an effective anti-spam strategy. You can't afford not to.**

## E-MAIL IS UNDER ATTACK

While this paper addresses the issue of spam, spam is only one part of what the META Group refers to as e-mail hygiene.<sup>1</sup> As you consider anti-spam products, it is worth considering the META Group's

<sup>1</sup>"The Battle for Port 25, Web and Collaboration Strategies," by Matt Cain. 31 May 2002. Published by the META Group as file WCS 1136.

suggestion that spam containment should be part of a comprehensive e-mail hygiene program.

Dealing with various issues in e-mail hygiene with separate products and methods dramatically increases the costs of e-mail management compared to using a single product.

When you are looking for answers to e-mail issues, we suggest you make sure you are looking at the big picture, and select a manageable, cost-effective solution that will deal with all your e-mail hygiene issues.

#### WHAT IS SPAM?

We've heard as many definitions as there are people who talk about the topic. At Novell and Beginfinite, we classify spam into three groups:

1. Hard-core Spam (schemes, hair restoration, pornography...)
2. Friendly Spam (benevolent messages from legitimate companies)
3. Co-worker Spam (jokes, Chain letters, and other counter-productive material)

#### Hard-core Spam

The **first category**, which consists largely of **unsolicited shady offers**, is what enrages most people. E-mail from people you've never heard of. E-mail without a single word in any language you—or Babelfish—can recognize. Ads for get rich schemes, drugs of various sorts, debt consolidation, dating services that promise you needn't be lonely tonight, and more and worse.

Even in this category, what one company considers spam can be critical e-mail to another. Most companies don't want their employees

to receive e-mails about Viagra. However, e-mails on that topic could be very important to a pharmaceutical company. It is very important that you are able to tailor your anti-spam solution to your needs.

#### Friendly Spam

The **second class of spam** is what we call "**friendly spam**." The mailing lists you and your staff have signed up for are a good example. Some are work related, such as technical support forums, discussion lists for personnel managers, and so on. Others are commercial but useful—who wouldn't want to know when your vendor is having a great sale on toner or ink for the ever-hungry printers? All of these take time to read, but are generally welcome, and come from organizations that will let you off the list when you request it.

Friendly spam can become a problem when employees leave their company. Their old e-mail address may get deleted, but their subscriptions to newsletters, bulletins and other types of friendly spam keep arriving and clogging the postmaster account with mountains of undeliverable mail.

#### Co-worker Spam

The **third class of spam** is the **seemingly benign junk e-mail people send each other**. Things like chain letters, announcements of cake sales or other fundraisers for charities, gambling (office pools), jokes, and sometimes, pornography. All of these can impact the productivity of your office, and in some cases may leave you open to legal actions brought by offended employees.

<sup>2</sup>Legal issues in e-mail harassment, from "DominoPower," <http://www.dominopower.com/issues/issue199812/legal1001.html>

<sup>3</sup>No Spam Shortage Here—Web & Collaboration Strategies," by Matt Cain. 1 May 2002. Published by the META Group as file WCS 1122.

<sup>4</sup>Washington Post, "Making Spam Go Splat—Sick of Unsolicited E-mail, Businesses are Fighting Back," Caroline E. Mayer and Ariana Eunjung Cha, Washington Post Staff Writers, June 9, 2002; Page H1.

Table 1—Annual corporate spam Costs, in US Dollars (assuming 20 spams per day the first year, 100% per year growth in spam, 15 seconds to recognize and delete each spam, and a staff cost of \$24.00 per hour)

Courts in many countries, including the US and EU, have ruled that because e-mail is a corporate asset, a company is responsible for it. A joke listing "25 ways beer is better than women" cost Chevron 2.2 million dollars. A racial joke that offended some employees caused Morgan Stanley Dean Witter & Co. to face a 60 million-dollar lawsuit. Even winning these cases can be expensive—the fees for the discovery process and the costs of the lawsuit itself can rapidly approach \$1,000,000. Even if you avoid a lawsuit, the cost of finding and training a replacement for an offended employee who leaves your company can easily reach \$100,000.<sup>2</sup>

Having an e-mail policy is not enough—it has to be enforced, before the spam hits the fan. An anti-spam product that can examine internal mail can control this problem without depending on employees to show self-restraint.

Every industry study suggests that the volume of spam is growing, even though they can't agree

on how quickly. The META Group estimates that medium sized businesses are presently routinely receiving as many as 20,000 daily spam messages.<sup>3</sup> According to the Washington Post, estimates of the annual growth range from 100 to 600%.<sup>4</sup>

#### HOW MUCH DOES SPAM COST A COMPANY?

The potential costs of litigation are a fairly obvious, if uncertain, cost of internal spam. However, spam is expensive even if you aren't sued. We often hear people say, "What's the big deal? I just hit delete and get on with my day!" And a few years ago that was a very reasonable approach.

However, with the astronomical growth of spam, that has become an increasingly expensive option. In the chart below, we examine the labor cost of "just deleting spam" for companies ranging from the classic "one man shop" to a company with 1,000 employees using e-mail.

NUMBER OF EMPLOYEES	1	10	100	1,000
Cost of spam in first year	\$ 730	\$7,300	\$73,000	\$ 730,000
Cost of spam in second year	1,460	14,600	146,000	1,460,000
Cost of spam in third year	2,290	29,200	292,000	2,920,000

Of course, that is just part of the picture. Companies that are required to archive all e-mail received by their employees will have to deal with a growing storage requirement. While storage keeps getting cheaper, preventing spam is more cost effective than archiving it.

Further, spam can be demoralizing. Seeing messages that offend one's sensibilities and moral standards casts a pall on the workday. Whether it's an accountant fuming over an illegal get-rich scheme, a religious person offended by an ad for a porno site, or a non-religious person offended by an ad for a church group—time is wasted while they regain their composure. Getting rid of spam has a very positive impact on staff morale.

Spam is a slow growing virus, gobbling up your employees' productive hours as well as your network bandwidth and your storage space. The sooner it is stopped, the better.

#### WHAT CAN YOU DO ABOUT SPAM?

There are as many answers to that question as there are people who answer it. **Many** of the "cures" we hear about are **not** geared for a **corporate environment**, but because they are suggested all too often for corporate use, we feel we should discuss them. The first we always hear about is, "**Just hit the delete key.**" This is like holding back the tide with a spoon and is **not recommended**.

There are preventative measures individuals can take. **Never, ever ask a spammer to remove you from their list.** At the bottom of most spam messages, you'll find a "friendly" message telling you that if you want to be removed from spammer's mailing list, just click on a link or reply to the e-mail and place the word *remove* in subject. By requesting to be removed, you are unwittingly notifying the spammer that your e-mail address is active. This usually results in a lot more spam being sent to you.

Spammers harvest addresses from Web sites you visit and from news groups you contribute to. If you make sure your correct e-mail address isn't in your browser and newsreader, spammers can't harvest your address.

This is more complicated for news group users because they want the members of a news group to be able to contact them, while remaining

spam-free. Because of the amount of data in newsgroups, spammers use programs to harvest the addresses. By adding words like "nospam" to the e-mail addresses in their news reader setup, people confuse the harvester programs while letting people figure out the real address.

We feel the life expectancy of tricks like these is limited, as address harvesting software will become more sophisticated. Still, identity hiding **can delay spam problems** if you take these steps as soon as you get an e-mail address. Once your e-mail address is harvested, the cat is out of the bag. Spammers trade and save lists of addresses, so the amount of spam you receive will increase over time even if you start hiding your identity after it has been harvested. A staff member received spam with eight of his former e-mail addresses on it. One was nine years old and hadn't been used for eight years. We feel identity hiding has **limited effectiveness** in a corporate environment.

On a more active level, your staff can use the **spam control functions** built in to their **e-mail client** software to filter out spam. However, this means that instead of doing the work you are paying them to do, they are spending their time playing with anti-spam rules. And without centralized management, your employees will be duplicating each other's efforts (if they take advantage of these tools at all). While more effective than the "just hit delete" approach, it is still a waste of staff time and we **can't recommend** it for offices with more than a few people.

Some people use **disposable e-mail accounts**, accounts they use until too much spam is being received, at which point they switch to a new e-mail account. While this works, the price is quite high—loss of business continuity. The business costs of changing an e-mail address are much the same as moving your business or changing your phone number. You have to let customers know you've moved, you have to change your business cards and stationary, and there is a real chance that you won't notify someone important of the change and lose their business altogether. We see this as a poor way for individuals to manage spam, and altogether **counterproductive for a business.**

#### DESKTOP PROTECTION

There are **stand-alone personal anti-spam products** that can stop spam before it's downloaded to your staff's PCs. However, these are products designed for single end users without centralized management. They are worth using in home or home office environments, but the cost per user and the cost of deployment and maintenance make this **hard to recommend to a business environment.**

With the end-user products out of the way, let's discuss **products aimed at the corporate environment.**

#### SPAMMER LISTS

Many e-mail servers, anti-spam products, anti-spam services, and e-mail content managers let you use **Real-time Black hole List (RBL)** services. These services track the IP addresses and addresses of spammers and open relays.

Some also track dial up access lines, which shouldn't have e-mail servers on them. Any e-mail that comes from these sources is dropped, as if into a black hole. However, spammers are well aware of RBL and as a result, change accounts and servers very often, so the RBL lists are always outdated and the amount of dropped spam is very low. It's too easy for a spammer to change/spoof domains, which makes RBLs lists bloated with out-of-date information. We agree with the META Group's finding that content filtering is much more effective.<sup>5</sup> For instance, a rule blocking "Viagra" can prevent spam from several sources with one rule. In fact, 20 or 30 smart content filters can probably reduce spam by at least 60%.

The tests we've seen that are most favorable to RBL's show they drop about 12% of the incoming spam, while also dropping as much as 5% of the legitimate e-mail.<sup>6</sup> We **recommend against** the use of **RBLs** because of their low effectiveness and the danger of losing important e-mail.

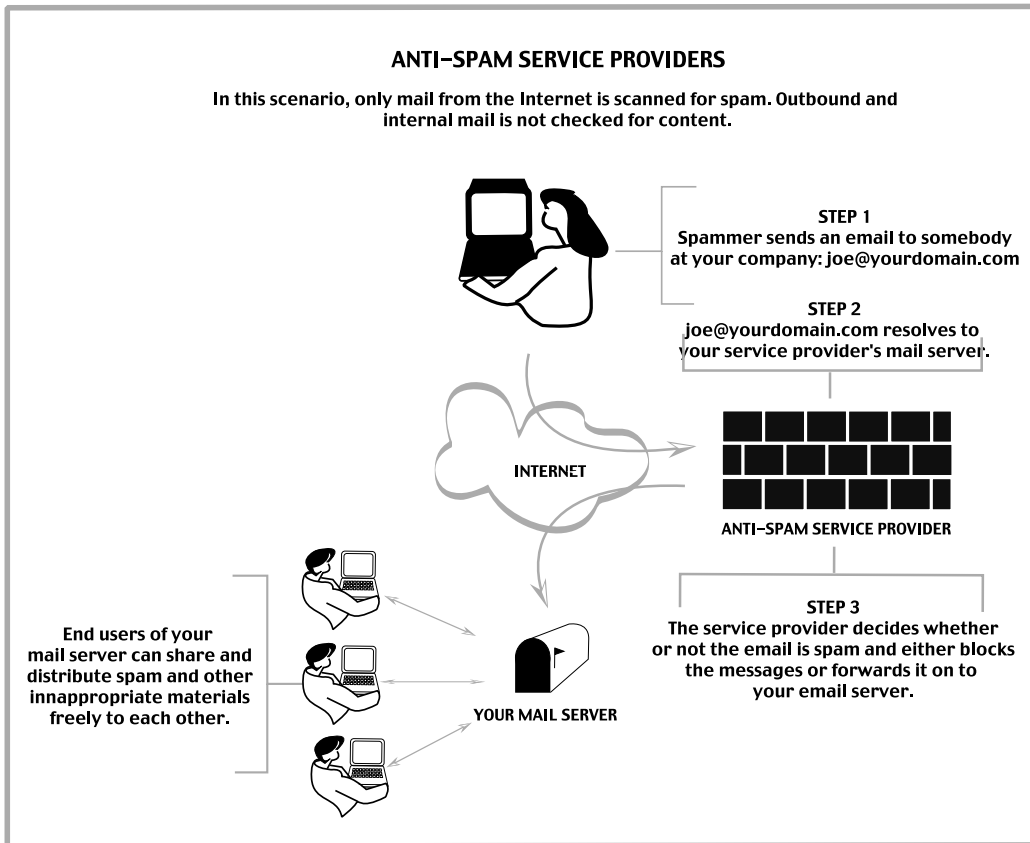
#### ANTI-SPAM SERVICE PROVIDERS

A number of companies offer **anti-spam services.** These services are attractive for less sophisticated shops, or shops whose MIS staff is already over extended. While it allows specialists to handle your spam, it also means that all your e-mail will have to pass through the vendor's servers. Insuring that your e-mail will reach you correctly in the event your vendor has technical problems or goes out of business will require careful setup of your DNS records, and could require action if the DNS setup is incorrect. It is important to properly

<sup>5</sup>"No Spam Shortage Here—  
Web & Collaboration Strategies,"  
by Matt Cain. 1 May 2002.  
Published by the META Group  
as file WCS 1122.

<sup>6</sup>"RBL Report," by Jason  
Gunthorpe in the Debian  
Developer's mailing list  
([debian-devel@lists.debian.org](mailto:debian-devel@lists.debian.org)).  
Archived at <http://lists.debian.org/debian-devel-200003/msg01325.html>

"Brightmail, Inc. Anti-Spam  
Service: Comparative  
Performance Test," by eTesting  
Labs under contract to  
BrightMail. Available at  
<http://www.etestinglabs.com/main/reports/bmspam2.pdf>



research your potential anti-spam service provider. After all, they will be processing all of your inbound and outbound Internet mail. This raises security and Quality of Service concerns. Every organization will have its own definition of what is or is not spam. Many service providers may use the same criteria to identify spam on behalf of all of their customers. As mentioned earlier, messages that discuss Viagra may be unwelcome in most industries, but not in the pharmaceutical or health care industries.

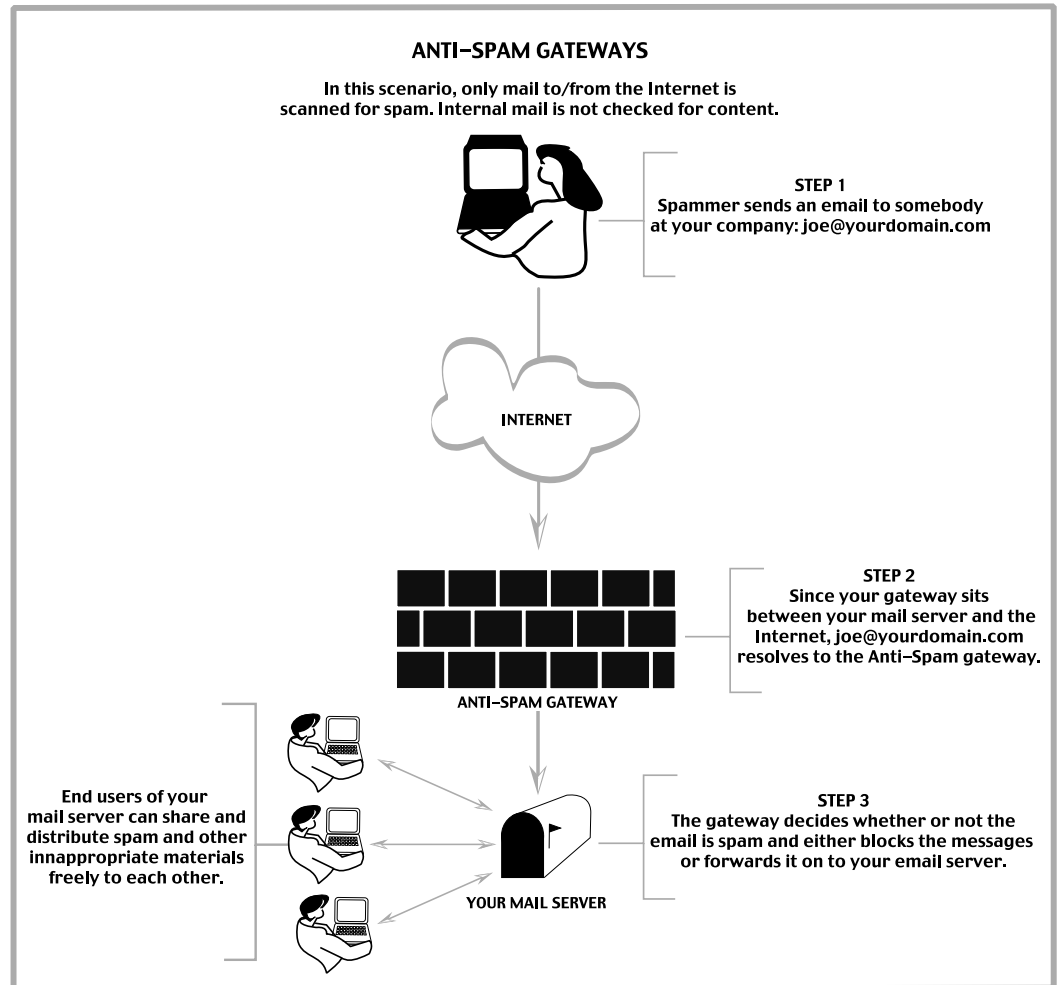
Of course, if your vendor fails, you will again get the spam they were blocking for you. The final weakness of this approach is that it will not protect you against internal spam, potentially the most

expensive spam. In the end, we see this as being best used as interim solution, but we **don't recommend** it as a long-term solution.

### ANTI-SPAM GATEWAYS

There are **stand-alone e-mail content management systems** that can handle spam effectively. Most of these are run on a server separate from your e-mail server, so you will need to purchase, install, and maintain another server. These products offer centralized control over external spam, which is a big step in the right direction, but because they cannot scan the e-mail inside your company they can not protect against internal, co-worker spam, which is the potentially most damaging form of spam.





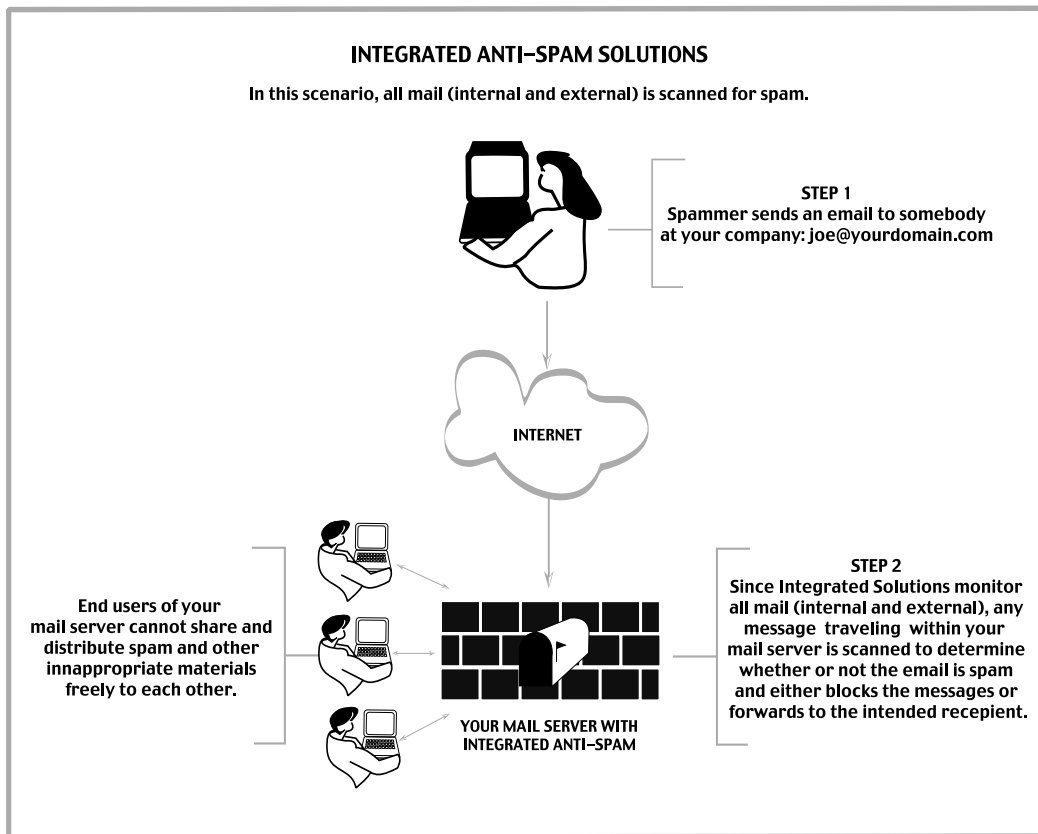
Because of their lack of integration, their inability to protect from internal spam, and the cost of adding another server, these products cannot provide a complete anti-spam solution and we can't recommend them.

#### INTEGRATED SOLUTIONS

Some content management products go a step further by being designed to work with a particular mail system, like Microsoft® Exchange, Lotus Notes® or Novell® GroupWise®. This usually allows them to run on the same server that is providing your

e-mail services and often they can protect your internal e-mail from co-worker spam. If you are considering purchasing this sort of product, make sure it can stop internal spam as well as external spam before making your final decision. We feel that only an integrated solution that is capable of stopping both internal and external spam can be recommended for comprehensive spam prevention.

Integrated solutions normally offer centralized management capabilities, the ability to stop internal and external spam, and can archive e-mail for legal and auditing purposes. We believe



that fully integrated solutions offer the most comprehensive anti-spam and content control coverage for your enterprise.

### ALL-IN-ONE PRODUCTS

Finally, there are a few all-in-one e-mail servers and content management systems on the market. These are attractive if you don't already have an e-mail system in place, but converting to one could be prohibitively expensive.

### CONCLUSION

By this time two things should be clear—regardless of your e-mail environment, you can't afford to not install a good anti-spam product. The cost of spam, even without lawsuits from offended employees,

is just too high to be borne. Even with as few as 10 employees, an effective anti-spam product will pay for itself in the first year.

Further savings can be obtained by using an integrated e-mail management tool that will handle all your spam, anti-virus, and e-mail archiving needs instead of using different products for each phase of the e-mail management which would increase procurement and management costs.

### About Beginfinite

Beginfinite Inc. is a leading developer of server-based eSecurity solutions designed to protect and accelerate electronic collaboration in the connected economy. Beginfinite delivers

sophisticated electronic defenses that are easy to install, intuitive to use and extremely robust. Beginfinite has a global presence with a worldwide network of resellers, and has forged an array of technology partnerships with companies including Novell, Inc. For more information on Beginfinite or its GWAVA™ family of solutions, call 866-GO-GWAVA, or visit Beginfinite's Web site at <http://www.gwava.com>.

#### About Novell

Novell, Inc. (Nasdaq: NOVL) is the leading provider of Net business solutions designed to secure and power the networked world. Novell and

its eServices company, Cambridge Technology Partners, help organizations solve complex business challenges, simplify their systems and processes, leverage emerging Web services, and capture new opportunities with one Net solutions. Novell provides worldwide channel, developer, consulting and education programs to support its offerings. For more information on Novell solutions and services, contact Novell's Customer Response Center at (888) 321-4CRC (4272) or visit <http://www.novell.com>. Press can find Novell announcements and company information at <http://www.novell.com/pressroom>.

© 2002 Novell, Inc. All rights reserved. Novell and GroupWise are registered trademarks, and Cambridge Technology Partners is a registered service mark of Novell, Inc. in the United States and other countries.

© 2002 Beginfinite, Inc. All rights reserved. GWAVA is a trademark of Beginfinite, Inc. in the United States, Canada and other countries.

\*Microsoft is a registered trademark of Microsoft Corporation. Lotus Notes is a registered trademark of Lotus Development Corporation. All other third-party trademarks are the property of their respective owners.

#### Novell Product Training and Support Services

For more information about Novell's worldwide product training, certification programs, consulting and technical support services, please visit: [www.novell.com/services](http://www.novell.com/services)

#### For More Information

Contact your local Novell Solutions Provider, or visit the Novell Web site at: [www.novell.com](http://www.novell.com)

Contact Beginfinite at:  
866 GO GWAVA  
1 514 639 4850  
[www.gwava.com](http://www.gwava.com)

You can purchase Novell Solutions online at: [www.novell.com/shopnovell](http://www.novell.com/shopnovell)

You may also call Novell at:

1 888 321 4272 US/Canada  
1 801 861 4272 Worldwide  
1 801 861 8473 Facsimile

**Novell, Inc.**  
1800 South Novell Place  
Provo, Utah 84606 USA

[www.novell.com](http://www.novell.com)  
[www.gwava.com](http://www.gwava.com)



**Novell**