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
THE MULTICLOUD ENTERPRISE
JUNIPER AND PWC LED 200+ TECH INTERVIEW

**REGIONS**
67% are from United States/Canada
- Central Asia 8%
- Other 3%
- South/Central America 1%
- Europe 15%
- Australia 2%
- Singapore or Hong Kong 4%

**ROLES**
52% are CIO / Head of IT within IT organizations
- Influencers 10%
- VP/Manager of IT 38%
- CIO / Head of IT 52%
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

Single vendor, 27%

Multi-vendor, 73%

23% 77%
23%

36% 64%
36%

Large Medium

Multi-vendor Single vendor

PwC | Enterprise data center buyer survey & interview insights
Source: www.juniper.net
CLOUD DEPLOYMENT STRATEGY

CIO IS PIVOTING TOWARDS

<table>
<thead>
<tr>
<th>CIO</th>
<th>VP/Manager of IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>15%</td>
</tr>
<tr>
<td>Automation and orchestration</td>
<td>17%</td>
</tr>
<tr>
<td>TCO savings</td>
<td>12%</td>
</tr>
<tr>
<td>Agility</td>
<td>11%</td>
</tr>
<tr>
<td>Technology innovation</td>
<td>9%</td>
</tr>
<tr>
<td>Openness</td>
<td>7%</td>
</tr>
<tr>
<td>Universal building blocks</td>
<td>7%</td>
</tr>
<tr>
<td>Carrier grade</td>
<td>7%</td>
</tr>
<tr>
<td>Workload awareness</td>
<td>5%</td>
</tr>
</tbody>
</table>

Source: www.juniper.net
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.
CLOUD SECURITY MODEL
OPERATING AS MULTICLOUD

Public Cloud

Data Center

Public WAN

Data Center

Private WAN

Campus

Branch

Secure

See

Orchestrate

Connect

End to End

CONTRAIL SECURITY

SRX Series

CONTRAIL Enterprise Multicloud

EX / MX / QFX Series

vMX / vSRX

Junos Software
Secure

CONTRAIL

SINGLE SDN / SECURITY DEPLOYMENT
(Offering connectivity & security layer for multiple environments)
SECURING THE CLOUD WITH NEXT GENERATION FIREWALL SERVICES

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

Ingress
- Heuristics for evasive and tunneled apps
- More application signatures
- Open signature language
FLEXIBLE NETWORK ARCHITECTURE IN THE CLOUD

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

- **Signatures**: Rule-Based Detection (i.e.: Antivirus)
- **1st-Generation**: Behavior Analysis with Heuristics
- **2nd-Generation**: Behavior Analysis with Machine Learning

Threat Detection Capability
Correlated lateral and perimeter traffic with combined web and email visibility
SECURITY APPLICATIONS - MACHINE LEARNING

Behavior Data → Static Data → Reputation Data → Machine Learning → Detection, Classification, Risk Assessment
MACHINE LEARNING EXAMPLE
KAGGLE ML COMPETITION

Predict service faults on Australia’s largest telecommunications network

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

<table>
<thead>
<tr>
<th>Features</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack: YES</td>
<td>Attack: No</td>
</tr>
<tr>
<td>Sample traffic data</td>
<td>Sample traffic data</td>
</tr>
</tbody>
</table>
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.
um_shells; continuous.
um_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.
srv_rerror_rate; continuous.
srv_ulevs_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_diff_srv_port_rate; continuous.
dst_host_same_dport_rate; continuous.
dst_host_diff_host_rate; continuous.
dst_host_same_src_port_rate; continuous.
dst_host_srv_rate; continuous.
dst_host_srv_serror_rate; continuous.
dst_host_srv_rerror_rate; continuous.

Attack Types

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

- Intrusion Detection System
  - Data collection techniques
    - HIDS
    - NIDS
  - Data analysis techniques
    - Specification based
    - Anomaly based
    - Signature based
    - Nearest neighbor based
    - Clustering based
    - Statistical based
    - Classification based
    - Others
    - K-Means
    - SVM
    - Fuzzy Logic
    - Genetic Algo
    - Decision Tree
    - Naive Byesian
    - Neural Network

Source: https://www.slideshare.net/SujeetSuryawanshi/nsl-kdd-cup-99-dataset-anomaly-detection-using-machine-learning-technique
<table>
<thead>
<tr>
<th>TECHNIQUES</th>
<th>Nearest neighbor based detection techniques</th>
<th>Clustering-based anomalies detection techniques</th>
<th>Statistical techniques</th>
<th>Classification techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assumption</td>
<td>Normal data instances present in dense neighbourhoods</td>
<td>belong to a cluster in the data, lie close to their closest cluster centroid, belong to large and dense clusters, does not belong to any cluster, are far away from their closest cluster centroid, are either too small or too sparse clusters.</td>
<td>occur in high probability regions of a stochastic model</td>
<td>A classifier that can distinguish between normal and anomalous classes can be learnt in the given feature space.</td>
</tr>
<tr>
<td>Anomalies</td>
<td>occur far from their closest neighbours</td>
<td>occur in the low probability regions of the stochastic model</td>
<td>Fast testing phase process</td>
<td></td>
</tr>
<tr>
<td>Advantages</td>
<td>• Unsupervised/semi-supervised mode • Simplest approach</td>
<td>• Unsupervised • Fast comparison</td>
<td>• Unsupervised and simple • Confidence interval is provided with anomaly score</td>
<td>• Improved efficiency with ensemble methods</td>
</tr>
<tr>
<td>Disadvantages</td>
<td>• 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</td>
<td>• 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</td>
<td>• 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 variables</td>
<td>• Heavy dependency and reliability on training data • Class imbalance problem</td>
</tr>
</tbody>
</table>

Source: https://www.slideshare.net/SujeetSuryawanshi/nsl-kdd-cup-99-dataset-anomaly-detection-using-machine-learning-technique
SIMULATION IN MS AZURE ML STUDIO
## ORIGINAL DATA SET

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

<table>
<thead>
<tr>
<th>duration</th>
<th>protocol_type</th>
<th>service</th>
<th>flag</th>
<th>src_bytes</th>
<th>dst_bytes</th>
<th>land</th>
<th>wrong_fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>tcp</td>
<td>ftp_data</td>
<td>SF</td>
<td>491</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>udp</td>
<td>other</td>
<td>SF</td>
<td>146</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>private</td>
<td>S0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>http</td>
<td>SF</td>
<td>232</td>
<td>8153</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>http</td>
<td>SF</td>
<td>199</td>
<td>420</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>private</td>
<td>REJ</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>private</td>
<td>S0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>private</td>
<td>S0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>remote_job</td>
<td>S0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>private</td>
<td>S0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>private</td>
<td>REJ</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>private</td>
<td>S0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>http</td>
<td>SF</td>
<td>287</td>
<td>2251</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>tcp</td>
<td>ftp_data</td>
<td>SF</td>
<td>334</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
# SIMULATION RESULT

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

<table>
<thead>
<tr>
<th>rows</th>
<th>columns</th>
<th>Algorithm, features</th>
<th>AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2</td>
<td>view as</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Bar chart]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logistic Regression, all features</td>
<td>0.784702</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Boosted Decision Tree, all features</td>
<td>0.925706</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logistic Regression, 15 features</td>
<td>0.893628</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Boosted Decision Tree, 15 features</td>
<td>0.920517</td>
</tr>
</tbody>
</table>
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

Perimeter

Machine Learning

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)

IPS

Sandbox

HoneyPot

SWG
JUNIPER JATP: MACHINE LEARNING MODEL GENERATION

Trace File 1
[00000 - 0.063] T[13596] 0x1 = GetVersionExW(out: 6, out: 1, out: 7600, out: 2, out: '')
[00003 - 0.110] T[13600] 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, 0x2a, 0x2b, 0x2c, 0x2d, 0xb)

Trace File 3
[00000 - 0.717] T[13576] 0xd0 = CreateFileW(path: "C:\Program Files\Common Files\plugin_host\P3omQ6uUYGM2 888uu", bits: 0x40000000, bits: 0, enum: 2, bits: 0x80, 0)

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

Supervised Automated Model Generation

Classifier Models
Multiple Classifiers
Different Sensitivity
Classifiers per File Type

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

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

Trace File 1
Trace File 2
Trace File 3
JATP: KILL CHAIN ALIGNMENT
## ATP: THREATS PREVENTED

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WannaCry</strong></td>
<td>Exploits vulnerabilities in SMBv1 that allows remote code execution</td>
</tr>
<tr>
<td><strong>Locky</strong></td>
<td>Uses VB macros to download payload, encrypts disk with key obtained from C&amp;C server</td>
</tr>
<tr>
<td><strong>Zepto</strong></td>
<td>Locky variant that renames files with .zepto extension</td>
</tr>
<tr>
<td><strong>Kovter’s</strong></td>
<td>Almost fileless malware! Uses obfuscated Javascript and ‘garbage’ batch files</td>
</tr>
</tbody>
</table>

### 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

協作  Orchestrate
検查  Detection
保安  Secure
報告  Report

Secure the Multi Cloud

CONTRAIL SECURITY

JATP
SKY ATP
SRXSeries
vSRX
APPFORMiX
SECURITY PORTFOLIO

Price / Performance, Scale and Efficacy Leadership

SDSN

More NGFW Performance and Features in 2018

Branch  Campus  Data Center  Cloud  Service Provider
CLOUD SECURITY ENFORCEMENT
Pervasive Security without complexity

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

Access
Devices
Connectivity

Public Cloud
SAAS Applications

Private Cloud
Data Center

Orchestration
CONTRAIL SECURITY

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
- Single policy
- No Policy Rewrite ...
  Define Once → Enforce Everywhere
- 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

Orchestration
- We b
- Ap p
- DB
- Controller
- Host-Based FW
- OpenStack
- MESOS
- kubernetes
- vmware vsphere
- amazon web services

DEFINITION
- DEFINITION

ENFORCEMENT
- ENFORCEMENT
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
# JUNIPER SECURITY, SUPERIOR EFFICACY

## Data Center Intrusion Prevention System – Security Effectiveness

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Security Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper SRX5400</td>
<td>98.7%</td>
</tr>
<tr>
<td>PAN PA-7050</td>
<td>94.2%</td>
</tr>
<tr>
<td>Cisco</td>
<td>Did Not Participate</td>
</tr>
</tbody>
</table>

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

## Next Generation Firewall – Security Effectiveness

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Security Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper SRX5400</td>
<td>98.0%</td>
</tr>
<tr>
<td>Cisco ASA5585-X</td>
<td></td>
</tr>
<tr>
<td>Cisco FirePower 8350</td>
<td></td>
</tr>
<tr>
<td>PAN PA-7050</td>
<td>95.9%</td>
</tr>
</tbody>
</table>

Source: NSS Labs, 2016 Next Generation Firewall Comparative Report
Reporting

IT AUTOMATION

OPERATIONS ANALYTICS
Stream analysis for real-time risk analysis

STATE-DRIVEN ORCHESTRATION
Prevent service disruptions

ROLE-BASED MONITORING & ALARMS
Know your enterprise cloud from the bottom up

DATA-DRIVEN CAPACITY PLANNING
Enhance reliability and improve your enterprise cloud ROI

DEVOPS READY
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