ON SCANNING THE INTERNET
OR....
THE CURSE OF IN-THE-CLOUD URL SCANNING

CATALIN COSOI
Head of Online Threats

bitdefender

What Urls Am I Talking About?

Phishing

- Social Media Accounts
- Online Gaming Accounts
- WebMail Accounts
- Financial Institutions

Fraudulent Websites

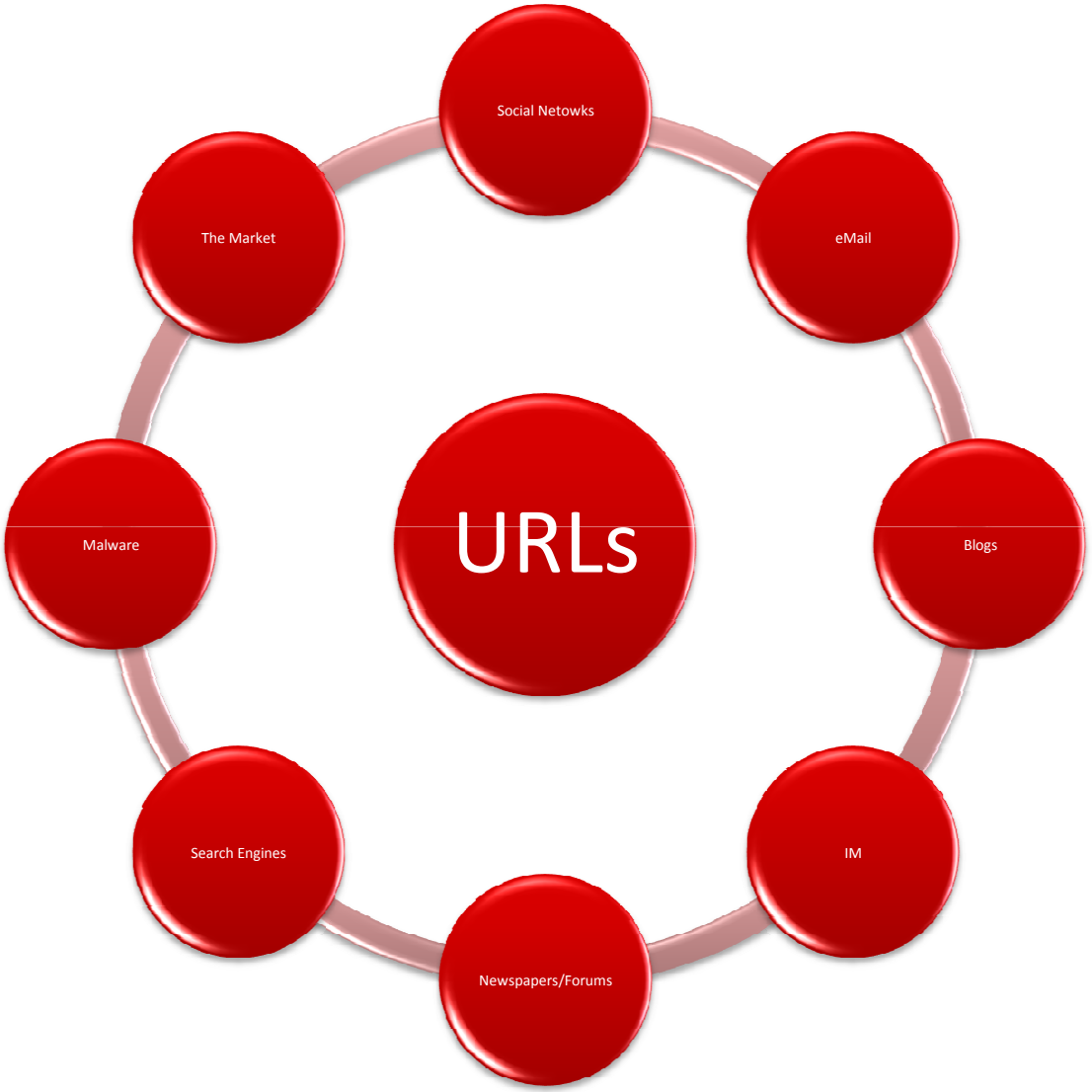
- Fake Mortgage Websites
- Fake shipping Websites
- Fake (cheap) pills
- …. Actually all scams go here

Malware

- Old school Malware
- Fake AVS
- etc

bitdefender

Where Do Urls Come From?



bitdefender

Contents

- Short intro into the cloud
- Pros and Cons of cloud computing
- And some more pros and cons
- Some of our stories
- Obviously, some conclusions

bitdefender

What is the Cloud? Where is the Cloud?

- Cloud Computing in the security industry has multiple definitions and several approaches.
- Security in the cloud means:
  - URL scanning
  - AV scanning
  - Spam scanning
  - RBL
  - And more

bitdefender

Current Status of the Cloud Paradigm

- Pro Cloud
- Against Cloud
- A hybrid approach is better

bitdefender

Why Should We Go for it? (the Strenghts)

- No versioning (no large product updates)
- Low resource consumption
- Higher speed
- Not OS dependant
- Not hardware dependant
- Instant access to updates
- New technologies available like outbreak detection or statistics based algorithms
- Sometimes…. It is also cheaper

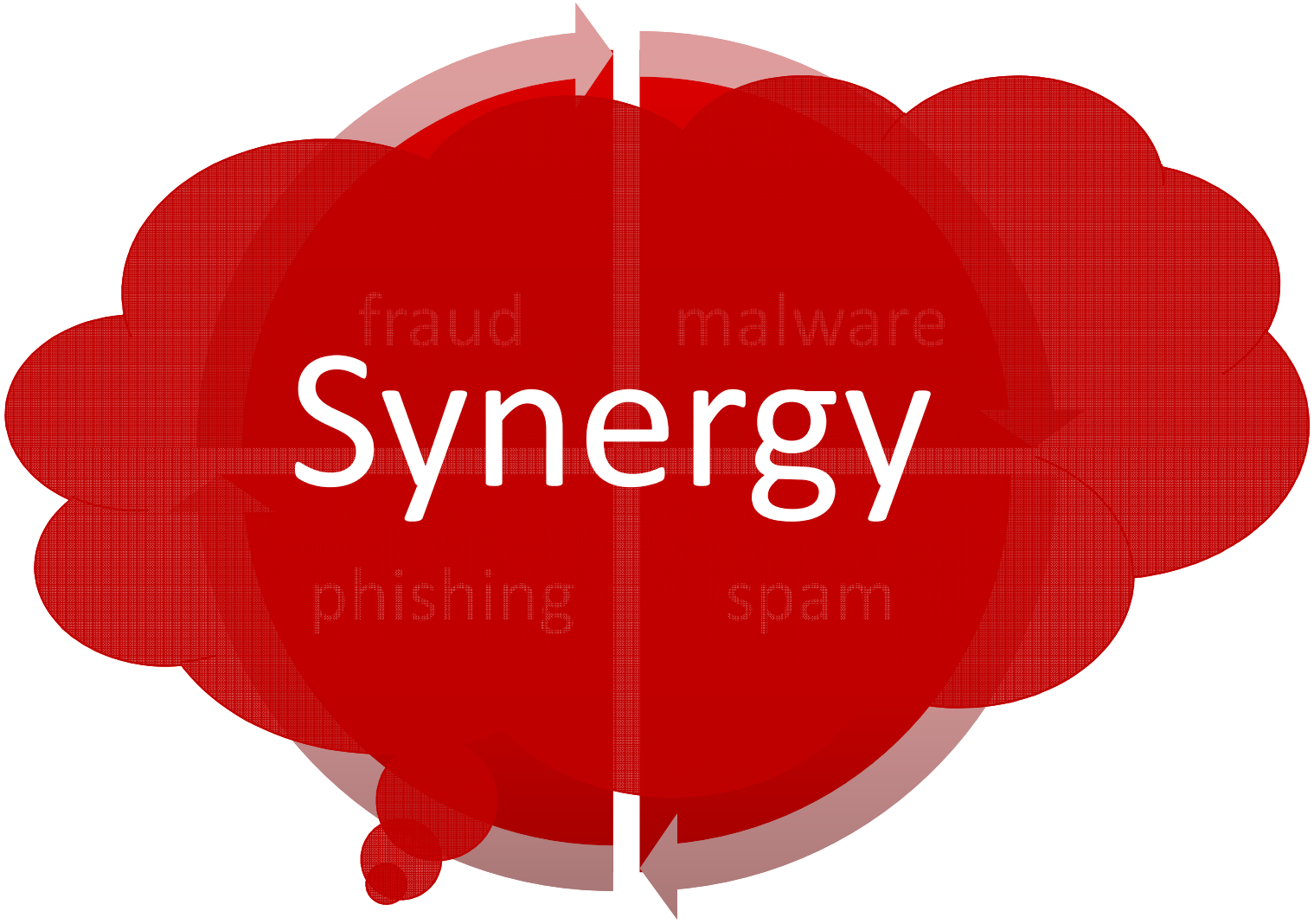
bitdefender

Why We Shouldn't? (the Weaknesses)

- No internet connection means no cloud
- Susceptible to DDOS attacks
- Resource Consumption just moved in the cloud. It didn't vanished!
- Connection spikes can cause false negatives (or, even DDOS->self)
- Instant updates can also mean instant faulty updates
- Data center failure means no detection (the cleaning lady effect)

bitdefender

So What Does Exactly Cloud Offer Me?



bitdefender

What Else Can Cloud Offer?

- Opens the door to a new set of
  - Applications
  - Devices
  - Operating systems

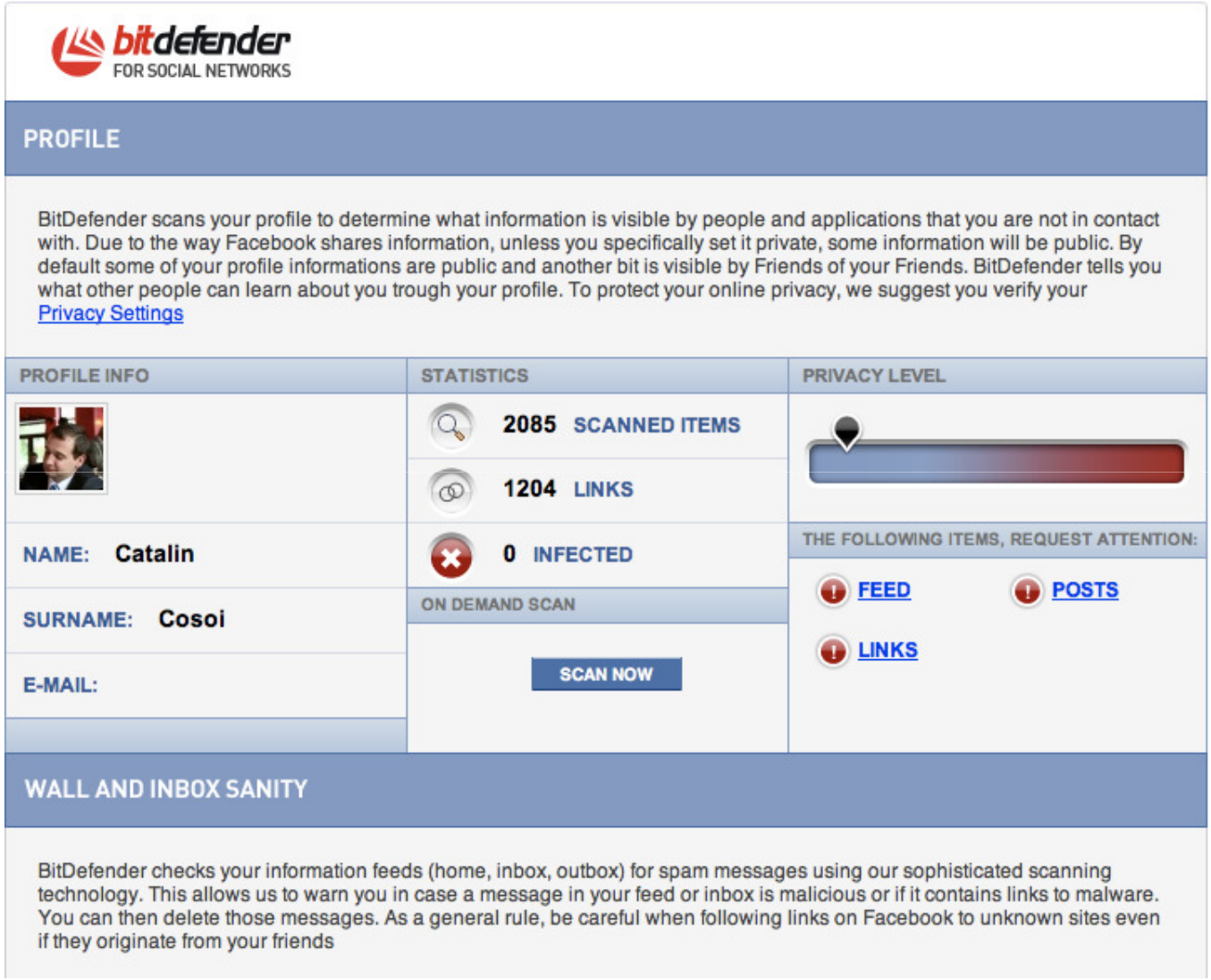
bitdefender

saf.li

bitdefender

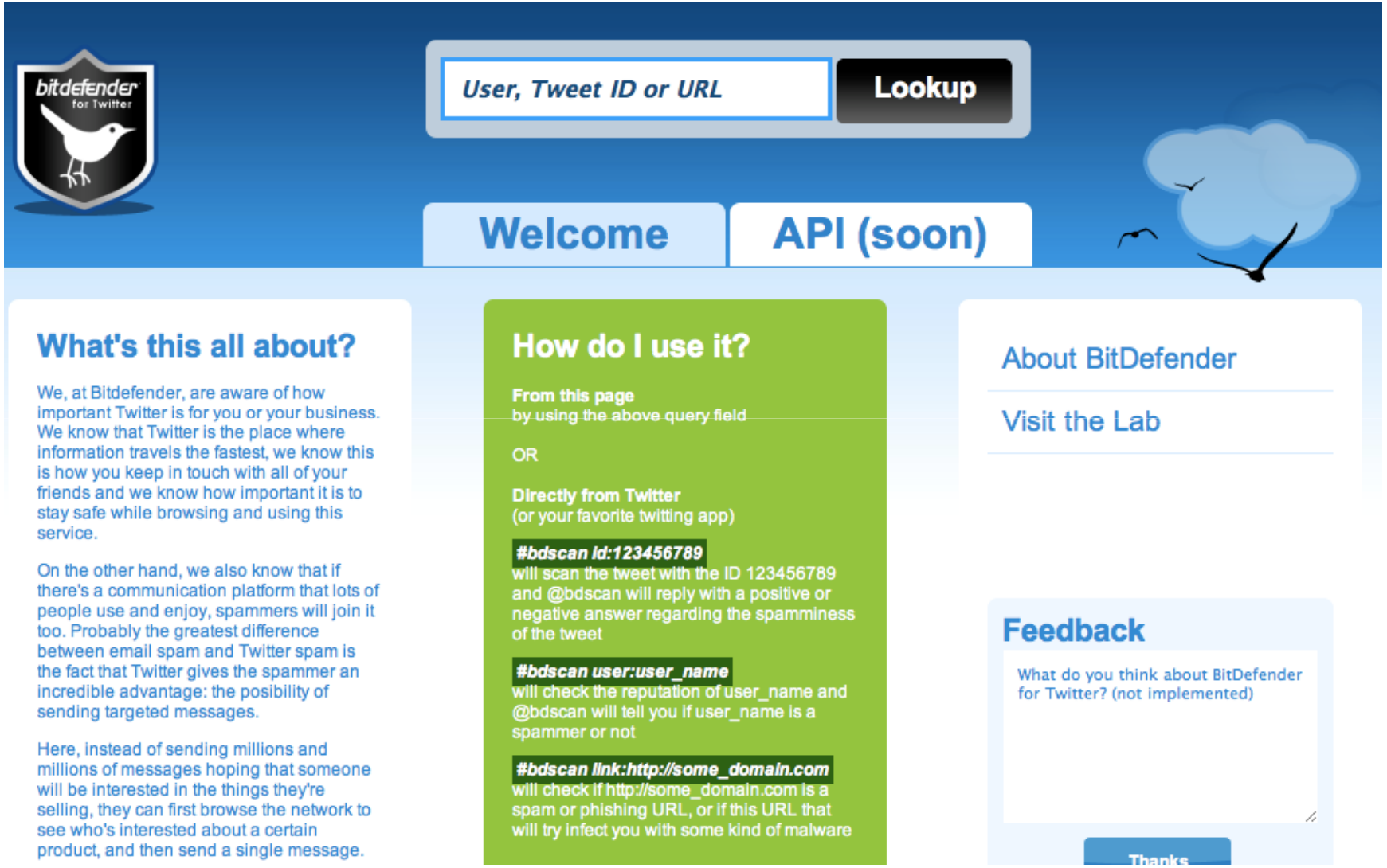
Provide Help For the Bloggers (WP Users and More)

Offer Support to Facebook Users



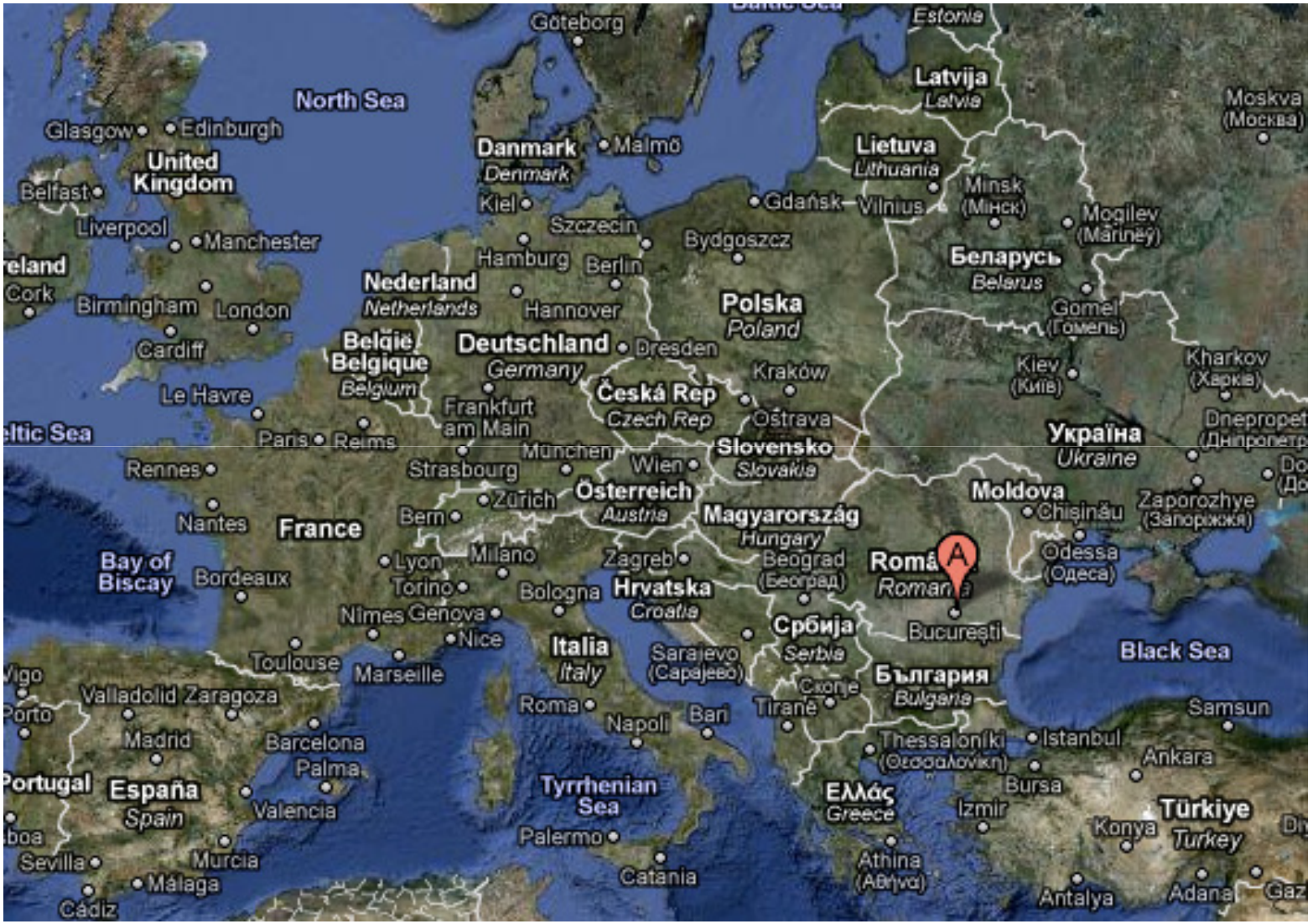
bitdefender

Assist Twitter Users



bitdefender

geoIP Based Attacks



bitdefender

You Have to Login First!

- HTTPS webpages
- Sites where you have to login
- Sites that require user interaction

bitdefender

Size Does Matter!

- Several sources of URLs means an extremely large number of URLs
- Several clients that query the cloud means a massive number of links that have to be analyzed
- Links have various statuses (clean, infected, phishing, fraud) which change dynamically
- So, one has to move fast…

bitdefender

Lies, Damned Lies and Statistics

- Targeted attacks stay under the
- Slow spreading malware too

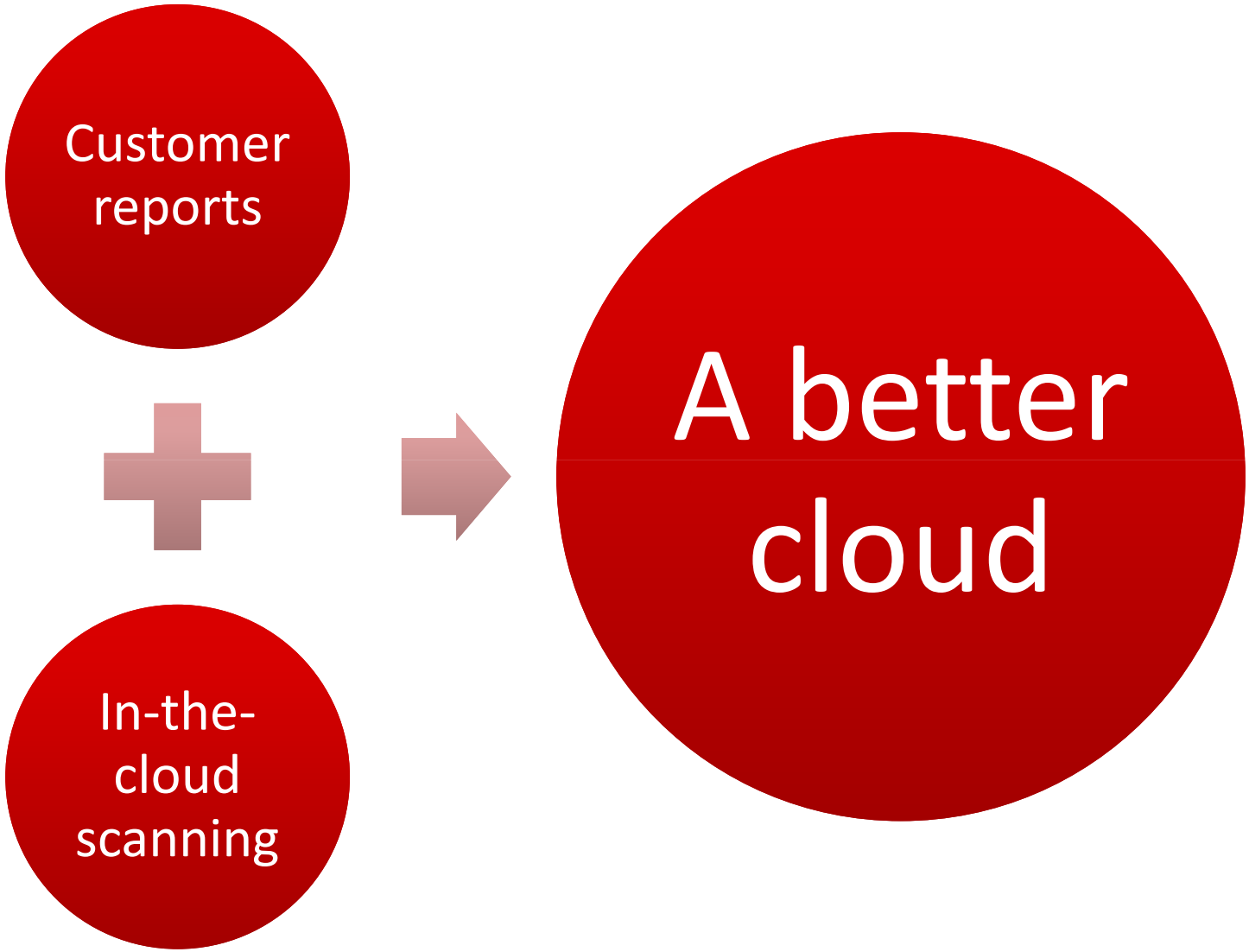
bitdefender

Not Everyone Presses the “Like” Button

- Not everybody likes us
  - Website owners
  - ISPs
  - Maybe even social networks?
  - And hopefully the bad guys

bitdefender

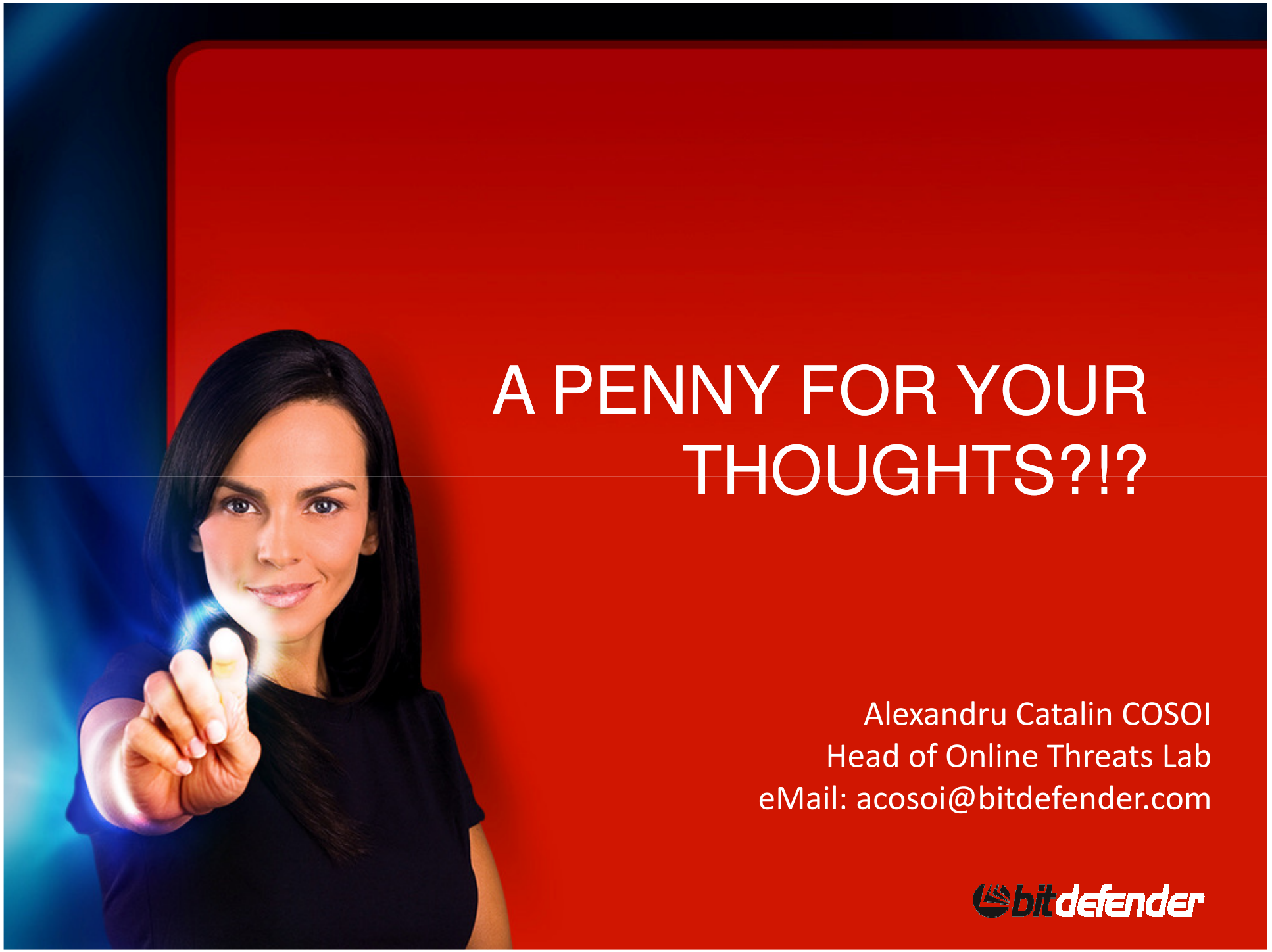
Enhancing the Cloud



Conclusions

- We believe that a hybrid approach is best
- The cloud should be used as another filtering method and not as a universal solution
- Not only there should be a hybrid approach, but also these techniques have to be interconnected
- Although it looks quite easy in theory, creating and maintaining a cloud architecture is not an easy process

bitdefender



A PENNY FOR YOUR THOUGHTS?!?

Alexandru Catalin COSOI
Head of Online Threats Lab
eMail: acosoi@bitdefender.com

bitdefender