

EMAIL THREAT MANAGEMENT

Complete email threat management to secure your enterprise from malicious threats and inappropriate email use

As email continues to propagate itself into one of the most widely used enterprise communication tools, enterprises are faced with the challenge of ensuring appropriate employee use and a safe and efficient network.

With about 40% of global email traffic consisting of spam (IDC), enterprises are bombarded with a multitude of complex, new and ever-changing content-based security threats including phishing, pharming, spam, viruses, spyware, adware, trojans, worms and other malicious attacks.

The iSheriff™ ETM is a powerful option for protecting your organisation from the ever-increasing flood of unsolicited spam and junk emails that consume valuable network and disk storage resources, distract and cause frustration for your users and even threaten to expose your organisation to the risk of litigation from persons accidentally exposed to offensive or objectionable material.

Furthermore, this protection occurs in real time with an all-in-one appliance solution for Anti-Virus, Anti-Spyware and Anti-Spam.

KEY BENEFITS

ZERO-DAY PROTECTION

iSheriff™ ETM provides superior zero day protection against new or unknown threats through a series of comprehensive threat detection capabilities scanning your network application and protocol layers.

- **Real time behavioural analysis** of indicative data attributes and user behaviour
- **Protocol Anomaly Detection & Blocking** of non-conforming traffic and quarantining of threats
- **Pattern Matching** of high risk miscellaneous code known to spread viruses or attacks which are blocked and deleted before they enter your network

POWERFUL SCALABILITY

With its unique development on the hardened and secure iSheriff™ OS platform, iSheriff™ ETM delivers powerful scalability and reliability with negligible impact on the user's experience.

Greater reliability and accuracy is further harnessed through our holistic document analysis, intelligent tokenising of message content, anti-avoidance strategies and genre-specific analysis.

BETTER VALUE, REDUCED COMPLEXITY

Designed around our patented Media Control Engine (MCE), our highly stable and efficient architecture allows the seamless integration of key 'plug and play' modules to protect and report against malicious threats affecting your network.

Furthermore, this sophisticated architecture does not require additional application software or licenses, and results in reduced server, database hardware and administrative resources.

FLEXIBLE POLICY MANAGEMENT

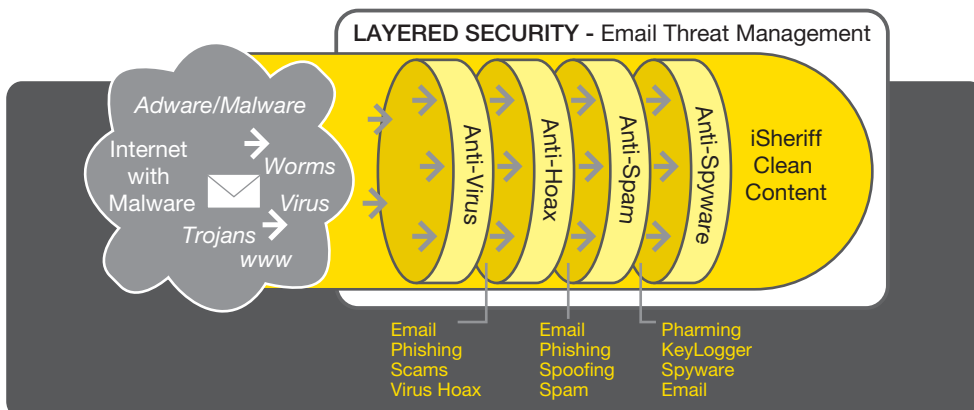
Achieve flexible policy management with our fully integrated iSheriff™ Reporter, an easy-to-

use common reporting and management interface with rich features, a wide variety of pre-defined or customised reporting templates and statistical summaries.

- Innovative "virtualisation" capability for highly scalable enterprises, allowing multiple administrators to remotely maintain their own policies, settings and reports
- Scalable Vector Graphics (SVG) for interactive reports at the user, site, workgroup or organisational level
- Time based policy enforcement
- Personalised end user controls
- Block, allow or report internet content access by category, content-type (MIME), file extension and custom email lists
- Bill back internet access costs to specific departmental units

Our web interface also enables you to define options for dealing with intercepted spam,

- Client Managed Quarantine of suspect emails
- Centrally Managed Quarantine of suspect emails for later examination
- Bouncing of emails silently back to the sender
- Tagging of emails by addition of hidden headers or prefixing of some identifying text to the email subject, allowing the administrator to set up the mail client to filter the tagged email directly into a spam folder for review



KEY BENEFITS

COMPLIANCE REGULATION

Governments around the world are enforcing regulatory measures for tighter network security by ensuring you build and maintain a secure network, protect sensitive information, have strong policy enforcement and regularly monitor and test your network.

iSheriff™ ETM makes compliance easier by complying with SOX, ISO 7799, Basel II and FISMA.

KEY FEATURES

ANTI-VIRUS FILTERING

- Adware
- Application
- Joke, Junk, MSH virus, Trojan, virus, worm

VIRUS HOAX PROTECTION

- Chain letter
- False alarm
- Misunderstanding
- Scams
- Phishing / Pharming
- Scare
- Virus Hoax

ANTI-SPAM FILTERING

- Behaviour based detection of malicious spam
- Anti-spoofing
- Phishing / pharming
- Anti-spyware (attachments)
- Denial of service

ANTI-SPYWARE FILTERING

- All spyware
- Spyware trojan
- Spyware worm
- Directory Harvest Attacks (DHA)
- Pharming
- KeyLogger protection
- DOS protection

ADMINISTRATION

- Secure remote web-based administration
- User account administration
- Comprehensive in-built interactive reporting, statistics and graphs
- Packaged filtering policies
- Bill-back Internet access costs
- LDAP integration
- Administrator / end user defined blacklist & white list support
- Multiple domain support

SUPPORT

- Technical support 24/7
- Installation & set up
- Maintenance
- Hardware support & warranty

SPECIFICATIONS



Hardened and secure iSheriff™ OS

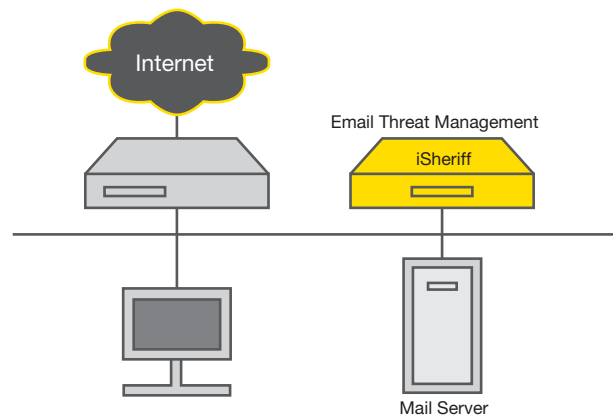
HP Integrity rx1620-2 Server

HP Integrity rx2620-2 Server

HP Integrity rx4640-8 Server

Users	1,000	5,000	20,000+
Processors	1-2	2	8
Microprocessor type	Intel® Itanium® 2 processor 1.6 GHz w/ 3MB & 533MHz FSB	Intel® Itanium® 2 processor 1.6 GHz w/ 3MB & 400MHz FSB	Intel® Itanium® 2 processor 1.6 GHz w/ 6MB L3 cache
Memory	Up to 16GM	Up to 32GM	Up to 128GB
Internal Storage (max)	Up to 600GB	Up to 900GB	Up to 600GB
Dimensions	26.8"D 19"W 1.7"H	26.8"D 19"W 3.4"H	27.2"D 19"W 6.8"H

SIMPLE AND COST EFFECTIVE DEPLOYMENT



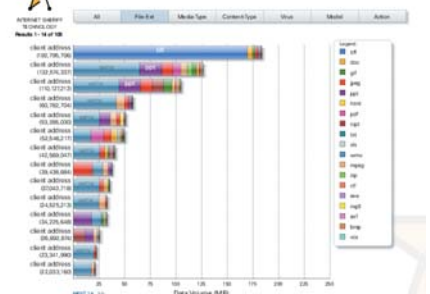
REPORTING SAMPLE

Description	Configuration	Diagnostics	Status/Status	Module	Status	Enable/Disable
Module	Config	Diagnostic	Module	Module	Active	Enabled
Web Management Interface	Config		web_2	Active	Enabled	
URL Cache	Config	Diagnostic	urlcache_3	Active	Enabled	
Filter Policy	Config		filterpolicy_2	Active	Enabled	
Web Filter	Config		webfilter_3	Active	Enabled	
Email Mining	Config		emailminer_1	Active	Enabled	
Anti-Virus Protection	Config		antivirus_1	Active	Enabled	
SMTP	Config		smtp_1	Active	Enabled	
SMTP	Config		smtp_2	Active	Enabled	
Message Transfer Agent	Config		mta_1	Active	Enabled	
POP	Config		pop_1	Active	Enabled	
Command Line Interface	Config		cli_1	Active	Enabled	
Report	Config		report_1	Active	Enabled	
DSGWA	Config		dsdwa_1	Active	Enabled	
DSGWA	Config		dsdwa_2	Active	Enabled	
LDAP Directory Service Integration	Config	Diagnostic	status	Active	Enabled	

Packaged Reports



Received Email Report of Data Volume Allowed by User and File-Extension for the Month of May 2006



Data Volume by User & File Extension

SUMMARY

Internet Sheriff Technology Limited was founded in 1999 to meet the growing need for emerging enterprise content security threats. We responded by developing a multi-layered defence line of security measures with our unique and patented Content Classification Engine delivering superior real time protection, simplicity and extensive scalability.

Our company has more than 1 million users spanning the globe with a diversified base of customers across industry, serving enterprises of all sizes. Unique to our company is the ability to provide Internet Service Providers (ISPs) with services to on-sell to their own customers.



Internet Sheriff Technology Ltd ACN 084 983 086

Head Office Level 1, 59 Parraween Street Cremorne NSW 2090 Australia
P +61 2 9904 9273 **F** +61 2 9908 7266 **E** info@isheriff.com **W** www.isheriff.com

Contact us today for a free 30-day trial at www.isheriff.com