

YAHOO!

Building Security at Scale

PRESENTED BY **Alex Stamos** | Black Hat USA 2014 | August 7, 2014

Agenda

- The Security Industry and Web Scale Problems
- Combating Security Nihilism
- What is Yahoo doing about it?

Theses

- The security industry has failed to consider the needs of scale, including diversity of user base
- A post-Snowden nihilism is affecting our industry's approach to securing users
- Enterprise security teams need to evolve to proactively gain trust

The Security Industry and Web Scale Problems

What do I mean by scale?

Amount of

- › Data
- › Systems
- › Users

Diversity of

- › Users
- › Threat Models

Who is the prototypical customer of security products?

Bank of America 

*PayPal*TM

EXTRADE[®]

Goldman
Sachs

YAHOO!

	Big Banks	Web Scale
Customers	x 10	x 10
Concurrent Users	x 10	x 10
Front-End Servers	x 10	x 10
Total Servers	x 10	x 10
Customer Value	\$100's	\$.01s
Cust Stickiness	High	Low-Medium
Meat-Space Identity	Strong	Weak
Post-Facto Action?	Yes	Rarely

Most security companies are aiming for this



[1]



[2]

Our reality is more like this

[1] Flickr user Kevin Gebhart [CC BY-NC-SA 2.0](#)
[2] Flickr user Dan Buczynski [CC BY-NC-ND 2.0](#)

Things People Try to Sell Us

What they try to sell us:

What we would buy:



[1]

Super smart pizza boxes

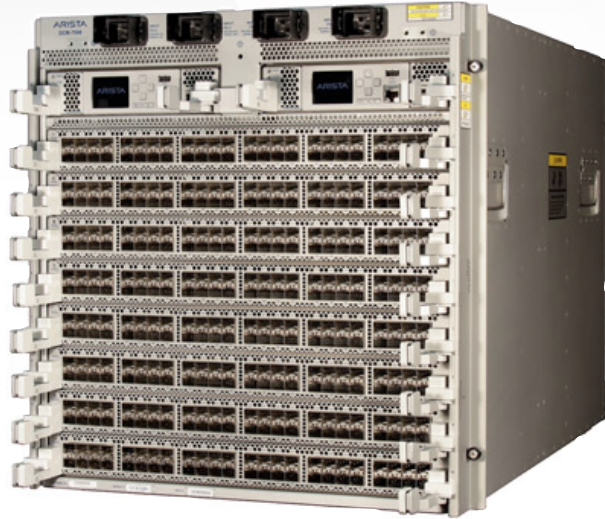


[2]

Software sensors with centralized intelligence

[1] Flickr user ms.ahr [CC BY 2.0](#)

[2] Flickr user Mike Fleming [CC BY SA 2.0](#)



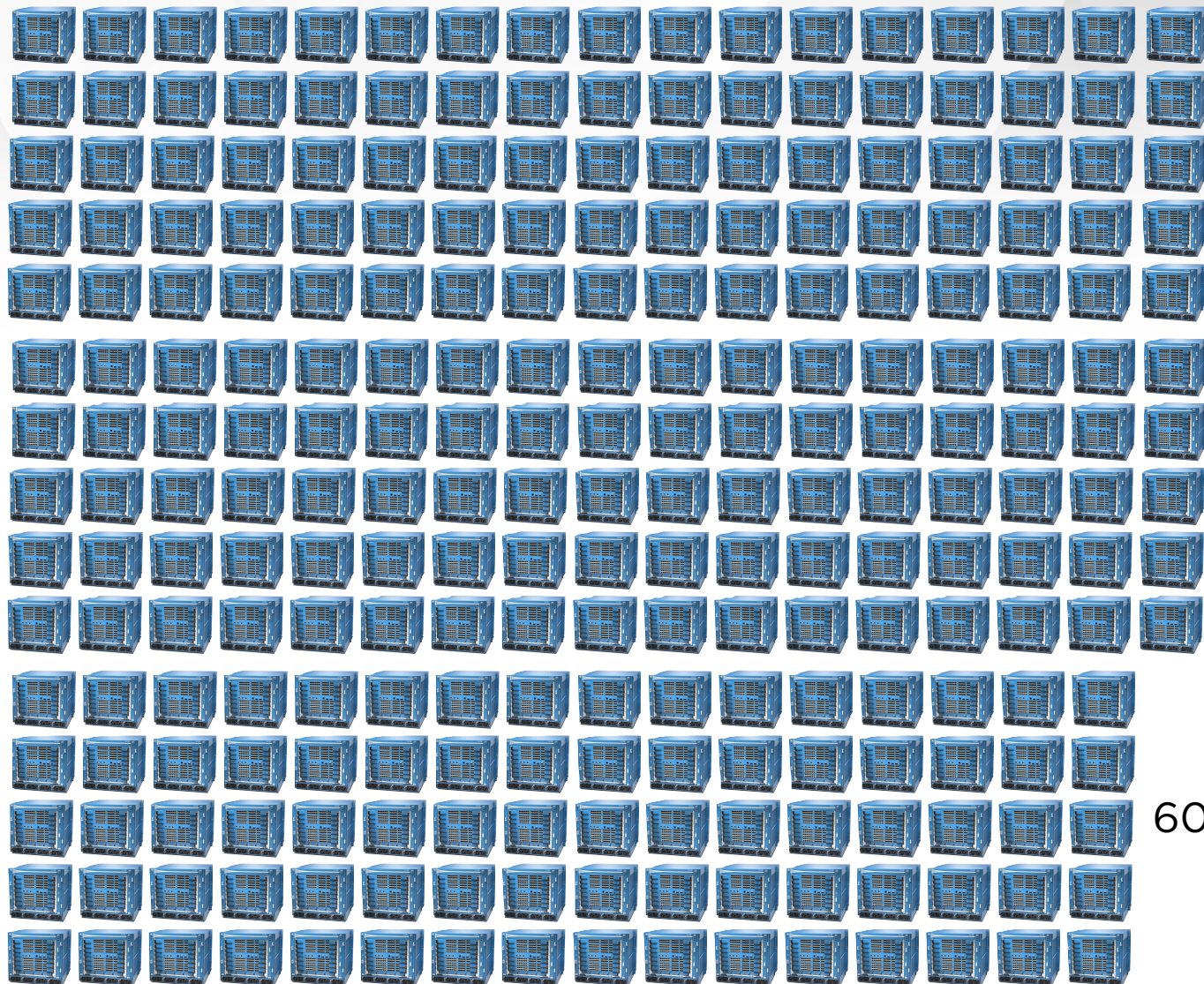
Arista 7508E
1152 x 10GbE
30Tbps backplane
5kW



Palo Alto 7050
120Gbps throughput
2.4kW



5kW



600kW

YAHOO!

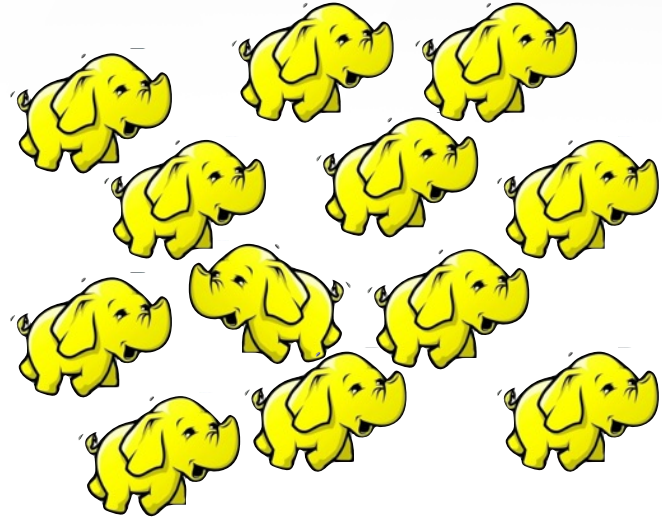
What they try to sell us:



[1]

Databased back SIEM

What we would buy:



Hadoop based
anomaly detection

[1] Flickr user Bob Mical [CC BY 2.0](#)

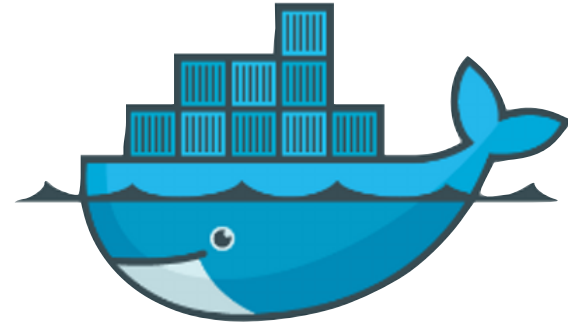
What they try to sell us:



[1]

Windows Anti-APT
Virtualization or
Kernel Firewall

What we would buy:



Docker HIDS

[1] Flickr user broterham [CC BY NC 2.0](https://creativecommons.org/licenses/by-nc/2.0/)

Free Business Ideas

- Freemium Key Management System
 - › Bootstrap via manual approval, trust in network, or remote attestation
 - › Create master cert, view into corporate key space with lazy security checks
- Freemium Overlay Network
 - › Goes great with key manager!
 - › Allow for easy IP management across public/private cloud
 - › Could be IPv6 only. Terminate inside of containers?
- Bug Bounty with Automatic Verification
 - › We're building this ourselves with Selenium

More Free Ideas

- ARM CoreOS Servers with Lightweight Remote Attestation
 - › ARM is going to be big in Big Data environments
 - › At scale building systems remotely is currently terrifying
 - › Any scale organization does not have 100% physical control
- OpenSSL with Remotable Handshake
 - › Why are we putting private keys on the most exposed systems?
 - › Need to remote the handshake to an HSM or TXT backed key server
 - › Should get 20:1 ratio

Breaking through the excuses

Security Nihilism



[1]

We believe zat nothing...
ist secure enough vor ze real world, Lebowski!

“Your system is not secure against this [advanced attack/unlikely scenario] therefore it shouldn't exist”

We need to build systems for all levels of user and adversary

“That's just security through obscurity!”

Non-obvious protections can increase the chance of catching an attacker in time, especially for interactive systems

“The [NSA/FSB/PLA] will just own up the user’s system and get the data that way”

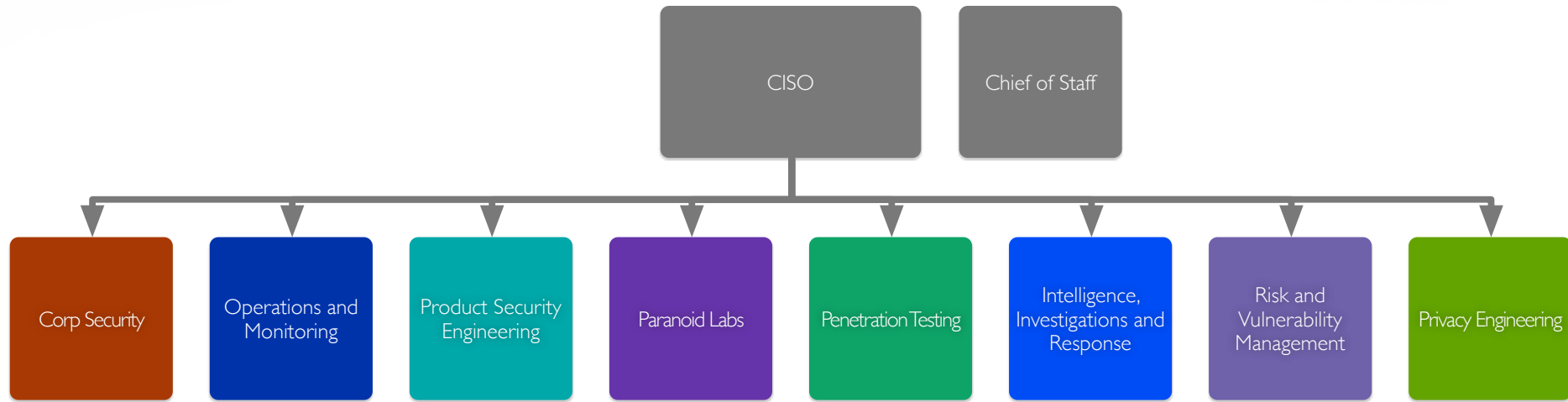
Forcing an adversary to expend resources and risk detection is a valid goal

“Users are idiots and will screw this up”

A system is only secure if it is safe, by default, for the 25th percentile user

What are we doing about it?

The New Yahoo Paranoids



New Yahoo Paranoids



Chris Rohlf



Doug DePerry



Yan Zhu

Transport Encryption

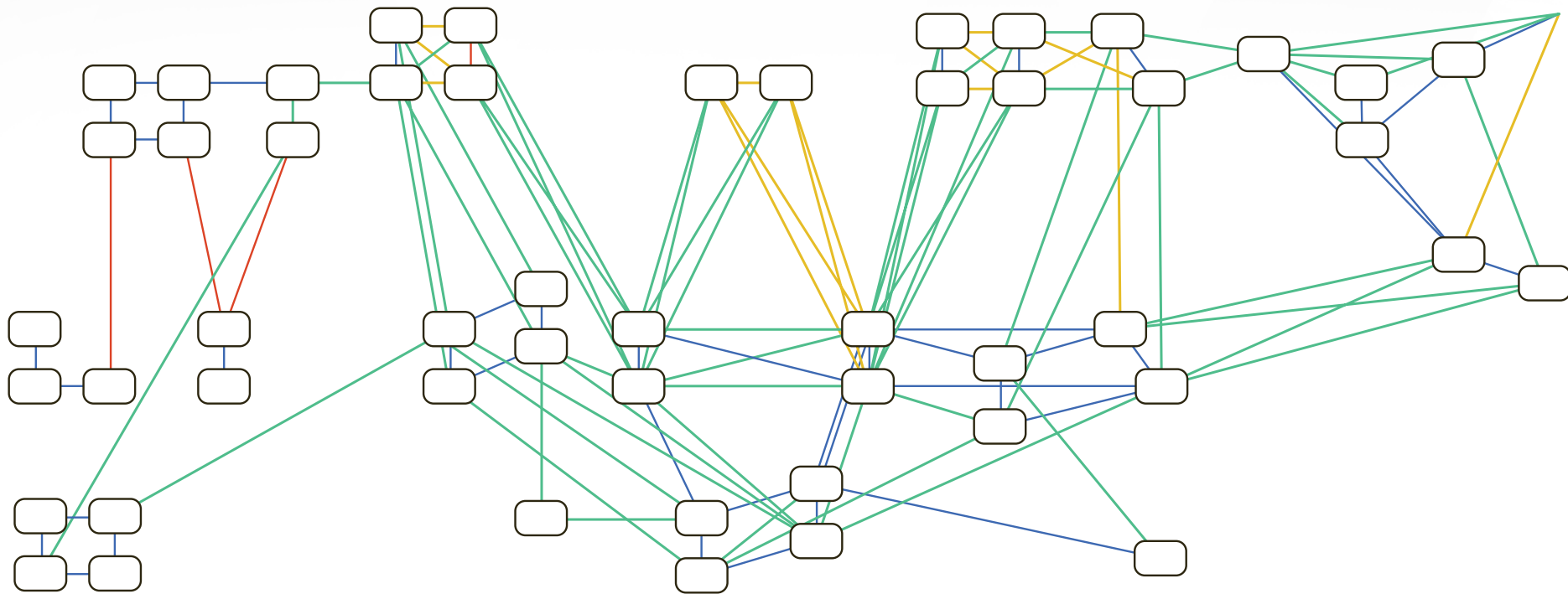
Complete

- › TLS 1.2
- › ECDH(E)
- › AES-GCM
- › RSA 2048

Next up

- › HSTS and pre-load
- › ECDSA certificates
- › Certificate Transparency
- › ChaCha20 and Poly1305
- › STARTTLS Pinning

Backbone Encryption

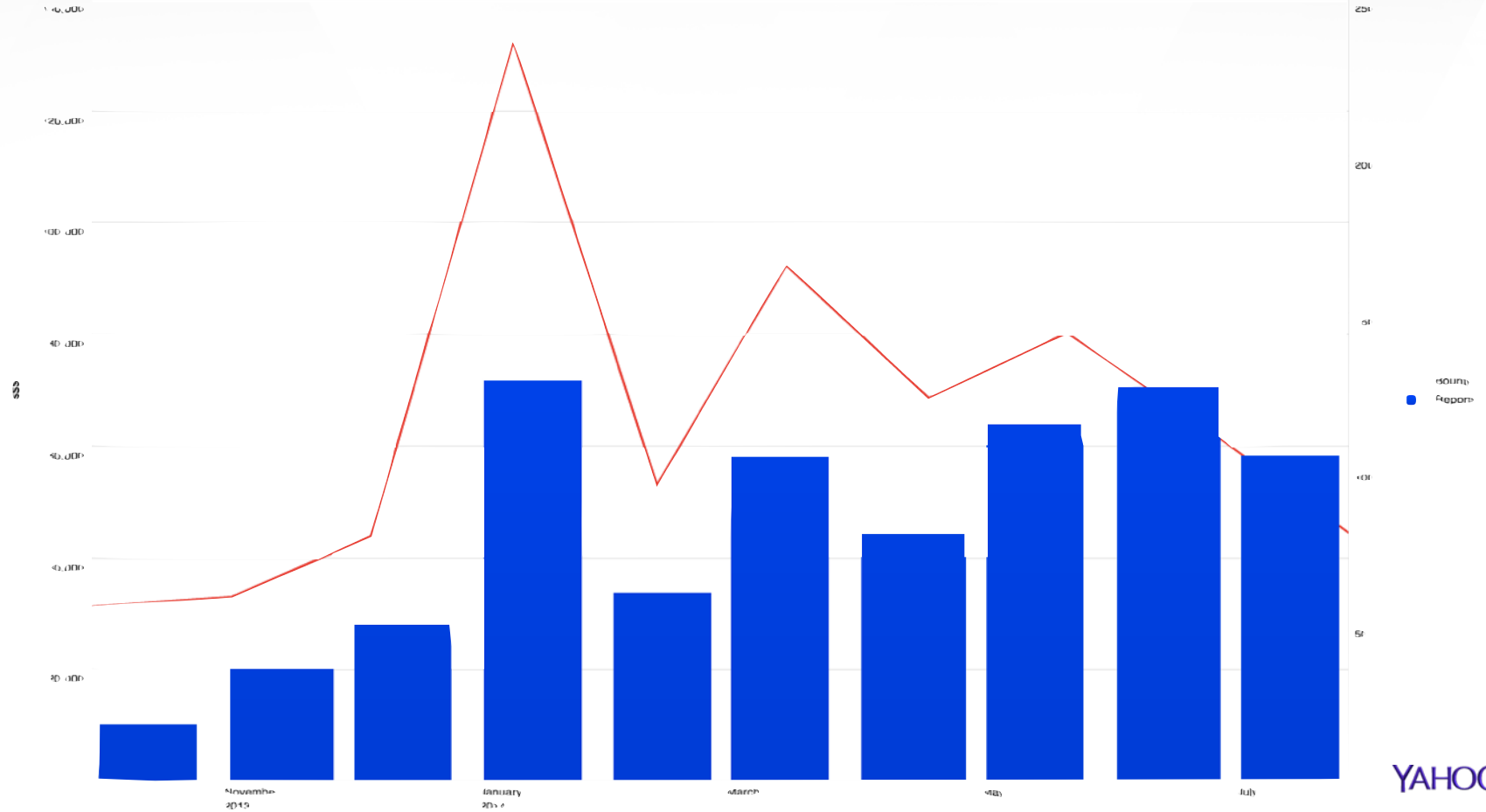


Self-Service Security

- Our scaling challenges in providing app sec services:
 - › Breadth: 80+ products in 60+ countries
 - › Speed: multiple daily web pushes and weekly mobile
- Any large org needs to create self-service options
 - › Mobile libraries
 - Authentication and device identity
 - TLS with pinning
 - › Mobile code scanning portal
 - › CI/CD Scanner integration
 - Open-source coming!

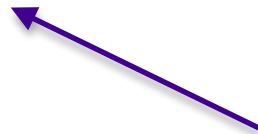
Bug Bounty

Bounty amount by month

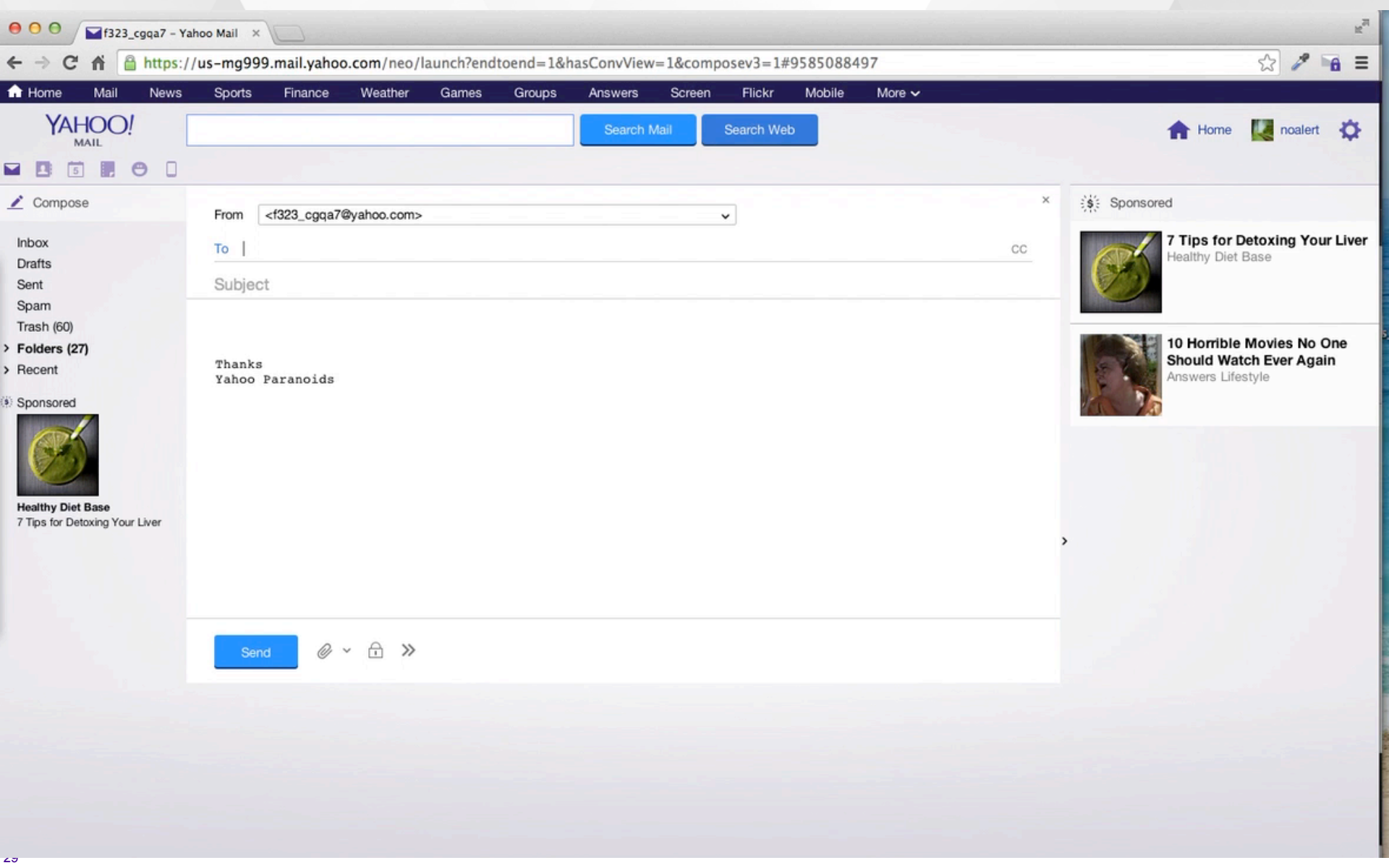


Bug Bankruptcy

- Important factors in getting bugs closed:
 - › Detailed descriptions and mitigation instructions
 - › Accurate prioritization
 - › Consistent follow-up and real-time reporting
 - › Executive visibility
 - › Convincing company that you are a madman



Works well for me




Search Mail

Search Web

- Inbox
- Drafts
- Sent
- Spam
- Trash (60)
- > Folders (27)
- > Recent

Sponsored



Healthy Diet Base
7 Tips for Detoxing Your Liver

From <f323_cgqa7@yahoo.com>

To | CC

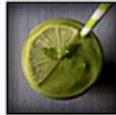
Subject

Thanks
Yahoo Paranoids


Send

Attachment, Lock, Double Arrow icons

Sponsored



7 Tips for Detoxing Your Liver
Healthy Diet Base



10 Horrible Movies No One Should Watch Ever Again
Answers Lifestyle

The Future is Bright

- Our profession has never been so impactful on...
 - › Individuals
 - › Nation-States
 - › History
- With great power...
 - › It is impossible to work in this field without being a moral actor
- Remember that trust is more than security!
- Take this opportunity to do something that you will remember with pride

Thank you

stamos@yahoo-inc.com