NEXT-GENERATION APPLICATION SECURITY FOR TODAY’S MODERN DATA CENTER

Chris Christiansen

Program Vice President Security Products
and Services Group

IDC

David Koretz

Vice President of Security Products,
Strategy & GM Counter Security

Juniper Networks

OUR SPEAKERS

Chris Christiansen

Program Vice President Security Products and Services Group

IDC

David Koretz

Vice President of Security Products, Strategy & GM Counter Security

Juniper Networks

Data Center Security:

Threats and Solutions for Enterprise vs. Campus/Branch

Juniper/IDC Webinar presented by:

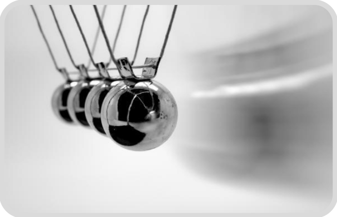
Christian Christiansen

Program Vice President

IDC Security Products & Services

Agenda

Widening Gap



Threats and Defenses:
Enterprise vs. Campus/Branch

Recommendations

IT Buyer Issues in 2013

Reduce Costs

- Consolidate
- Virtualize
- Automate
- Optimize
- Host/Outsource

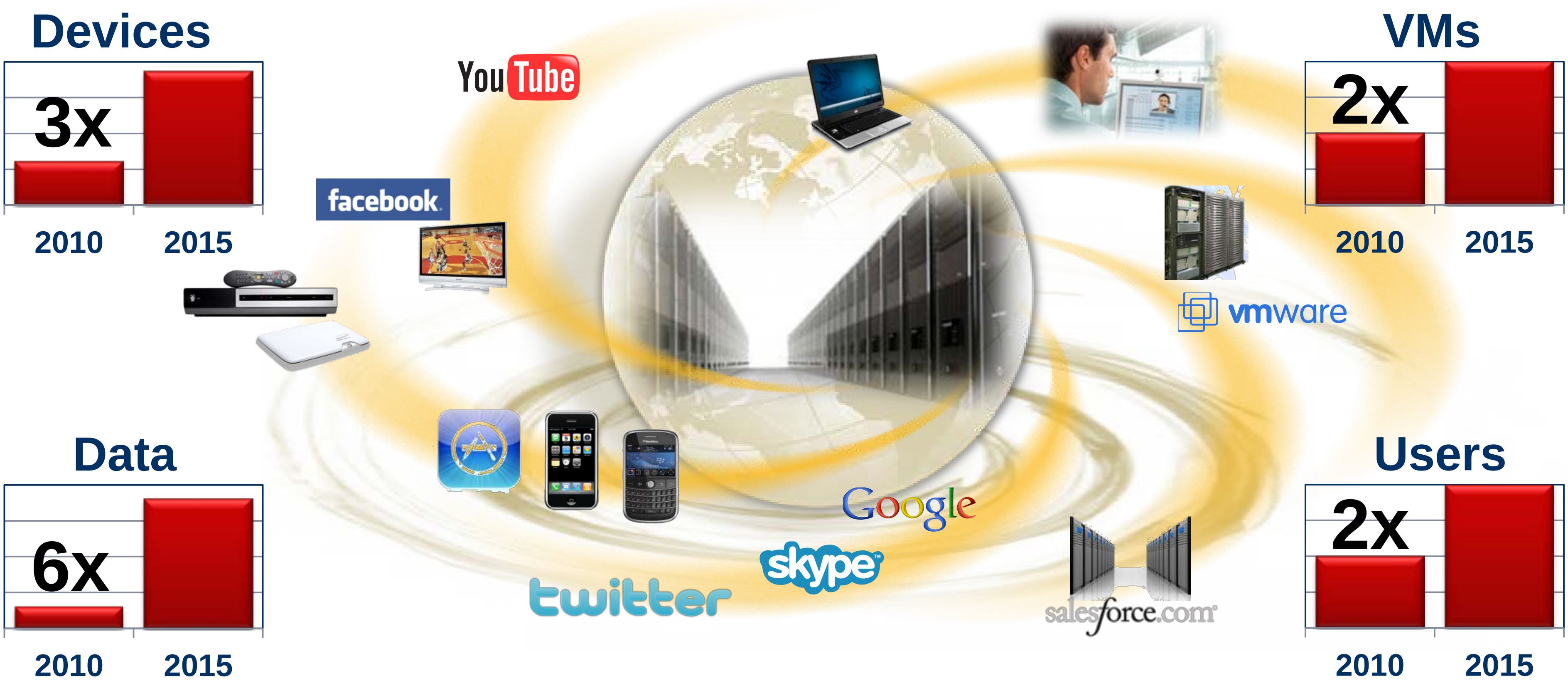
Biz Alignment

- Biz Efficiency
- Innovate
- Modernize
- Mobile/Social
- Biz Analytics

Risk Management

- Mission Critical
- Biz Continuity
- Disaster Recovery
- Security
- IT Governance
- Compliance

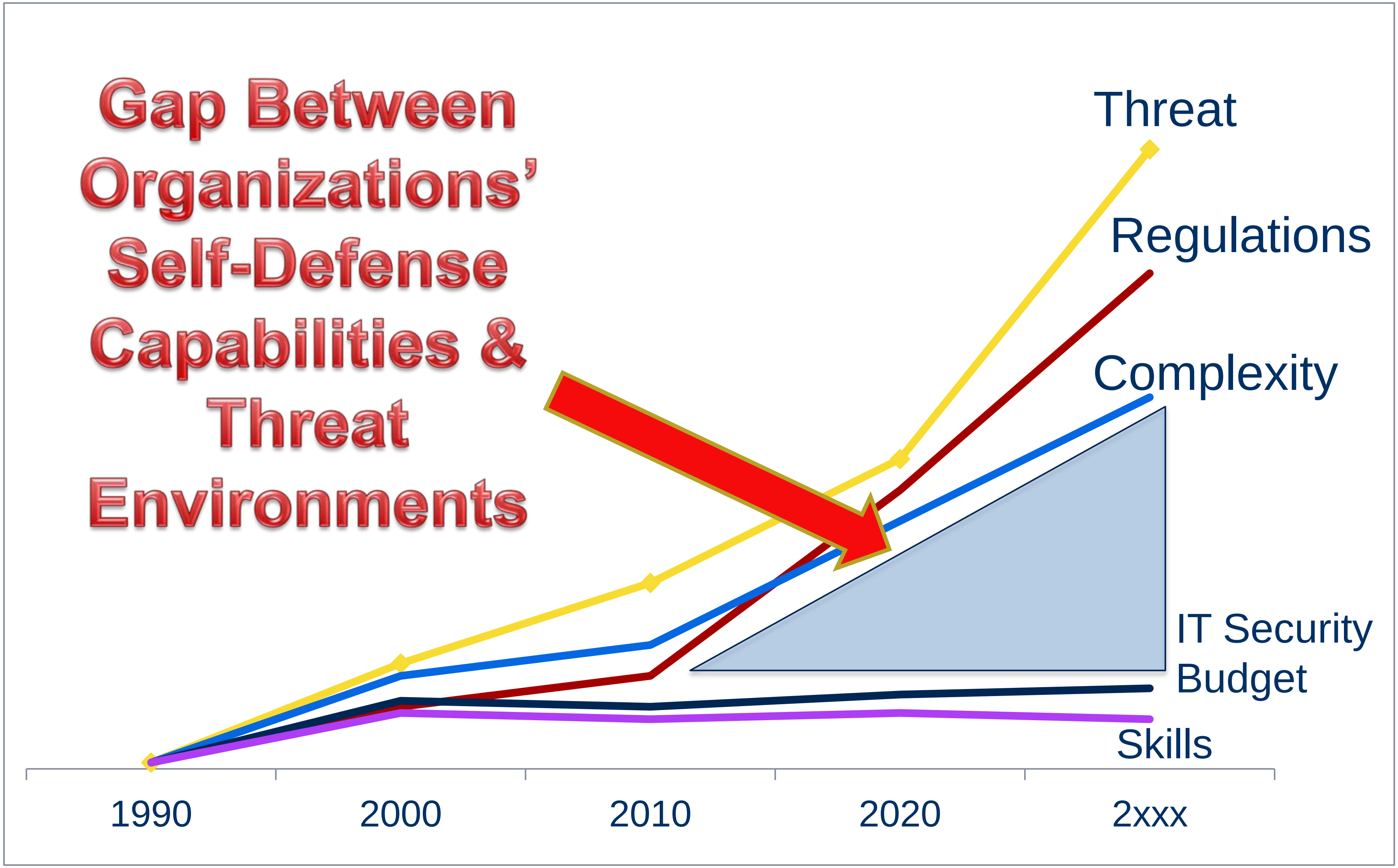
Explosion in Devices and Data Challenges the Datacenter



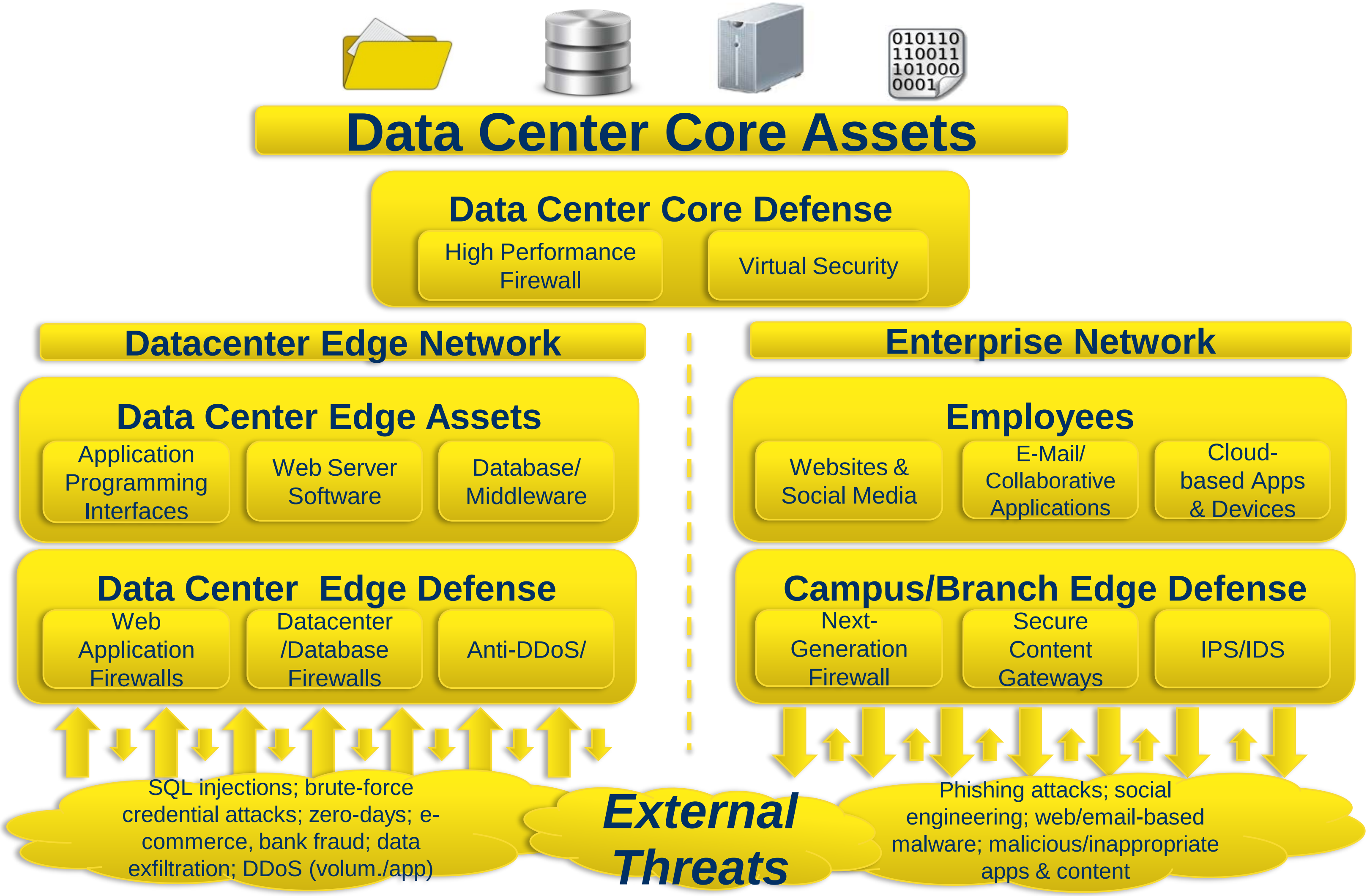
Security To Do List

- Protect IT assets (clicks & mortar): Infrastructure, hardware, data, information, knowledge and experience
- Protect IT users: Wherever they are, whatever they are connecting with, whoever they are talking to
- Protect and defend intangible corporate assets: brand reputation, key processes, business confidentiality
- Respect laws, regulations, policies, bodies, etc.
- Downsize the budget…
- Love cloud computing… (or try to!)
- Face security solution sprawl

Increasing Security Gap



Threat & Defenses Differ Between Data Center & Campus/Branch



Data Center Core Assets

Data Center Core Defense

- High Performance Firewall
- Virtual Security

Datacenter Edge Network

Data Center Edge Assets

- Application Programming Interfaces
- Web Server Software
- Database/ Middleware

Data Center Edge Defense

- Web Application Firewalls
- Datacenter /Database Firewalls
- Anti-DDoS/

SQL injections; brute-force credential attacks; zero-days; e-commerce, bank fraud; data exfiltration; DDoS (volum./app)

Enterprise Network

Employees

- Websites & Social Media
- E-Mail/ Collaborative Applications
- Cloud-based Apps & Devices

Campus/Branch Edge Defense

- Next-Generation Firewall
- Secure Content Gateways
- IPS/IDS

Phishing attacks; social engineering; web/email-based malware; malicious/inappropriate apps & content

External Threats

Source: IDC

Applications & Data Differences

Data Center Core

- Inside perimeter
- Strictly internal applications & data
- Back office operations

Datacenter Edge

- Externally facing applications & data
- Focus on customer & anonymous user access

Campus/Branch

- Real perimeter
- Focus on egress points of network
- Employee access

Network Traffic Differences

Data Center Core

- All internal traffic
- Hardly any external traffic

Datacenter Edge

- Mostly Inbound traffic (internal & external sources)
- Little outbound traffic
- Externally facing web applications (customer portals)

Campus/Branch

- Mostly outbound traffic from internal sources
  - Employees
  - Web services
  - Applications

Security Problems & Solutions

Data Center Core

- Virtualized & physical assets require scalability & performance
- Highly targeted attacks with planning & reconnaissance
- Largely immune to DDOS because of authentication/authorization
- Solutions: High performance FW, virtualized security, centralized policy

Datacenter Edge

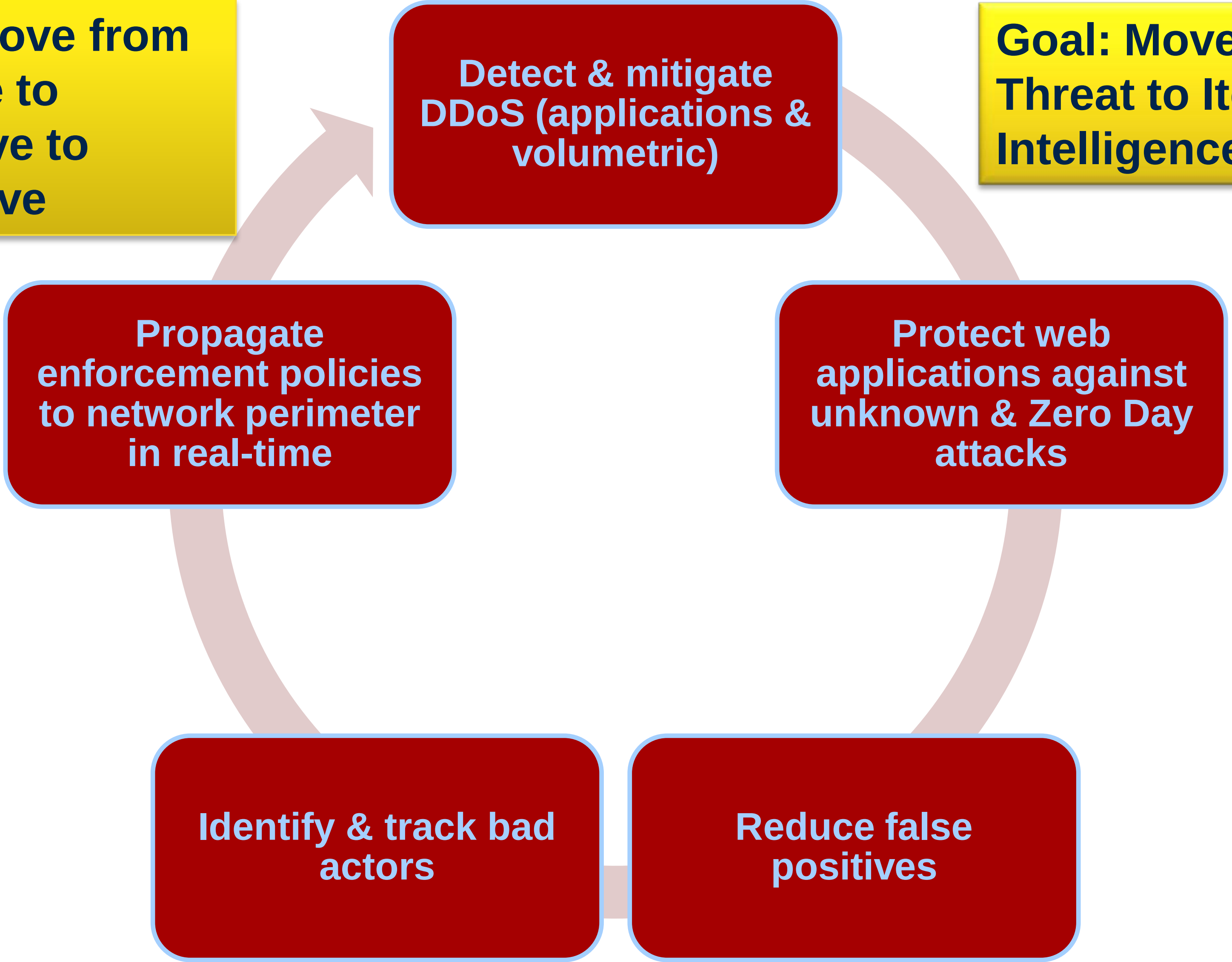
- Large groups of unknown/anonymous users
- Needs availability, response time, avoidance of false positives, granular filtering, discriminate between users & attackers
- Attacks: automated/manual vulnerability analysis, SQL injection, privilege escalation, DDOS masking of other attacks
- Solutions: DDOS mitigation, L7 defense, web security, integration with perimeter FW

Campus/Branch

- High traffic volumes from internal and supposedly trusted sources, productivity issues, accidental malware infections, business disruptions
- Attacks: phishing, social engineering, web based malware
- Solutions: multi-function with integrated applications control, user/device authentication, intrusion prevention, malware scanning

Two Goals & 5 Key Requirements for Effective Data Center Security

Goal: Move from reactive to proactive to predictive



Detect & mitigate DDoS (applications & volumetric)

Protect web applications against unknown & Zero Day attacks

Reduce false positives

Identify & track bad actors

Propagate enforcement policies to network perimeter in real-time

Goal: Move from Threat to Iterative Intelligence

Final Thoughts….

- CIOs pay attention to time, money and people
- Workloads differ across datacenter core, datacenter edge, and campus/branch
- Attacks & security solution differ markedly by datacenter type
- One size security solutions do not work
- Different solutions needed for different environments

Contact Information

Email me at:

cchristiansen@idc.com

Follow me at:

twitter.com/@cchristiansen

SECURITY AT THE DATA CENTER EDGE AND CORE

David Koretz, Vice President of Security Products, Strategy & GM Counter Security

Juniper Networks

AGENDA

1. Different security needs in campus and data center
2. The Problem of Known v Unknown Attacks
3. New techniques detecting the unknown attack
4. Data Center Security Solution

DIFFERING SECURITY NEEDS

Campus Edge

- 5 Tuple Firewall
- Integrated IPS
- Extra Firewall Intelligence (AD integration) for User Control
- Application Visibility and Control

Datacenter Edge

- Web Application Security
- DDoS Mitigation
- Zero False Positives
- High Availability of Critical Business Resources

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 – lack of consistent enforcement at the enterprise edge

Sources: KRC Research and Juniper Mobile Threat Center

THE PROBLEM OF SIGNATURE-BASED SECURITY

40

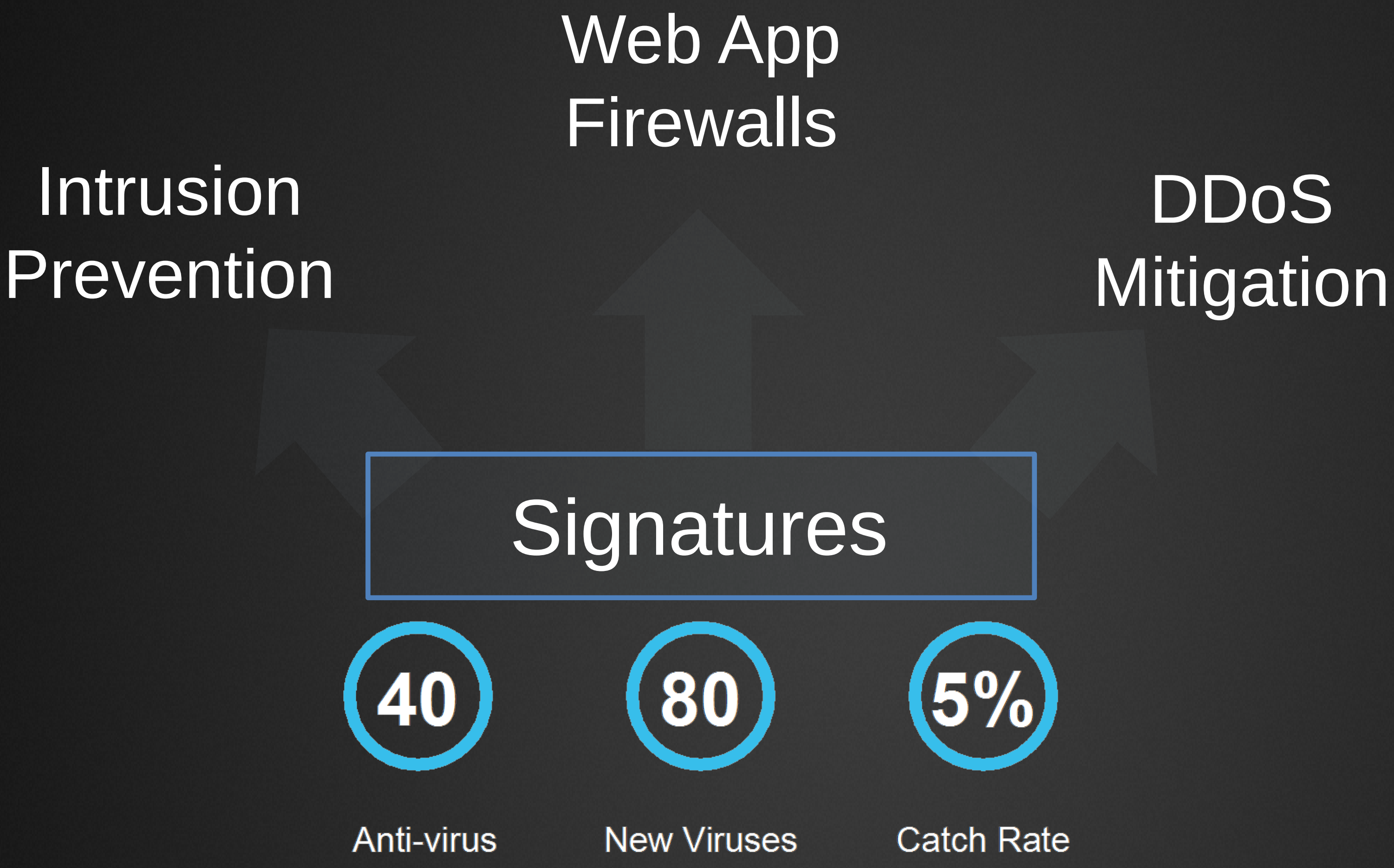
Anti-virus

80

New Viruses

5%

Catch Rate



Web App Firewalls

Intrusion Prevention

DDoS Mitigation

Signatures

40

Anti-virus

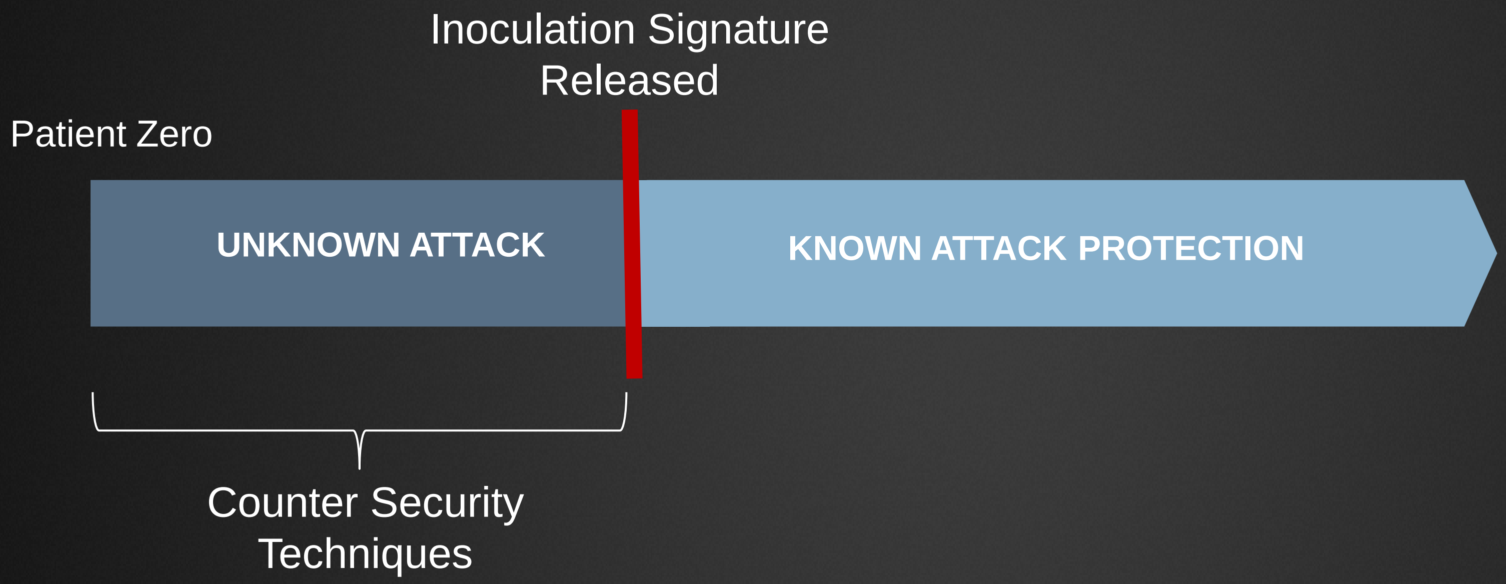
80

New Viruses

5%

Catch Rate

NO-ONE WANTS TO BE PATIENT ZERO



THREE NEW TECHNIQUES IN DATACENTER SECURITY

INTRUSION DECEPTION

Detects and blocks unknown hackers attacking Web applications

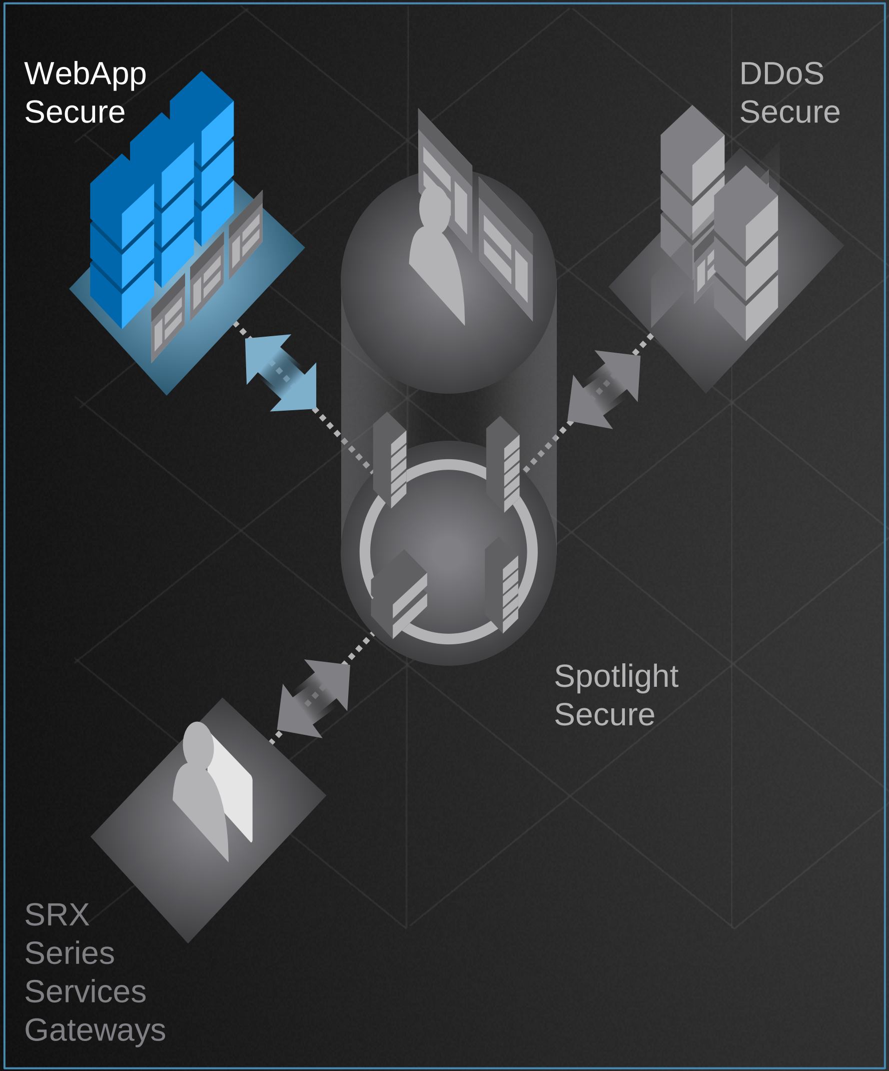
CHARM SCORE & CLOSED LOOP PROCESS

Detects and mitigates unknown DDoS attacks

DEVICE FINGERPRINTING

Uses shared knowledge from previous attacks to prevent serial unknown attackers

NEXT GENERATION DATACENTER SECURITY: WEBAPP SECURE



WebApp Secure

What it is

- Continuously monitors web apps to stop hackers and botnets
- Collects forensic data on hacker device, location, and methods
- Continuously updates on-board hacker profile information

Why it’s different

- Accurate threat mitigation with near-zero false positives
- Hacker profile sharing for global protection surface
- Flexible deployment (i.e., appliance, VM, AWS)

Spotlight Secure

DDoS Secure

SRX Series Services Gateways

INTRUSION DECEPTION

Detect

“Tar Traps” detect threats without false positives.

Track

Track IPs, browsers, software and scripts.

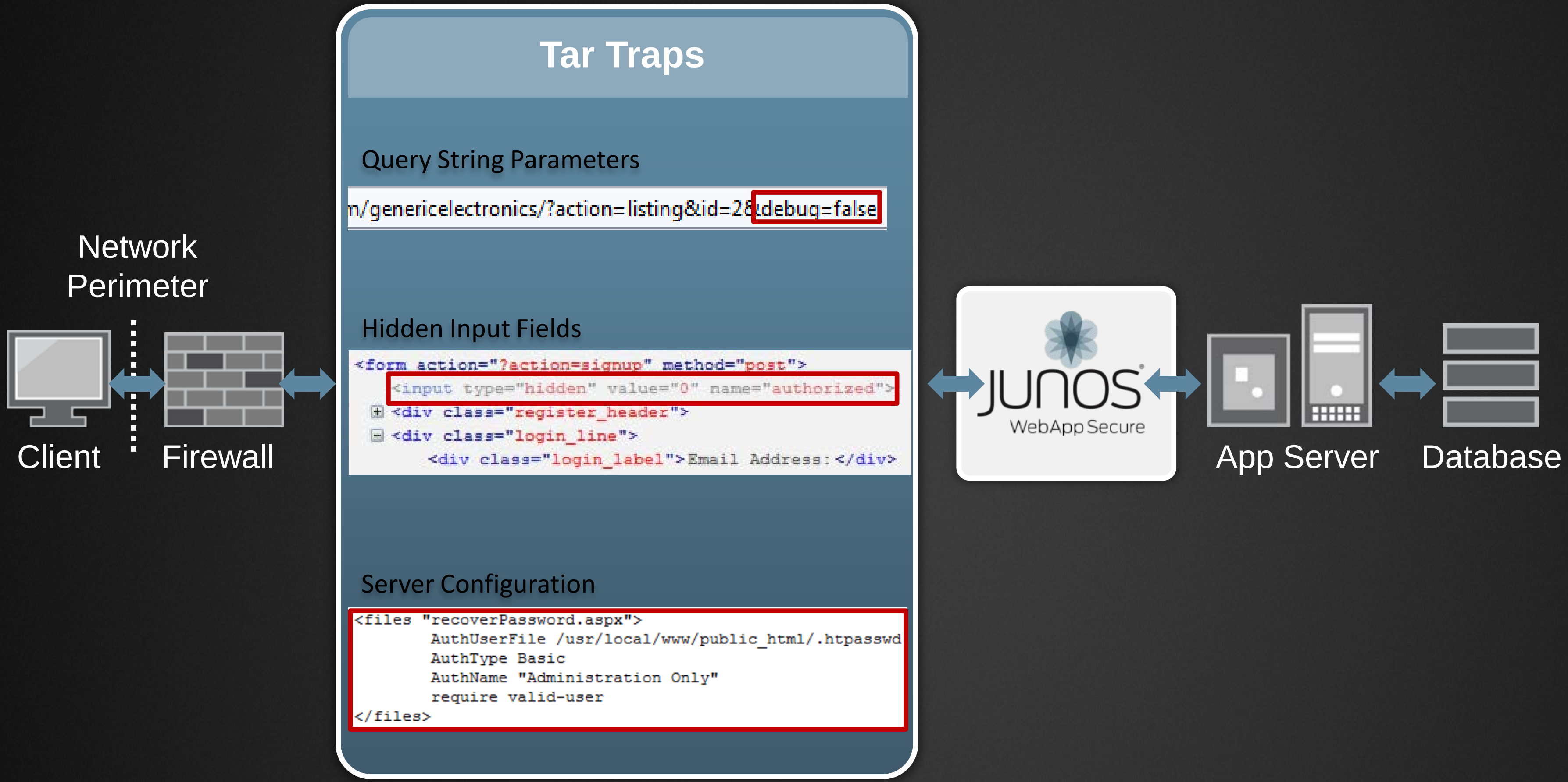
Profile

Understand attacker’s capabilities and intents.

Respond

Adaptive responses, including block, warn and deceive.

DETECTION BY DECEPTI0N



Query String Parameters

```
n/genericelectronics/?action=listing&id=2&debug=false
```

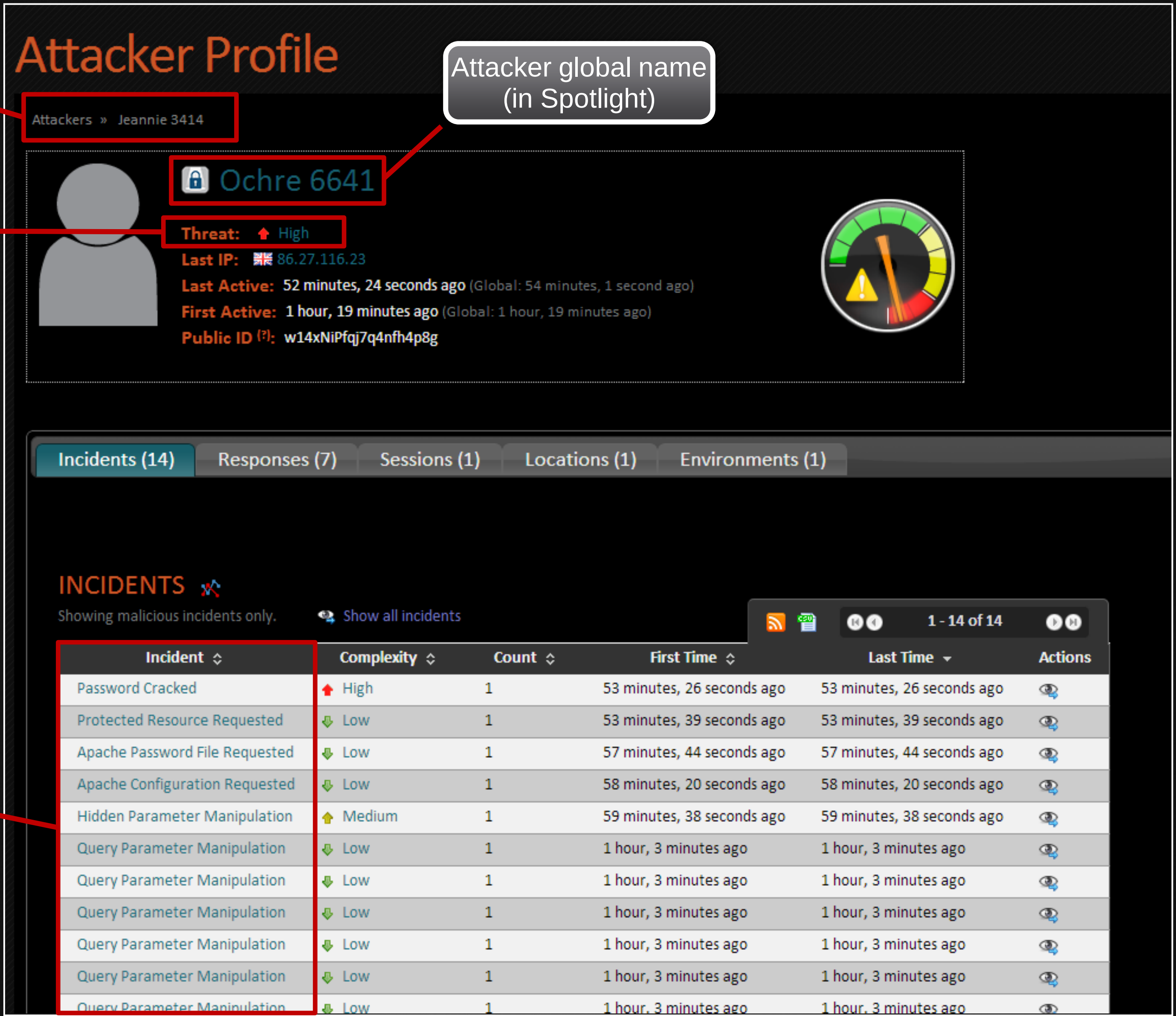
Hidden Input Fields

```
<form action="?action=signup" method="post">
    <input type="hidden" value="0" name="authorized">
  ⊞ <div class="register_header">
  ⊟ <div class="login_line">
        <div class="login_label">Email Address: </div>
```

Server Configuration

```
<files "recoverPassword.aspx">
        AuthUserFile /usr/local/www/public_html/.htpasswd
        AuthType Basic
        AuthName "Administration Only"
        require valid-user
</files>
```

SMART PROFILE OF ATTACKER



Attacker local name (on machine)

Attacker threat level

Attacker global name (in Spotlight)

Incident history

Attacker Profile

Attackers » Jeannie 3414

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

INCIDENTS

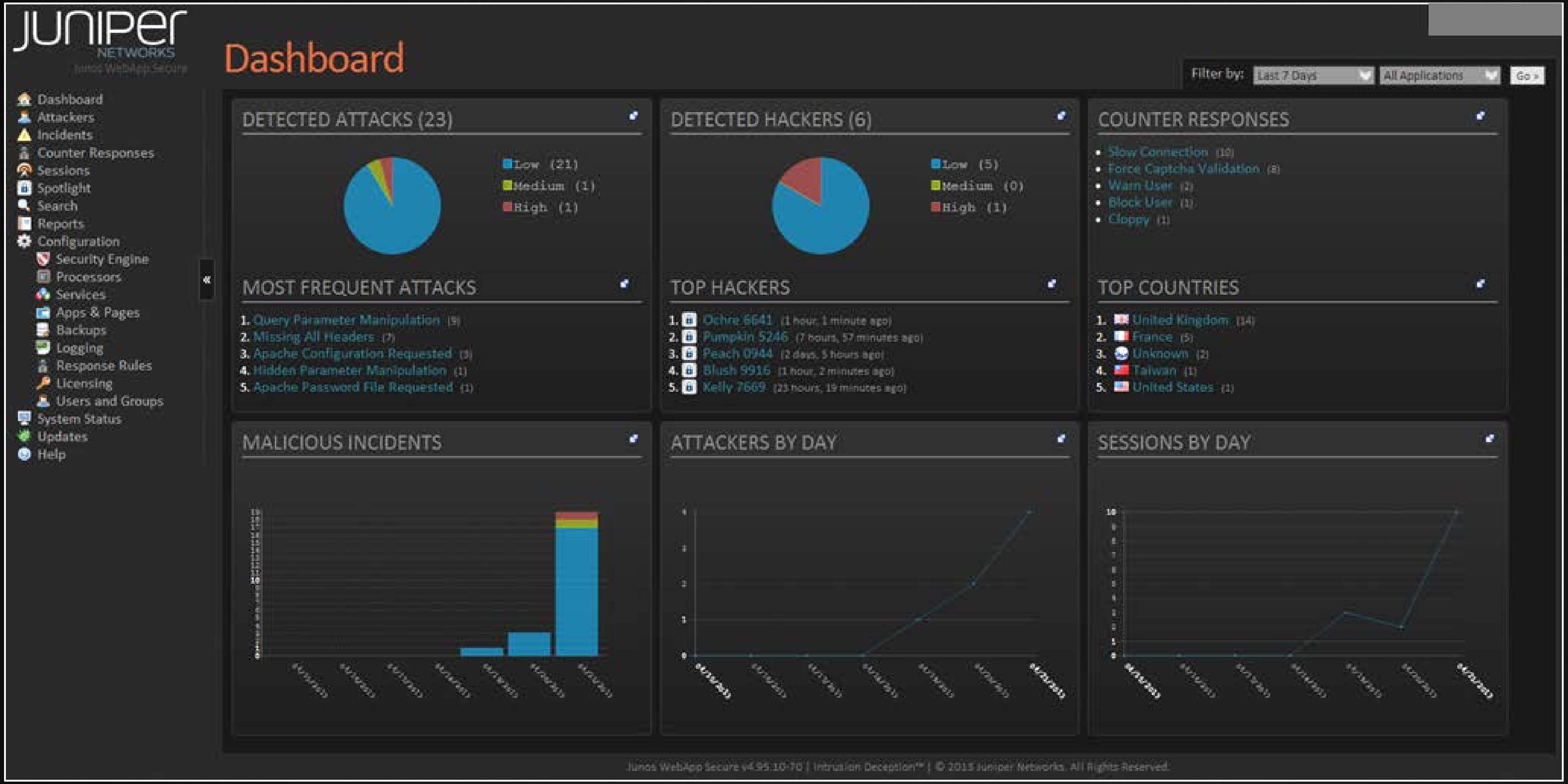
Showing malicious incidents only.

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	👁

REAL-TIME VISIBILITY



Dashboard

DETECTED ATTACKS (23)

DETECTED HACKERS (6)

COUNTER RESPONSES

- Slow Connection (10)
- Force Captcha Validation (8)
- Warn User (2)
- Block User (1)
- Cloppy (1)

MOST FREQUENT ATTACKS

1. Query Parameter Manipulation (9)
2. Missing All Headers (7)
3. Apache Configuration Requested (3)
4. Hidden Parameter Manipulation (1)
5. Apache Password File Requested (1)

TOP HACKERS

1. Ochre 6641 (1 hour, 1 minute ago)
2. Pumpkin 5246 (7 hours, 57 minutes ago)
3. Peach 0944 (2 days, 5 hours ago)
4. Blush 9916 (1 hour, 2 minutes ago)
5. Kelly 7669 (23 hours, 19 minutes ago)

TOP COUNTRIES

1. United Kingdom (14)
2. France (5)
3. Unknown (2)
4. Taiwan (1)
5. United States (1)

MALICIOUS INCIDENTS

ATTACKERS BY DAY

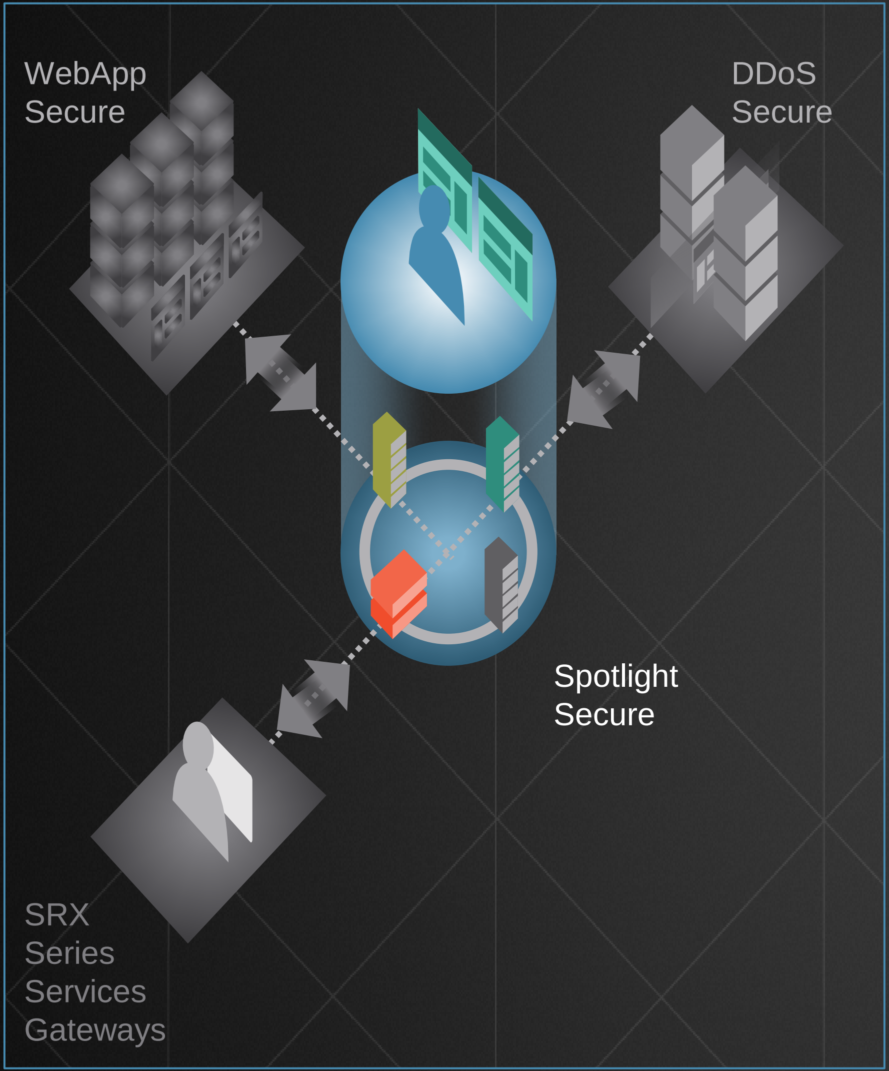
SESSIONS BY DAY

Junos WebApp Secure v4.95.10-70 | Intrusion Deception™ | © 2013 Juniper Networks. All Rights Reserved.

- Web-based console
- Real-time
- On-demand threat information

- SMTP alerting
- Reporting (PDF, HTML)
- CLI for exporting data into SIEM tool

NEXT GENERATION DATACENTER SECURITY: SPOTLIGHT SECURE INTELLIGENCE SERVICE



WebApp Secure

Spotlight Secure

What it is

- Aggregates hacker profile information from global sources in a cloud-based database
- Distributes aggregated hacker profile information to global subscribers

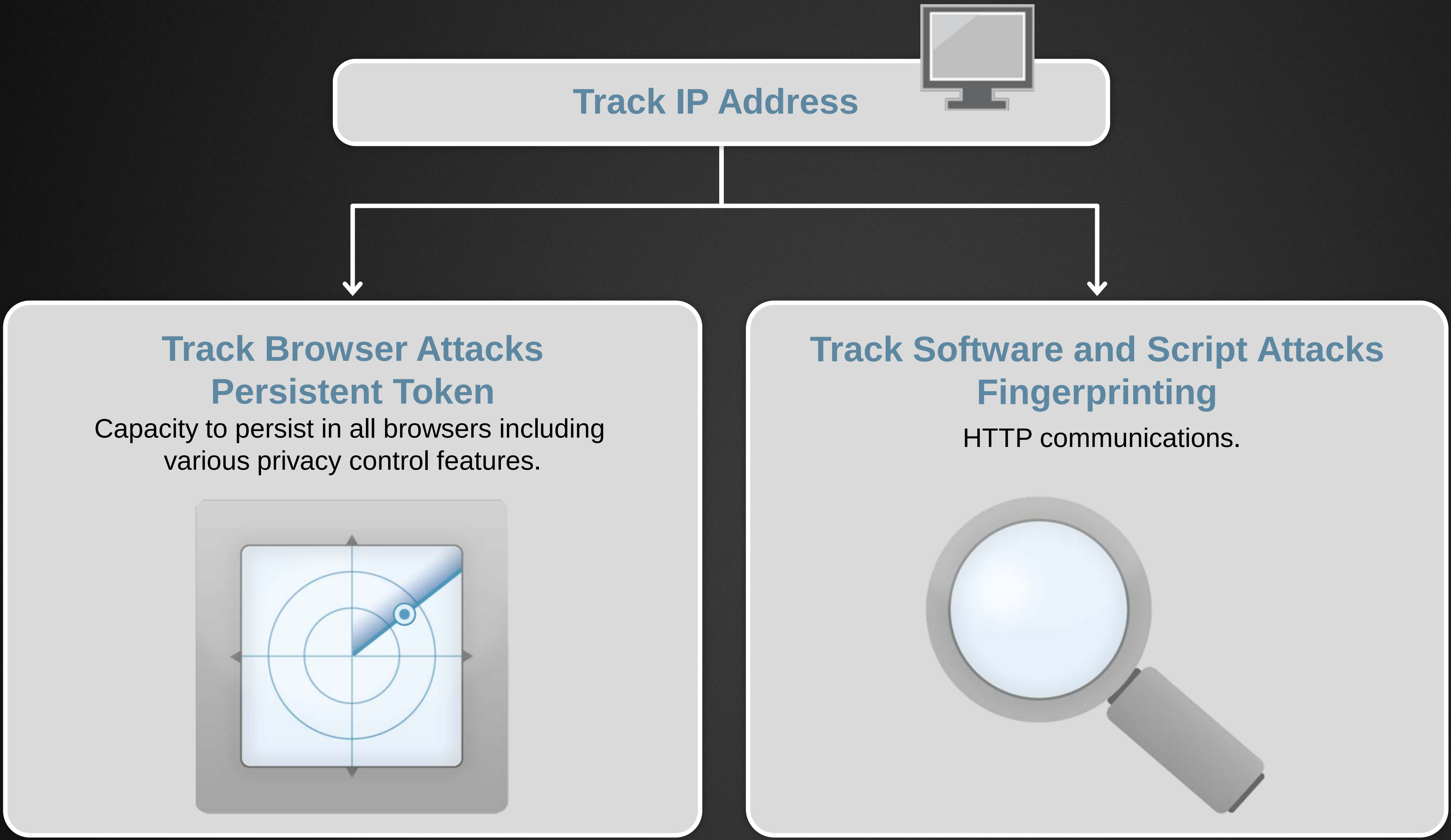
Why it's different

- High accuracy zero day attacker detection and threat mitigation
- Only solution to offer device-level hacker profiling service
- Can block a single device/attacker

DDoS Secure

SRX Series Services Gateways

TRACK ATTACKERS BEYOND THE IP



Track IP Address

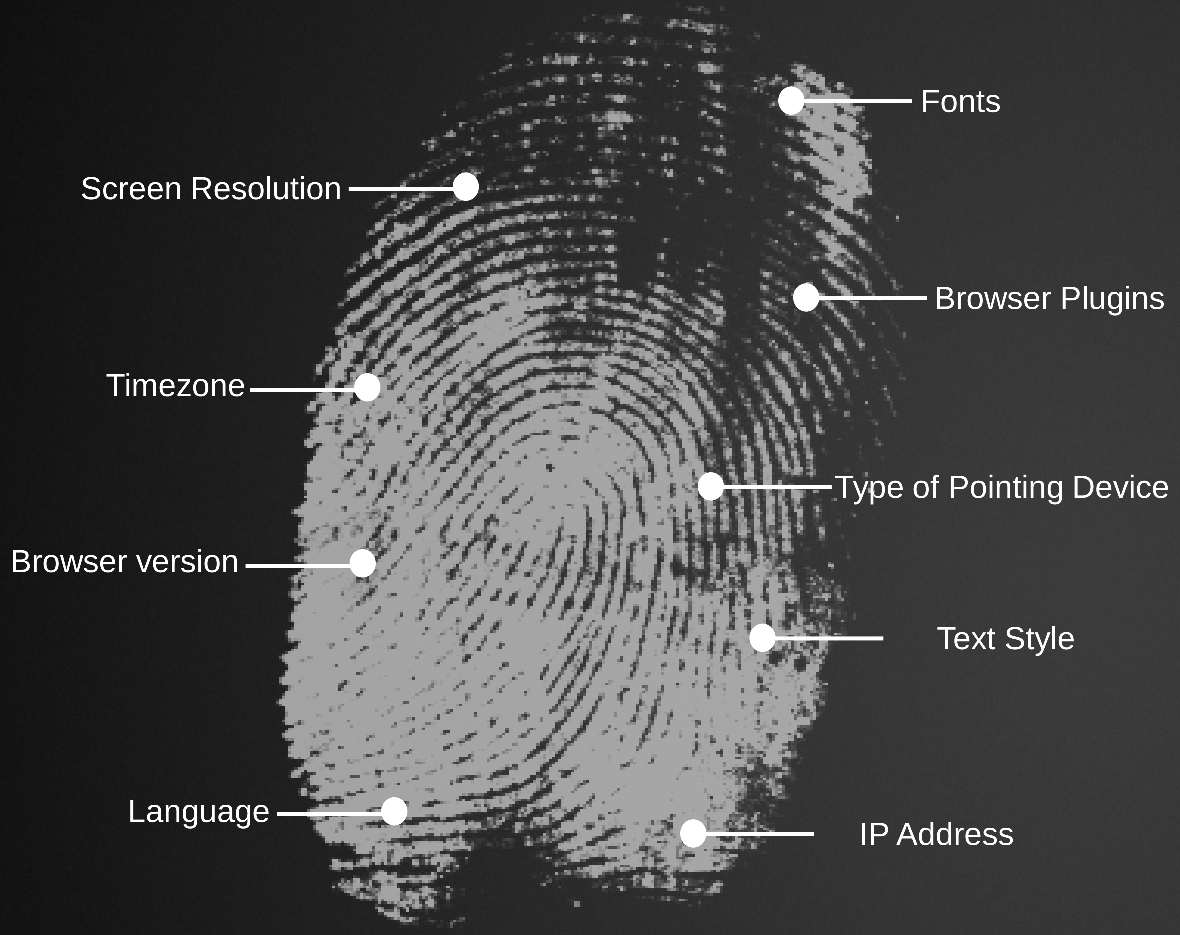
Track Browser Attacks
Persistent Token

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.

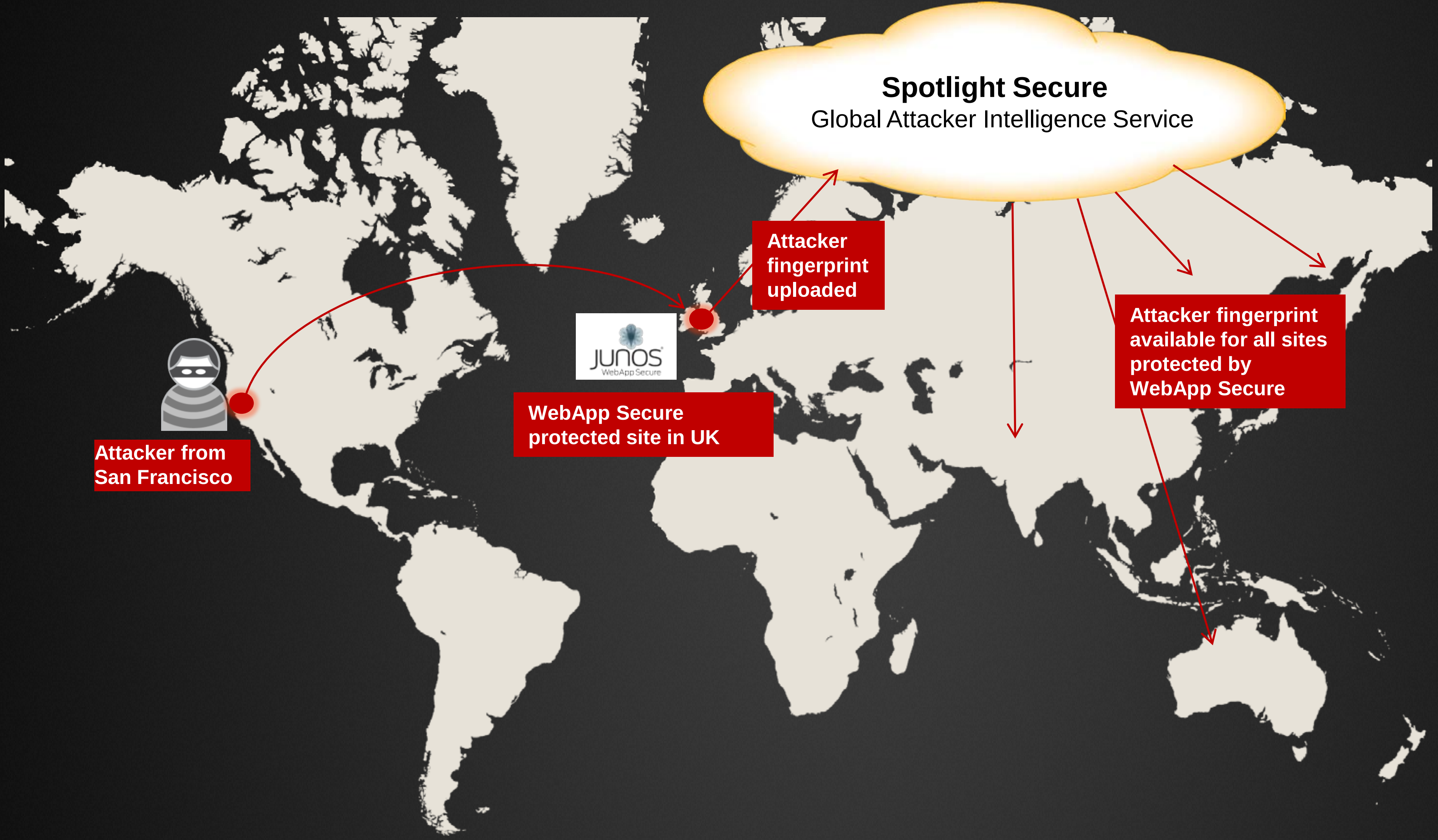
~ Real Time

availability of fingerprints

False Positives

nearly zero

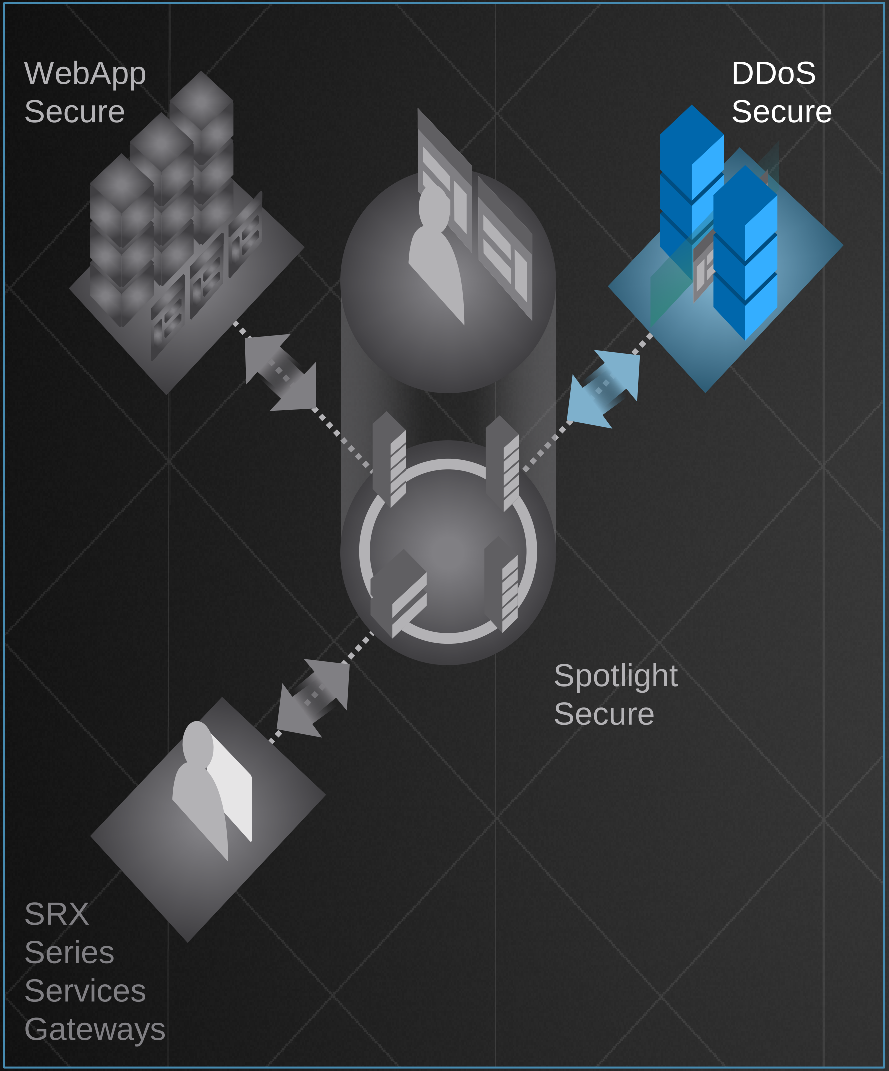
SPOTLIGHT SECURE



Spotlight Secure
Global Attacker Intelligence Service
Attacker fingerprint uploaded
JUNOS
WebApp Secure
WebApp Secure protected site in UK
Attacker from San Francisco
Attacker fingerprint available for all sites protected by WebApp Secure

Detect Anywhere, Stop Everywhere

NEXT GENERATION DATACENTER SECURITY: DDOS SECURE



Spotlight Secure

WebApp Secure

DDoS Secure

What it is

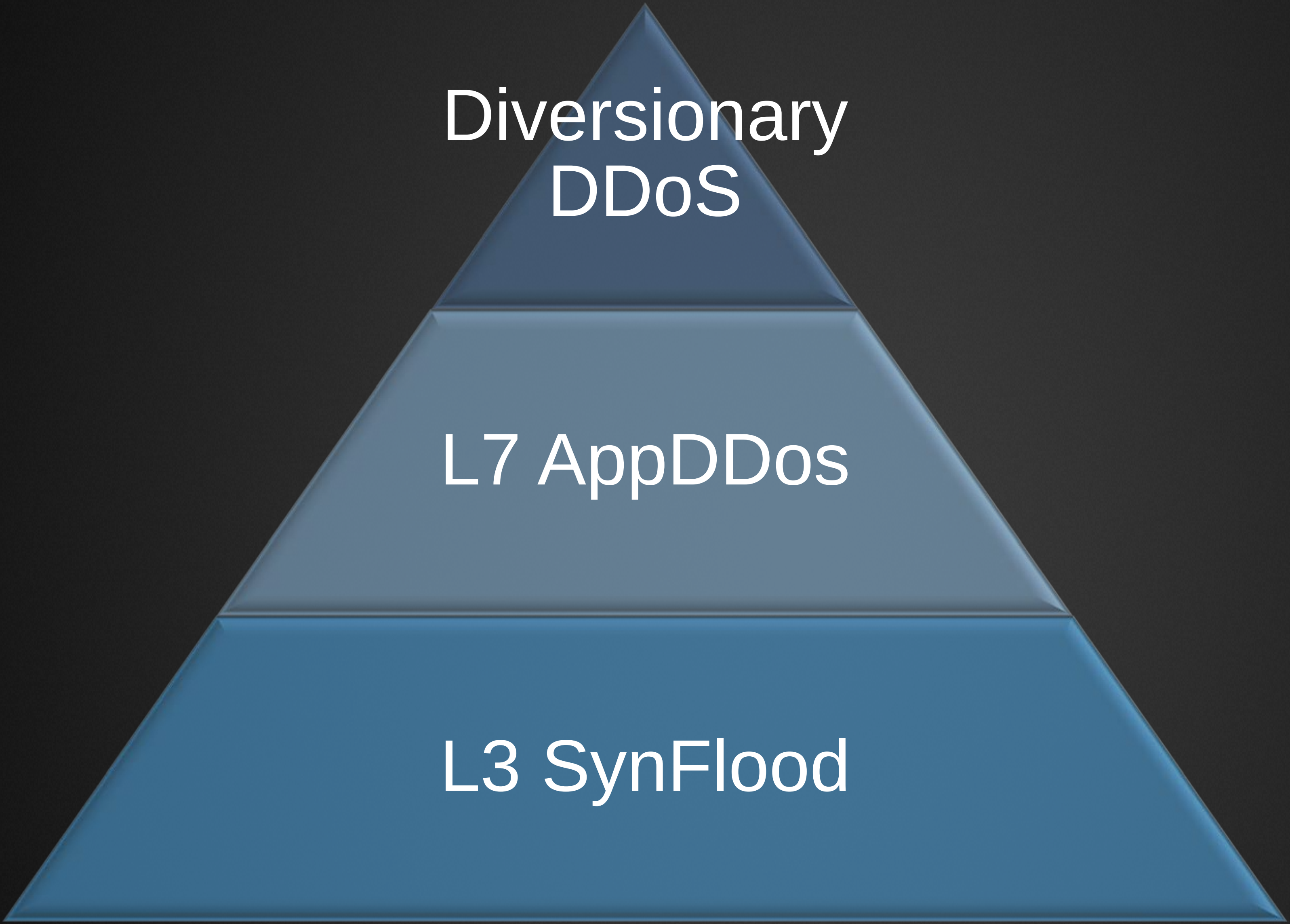
- Large-scale DDoS attack mitigation
- Slow and low DDoS attack mitigation
- Zero-day protection via combination of behavioral and rules-based detection

Why it’s different

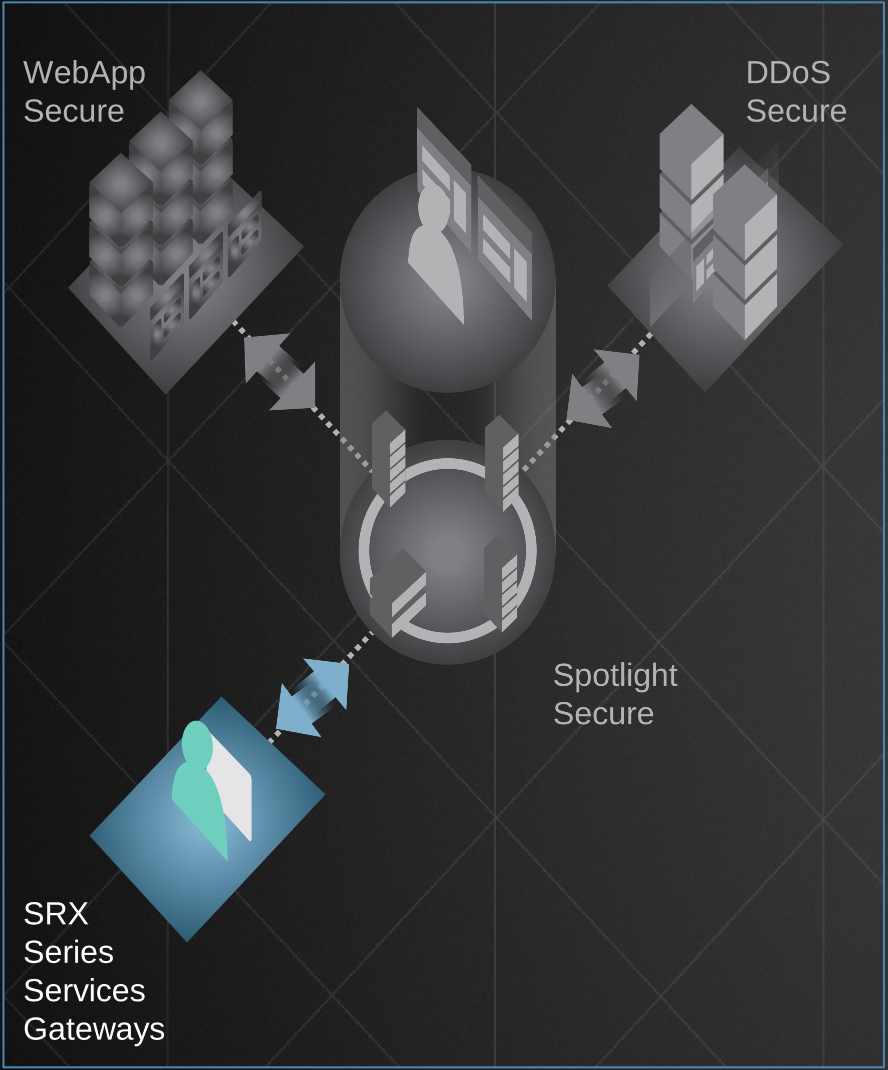
- Broadest protection with deployment ease
- Industry leading performance – 40Gb throughput
- Ease of use through automated updating
- Flexible deployment (i.e., 1U appliance, VM)

SRX Series Services Gateways

THE EVOLUTION OF DDOS



NEXT GENERATION DATACENTER SECURITY: SRX SERIES



Spotlight Secure

WebApp Secure

DDoS Secure

SRX Series Services Gateways

Value

- Investment Protection
- Scale
- Business continuity (HA, ISSU)

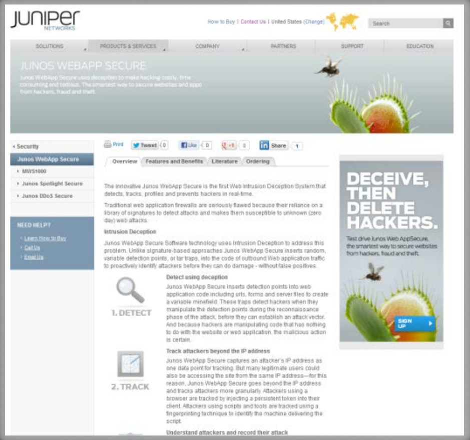
Scale

- 2X throughput increase (200G)
- 3X session scale increase (20M➔60M➔100M)
- Future SW increase with existing cards

DETECT UNKNOWN ATTACKERS LOCALLY AND PREVENT GLOBALLY

WEBAPP SECURE

Intrusion Deception



JUNOS WEBAPP SECURE

Junos WebApp Secure uses deception to make hacking costly, time consuming and tedious. The smartest way to secure websites and apps from hackers, fraud and theft.

The innovative Junos WebApp Secure is the first Web Intrusion Deception System that detects, tracks, profiles and prevents hackers in real-time.

Traditional web application firewalls are seriously flawed because their reliance on a library of signatures to detect attacks and makes them susceptible to unknown (zero day) web attacks.

Intrusion Deception

Junos WebApp Secure Software technology uses Intrusion Deception to address this problem. Unlike signature-based approaches Junos WebApp Secure inserts random, variable detection points, or tar traps, into the code of outbound Web application traffic to proactively identify attackers before they can do damage - without false positives.

Detect using deception

Junos WebApp Secure inserts detection points into web application code including urls, forms and server files to create a variable minefield. These traps detect hackers when they manipulate the detection points during the reconnaissance phase of the attack, before they can establish an attack vector. And because hackers are manipulating code that has nothing to do with the website or web application, the malicious action is certain.

Track attackers beyond the IP address

Junos WebApp Secure captures an attacker's IP address as one data point for tracking. But many legitimate users could also be accessing the site from the same IP address—for this reason, Junos WebApp Secure goes beyond the IP address and tracks attackers more granularly. Attackers using a browser are tracked by injecting a persistent token into their client. Attackers using scripts and tools are tracked using a fingerprinting technique to identify the machine delivering the script.

Understand attackers and record their attack

DECEIVE, THEN DELETE HACKERS.

Test drive Junos Web AppSecure, the smartest way to secure websites from hackers, fraud and theft.

SPOTLIGHT SECURE

Attacker Intelligence Service

SEE NETWORK SECURITY IN A WHOLE NEW LIGHT

Discover our next-generation data center security products.

UNDERSTAND THE LATEST SECURITY THREATS AND THE NEWEST TECHNOLOGY TO DEFEAT THEM.

Download the Ponemon Report.

WORRIED ABOUT WEB APPS?

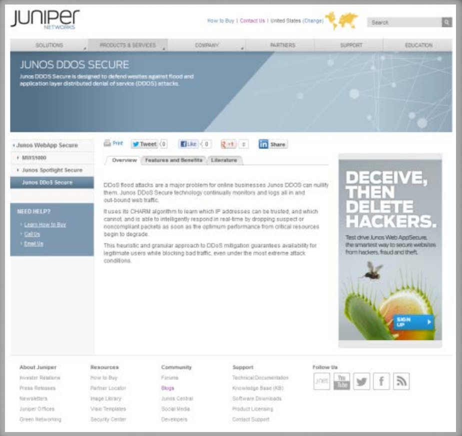
65% of companies worry most about web app attacks.*

JuniperSecurity [illegible]

MT Thanks > @[illegible] As I said last time, Juniper Webapp Secure (nee Mykonos) is the greatest trolling security program I've [illegible]

DDoS SECURE

Volumetric and Low and Slow Protection



JUNOS DDOS SECURE

Junos DDOS Secure is designed to defend wesites against flood and application layer distributed denial of service (DDOS) attacks.

DDoS flood attacks are a major problem for online businesses Junos DDOS can nullify them. Junos DDoS Secure technology continually monitors and logs all in and out-bound web traffic.

It uses its CHARM algorithm to learn which IP addresses can be trusted, and which cannot, and is able to intelligently respond in real-time by dropping suspect or noncompliant packets as soon as the optimum performance from critical resources begin to degrade.

This heuristic and granular approach to DDoS mitigation guarantees availability for legitimate users while blocking bad traffic, even under the most extreme attack conditions.

DECEIVE, THEN DELETE HACKERS.

Test drive Junos Web AppSecure, the smartest way to secure websites from hackers, fraud and theft.

WWW.JUNIPER.NET

Q&A

Chris Christiansen

Program Vice President Security Products and Services Group

IDC

David Koretz

Vice President of Security Products, Strategy & GM Counter Security

Juniper Networks

THANK YOU FOR JOINING US!

FOR MORE INFO PLEASE VISIT:
WWW.JUNIPER.NET

PROGRAM NOTE:

This webcast is sponsored by Juniper Networks. Any editorial supplied by Juniper Networks is independent of IDC analysis.

All IDC materials are used by Juniper Networks with IDC’s permission and in no way does the use or publication of IDC research indicate IDC’s endorsement of Juniper Networks products and/or strategies. Any other reproduction of this webcast in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable.

IDC disclaims all warranties as to the accuracy, completeness or adequacy of such information. IDC shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.