JUNIPER NETWORKS

SECURITY FOR VIRTUALIZATION AND CLOUD

Andy Leung

Director, APAC Product Management

AGENDA

□ The MultiCloud Enterprise

□ Cloud Security Model

□ Advanced threat detection

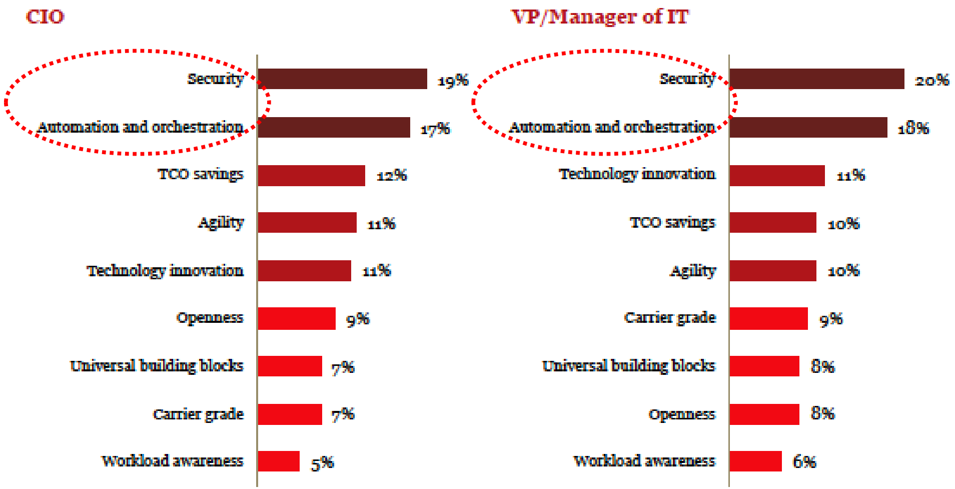
□ Juniper Security Solution

□ Summary

THE MULTICLOUD ENTERPRISE

BUYING STRATEGY

CIO IS PIVOTING TOWARDS



MITIGATING
RISK
(security)

MODERNIZING THEIR
DATA CENTERS
(automation, agility)

PwC | Enterprise data center buyer survey & interview insights

Source: www.juniper.net

KEY FINDINGS

100%

of enterprise workloads are shifting from on-premises to public cloud in the next 1-3 years

73%

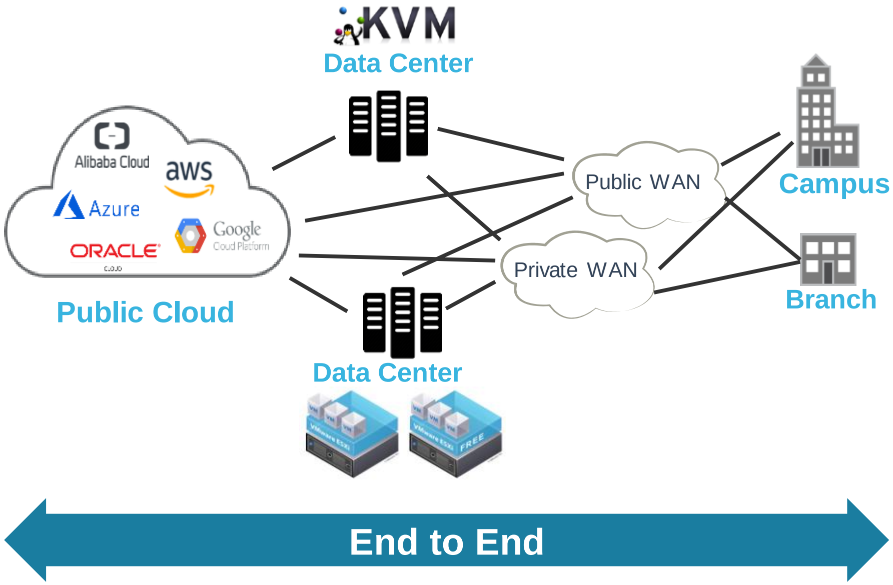
of enterprise has a mult-vendor Strategy, with Tech, Manufacturing, and Public Section leading the way

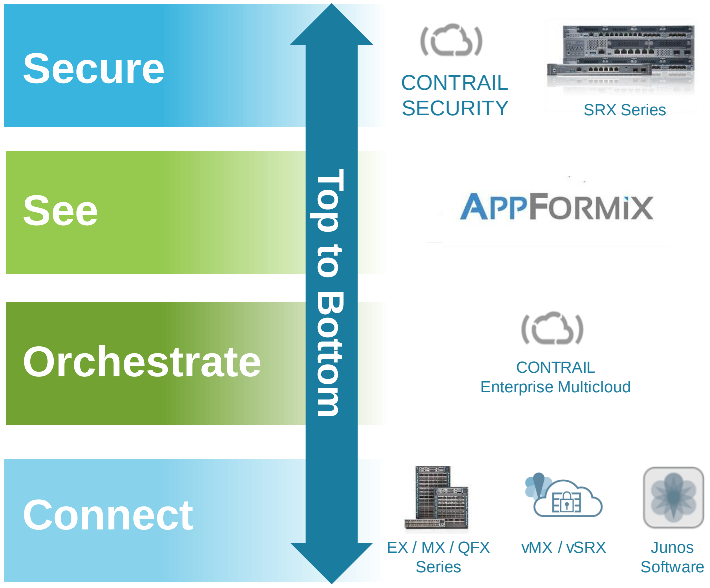
Security

Is the leading concern for using the cloud
And Automation is also important.

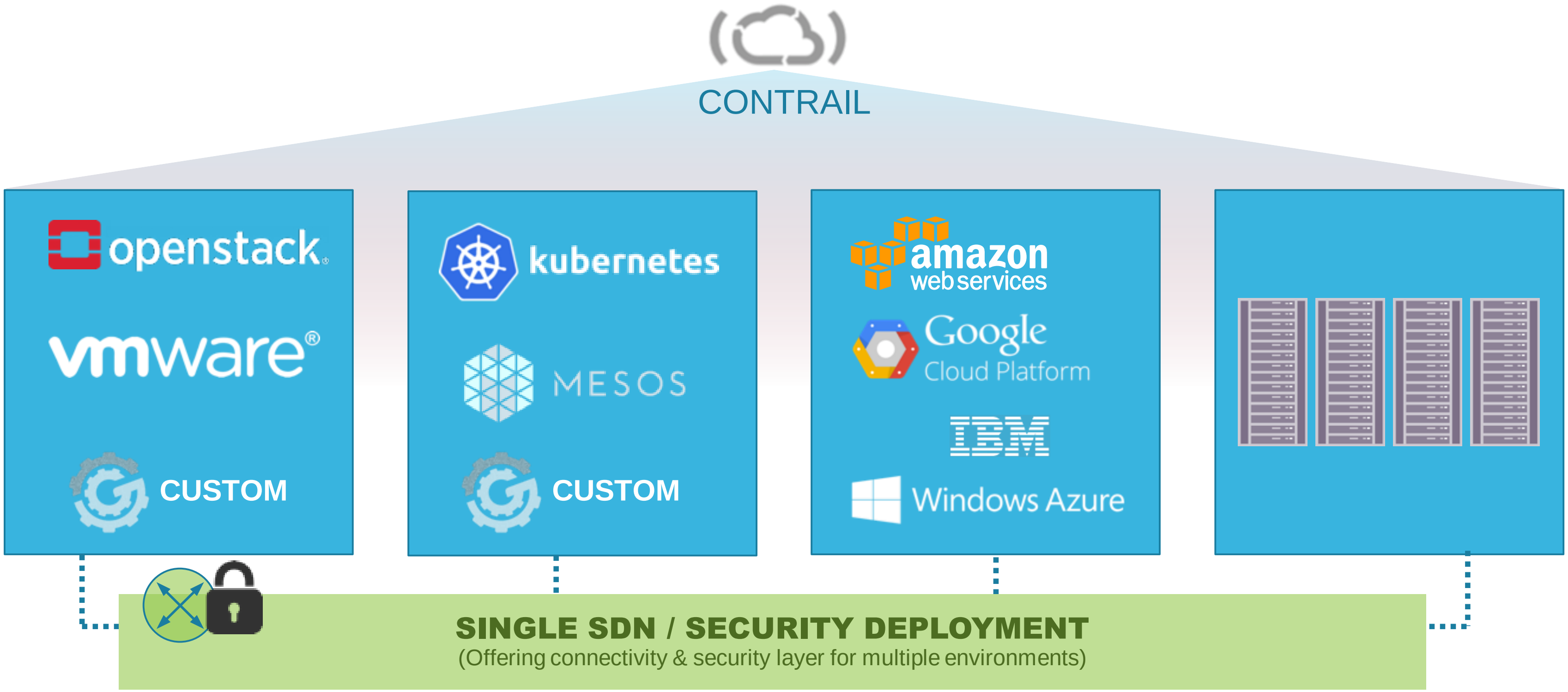
CLOUD SECURITY MODEL

OPERATING AS MULTICLOUD





Secure


CONTRAIL
openstack
vmware
CUSTOM
kubernetes
MESOS
CUSTOM
amazon web services
Google Cloud Platform
IBM
Windows Azure
SINGLE SDN / SECURITY DEPLOYMENT
(Offering connectivity & security layer for multiple environments)

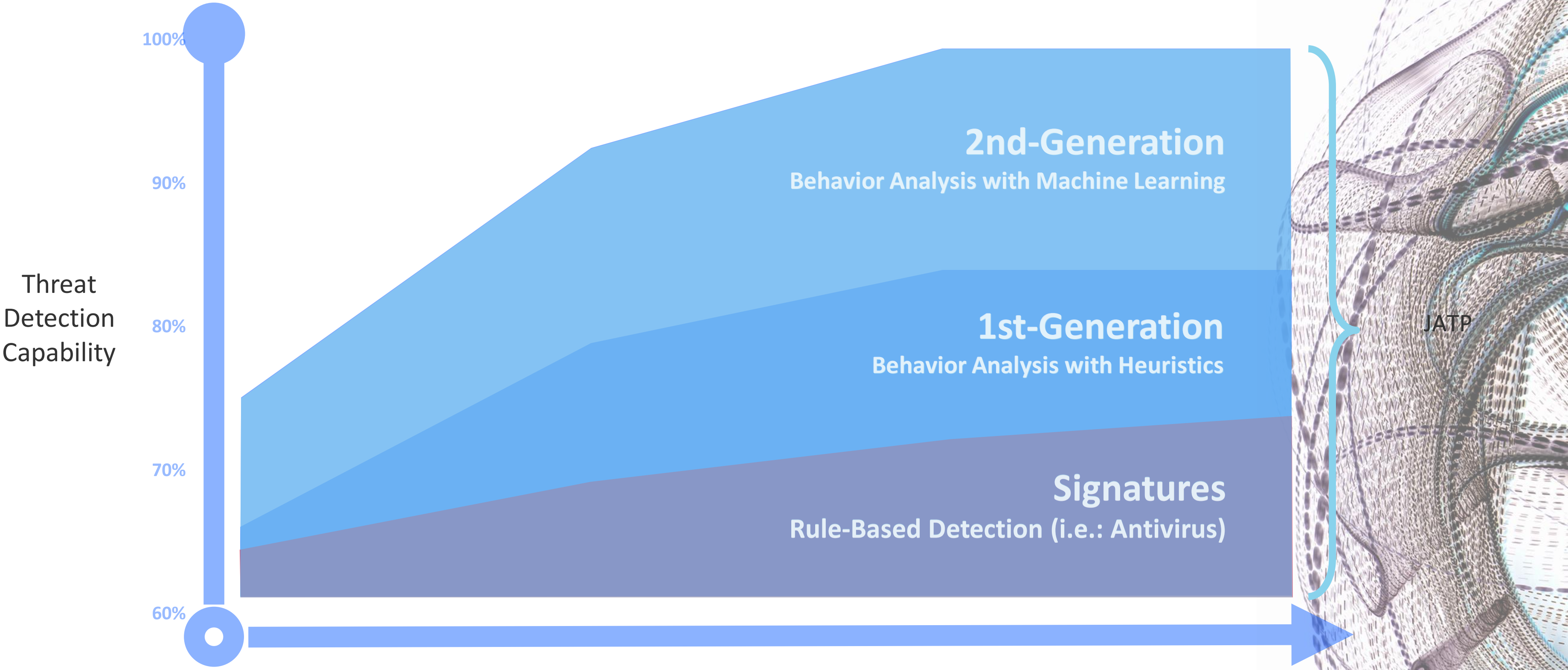
CLOUD SECURITY MODELS

Deploying steps:

- Architecture (i.e., Planning the deployment steps)
- Orchestration (i.e., Manage all the instances)
- Detection (i.e., Advanced Threat Detection)
- Mitigation (i.e., Stop the illegal activities and access)
- Report (i.e. Telemetry and Logging)

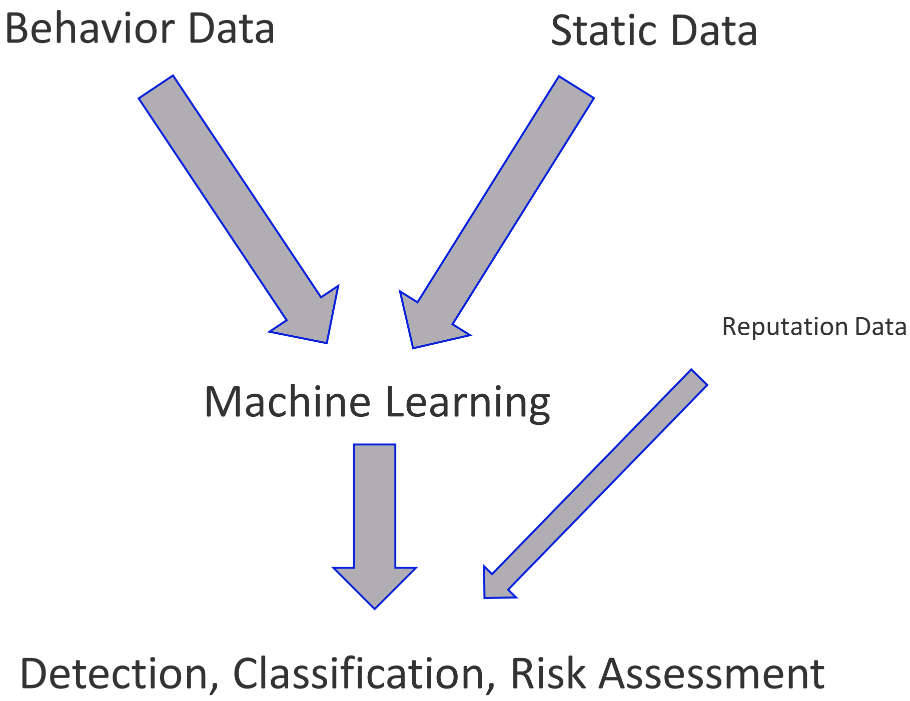
ADVANCED THREAT DETECTION

DEEP LEARNING SOLVES THE SIGNATURE GAP



JUNIPER NETWORKS

SECURITY APPLICATIONS - MACHINE LEARNING



Behavior Data

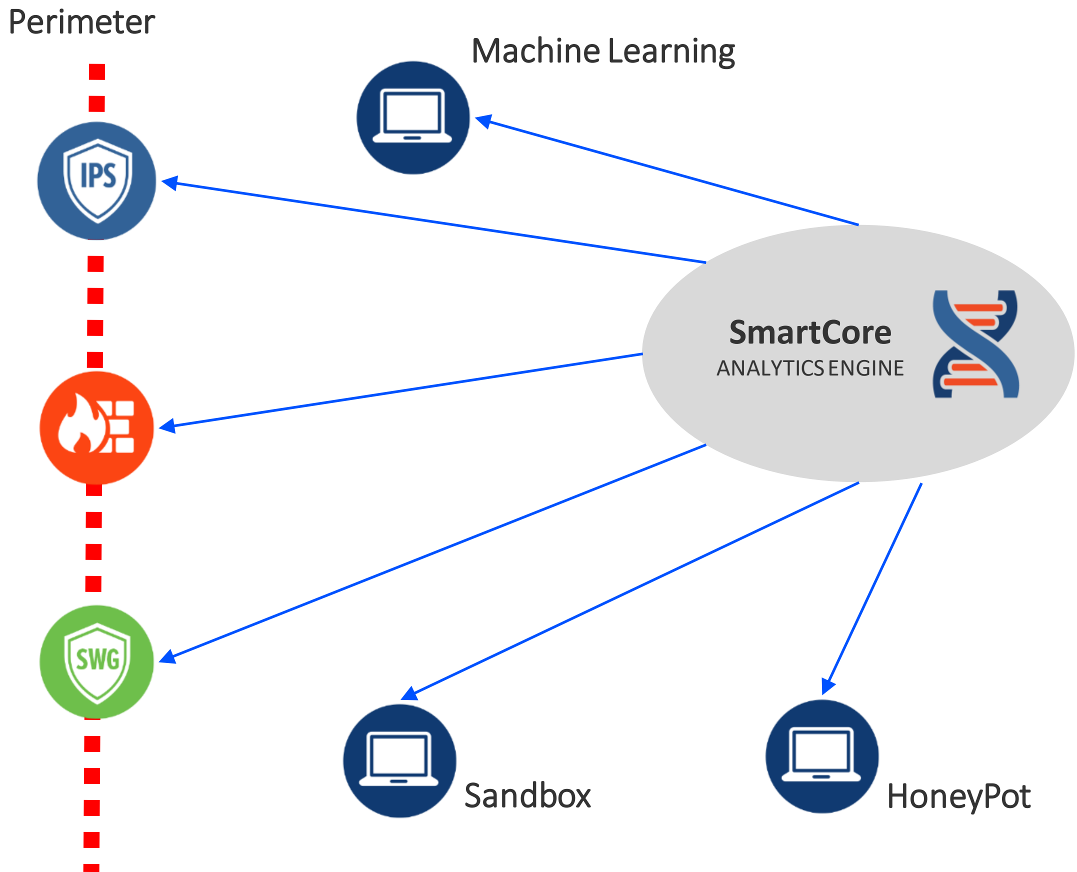
Static Data

Reputation Data

Machine Learning

Detection, Classification, Risk Assessment

MULTI-LAYER THREAT MITIGATION: STRONGER SECURITY


Perimeter

Machine Learning

SmartCore
ANALYTICS ENGINE

Sandbox

HoneyPot

Mitigation & Enforcement

Publish Blocking Data
To Existing: FW, IPS and SWG
API based or manual

IPS SWG

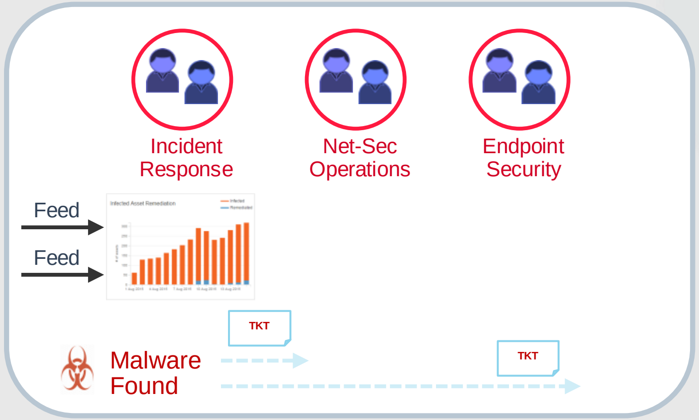
One-touch mitigation for IR teams

Infection Verification

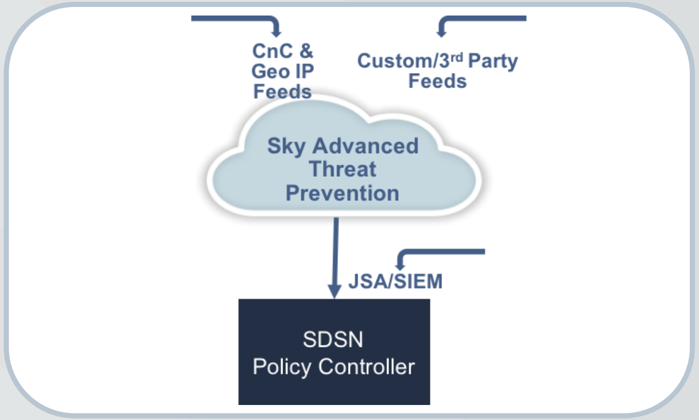
Verify infection on suspect endpoints before cleaning (Native, Carbon-Black, Tanium, Crowdstrike)

Automate Threat Remediation

MANUAL THREAT WORKFLOWS



Automated Threat Remediation



Multiple Teams

Threat Detection → Enforcement Delays

Vendor specific threat feeds

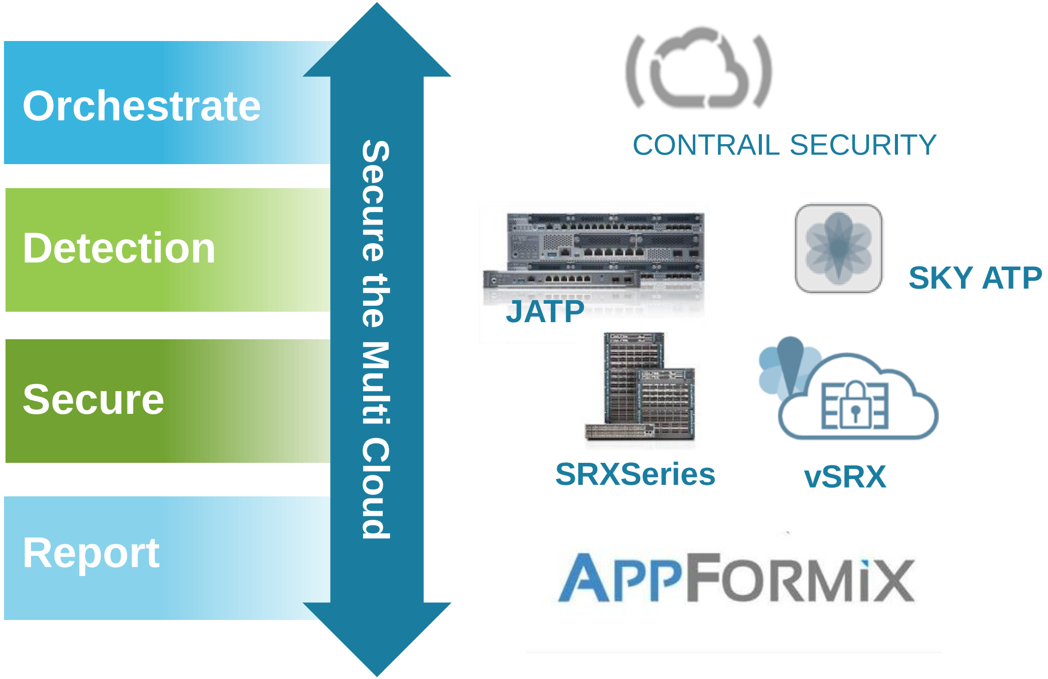
Cohesive Threat Management System

Automation across Network & Security

Open API and 3rd Party Threat Feed Collation

JUNIPER CLOUD SECURITY SOLUTION

JUNIPER MULTI CLOUD SECURITY



Orchestrate

Detection

Secure

Report

Secure the Multi Cloud

CONTRAIL SECURITY

JATP

SKY ATP

SRXSeries

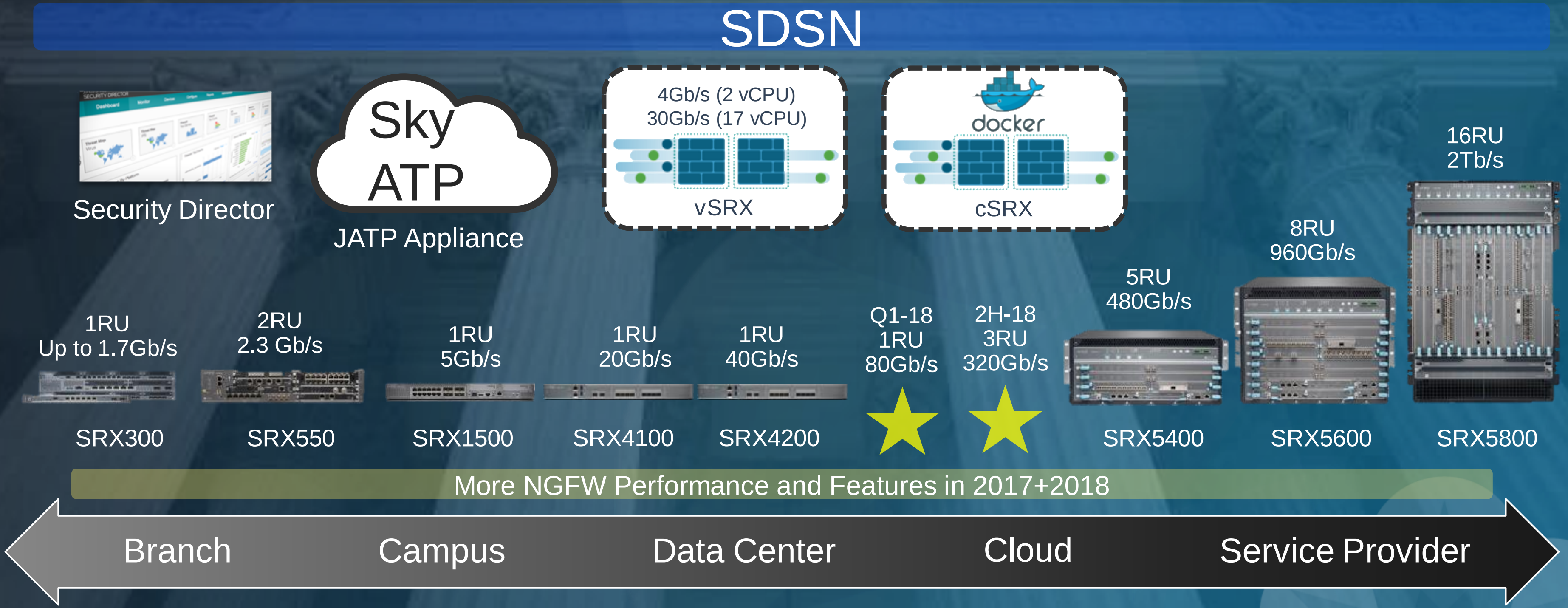
vSRX

APPFORMIX

Secure

SECURITY PORTFOLIO

Price / Performance, Scale and Efficacy Leadership



SDSN

Security Director

Sky ATP

JATP Appliance

4Gb/s (2 vCPU)
30Gb/s (17 vCPU)
vSRX

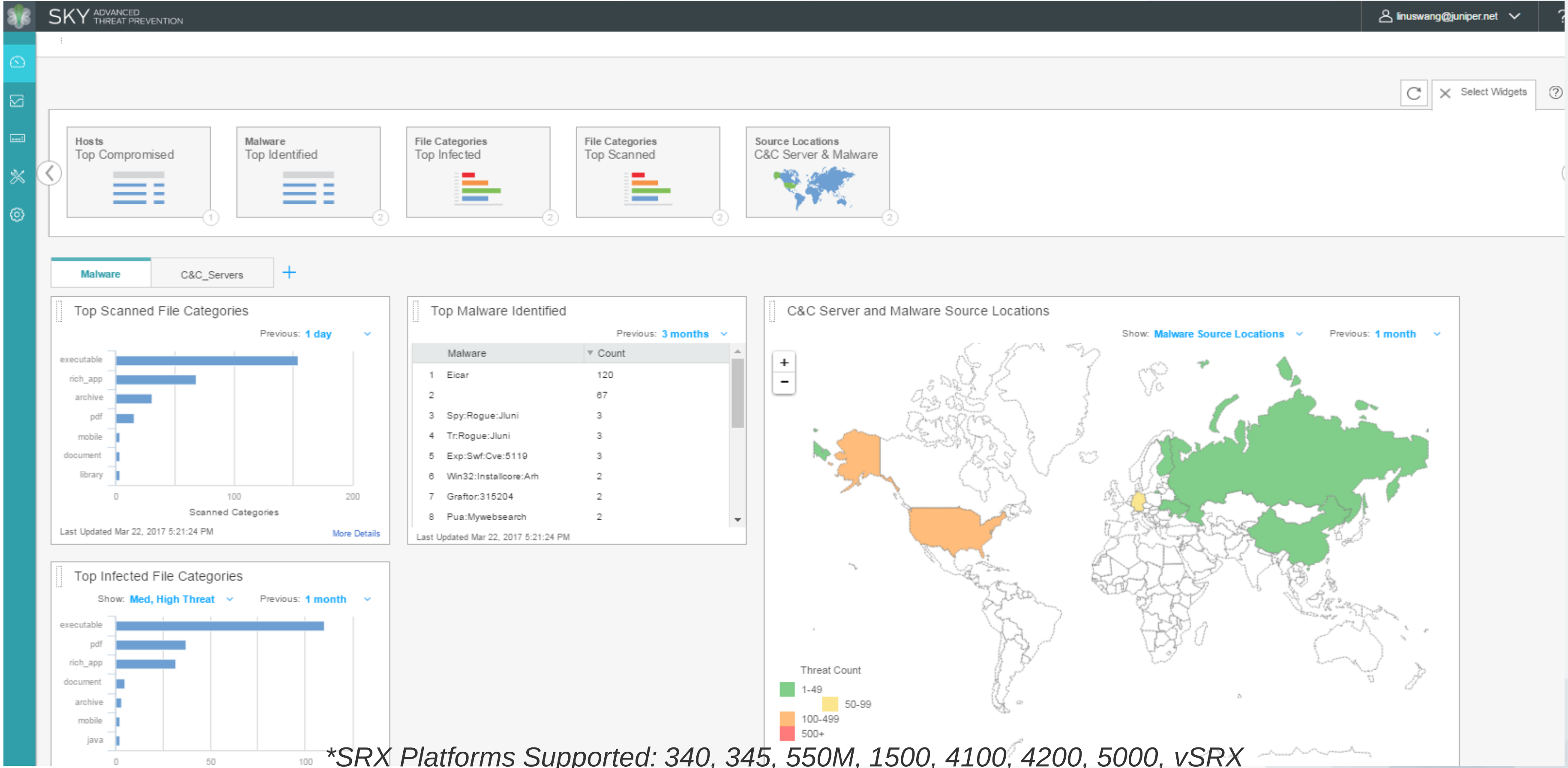
docker
cSRX

1RU Up to 1.7Gb/s	2RU 2.3 Gb/s	1RU 5Gb/s	1RU 20Gb/s	1RU 40Gb/s	Q1-18 1RU 80Gb/s	2H-18 3RU 320Gb/s	5RU 480Gb/s	8RU 960Gb/s	16RU 2Tb/s
SRX300	SRX550	SRX1500	SRX4100	SRX4200	★	★	SRX5400	SRX5600	SRX5800

More NGFW Performance and Features in 2017+2018

Branch — Campus — Data Center — Cloud — Service Provider

SKY ATP (ADVANCED THREAT PREVENTION)



Top Scanned File Categories

Previous: 1 day

Last Updated Mar 22, 2017 5:21:24 PM

Top Malware Identified

Previous: 3 months

	Malware	Count
1	Eicar	120
2		67
3	Spy:Rogue:Jluni	3
4	Tr:Rogue:Jluni	3
5	Exp:Swf:Cve:5119	3
6	Win32:Installcore:Arh	2
7	Graftor:315204	2
8	Pua:Mywebsearch	2

Last Updated Mar 22, 2017 5:21:24 PM

C&C Server and Malware Source Locations

Show: Malware Source Locations Previous: 1 month

Top Infected File Categories

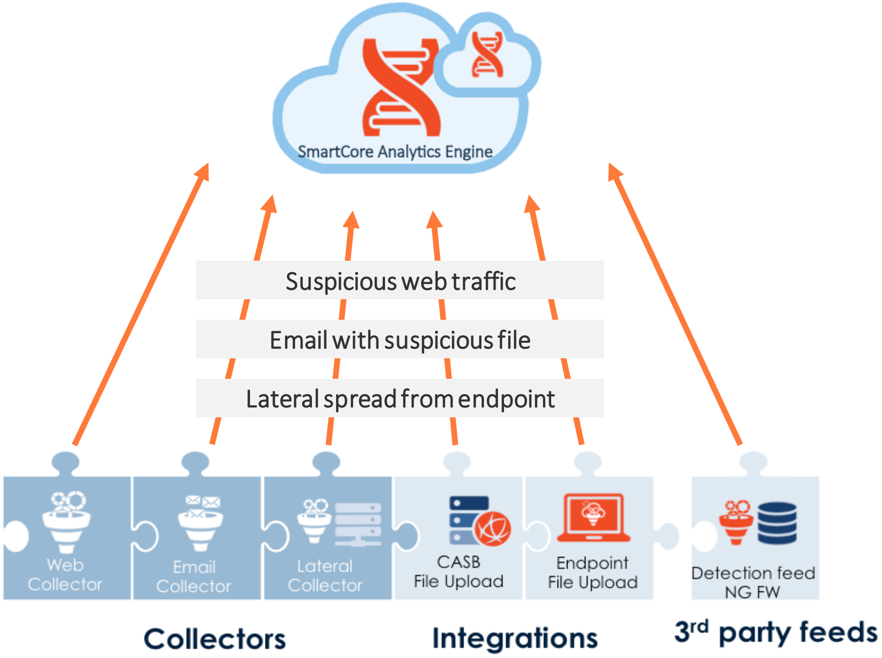
Show: Med, High Threat Previous: 1 month

SRX Platforms Supported: 340, 345, 550M, 1500, 4100, 4200, 5000, vSRX

SKY ATP / JATP: FAST DISCOVERY

Integration

Advanced Threat Detection With Complete Visibility

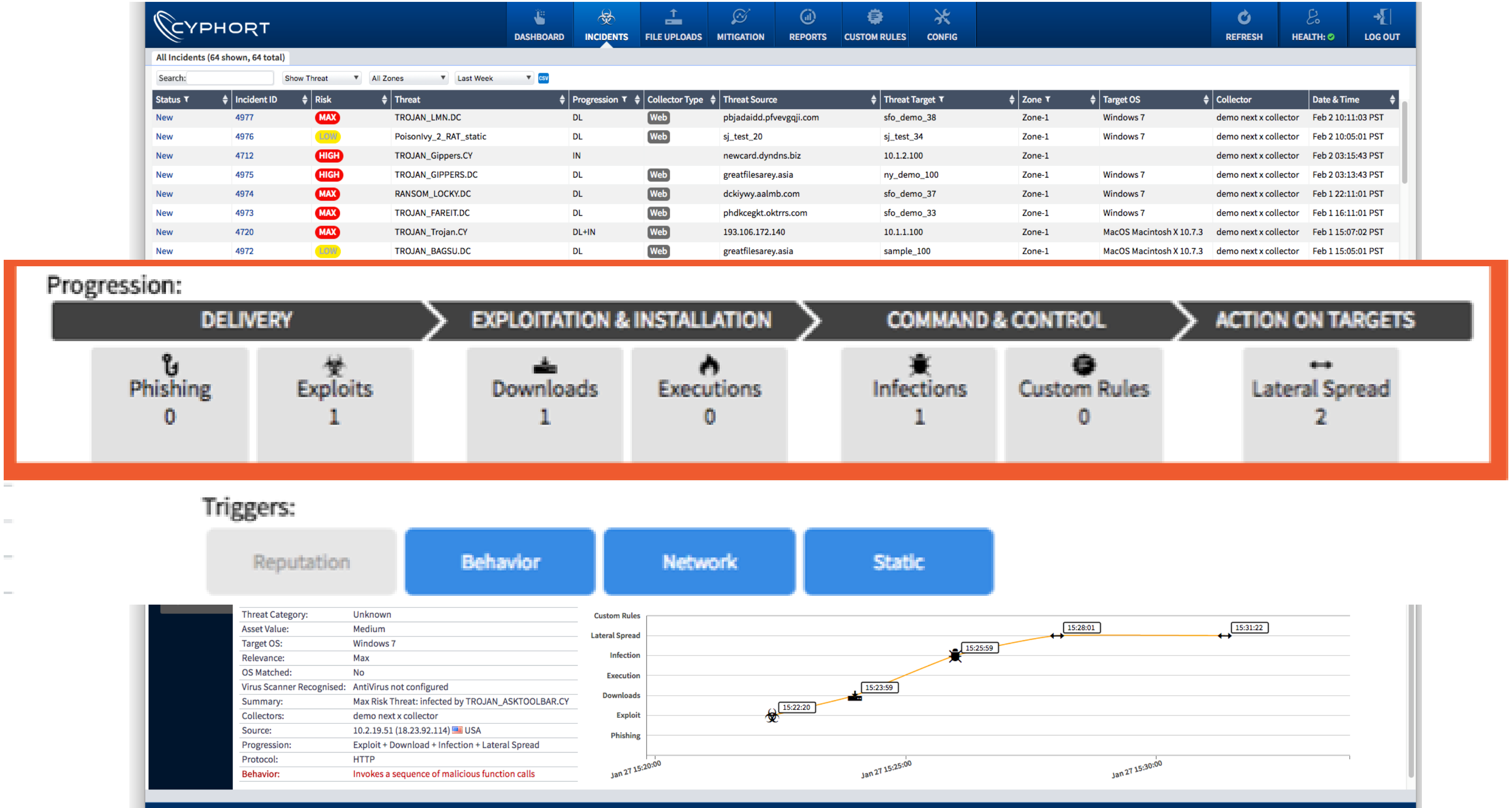


Key Platform Features

- Distributed, scale-out architecture
- Deployable in cloud or on-premise
- Web, email (N/S), lateral spread, File upload (E/W)
- Multi-stage behavioral analysis & machine learning
- Full Incident view and RISK based prioritization
- Threats typically detected in less than 15 seconds
- 10x cost savings in MSSP/Cloud deployments
- Certified by ICSA Labs

Detection

ADVANCED THREAT DETECTION: KILL CHAIN ALIGNMENT



All Incidents (64 shown, 64 total)

Search: Show Threat ▾ All Zones ▾ Last Week ▾ CSV

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector	Date & Time
New	4977	MAX	TROJAN_LMN.DC	DL	Web	pbjadaidd.pfvevgqji.com	sfo_demo_38	Zone-1	Windows 7	demo next x collector	Feb 2 10:11:03 PST
New	4976	LOW	PoisonIvy_2_RAT_static	DL	Web	sj_test_20	sj_test_34	Zone-1	Windows 7	demo next x collector	Feb 2 10:05:01 PST
New	4712	HIGH	TROJAN_Gippers.CY	IN		newcard.dyndns.biz	10.1.2.100	Zone-1		demo next x collector	Feb 2 03:15:43 PST
New	4975	HIGH	TROJAN_GIPPERS.DC	DL	Web	greatfilesarey.asia	ny_demo_100	Zone-1	Windows 7	demo next x collector	Feb 2 03:13:43 PST
New	4974	MAX	RANSOM_LOCKY.DC	DL	Web	dckiywy.aalmb.com	sfo_demo_37	Zone-1	Windows 7	demo next x collector	Feb 1 22:11:01 PST
New	4973	MAX	TROJAN_FAREIT.DC	DL	Web	phdkcegkt.oktrrs.com	sfo_demo_33	Zone-1	Windows 7	demo next x collector	Feb 1 16:11:01 PST
New	4720	MAX	TROJAN_Trojan.CY	DL+IN	Web	193.106.172.140	10.1.1.100	Zone-1	MacOS Macintosh X 10.7.3	demo next x collector	Feb 1 15:07:02 PST
New	4972	LOW	TROJAN_BAGSU.DC	DL	Web	greatfilesarey.asia	sample_100	Zone-1	MacOS Macintosh X 10.7.3	demo next x collector	Feb 1 15:05:01 PST

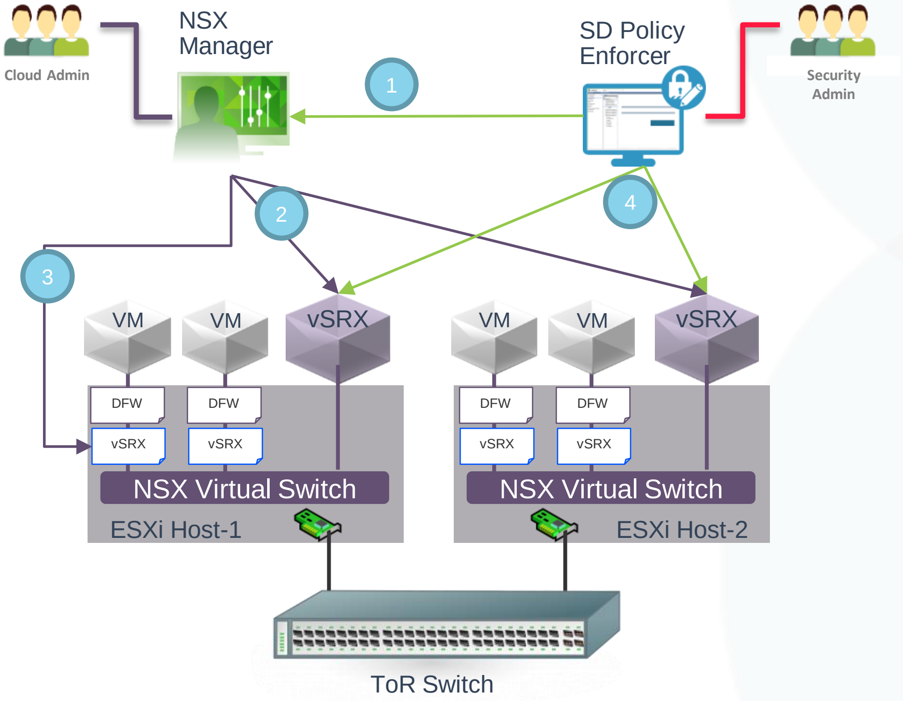
Progression:

DELIVERY		EXPLOITATION & INSTALLATION		COMMAND & CONTROL		ACTION ON TARGETS
Phishing 0	Exploits 1	Downloads 1	Executions 0	Infections 1	Custom Rules 0	Lateral Spread 2

Triggers:

Threat Category:	Unknown
Asset Value:	Medium
Target OS:	Windows 7
Relevance:	Max
OS Matched:	No
Virus Scanner Recognised:	AntiVirus not configured
Summary:	Max Risk Threat: infected by TROJAN_ASKTOOLBAR.CY
Collectors:	demo next x collector
Source:	10.2.19.51 (18.23.92.114) 🇺🇸 USA
Progression:	Exploit + Download + Infection + Lateral Spread
Protocol:	HTTP
Behavior:	Invokes a sequence of malicious function calls

NSX INTEGRATION – VSRX PROVISIONING AND MANAGEMENT



0 NSX deployed and SD/PE installed

1 SD Registers vSRX Service w/ NSX

2 NSX provisions vSRX on all NSX hosts

3 NSX provisions vSRX redirection rules

4 SD provisions licenses & default policy for vSRX

Initial Provisioning Complete

SUMMARY

SKY ATP: THREATS PREVENTED

WannaCry

- Exploits vulnerabilities in SMBv1 that allows remote code execution

Locky

- Uses VB macros to download payload, encrypts disk with key obtained from C&C server

Zepto

- Locky variant that renames files with .zepto extension

Kovter’s

- Almost fileless malware! Uses obfuscated Javascript and ‘garbage’ batch files

……………………..and many more!

Detection

✓ ***Machine Learning** at every stage*

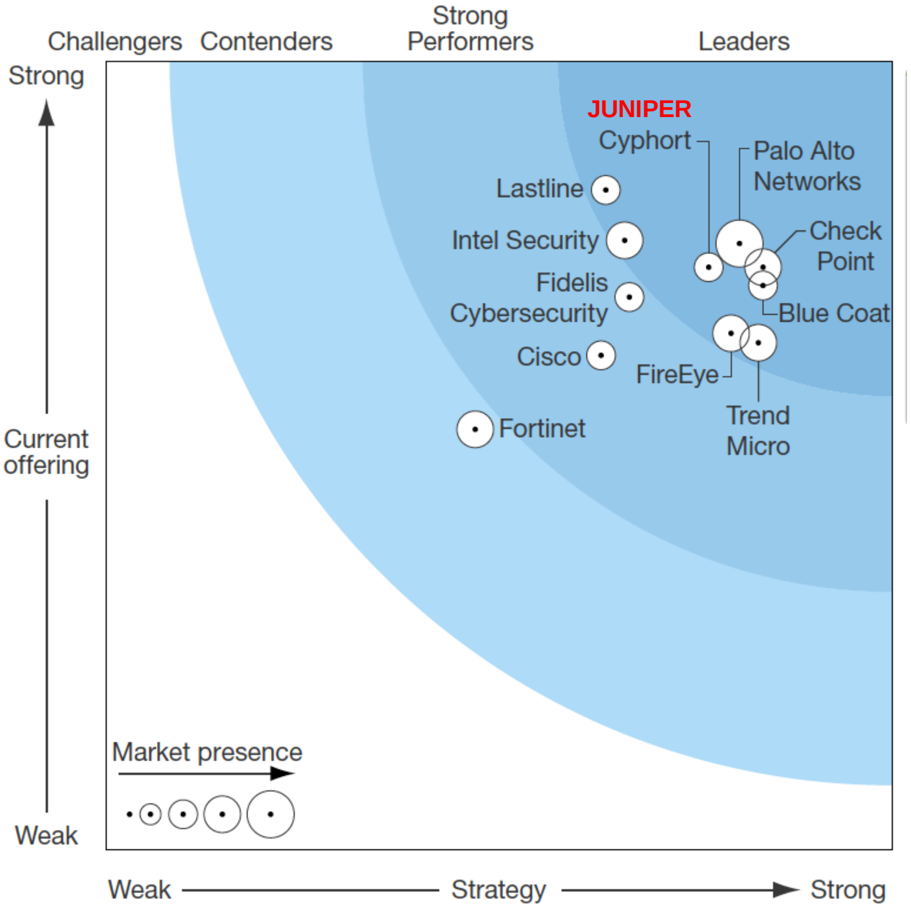
✓ ***Deception Techniques** and **Behavioral analysis** are used to differentiate malware from good software*

✓ *Thousands of features from static, dynamic and hybrid analysis are extracted from a large, continually-updated collection of samples – both malicious and benign – to construct a machine learning classifier that identifies and blocks previously unseen malware types*

JUNIPER NETWORKS ATP CERTIFIED BY ICSA LABS

Juniper Networks ATP solution is the only one certified by ICSA Labs in 2017 to provide 100% detection of advanced threats.

WAVE LEADER IN AUTOMATED MALWARE ANALYSIS



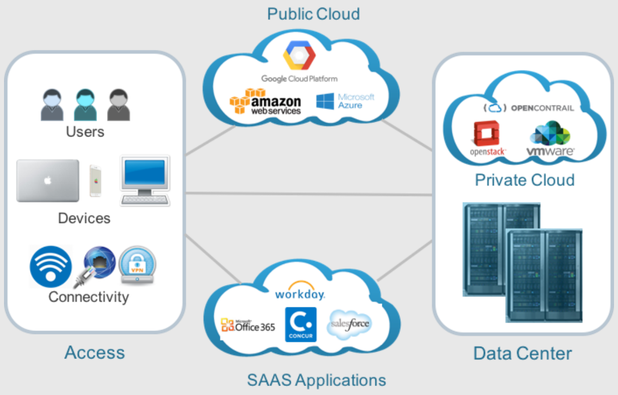
FORRESTER®

Source: Forrester Report Malware Analysis 2016

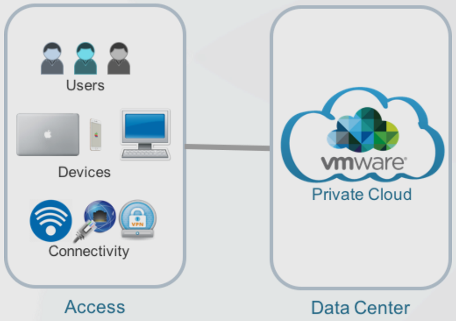
SUMMARY

Pervasive Security, Without Complexity

Cloud



Data Center



Juniper SRX & Sky ATP

AWS, Azure for Public Cloud

Vmware NSX for Private Cloud

Threat Remediation & Micro-segmentation

Thank You