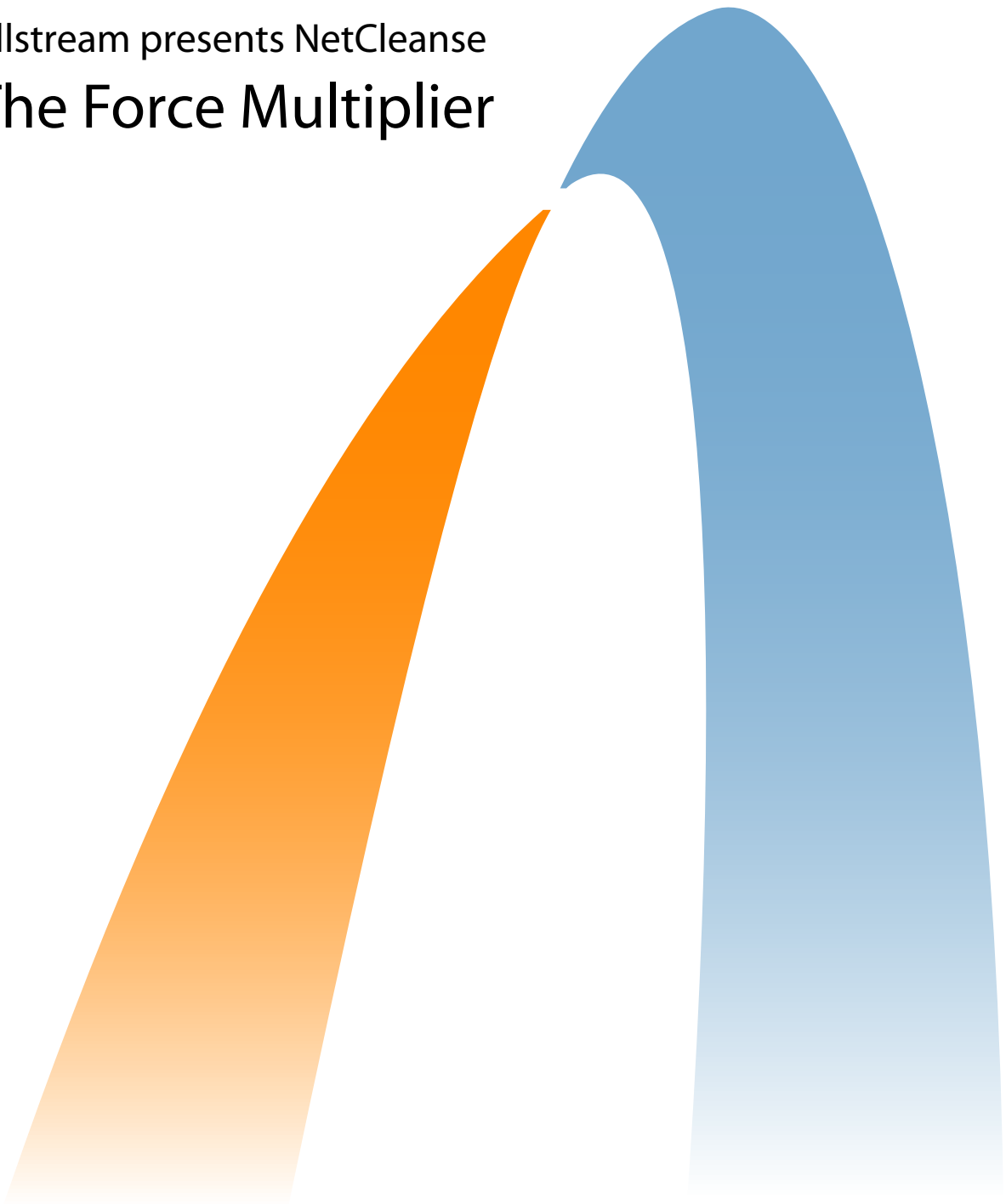


Allstream presents NetCleanse
The Force Multiplier



The Force Multiplier

Summary

There are unnumbered techniques for defending computers and networks from viruses and spam. Merely adding them together creates a cocktail of systems which are not nearly as effective as systems that are engineered deliberately to use the best of the techniques available.

Allstream will demonstrate that NetCleanse manages to combine all of the pros of gateway and managed service defenses with none of the negatives.

Addition versus Multiplication

This white paper discusses the benefits and negatives with two types of anti-spam and anti-virus products: gateway defenses and managed services.

While successful and mature technologies, both these methods have notable drawbacks which is why they are often used in combination. We will prove that adding perimeter defense on top of a managed system is not as effective as combining such that they evolve into a new breed of product.

It is Allstream's belief that merely adding the qualities of gateway and managed services is not as effective as combining them. Joining them at "the genetic level" effectively acts as a force multiplier which allows for new services that merely adding the two types together does not permit.

This structural difference multiplies the benefits of traditional gateway and managed services and NetCleanse.

- In part one, we will discuss the benefits and drawbacks of traditional gateway defenses.
- In part two, will discuss the benefits and drawbacks of traditional managed services
- Part three is where we demonstrate how NetCleanse combines the best of the two systems above, with none of the drawbacks.



Part 1

Gateway Defense

Perimeter defenses defend private networks by filtering mail viruses at the gateway. Typically, these are software additions run at the point where e-mail enters your system.

Gateways are a proven technology and provide a solid defense against mail-based virus attacks provided they are properly configured. Your firm's information technology staff must maintain the virus definitions and adjust the Gateway filters and software to ensure proper functioning.

E-mail viruses spread amazingly quickly, replicating themselves rapidly as they harvest contact information in e-mail address books. Preventing viruses from entering corporate networks is vital: gateway or perimeter defenses can be updated much more speedily than the individual anti-virus definitions on company desktops.

This cuts maintenance costs. This is particularly important as companies grow.

Cons

Misconfiguring gateway protection, or not updating them, can cause problems which are not visible until a virus outbreak has spread. It is fair to say that all IT employees have some knowledge in network security, but not all of them have expertise in this area.

Moreover, not all viruses are e-mail based exclusively.

As anyone who has suffered through recent years is aware, viruses are increasingly a blended threat which spread by a combination of methods. Gateway defenses often do not cover all points of entry such as web-based mail accounts which users may be checking from work.

The seriousness of that threat cannot be underestimated.

This brings us to section two, Managed Services.



Part 2

Managed Services

Traditional managed anti-spam and anti-virus services operate differently from software and hardware that arrives in a box to be installed at the customer's establishment.

E-Mail sent to and by the customer is routed first through the managed service for analysis and filtering of spam and viruses.

The benefits and side effects are notable.

Managed services eliminate the need to employ security experts in house. It also reduces the risk that IT staff who are less expert in security than in other areas of computer services, may misconfigure the security system or fail to update it correctly.

There is also a low cost of entry. Managed services can be up and running nearly immediately as they are subscription services without any need to implement expensive hardware.

Cons

Mail is routed through another private company. The managed service provider has complete access to any mail sent to and from your address.

Privacy is also a notable concern. Managed services to date work by creating a detour in your private network to theirs. For any firm, profession or body that must guarantee privacy in communications, traditional managed services are simply not a legally defensible option. This is a particular concern to legal, health and institutions which have obligations to safeguard personal records.

Part 3

Addition versus Multiplication

Adding a Gateway service to a Managed Service will still leave you with all of the negatives outlined above. NetCleanse, however, has all of the pros outlined above and none of the cons. This provides multiple benefits.

NetCleanse is a gateway protection and managed service that lives on your property. It is easy to configure and operate—like any gateway product—but no mail is re-routed to third parties. This means your private mail remains private—a necessity for professional security.

To configure a NetCleanse account, one need only enter your firm's IP information into our on-line service account for. A boot disc image is created which you install on a server on your property. The hardened LINUX operating system and NetCleanse are downloaded to the server in approximately 20 minutes.

The difference between having a traditional managed service and a gateway and NetCleanse is this:

- You have all the privacy benefits and control of gateway
- Low cost of ownership
- The expert supervision of a managed service
- HTTP and FTP scanning in addition to SMTP defense

What do we mean by a force multiplier?

We mean NetCleanse can take the offensive.

As reports start filtering in from around the world about virus outbreaks, our engineers add what ever descriptive information is available to our blocking list: be it name, extension or file size.

It may be some hours yet before a virus definition is forthcoming from the AV firms. The ability to generate stop gap measures on the fly lets NetCleanse take the initiative against virus outbreaks without having to wait for your employees to arrive in the morning to configure the defenses, or AV companies to develop "perfect" definitions.

DCS

NetCleanse can also take the offensive against spam.

The Digital Clearinghouse Service analyzes each numeric stamp associated with e-mail that is sent through the internet. (NetCleanse doesn't create this number, it is part of the internet mail protocol.)

All mail passing through NetCleanse's servers around the world has its serial number flagged. Logically, if an e-mail with the same identity number begins appearing around the world, it is likely to be spam. This means we can identify spam as spam *before* it is delivered to your network.

As an internet service provider, Allstream believes a proactive approach to security is best.



Part 4

Conclusion

No more security cocktails

Layering defenses is an additive approach. NetCleanse is a force multiplier as the defensive characteristics of both gateway and managed services work together to provide new types of benefits not existing previously.

- NetCleanse provides all the speed and power of gateway virus and spam defenses, with the supervision and expertise of managed services, all the while defending against blended threats of web and FTP infections.
- Moreover, your mail remains *your* mail.
- Our contact with the NetCleanse server on your property is limited to diagnostics and ten minute updates. Your mail is not routed through any hardware outside of your premises.

None of these benefits are provided by adding any competing gateway defense to competing managed services.

Technical Support

If you have a technical support question, please consult the NetCleanse Technical Support section of our website at <http://www.allstream.com>

Copyright Notice

The content of this manual is for informational use only, and may change without notice. NetCleanse Technologies Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

