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

Swastik Bihani
Product Management
April 7, 2014

4,771 IT EXECS 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

Sources: KRC Research and Juniper Mobile Threat Center

THE PROBLEM OF SIGNATURE-BASED SECURITY

Anti-virus

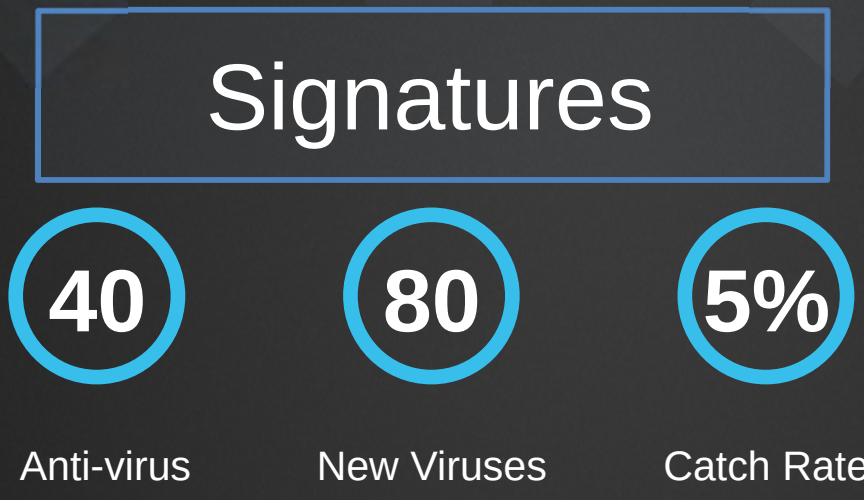
New Viruses

Catch Rate

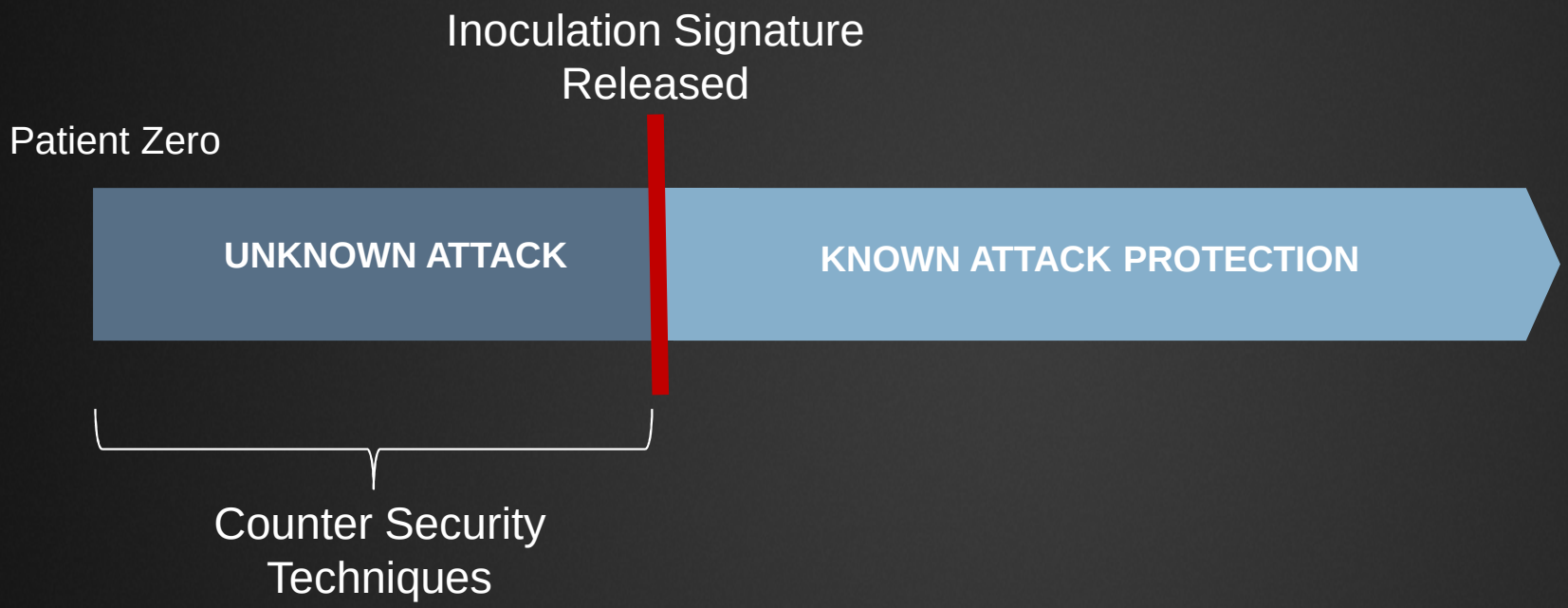
Web App
Firewalls

Intrusion
Prevention

DDoS
Mitigation



NO-ONE WANTS TO BE PATIENT ZERO



juniper NETWORKS

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.

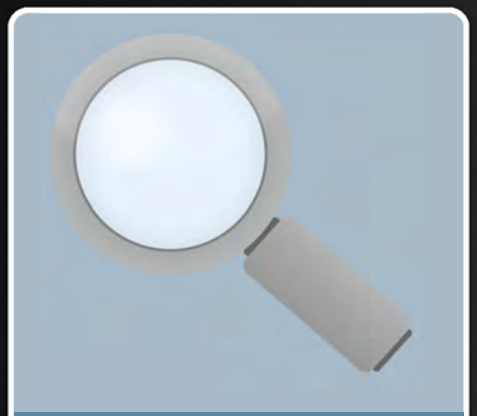
Any alteration of the tar traps results in attack identification with almost 100% certainty, while the traps are not even rendered on a normal browser.

SIGNATURES VERSUS DECEPTION

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

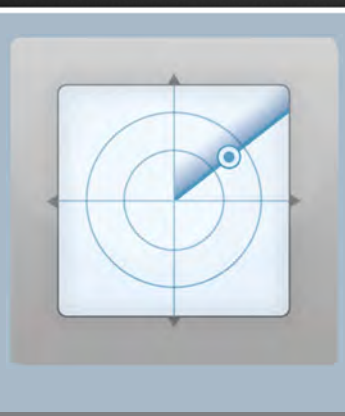
- They do different things.
- They catch different attacks.
- They rely on different techniques.
- They reinforce each others strengths and compensate for each others weaknesses

INTRUSION DECEPTION



Detect

“Tar Traps” detect threats without false positives.



Track

Track IPs, browsers, software and scripts.

Profile

Understand attacker’s capabilities and intents.

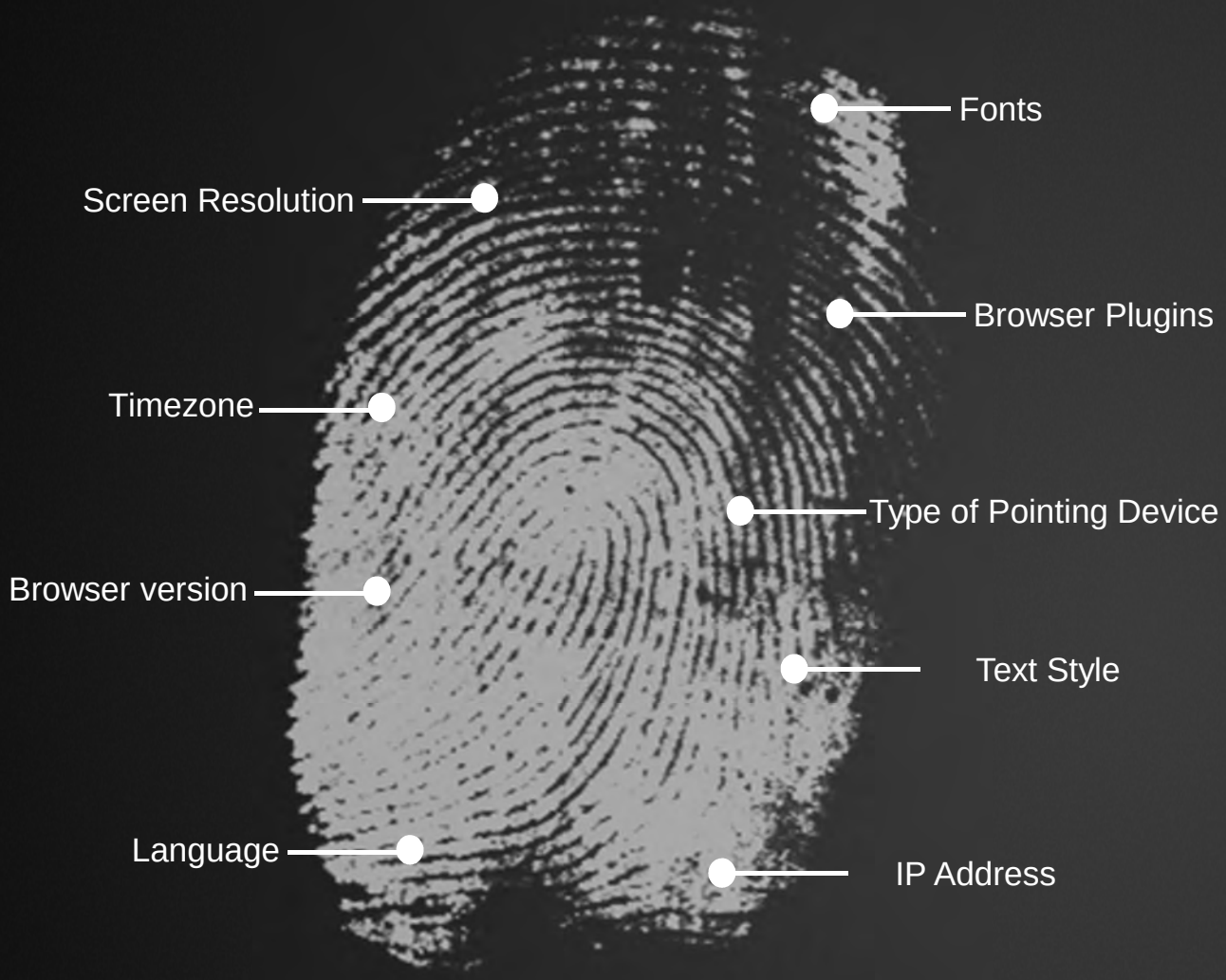
Respond

Adaptive responses, including block, warn and deceive.

DETECTION BY DECEPTION

TRACK ATTACKERS BEYOND THE IP

FINGERPRINT OF AN ATTACKER



200+
attributes used to create the fingerprint.

~ Real Time
availability of fingerprints

False Positives
nearly zero

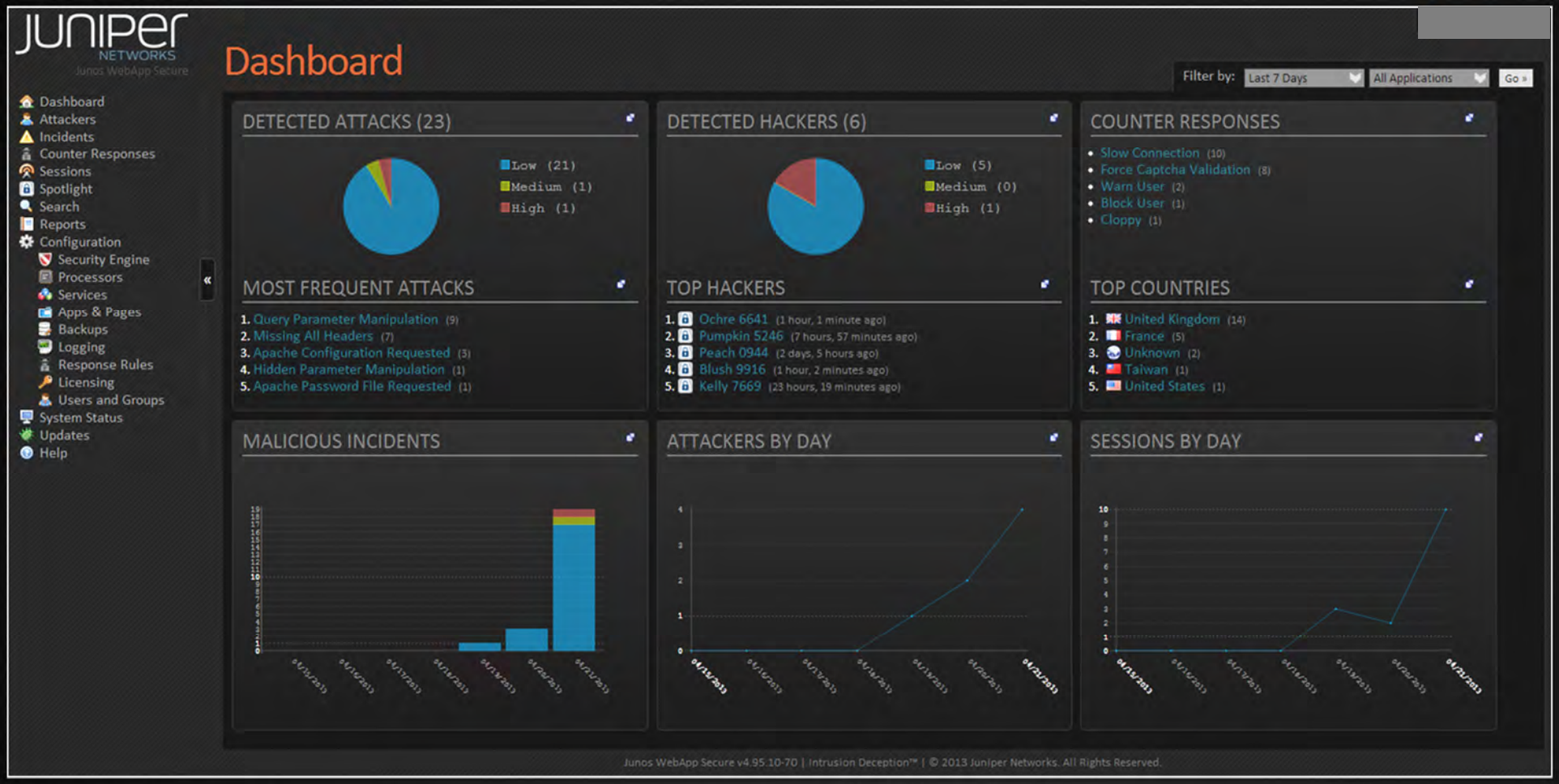
SMART PROFILE OF ATTACKER

Attacker local name (on machine)

Attacker threat level

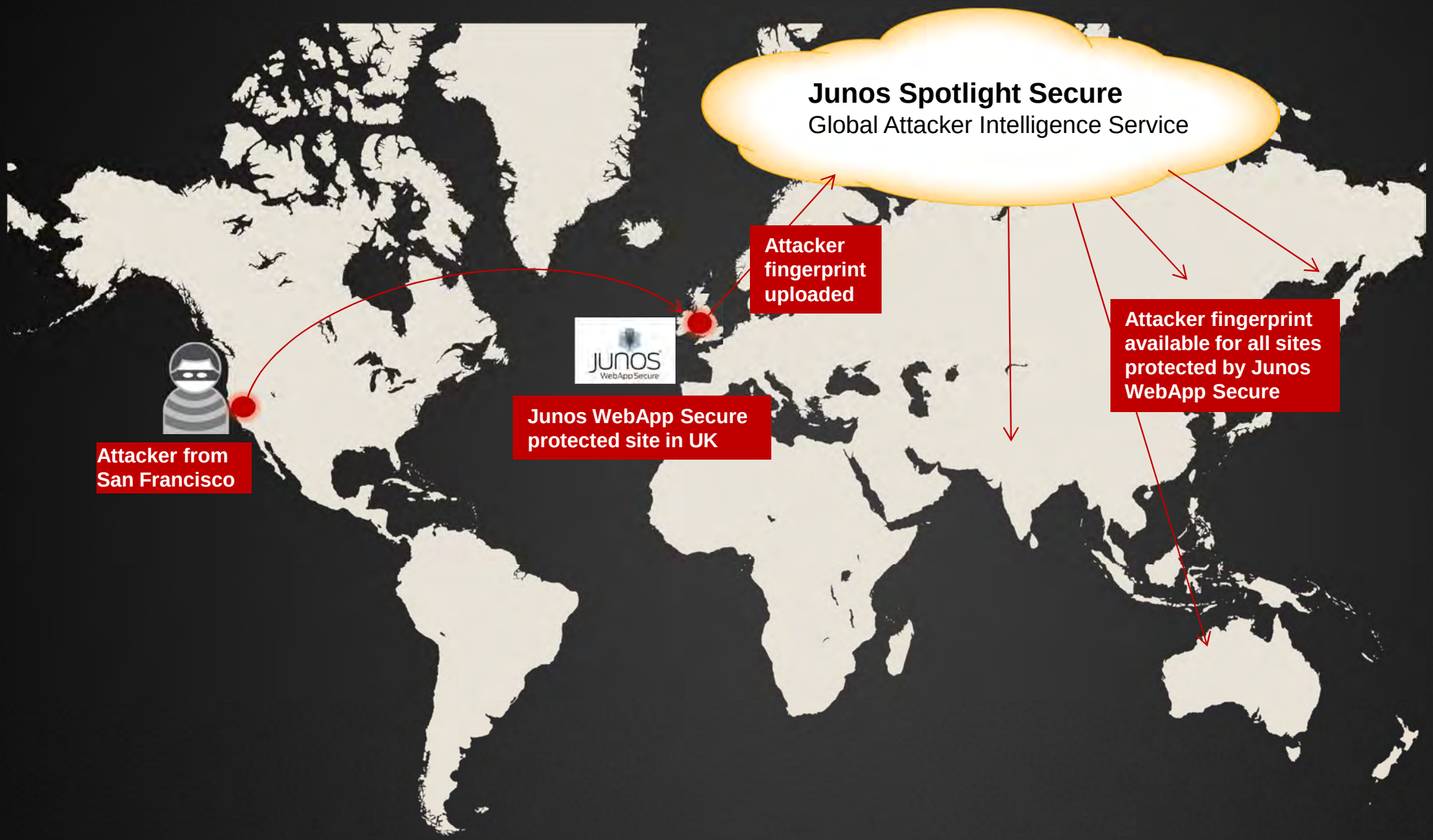
Incident history

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

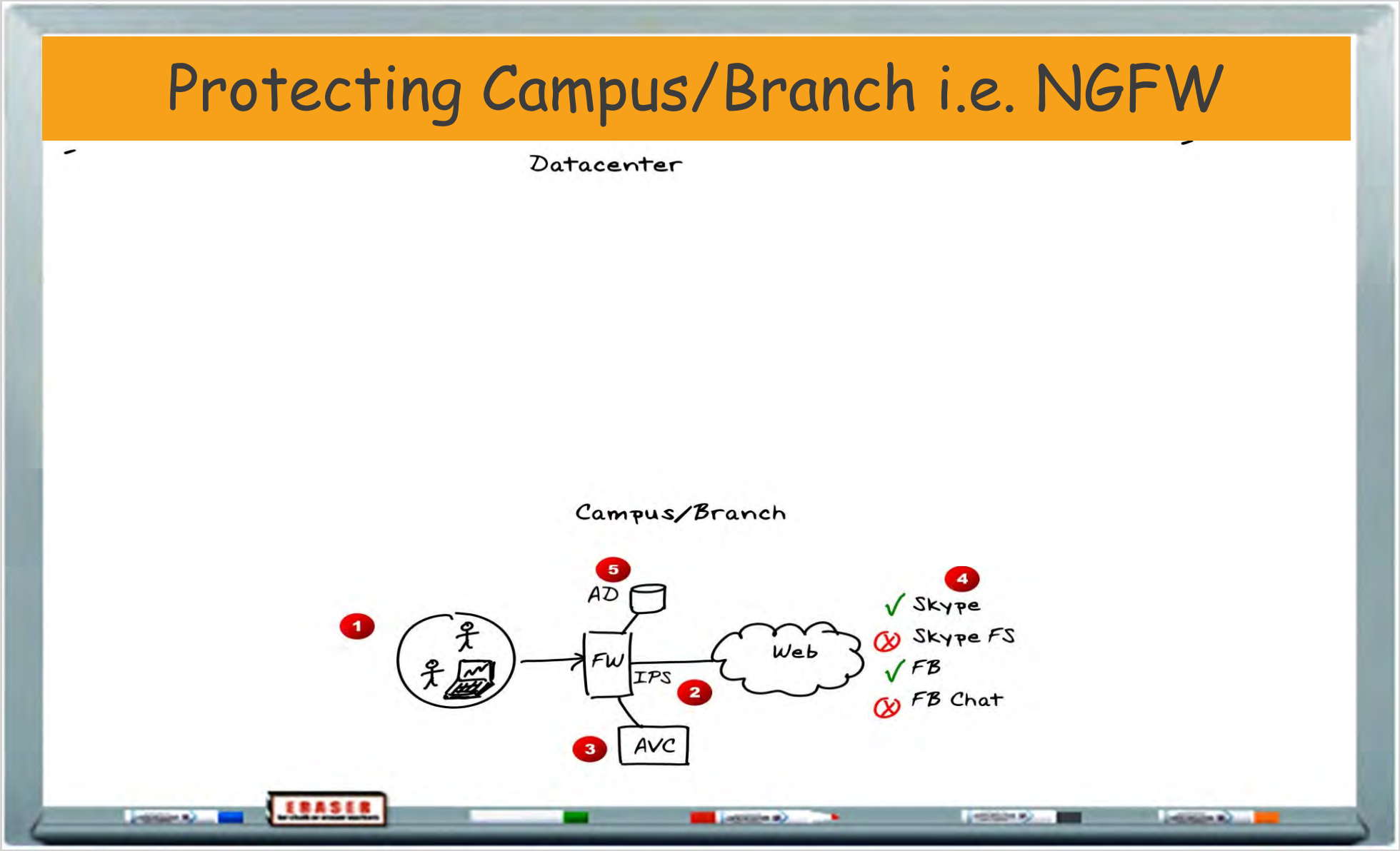
WHITEBOARDING

What Problems are we Solving?

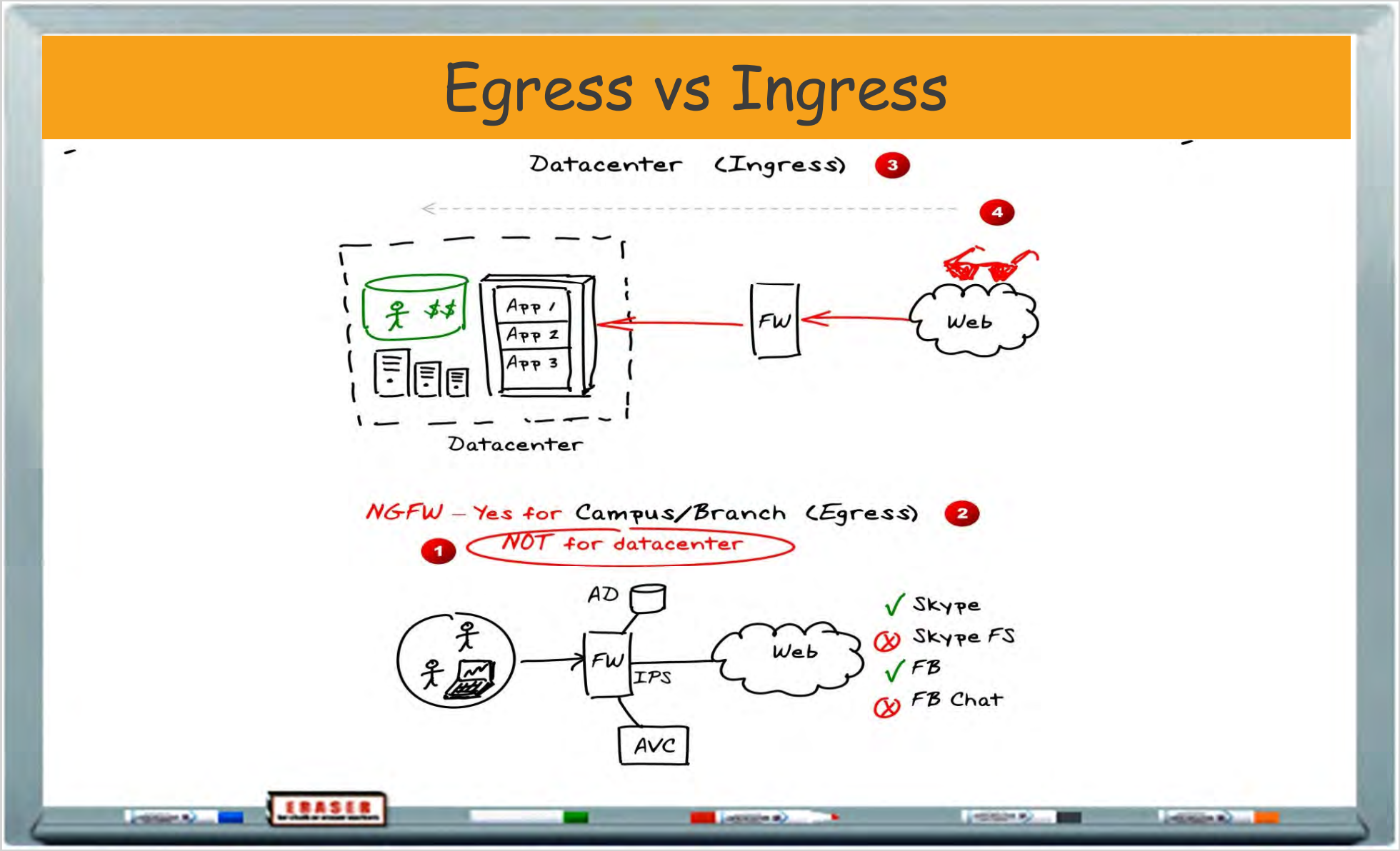
1. Datacenter

2. Campus/Branch

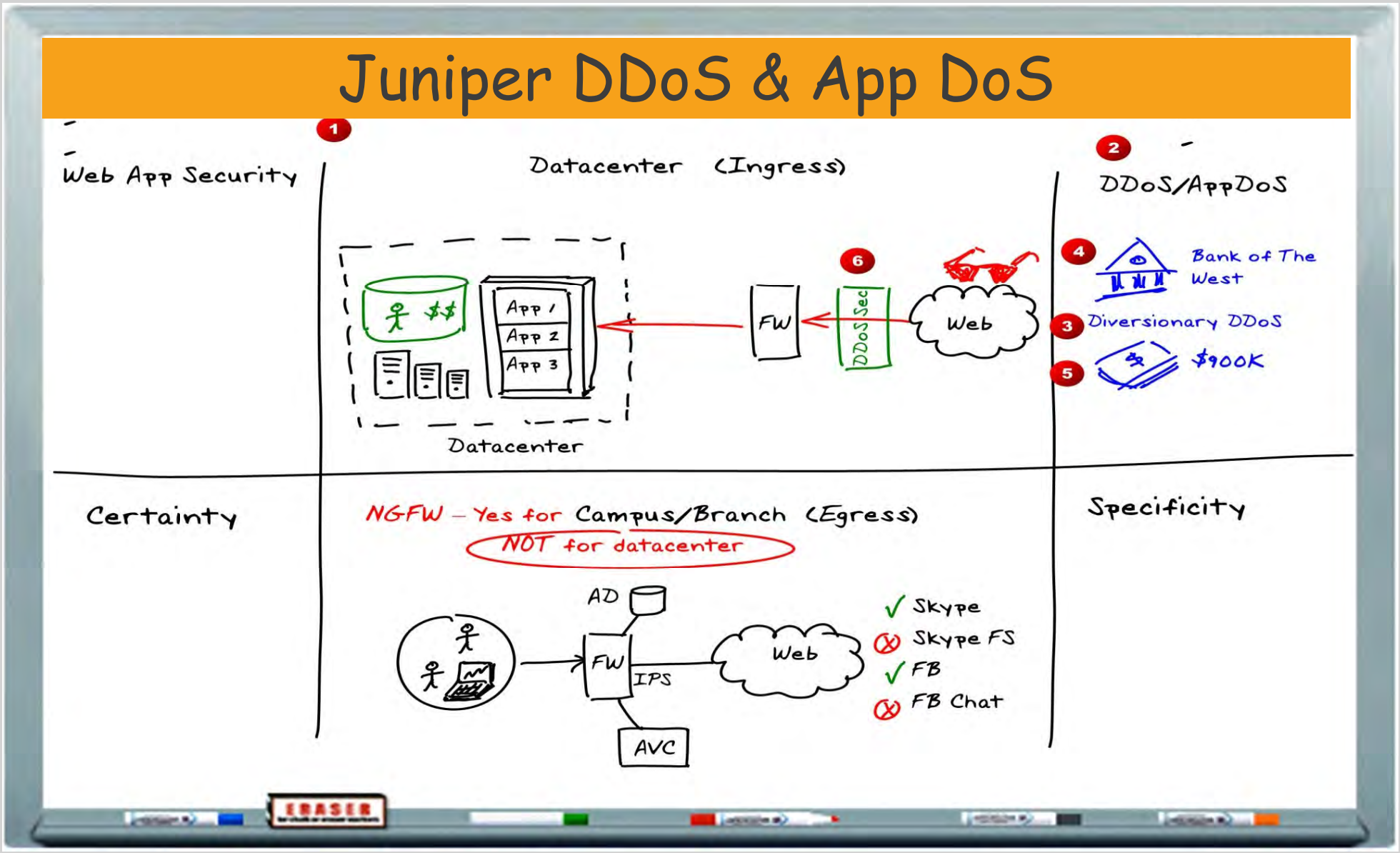
Protecting Campus/Branch i.e. NGFW



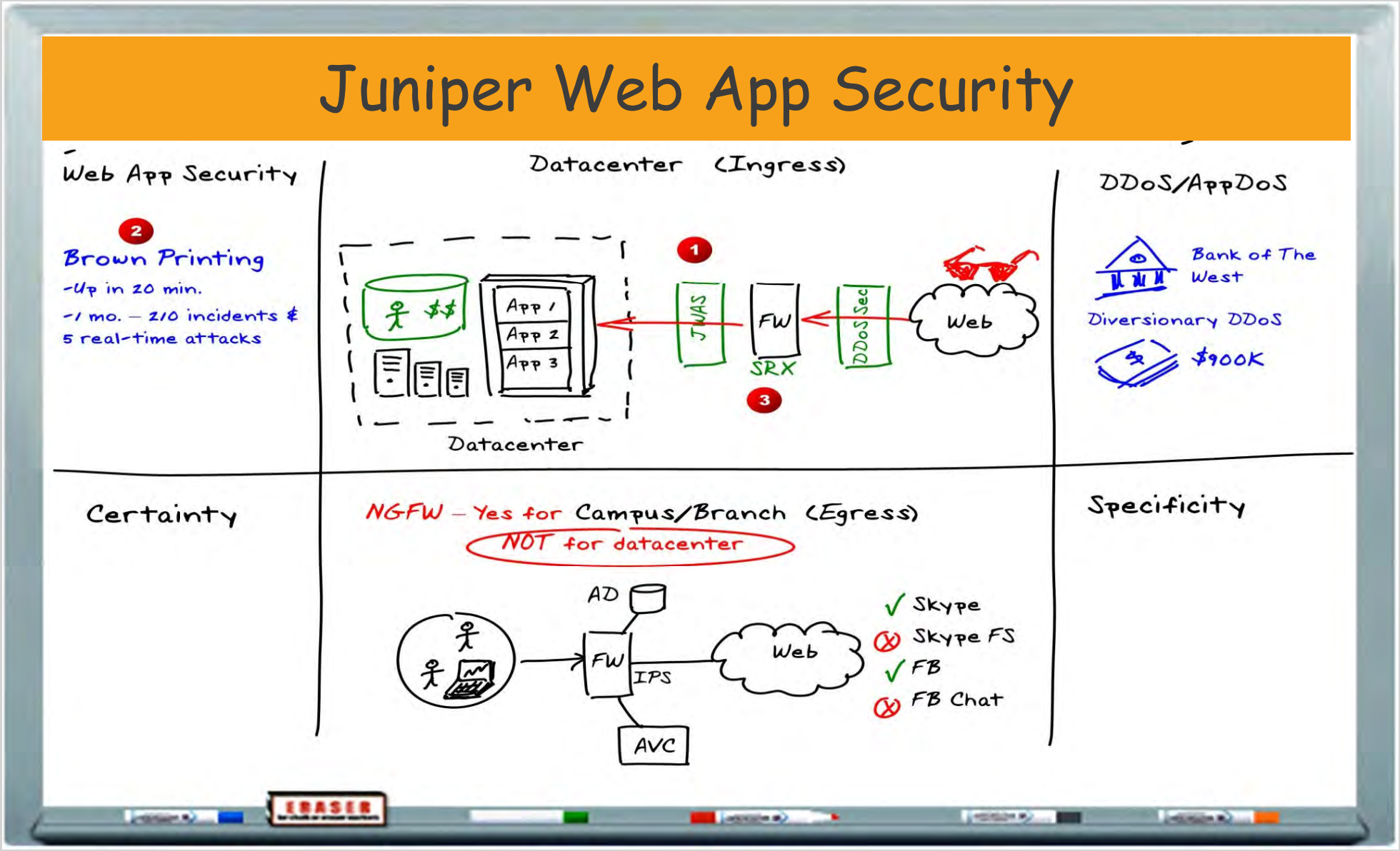
Egress vs Ingress



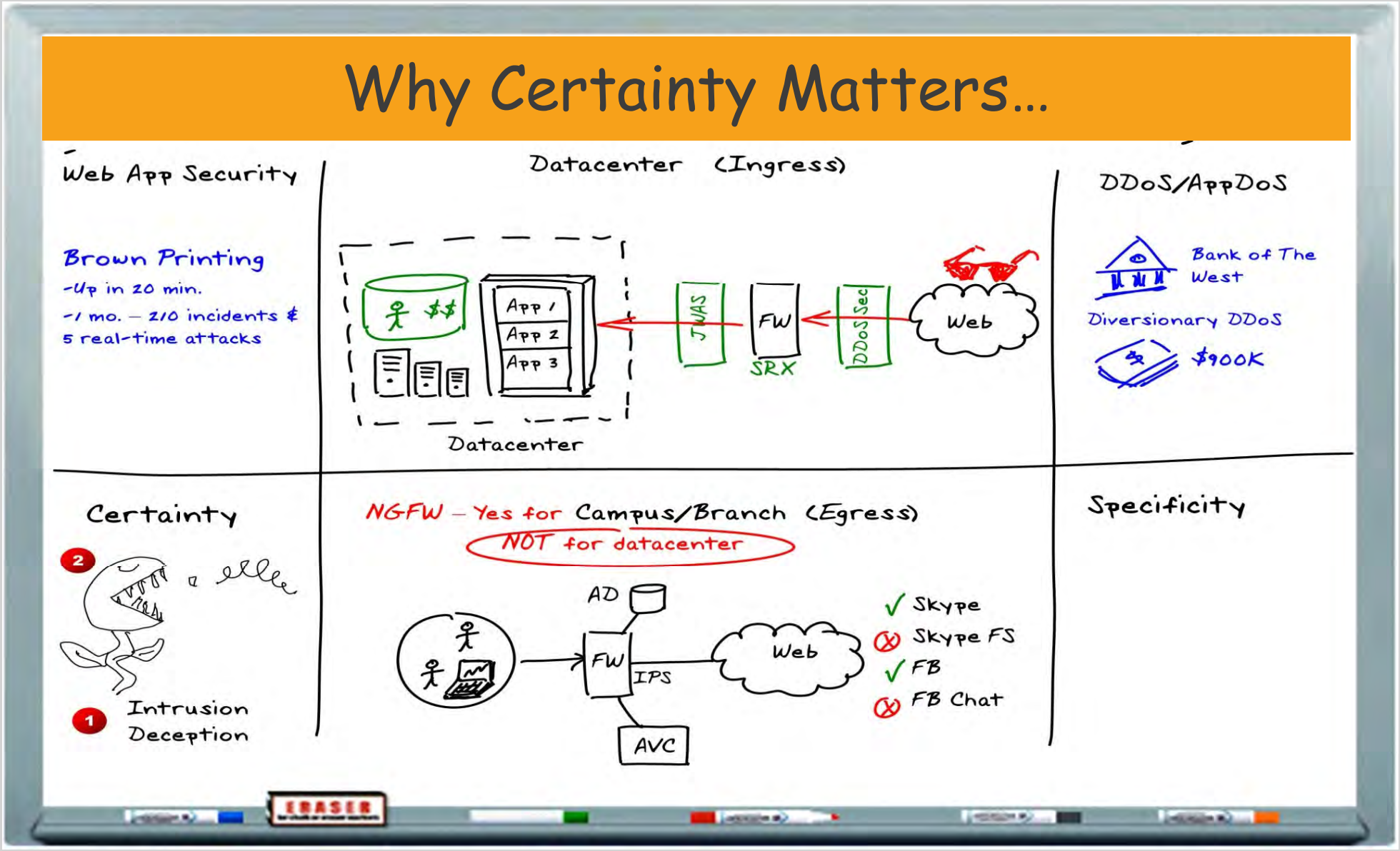
Juniper DDoS & App DoS



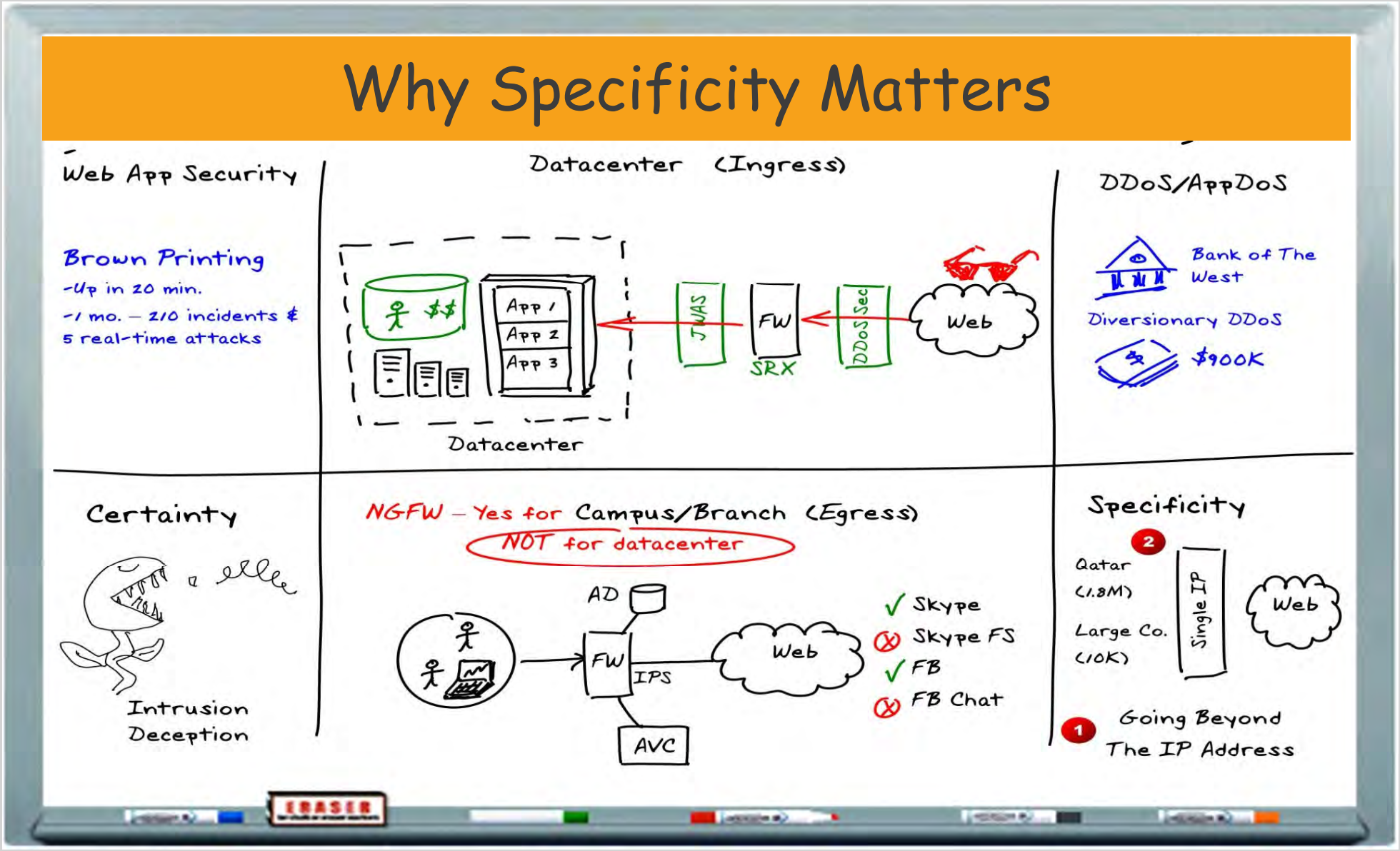
Juniper Web App Security



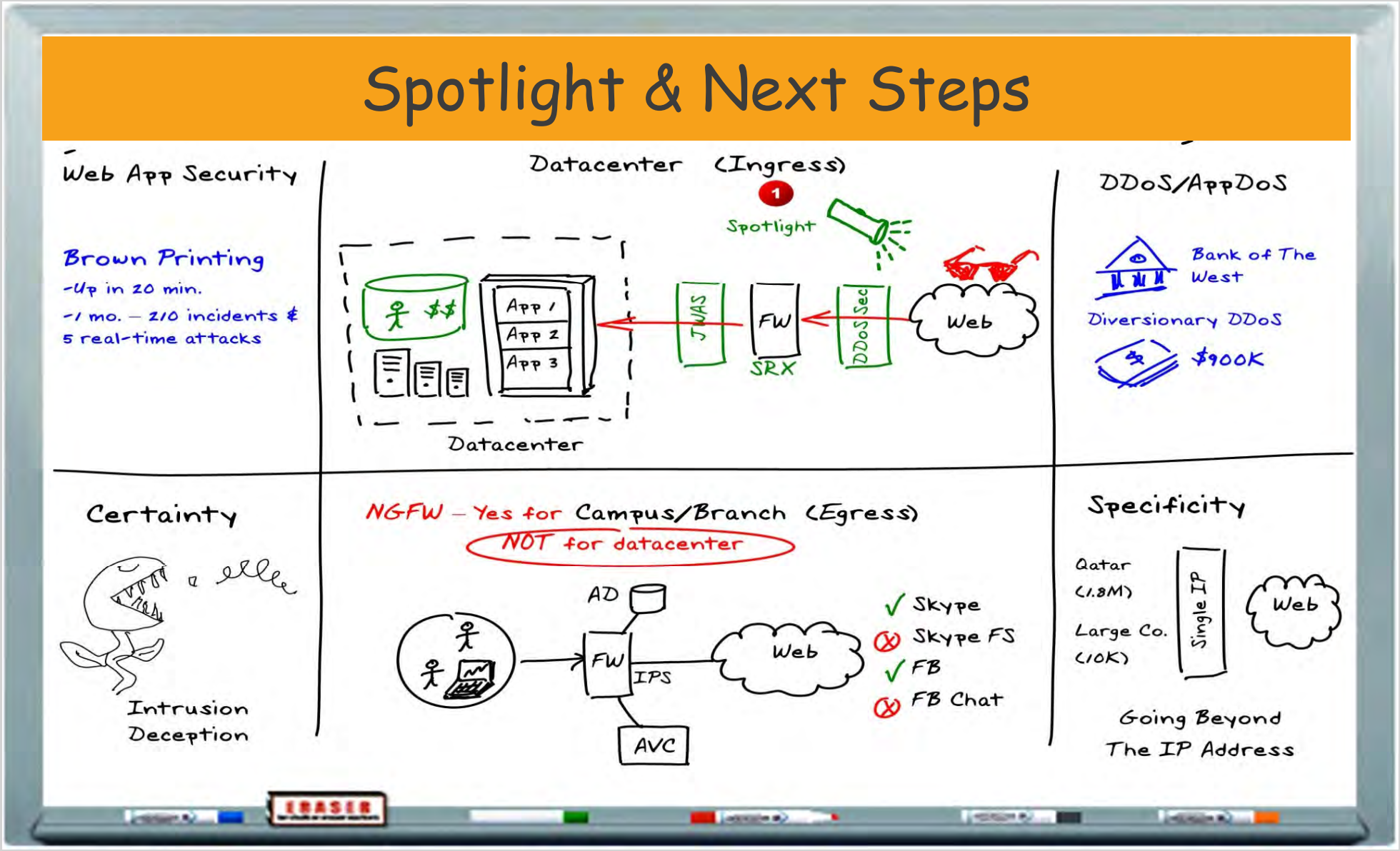
Why Certainty Matters…



Why Specificity Matters



Spotlight & Next Steps



THANK YOU!

FOR MORE INFO PLEASE VISIT:
WWW.JUNIPER.NET