

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

Web App Firewalls

Intrusion
Prevention

DDoS
Mitigation

Signatures

40

Anti-virus

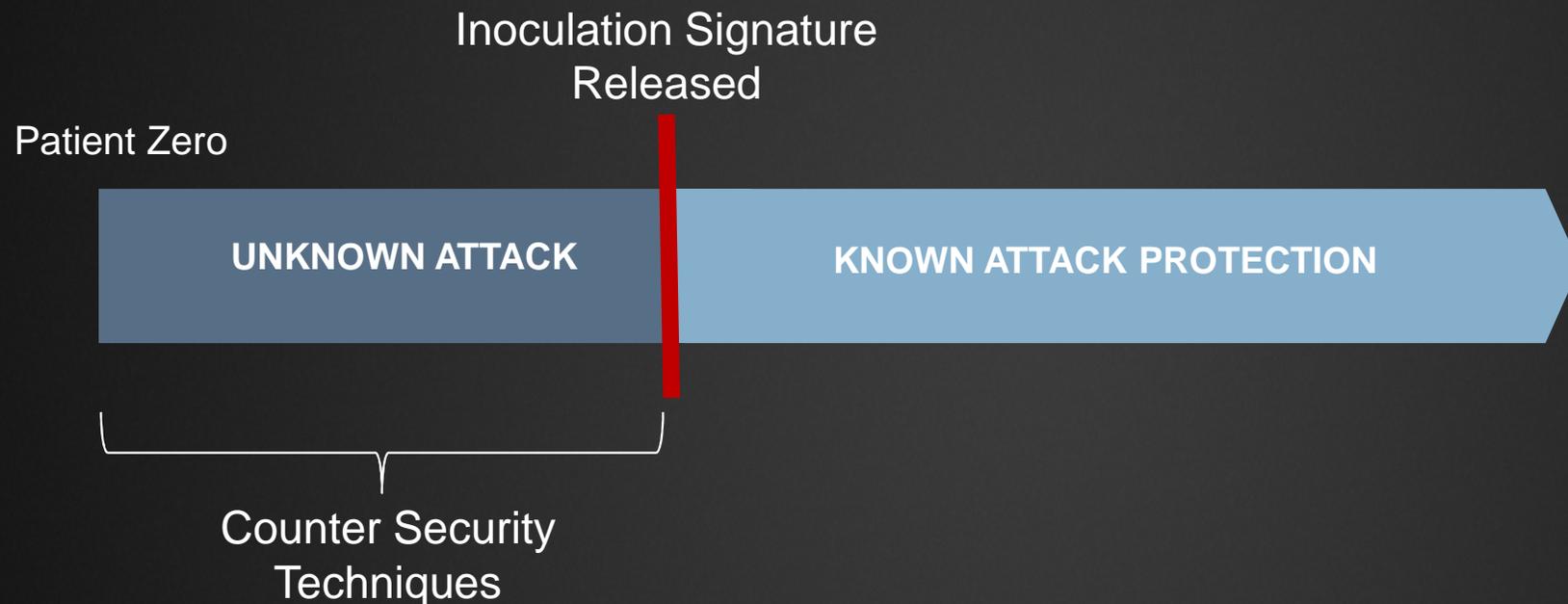
80

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.

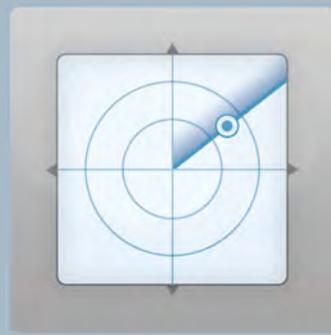
- They do different things.
- They catch different attacks.
- They rely on different techniques.
- They reinforce each others strengths and compensate for each others weaknesses

INTRUSION DECEPTION



Detect

“Tar Traps” detect threats without false positives.



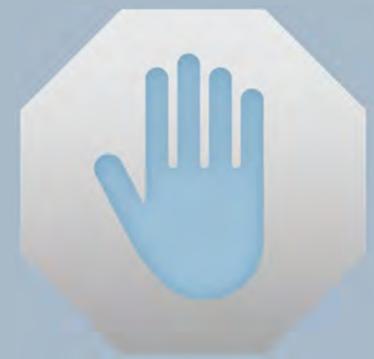
Track

Track IPs, browsers, software and scripts.



Profile

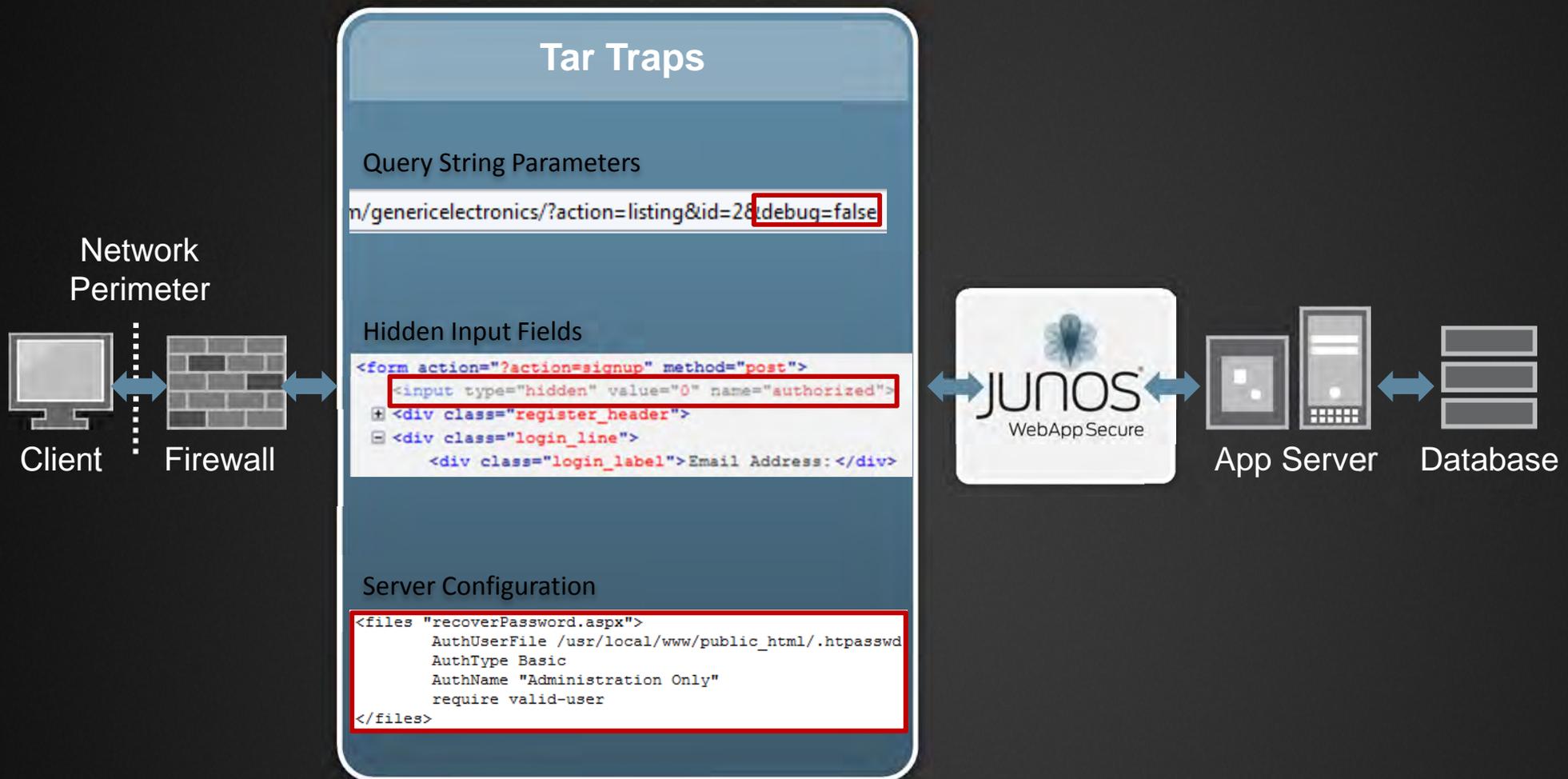
Understand attacker’s capabilities and intents.



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.

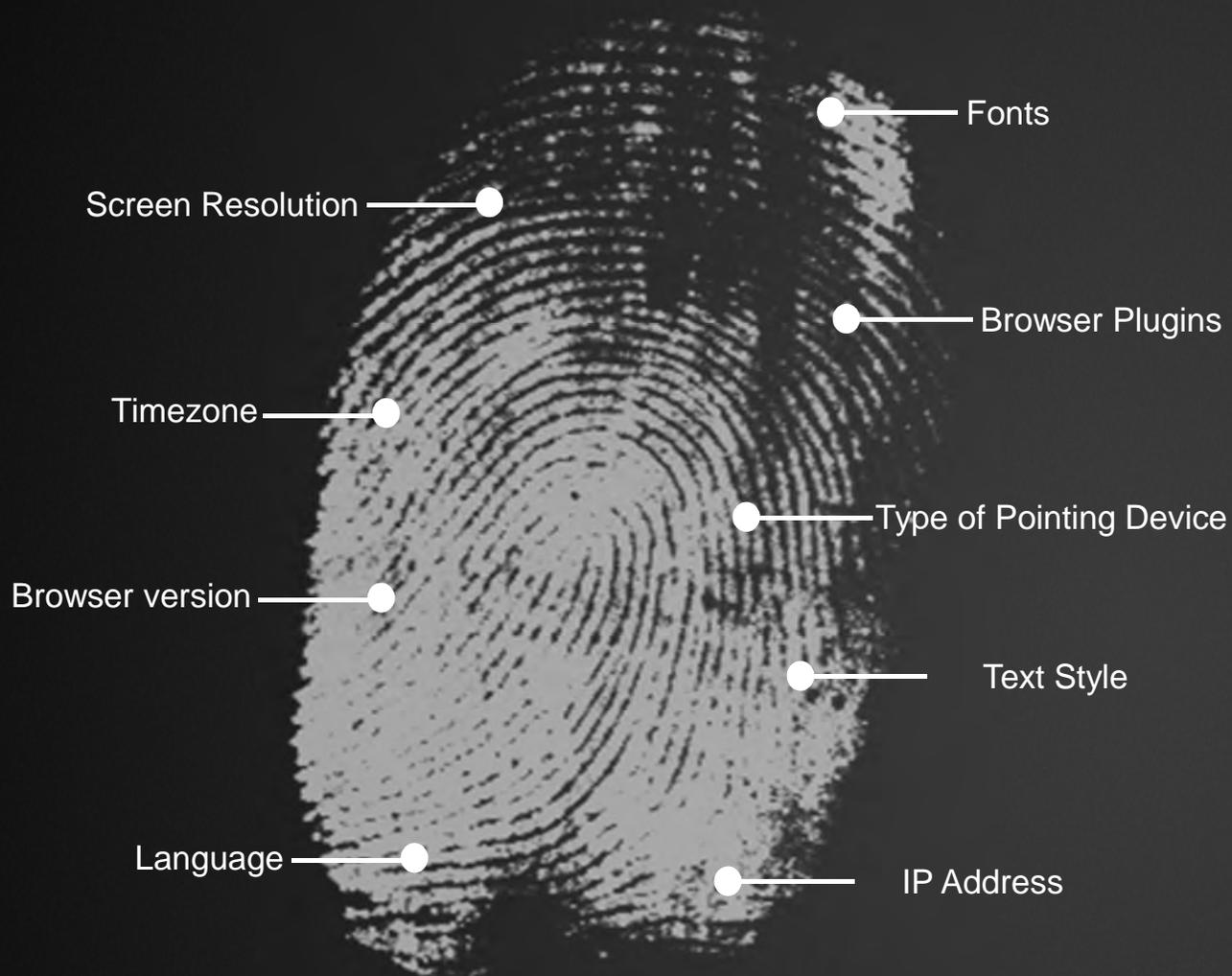


Track Software and Script Attacks Fingerprinting

HTTP communications.



FINGERPRINT OF AN ATTACKER



200+

attributes used to create
the fingerprint.

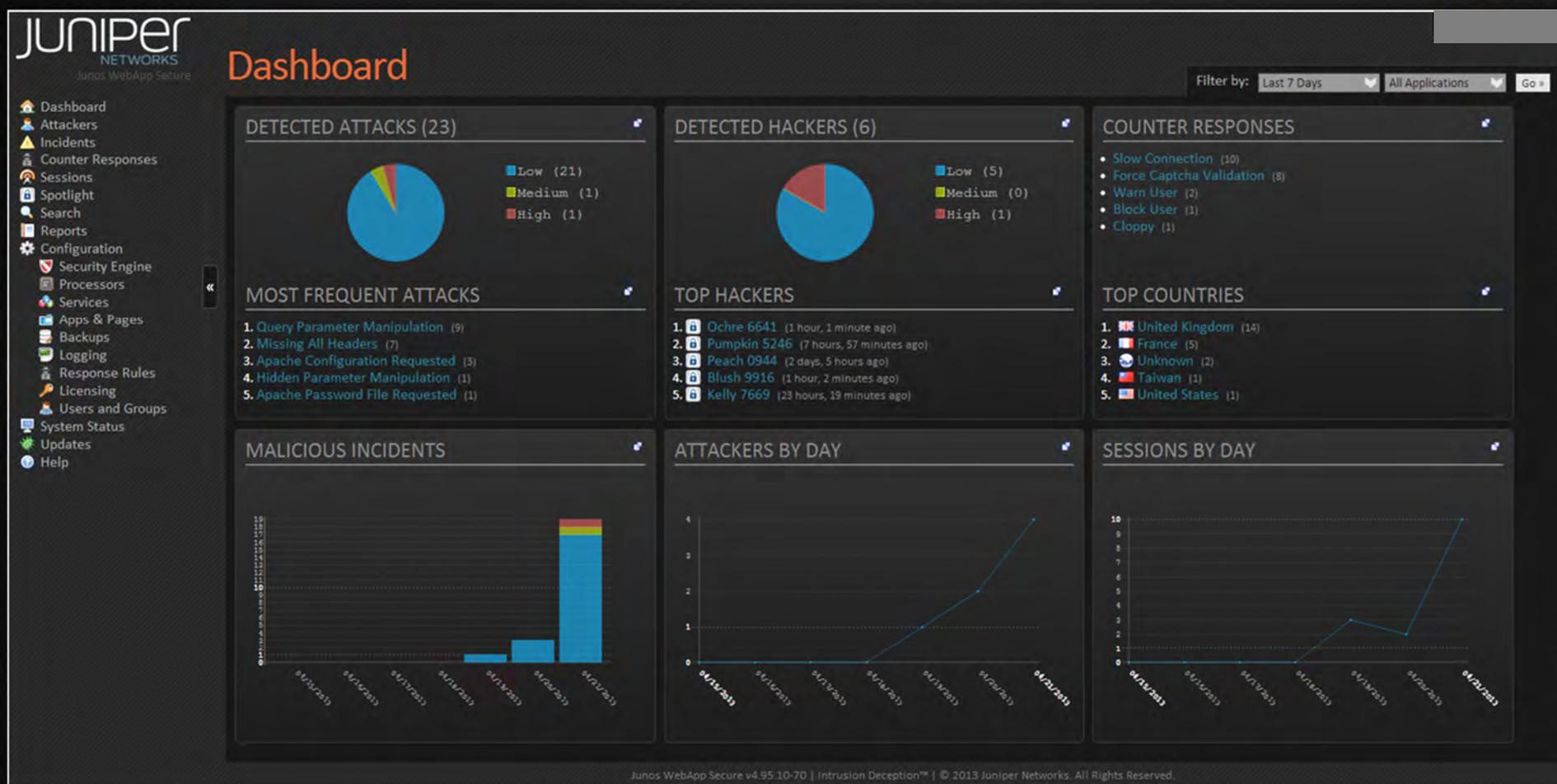
~ Real Time

availability of fingerprints

False Positives

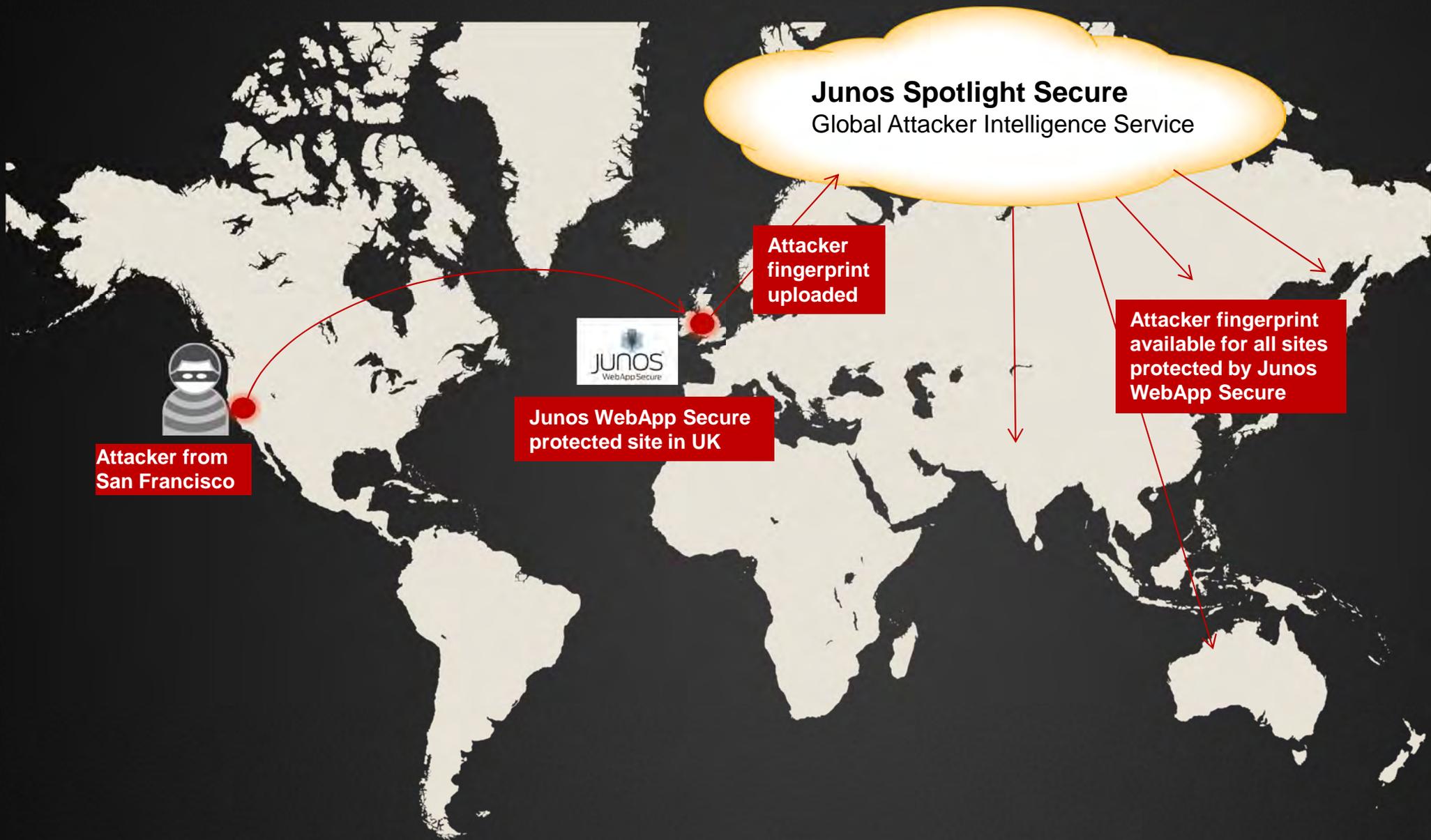
nearly zero

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



The screenshot shows the Juniper WebApp Secure product page. The main headline is "DECEIVE, THEN DELETE HACKERS." Below this, there is a sub-headline "1. DETECT" and a description of the product's capabilities. The page includes a navigation menu, a search bar, and social media links. A sidebar on the right contains a "DECEIVE, THEN DELETE HACKERS." graphic and a "LEARN MORE" button.

JUNOS SPOTLIGHT SECURE

Attacker Intelligence Service



The screenshot shows the Juniper Spotlight Secure product page. The main headline is "SEE NETWORK SECURITY IN A WHOLE NEW LIGHT" with a sub-headline "Discover our next-generation data center security products." Below this, there is a sub-headline "2. TRACK" and a description of the product's capabilities. The page includes a navigation menu, a search bar, and social media links. A sidebar on the right contains a "DECEIVE, THEN DELETE HACKERS." graphic and a "LEARN MORE" button.

JUNOS DDOS SECURE

Volumetric and Low and Slow Protection



The screenshot shows the Juniper DDOS Secure product page. The main headline is "JUNOS DDOS SECURE" with a sub-headline "Junos DDOS Secure is designed to defend against flood and application layer distributed denial of service (DDoS) attacks." Below this, there is a sub-headline "3. TRACK" and a description of the product's capabilities. The page includes a navigation menu, a search bar, and social media links. A sidebar on the right contains a "DECEIVE, THEN DELETE HACKERS." graphic and a "LEARN MORE" button.

WWW.JUNIPER.NET

WHITEBOARDING

What Problems are we Solving?

1 Datacenter

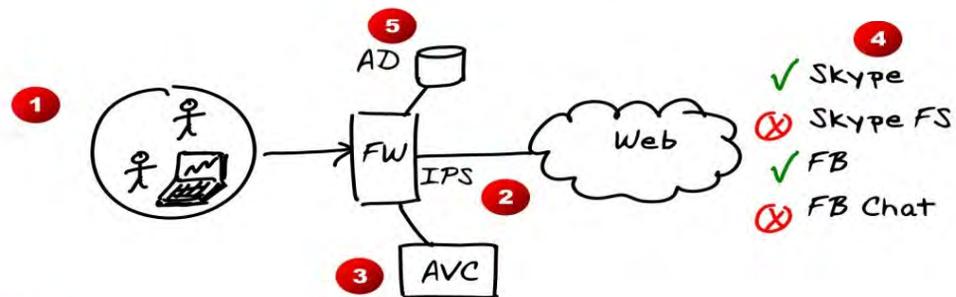
2 Campus/Branch

ERASER
For Whiteboards and Glass Surfaces

Protecting Campus/Branch i.e. NGFW

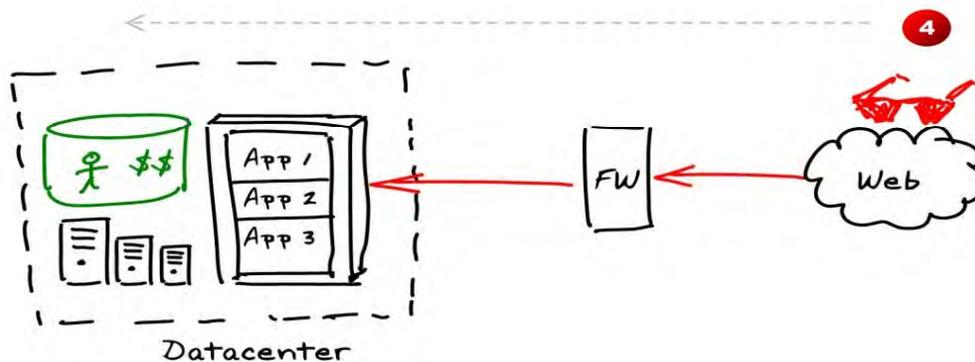
Datacenter

Campus/Branch



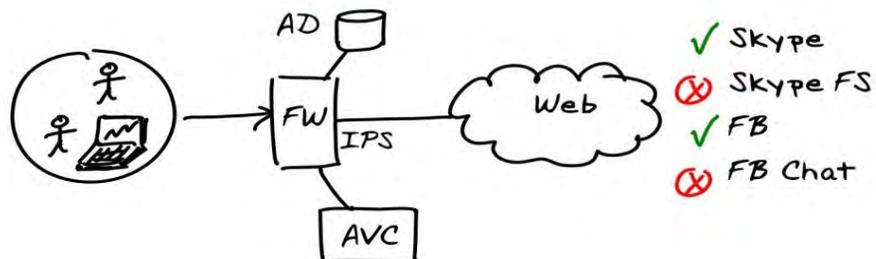
Egress vs Ingress

Datacenter (Ingress) 3



NGFW - Yes for Campus/Branch (Egress) 2

1 NOT for datacenter

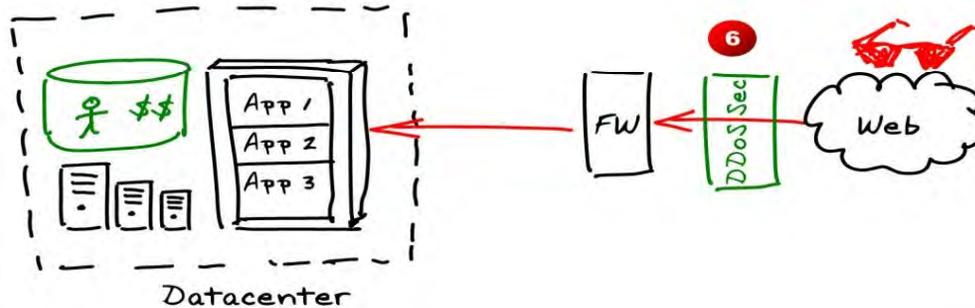


Juniper DDoS & App DoS

Web App Security

1

Datacenter (Ingress)



2

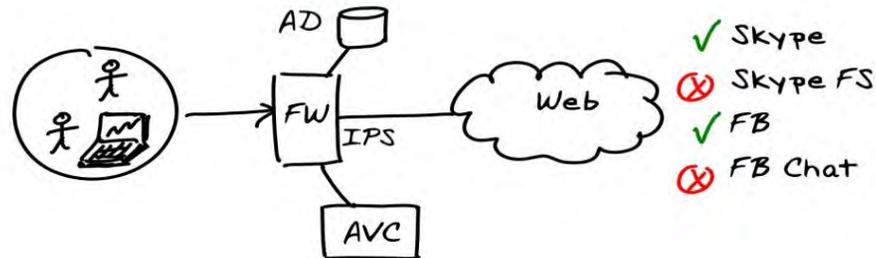
DDoS/AppDoS

- 4 Bank of The West
- 3 Diversionary DDoS
- 5 \$900K

Certainty

NGFW - Yes for Campus/Branch (Egress)

NOT for datacenter



- ✓ Skype
- ⊗ Skype FS
- ✓ FB
- ⊗ FB Chat

Specificity



Juniper Web App Security

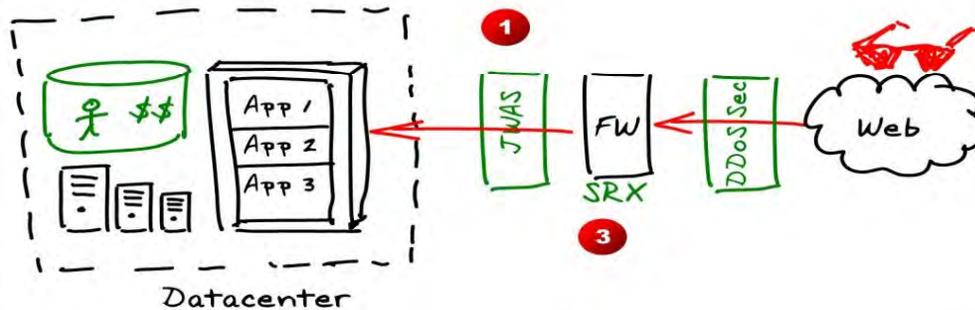
Web App Security

2

Brown Printing

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

Datacenter (Ingress)



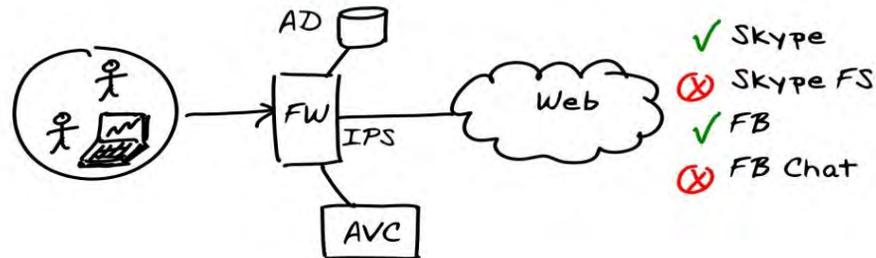
DDoS/AppDoS

- Bank of The West
- Diversinary DDoS
- \$900K

Certainty

NGFW - Yes for Campus/Branch (Egress)

NOT for datacenter



Specificity

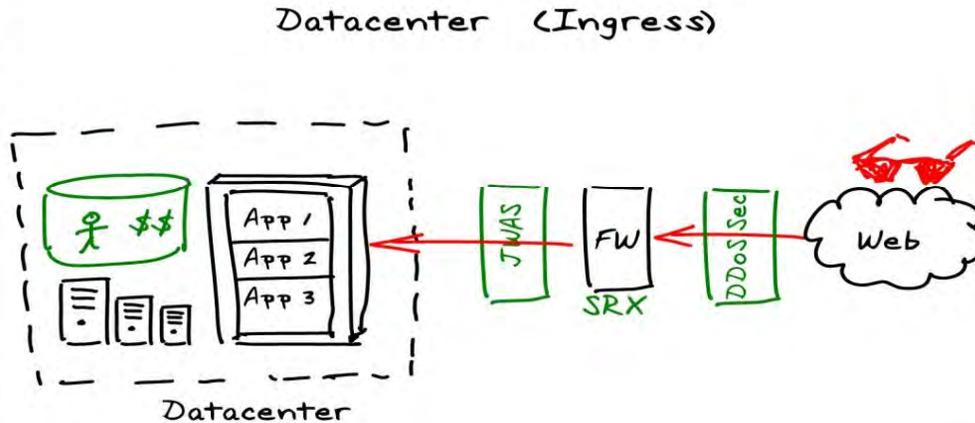


Why Certainty Matters...

Web App Security

Brown Printing

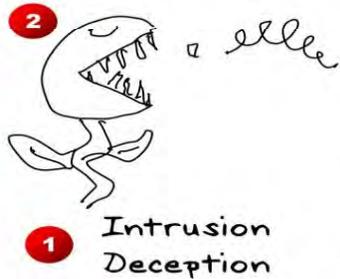
- Up in 20 min.
- 1 mo. - 210 incidents & 5 real-time attacks



DDoS/AppDoS

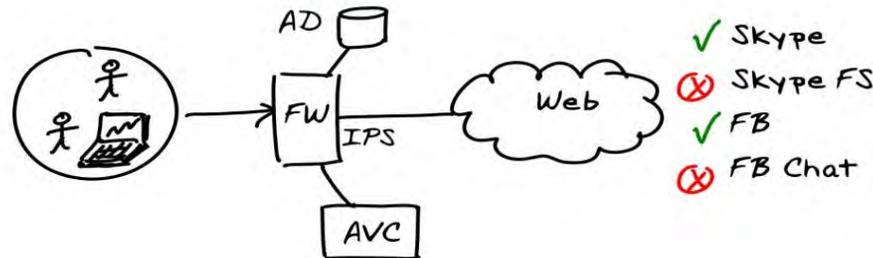


Certainty



NGFW - Yes for Campus/Branch (Egress)

NOT for datacenter



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

Specificity

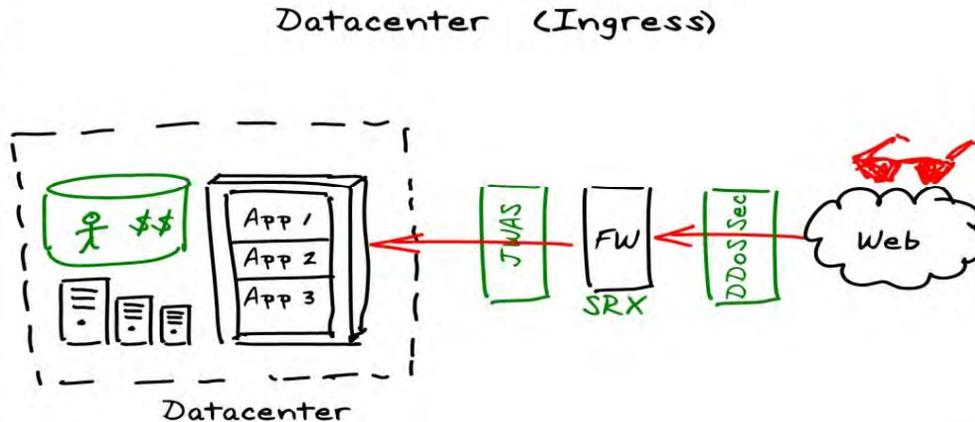


Why Specificity Matters

Web App Security

Brown Printing

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



DDoS/AppDoS

Bank of The West

Diversitory DDoS

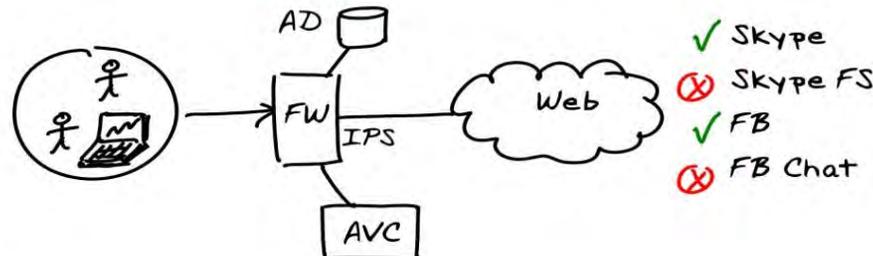
\$900K

Certainty

Intrusion Deception

NGFW - Yes for Campus/Branch (Egress)

NOT for datacenter



Specificity

Qatar (1.8M) 2

Large Co. (10K)

Single IP

1 Going Beyond The IP Address

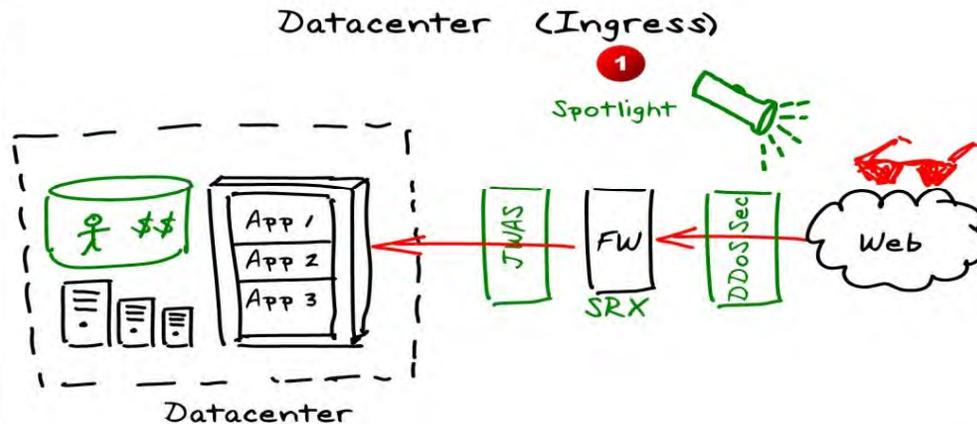


Spotlight & Next Steps

Web App Security

Brown Printing

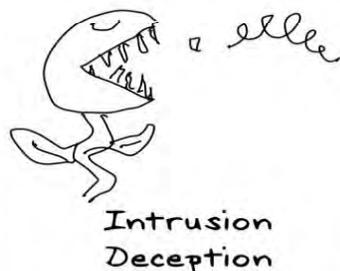
- Up in 20 min.
- 1 mo. - 210 incidents & 5 real-time attacks



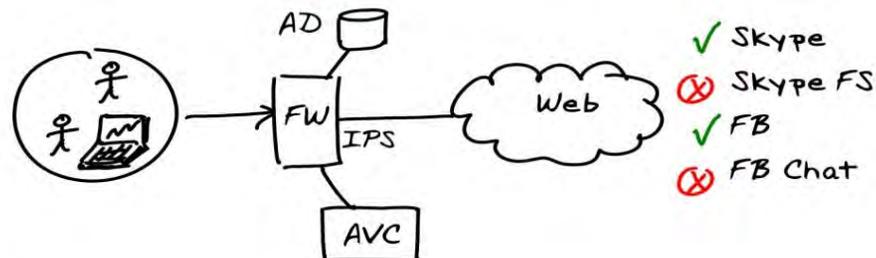
DDoS/AppDoS



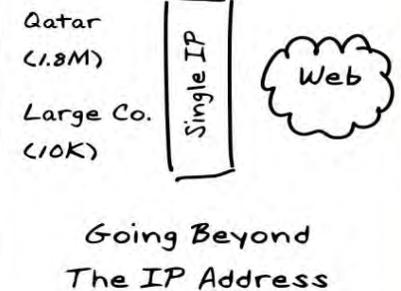
Certainty



NGFW - Yes for Campus/Branch (Egress) NOT for datacenter



Specificity



THANK YOU!

FOR MORE INFO PLEASE VISIT:

WWW.JUNIPER.NET