SUNBELT MESSAGING NINJA™

Flexible Messaging Security.

Your Weapon: Sunbelt Messaging Ninja.

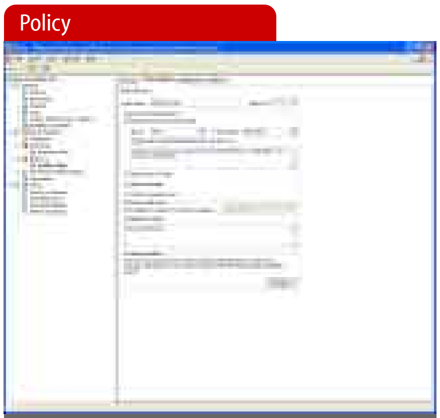
Sunbelt Messaging Ninja is an advanced and powerful, policy-based messaging security framework that provides you as a system administrator the weapon to enforce email security policies that protect your network against spam, phishing, viruses and other messaging security threats.

Ninja provides a layered security approach for message inspection, cleansing and management. By using multiple scanning engines for anti-spam and anti-virus, while integrating other messaging security rules, all treatment of messages occurs at the server, not at your end-users' workstations – no client software needed.

Policy-based plug-in management.

Ninja's plug-in architecture was designed with flexibility and extendibility in mind. That way you get a robust messaging framework that enables you to manage your entire messaging security. You can create customizable policies utilizing Ninja's integrated plug-in management.

Policy



Select simple configuration options for setting up an anti-virus policy

Ninja will initially include plug-ins for anti-spam, anti-virus, and attachment filtering. The framework is built to accommodate the integration of additional plug-ins in the future which will include disclaimers, content filtering, archiving, content auditing, and more.

With extensive policy creation capabilities, you can create custom policies for groups of users or a single user using Active Directory. You can set parameters based on user and/or organizational requirements. If you wish, you can simply associate all users with Ninja's default plug-in policies and have a powerful messaging protection solution in place in just a few minutes.

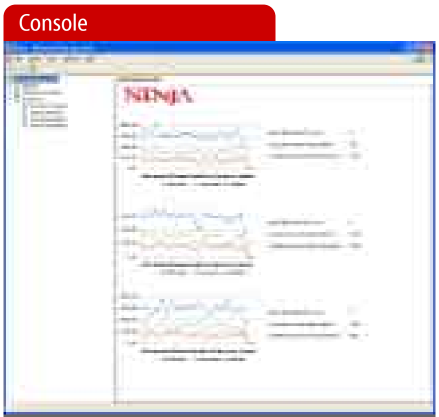
You can also create separate policy templates for different groups or individuals. And, you don't have to set up and maintain lists of blocked IP addresses and constantly create all sorts of custom rules. You have the flexibility to fine tune the aggressiveness of detection for all messaging plug-ins.

Fast deployment in Exchange 2000/2003 environments.

Ninja's management console enables you to install, configure and manage your full messaging security from one central location. Designed as an MMC snap-in, deployment is simple with a minimum of configuration effort needed.

Ninja seamlessly integrates with Microsoft® Exchange and provides spam, virus, and file attachment protection. Additionally, Ninja makes it easy to create policies across multiple messaging plug-ins with an MMC interface for remote management.

Console



When you first launch Ninja you get an at-a-glance view of your messaging traffic

Multiple scanning engines for higher detection and protection.

Ninja is designed to meet both the spam and virus protection needs of your organization. With multiple spam and virus scanning engines, you automatically receive higher detection rates and a more accurate response to the messaging threats that attempt to enter your network.

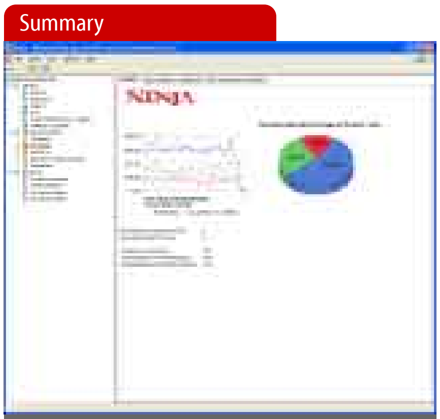
As an integrated email content inspection, anti-spam and anti-virus solution, Ninja not only scans and eliminates viruses and other dangerous message content, but also filters attachments at the Exchange server, before they reach your users and as they are sent between users.

SUNBELT SOFTWARE

Server-based enterprise anti-spam filtering.

For its anti-spam capabilities, Ninja includes Cloudmark's™ anti-spam engine, Sunbelt's own anti-spam engine and support for Real-time Blackhole Lists (RBLs). This plug-in delivers superior spam detection using heuristic functionality with signature lookup capabilities. Ninja can be configured to delete, centrally quarantine, add Subject line identification, or send to a custom folder in the end-user's Exchange mailbox.

Summary



View summary information for total spam activity

Custom rules capabilities gives you the ability to control spam and any other kind of email. You can supplement the spam detection engine with a variety of rules created on a number of email message properties such as body, sender IP, header, or subject. With the ability to strip HTML content prior to scanning, as well as an option to add cumulative points for words or phrases that appear multiple times in a single message, you can control how email is scored based on your custom rule selections. Also, custom rules can be written using regular expressions which allows for even more powerful filtering.

With the increasing number of phishing attacks, identifying legitimate email addresses from spoofed addresses is important. Using the Sender Policy Framework (SPF), users are able to test whether a specific email originated from its claimed domain. Ninja allows users to participate in SPF, helping reduce the risk of phishing and fraudulent email.

Aggressive virus detection and elimination.

Ninja uses multiple industrial strength anti-virus engines to scan inbound and outbound email. With two anti-virus plug-ins using Authentium and BitDefender, you dramatically reduce your chances of infection. You can set scanning parameters at the policy level including per-attachment scanning that allows you to disinfect and/or quarantine pieces of an email, essentially breaking apart the email message and only quarantining infected files instead of stripping all attachments. You can also allow for quarantine and unquarantine actions at the policy level and set per-policy notifications to other key contacts within your organization. Additionally, both sender and receiver notifications can be set for any viral activity detected.

With this layered approach, Ninja not only quarantines and cleans viruses but also blocks potentially hazardous file attachments and looks for common virus signatures during the scanning process including inspection of compressed files such as RAR and ZIP files within emails. Ninja automatically checks for updates to the virus definition files ensuring the best possible virus protection.

Email content inspection and attachment filtering.

Using Ninja's powerful policy-based attachment cleansing capabilities, you can configure inspection and filtering on a per-policy basis. Ninja's intelligent Suspicious Mail Attachment Removal Technology (S.M.A.R.T) filter scans the header of a file to verify that an attachment is what it says it is and has not just been renamed. *No more renaming .exe files to get around the filters.*

You can set rules based on users and file types that enable you to quarantine potentially harmful content or attachments by file extension including .doc, .exe, .dll, .pdf, visual basic scripts and more. For example, you could allow certain users to send .exe files internally while blocking them from being sent externally. No other messaging solution in the industry utilizes policies to manage your attachment filtering!

Configurable reporting options for all plug-ins.

Ninja delivers system reporting for all plug-ins with a set of pre-defined reports with the ability to generate custom reports based on individual needs. The database-driven reporting engine can generate reports with information at the system, group, and/or user level. You can choose reporting options to show the number of inbound mail messages scanned, number of spam deleted or marked, number of viruses intercepted, number of filters triggered, percentage of viruses by name, and more.

Technical Specifications

Component	Requirement	Recommendation
Processor	Intel Pentium or compatible 1Ghz or higher processor	Intel Pentium or compatible 2.4-MHz processor
Operating system and software	Microsoft Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server with SP3 or later Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition Windows XP Professional SP1 for client tools .NET Platform 1.1 SP1 MDAC 2.8 SP1 Microsoft Exchange Server 2000 SP3 or Microsoft Exchange 2003 SP1 *Note:* Ninja Messaging Suite 2.0 does not run on 64-bit editions of Windows Server 2003.	Windows Server 2003 Windows XP professional SP2 for client tools
Memory	256 MB of RAM	768 MB of RAM
Available hard-disk space	100 MB on the hard disk where you install Ninja Messaging Suite 2.0 Additional disk space as needed for the quarantine store.	
Drive	CD drive	
Display	VGA or higher resolution monitor	
Input device	Microsoft Mouse or compatible input device	
File format	Disk partitions must be formatted for the NTFS file system This requirement applies to: - System partition - Partition storing Ninja Messaging Suite binaries - Partitions containing quarantine store files - Partitions containing database files	

SUNBELT MESSAGING NINJA™

Features are subject to change without notice.
All products mentioned are trademarks or registered trademarks of their respective companies.

smndatasheet May 2005