Application Security Tradeoffs

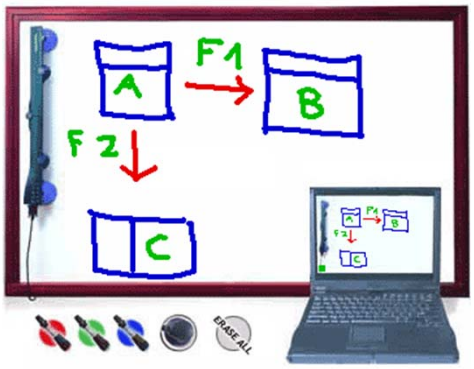
Anoop Reddy
July, 2010
Citrix Systems

OWASP

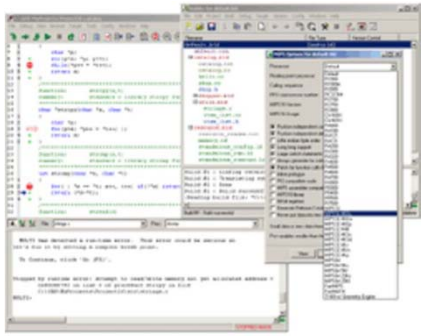
Security Tradeoff Decisions

- Explicit security tradeoffs
  -  Panel discussion at SXSW (Meebo, Facebook etc.)

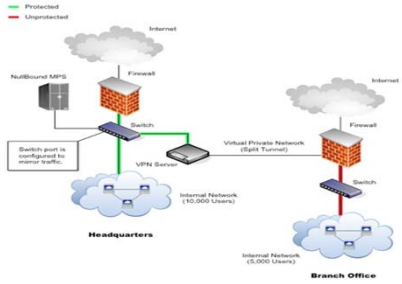
Security Tradeoffs



Design

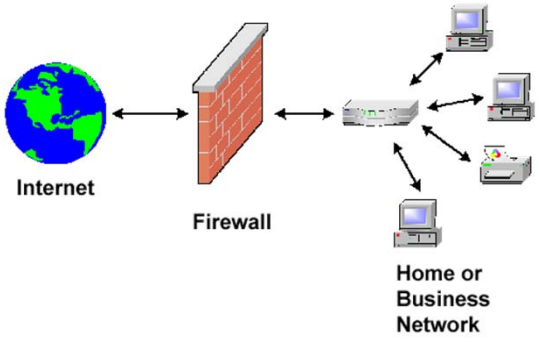


Development



Deployment

Security Deployment Technologies

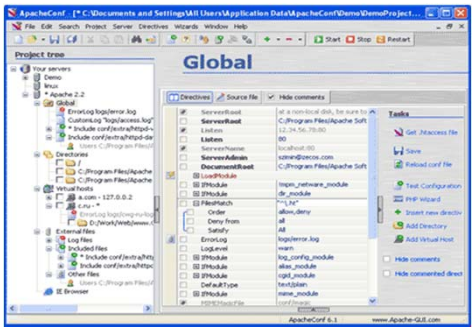


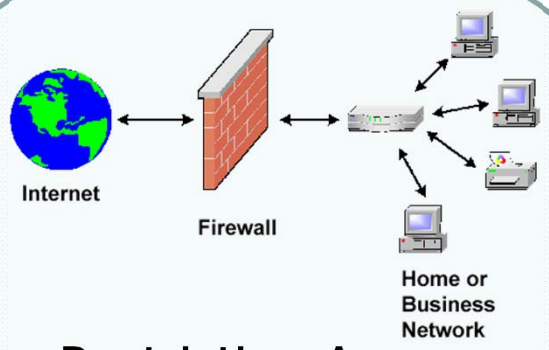
Intrusion Prevention

Web Application Firewalls

Scanning Tools

Anti-Virus





Restricting Access

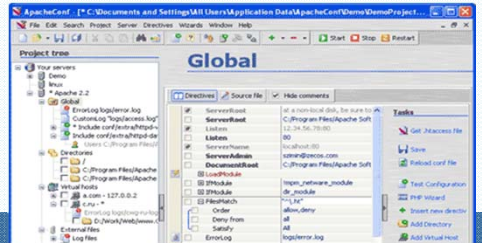
Intrusion Prevention

Active and Passive
Security Checks

Web Application
Firewalls

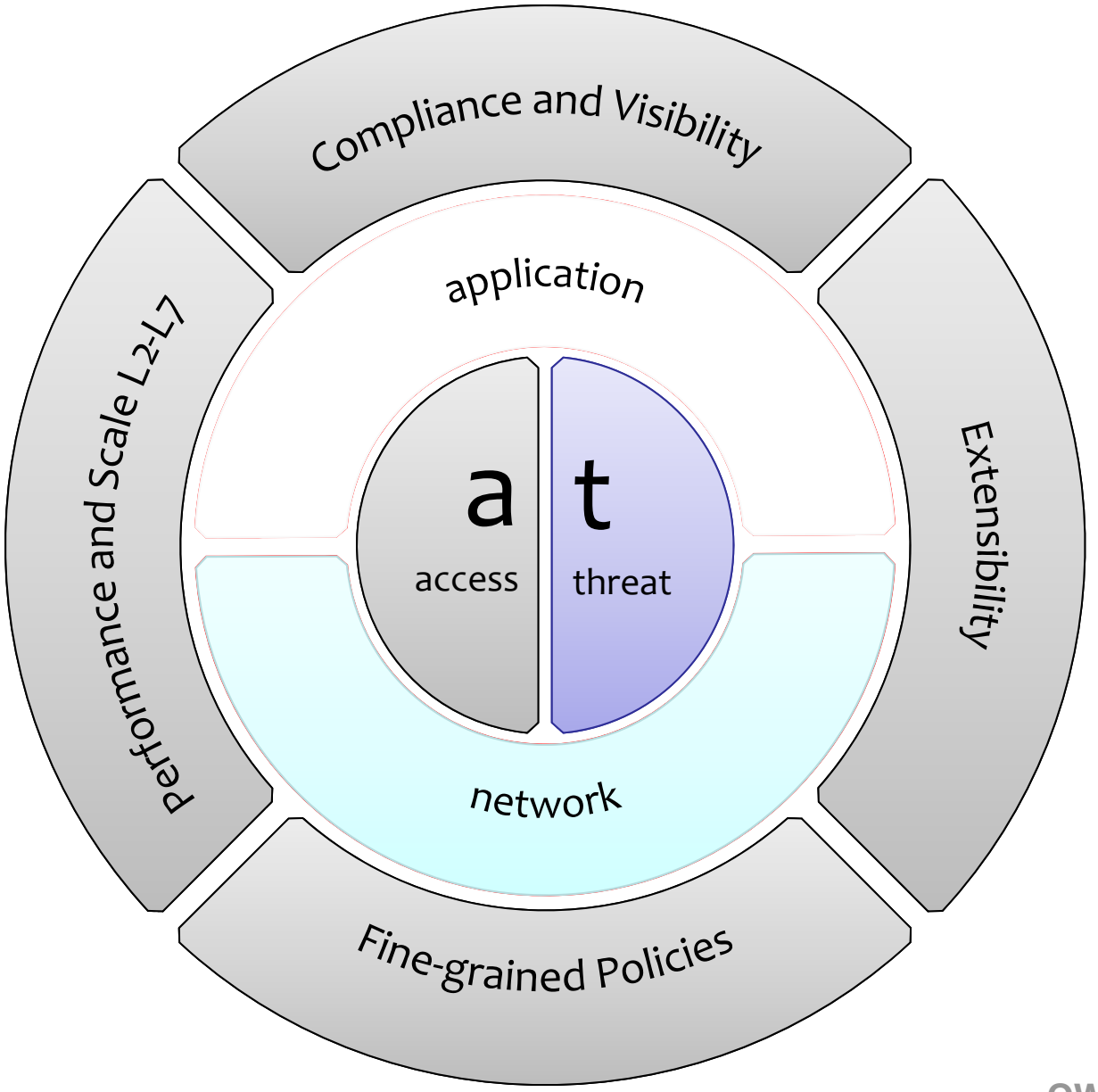
Scanning Tools

Vulnerability Assessment
and Configuration



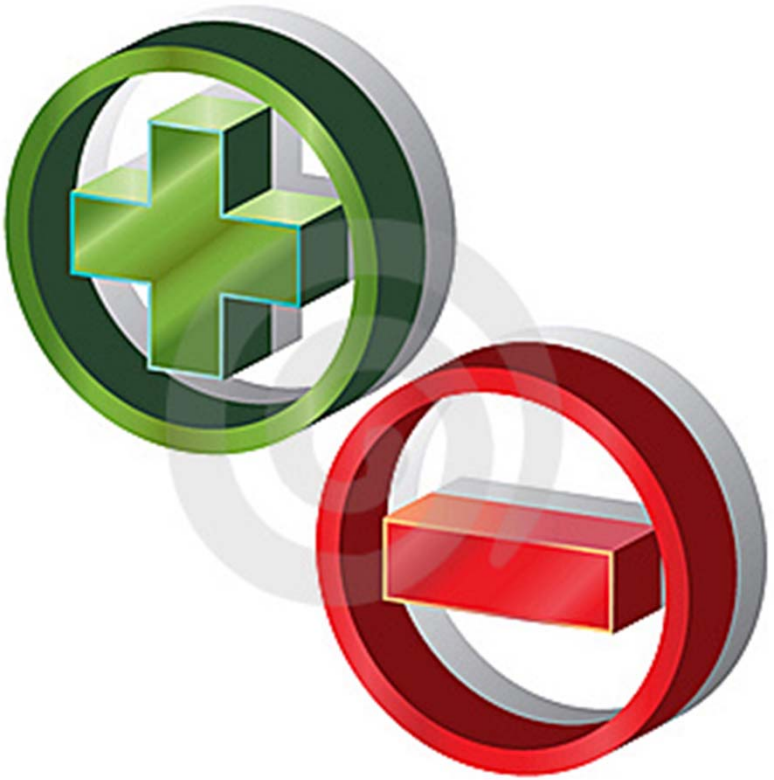
Consolidation of Security Technologies

- Does it always makes sense?


Compliance and Visibility
application
a
access
t
threat
network
Extensibility
Fine-grained Policies
performance and Scale L2-L7

Security Models

- Positive Security Model
- Negative Security Model

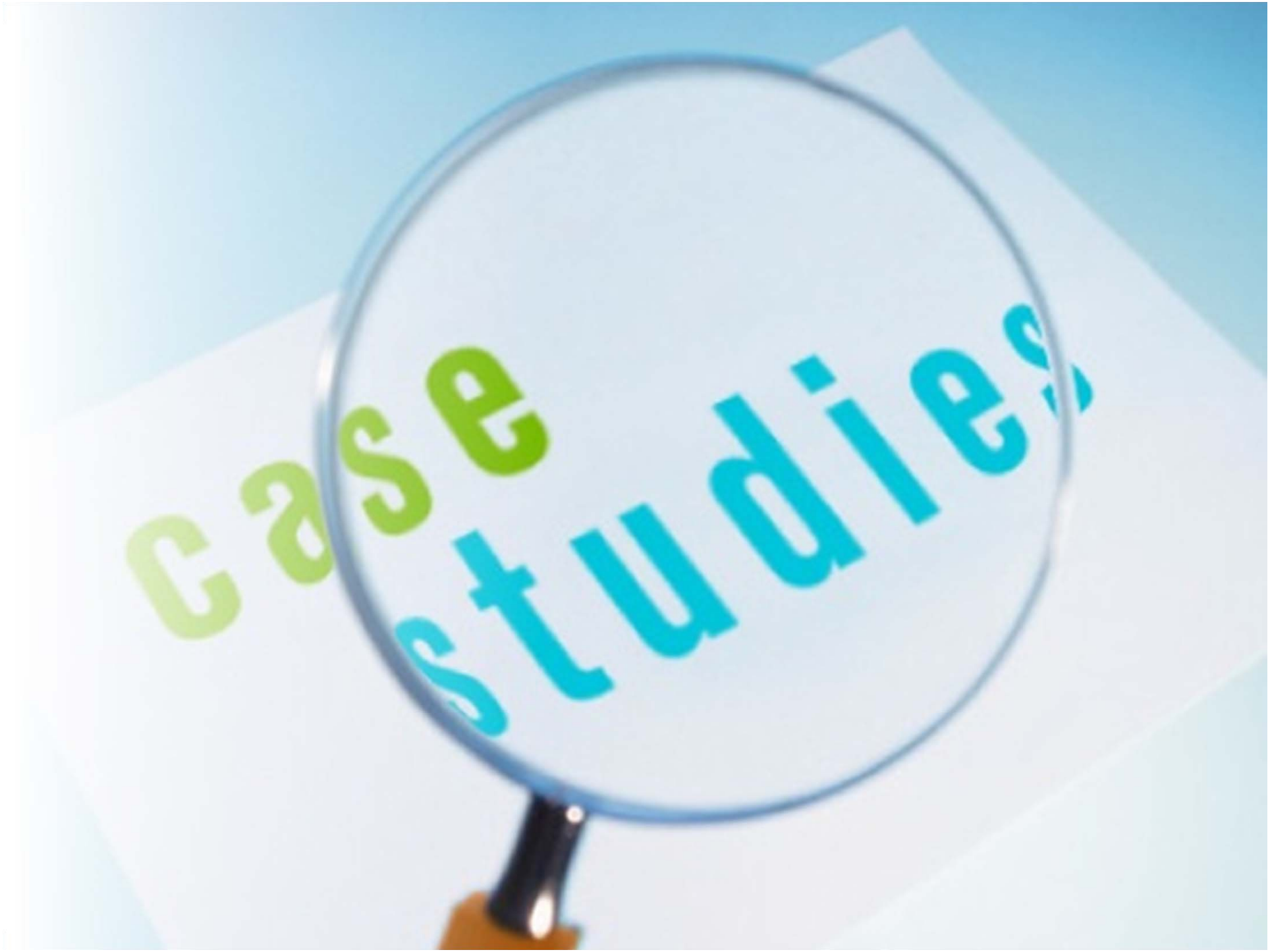


Negative Security Model

Keep the Bad

Positive Security Model

Only allow the good guys in


case
studies

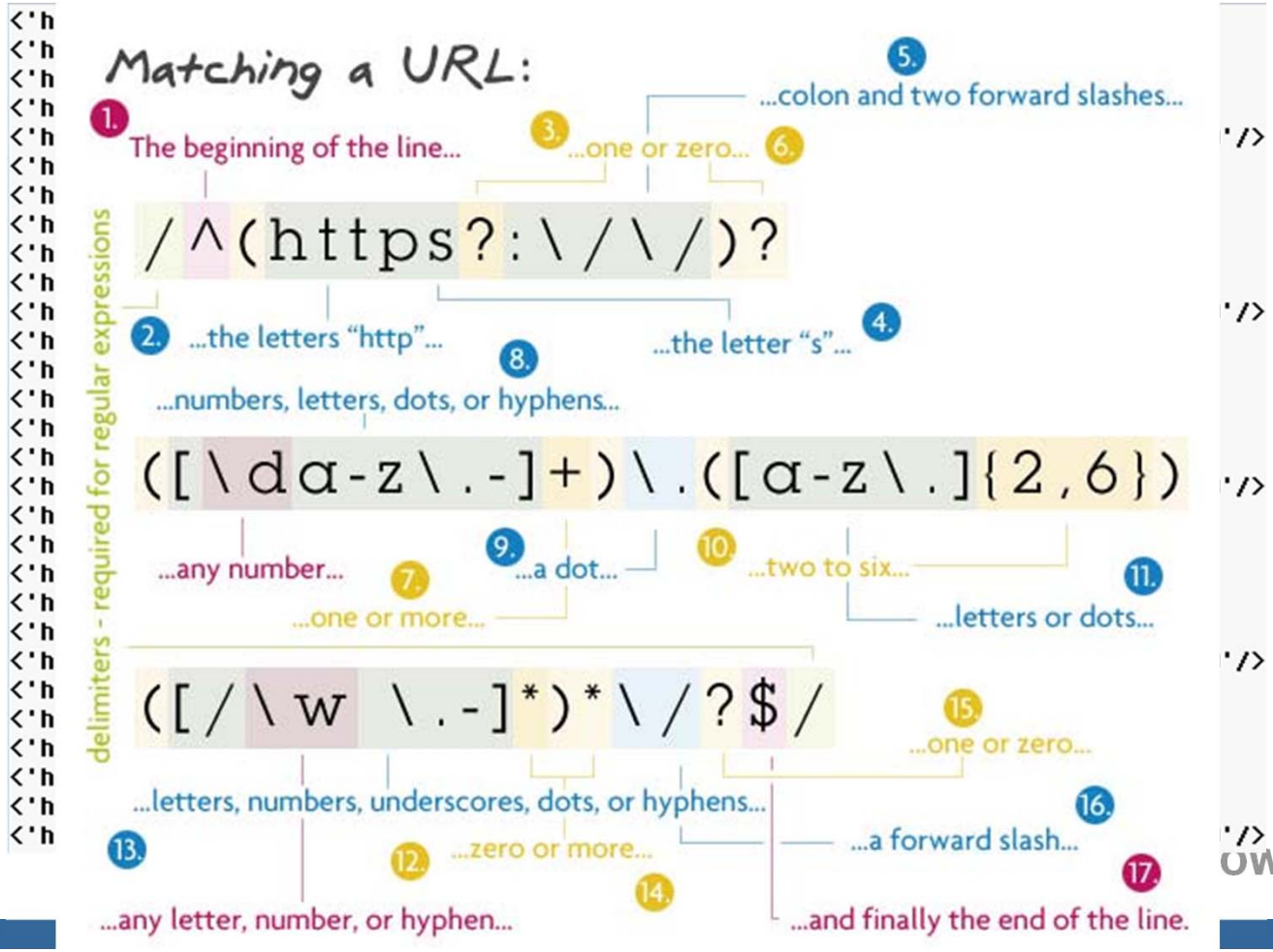
Restricting URL access

- Block known attacks in URLs
  - Attack Signatures

BLEEDING-EDGE EXPLOIT Microsoft MHTM...	any	TCP any	mhtml:file:
BLEEDING-EDGE EXPLOIT Cisco Telnet Buf...	any	TCP 23	??????????????????a~ %%%%%%XX
BLEEDING-EDGE DOS Cisco Router HTTP DoS	any	TCP 80	/%%
BLEEDING-EDGE EXPLOIT Catalyst SSH pr...	any	TCP 22	a%a%a%a%a%a%a%a%
BLEEDING-EDGE EXPLOIT Catalyst 3500 ar...	any	TCP 80	/exec/show/config
BLEEDING-EDGE EXPLOIT Cisco IOS HTTP ...	any	TCP 80	/error?/
BLEEDING-EDGE DOS Cisco 514 UDP flood ...	any	UDP 514	%%%%%%XX%%%%%%
BLEEDING-EDGE DOS Catalyst memory lea...	any	TCP 23	AAA[0A]
BLEEDING-EDGE EXPLOIT Cisco %u IDS ev...	any	TCP 80	%u002F
BLEEDING-EDGE EXPLOIT Cisco IOS HTTP ...	any	TCP 80	/TEST?/
BLEEDING-EDGE VIRUS Agobot/Phatbot In...	any	TCP any	221 Goodbye, have a good infection :).[0D 0A]
BLEEDING-EDGE P2P Phatbot Control Con...	any	TCP any	Wonk- || [00]#waste[00]
BLEEDING-EDGE DOS SSL Bomb DoS Attempt	any	TCP 443	[16 03 00] || [01] || [FF]
BLEEDING-EDGE EXPLOIT NII Microsoft AS...	any	TCP 139	[A1 05]#[03 03 01 07]
BLEEDING-EDGE Malware rcprograms	any	TCP 80	update.rcprograms.com
BLEEDING-EDGE Malware Gator Cookie	any	TCP 80	webpdpcookie || .gator.com
BLEEDING-EDGE Malware Gator Agent Traffic	any	TCP 80	User-Agent: Gator
BLEEDING-EDGE EXPLOIT CVS server heap...	any	TCP 2401	Entry aaaaaaaaaaaa

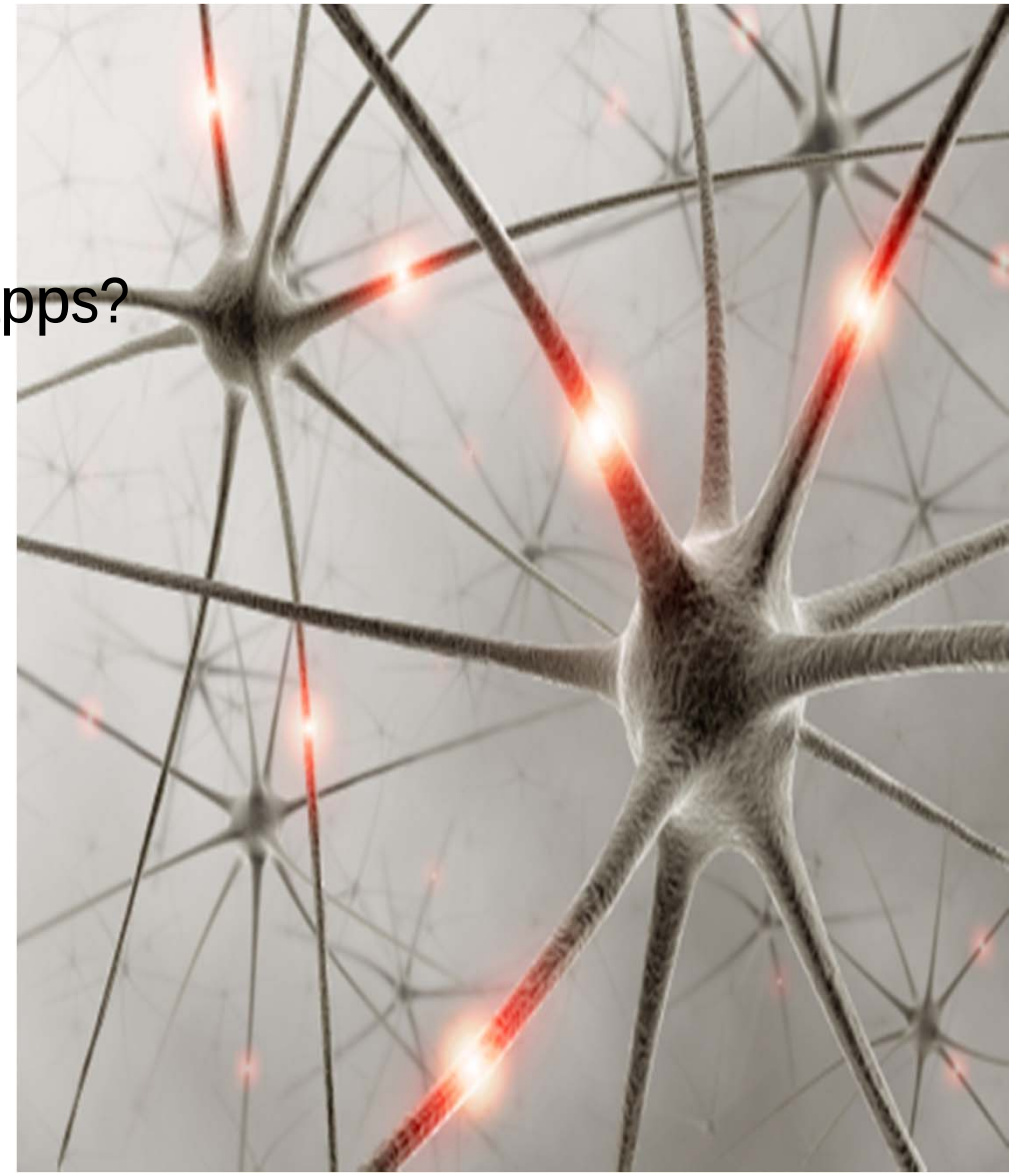
Restricting URL Access

- Only allow configured URLs



Ease Management by Learning

- Static Learning
  - Training data
  - What about evolving apps?
- Adaptive Learning
  - Always learn
  - User customized

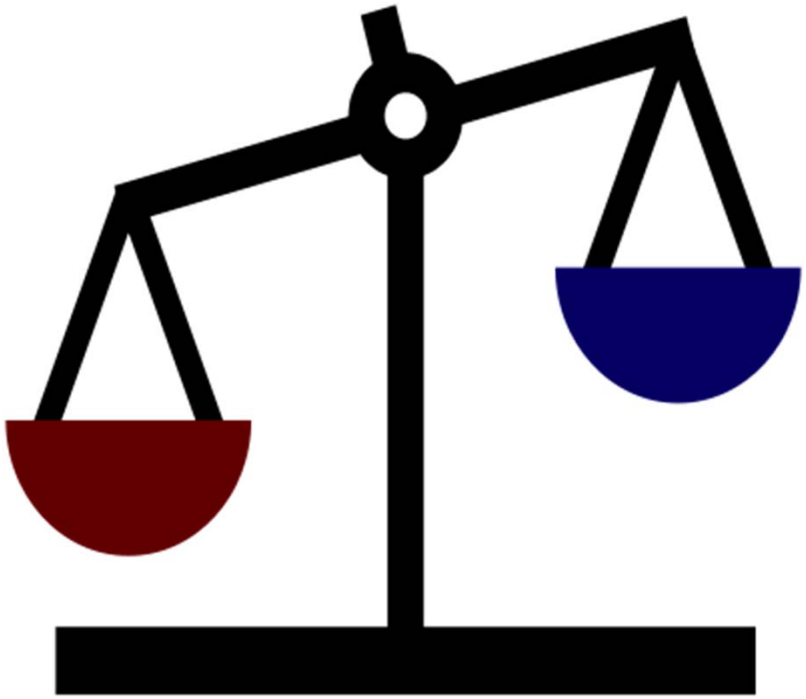


The Tradeoffs

Not enough security

vs.

Maintenance Headaches



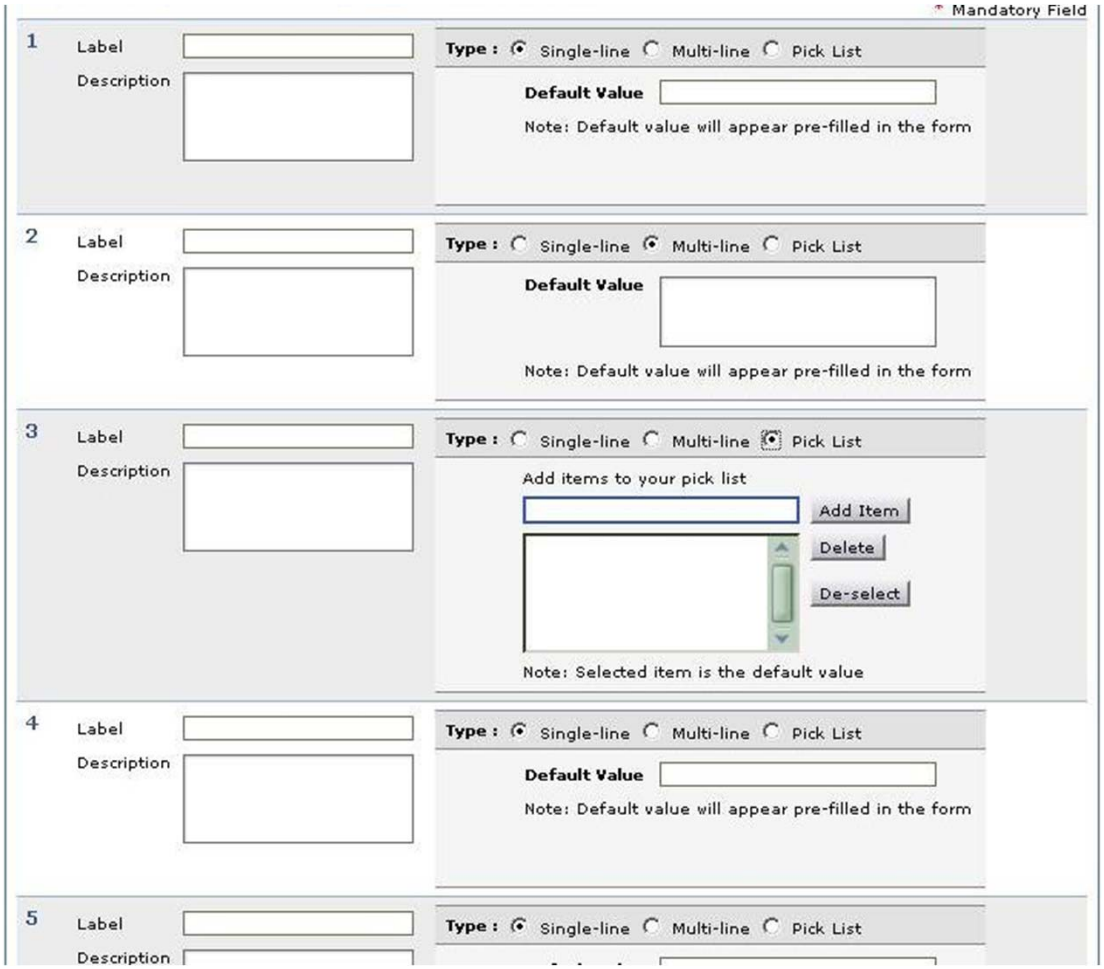
What actually gets deployed!

- First, I want to get ...

- Signatures no longer sufficient
- Fix only discovered vulnerabilities for now

Form Protections

- Scalable State Maintenance



Does this apply to my deployments?

- Need a template specific to my applications!

Know Your Security Tradeoffs!