

JUNOS WEB APP SECURE : RE-THINK SECURITY FOR UNKNOWN ATTACKS

Swastik Bihani

Product Management

April 7, 2014

4,771 IT EXECES WORLDWIDE AGREE

60%

Companies
hacked through
Web apps in past
12 months.

53%

Of attacks were
external, targeting
the datacenter.

60%

Of security
professionals
say NGFW & IP
reputation don't
address the
problem.

- Signature and IP/reputation blocking are inadequate
- DDoS attacks increasing
- Web application security products not solving the problem
- No intelligence sharing

THE PROBLEM OF SIGNATURE-BASED SECURITY

40

Anti-virus

80

New Viruses

5%

Catch Rate

Intrusion
Prevention

Web App
Firewalls

DDoS
Mitigation

Signatures

40

Anti-virus

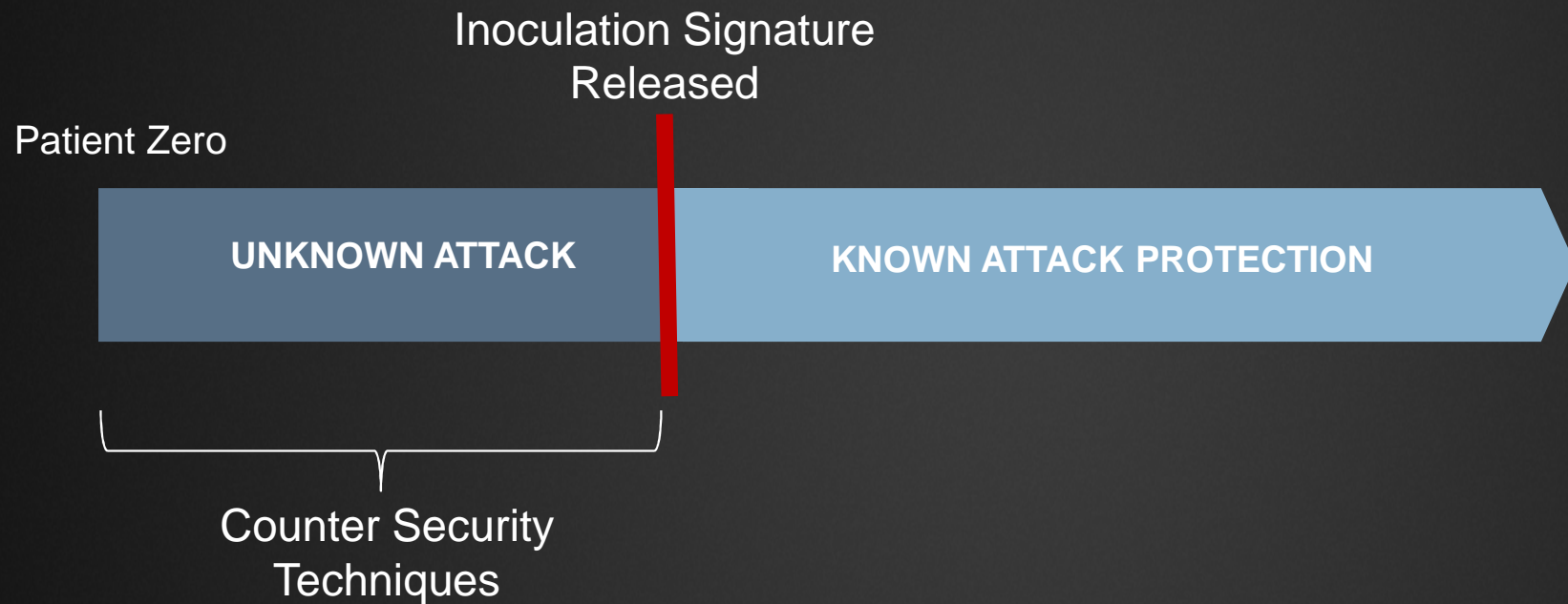
80

New Viruses

5%

Catch Rate

NO-ONE WANTS TO BE PATIENT ZERO



THE WAF WAY: SIGNATURE BASED DEFENSES

Conventional Web Application Firewalls rely primarily on signatures to identify attacks based on known characteristics.

Signature based identification is pattern matching and your defenses are only as good as the library of patterns you have at your disposal.

Highly specific patterns provide good matches with few false positives, but are easier to evade *because* they are so specific. Less specific patterns are harder to evade, but increase the chance of false positives.

THE JWAS WAY: DECEPTION BASED DEFENSES

Junos WebApp Secure is not a standard Web Application Firewall and does not rely on signatures the way the usual WAF does.

JWAS relies on deception to identify attackers, adding “Tar traps” to a protected site’s page that an attack tool or live attacker will see as a normal part of the page.

Any alteration of the tar traps results in attack identification with almost 100% certainty, while the traps are not even rendered on a normal browser.

SIGNATURES VERSUS DECEPTION

Conventional signature based identification and deception techniques are *complimentary* technologies.

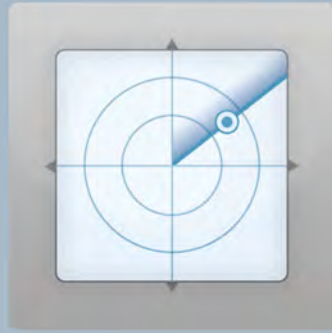
- They do different things.
- They catch different attacks.
- They rely on different techniques.
- They reinforce each others strengths and compensate for each others weaknesses

INTRUSION DECEPTION



Detect

“Tar Traps” detect threats without false positives.



Track

Track IPs, browsers, software and scripts.



Profile

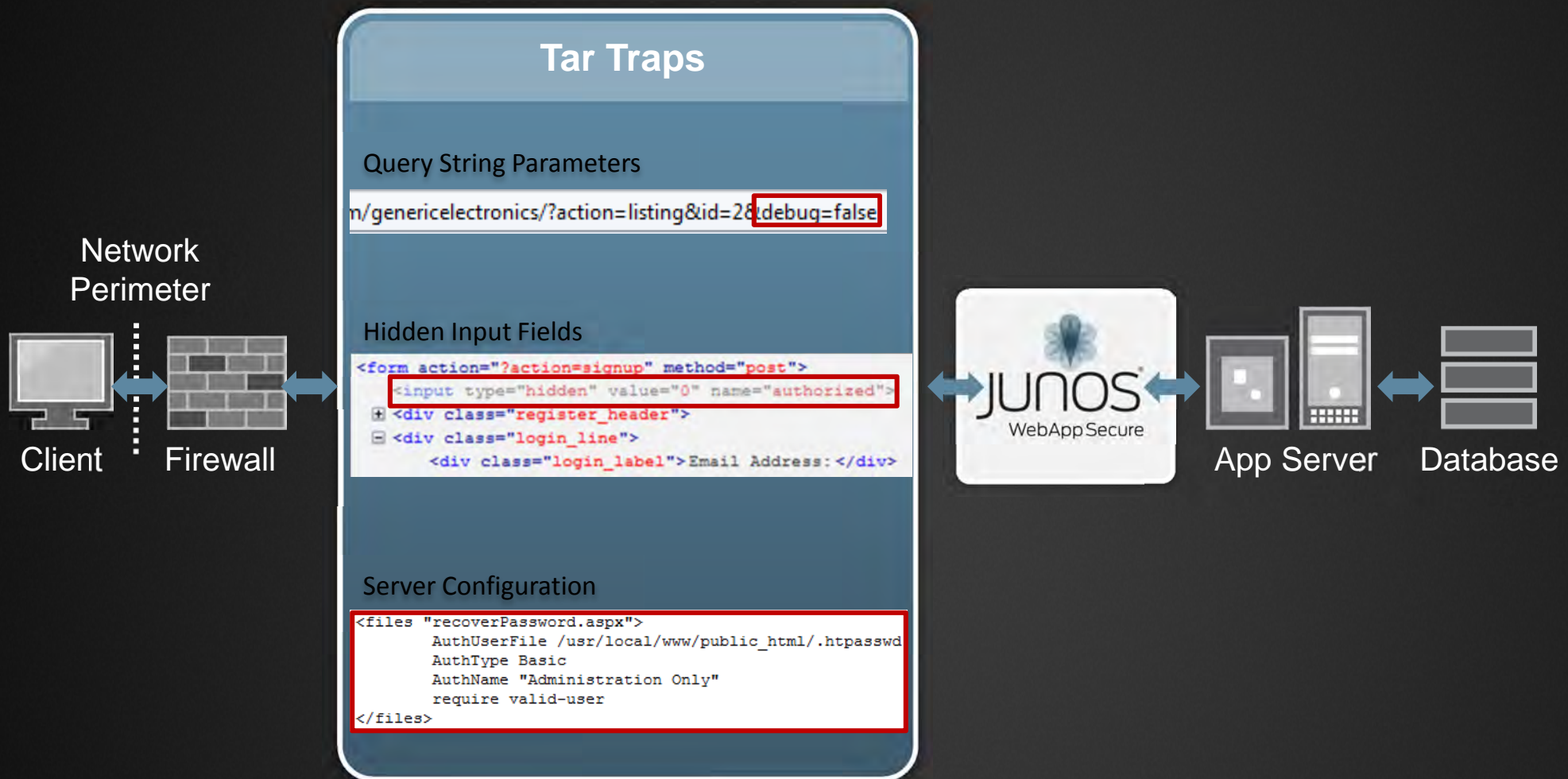
Understand attacker’s capabilities and intents.



Respond

Adaptive responses, including block, warn and deceive.

DETECTION BY DECEPTION



TRACK ATTACKERS BEYOND THE IP

Track IP Address



Track Browser Attacks Persistent Token

Capacity to persist in all browsers including various privacy control features.

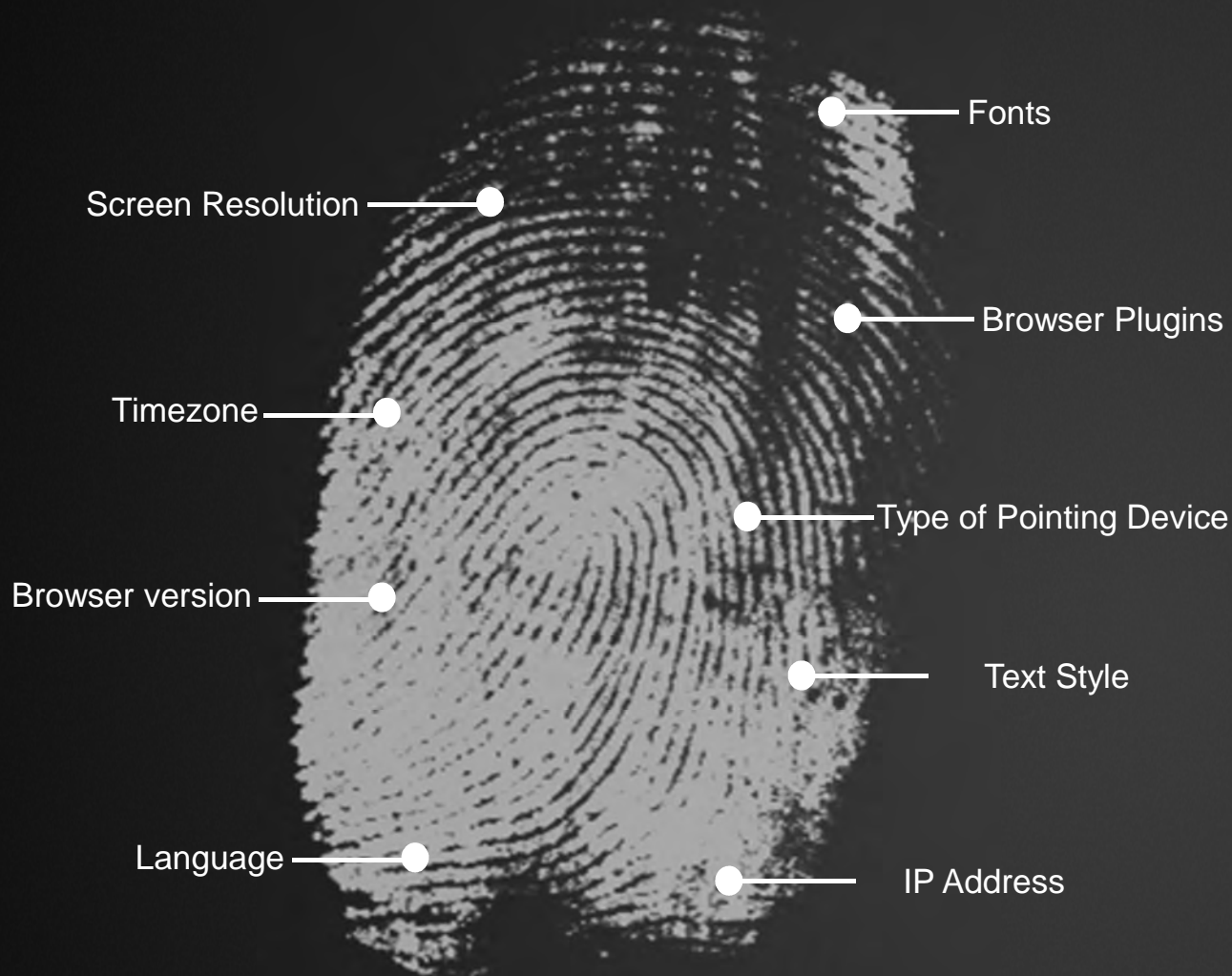


Track Software and Script Attacks Fingerprinting

HTTP communications.



FINGERPRINT OF AN ATTACKER



200+

attributes used to create
the fingerprint.

~ Real Time

availability of fingerprints

False Positives

nearly zero


SMART PROFILE OF ATTACKER

Attacker local name
(on machine)

Attacker Profile

Attackers » Jeannie 3414

Attacker global name
(in Spotlight)

 Ochre 6641

Threat:  High

Last IP:  86.27.116.23

Last Active: 52 minutes, 24 seconds ago (Global: 54 minutes, 1 second ago)

First Active: 1 hour, 19 minutes ago (Global: 1 hour, 19 minutes ago)

Public ID (?): w14xNiPfqj7q4nfh4p8g



Attacker
threat level

Incidents (14)

Responses (7)


Sessions (1)

Locations (1)

Environments (1)

INCIDENTS


Showing malicious incidents only.

 Show all incidents



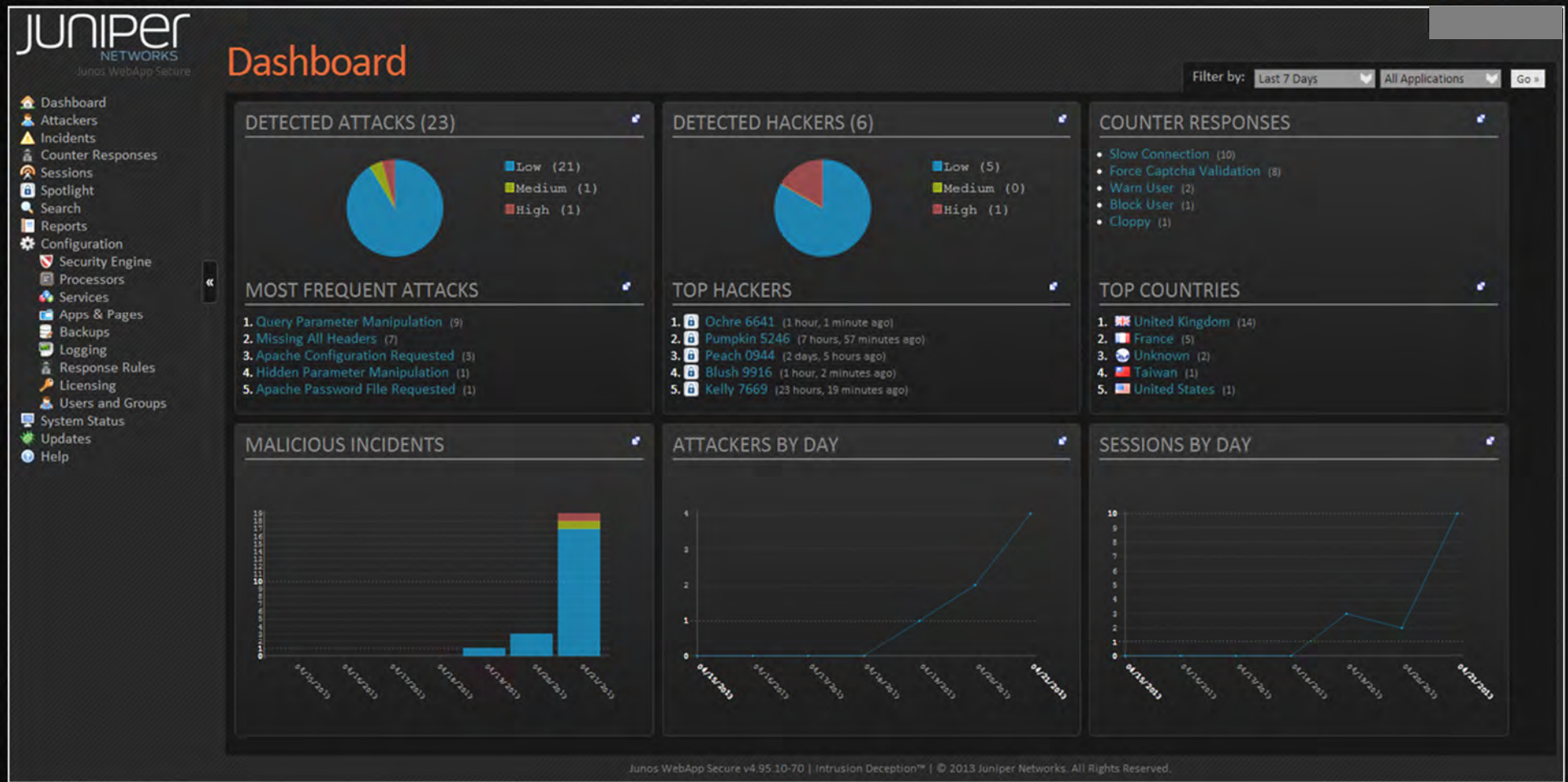
1 - 14 of 14



Incident 	Complexity 	Count 	First Time 	Last Time 	Actions
Password Cracked	 High	1	53 minutes, 26 seconds ago	53 minutes, 26 seconds ago	
Protected Resource Requested	 Low	1	53 minutes, 39 seconds ago	53 minutes, 39 seconds ago	
Apache Password File Requested	 Low	1	57 minutes, 44 seconds ago	57 minutes, 44 seconds ago	
Apache Configuration Requested	 Low	1	58 minutes, 20 seconds ago	58 minutes, 20 seconds ago	
Hidden Parameter Manipulation	 Medium	1	59 minutes, 38 seconds ago	59 minutes, 38 seconds ago	
Query Parameter Manipulation	 Low	1	1 hour, 3 minutes ago	1 hour, 3 minutes ago	
Query Parameter Manipulation	 Low	1	1 hour, 3 minutes ago	1 hour, 3 minutes ago	
Query Parameter Manipulation	 Low	1	1 hour, 3 minutes ago	1 hour, 3 minutes ago	
Query Parameter Manipulation	 Low	1	1 hour, 3 minutes ago	1 hour, 3 minutes ago	
Query Parameter Manipulation	 Low	1	1 hour, 3 minutes ago	1 hour, 3 minutes ago	
Query Parameter Manipulation	 Low	1	1 hour, 3 minutes ago	1 hour, 3 minutes ago	

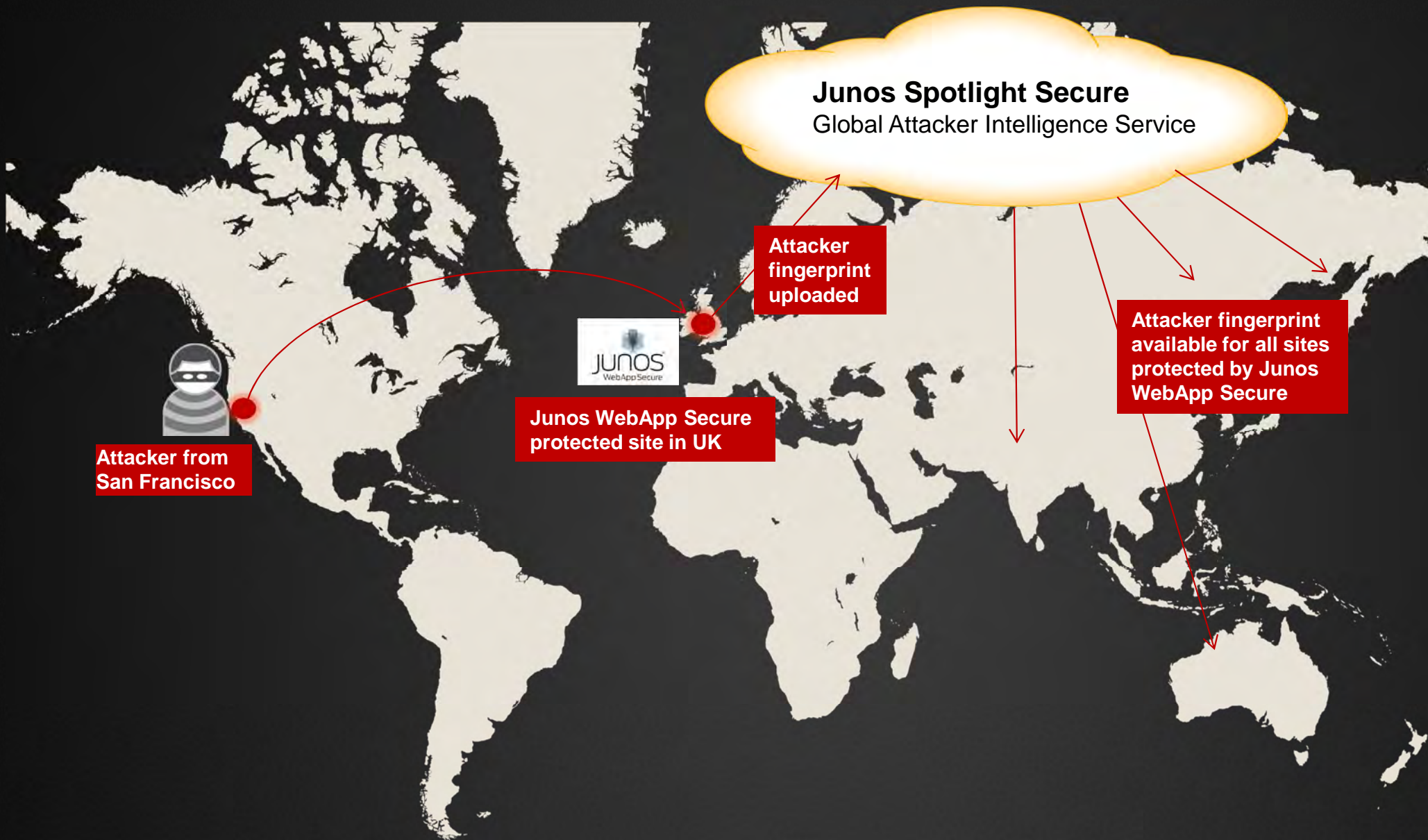
Incident history

REAL-TIME VISIBILITY



- Web-based console
- Real-time
- On-demand threat information
- SMTP alerting
- Reporting (Pdf, HTML)
- CLI for exporting data into SIEM tool

JUNOS SPOTLIGHT SECURE



Detect Anywhere, Stop Everywhere

DETECT UNKNOWN ATTACKERS LOCALLY AND PREVENT GLOBALLY

JUNOS WEBAPP SECURE

Intrusion Deception



JUNOS SPOTLIGHT SECURE

Attacker Intelligence
Service



JUNOS DDOS SECURE

Volumetric and Low and
Slow Protection



WWW.JUNIPER.NET

WHITEBOARDING

What Problems are we Solving?

1 Datacenter

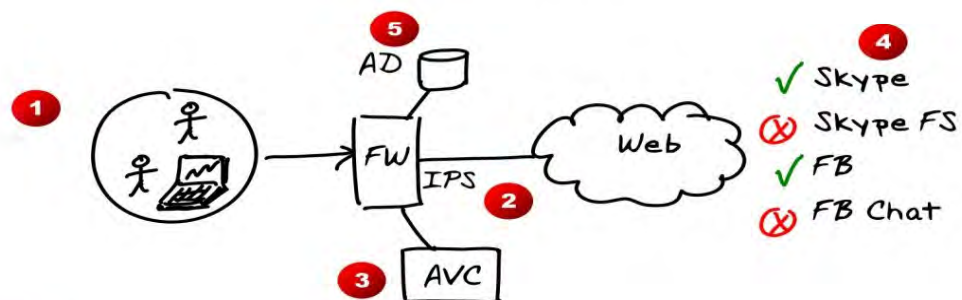
2 Campus/Branch

ERASER
for whiteboard or glass surfaces

Protecting Campus/Branch i.e. NGFW

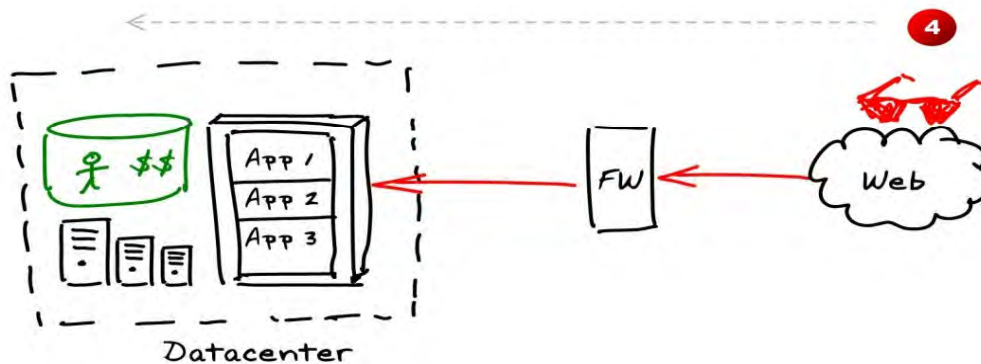
Datacenter

Campus/Branch



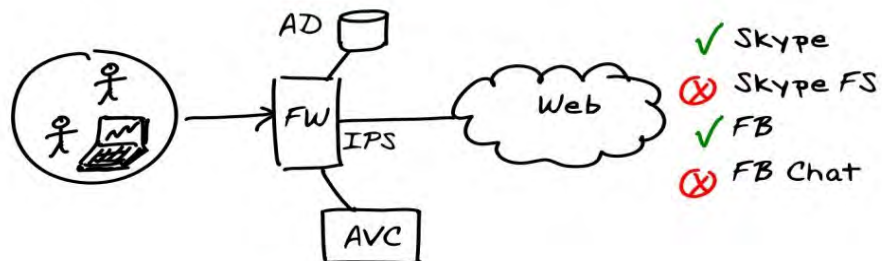
Egress vs Ingress

Datacenter (Ingress) 3



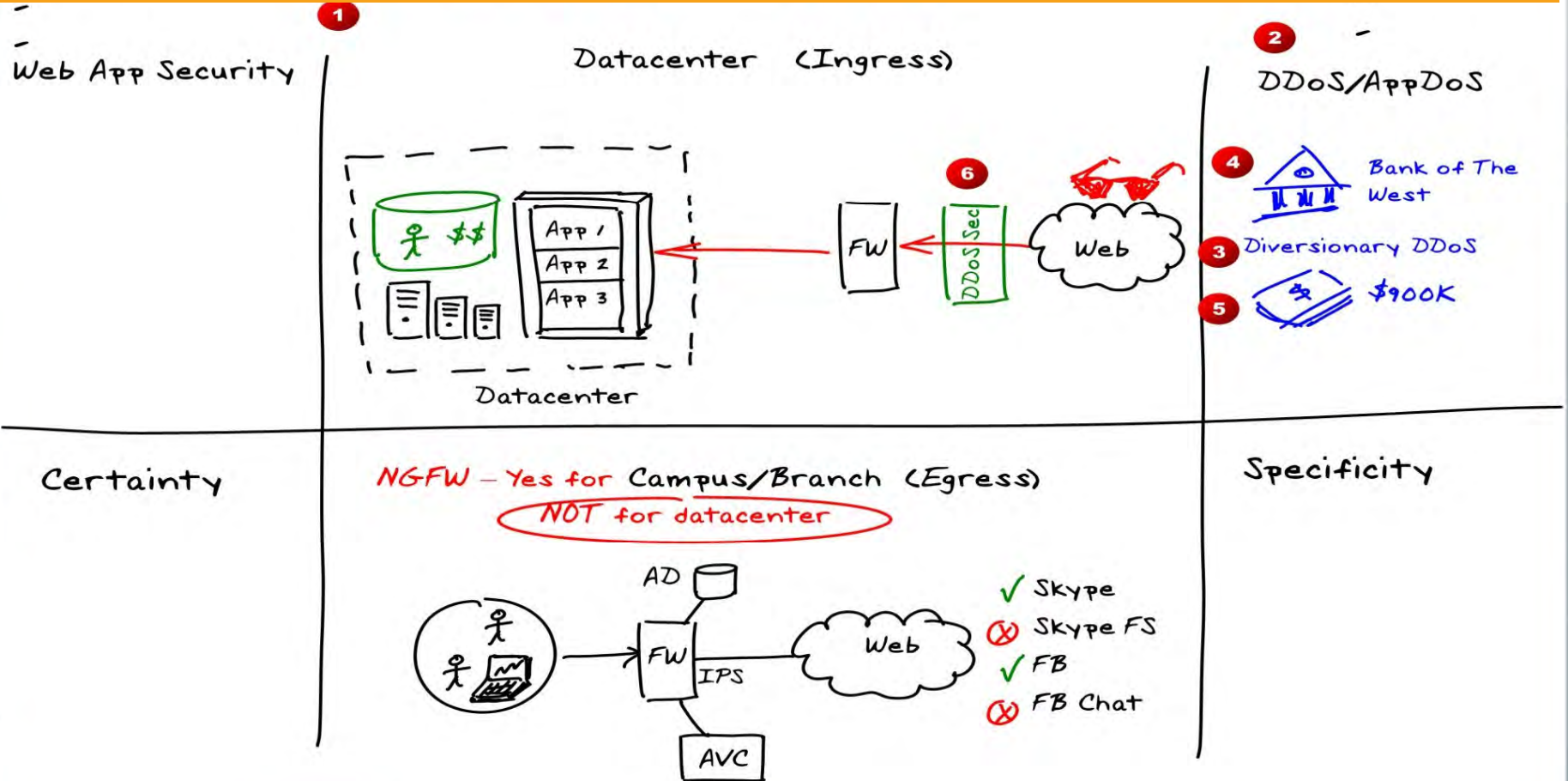
NGFW - Yes for Campus/Branch (Egress) 2

1 NOT for datacenter



ERASER

Juniper DDoS & App DoS



ERASER

Juniper Web App Security

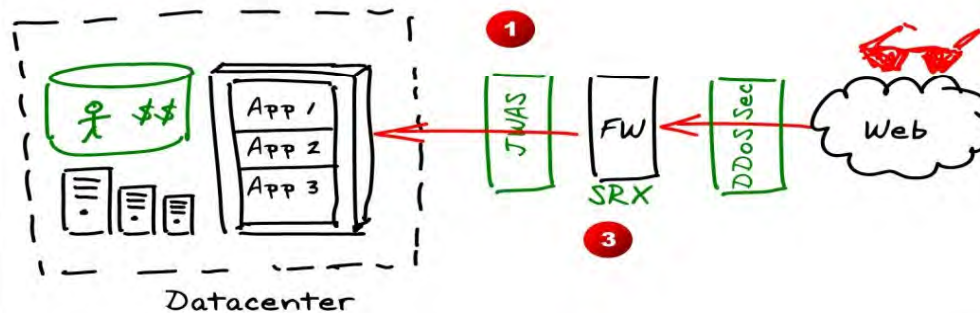
Web App Security

2

Brown Printing

- Up in 20 min.
- 1 mo. - 210 incidents &
- 5 real-time attacks

Datacenter (Ingress)



DDoS/AppDoS



Bank of The West

Diversiónary DDoS

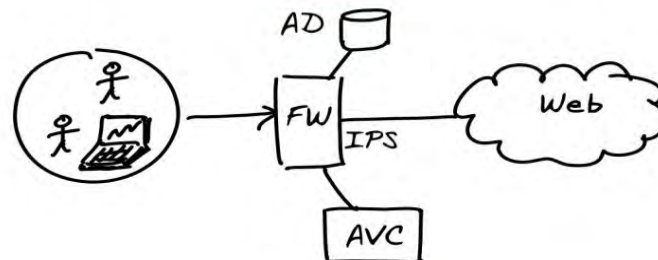


\$900K

Certainty

NGFW - Yes for Campus/Branch (Egress)

NOT for datacenter



- ✓ Skype
- ✗ Skype FS
- ✓ FB
- ✗ FB Chat

Specificity

ERASER

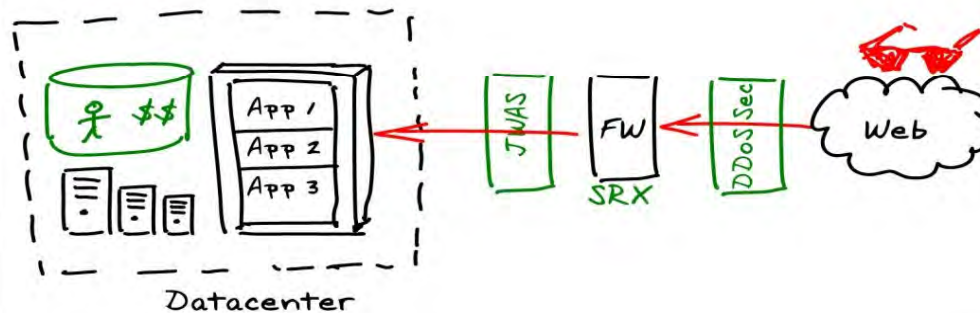
Why Certainty Matters...

Web App Security

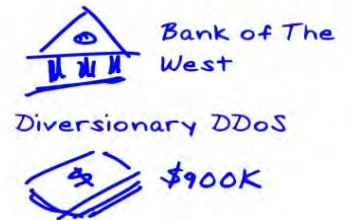
Brown Printing

- Up in 20 min.
- 1 mo. - 210 incidents &
- 5 real-time attacks

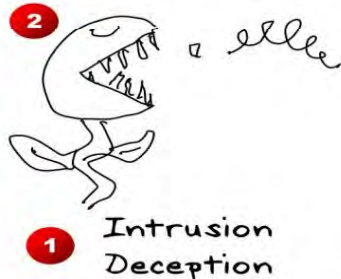
Datacenter (Ingress)



DDoS/AppDoS

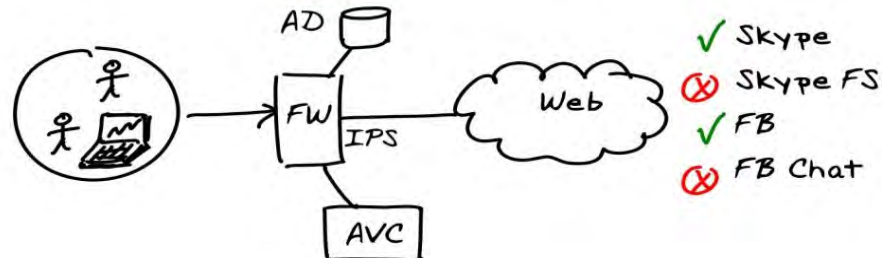


Certainty



NGFW - Yes for Campus/Branch (Egress)

NOT for datacenter



Specificity

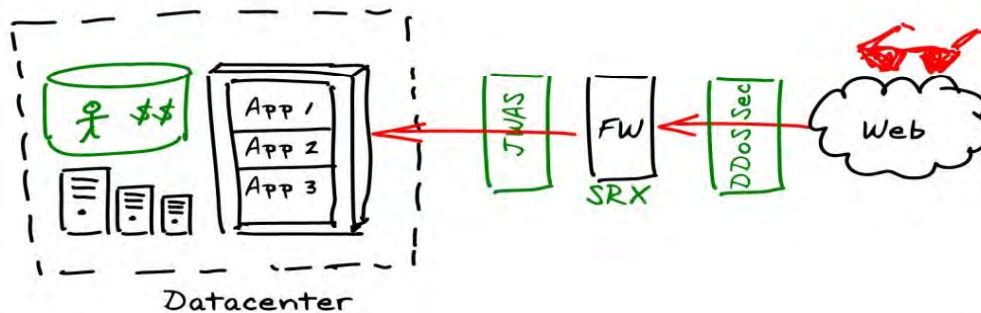
Why Specificity Matters

Web App Security

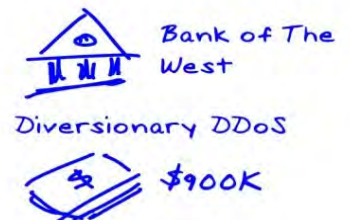
Brown Printing

- Up in 20 min.
- 1 mo. - 210 incidents &
- 5 real-time attacks

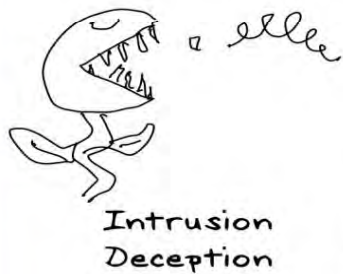
Datacenter (Ingress)



DDoS/AppDoS

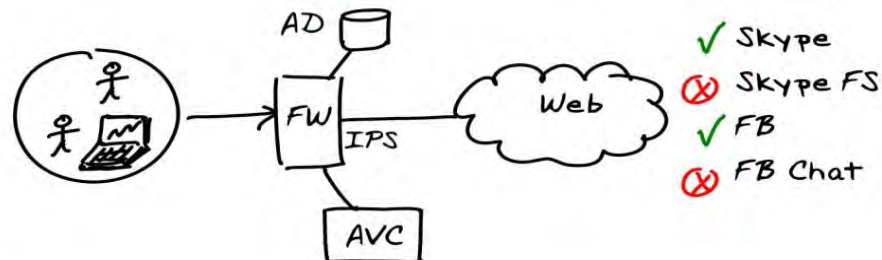


Certainty

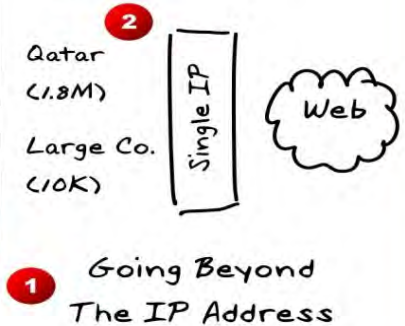


NGFW - Yes for Campus/Branch (Egress)

NOT for datacenter



Specificity



ERASER

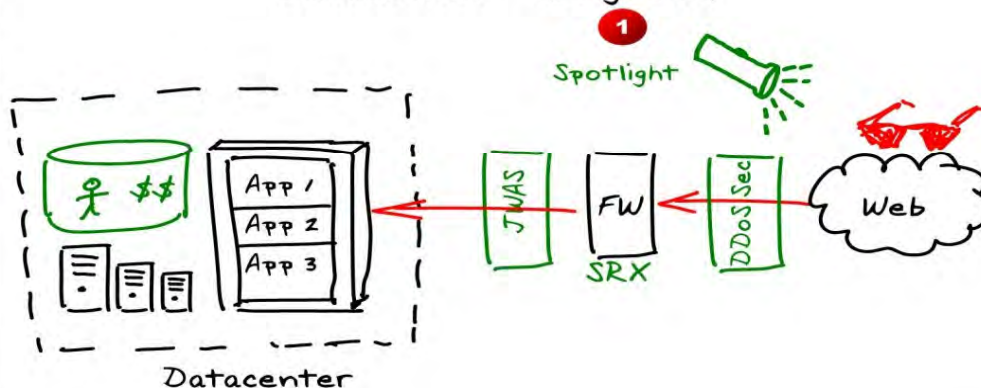
Spotlight & Next Steps

Web App Security

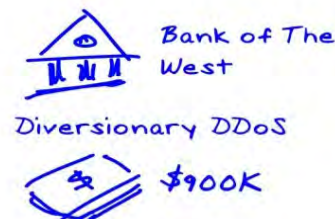
Brown Printing

- Up in 20 min.
- 1 mo. - 210 incidents &
- 5 real-time attacks

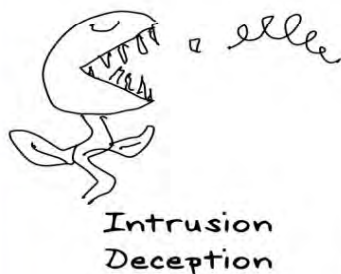
Datacenter (Ingress)



DDoS/AppDoS

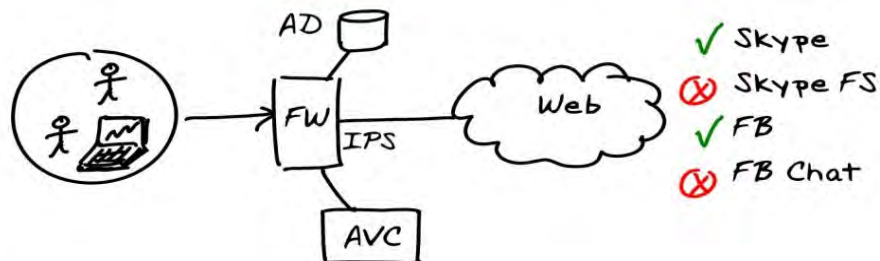


Certainty

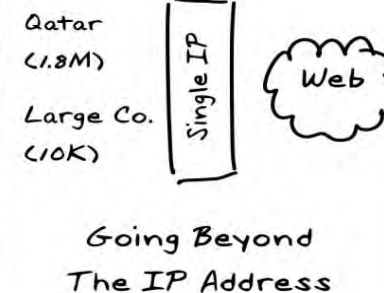


NGFW - Yes for Campus/Branch (Egress)

NOT for datacenter



Specificity



ERASER

THANK YOU!

FOR MORE INFO PLEASE VISIT:

WWW.JUNIPER.NET