建構IT資安防線-善用雲世代威脅情資實踐區域聯防

SDSN (Software Defined Secure Network)

CT Hu 胡昌臺

Juniper Networks

Engineering Simplicity

AGENDA

Security Challenges and Defenses

Security Intelligent and Automation

SDSN Use cases

Summary

The security model used across the globe

Almost every security solution and approach

point back to what worked in the past

is fundamentally broken

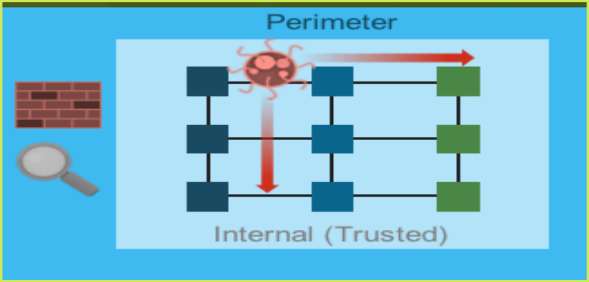
SECURITY CHALLENGE

THREAT SOPHISTICATION

- Advanced, Persistent, Targeted Attacks
- Automated Workflows
- Insider Attacks

CLOUD & IOT

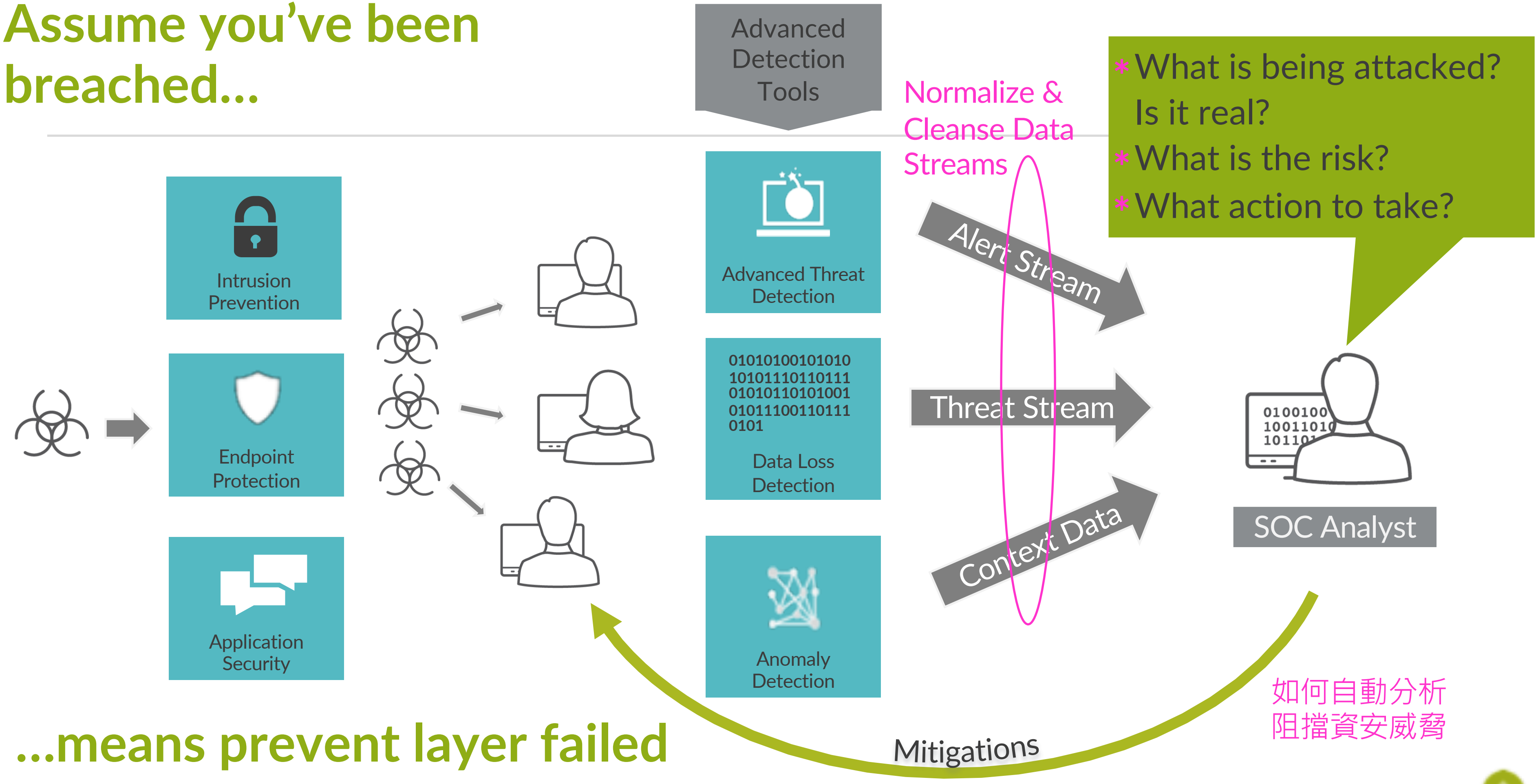
- Application Agility and Scale (Cloud)
- Diversity and Scale (IOT)



CURRENT SECURITY

- Perimeter Only Security
- Complex Rule Sets
- Manual Workflows

Assume you've been breached…



Advanced Detection Tools

Normalize & Cleanse Data Streams

- What is being attacked? Is it real?
- What is the risk?
- What action to take?

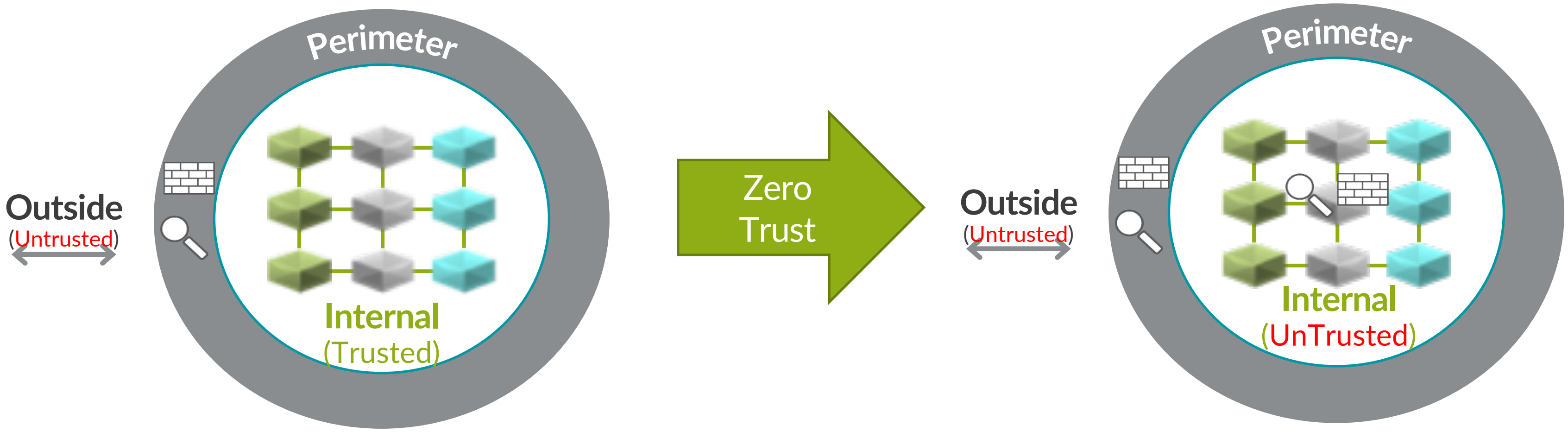
如何自動分析
阻擋資安威脅

…means prevent layer failed

ZERO TRUST SECURITY MODEL

Perimeter Oriented Security

Zero Trust Security Model



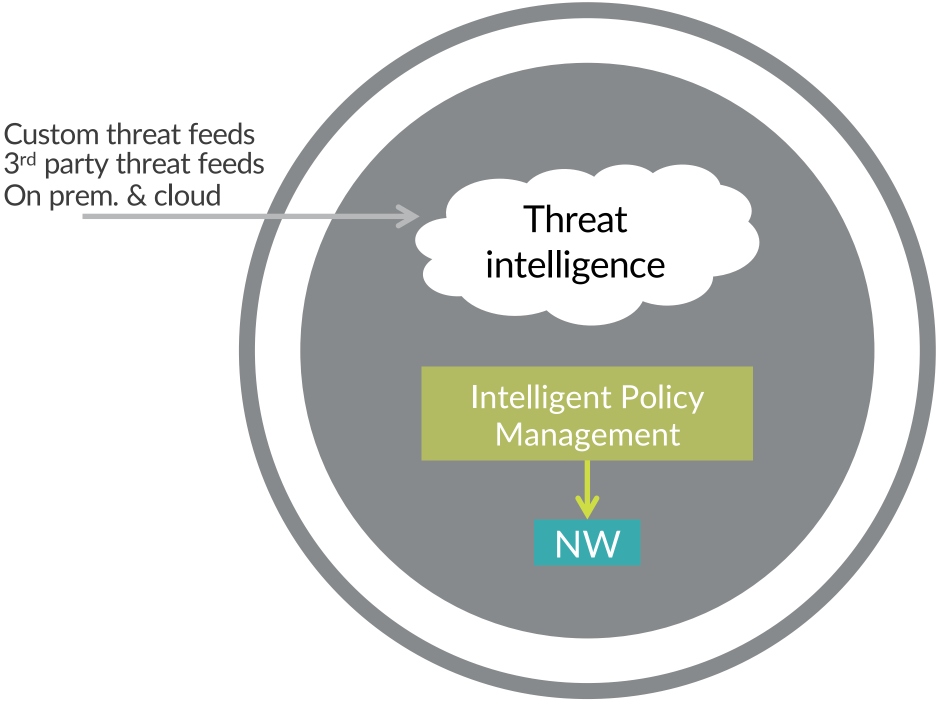
Network Security at Perimeter

Limited Threat Visibility

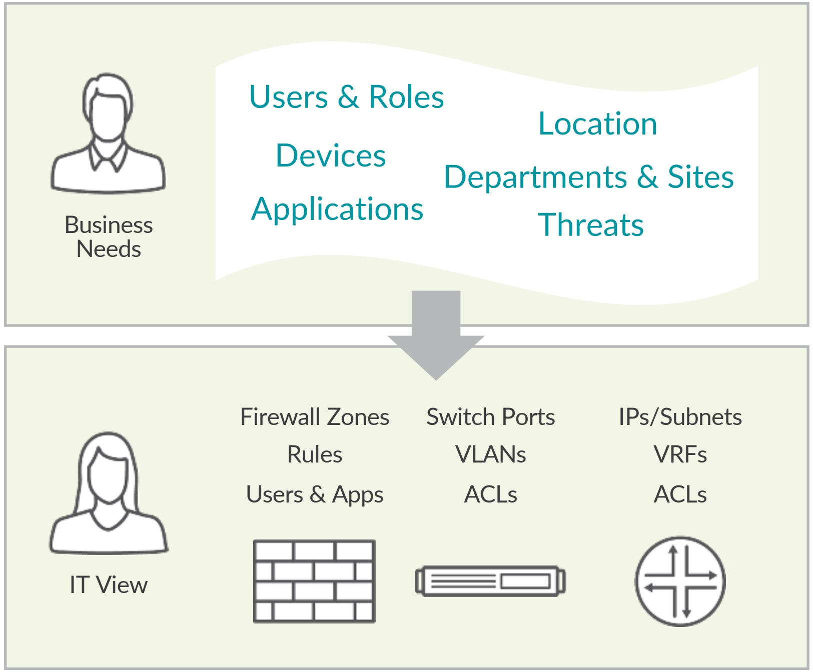
- ✓ Software Defined Secure Network
- ✓ Block Lateral Threat Propagation
- ✓ Comprehensive Threat Visibility

UNIFIED THREAT DETECTION & REAL-TIME PROTECTION

- ✓ Unified threat intelligence platform leveraging cloud economics
- ✓ Automatically normalize threat feeds based on business rules
- ✓ Enforce policy across the network in real-time



SECURITY POLICIES TIED TO BUSINESS OUTCOMES



- User intent based security policies (e.g. R&D workload should be isolated from production workload)
- Dynamic updates (e.g. workloads moving from private cloud to hybrid cloud)
- Correlation with asset and inventory management DBs

CHANGE IN MINDSET

Hardware defined → Software/cloud defined

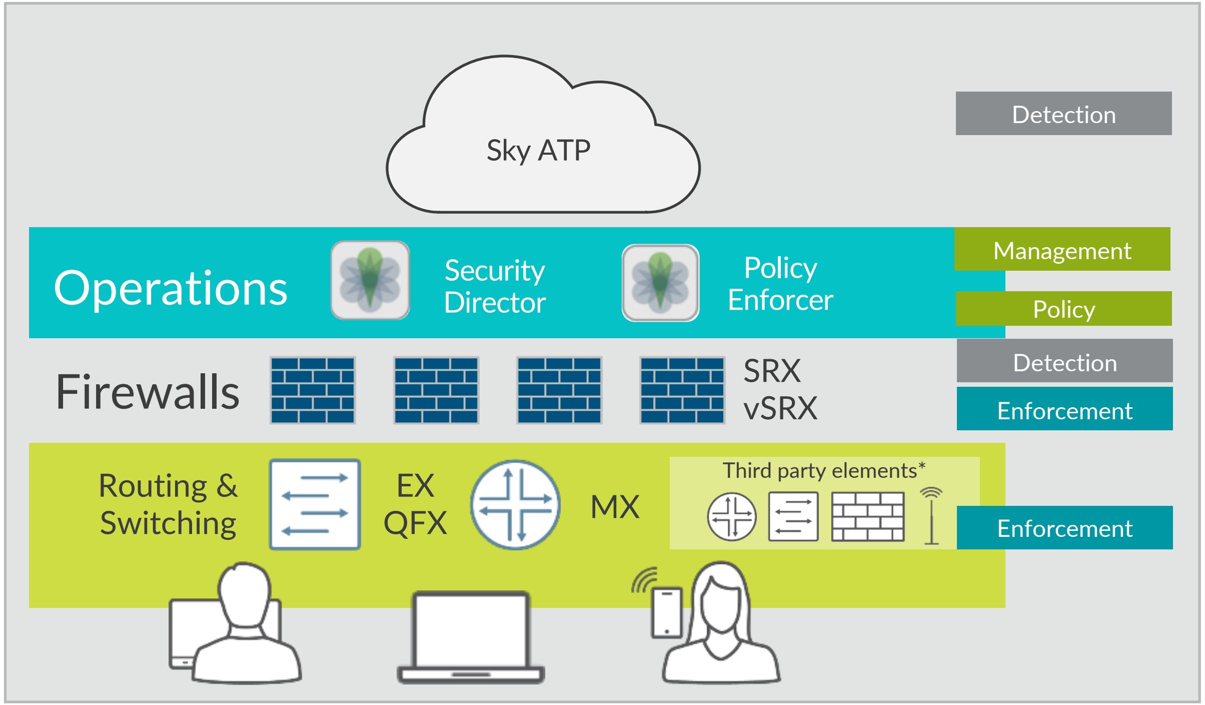
Perimeter → Zero Trust

Manual detection & enforcement → Automated when possible

Configuration driven → Business driven

Closed ecosystem → Open framework

SOFTWARE DEFINED SECURE NETWORKS



Enforcement

Pervasive

Multi-directional

Detection

Cloud-enabled

Multi-vendor

Policy & Mgmt

Automated

Intent Driven

AGENDA

Security Challenges and Defenses

Security Intelligent and Automation

SDSN Use cases

Summary

Current security models are based on time

Providing the ability to detect and prevent a new, previously unseen attack takes time

The solution is almost always an update that identifies the threat, not its behaviour

We need to focus on what something Does, not just what it is

MEMBER OF CYBER THREAT ALLIANCE (CTA)

Shared Intelligence for Better Security

What data intelligence is currently being shared?

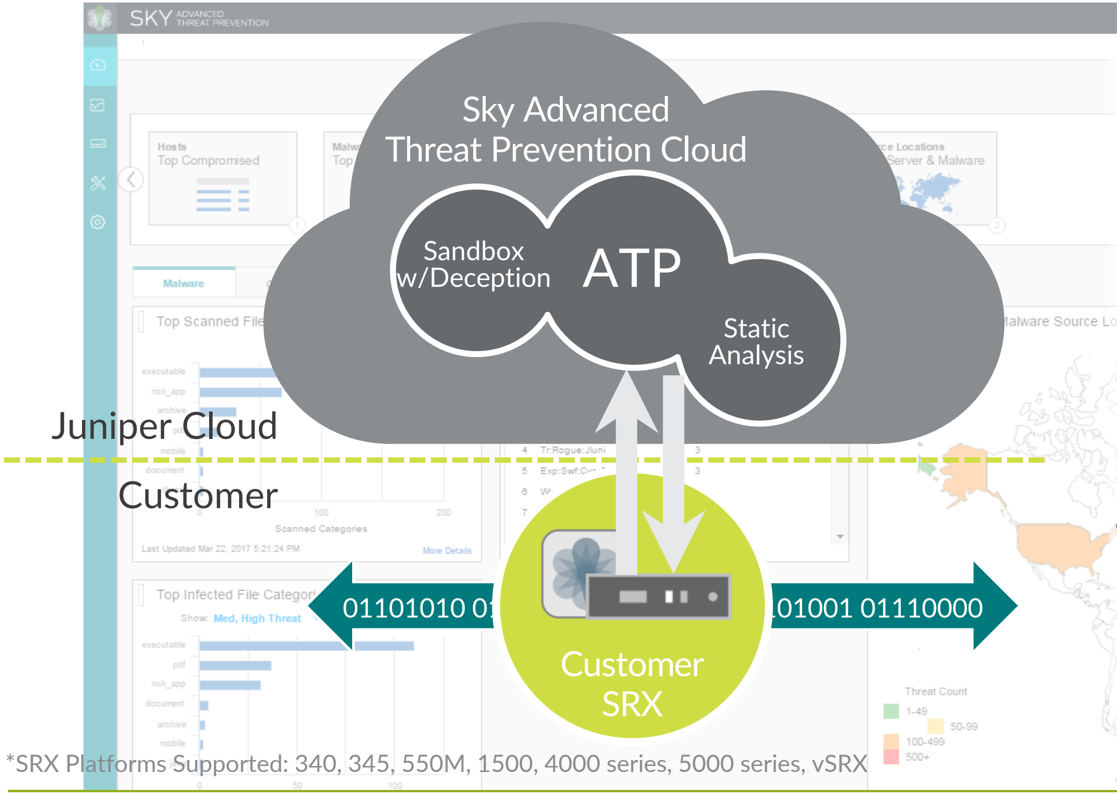
- Approximately 40,000 STIX™ packages per day, averaging over 300,000 points
- Packages include a range of observables and TTPs across the kill chain
- Observables include: files, Uniform Resource Identifiers (URIs), domain names, and addresses
- TTPs: Over 50 TTPs from Mitre's Common Attack Pattern Enumeration and Classification (CAPEC™) and Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)

CYBER THREAT ALLIANCE

Shared threat intelligence – increased protection for customers

Available April 2018

WHAT IS SKY ADVANCED THREAT PREVENTION

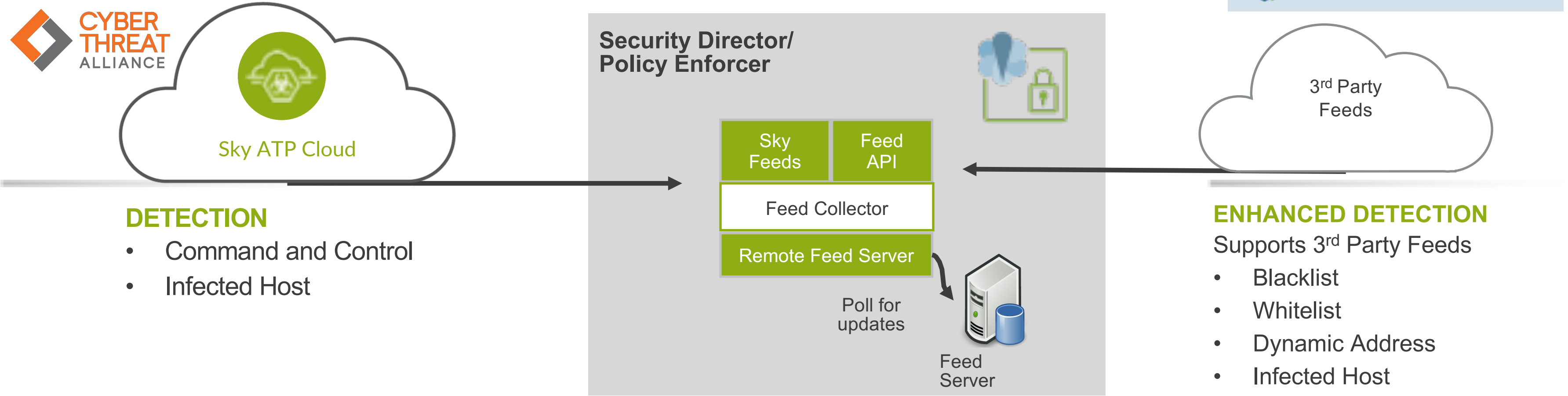


1. SRX extracts potentially malicious objects and files and sends them to the cloud for analysis
2. Known malicious files are quickly identified and dropped before they can infect a host
3. Multiple techniques identify new malware, adding it to the Known Bad list and reporting it to SecOps
4. Correlation between newly identified malware and known C&C sites aids analysis
5. SRX blocks known malicious file downloads and outbound C&C traffic

*SRX Platforms Supported: 340, 345, 550M, 1500, 4000 series, 5000 series, vSRX

CUSTOM FEED API SUPPORT

Threat Remediation of infected hosts leveraging 3rd party threat feeds



DETECTION

- Command and Control
- Infected Host

ENHANCED DETECTION

Supports 3rd Party Feeds

- Blacklist
- Whitelist
- Dynamic Address
- Infected Host

Key Features

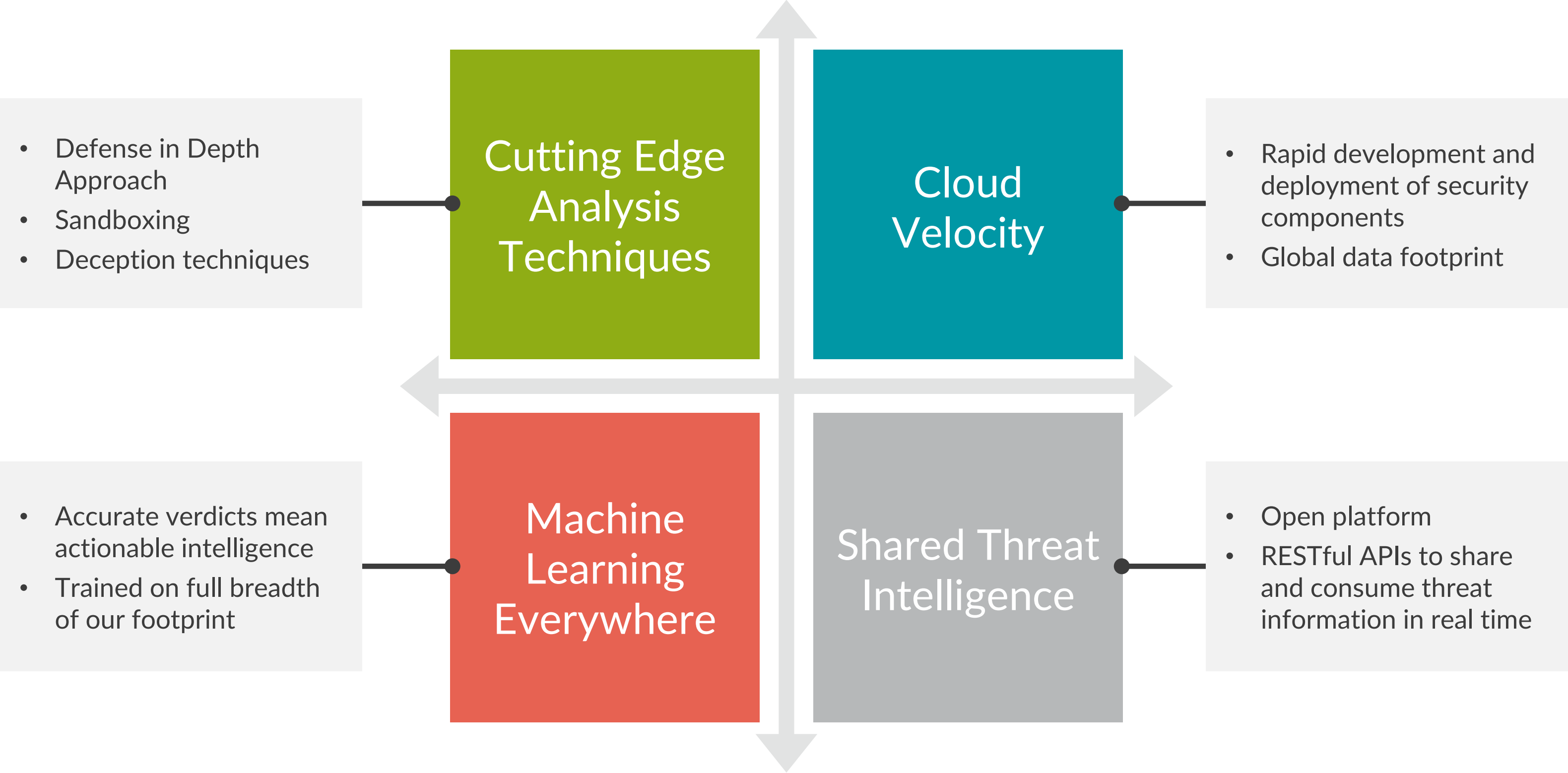
Blacklist: Entities in blacklist always get blocked by SRX
Whitelist: Entities in whitelist always get accepted by SRX
Dynamic Address: Entities in Dynamic Address Group can be used in firewall policy of SRX
Infected Host: Threat Prevention Policy enforced for entities identified as infected hosts

Customer Benefits

Enables customers to leverage existing, trusted threat feed sources to take threat remediation actions w/ Policy Enforce

- Push to PE with “Threat Feed API”, or
- Configure PE to poll from remote feed server

SKY ATP EFFICACY



- Defense in Depth Approach
- Sandboxing
- Deception techniques

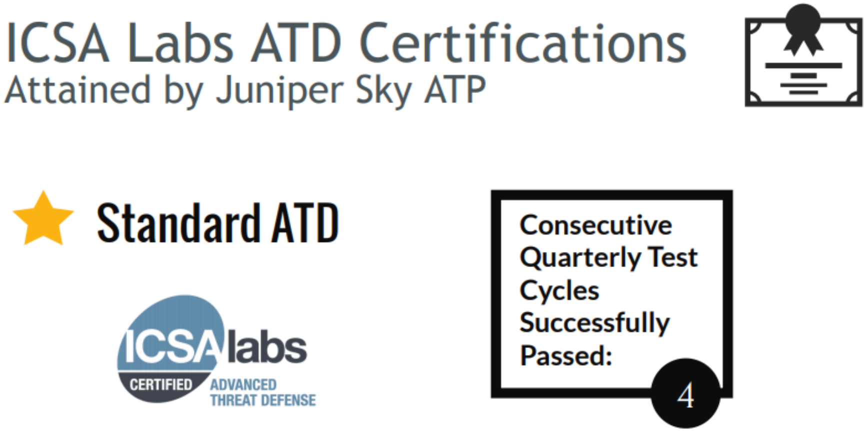
Cutting Edge Analysis Techniques
Cloud Velocity
Machine Learning Everywhere
Shared Threat Intelligence

- Rapid development and deployment of security components
- Global data footprint

- Accurate verdicts mean actionable intelligence
- Trained on full breadth of our footprint

- Open platform
- RESTful APIs to share and consume threat information in real time

SKY ATP ICSA LABS TEST REPORT

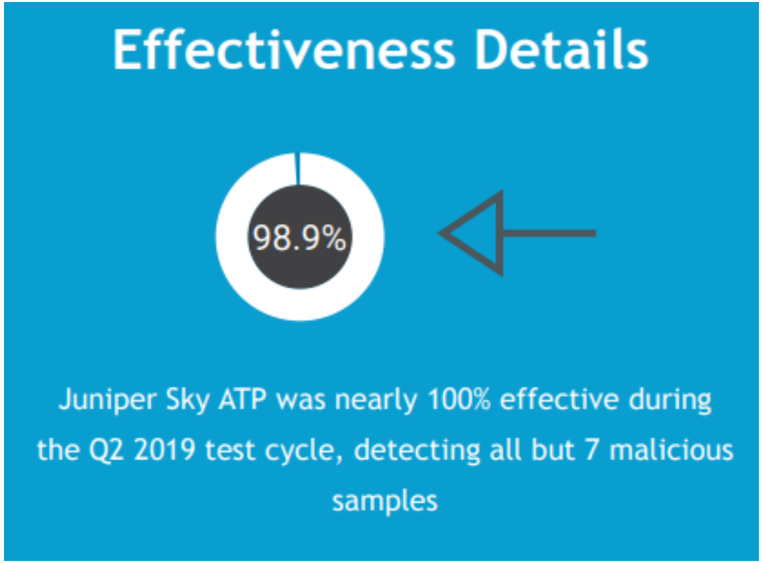


ICSA Labs ATD Certifications
Attained by Juniper Sky ATP

★ Standard ATD

ICSA labs
CERTIFIED
ADVANCED THREAT DEFENSE

Consecutive Quarterly Test Cycles Successfully Passed: 4



Effectiveness Details

98.9%

Juniper Sky ATP was nearly 100% effective during the Q2 2019 test cycle, detecting all but 7 malicious samples

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!

- ✓ **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

AGENDA

Security Challenges and Defenses

Security Intelligent and Automation

SDSN Use cases

Summary

Network Enforcement

The only consistent enforcement point across the business

Embed and Simplify security policies across the entire business

Leverage routing, switching, security and third party technologies

It's time to leverage the
Entire Network

SDSN DEMO

SDSN use case 1:

Threat Remediation of infected hosts for campus/office

DETECTION

Sky ATP – Known & Day-0 Malware analysis, Sandboxing, Infected Host identification, Command & Control, GeoIP

POLICY

Simplified Threat Remediation Policy (Block, Quarantine, Track) defined in Security Director Policy Enforcer

ENFORCEMENT

Juniper: SRX, vSRX, EX and QFX

Key Features

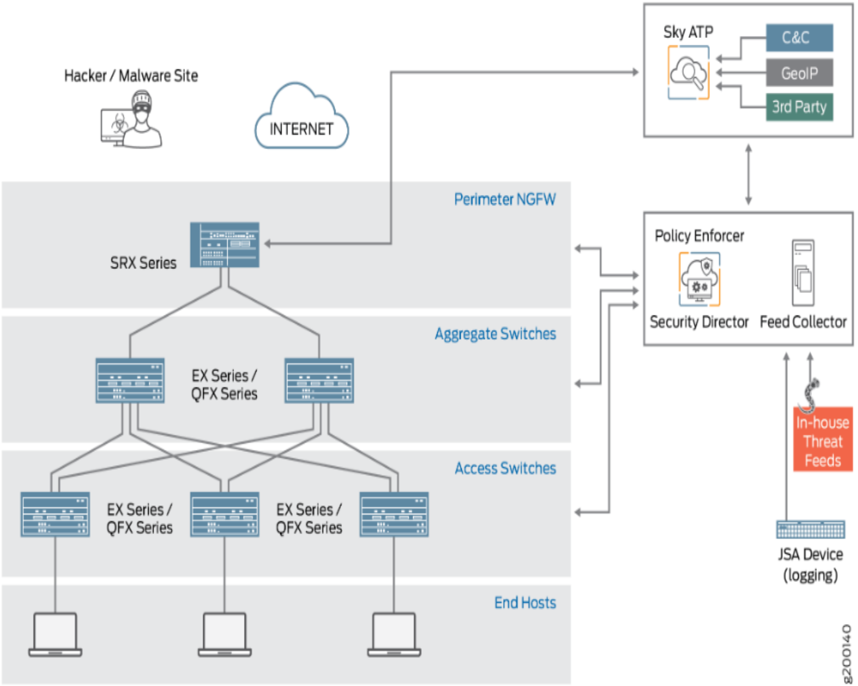
Security Fabric including Firewalls and Switches

Infected Host Blocking

- Perimeter Firewall level for north – south traffic
- EX/QFX switches to protect from lateral movement of threats

Infected Host Tracking

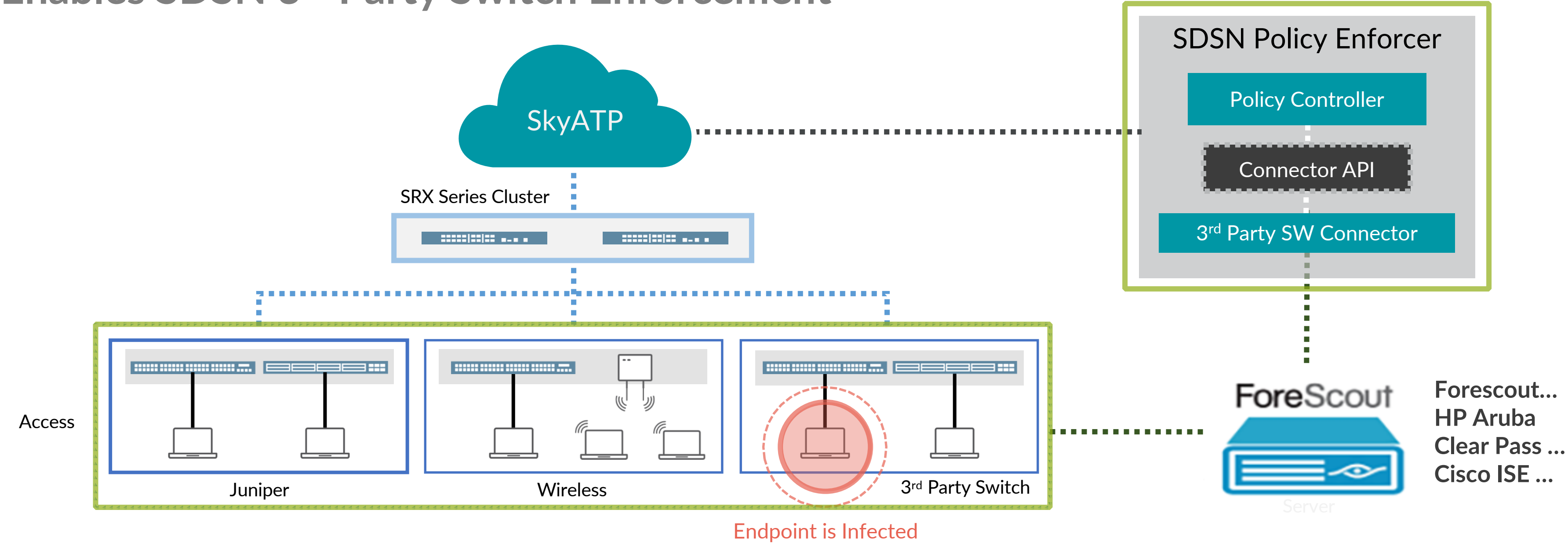
- Track infected host movement in network, and
- Quarantine or block infected hosts even if IP address changes



SDSN use case 2:

3rd Party Switch and Wireless Support

Enables SDSN 3rd Party Switch Enforcement

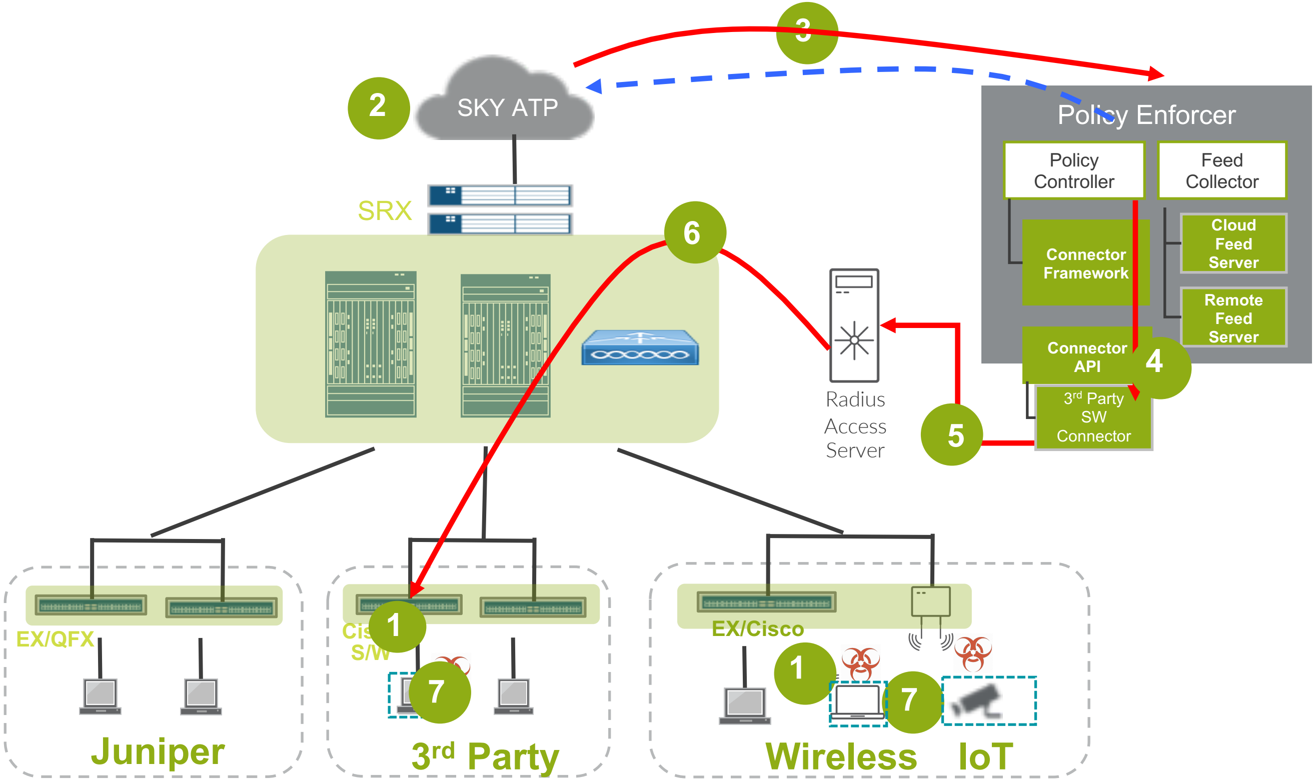


Continuous visibility and control of compromised hosts, preventing laterally spread threats

Available March 2018

SDSN use case 2:

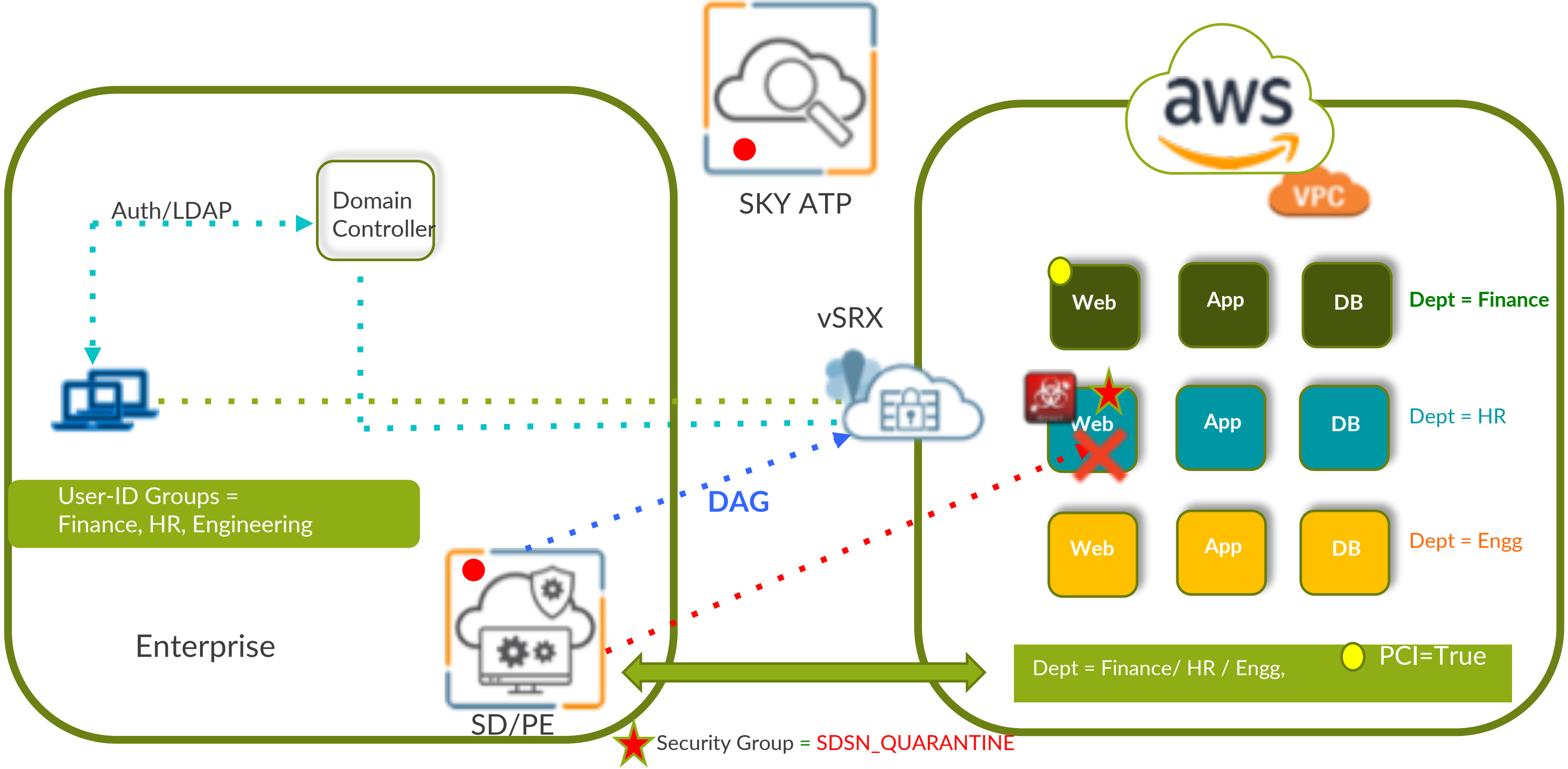
3rd Party Switch and Wireless Support



1. End user authenticates to network via 802.1x or mac authentication
2. Sky detects End Point getting the infected
3. Policy Enforcer downloads the Infected Host Feed.
4. PE enforces the Infected Host policy with the 3rd Party SW Connector calling the generic API
5. 3rd Party Connector
   - queries AAA Server for Endpoint details for Infected Host IP
   - initiates CoA for the Infected Host mac.
6. CoA action could be block or quarantine vlan.
7. Enforcement happens on the NAC device or WLC to block/Quarantine the infected host.
8. Policy enforcer Communicated the end host details back to sky

SDSN use case 3:

Threat Remediation on public Cloud



USER INTENT POLICIES

Security Team

DevOps Team

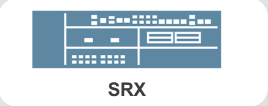
1. DEFINE META DATA

Attribute	Possible Values
STAGE	DEVTEST, STAGING, PROD
PCI	TRUE, FALSE
<custom>	<custom>

2. CREATE RULES

SRC	DEST	ACTIONS
STAGE= DEVTEST	STAGE=PROD <AND> PCI = TRUE	DENY

Rules with DAG



3. ASSIGN META-DATA

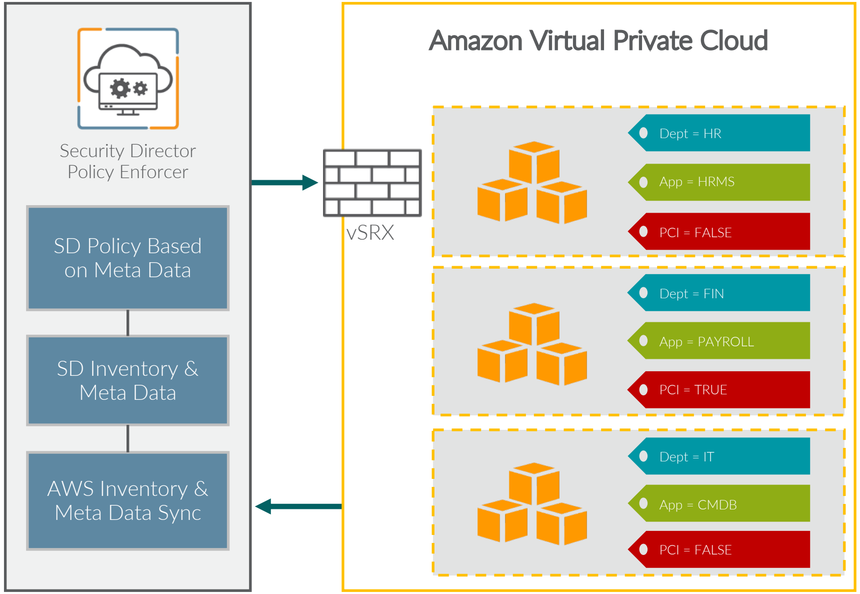
Name	IP Address	META-DATA
Foo	70.20.1.6	STAGE= DEVTEST, PCI=FALSE
Bar	80.10.2.4	STAGE=PROD

DAG updates…
…do not require commit

Benefits:

1. Better fit for cloud based policy workflows
2. Contextual picture about each end point in the network
3. Portable policy across different domains

POLICY ENFORCER – CLOUD INTEGRATION



Challenges

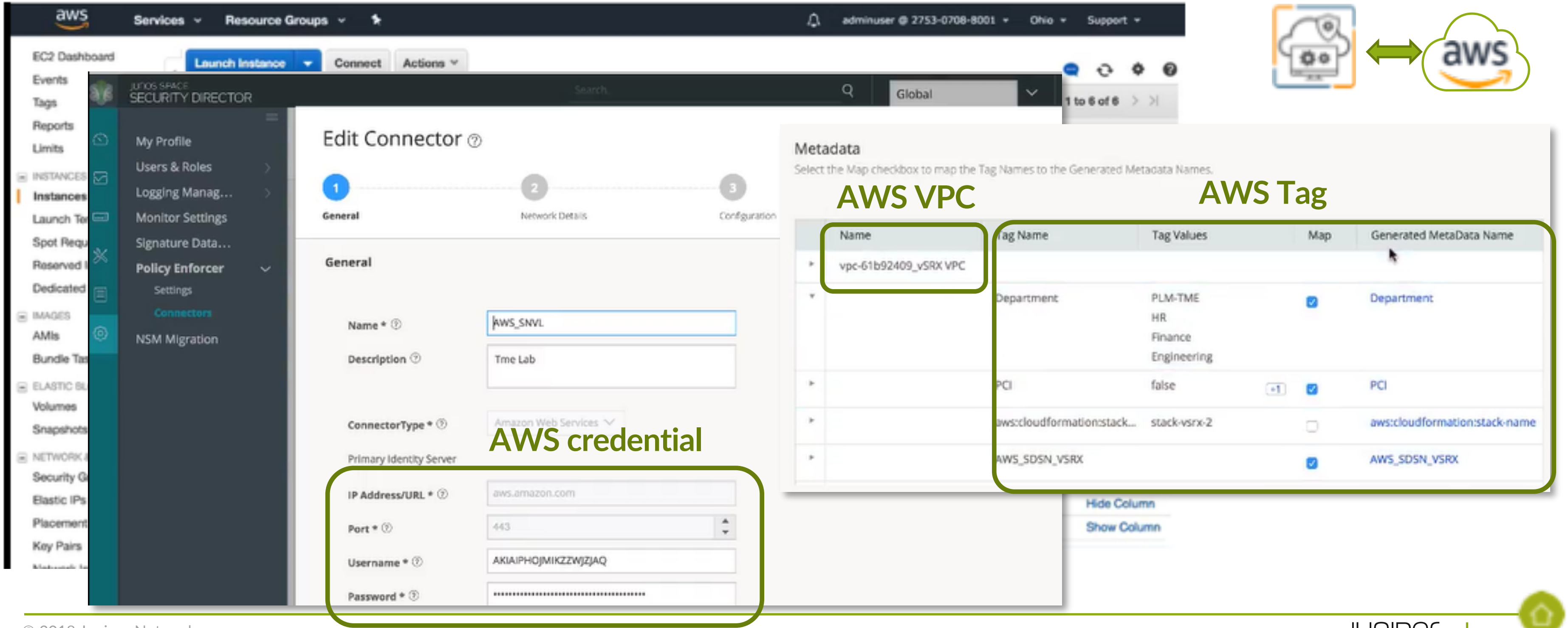
- Security Policy needs to support agile workloads
- Compliance for Amazon Virtual Private Cloud workloads
- Lateral threat propagation inside Amazon VPC

Solution

- Instantiates and manages VPC specific virtual SRX instances
- Policy Enforcer supports meta-data based policies to support agile workloads
- Access Control (L3, L7 FW), IPS and Threat Policies based on meta-data
- AWS workload inventory and meta-data sync up with Security Director

AWS Meta data based Firewall policies

PE connect to AWS and get the meta data information in the VPC



Edit Connector

General

Name *	AWS_SNVL
Description	Tme Lab
ConnectorType *	Amazon Web Services
Primary Identity Server	
IP Address/URL *	aws.amazon.com
Port *	443
Username *	AKIAIPHOJMIKZZWJZJAQ
Password *	••

AWS credential

Metadata

Select the Map checkbox to map the Tag Names to the Generated Metadata Names.

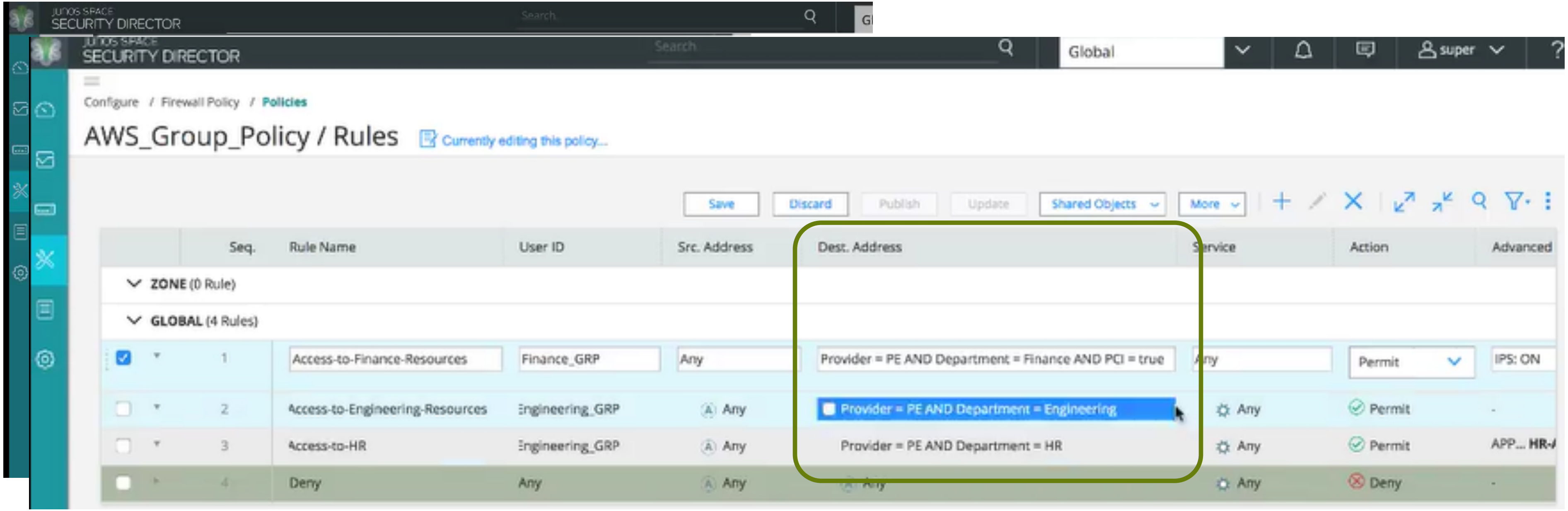
AWS VPC

AWS Tag

Name	Tag Name	Tag Values	Map	Generated MetaData Name
vpc-61b92409_vSRX VPC				
	Department	PLM-TME HR Finance Engineering	☑	Department
	PCI	false +1	☑	PCI
	aws:cloudformation:stack...	stack-vsrx-2	☐	aws:cloudformation:stack-name
	AWS_SDSN_VSRX		☑	AWS_SDSN_VSRX

AWS Meta data based Firewall policies

SD/PE can use security policy with the meta data



JUNOS SPACE SECURITY DIRECTOR
Search
Global
super
Configure / Firewall Policy / Policies
Currently editing this policy...
Save
Discard
Publish
Update
Shared Objects
More

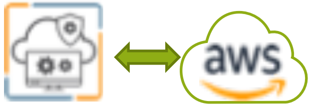
AWS_Group_Policy / Rules

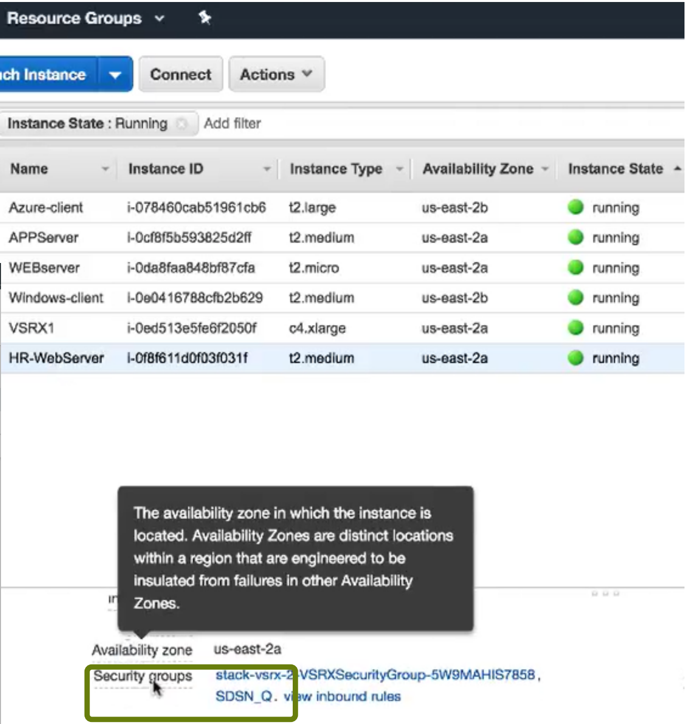
	Seq.	Rule Name	User ID	Src. Address	Dest. Address	Service	Action	Advanced
ZONE (0 Rule)								
GLOBAL (4 Rules)								
☑	1	Access-to-Finance-Resources	Finance_GRP	Any	Provider = PE AND Department = Finance AND PCI = true	Any	Permit	IPS: ON
□	2	Access-to-Engineering-Resources	Engineering_GRP	Any	Provider = PE AND Department = Engineering	Any	Permit	-
□	3	Access-to-HR	Engineering_GRP	Any	Provider = PE AND Department = HR	Any	Permit	APP... HR-
□	4	Deny	Any	Any	Any	Any	Deny	-

Meta data based policies

AWS Threat Remediation on AWS

SD assign Security Group for Quarantine





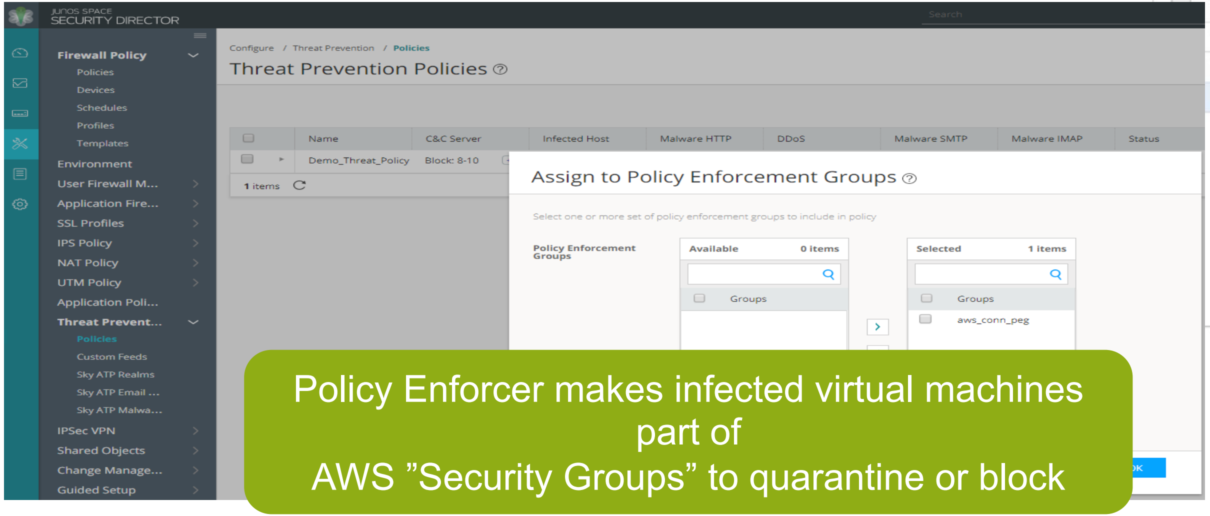
Name	Instance ID	Instance Type	Availability Zone	Instance State
Azure-client	i-078460cab51961cb6	t2.large	us-east-2b	running
APPServer	i-0cf8f5b593825d2ff	t2.medium	us-east-2a	running
WEBserver	i-0da8faa848bf87cfa	t2.micro	us-east-2a	running
Windows-client	i-0e0416788cfb2b629	t2.medium	us-east-2b	running
VSRX1	i-0ed513e5fe6f2050f	c4.xlarge	us-east-2a	running
HR-WebServer	i-0f8f611d0f03f031f	t2.medium	us-east-2a	running

The availability zone in which the instance is located. Availability Zones are distinct locations within a region that are engineered to be insulated from failures in other Availability Zones.

Availability zone us-east-2a

Security groups stack-vsrx-2-VSRXSecurityGroup-5W9MAHIS7858, SDSN_Q. view inbound rules

Dynamic Security Group



Threat Prevention Policies

Name	C&C Server	Infected Host	Malware HTTP	DDoS	Malware SMTP	Malware IMAP	Status
Demo_Threat_Policy	Block: 8-10						

1 items

Assign to Policy Enforcement Groups

Select one or more set of policy enforcement groups to include in policy

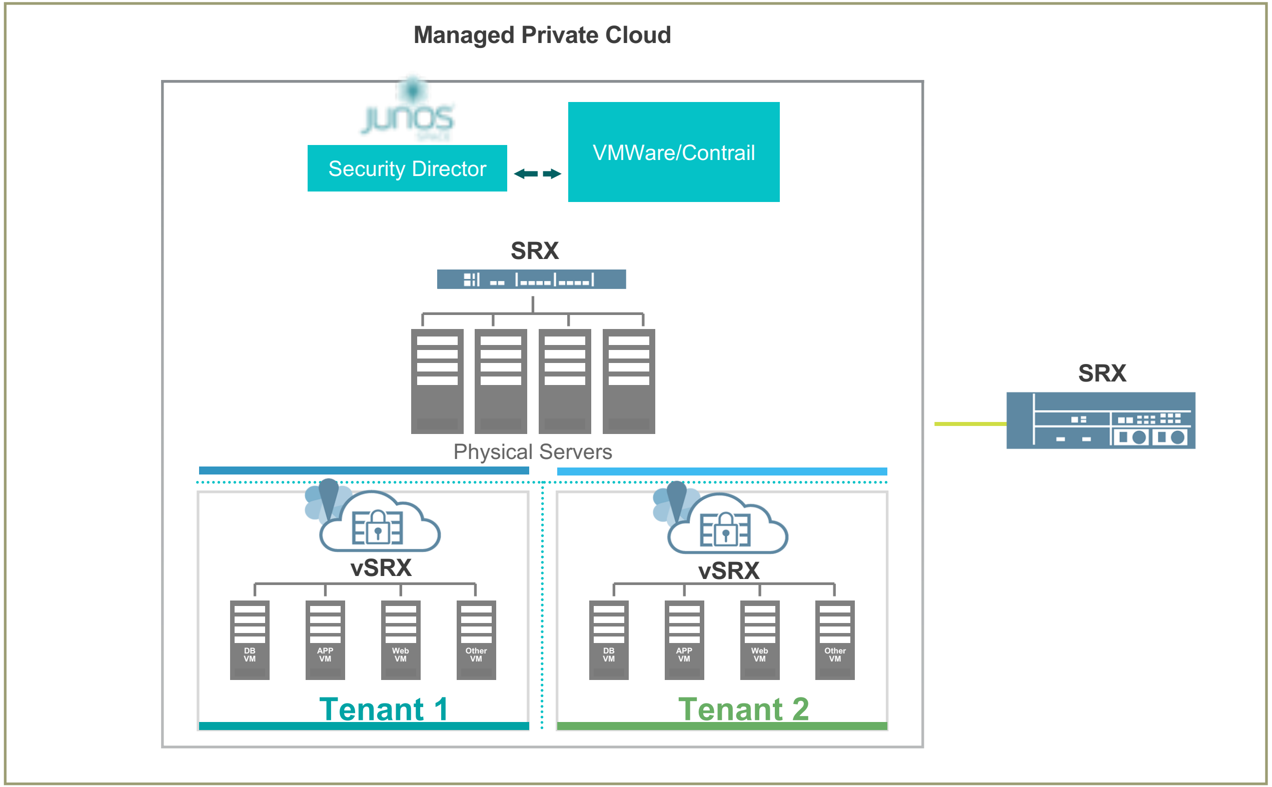
Policy Enforcement Groups

Available 0 items	Selected 1 items
Groups	Groups
	aws_conn_peg

Policy Enforcer makes infected virtual machines part of
AWS "Security Groups" to quarantine or block

SDSN use case 4:

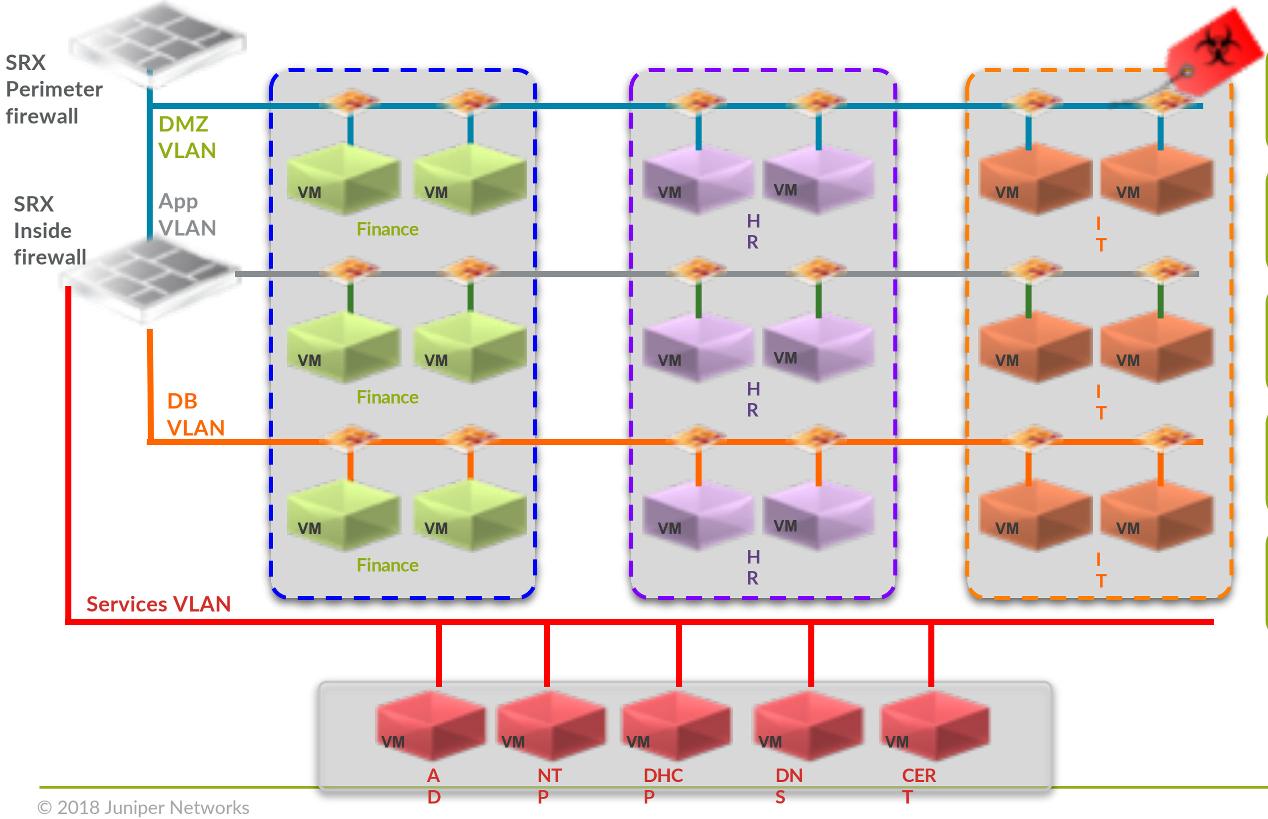
Use Case 4: (Private Cloud and MultiCloud)



Key Scenarios

- Security Director enables security policy configuration and management across physical & virtual environments
- SDSN Integration with VMWare NSX
- SDSN Threat Mitigation and Micro-segmentation
- Contrail vSRX and cSRX
- LDOM (Logical Domain) – High Scale Multi-Tenancy, RBAC, Per Tenant Advanced Security

VMWARE NSX MICRO-SEGMENTATION



vSRX for East-West traffic

Traffic between apps on same VLAN can now be firewalled

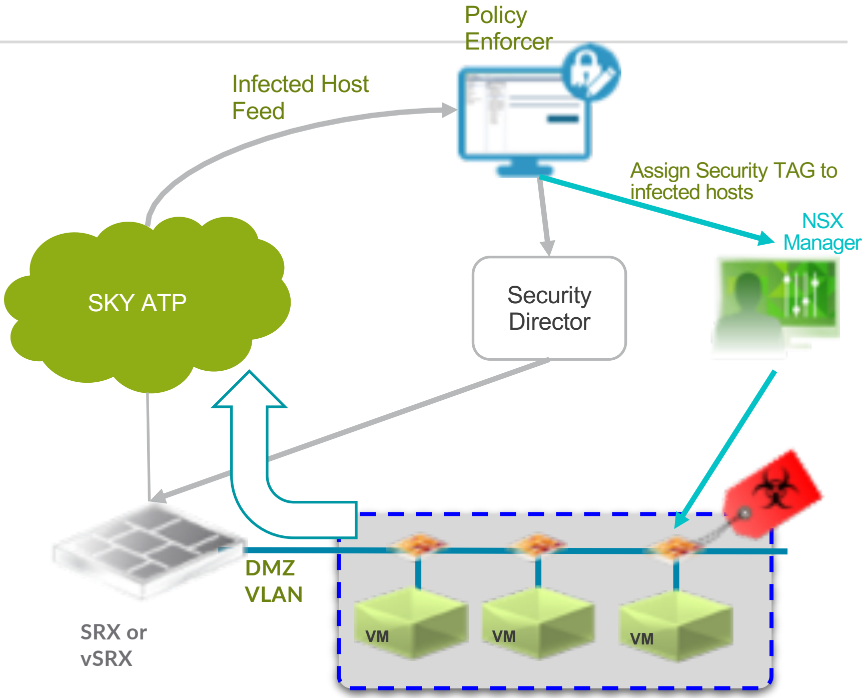
vSRX protects lateral movement of attacks inside the network

Dynamic VM “posture” based security orchestration

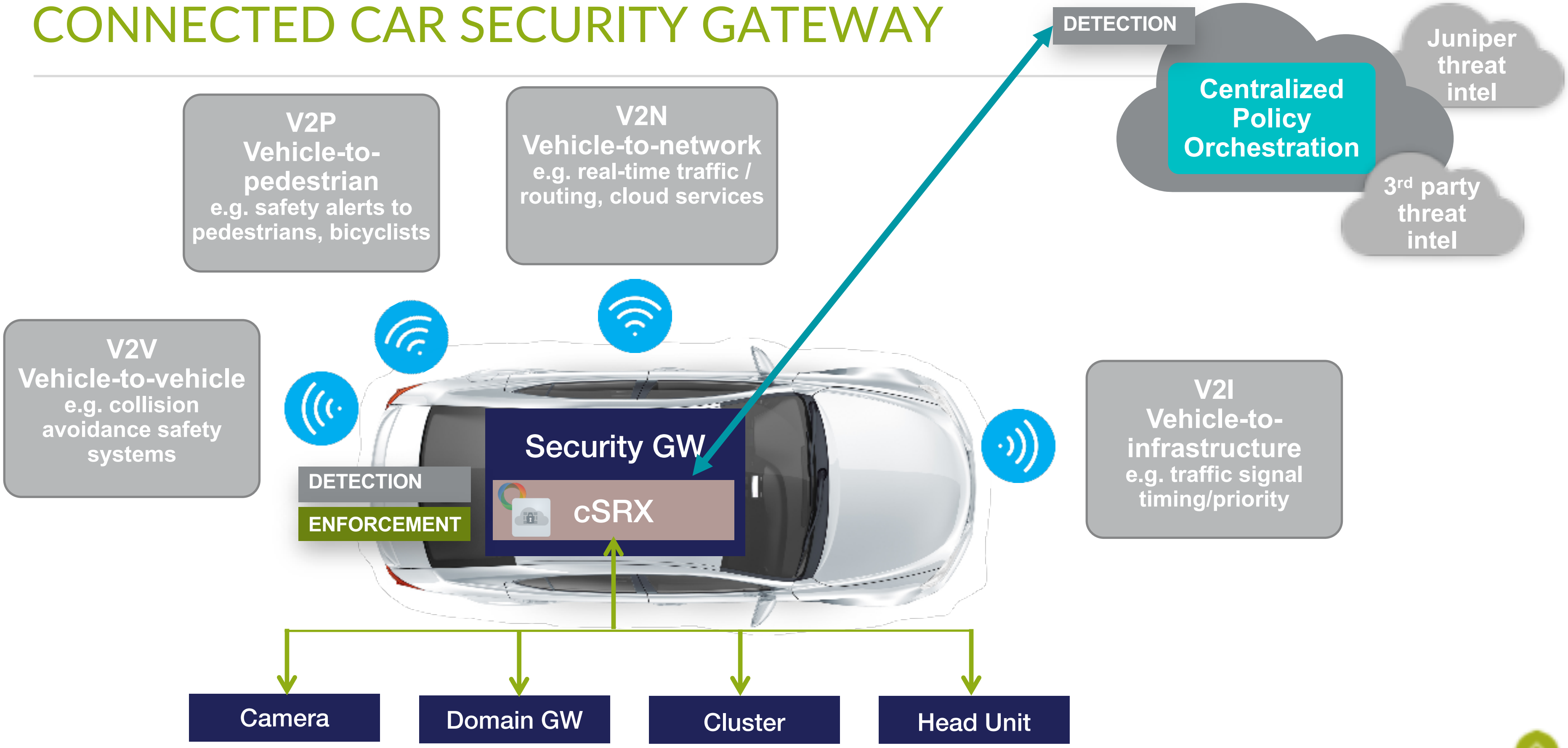
Visibility for east-west traffic

Automated Threat Remediation with NSX

1. Perimeter SRX forwards relevant traffic to SKY ATP
2. SKY ATP identifies Malware and Infected Hosts, and passes this information to Policy Enforcer
3. Policy Enforcer
    1. Pushes policy to SRX through SD related to infected host access
    2. Tags infected VMs using NSX Manager



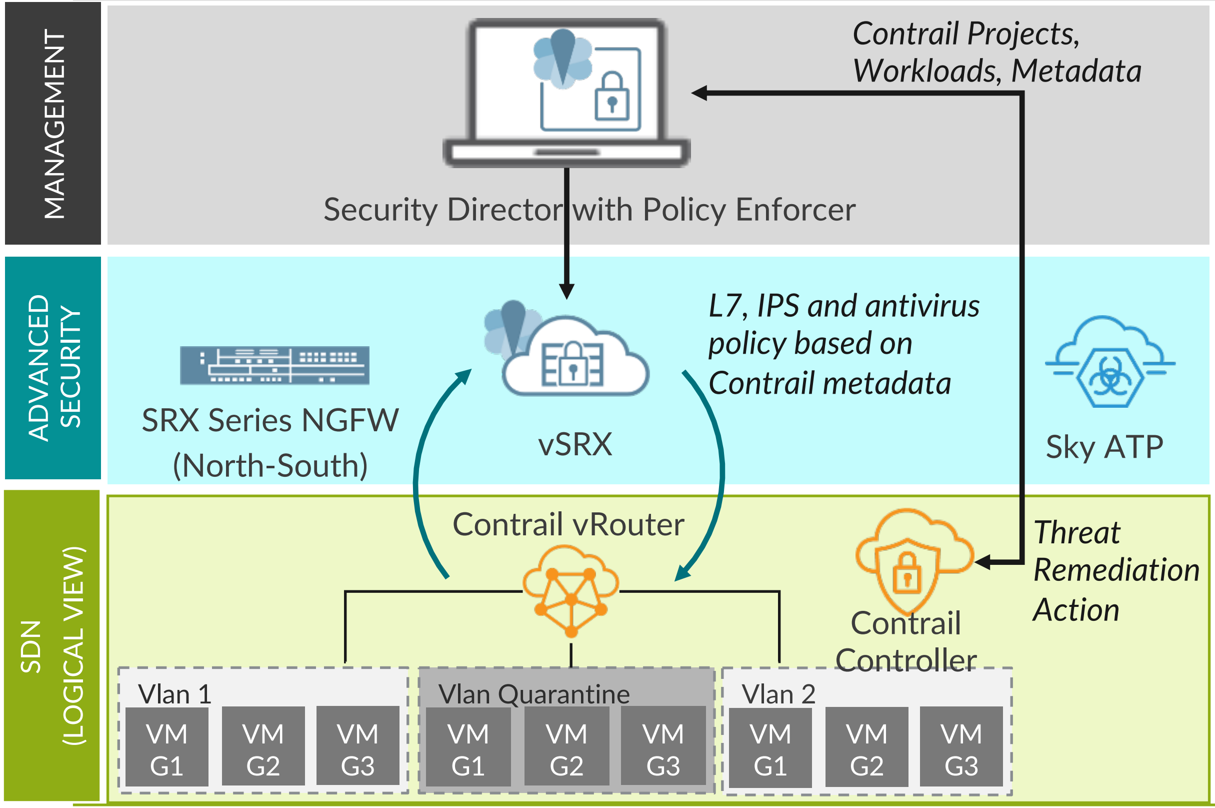
CONNECTED CAR SECURITY GATEWAY


DETECTION
Centralized Policy Orchestration
Juniper threat intel
3rd party threat intel
V2P
Vehicle-to-pedestrian
e.g. safety alerts to pedestrians, bicyclists
V2N
Vehicle-to-network
e.g. real-time traffic / routing, cloud services
V2V
Vehicle-to-vehicle
e.g. collision avoidance safety systems
V2I
Vehicle-to-infrastructure
e.g. traffic signal timing/priority
Security GW
cSRX
DETECTION
ENFORCEMENT
Camera
Domain GW
Cluster
Head Unit

Security Director

Contrail

CONTRAIL AND VSRX INTEGRATION



MANAGEMENT

Security Director with Policy Enforcer

Contrail Projects, Workloads, Metadata

ADVANCED SECURITY

SRX Series NGFW (North-South)

vSRX

L7, IPS and antivirus policy based on Contrail metadata

Sky ATP

SDN (LOGICAL VIEW)

Contrail vRouter

Contrail Controller

Threat Remediation Action

Vlan 1: VM G1, VM G2, VM G3

Vlan Quarantine: VM G1, VM G2, VM G3

Vlan 2: VM G1, VM G2, VM G3

Security Director/Policy Enforcer

- “User Intent Policy” for advanced security
- Workload & Meta-Data discovery from Contrail Threat Remediation Use Cases
- Security monitoring & reporting

Advanced Sec / Threat Mitigation

- Security Group dynamic changes
- Support for L7, IPS, AV, …
- Connect to Quarantine Virtual Network
- Block Access to PCI Network

Contrail

- Virtual Networking / Microsegmentation
- L2-L4 access control inside vRouter
- Service Chaining to include vSRX
- Contrail inventory and security TAG synchronization with Policy Enforcer

THREAT REMEDIATION with MX

MX C&C , GeoIP feeds for threat remediation

Use Case: Mitigation of DDoS attack

DETECTION

Detection from JSA or a third party detection mechanism is fed to Policy enforcer as a custom Feed

POLICY

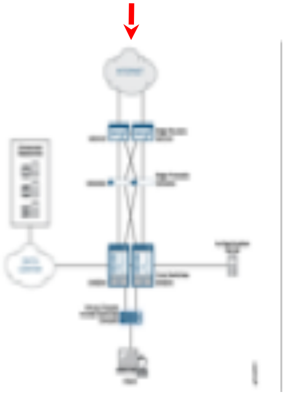
Simplified DDoS Policy (Block, Rate Limit, Forward to) defined in Security Director Policy Enforcer

ENFORCEMENT

Juniper: SRX, vSRX, MX

JUNIPER NETWORKS Corero

Embedded + Licensed splunk> Machine Learning



Key Features

Security Fabric including Firewalls and MX routers

DDoS remediation

- BGP flow spec is modified to take one of the possible actions
- Block - Block Route
- Rate Limit – Limit bandwith on flow route
- Forward to – next hop to reroute packet for scrubbing

Customer Benefits

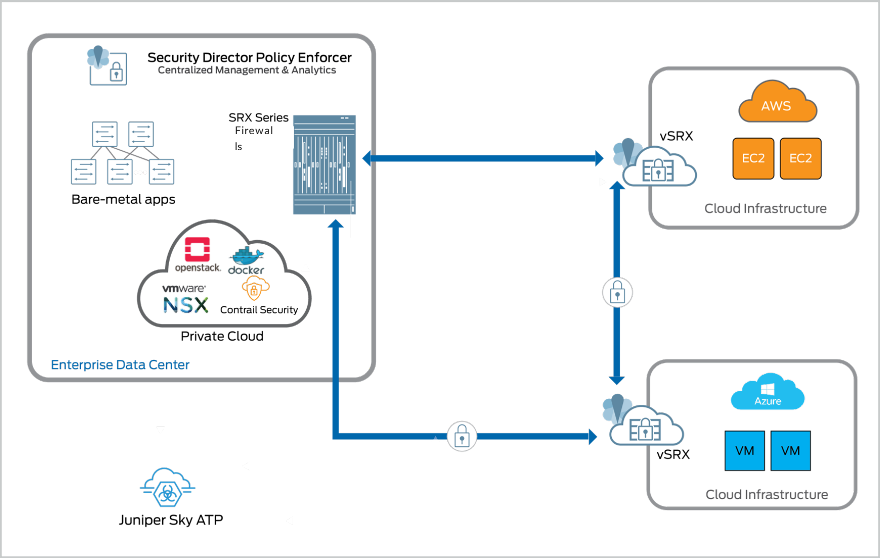
Automates DDoS remediation workflows

Reduced time to remediate = Reduced chances of service outage

Leverage Network (MX) and BGP flow spec to counter DDoS attack and effectively prevent service outage.

Remediation at the perimeter router protects down stream firewall and other devices.

ADVANCED CLOUD SECURITY



Consistent security across all clouds with vSRX firewalls

ATP for protection against sophisticated zero-day threats

Secure IPsec connectivity between cloud deployments

Carrier-grade routing on hardware and virtual firewalls

Comprehensive protection in N-S direction

What does SDSN mean to me

ATTACKS

Threat Remediation

✓ All Juniper

✓ Multi Vendor

CLEARPASS

Cisco ISE 2.2

ForeScout

Custom Connector

✓ Public/Private Cloud

AWS

vmware NSX

THANK YOU