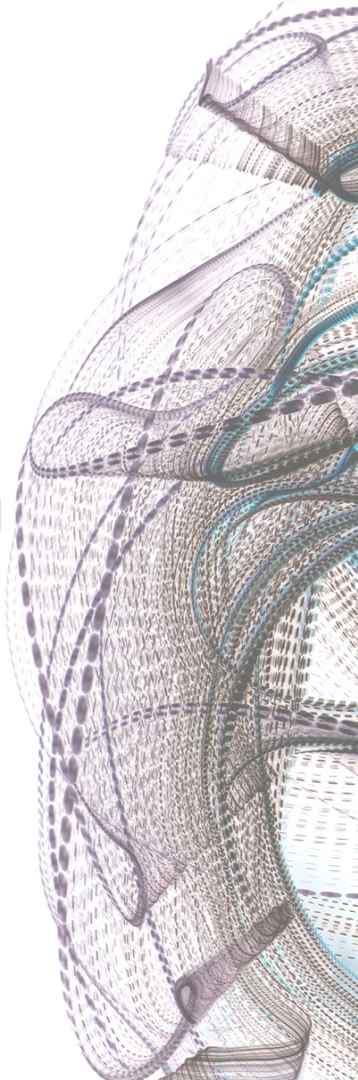
企業雲的威脅與防禦
SECURING THE MULTI-CLOUD ENTERPRISE

Andy Leung
Director, APAC Product Management

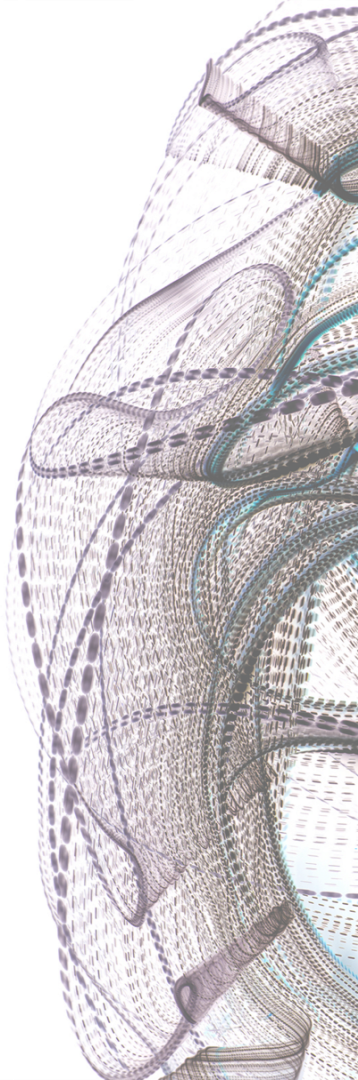
AGENDA

- The MultiCloud Enterprise
- Cloud Security Model
- Advanced threat detection with Machine Learning
- Juniper Security Solution
- Summary



JUNIPER NETWORKS

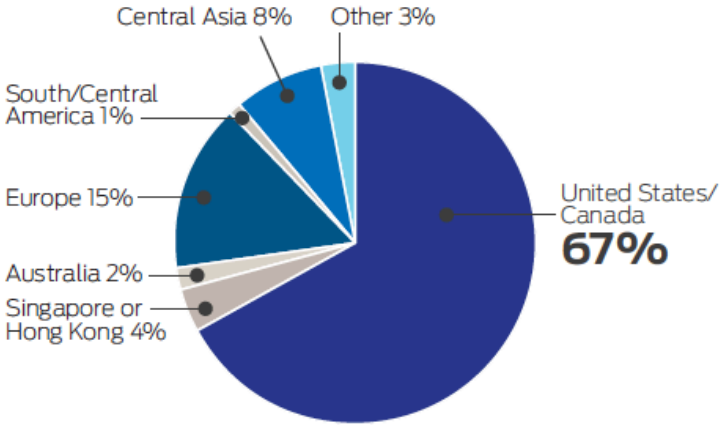
THE MULTICLOUD ENTERPRISE



JUNIPER AND PWC LED 200+ TECH INTERVIEW

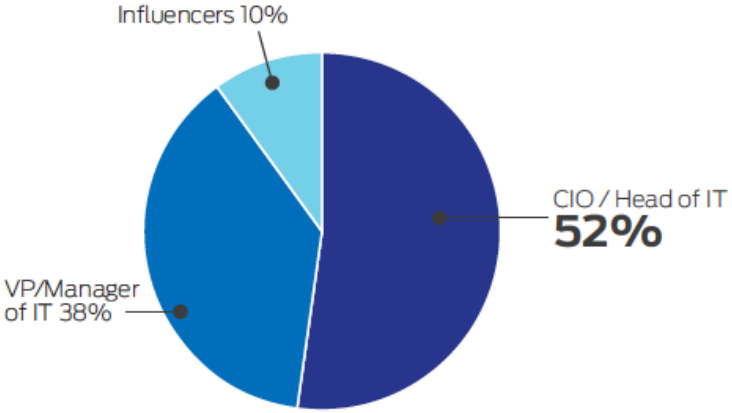
REGIONS

67% are from United States/Canada



ROLES

52% are CIO / Head of IT within IT organizations



pwc

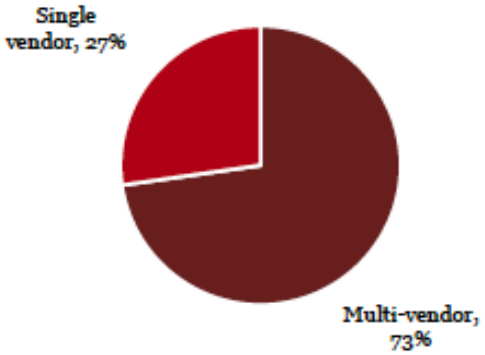
PwC | Enterprise data center buyer survey & interview insights

JUNIPER NETWORKS

BEST OF BREED STRATEGY

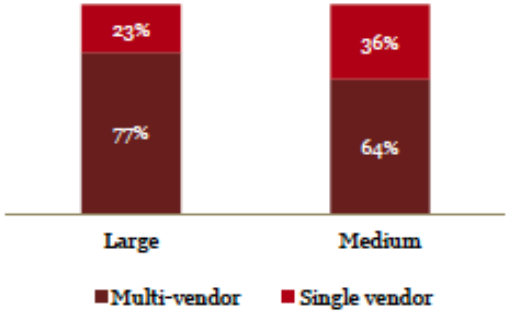
Vendor strategy

73% of the enterprises follow a multi-vendor data center strategy



Vendor strategy – organization size

77% of large organizations and 64% of medium organizations follow a multi-vendor data center strategy

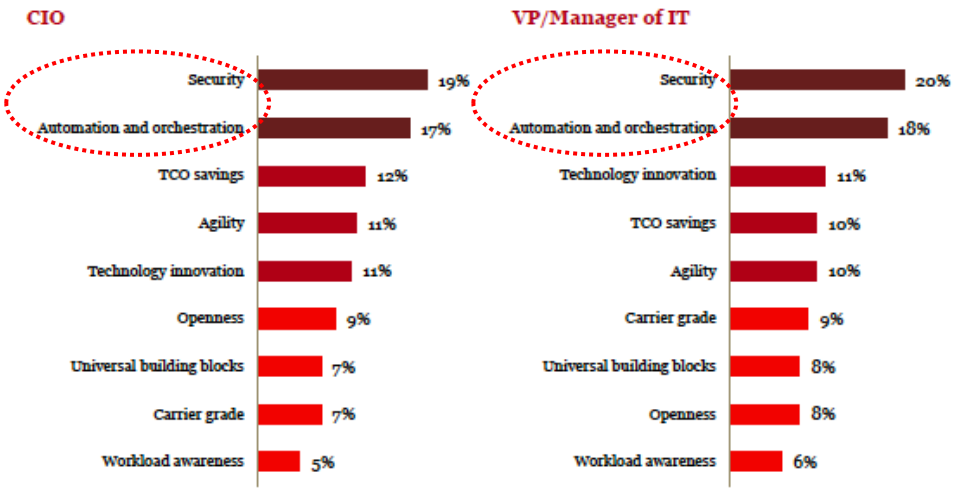


PwC | Enterprise data center buyer survey & interview insights

Source: www.juniper.net

CLOUD DEPLOYMENT STRATEGY

CIO IS PIVOTING TOWARDS



pwc

PwC | Enterprise data center buyer survey & interview insights

Source: www.juniper.net

JUNIPER NETWORKS

KEY FINDINGS

100%

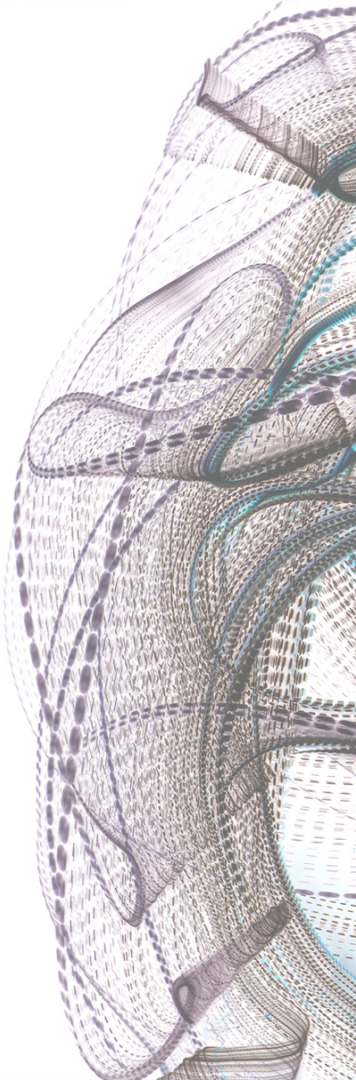
of enterprise workloads are shifting from on-premises to public cloud in the next 1-3 years

73%

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

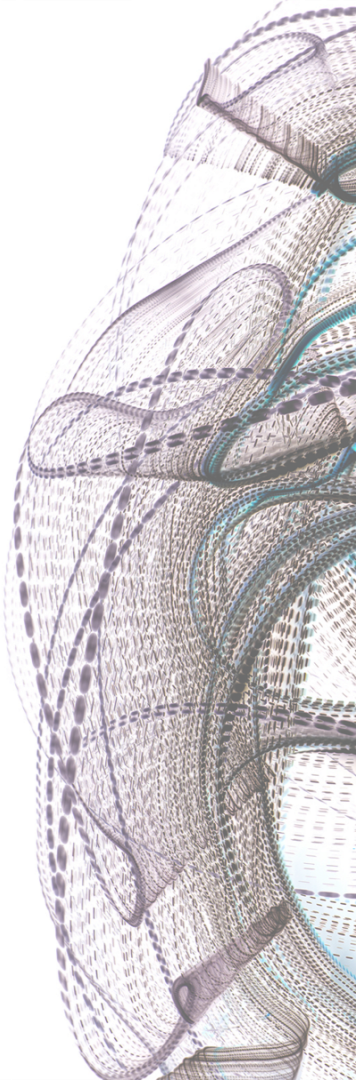
Security

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

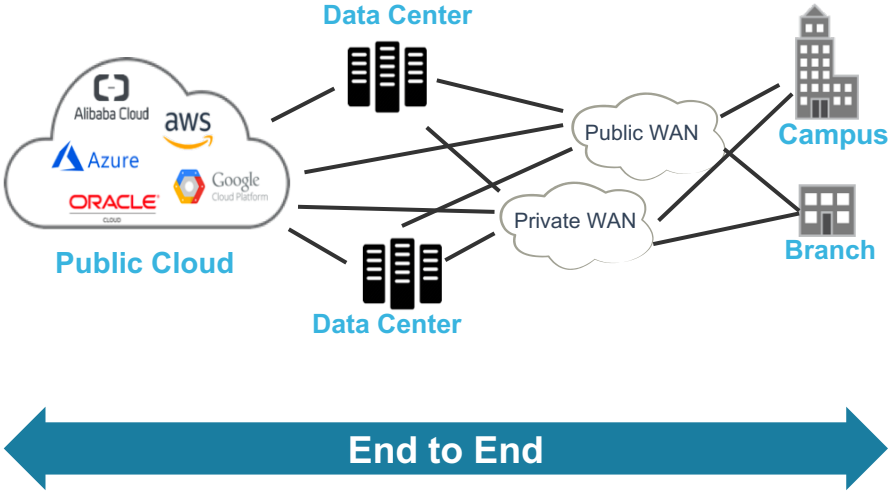


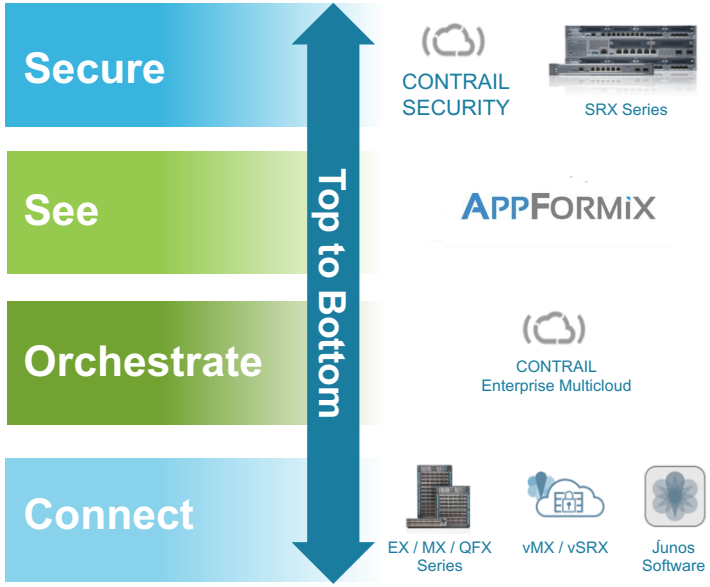
JUNIPER NETWORKS

CLOUD SECURITY MODEL



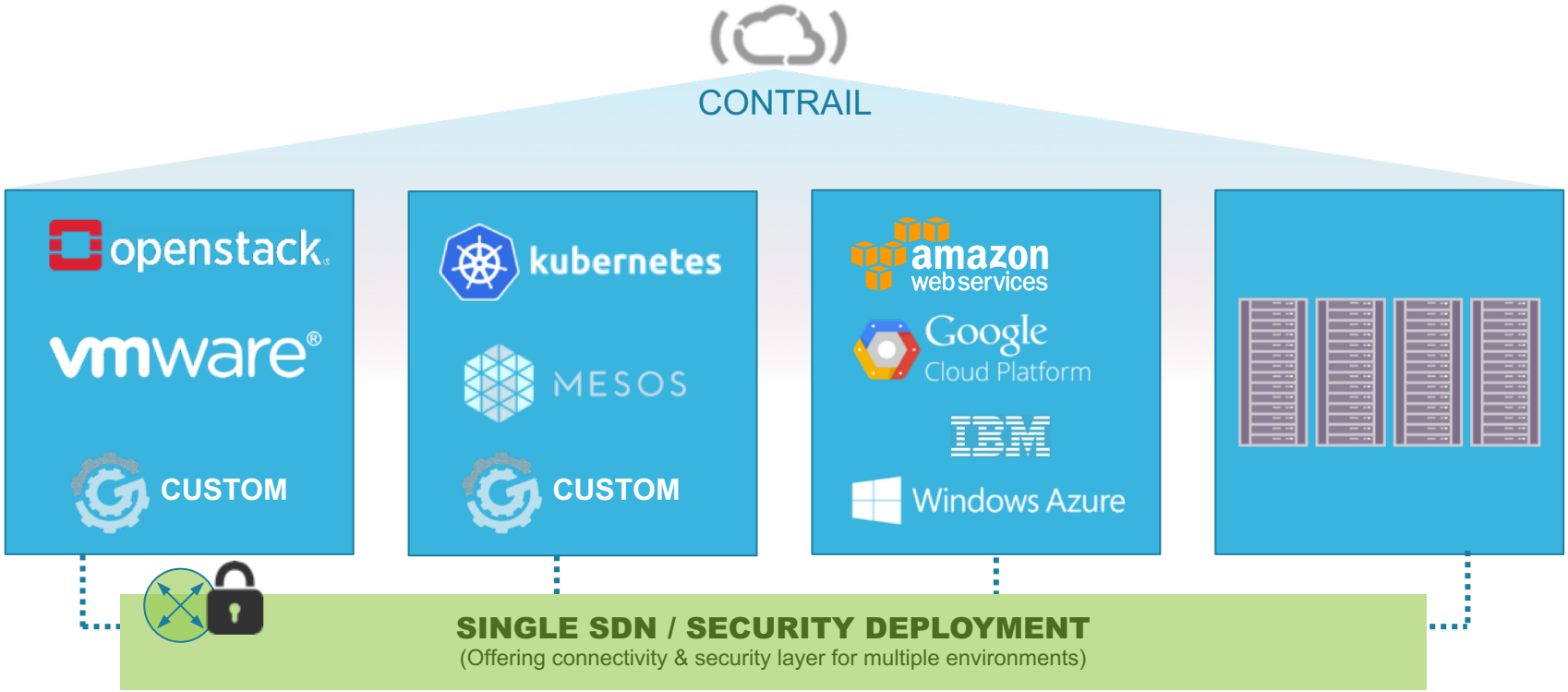
OPERATING AS MULTICLOUD





JUNIPER NETWORKS

Secure



JUNIPER NETWORKS

SECURING THE CLOUD WITH
NEXT GENERATION FIREWALL SERVICES

Ingress

- Heuristics for evasive and tunneled apps
- More application signatures
- Open signature language

App Tracking
- Understanding security risks
- Address new user behavior

App Firewall
- Block access to risky apps
- Allow user tailored policies

App QoS
- Prioritize important apps
- Rate-limit less important apps

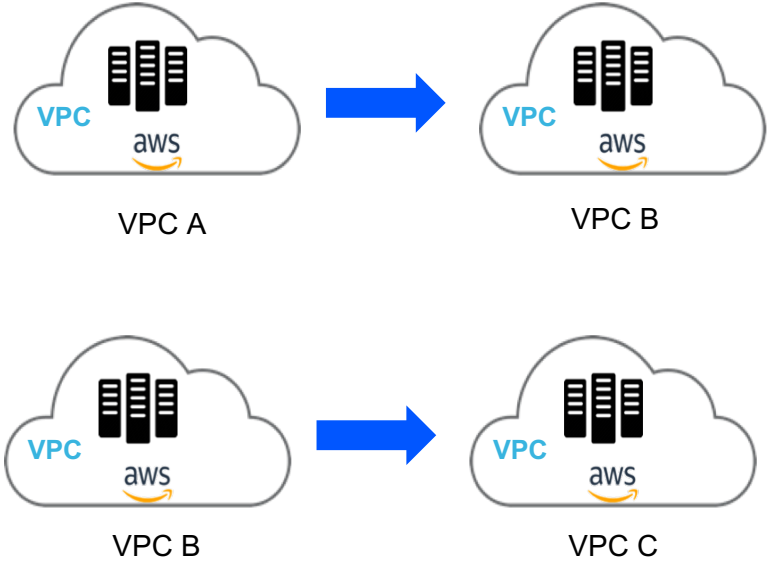
App Routing
- Define packet forwarding for Apps
- Create custom app environment

SSL Proxy
- SSL packet inspection

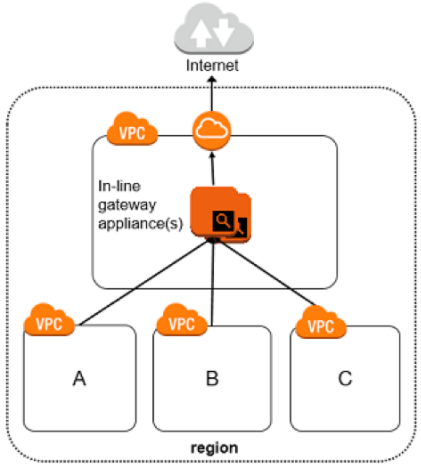
IPS
- Prevent application borne security threats

Egress

FLEXIBLE NETWORK ARCHITECTURE IN THE CLOUD

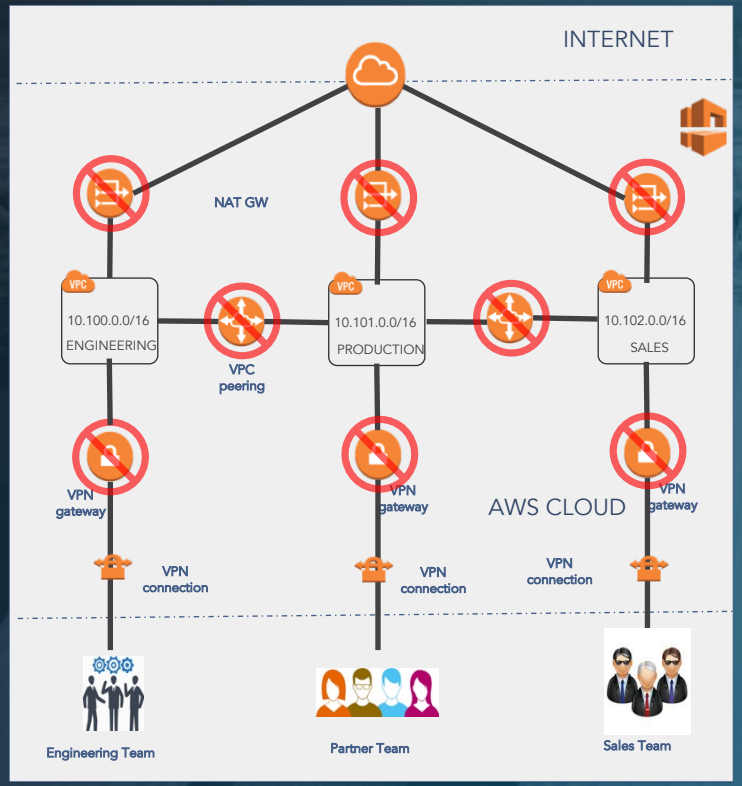


Traditional Design limitation



Transient VPC Architecture
By Juniper vSRX, vMX

VSRX TRANSIENT VPC – SIMPLIFY AWS ARCHITECTURE



Eliminate the dedicated NAT

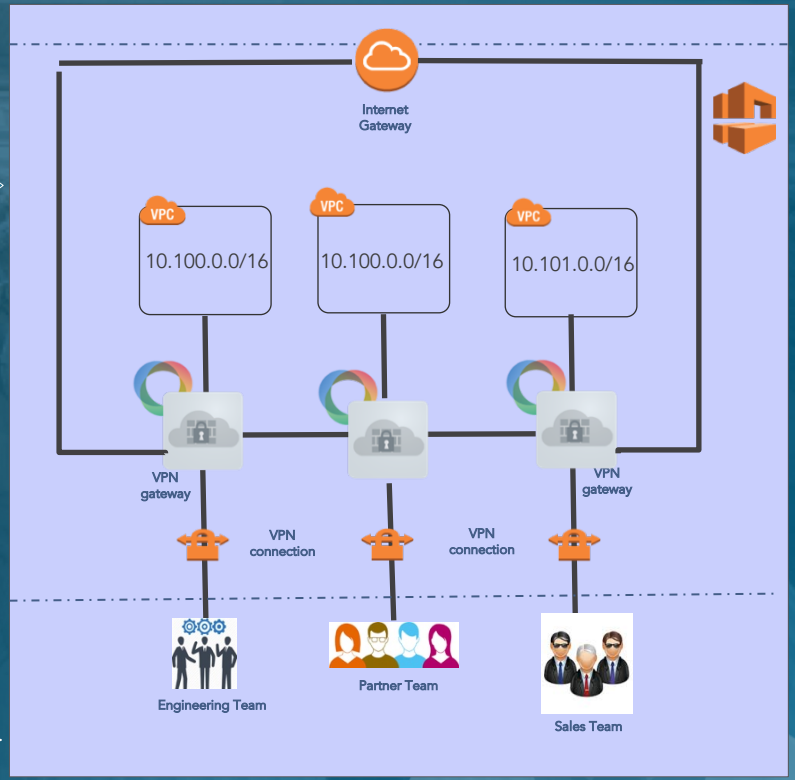
Eliminate the dedicated VPN gateway

Eliminate the VPC Peering module

Add Comprehensive security - **Intelligence** - at Ingress, Egress and between VPCs

Manage security from a single console (unified)

BETTER ROI



3 MAIN COVERAGE FOR CLOUD SECURITY

Correlated Visibility

Next-Gen Perimeter Defense
with Lateral Movement

Dynamic Detection

Machine Learning plus
Behavioral Inspection

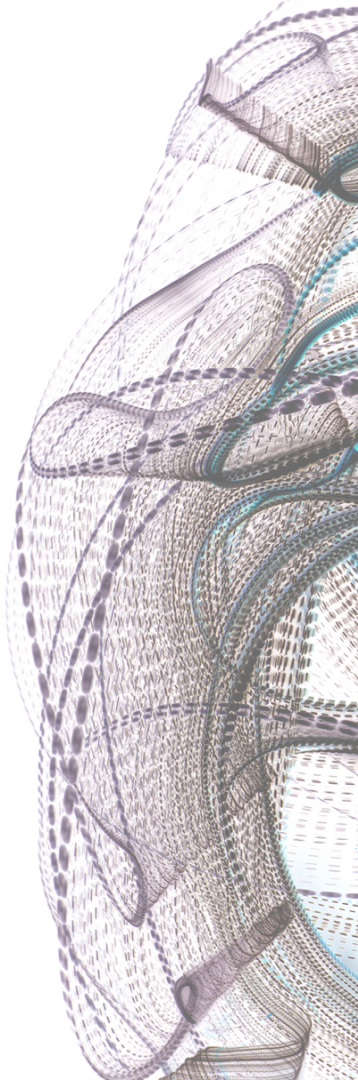
Virtualized Deployment

Flexible Software-based
Security Solution

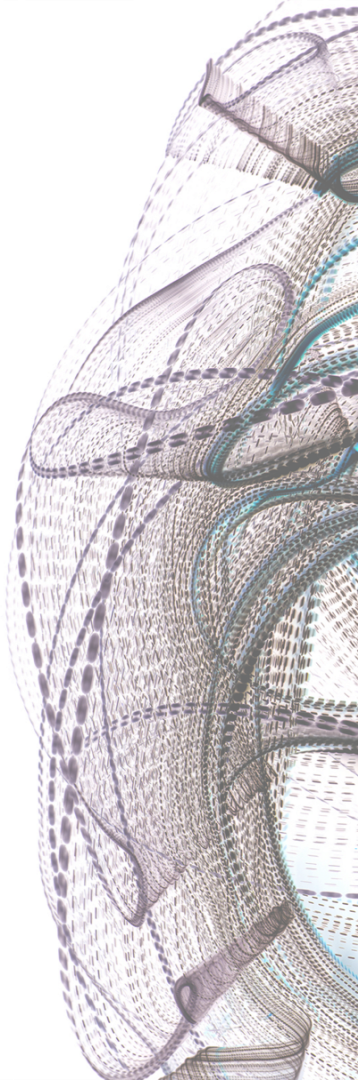
CLOUD SECURITY IN STEPS

Deploying steps:

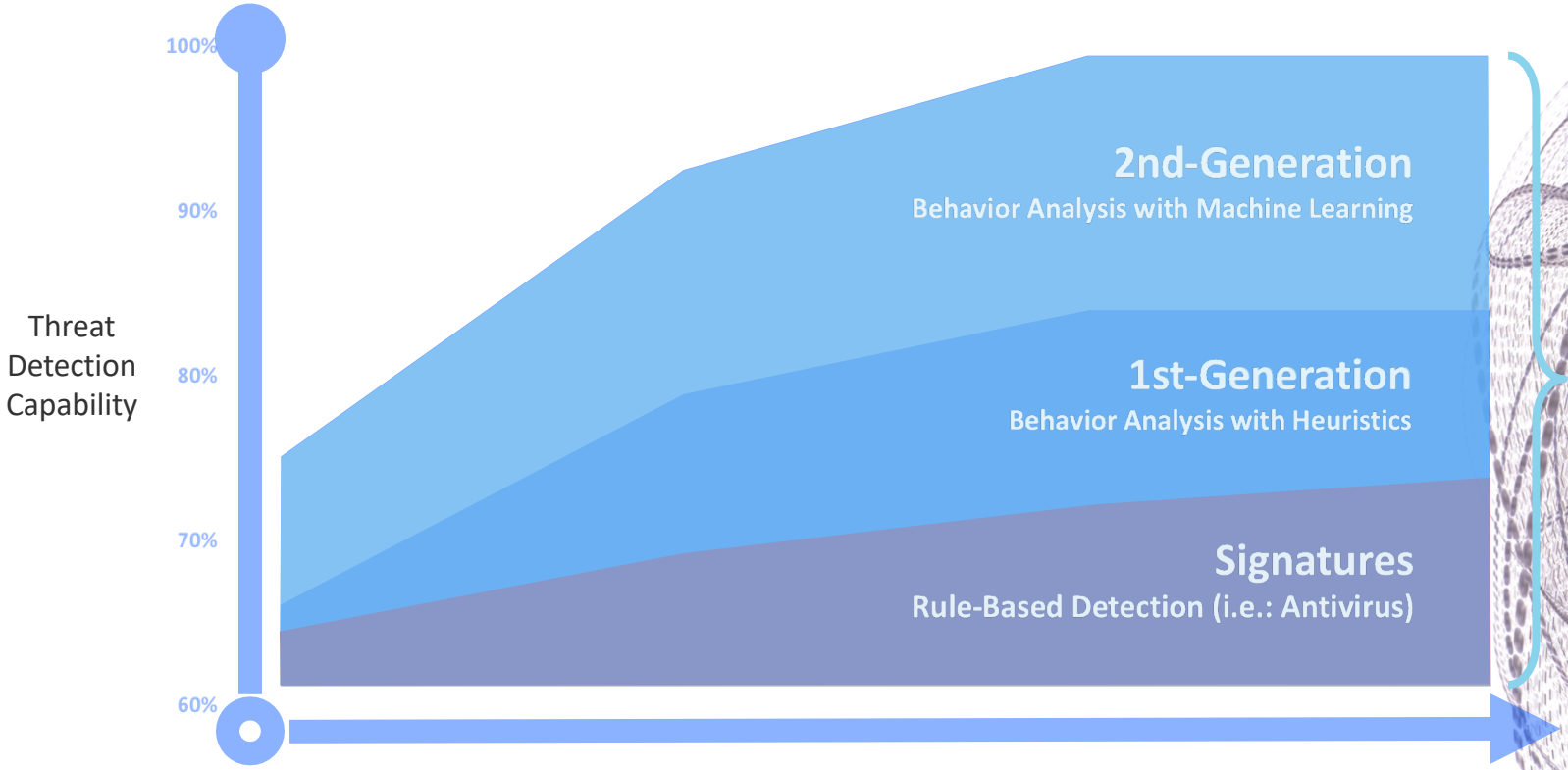
- Architecture (i.e., Planning the deployment steps)
- Orchestration (i.e., Manage all the instances)
- Detection (i.e., Advanced Threat Detection)
- Mitigation (i.e., Stop the illegal activities and access)
- Report (i.e. Telemetry and Logging)

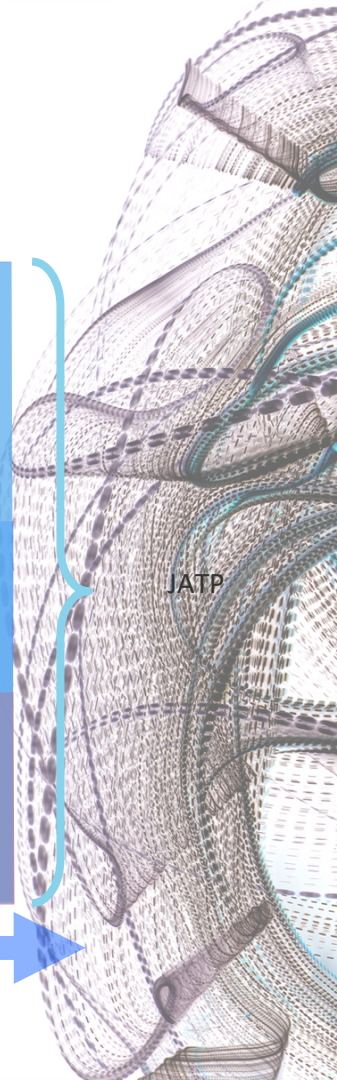


ADVANCED THREAT DETECTION WITH MACHINE LEARNING



DEEP LEARNING SOLVES THE SIGNATURE GAP



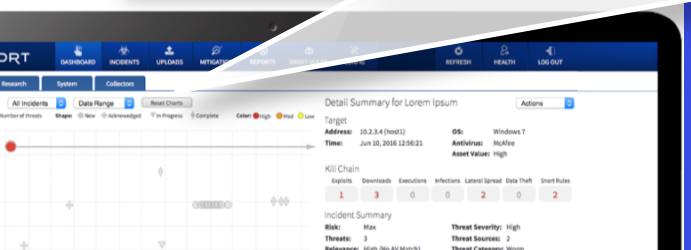


JUNIPER NETWORKS

KILLCHAIN

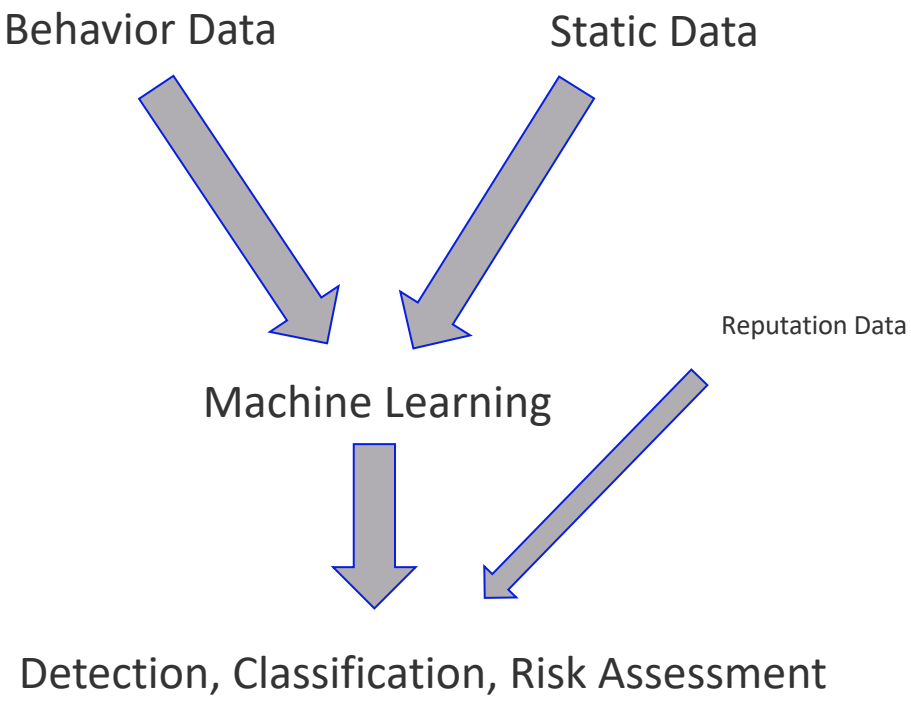
Kill Chain Progression

Exploit	Download	Install	C&C	Lateral Activity
Cyphort Chain Heuristics	Cyphort Static, Behavior, Reputation Engines	Cyphort IVP tool	Cyphort Correlation engine	Cyphort Lateral engine
XP alerts	DL alerts	EX alerts	IN alerts	LS alerts

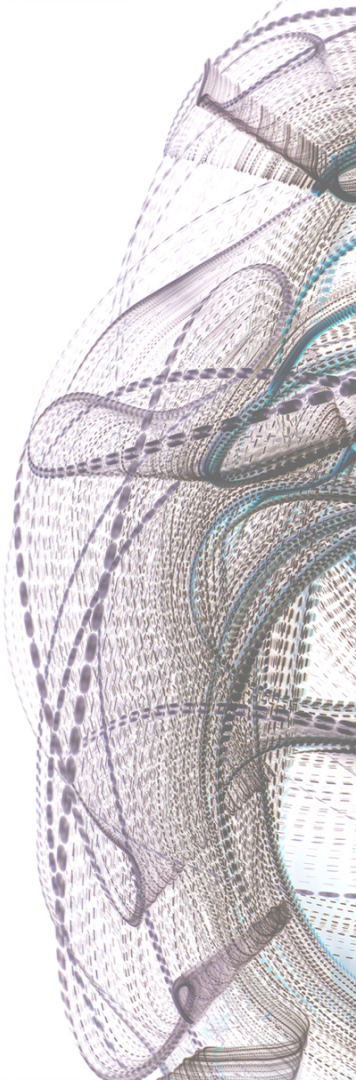


Correlated lateral and perimeter traffic with combined web and email visibility

SECURITY APPLICATIONS - MACHINE LEARNING

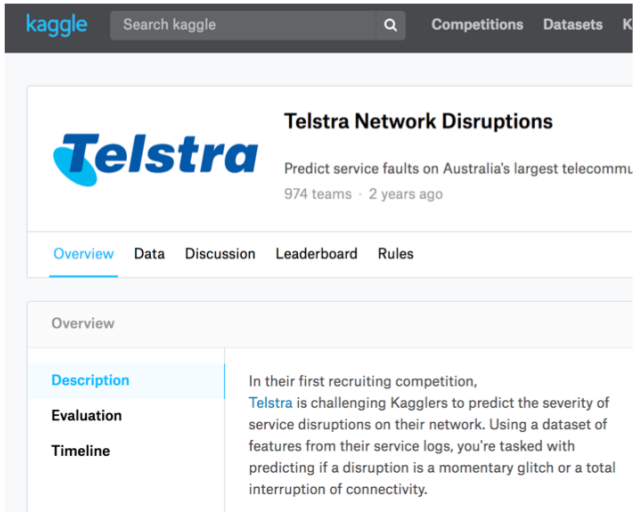


MACHINE LEARNING EXAMPLE



KAGGLE ML COMPETITION

Predict service faults on Australia's largest telecommunications network



Source: https://www.kaggle.com/c/telstra-recruiting-network

JUNIPER NETWORKS

KDD CUP 1999 ANOMALY TRAFFIC DETECTION

NATIONAL CONFERENCE
ON RECENT TRENDS AND
ADVANCES IN COMPUTING,
COMMUNICATION AND SECURITY

NSL KDD Cup 99 dataset Anomaly Detection using Machine Learning Technique

An Experiment and evaluation using Decision Tree

Source: https://www.slideshare.net/SujeetSuryawanshi/nsl-kdd-cup-99-dataset-anomaly-detection-using-machine-learning-technique

ML SAMPLE TEST DATA AND FEATURES

Sample traffic data

kddcup.data_10_percent

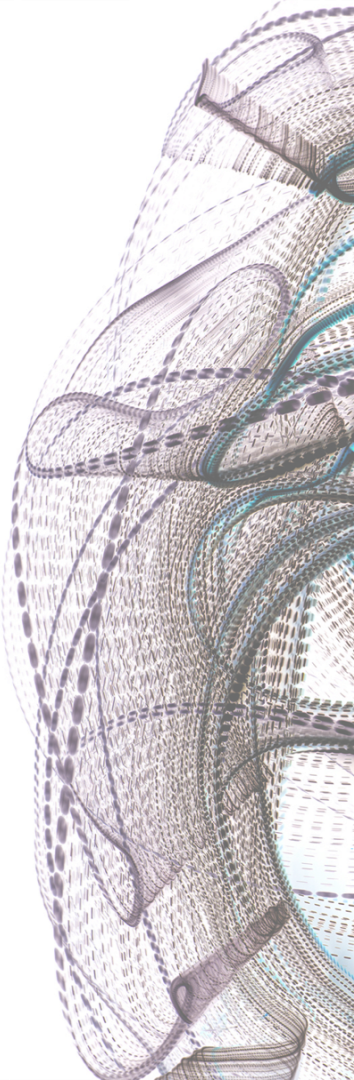
```
0,tcp,http,SF,181,5450,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,8,8,0.00,0.00,0.00,0.00,1.00,0.00,0.00,9,9,1.00,0.00,0.11,0.00,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,239,486,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,8,8,0.00,0.00,0.00,0.00,1.00,0.00,0.00,19,19,1.00,0.00,0.05,0.00,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,235,1337,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,8,8,0.00,0.00,0.00,0.00,1.00,0.00,0.00,29,29,1.00,0.00,0.03,0.00,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,219,1337,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,6,6,0.00,0.00,0.00,0.00,1.00,0.00,0.00,39,39,1.00,0.00,0.03,0.00,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,217,2032,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,6,6,0.00,0.00,0.00,0.00,1.00,0.00,0.00,49,49,1.00,0.00,0.02,0.00,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,217,2032,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,6,6,0.00,0.00,0.00,0.00,1.00,0.00,0.00,59,59,1.00,0.00,0.02,0.00,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,212,1940,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,2,0.00,0.00,0.00,0.00,1.00,0.00,1.00,1,69,1.00,0.00,1.00,0.04,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,159,4087,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,5,5,0.00,0.00,0.00,0.00,1.00,0.00,0.00,11,79,1.00,0.00,0.09,0.04,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,210,151,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,8,8,0.00,0.00,0.00,0.00,1.00,0.00,0.00,8,89,1.00,0.00,0.12,0.04,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,212,786,0,0,0,1,0,1,0,0,0,0,0,0,0,0,0,0,8,8,0.00,0.00,0.00,0.00,1.00,0.00,0.00,8,99,1.00,0.00,0.12,0.05,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,210,624,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,18,18,0.00,0.00,0.00,0.00,1.00,0.00,0.00,18,109,1.00,0.00,0.06,0.05,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,177,1985,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,28,119,1.00,0.00,0.04,0.04,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,222,773,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,11,11,0.00,0.00,0.00,0.00,1.00,0.00,0.00,38,129,1.00,0.00,0.03,0.04,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,256,1169,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,4,4,0.00,0.00,0.00,0.00,1.00,0.00,0.00,4,139,1.00,0.00,0.25,0.04,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,241,259,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,14,149,1.00,0.00,0.07,0.04,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,260,1837,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,11,11,0.00,0.00,0.00,0.00,1.00,0.00,0.00,24,159,1.00,0.00,0.04,0.04,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,241,261,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,2,2,0.00,0.00,0.00,0.00,1.00,0.00,0.00,34,169,1.00,0.00,0.03,0.04,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,257,818,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,12,12,0.00,0.00,0.00,0.00,1.00,0.00,0.00,44,179,1.00,0.00,0.02,0.03,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,233,255,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,2,8,0.00,0.00,0.00,0.00,1.00,0.00,0.00,25,54,189,1.00,0.00,0.02,0.03,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,233,504,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,7,7,0.00,0.00,0.00,0.00,1.00,0.00,0.00,64,199,1.00,0.00,0.02,0.03,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,256,1273,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,17,17,0.00,0.00,0.00,0.00,1.00,0.00,0.00,74,209,1.00,0.00,0.01,0.03,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,234,255,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,5,5,0.00,0.00,0.00,0.00,1.00,0.00,0.00,84,219,1.00,0.00,0.01,0.03,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,241,259,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,12,12,0.00,0.00,0.00,0.00,1.00,0.00,0.00,94,229,1.00,0.00,0.01,0.03,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,239,968,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,3,3,0.00,0.00,0.00,0.00,1.00,0.00,0.00,3,239,1.00,0.00,0.33,0.03,0.00,0.00,0.00,0.00,normal.
0,tcp,http,SF,245,1919,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,13,13,0.00,0.00,0.00,0.00,1.00,0.00,0.00,13,249,1.00,0.00,0.08,0.03,0.00,0.00,0.00,0.00,normal.
```

Features

Results

Attack: YES

Attack: No



JUNIPER NETWORKS

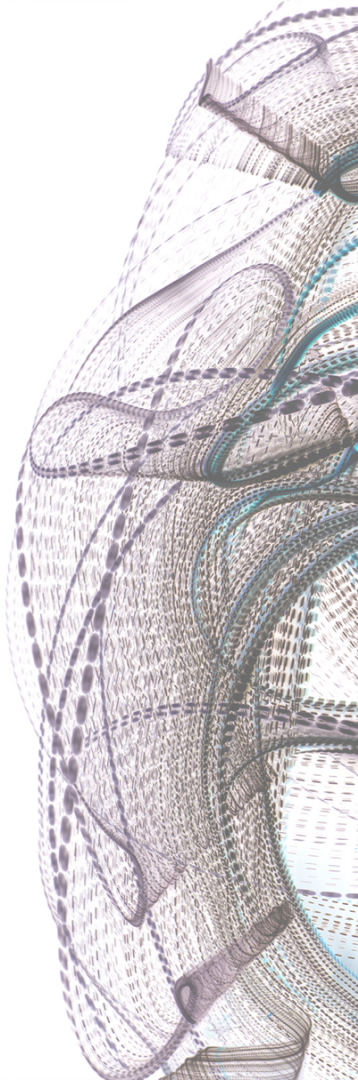
ML SAMPLE TEST DATA AND FEATURES

Features:

```
duration: continuous.
protocol_type: symbolic.
service: symbolic.
flag: symbolic.
src_bytes: continuous.
dst_bytes: continuous.
land: symbolic.
wrong_fragment: continuous.
urgent: continuous.
hot: continuous.
num_failed_logins: continuous.
logged_in: symbolic.
num_compromised: continuous.
root_shell: continuous.
su_attempted: continuous.
num_root: continuous.
num_file_creations: continuous.
num_shells: continuous.
num_access_files: continuous.
num_outbound_cmds: continuous.
is_host_login: symbolic.
is_guest_login: symbolic.
count: continuous.
srv_count: continuous.
serror_rate: continuous.
srv_serror_rate: continuous.
rerror_rate: continuous.
srv_rerror_rate: continuous.
same_srv_rate: continuous.
diff_srv_rate: continuous.
srv_diff_host_rate: continuous.
dst_host_count: continuous.
dst_host_srv_count: continuous.
dst_host_same_srv_rate: continuous.
dst_host_diff_srv_rate: continuous.
dst_host_same_src_port_rate: continuous.
dst_host_srv_diff_host_rate: continuous.
dst_host_serror_rate: continuous.
dst_host_srv_serror_rate: continuous.
dst_host_rerror_rate: continuous.
dst_host_srv_rerror_rate: continuous.
```

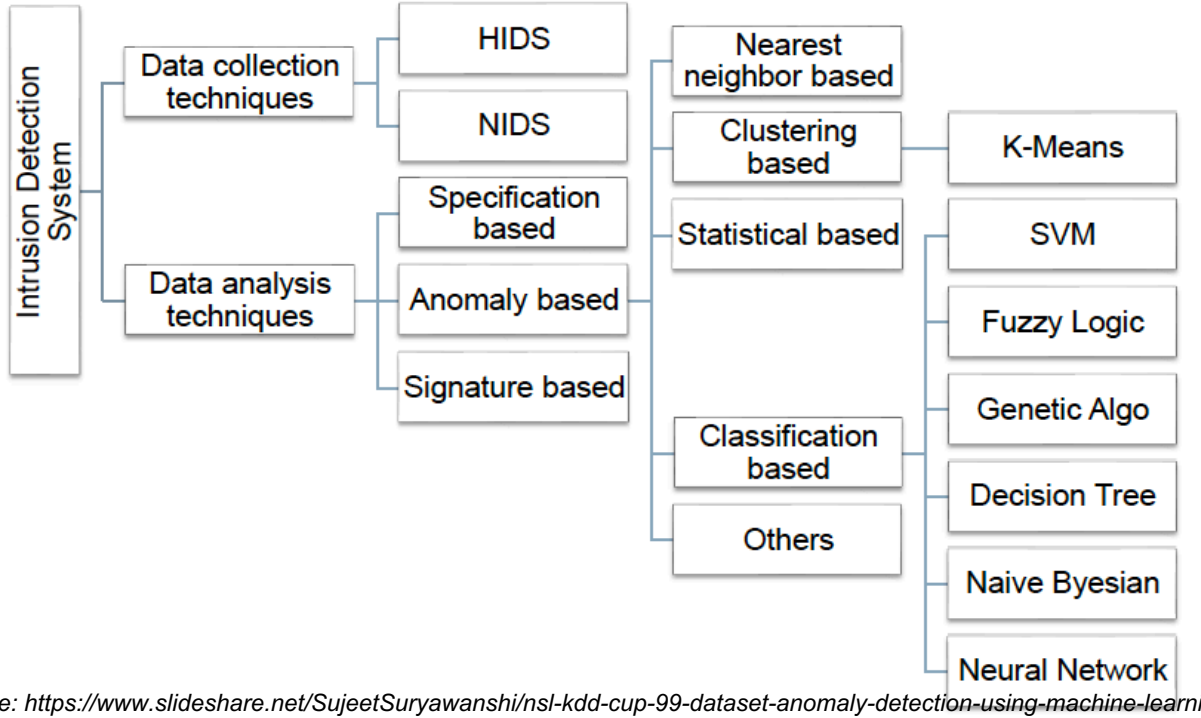
Attack Types

Buffer_overflow
ftp_write
Guess_passwd
Imap
Ipsweep
Land
Loadmodule
Mutlihop
Neptune
Nmap
Normal
Perl
Phf
Pod
Portsweep
Rootkit
Satan
Smurf
Spy
Teardrop
warezclient



JUNIPER NETWORKS

CLASSIFICATION OF IDPS

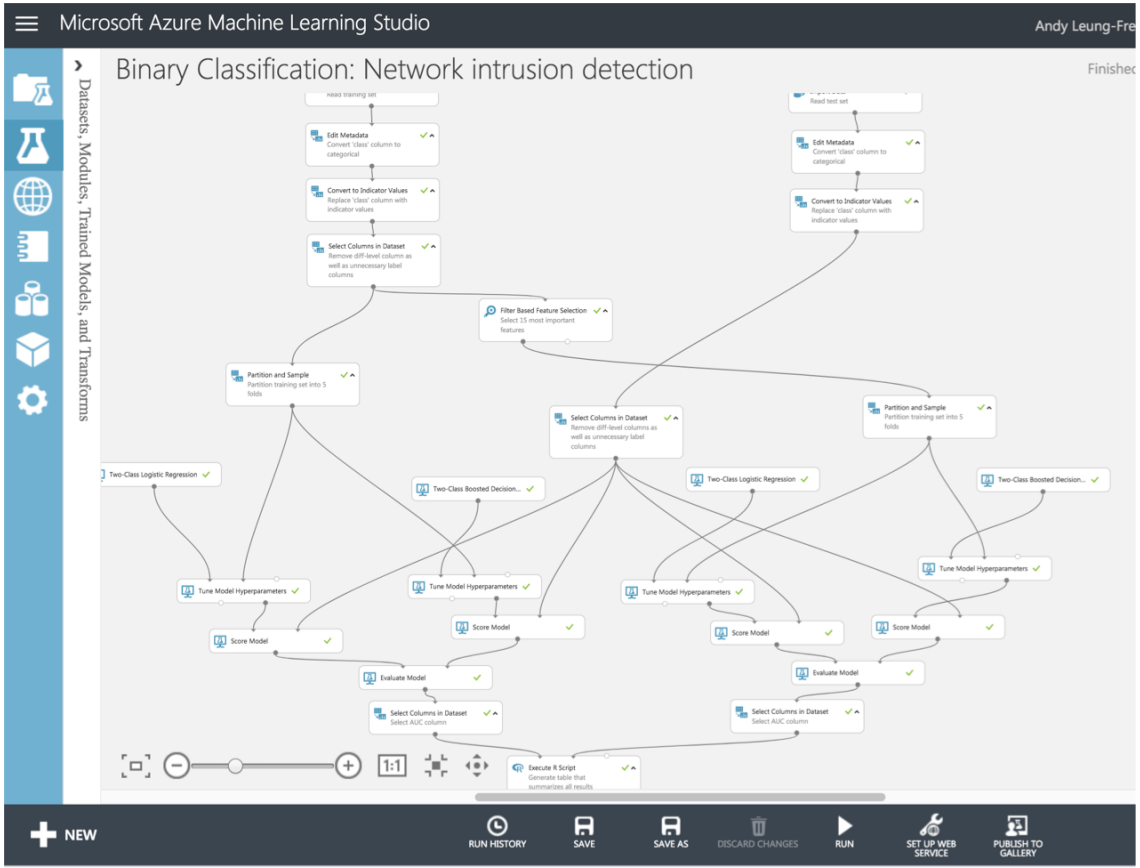


Source: https://www.slideshare.net/SujeetSuryawanshi/nsl-kdd-cup-99-dataset-anomaly-detection-using-machine-learning-technique

TECHNIQUES		Nearest neighbor based detection techniques	Clustering-based anomalies detection techniques	Statistical techniques	Classification techniques
Assumption	Normal data instances	present in dense neighbourhoods	belong to a cluster in the data, lie close to their closest cluster centroid, belong to large and dense clusters,	occur in high probability regions of a stochastic model	A classifier that can distinguish between normal and anomalous classes can be learnt in the given feature space.
	Anomalies	occur far from their closest neighbours	does not belong to any cluster, are far away from their closest cluster centroid, are either too small or too sparse clusters.	occur in the low probability regions of the stochastic model	
Advantages		• Unsupervised/semi-supervised mode • Simplest approach	• Unsupervised • Fast comparison	• Unsupervised and simple • Confidence interval is provided with anomaly score	• Fast testing phase process • Improved efficiency with ensemble methods
Disadvantages		• High computational cost in testing phase • Difficult where several regions are with widely differing densities. • Difficult to identify in case if anomalies are present in groups. • Dependent on the proximity measures used	• High computation cost in cluster formation phase • A data object not belonging to any cluster may be a noise rather than an anomaly • Not suited for large datasets • Fail to label anomalies in certain cases	• Fail to label the anomalies correctly in certain cases • Difficult to find best statistic • For multivariate data it fails to capture the interactions between different attributes	• Heavy dependency and reliability on training data • Class imbalance problem

Source: https://www.slideshare.net/SujeetSuryawanshi/nsl-kdd-cup-99-dataset-anomaly-detection-using-machine-learning-technique

SIMULATION IN MS AZURE ML STUDIO



JUNIPER NETWORKS

ORIGINAL DATA SET

Binary Classification: Network intrusion detection › Convert to Indicator Values › Results dataset

rows	columns
125973	66

view as

duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragmen
0	tcp	ftp_data	SF	491	0	0	0
0	udp	other	SF	146	0	0	0
0	tcp	private	S0	0	0	0	0
0	tcp	http	SF	232	8153	0	0
0	tcp	http	SF	199	420	0	0
0	tcp	private	REJ	0	0	0	0
0	tcp	private	S0	0	0	0	0
0	tcp	private	S0	0	0	0	0
0	tcp	remote_job	S0	0	0	0	0
0	tcp	private	S0	0	0	0	0
0	tcp	private	REJ	0	0	0	0
0	tcp	private	S0	0	0	0	0
0	tcp	http	SF	287	2251	0	0
0	tcp	ftp_data	SF	334	0	0	0

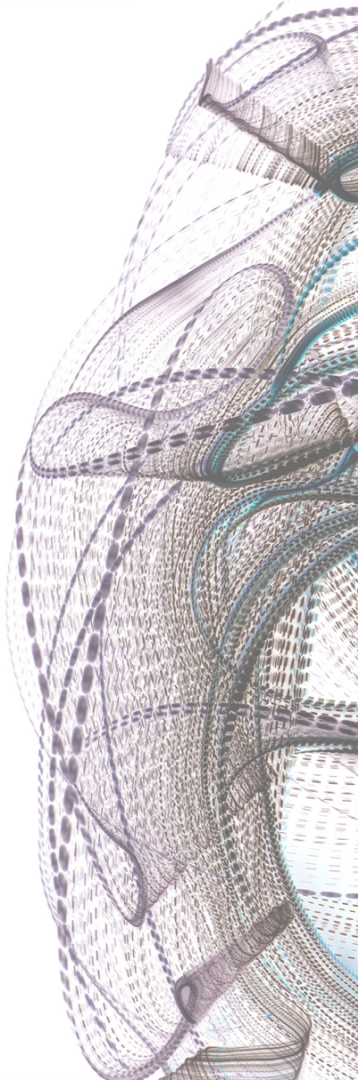
SIMULATION RESULT

Binary Classification: Network intrusion detection › Execute R Script › Result Dataset

rows	columns
4	2

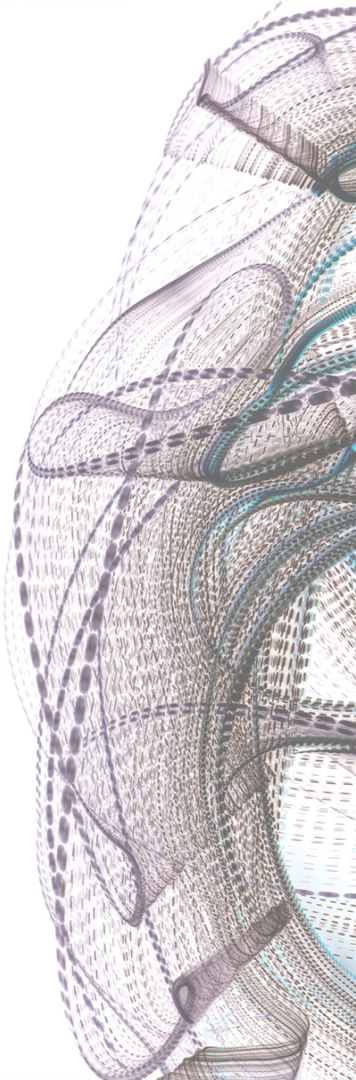
view as

Algorithm, features	AUC
Logistic Regression, all features	0.784702
Boosted Decision Tree, all features	0.925706
Logistic Regression, 15 features	0.893628
Boosted Decision Tree, 15 features	0.920517

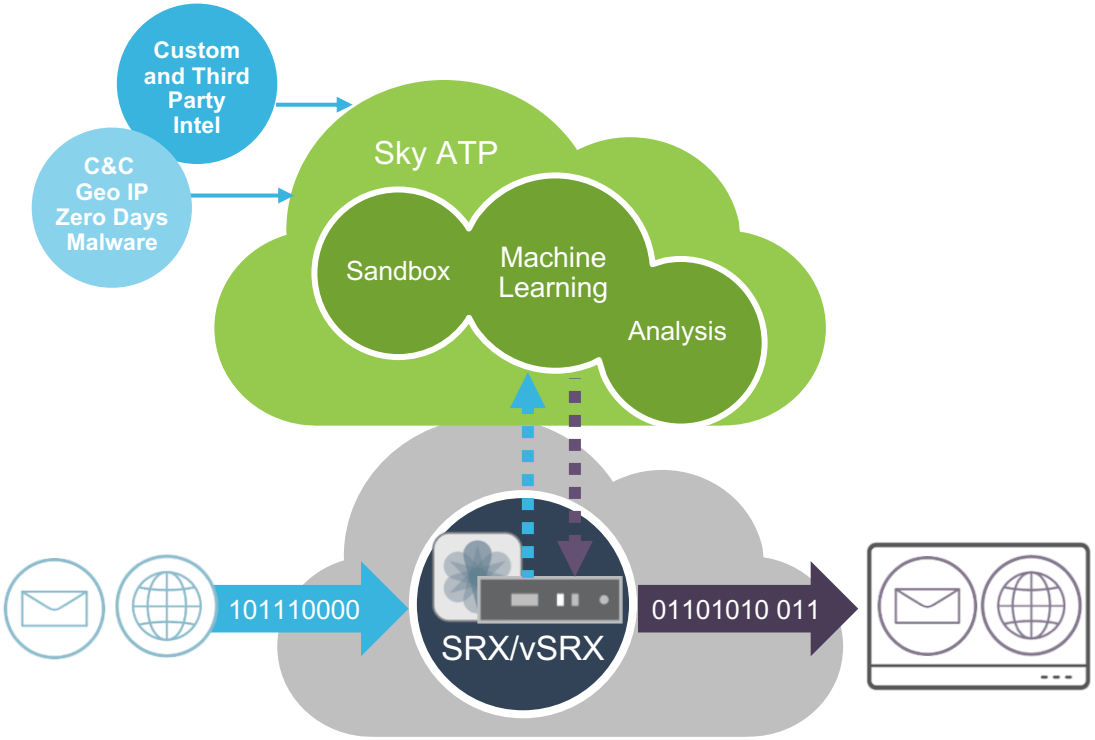


JUNIPER NETWORKS

JUNIPER CLOUD SECURITY SOLUTION



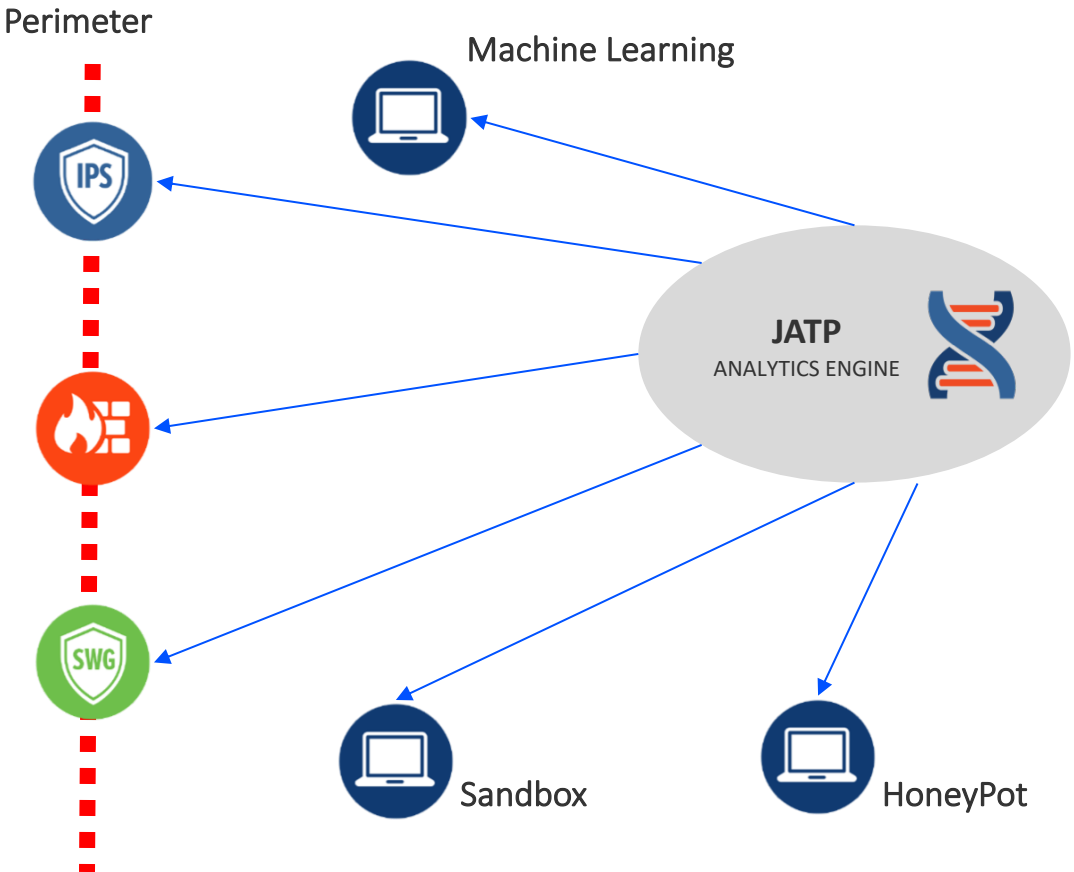
SECURE THE CLOUD WITH
SKY ADVANCED THREAT PREVENTION (ATP) AND JATP



- Protects against advanced malware like ransomware
- Stops advanced persistent threats
- Sophisticated deception techniques to expose evasive malware
- Key component of the Software Defined Secure Networks (SDSN) platform

JATP APPLIANCE

MULTI-LAYER THREAT DETECTION



Mitigation & Enforcement

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

One-touch mitigation for IR teams

Infection Verification

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

JUNIPER JATP: MACHINE LEARNING MODEL GENERATION

Trace File 1

[00000 - 0:063] T(3596) 0x1 = GetVersionExW(out: 6, out: 1, out: 7600, out: 2, out: "")
[00003 - 0:110] + T(3600) 0 = ZwDelayExecution(bool: 0, size: 5000)

Trace File 2

[00019 - 0:140] T(3940) 0x30152 = CreateWindowExW(bits: 0,
[00022 - 0:265] T(3940) 0x103 = RegEnumKeyExW(0xfa,
[00023 - 0:265] T(3940) 0xf8 = CreateFileMappingA(0xffffffff

Trace File 3

[00000 - 0:717] T(3576) 0xd0 = CreateFileW(path: "C:\Program Files\Common Files\plugin_host\P3omQ6uUYGM2888uu7", bits: 0x40000000, bits: 0, 0, enum: 2, bits: 0x80, 0)

Training Set
~ 5K features
~100K samples per file type

Trace Types
Trampoline Hook (winapi)
Kernel Tracer (ktrace)
Emulation (JS, VBA)

Supervised Automated Model Generation

Models Used
Decision Tree + Metacost (2012)
Logistic Regression (2013-2015)
SVM (2013)
Random Forest (with active learning)
CNN experimentation (2017)

Classifier Models

Multiple Classifiers
Different Sensitivity
Classifiers per File Type

Detection

JATP: KILL CHAIN ALIGNMENT

CYPHORT

DASHBOARD | INCIDENTS | FILE UPLOADS | MITIGATION | REPORTS | CUSTOM RULES | CONFIG | REFRESH | HEALTH: | LOG OUT

All Incidents (64 shown, 64 total)

Search: | Show Threat | All Zones | Last Week

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	Poisonlvy_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:

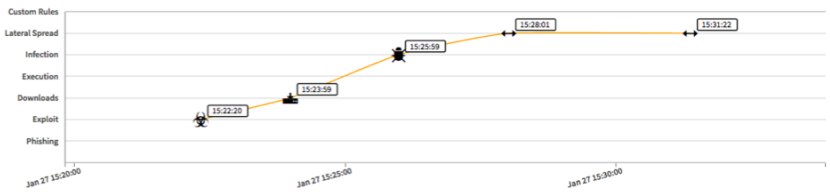
DELIVERY → EXPLOITATION & INSTALLATION → COMMAND & CONTROL → ACTION ON TARGETS

Phishing	Exploits	Downloads	Executions	Infections	Custom Rules	Lateral Spread
0	1	1	0	1	0	2

Triggers:

Reputation | Behavior | Network | Static

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



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

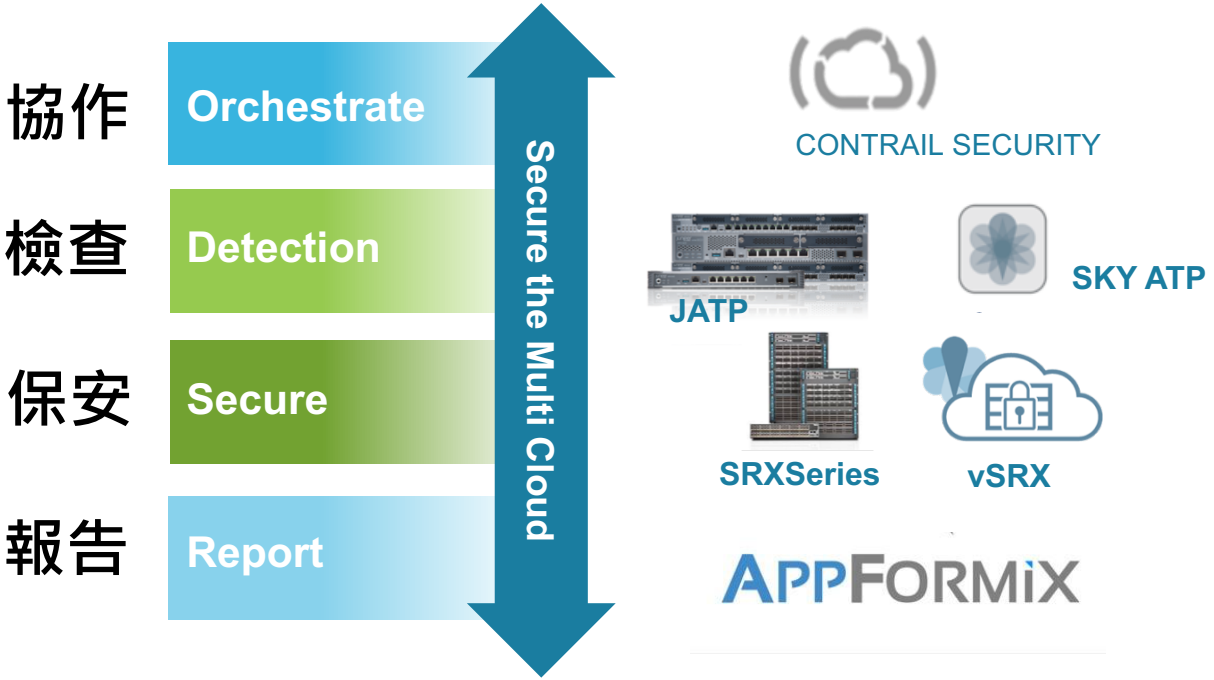
- Almost fileless malware! Uses obfuscated Javascript and 'garbage' batch files

……..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 MULTI CLOUD SECURITY



SECURITY PORTFOLIO

Price / Performance, Scale and Efficacy Leadership

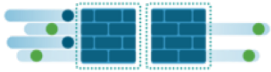
SDSN

Security Director

Sky ATP

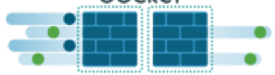
JATP Appliance

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	1RU 80Gb/s	2H-18 3RU 320Gb/s	5RU 480Gb/s	8RU 960Gb/s	16RU 2Tb/s
SRX300	SRX550	SRX1500	SRX4100	SRX4200	SRX4600	★	SRX5400	SRX5600	SRX5800

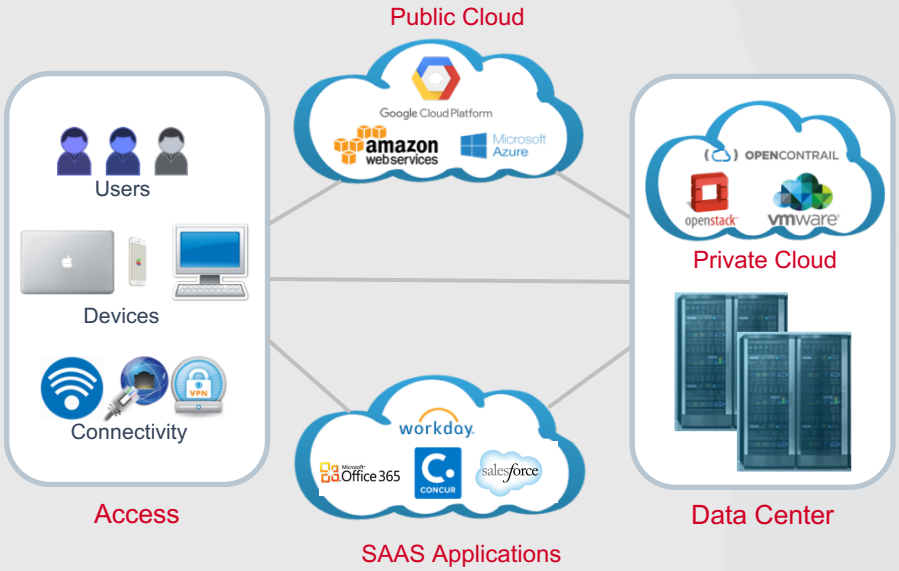
More NGFW Performance and Features in 2018

Branch → Campus → Data Center → Cloud → Service Provider

CLOUD SECURITY ENFORCEMENT

Orchestration

Pervasive Security without complexity



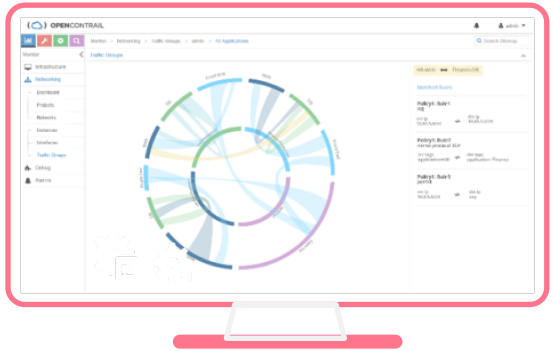
- Consistent security for on premise & Cloud
- User and Application Mobility
- Enforcement at Network & Firewall Layers
- Eco-System Approach

CONTRAIL SECURITY

Orchestration

Application Flow Visualization & Policy Config

Discover Inter- and Intra-application traffic flows without enforcing policies

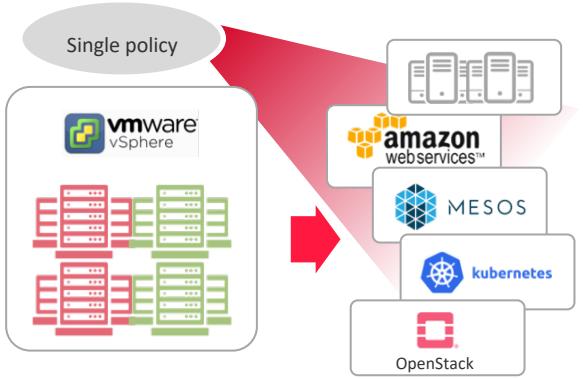


- *Offer visualization, analytics, and orchestration for security configurations*
- *Provide reporting, troubleshooting and compliance*

Consistent Automated Intent-driven Policy

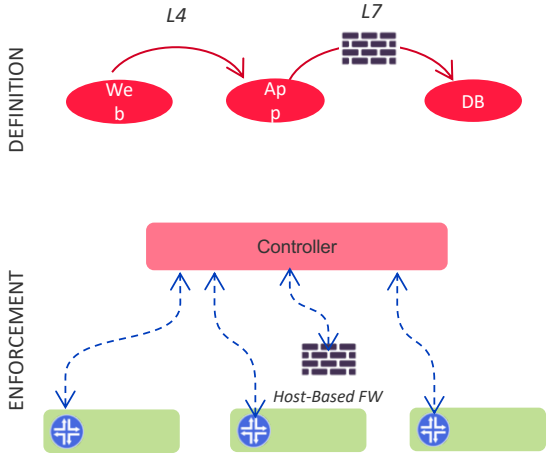
Security Admin

No Policy Rewrite …
Define Once → Enforce Everywher



- *How to extend the same set of policies to Mesos, AWS, Kubernetes, Bare Metal Servers → without policy rule explosion*

Scalable & Performant Multi-point Enforcement



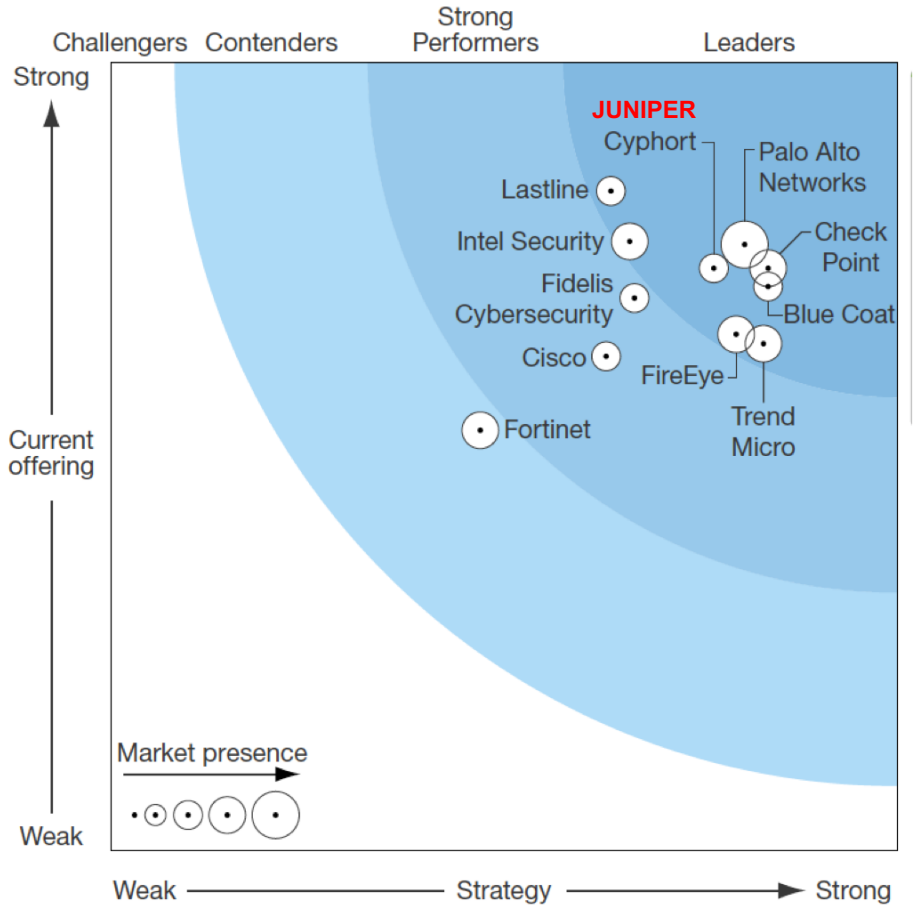
- *L4 Enforcement at the vRouter*
- *L7 enforcement at the L7 Firewall*

Secure

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

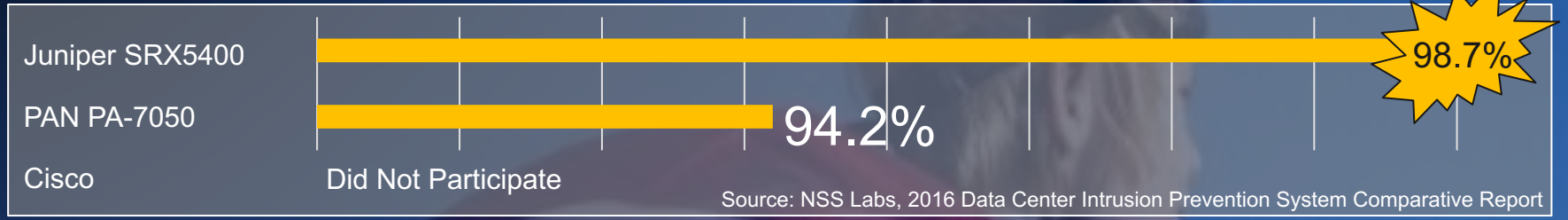


Source: Forrester Report Malware Analysis 2016

Secure

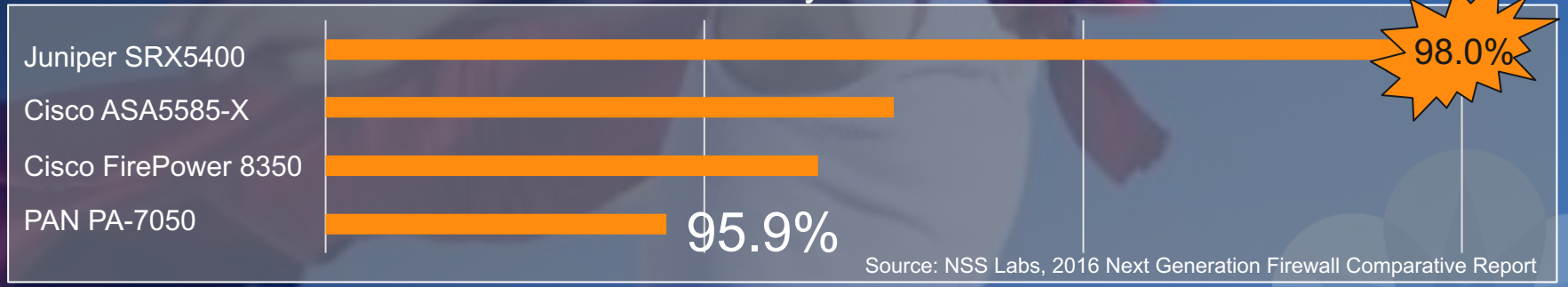
JUNIPER SECURITY, SUPERIOR EFFICACY

Data Center Intrusion Prevention System – Security Effectiveness



Source: NSS Labs, 2016 Data Center Intrusion Prevention System Comparative Report

Next Generation Firewall – Security Effectiveness



Source: NSS Labs, 2016 Next Generation Firewall Comparative Report

Reporting

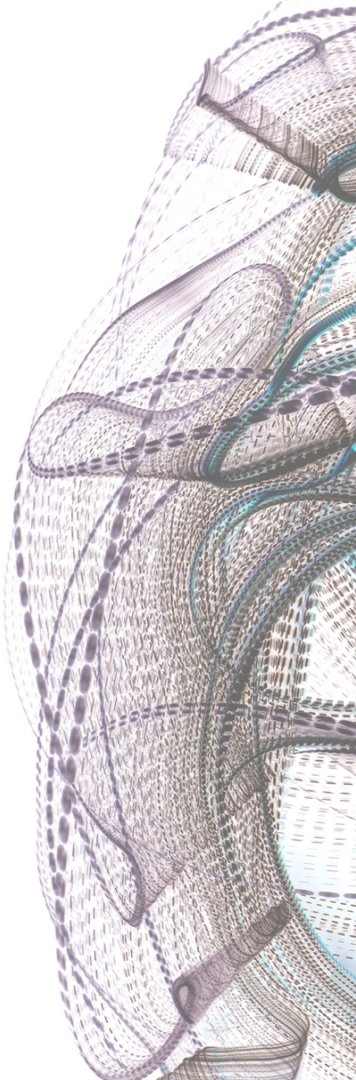
Report

APPFORMIX

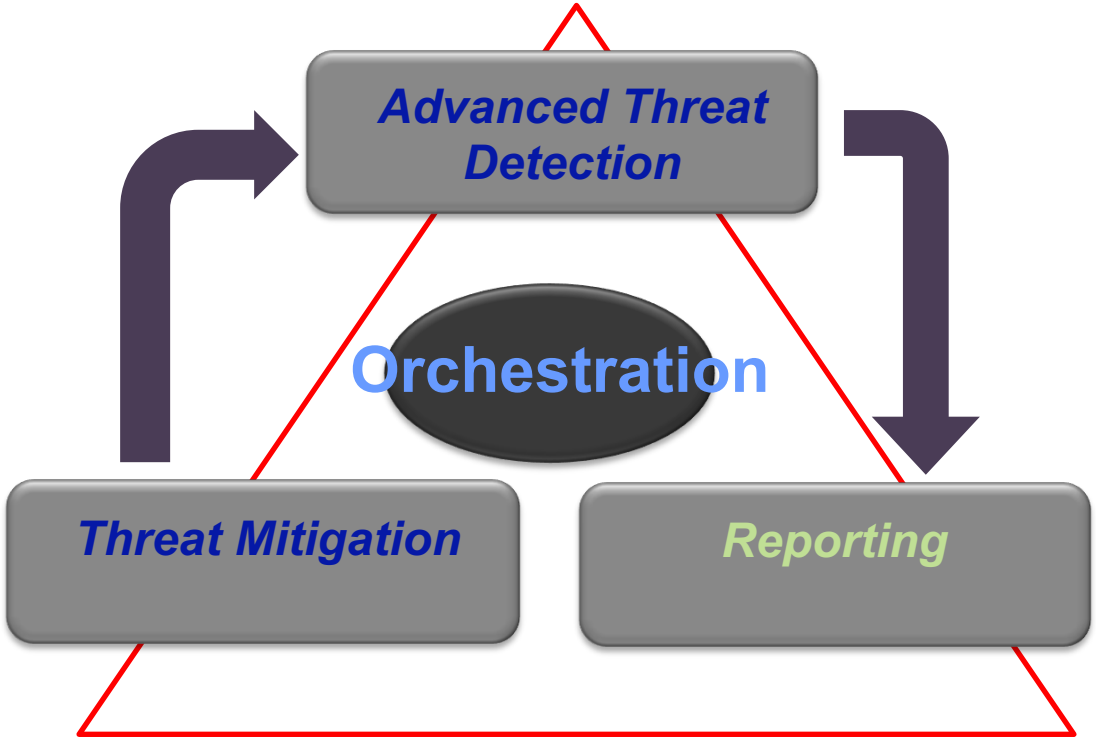
IT AUTOMATION → DEVOPS READY

OPERATIONS ANALYTICS	STATE-DRIVEN ORCHESTRATION	ROLE-BASED MONITORING & ALARMS	DATA-DRIVEN CAPACITY PLANNING
Stream analysis for real-time risk analysis	Prevent service disruptions	Know your enterprise cloud from the bottom up	Enhance reliability and improve your enterprise cloud ROI

SUMMARY

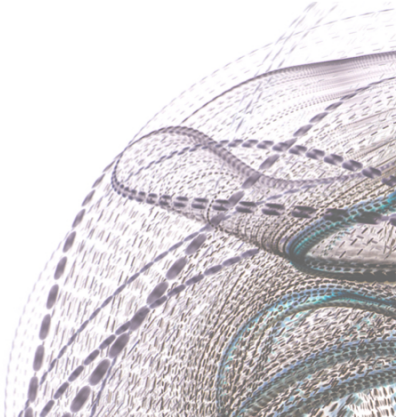


JUNIPER NETWORK CLOUD SECURITY



- **Detection** – **Machine learning and behavioral analysis** engine continuously collects and detects web, email, and lateral threats that have bypassed first line of security defense
- **Analytics** – **Analytics engine** correlates and consolidates threat info with event data from other security tools, then presents **timeline view** of complete security incident
- **Mitigation** – Creates policies to strengthen in-line security tools against future attacks, and isolate infected hosts – all enforced through **one-touch mitigation**

Thank You



JUNIPER NETWORKS