



How Postini is Helping You Defend Against Virus Attacks

Adam Swidler - Senior Manager, Solutions Marketing

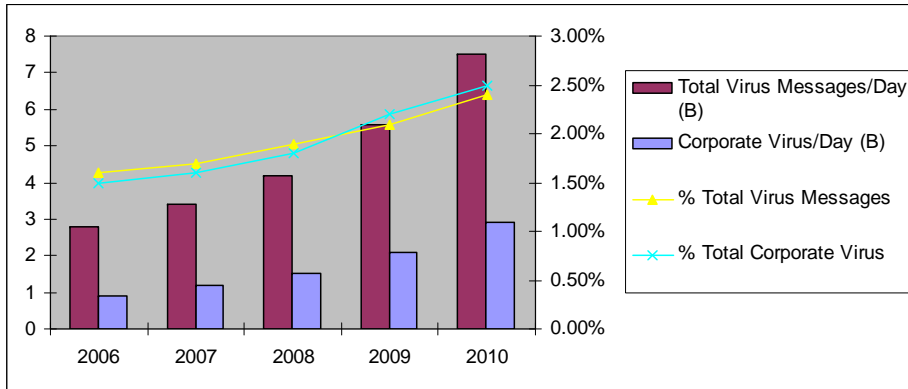
Barry Schmell - Senior Technical Trainer

Agenda



- The threat landscape
- Solution overview
- Best practices
- Summary and Q&A
 - Submit questions on-line via WebEx chat window, addressed to Barry Schmell

Threat landscape for virus attacks



Source: Radacati

Event Tracking
Significant incidents recently reported to HackerWatch.org

24 Hours	8,537,954
7 Days	56,887,420
30 Days	178,730,840

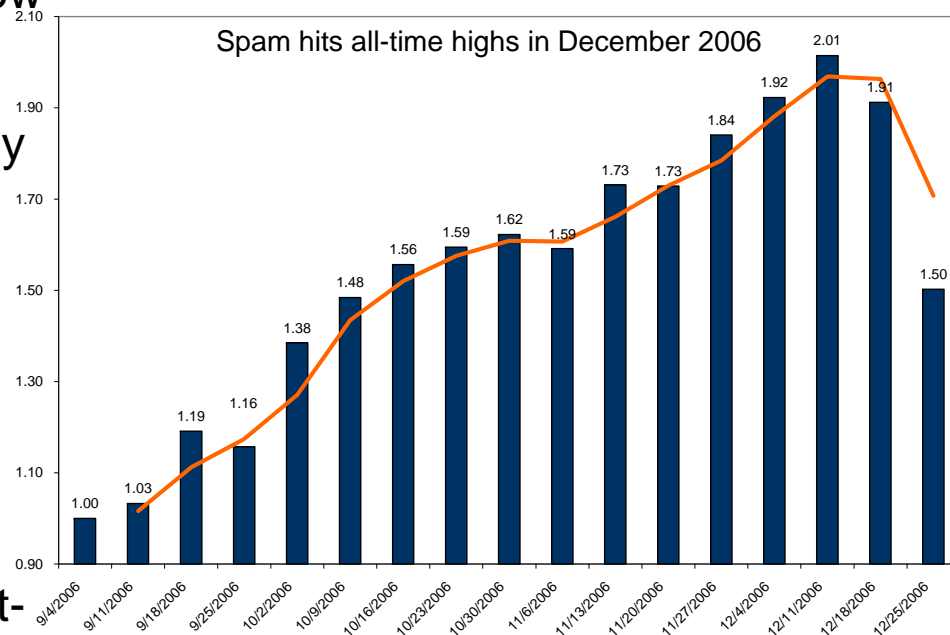


- Virus infected corporate Email expected to grow > 25% per year
- Expected to pass 2 Billion infected corporate email by 2009
- Millions of significant incidents each day reported to McAfee's Hacker Watch
- Vulnerabilities are actually on the increase
 - Highest number ever recorded from Jan to June 2006¹
- Virus attacks are crossing over into other channels such as web and instant messages

¹ Symantec Internet Security Threat Report

Spam & virus attacks are increasingly related

- Total email spam volumes are up 158% in Q4 2006¹
 - More than 94% of all email is now spam
- Driven by bot-nets (networks of compromised computers, infected by hackers)
- Spam and virus activity are increasingly linked to each other
 - December 2006 - “Happy New Year”
 - January 2007 - “Storm”
- Virus infected spam email sent by bot-nets zombies, designed to harvest more computers into the bot-net
- Viruses are spreading across different channels such as Web and instant messaging



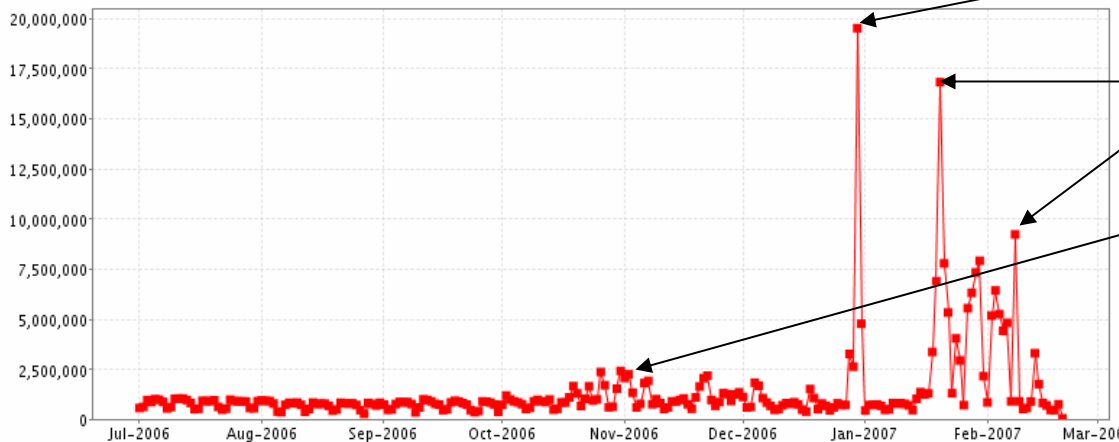
Weekly data, normalized to September 1, 2006 = 1.00, source: Postini

¹ vs. same period last year

Virus attack trends



Overall virus blocking Jul 2006 - Feb 2007



- “Happy New Year” attack spike
- “Storm” attack and variations
- Stration attacks
- Trend of significant increases in attack volume
- 23 days with virus attacks greater than any day in previous 6 months

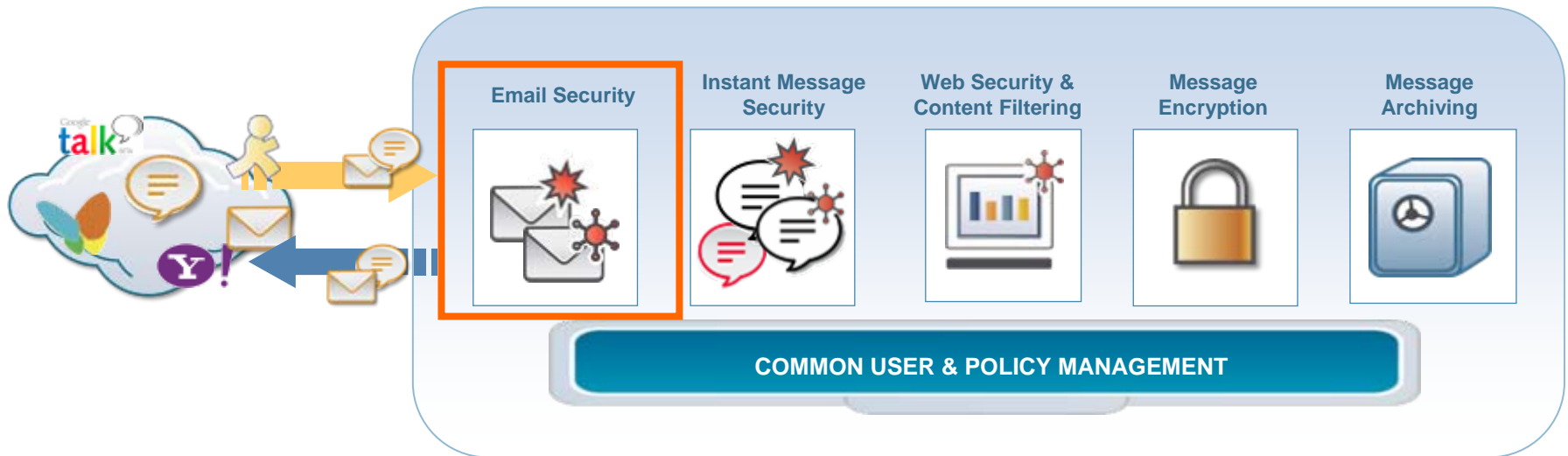
Agenda



- The threat landscape
- Solution overview
- Best practices
- Questions & answers
 - Submit questions on-line via WebEx chat window, addressed to Barry Schmell

Postini Communications Suite

Postini Communications Security Solution Complete, tightly Integrated suite of Email, IM, Web security services



UNIFIED ADMINISTRATION



- Unmatched productivity and trust
- Improved compliance
- Decreased business risk
- 99.999% availability
- Real-time control and visibility

Have a question? Submit it via the
WebEx chat window to Barry Schmell

Postini Email Security Service

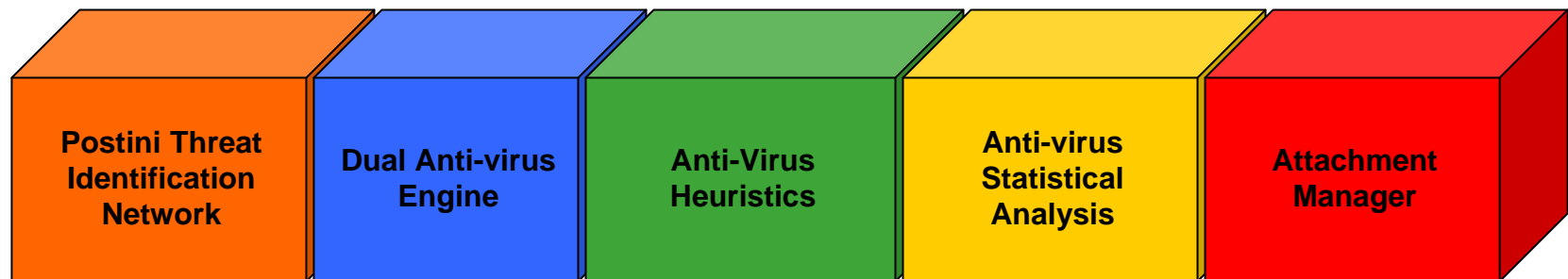
- Most effective spam filtering architecture
 - Highest catch rates
 - Lowest false positives
- PreEMPT anti-virus protection
 - Blocks viruses before they reach corporate networks
- Flexible policy framework
- Industry leading managed service
 - Scalable
 - Five 9's availability
 - Easy to manage and deploy



Postini's PreEMPT Provides Zero-Hour Virus Protection

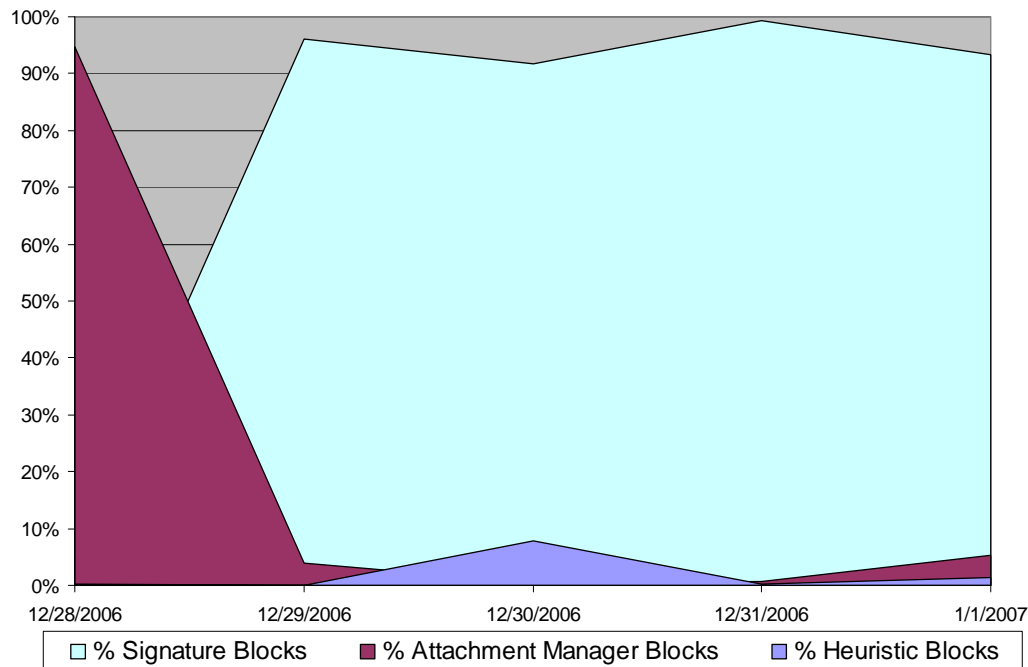


- PreEMPT: Postini real-time evaluation and detection technology for virus protection
 - Five Layers of defense
 - Each layer has a specific capability to defend against viruses



- Tracks behavior of compromised spam zombies sending spam and viruses
- Blocks connection in real time based on overall behavior without need of signatures
- Best-in-class commercial protection from McAfee and Authentium
- Early access to latest signatures, checks every 60 seconds
- Mimics program execution and identifies which Windows operating system calls are made
- Identification of MIME exploits, active code, message fragments and other suspicious message characteristics
- Advanced statistical analysis engine that models risk with complex message attribute model
- Policy control for executables, multimedia and other high-risk data types

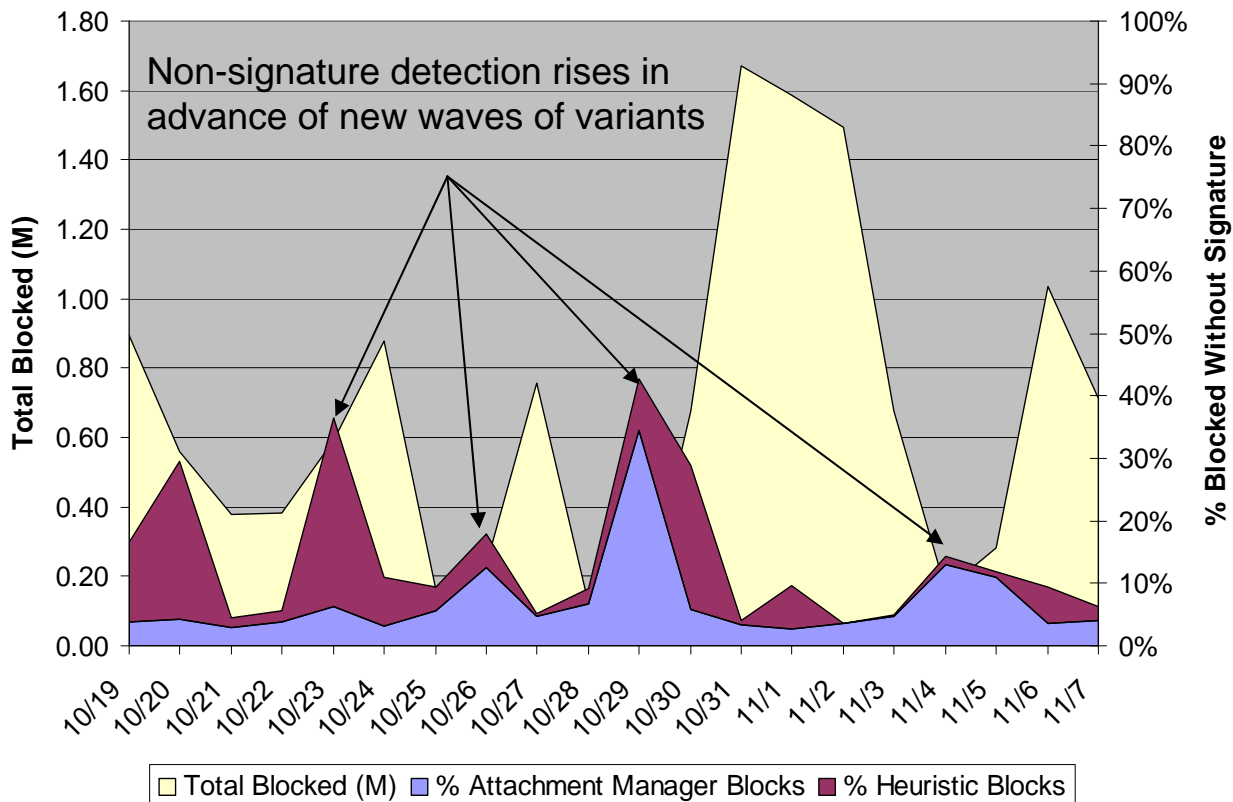
PreEMPT protection in action: “Happy New Year “



- Major virus attack just ahead of Jan 1
- Huge spike in volume, approx 20X average virus volume
- Advanced detection with PreEMPT technology is blocking over 95% in the early hours of attack
- Signature blocking takes over after that
- Postini blocks over 25M infected messages, 19M on Dec 30th alone

PreEMPT protection in action: "Stration"

Q4 2006 Stration Outbreak



- First variants seen in August and new strains seen through December 2006
- Each new wave of attack saw advanced protection by PreEMPT
- Attacks caught without signatures in early hours
- Attachment Manager catches, blocking dangerous executables
- Anti-virus heuristic catches included
 - MIME anomalies
 - Compression characteristics
- PreEMPT layers work together to provide complete protection

Have a question? Submit it via the WebEx chat window to Barry Schmell

Postini anti-virus protection enhancements



- Attachment Manager will open compressed/archive files and inspect the contents (Q2 2007 delivery)
- Early Detection Quarantine will identify suspicious email and quarantine it for a specific period of time (Q2/Q3 delivery)
 - Messages can be inspected by users and are re-scanned before forwarding
- Additional heuristics based on internet traffic patterns and on message properties (on-going)
 - Will be used by standard quarantine and early detection quarantine



Polling Question #1

Agenda



- The threat landscape
- Solution overview
- Best practices
- Summary and Q&A
 - Submit questions on-line via WebEx chat window, addressed to Barry Schmell

The Basics



- Update DNS MX Records
 - Starts mail flow through Postini
- Add Users
 - Starts filtering of user email messages
- Secure firewall
 - Limit Port 25 to Postini IP Addresses and any other significant IP Addresses
 - IP address range is identified in the Administration Guide

Recommended Settings



- Virus Blocking
 - Non-account Virus Blocking – On
 - Virus Cleaning – Off (not relevant today)
 - Virus Fragmenting - On
 - Virus Disposition – Delete
- General Settings
 - Non-account Bouncing – On (After adding all users)
- User Access to the Message Center
 - Virus Settings - None
- Default User Settings
 - Virus blocking – Enabled and Organization Default

Virus Protection Settings

Have a question? Submit it via the
WebEx chat window to Barry Schmall

Recommended Settings continued

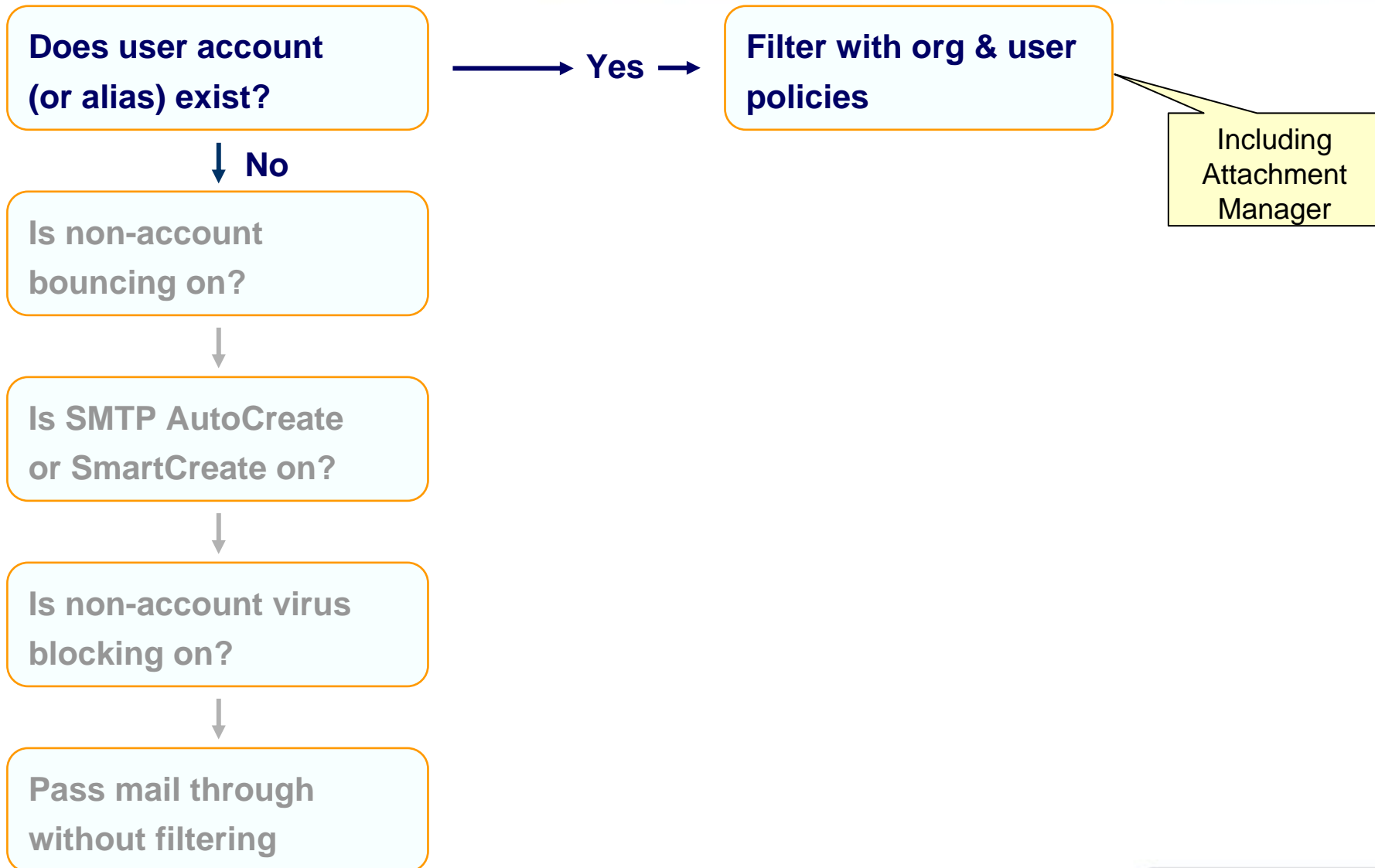


- Attachment Manager
 - System Threats should include:
 - Executables: exe, ini, ins, iw, class, js, scr, vbs, com, pif
 - Compressed: hex, hqx, sea, sit, tar, zip, zoo, lzh, bz, bz2, gz, tgz
 - To meet Service Level Agreements
 - Bounce is recommended disposition
 - To meet your business requirements
 - Quarantine is recommended disposition
 - Consider Quarantine Redirect rather than User Quarantine
- Notifications
 - Enable Attachment Manager Inbound notifications
 - Send to User, Quarantine Redirect, Or Both

Attachment Manager Settings

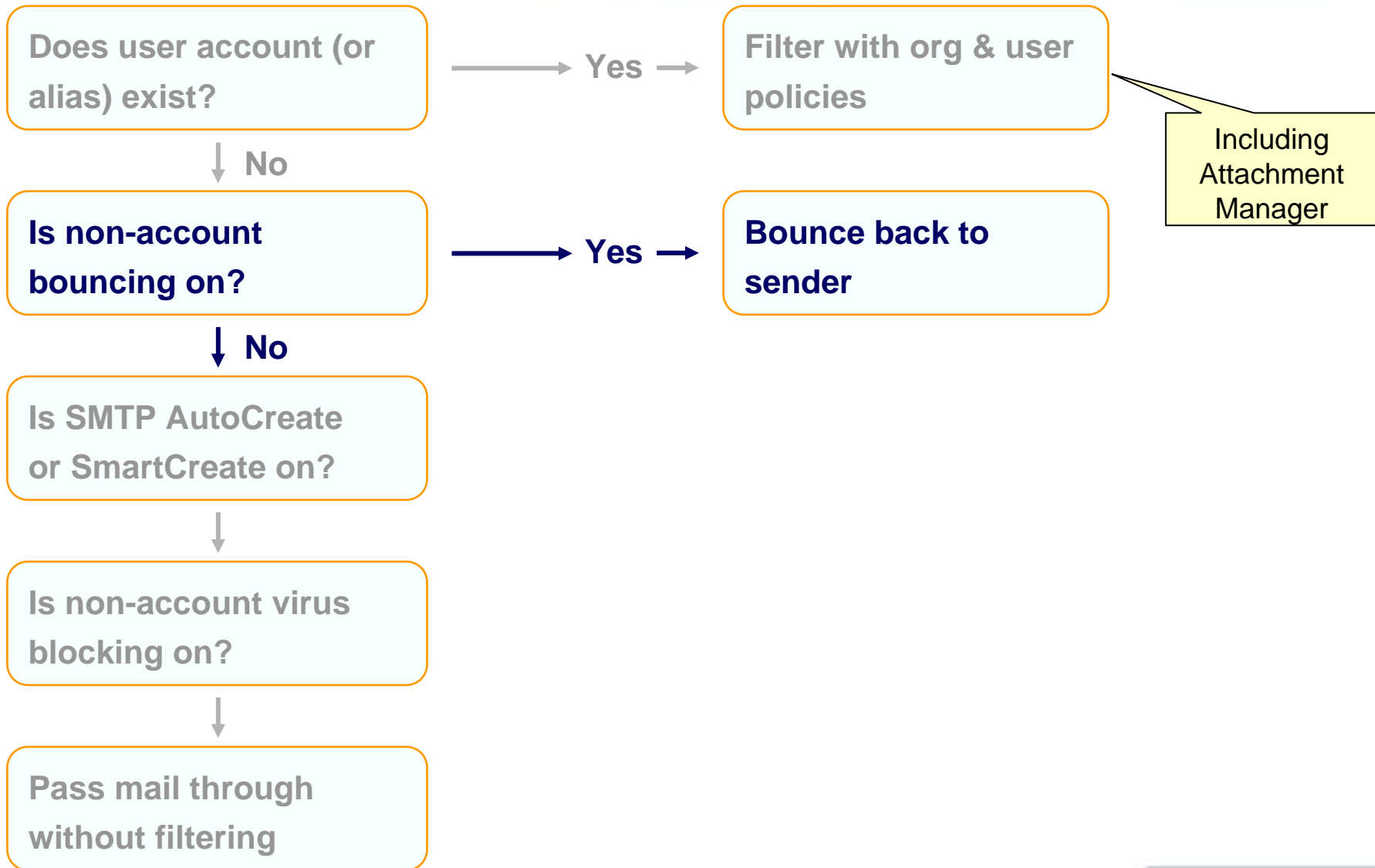
Have a question? Submit it via the
WebEx chat window to Barry Schmall

User Validation



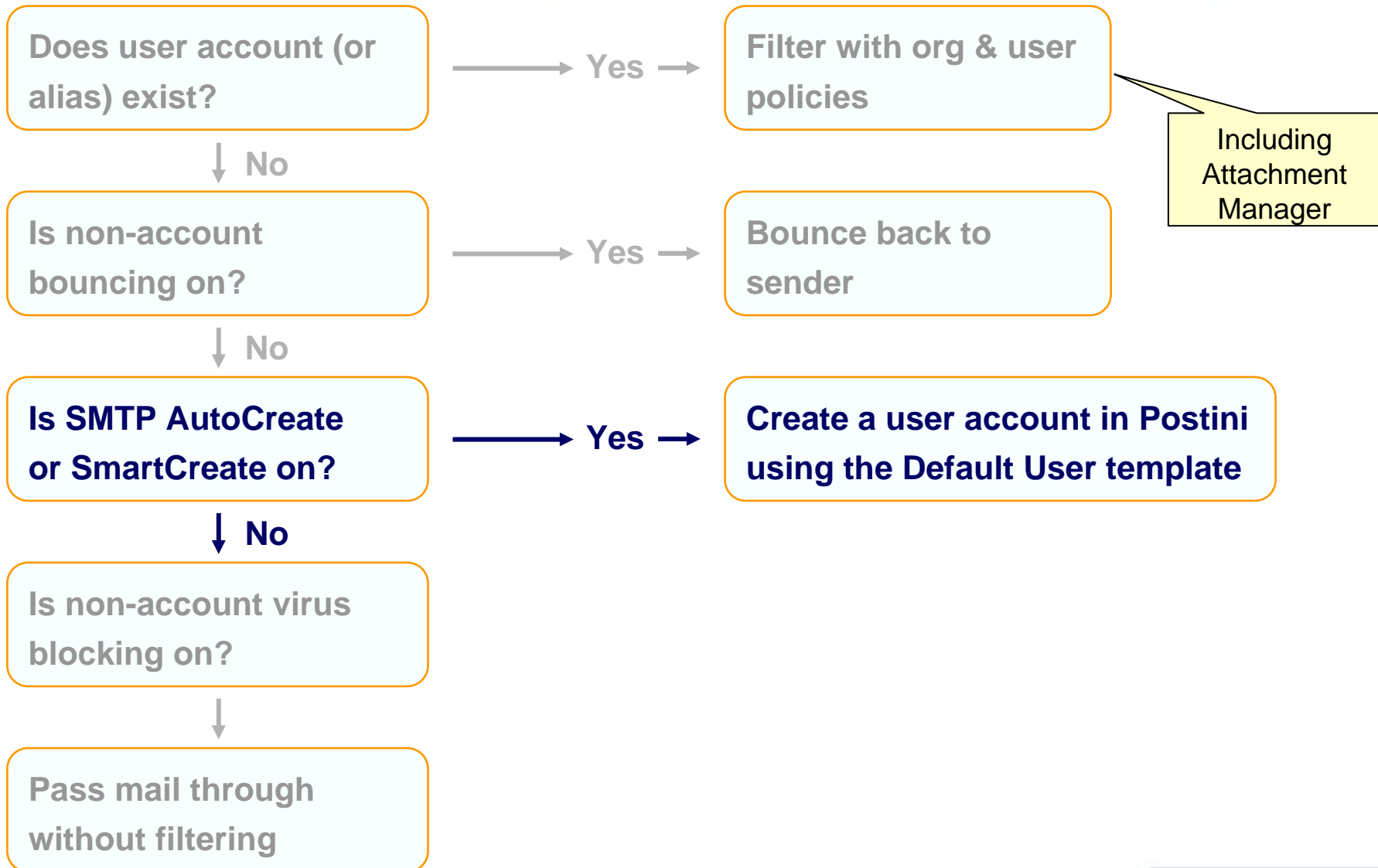
Have a question? Submit it via the WebEx chat window to Barry Schmell

User Validation



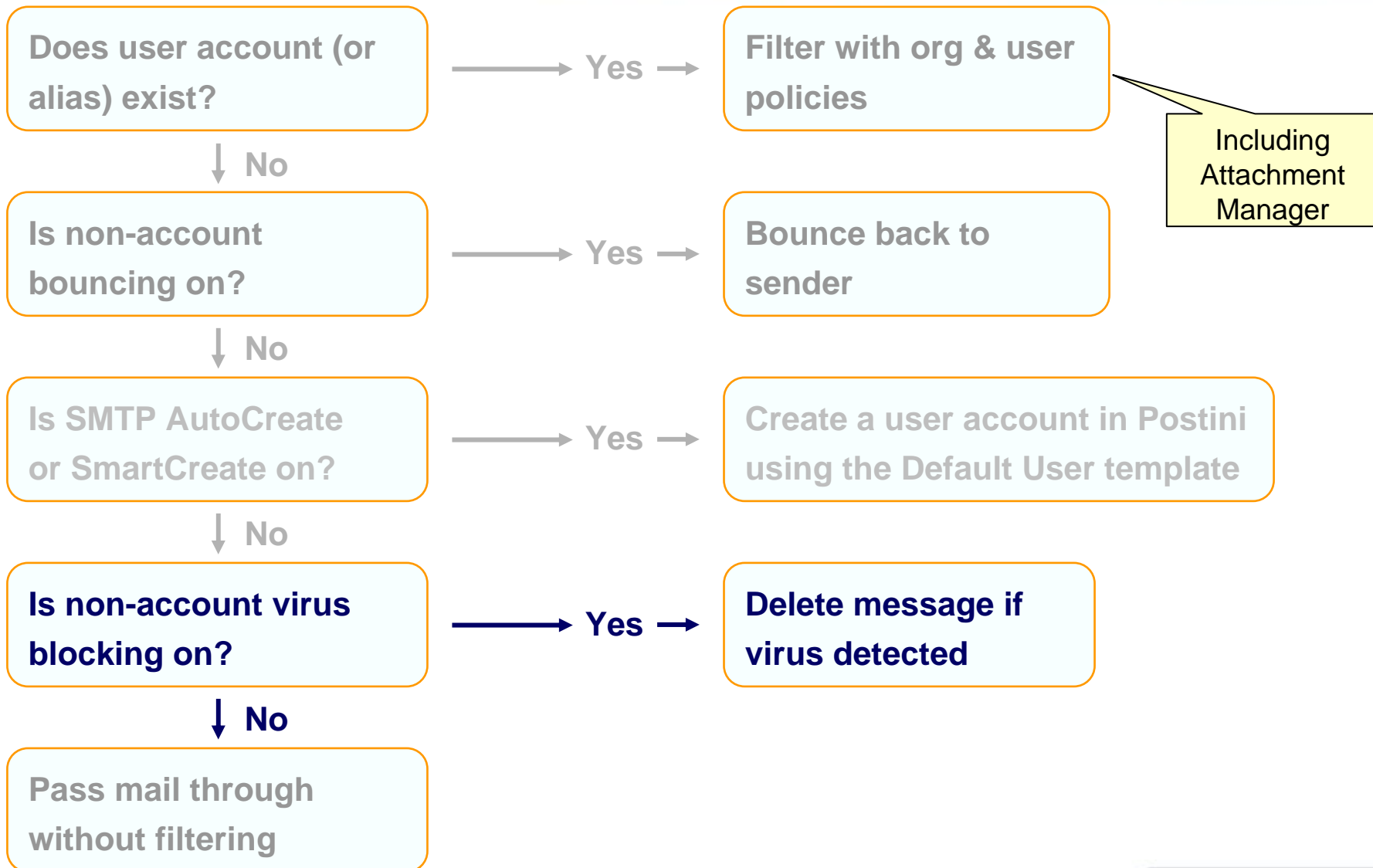
Have a question? Submit it via the WebEx chat window to Barry Schmell

User Validation



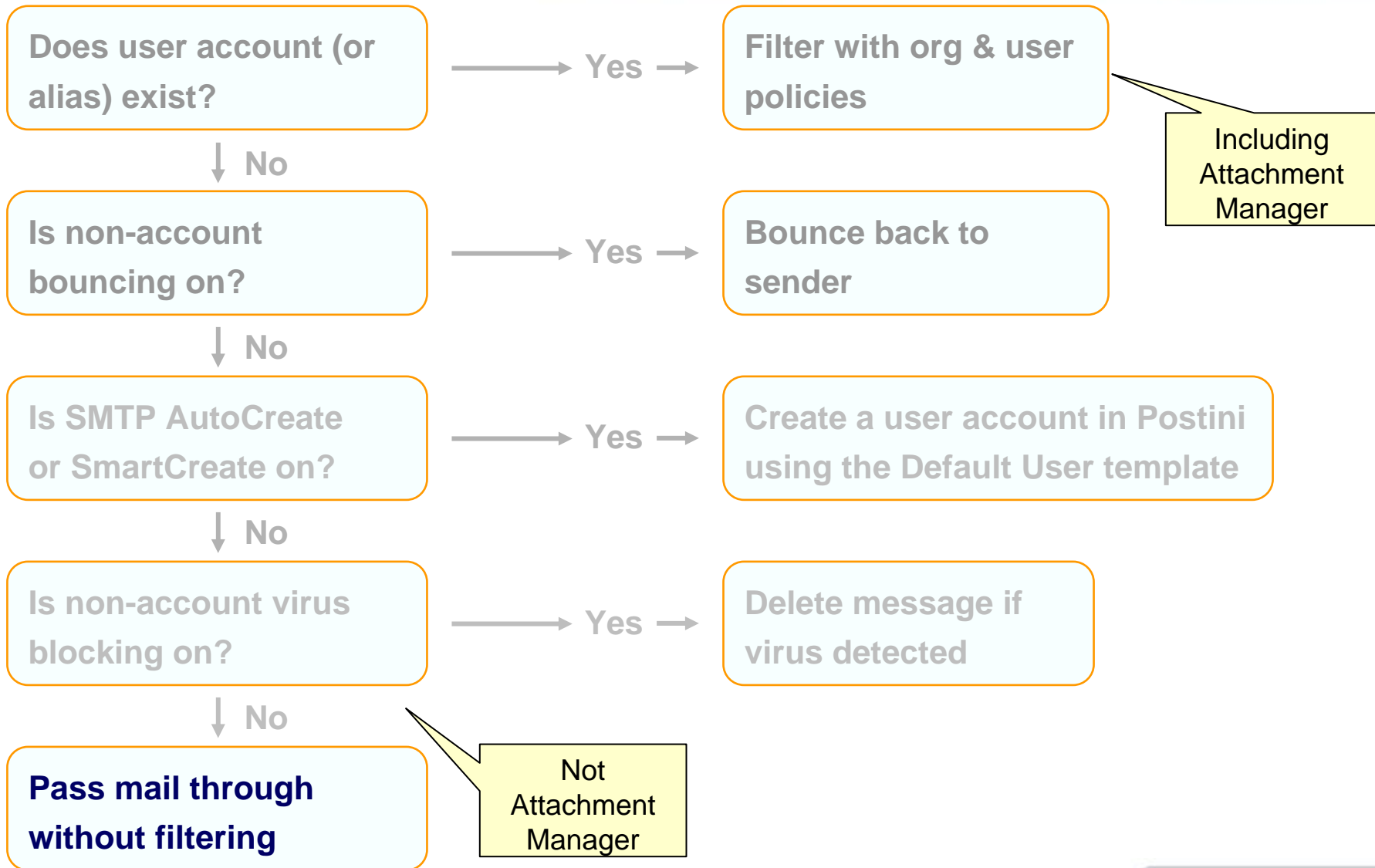
Have a question? Submit it via the WebEx chat window to Barry Schmell

User Validation



Have a question? Submit it via the WebEx chat window to Barry Schmell

User Validation



Have a question? Submit it via the WebEx chat window to Barry Schmell

Best Practices



- **Configure Email Server Config settings**
 - Connection Manager server protections
 - Enable Virus Outbreak protection, in addition to other attack protections
 - No need to configure Alerts for Virus Outbreak
- **Lock down firewall**
 - Limit access to port 25
- **Add users, user aliases, and mailing lists**
 - Default User spam filtering and virus settings
 - Non-account bouncing
 - Methodologies to manage users
- **Consider Directory Sync and enable Non-account bouncing**

Protect server and add users

Commonly Overlooked



- Adding additional domains and domain aliases
 - Update DNS MX records, as well

- Locking down the firewall

- Postini provides “Front-End” virus protection
- Don’t forget the “Side-Door” and “Back-Door”
 - Your corporate servers
 - Employee desktops
 - Employee laptops
 - Portable devices – travel, removable disks, downloads...
 - Instant Messaging sessions (Postini Instant Message Security)
 - Web surfing (Postini Web Security)



Polling Question #2

Summary

- Virus attacks are increasing in volume and sophistication
- Attacks are increasingly coming through web and instant messages
- Postini services are unmatched and we are continually investing to improve them
- Clients should leverage best practices and review them on a frequent basis
- Resources and information available at the Support Portal
- For more information on instant messaging and web security solutions, attend next week's webinar or call 888-584-3150



Q & A



Joining our panel for Q&A:

- Adam Dawes, Director of Product Management
- Kevin Lund, Principal Systems Architect

Submit questions on-line via WebEx chat window,
addressed to [Barry Schmell](#)



How Postini is Helping You Defend Against Virus Attacks