USING YOUR EXISTING IT SECURITY SOLUTIONS TO ENABLE TRUE BUSINESS VALUE

Webinar 25<sup>th</sup> February 2015



#### **Todays 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**





# **Email Signatures**

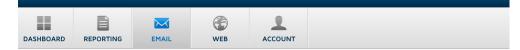
- Add an Outbound Annotation or Disclaimer to every Outbound email message
  - Marketing messages
  - Company announcements

websense:

Th

Web

Opt-out links…



Email > Policies > test > Outbound Annotation List > Add Outbound Annotation

#### Add Outbound Annotation

Define an annotation that will be added to messages passing through the cloud service.

Domain or address list: Domain Users Email addresses, domain names or groups (no wildcards, comma separated) Position: Bottom 🔻 Websense Scores Frost & Sullivan Australian Secure Content Lessons Learned from the Biggest Security Breaches LIVE Webcast: Wednesday, Nov. 5, 2014: 1:30 p.m. AEDT DO YOU HAVE Office of t 🔊 TRITON WHAT IT TAKES? OPERATION Spear Phish Start Your Mission Seven Stages of Advanced Websense Scores Frost & Sullivan Australian Secure Content Management Vendor Award For Third Consecutive Year... FROST & SULLIV Gartner Security & Risk Gartner. Management Summit 2012 Summits 16-17 July | Sydney, Australia Learn More

#### **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.

|   | 1 7   |  |  |  |  |
|---|---|--|--|--|--|
| P | <u>vlicies</u> > <u>Add Inbound Policy</u> > <u>Add Rule</u> > Add Action |  |  |  |  |
|   | Notificatio   | n Properties   |  |  |  |
|   | Configure t   | gure the contents of a notification message, including the sender, recipient, subject, message body, and any attachment, if desired. |  |  |  |
|   | Sender:   | C Original email sender<br>C Administrator<br>© Custom:  |  |  |  |
|   |   | sales@websense.com   |  |  |  |
|   | Recipient:  | ✓ Original email sender  |  |  |  |
|   |   | Original email recipient   |  |  |  |
|   |   | Administrator  |  |  |  |
|   |   | Custom:  |  |  |  |
|   |   |  |  |  |  |
|   |   | Enter at least 1 email address. Separate multiple addresses with a semicolon.  |  |  |  |
|   | Subject:  | Thank you for your enquiry   |  |  |  |
|   | Content:  | Your request has been forwarded to a sales<br>representative who will be back in contact with<br>you shortly.                        |  |  |  |
|   |   | Please visit www.websense.com for more   |  |  |  |
|   | 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.

websense

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

Page 8

## **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  |   |                      |  |  |
|--|---|----------------------|--|--|
| B I × <sub>2</sub> × <sup>2</sup> T• TF• HI•   | ification: _REASON_ : _REASONINFO_ :<br>T₂ T₂ I III III III IIII IIIIIIIIIIIIII | Change character set |  |  |
| A message sent to you from outside your company has been _DISPOSITION_ by your email security serviceNOTIFIED_ADMINNOTIFIED_SENDER_ Please refer to the organisations Acceptable Use Policy at:- http://intranet/email_aup/ If you require further information, you may contact your <u>Mail Administrator</u> . |   |                      |  |  |
| Message Details  |   |                      |  |  |
| Sender:  | SENDER  |                      |  |  |
| Subiect:   | 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 se             |
| B I x₂ x² T- fT- HI- T₂ T₂ IΞ ΕΞ 📅 🤊 🗠 🕼 🐼 Variables/tokens  | 3                               |
| You recently sent an email with the below details:-  |                                 |
| Subject: _SUBJECT_<br>Recipients: _RECIPIENTS_   |                                 |
| This email contained an image and has been quarantined.<br>Please note that this organisation has a very strict policy around the distribution of non-busine | ss related images within email. |
| If you believe that this email was legitimate then please release the email from your email qua  | rantine.                        |
| If you wish to delete the email, either delete it from your quarantine or it will automatically be d   | leleted in 7 days.              |
| Please review the organisations Email acceptable use policy on the Intranet at:-<br>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 or domain 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.

| Original Email or Domain Address | 🖍 Rewritten Email or Domain Address |
|----------------------------------|-------------------------------------|
| @company1.com                    | @combinedco.com                     |
| @company2.com                    | 🔪 @combinedco.com                   |
|                                  |                                     |

Page 11

# WEB IDEAS





## **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 & reacceptance
  - 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.

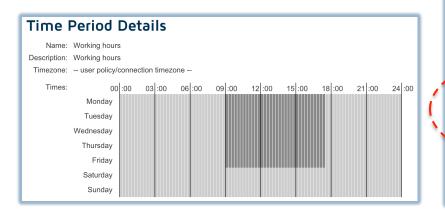
I agree to accept the terms of this policy.

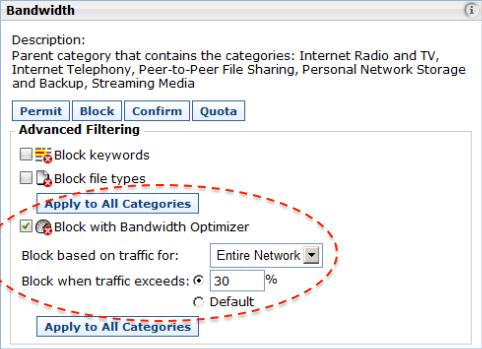
Continue



# **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





# 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 <u>safely</u> enable social media use by user group policies
- Great enabler for business, increasing amount of business communications are via social media...



Update an existing AUP to address social media concerns. Don't have an AUP? Create one for your organization using templates available online or at www.m86security.com.

Acceptable Behavior

Which

Sites?

Separate

Networks

**Privacy** 

Settings

Start by expanding your current email communications policy, including its definitions of acceptable language and behavior, to all Internet use within the company. Through policy, inplement unacceptable language and image filters and apply these to all users. Global organizations should consider any local customs, colloquialisms or phrases to take into account.

Limite access to well-known social media sites or list only sites that pertain to your business. This is easy to enforce through technical policy controls because it's a matter of blocking only. Sites can also be blocked or allowed by time of day.

Consider creating policies for "two networks": one work-related and one personal. Limit access to personal networks to lunch times or after hours, and allow open access to work-related networks. Because sites like Facebook serve dual purposes, it's difficult to limite access by site.

Review all privacy settings available on social media sites that contain your corporate profile. Most of these sites default to open access, so it's critical to ensure that adequate privacy settings are selected.

Educate employees about privacy settings are well. Opting for minimal security can open an employee's system to malware, which can also infect the organization's network.



Allowed

**Plug-ins** 

Determine what level of social networking activity is acceptable for your organization. For example, allow some employees to post only to the corporate profile, but allow view-only access (no posting ability) to employees except during limited times during the day. Look for granular social network controls that can be set by network.

Limit the installation of plug-ins for games or other embedded features on social networks. Unrestricted use of these features can negatively impact network security as well as employee productivity. Look for granular social network controls that can be set by network.

## Safely Enabling YouTube

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

Categories

© 2015 Websense,

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

| Search Q  | Quick select | $\overline{\mathbf{v}}$   |     |
|---|--------------|---|-----|
| Standard Categories   |              | Action  |     |
| <sup></sup> Unknown<br>■ Abortion   |              | 📟 🛛 🔍 Require user authentication   |     |
| Adult Material  |              |   |     |
| Advocacy Groups   |              | C     C |     |
| Bandwidth Educational Video   |              |   |     |
| - Entertainment Video   |              | Display the Access Blocked v page   | ge  |
| Internet Radio and TV   |              | End users without exceptions configured cannot acce   | ess |
| <ul> <li>Internet Telephony</li> <li>Peer-to-Peer File Sharing</li> </ul> |              | <ul> <li>TouTube because the category is blocked.</li> <li>Filter using YouTube for Schools account</li> </ul>  | -   |
| - Personal Network Storage and  | d Backup     | Account code: 22m57rmkf6tq  |     |
| <ul> <li>Streaming Media</li> <li>Surveillance</li> </ul>                 |              |   | -   |
| - Viral Video   |              | Category Info   |     |
| YouTube   |              | Category used to manage the YouTube domain  |     |
| Business and Economy  |              |   |     |
| Collaboration - Office  |              |   |     |
| <sup>i</sup> Drugs  |              |   |     |

# **Application Protocol Filtering**

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

| Protocol Filter: Monitor Only   | 💛 🗒 🕼 Gizmo Project  |
|---|--|
| Description:<br>Permits access to all protocols.  | Gmail Chat   |
|   | This filter is active in: <u>3 policies</u>  |
|   | Changes to this filter affect all listed policies.   |
| All Protocols User Defined Database SQL Net File Transfer Gopher Gopher Gopher Gomman Messaging / Chat Gomman Messaging / Chat Gomman Gomman Me | Permit       Block         Apply to Group         Advanced       Image: Constraint of the second |
| Gizmo Project   | Ö Default  |

# ADMINISTRATION IDEAS

BRAVE THE NEW WORLD.



## **Delegated Administration**

- Enabling the helpdesk for Email guarantine
- 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?

|                       | Admins                        |                            |                         |   |  |  |  |  |
|-----------------------|-------------------------------|----------------------------|-------------------------|---|--|--|--|--|
|                       | Delegated Administration      |                            |                         |   |  |  |  |  |
|                       | 📳 View Administrator Accounts |                            |                         |   |  |  |  |  |
| L                     |                               |                            |                         |   |  |  |  |  |
| Role Type Description |                               |                            |                         | Description   |  |  |  |  |
| L                     |                               | Super Administrator        | Policy and reporting    | Super Administrator                                   |  |  |  |  |
| L                     |                               | Departmental Adminstration | Policy and reporting    | Administration Role to manage set group of users      |  |  |  |  |
| L                     |                               | HR User                    | Investigative reporting | Reporting role to run user investigation reports only |  |  |  |  |



| Roles > Edit Role |
|-------------------|
|-------------------|

Role

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

| ole Name:  | Quarantine | Administrator |
|------------|------------|---------------|
| ore manne. | Quarantine | Administrator |

| Administrators with this role can manage<br>specific queues, troubleshoot from logs, and<br>release messages to users from assigned | <b></b>                 |
|---|-------------------------|
| aueues.   |                         |
| ·   | $\overline{\mathbf{v}}$ |

#### Managed users and groups: (i)

User Name +

\*@websense.com

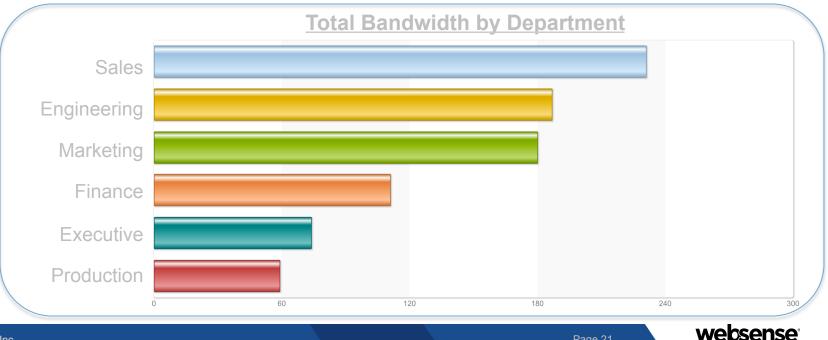
Page 20

websense

Web

#### **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

| spikunk> App:<br>Visualization v Analysis v Comprehensive v Help v Spikunk v  | v Mesay:   | ormat st                        |
|---|--|---------------------------------|
| Websense WSG  |  |                                 |
| Search<br>Last 24 hours v * Solonet   |  |                                 |
| GeolP   |  | 4m a;                           |
| Conds   | Andrew Street Constrained and Andrew Street Constrained and Co |                                 |
|   | Normal         Log         Log         Log         Addama         Hoge         Hoge <t< td=""><td></td></t<>  |                                 |
| Severity 4m app Mahaze 4m app   | Top 20 Sources 4m apr Top 20 Targets 4m apr Top 20 Dest Ports 4m apr Sensors   | 4m a                            |
| mer of the | 172.88.8.11<br>18.181.11 - 78.181.01 - 20<br>.00 - 70  |                                 |
| About Sunnert Elle a Run Documentation Privacy Policy   |  | 5.3014 Geburk Inc. All risks re |

| Enable SIEM integration for this Policy Server |   |             |  |  |
|--|---|-------------|--|--|
| IP address or hos                              | Port: 514   |             |  |  |
| Transport protoco                              | DI:  TCP UDP  |             |  |  |
| SIEM format:                                   | syslog/key-value pairs (Splunk and  | d others) 🔻 |  |  |
| Format string:                                 | syslog/CEF (ArcSight)<br>syslog/key-value pairs (Splunk and<br>syslog/LEEF (QRadar)<br>Custom | d others)   |  |  |

© 2015 Websense, Inc.

# Thank you...

BRAVE THE NEW WORLD.