



USING YOUR EXISTING IT SECURITY SOLUTIONS TO ENABLE TRUE BUSINESS VALUE

Webinar 25th February 2015



websense
TRITON
AP-WEB

Today's Speaker



Bradley Anstis

- Sales Engineering Manager, ANZ
- Speaker on internet security technology and malware trends
- Over 20 Years of IT industry experience with more than 10 years specifically within Internet Security
- banstis@websense.com
- This session is being recorded and the slides will be made available
- Questions are welcome throughout the session through the question panel

Objective of Todays Session

- This is not a security focussed session
- We will talk about features available in Websense products, but they might be available in the products you currently use as well?
- I am hoping to change the way you consider your current IT security products, particularly your Email & Web security gateways and give you some ideas to start using some of the functionality you have already paid for to benefit your business
- This is not a sales pitch...

How to Evolve From Being Department No!

1. Find ways of enabling true business value
 - Social media
 - BYOD
 - Web 2.0
 - Marketing
 - ...
2. Determine your security strategy around the idea
3. Pitch it to management
4. Enjoy being taken a lot more seriously...
5. Get in front of change, not as an after thought...





EMAIL IDEAS

BRAVE THE NEW WORLD.

Email Signatures

- Add an Outbound Annotation or Disclaimer to every Outbound email message
 - Marketing messages
 - Company announcements
 - Opt-out links...

Email Auto Replies

- Used in conjunction with generic enquiry email addresses
- Immediately reply to an incoming enquiry
- Redirect the email to a particular employee
- Potentially also further optimise by detecting actual product being requested, send back link to datasheet, redirect to best rep.

Policies > Add Inbound Policy > Add Rule > Add Action

Notification Properties

Configure the contents of a notification message, including the sender, recipient, subject, message body, and any attachment, if desired.

Sender: ☐ Original email sender
☐ Administrator
☒ Custom:

Recipient: ☒ Original email sender
☐ Original email recipient
☐ Administrator
☐ Custom:

Enter at least 1 email address. Separate multiple addresses with a semicolon.

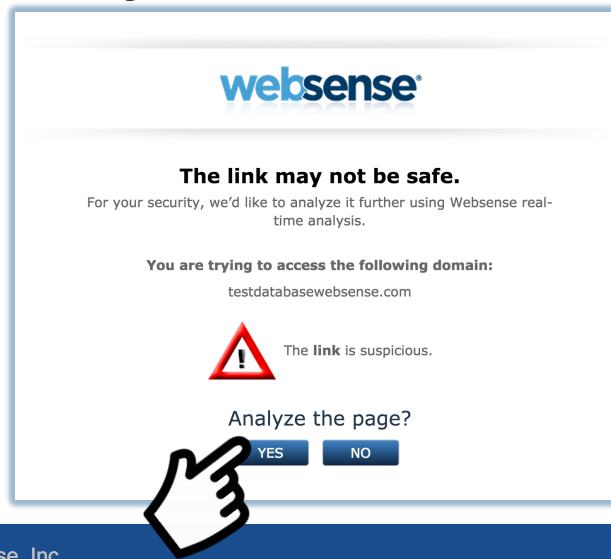
Subject:


Content:

Attachment: ☒ Do not attach message

Phishing Education At Point of Click

- Educate your users at the time possible infection...
- Upcoming feature around managing and measuring the effectiveness of phishing education



**Phishing Attack Blocked**

The email containing the website you requested is classified as a Phishing Attack and has been blocked for your protection.

SAFEGUARD yourself and **NEVER** click on a link embedded in a suspicious email.

What is a phishing attack?

- Fake emails sent by hackers/thieves disguised as a legitimate source in an attempt to steal confidential information through phony embedded links.
- The emails often request personal information such as bank/credit card numbers, social security numbers, passwords, etc.
- This information is used for malicious purposes and can lead to identity theft and significant financial or data loss.

Common tactics and signs of phishing emails:

- Usually poor spelling, grammar, and repeated words or sentences.
- Threats that your account has been compromised or will be closed.
- Spoofing popular websites (PayPal, Facebook, etc.) by using company logos that appear to be legitimate.
- Urgent emails posing as family members or friends requesting money.

Example of a phishing email:

Dear Member
As a part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Poor grammar *Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link bellow to fill the Copyright Law form:*

Embedded links <http://www.facebook.com/application-form>






Customising Block Messages

- Point to your Intranet pages for immediate education customised to your organisation
- Insert text, images, video's & links
- Acceptable Use Policy training/test
- Contacts for further help
- Organisation best practices review

Default Message Content

Subject line prefix: Notification: _REASON_ : _REASONINFO_ :

[Change character set](#)

B *I* x x² **T** **rT** **H** **L**      Variables/tokens

A message sent to you from outside your company has been _DISPOSITION_ by your email security service.

_NOTIFIED_ADMIN_ _NOTIFIED_SENDER_

Please refer to the organisations Acceptable Use Policy at:-

http://intranet/email_aup

If you require further information, you may contact your [Mail Administrator](#).

Message Details	
Sender:	SENDER
Subject:	SUBJECT

Inappropriate Image Education












- Do not implement as an absolute block – False Positive too high
- Implement as an opportunity to train the user when they are sending images inserted or attached to email

Default Message Content

Subject line prefix:

Image Distribution through Email Policy

[Change character set](#)

B *I* **x₂** **x₂** **T** **tT** **H** **I** **T**            **Variables/tokens**

You recently sent an email with the below details:-

Subject: _SUBJECT_
Recipients: _RECIPIENTS_

This email contained an image and has been quarantined.
Please note that this organisation has a very strict policy around the distribution of non-business related images within email.

If you believe that this email was legitimate then please release the email from your email quarantine.

If you wish to delete the email, either delete it from your quarantine or it will automatically be deleted in 7 days.

Please review the organisations Email acceptable use policy on the Intranet at:-
http://intranet/email_AUP

Rewriting Email Addresses – Inbound & Outbound

- Can be used for multiple organisations to appear as one
- Very useful after mergers/acquisitions
- Applied to both incoming & outgoing email
 - Outbound: All email looks to be from the same domain
 - Inbound: All email redirected to the correct internal domain & user

Envelope Sender and Message Header Rewrite List

Specify the sender email address (user@mycompany.com) or domain address (@mycompany.com) you want Email Security Gateway to use for redirecting messages. Rewritten entries include address elements found in the message header. You can rewrite address. You cannot rewrite an email address as a domain address. Similarly, a domain address may be rewritten only as a domain address.

<input type="checkbox"/>	Original Email or Domain Address	Rewritten Email or Domain Address
<input type="checkbox"/>	@company1.com	@combinedco.com
<input type="checkbox"/>	@company2.com	@combinedco.com




WEB IDEAS

BRAVE THE NEW WORLD.

Block Page Customisation

- Customise to suit your organisation
- Direct users to your Intranet
- Customise with your organisations imagery & style
- Use for:-
 - AUP acceptance prior to web surfing
 - AUP update education & re-acceptance
 - Other organisation announcements, outage notifications...




Acceptable Use Policy

Your organisation requests that you accept the terms of its Acceptable Use Policy.
This policy can be found on the organisations Intranet at:-

https://intranet/web_aup.html

For more information, contact your company administrator.

☐ I agree to accept the terms of this policy.

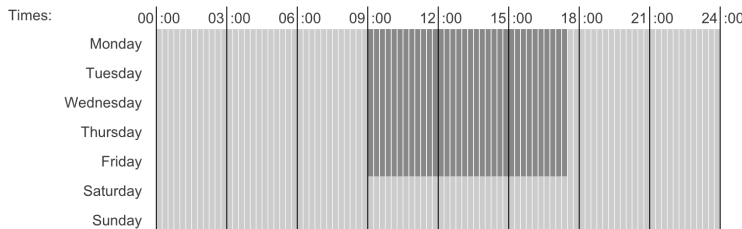


Business Application Performance

- Ensure Optimal Performance of business applications & websites by prioritising those applications over lower priority applications & websites, can be done via:-
 - Bandwidth optimisation
 - Usage Quota's
 - Time of day filtering

Time Period Details

Name: Working hours
Description: Working hours
Timezone: -- user policy/connection timezone --



Bandwidth

Description:
Parent category that contains the categories: Internet Radio and TV, Internet Telephony, Peer-to-Peer File Sharing, Personal Network Storage and Backup, Streaming Media

Permit **Block** **Confirm** **Quota**

Advanced Filtering

- ☐ Block keywords
- ☐ Block file types
- ☒ Block with Bandwidth Optimizer

Block based on traffic for: Entire Network

Block when traffic exceeds: 30 %

☐ Default

Apply to All Categories

Enforcing Email & Web Acceptable Use Policies

- Instead of just filing AUP's, enforce them
- Involve HR!!!
- Ensure they are enforced consistently
- Use breeches as an opportunity for education (Depending on seriousness)
- Done properly this action can be a legal defence from employee driven legal action – but get legal advise

AUP Basics

- Allow limited personal use of Web and email
- Outline what is acceptable and what is not; while preserving company culture
- Be consistent with enforcement and setting precedents
- All email should be identified with a name or email address – avoid spoofing
- Copyright - inform staff on copyright issues relating to email or Internet documents
- Monitoring and enforcement - inform staff about what is acceptable inside business hours and what is acceptable outside of business hours, if there is any difference. This needs to be clearly stated in the policy
- Reserve the right to monitor all messages/files on the company network

Safely Enabling Social Media

- Does your Web AUP include Social Media?
- Use granular social media controls to safely enable social media use by user group policies
- Great enabler for business, increasing amount of business communications are via social media...



Safely Enabling YouTube

- Lockdown YouTube access to just the video's you publish through your organisations YouTube channel + YouTube Education video's

Categories

Choose actions for web categories to restrict access to your end users. Requests are assigned to at least one category, using the Unknown category.

Standard Categories

- Unknown
- Abortion
- Adult Material
- Advocacy Groups
- Bandwidth
 - Educational Video
 - Entertainment Video
 - Internet Radio and TV
 - Internet Telephony
 - Peer-to-Peer File Sharing
 - Personal Network Storage and Backup
 - Streaming Media
 - Surveillance
 - Viral Video
 - YouTube
- Business and Economy
- Collaboration - Office
- Drugs

Action

☐ Do not block

☐ Require user authentication

☐ Confirm

☐ Use Quota

☒ Block access

Display the page

End users without exceptions configured cannot access YouTube because the category is blocked.

☒ Filter using YouTube for Schools account

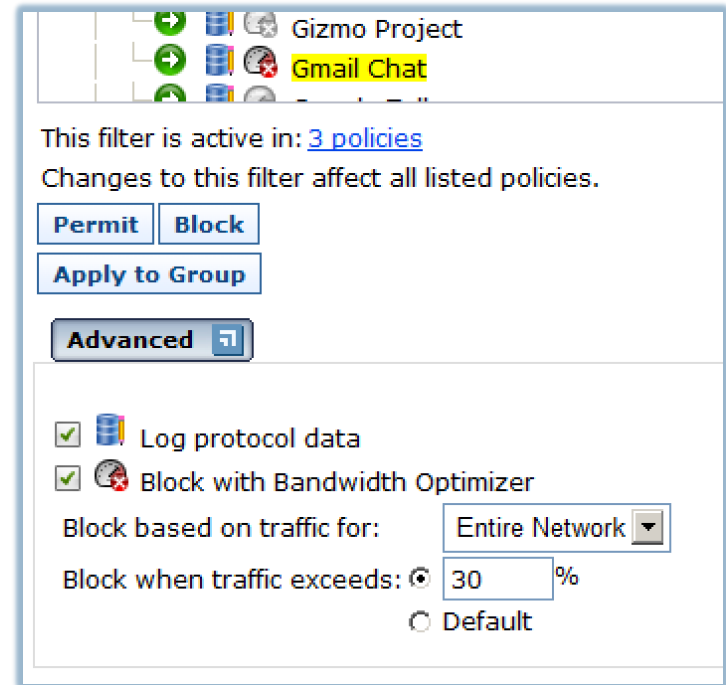
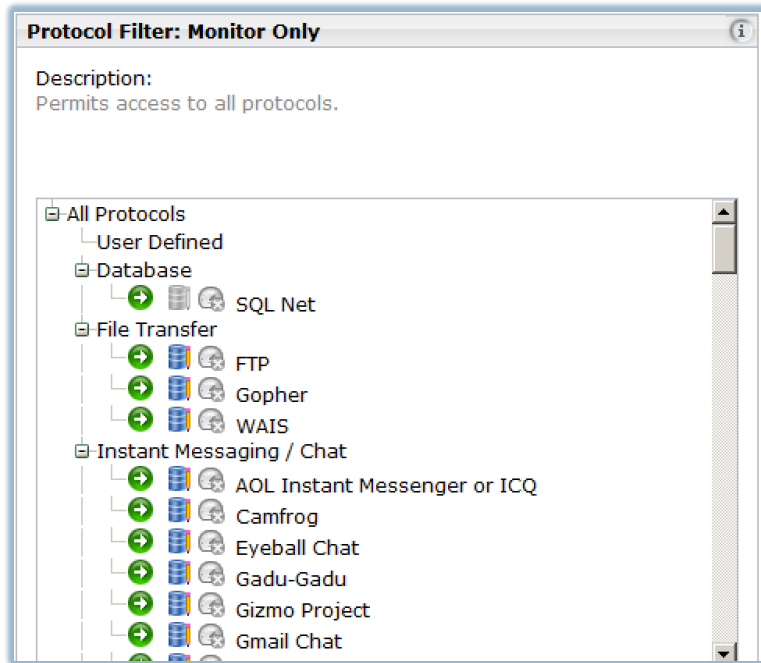
Account code:

Category Info

Category used to manage the YouTube domain

Application Protocol Filtering

- Connect Websense appliance to spanned network port to use the Network Agent function





ADMINISTRATION IDEAS


BRAVE THE NEW WORLD.

Delegated Administration

- Enabling the helpdesk for Email quarantine
- Enabling HR to run user investigation reports
- Delegate Spam Management to others
- What else can be delegated?
 - Organisation allow/block lists for email or web
 - Regular departmental reporting – schedule & email?

Web Admins

Delegated Administration

 View Administrator Accounts |

<input type="checkbox"/>	Role	Type	Description
<input type="checkbox"/>	Super Administrator	Policy and reporting	Super Administrator
<input type="checkbox"/>	Departmental Administration	Policy and reporting	Administration Role to manage set group of users
<input type="checkbox"/>	HR User	Investigative reporting	Reporting role to run user investigation reports only

Email Default Admins

<input type="checkbox"/>	Role
<input type="checkbox"/>	Super Administrator
<input type="checkbox"/>	Auditor
<input type="checkbox"/>	Reporting Administrator
<input type="checkbox"/>	Quarantine Administrator
<input type="checkbox"/>	Security Administrator
<input type="checkbox"/>	Policy Administrator
<input type="checkbox"/>	Group Reporting Administrator

Email Quarantine Role

Roles > Edit Role

Edit a role. Assign managed users, grant the necessary permissions.

Role Name: Quarantine Administrator

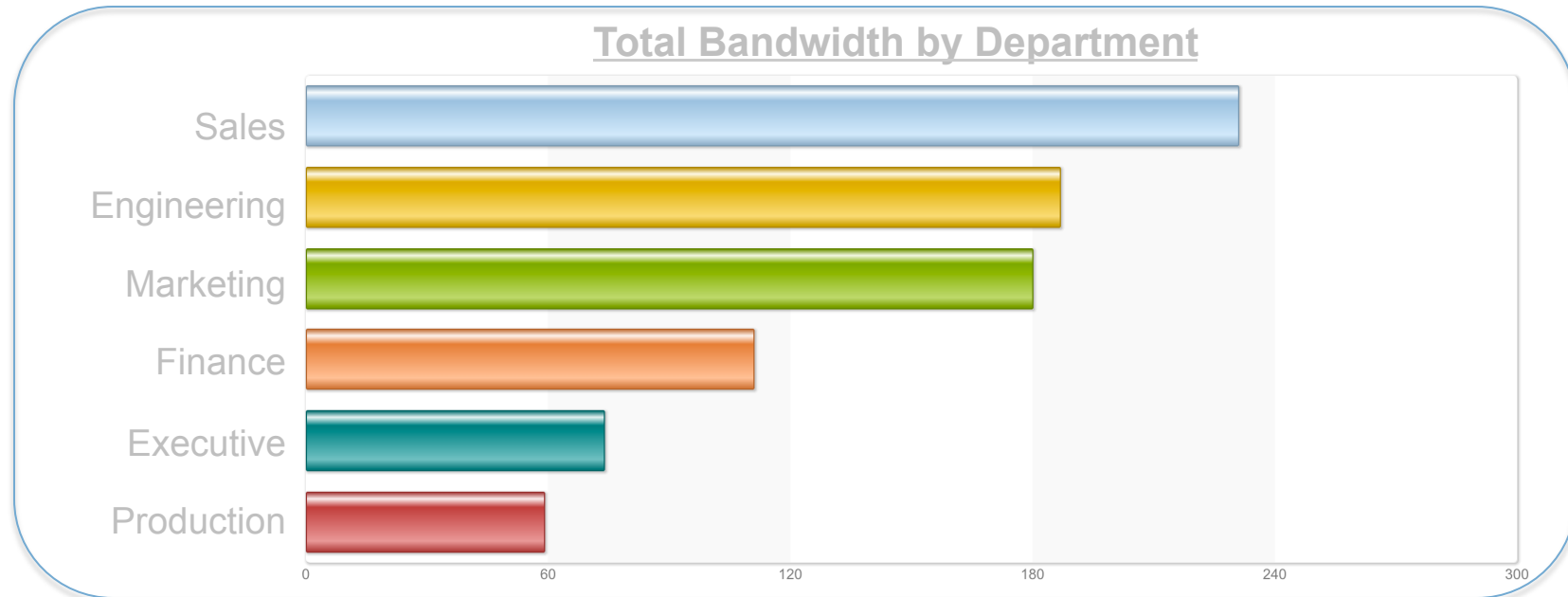
Description: Administrators with this role can manage specific queues, troubleshoot from logs, and release messages to users from assigned queues.

Managed users and groups: ⓘ

<input type="checkbox"/>	User Name
<input type="checkbox"/>	*@websense.com

BU Reporting to Allocate Cost

- Run total traffic reports to calculate proportionate departmental charging within your organisation
- Can run reports across Email & Web



Extended Reporting

- SIEM Integration
- Splunk Applications

☒ Enable SIEM integration for this Policy Server

IP address or hostname: 10.4.228.60

Port: 514

Transport protocol: ☒ TCP

☐ UDP

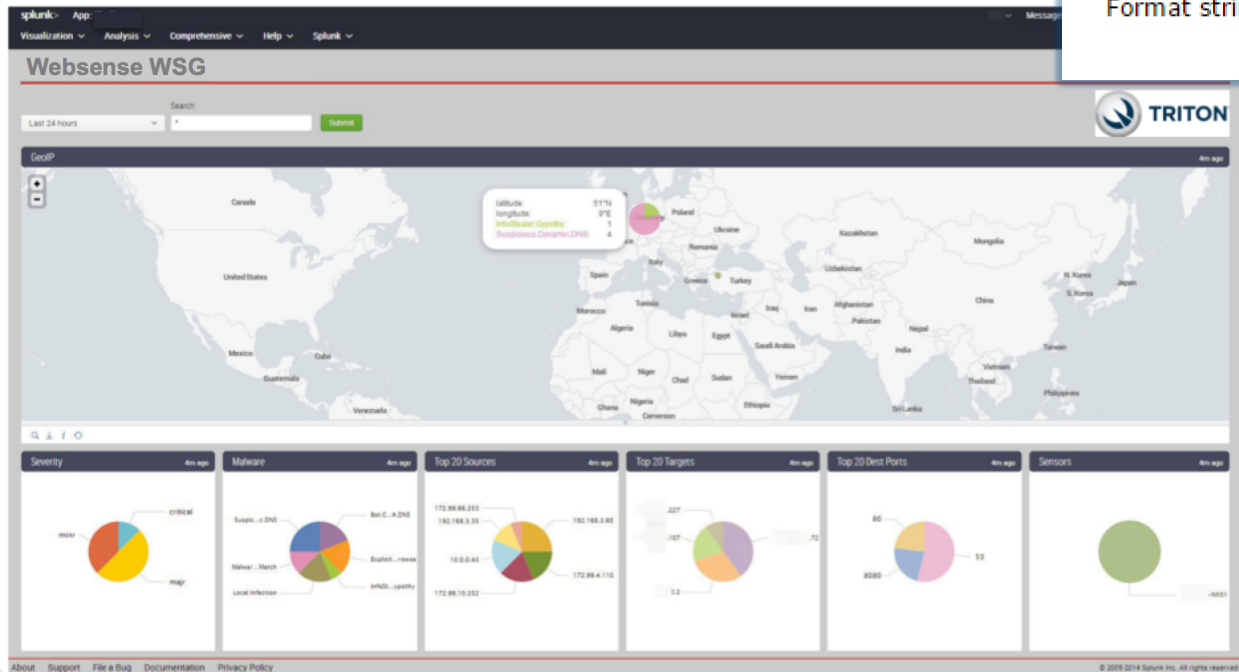
SIEM format: syslog/key-value pairs (Splunk and others) ▼

syslog/CEF (ArcSight)

Format string: **syslog/key-value pairs (Splunk and others)**

syslog/LEEF (QRadar)

Custom



websense®

Thank you...

BRAVE THE NEW WORLD.