

SAFECHAT®



The unique real-time manager
and moderator of Social Media
and Web 2.0 communications

SafeChat® seamlessly scans all internet traffic to identify the most common social media and Web 2.0 application use including Facebook, Twitter, Gmail, Windows Live Messenger, MSN, Google Talk and popular search engines, including YouTube. Once a communication stream has been identified it is directed through the SafeChat® Policy Enforcement Engine for real-time policy matching and enforcement.



SAFECHAT®



Internet use policies

The **SafeChat®** Policy Enforcement Engine is a fully customizable and flexible framework for an organization to set up as many rules as it requires that match its internet use policy. These rules can be flexibly applied to different groups and social media applications. The framework also provides a manager with the ability to implement time of day rules to manage staff productivity or to gain total visibility over usage of any social media application, such as Facebook, to address this directly.



Web 2.0 application detection system



Real-time policy enforcement framework

Custom dictionaries

Standard dictionaries

Group based activity control engine

Real-time alerting



Blocking/
Moderation

APPROPRIATE CONTENT AND WITH
IDENTITY MANAGEMENT CONTROLS

The unique capabilities of **SafeChat®** provide organizations with the ultimate controls over common social media applications.

Secure and manage your email

SafeChat® scans email and all common attachments, including Microsoft Office documents, PDFs, ZIP files, text files, Open Office documents, HTML and Rich text attachments.

Netbox BLUE

[Previous Message](#) | [Next Message](#) | [Back to Folder](#)

[Reply](#) | [Reply All](#) | [Forward](#) | [Delete](#) | [Redirect](#) | [Download Raw Message](#)

From: postmaster@example.safenetbox.biz
To: admin@example.com
Cc:
Date: Wed 02 Mar 2011 15:47:31
Subject: Alert message from Netbox "oxi"

This is an automated alert message from the Netbox "Customer Example" (example.safenetbox.biz).

A message was processed by the Netbox that triggered a content scanning rule. The details of the message are as follows:

From: John Smith (<http://www.facebook.com/profile.php?id=100000933382>)
To: David Adams (<http://www.facebook.com/profile.php?id=100000853791>)
User: jsmith
Send time: Wed 02 Mar 2011 15:47
Protocol: HTTP
Action: Send
Service: Webmail
Application: Facebook

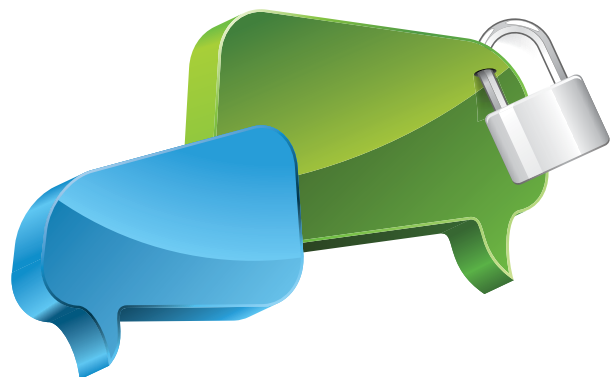
Summary:
List

Here is the customer database we discussed.

The content scanning rule was triggered for the following reasons:
- The text search criteria within rule confidential information was matched. Search term "customer database" was found in message.

If you have any questions, the administrator of this Netbox can be reached at popmaster@example.com

Automated alerts are sent to pre-defined managers immediately a policy is breached with full detail of the inappropriate communication.



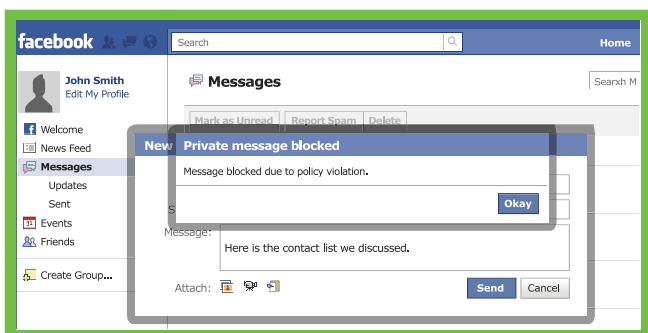
The unique real-time manager and moderator of Social Media and Web 2.0 communications.

"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that you'll do things differently." Warren Buffett

Secure browsing

SafeChat® also enables a business to manage search engine use utilizing SafeChat®'s alerting and reporting capabilities. This can be deployed for inappropriate search requests and, for example, to provide early alerting of self harm or mental health issues. It can also incorporate advanced web filtering capabilities, including category web filtering for ease of use.

The **SafeChat®** technology also provides real-time alerting and analysis with automated blocking and moderation. Web use is also fully managed if a customer uses the additional web content filtering service and this allows full historical reporting for detailed analysis of user or network web activity and policy breaches. SafeChat® can also be used to determine time of day usage policies on the network and company owned Windows and Mac OS devices*.



Messages are blocked bi-directionally in real-time, preventing issues from occurring and alerting managers of the policy breach.

The benefits SafeChat® brings include:

Reputational risk management across all internet communication channels, including email, Social Media, Search and Instant Messaging applications, such as Google Talk and Windows Live Messenger.

Additional SafeChat® features

Identity Management

An organization can ensure that any **SafeChat®** controlled communications (eg Facebook, email, Gmail, Twitter, Windows Live Messenger or Google Talk) is clearly connected back to a corporate identity and any appropriate disclaimers are presented with these communications.

SSL encrypted communication detection and analysis

SafeChat® is also able to detect, analyze and moderate, where required, encrypted traffic (i.e. SSL or HTTPS) across email, Search, Facebook, Gmail and Google Talk communication services.

Activity control

Organizations can use the **SafeChat®** framework to set up activity controls for different groups. This can be used to allow some groups to post content and status updates on tools such as Facebook, while other groups may only have read access permissions.

When used in conjunction with Netbox Blue's next generation Unified Threat Management (UTM) appliances, further features can be enabled including:





- Enterprise-class managed firewall
- Web 2.0 application management, alerting and controls (over 7,000 individual applications)
- Virus scanning of email and HTTP traffic on all network-based traffic (including HTTPS)
- Advanced spam detection and blocking
- Internet link aggregation and load balancing technology
- Internet quota and traffic management
- Real-time and historic reporting of all internet activity
- Zero Day Anonymous Proxy Prevention (ZDAPP)

*Windows refers to Windows Vista, XP and 7, and Mac OS refers to v 10.6.5 and later.











SafeChat® provides real-time management for many of the most popular Social Media applications, including:

SEARCH ENGINES

			
✓	✓	✓	✓

SafeChat® provides full analysis, real-time moderation and policy breach alerting of all search queries. This includes any search requests made on SSL encrypted (HTTPS) traffic as well as standard HTTP search requests. Further controls can be enforced to prevent YouTube uploads.

SOCIAL MEDIA APPLICATIONS

	Facebook	✓
	Twitter	✓
	Gmail	✓
	Windows Live Messenger	✓
	Windows Messenger	✓
	MSN	✓
	Google Talk	✓
	Jabber	✓

SafeChat® provides total control for a wide range of the most popular and ubiquitous Social Media applications. The controls extend to the following types of social collaboration tools:

- Chat – send and receive
- Instant Messaging – send and receive
- Friend requests and accept
- Wall comments (including attachments)
- Status updates (including attachments)
- Private messages (including attachments)
- Email (send and receive – including attachments)
- Tweets
- Re-tweets
- Posts

These controls extend to SSL encrypted (HTTPS) traffic.

SafeChat® can be deployed as a gateway solution or as an integral component of Netbox Blue's unique Borderless Internet Compliance framework, available on Windows and Mac OS devices. Networks of any size can be accommodated with the scalable framework, including hardware and VMware based management appliances that can sit in the cloud, in line or transparently in or off an organization's network. SafeChat® can also be deployed as part of a broader suite of internet management and security capabilities when integrated with Netbox Blue's award winning next generation Unified Threat Management solutions.

SafeChat® supports multiple languages and is unicode enabled, allowing it to identify alternative language character formats. The SafeChat® Management Server integrates with Microsoft Active Directory, Apple Open Directory and Novell eDirectory.



Why Netbox Blue?

Netbox Blue is a leading provider of innovative internet compliance, management and security solutions. Netbox Blue provides organizations with unique, real-time social media analysis and controls with predictive outcomes and benefits. The company owns granted patents around this unique technology and has other patents in the process of being granted. The company was established in 1999, is privately held and is based in Australia. It has a presence in over 19 countries and has partnerships and distribution agreements with some of the world's largest IT companies.

Head Office

37 Kennigo St, Spring Hill, QLD 4000, Australia
Phone: 1300 737 060 | **Fax:** 1300 737 069

Postal Address

PO Box 396, Fortitude Valley, QLD 4006, Australia

International Phone: +61 2 8090 7779

www.netboxblue.com