



# Software Defined Secure Networks

Seguridad Avanzada en Campus Complejos

José Fidel Tomás – fidel.tomas@juniper.net

# Security is in Transformation



## THREAT SOPHISTICATION

- Zero day attacks
- Advanced, persistent, targeted attacks
- Adaptive malware



## CLOUD

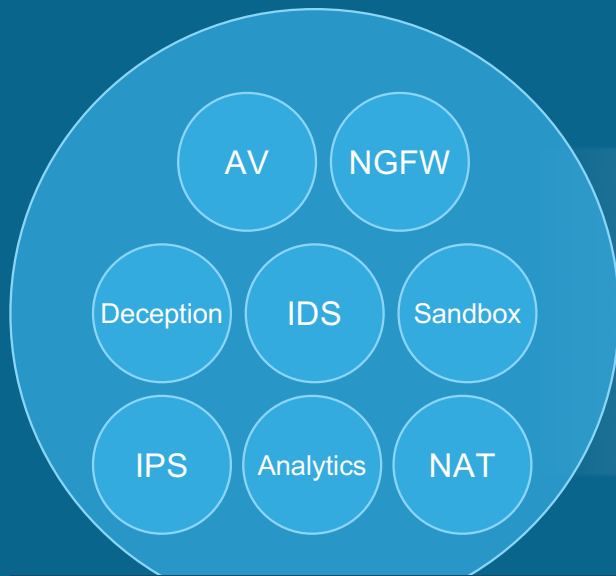
- Virtualization and SDN
- Applications, data, management in the cloud
- Application proliferation



## INFRASTRUCTURE

- Device proliferation and BYOD
- IoT based attacks
- Hybrid cloud deployments growing

# Demanding Software Defined Secure Networks



**Uncoordinated and  
firewall focused**



**Orchestrated, holistic system  
encompassing security + infrastructure**

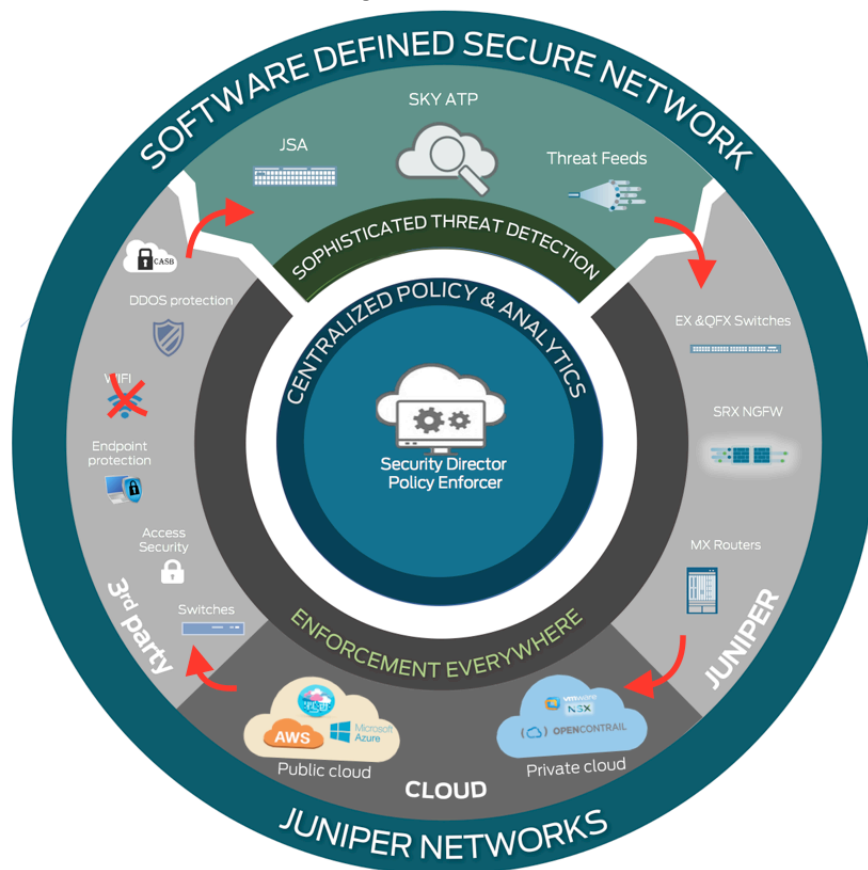
Global Policy Orchestration, Policy Engine

Open and Unified Threat Detection

Dynamic, Automated Enforcement

# Software Defined Secure Networks (SDSN)

## Unified Security Platform



### Detection

- Leverage entire network and ecosystem for advanced threat intelligence and detection

### Policy

- User intent based policy model
- Consistent policy enforcement across multiple enforcement domains
- Robust visibility and management

### Enforcement

- Utilize any point of the network including firewalls, switches, routers, 3<sup>rd</sup> party devices, SDN and public cloud platforms as a points of enforcement

***Network as a single enforcement domain - Every element is a policy enforcement point***



# SDSN Phase-1

## Use Case: Threat Remediation of infected hosts

### DETECTION

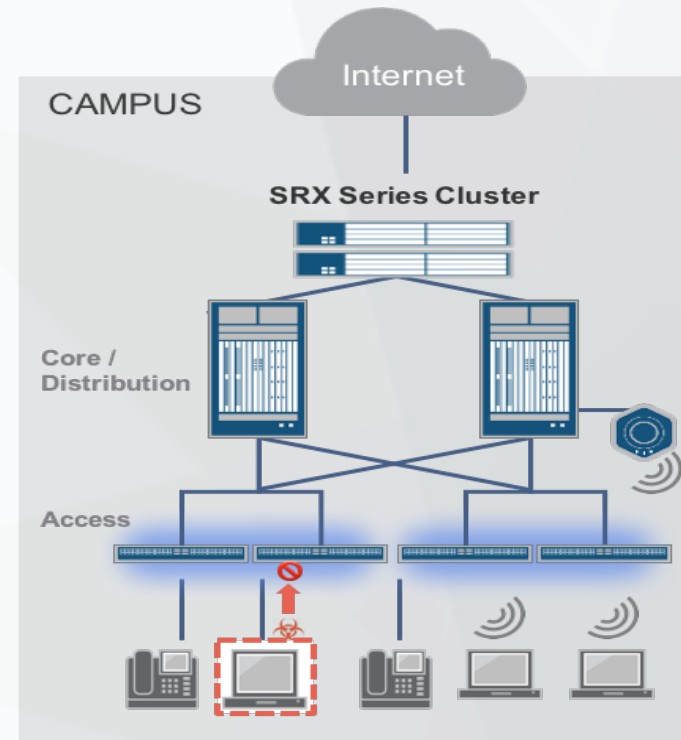
Sky ATP – Known & Day-0 Malware analysis, Sandboxing, Infected Host identification, Command & Control, GeolIP

### 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

## Customer Benefits

- Automates threat remediation workflows
- Real-time remediation of infected hosts
- Reduced time to remediate = Reduced exposure to attacks
- Leverage Network (EX/QFX) and Firewall (SRX/vSRX) to take remediation actions to address lateral movement of attacks inside the network in addition to limiting attacks from outside world

# SDSN Phase-2 Threat Remediation Enhancements

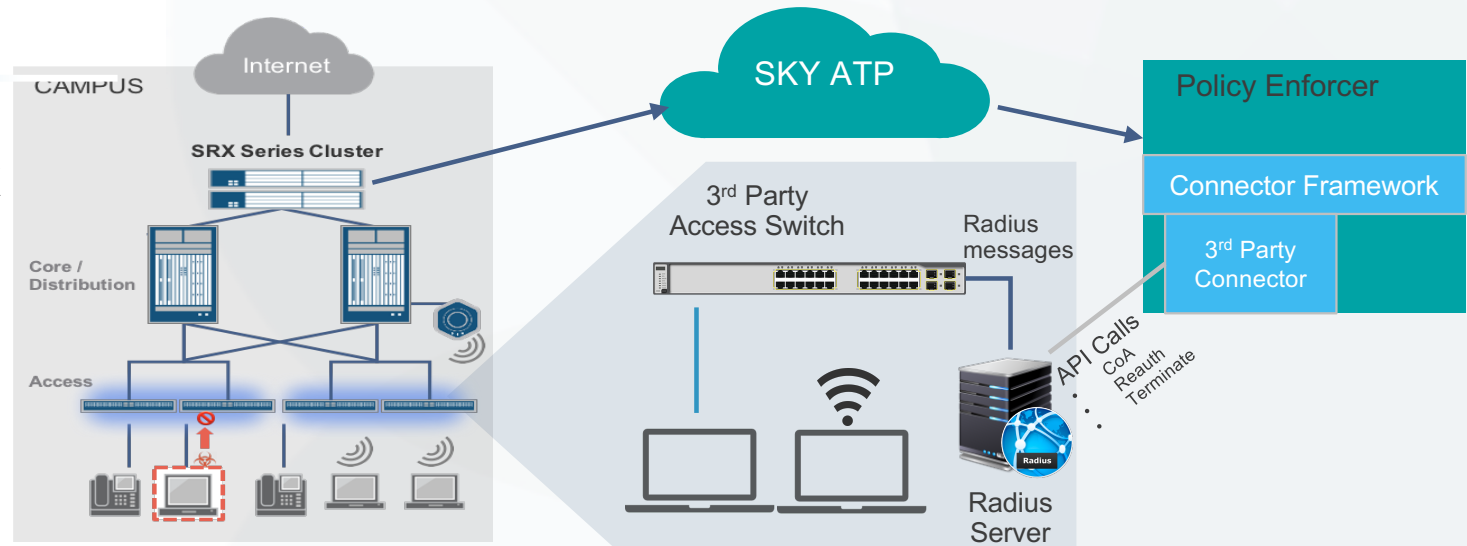
## Use Case: 3<sup>rd</sup> Party Switch and Wireless Support

### ENFORCEMENT

**Juniper:** SRX, vSRX, QFX and EX (+Fusion Support)

**3<sup>rd</sup> Party:** Access Switches with Radius(AAA) configured

**Wireless:** WLCs with Radius(AAA) configured



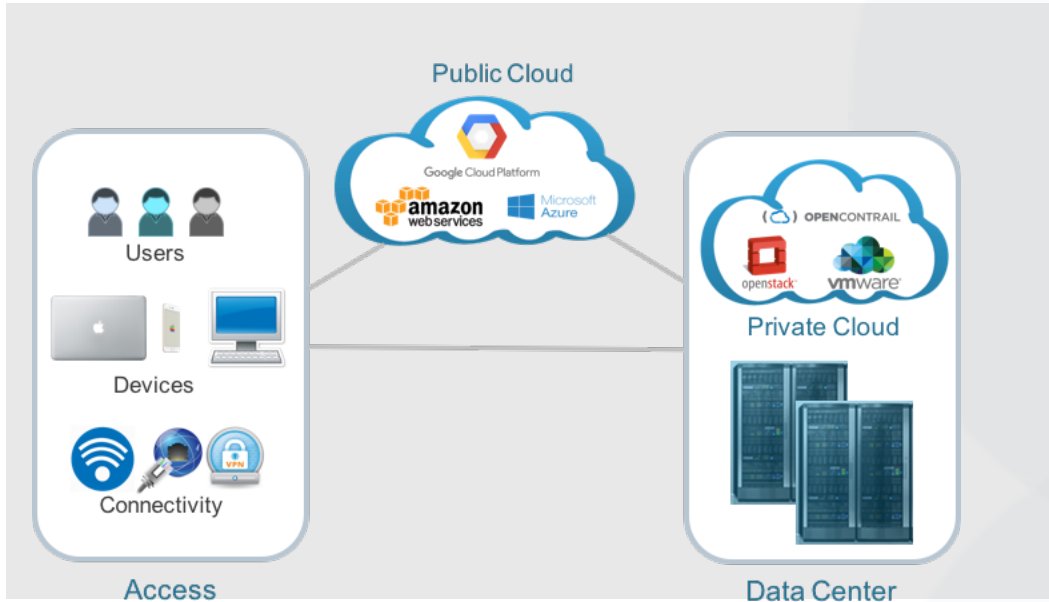
## Key Features

- Security Fabric to support 3<sup>rd</sup> party switches and wireless
- Infected Host Blocking
  - Juniper & 3<sup>rd</sup> party 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

## Customer Benefits

- Automates threat remediation workflows
- Real-time remediation of infected hosts
- Reduced time to remediate = Reduced exposure to attacks
- Network vendor agnostic mechanism for threat remediation

# SDSN Phase-3



**SDSN is a huge differentiator for Juniper**

**Complete Threat Remediation Use Case**  
Additional NAC vendor support , and JSA

**Introduce User Intent Based Policy Model**

Simplicity of policy to support agile applications & users

**Support Private & Public Cloud**

With vSRX on VMware NSX, Contrail, AWS

## Key Features

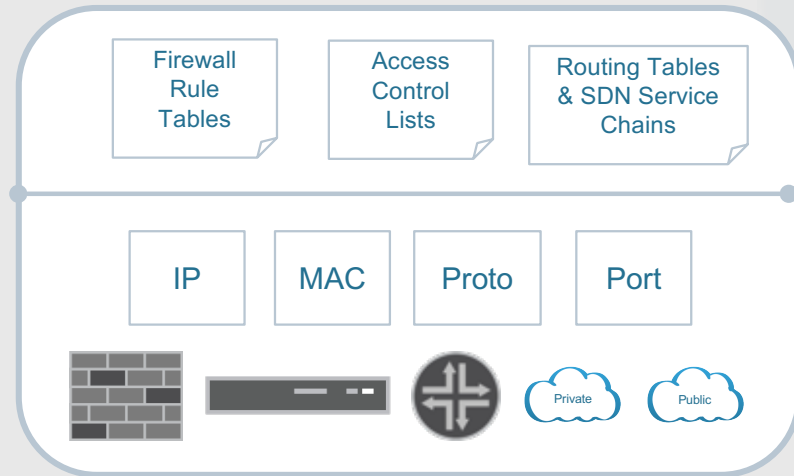
- User Intent Policy
- Hybrid Cloud Support
  - AWS
  - Contrail
- Additional Threat Remediation
  - JSA, Cisco ISE, Forescout

## Customer Benefits

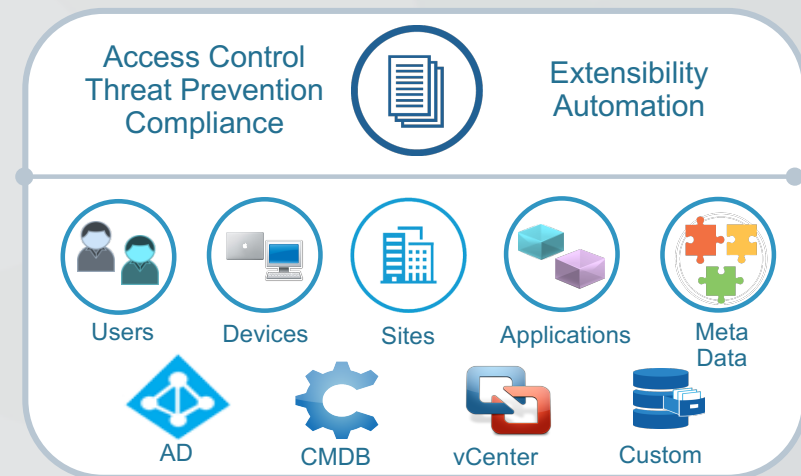
- Flexible and extensible policy - Security Policy is tied to a business intent and not to a network topology
- Enhanced user experience and optimized network operation - Unified Security Policy across all Juniper Product Lines
- Ubiquitous and multi-vendor enablement – work with 3<sup>rd</sup> party devices and works on-premise as well in the Cloud




# SDSN User Intent Policy Model

## Network Configuration



## User Intent Policy



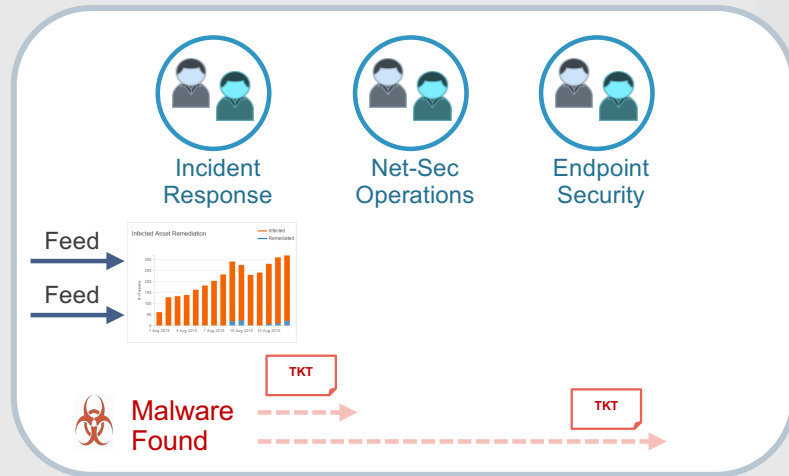
-  Islands of Management
-  Device/Platform specific configurations
-  Tough to automate, challenging compliance

-  Comprehensive Security
-  User Intent Based Policies
-  Native automation and compliance support

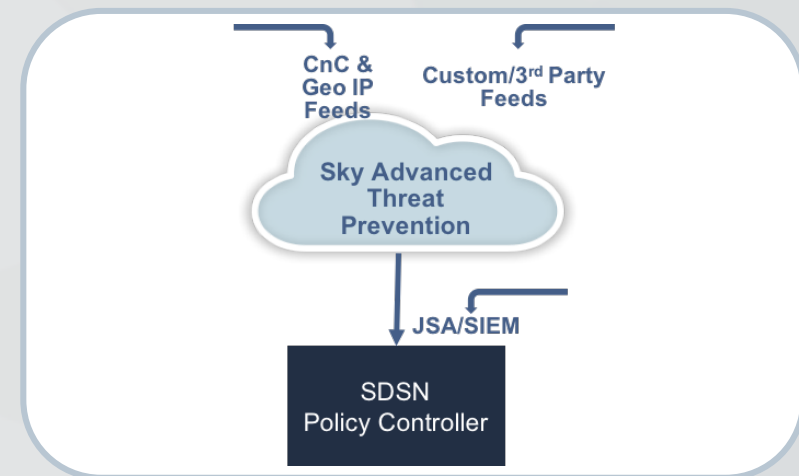


# SDSN – Threat Management

## Manual Threat Workflows



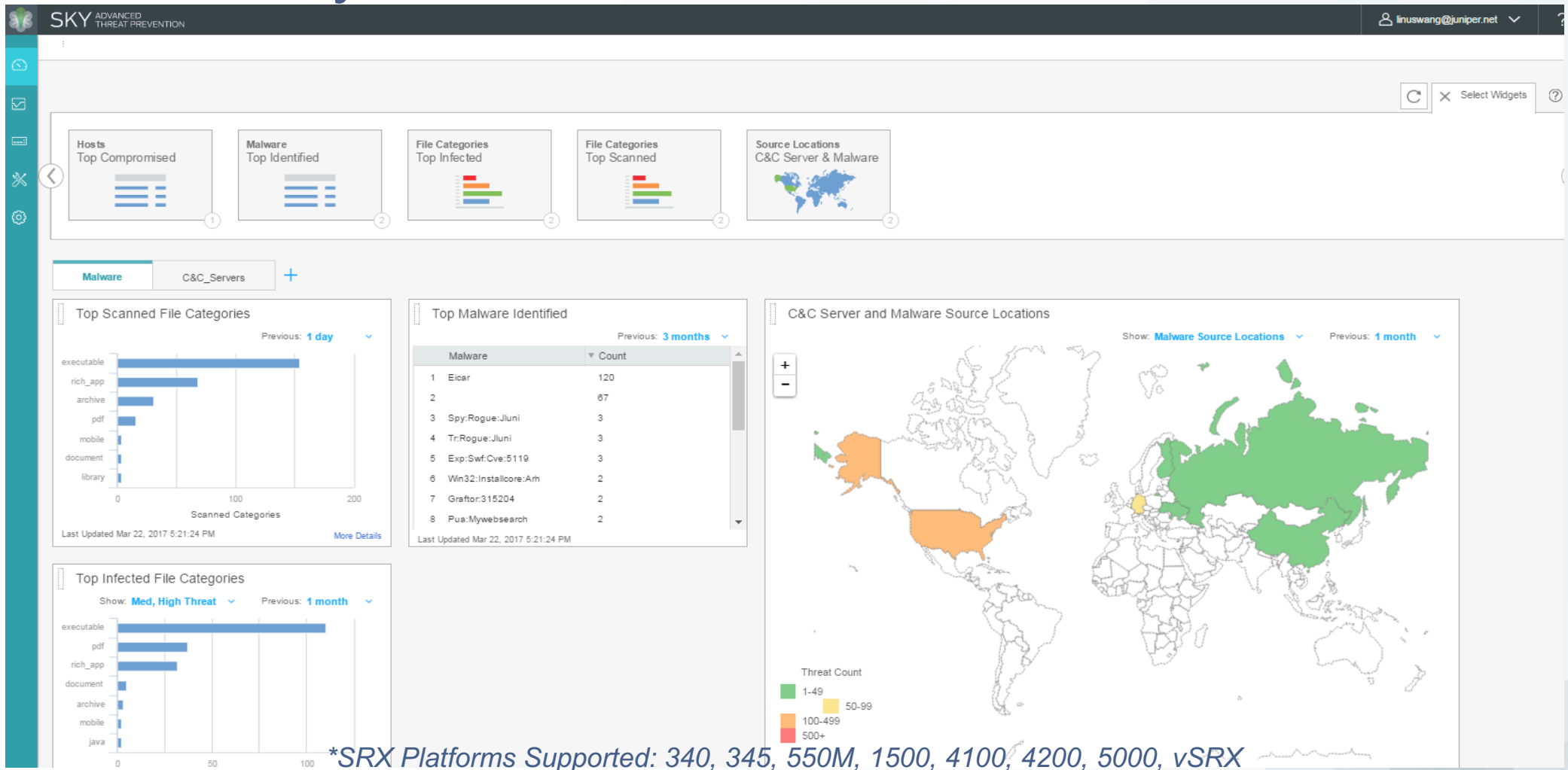
## Threat Management Automation



- Multiple Teams
- Threat Detection → Enforcement Delays
- Vendor specific threat feeds

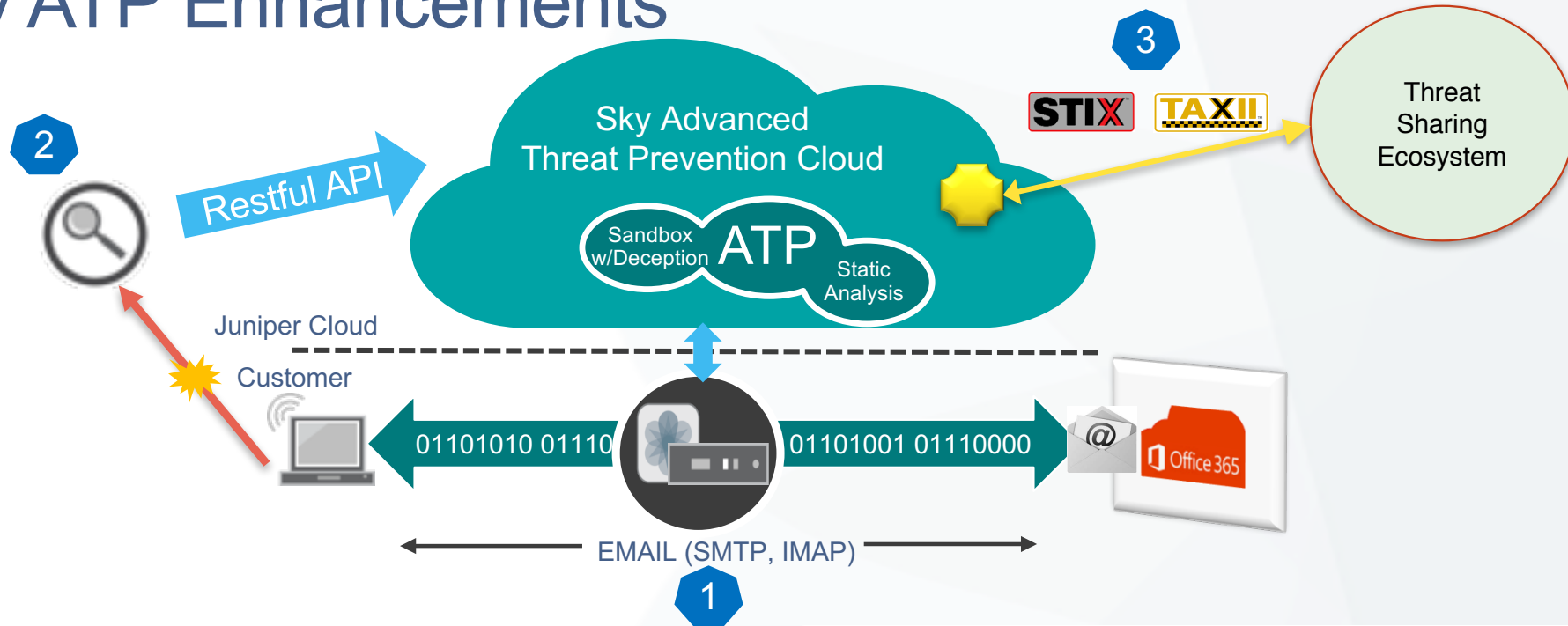
- Cohesive Threat Management System
- Automation across Network & Security
- Open API and 3<sup>rd</sup> Party Threat Feed Collation

# What is Sky Advanced Threat Prevention



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

# Sky ATP Enhancements



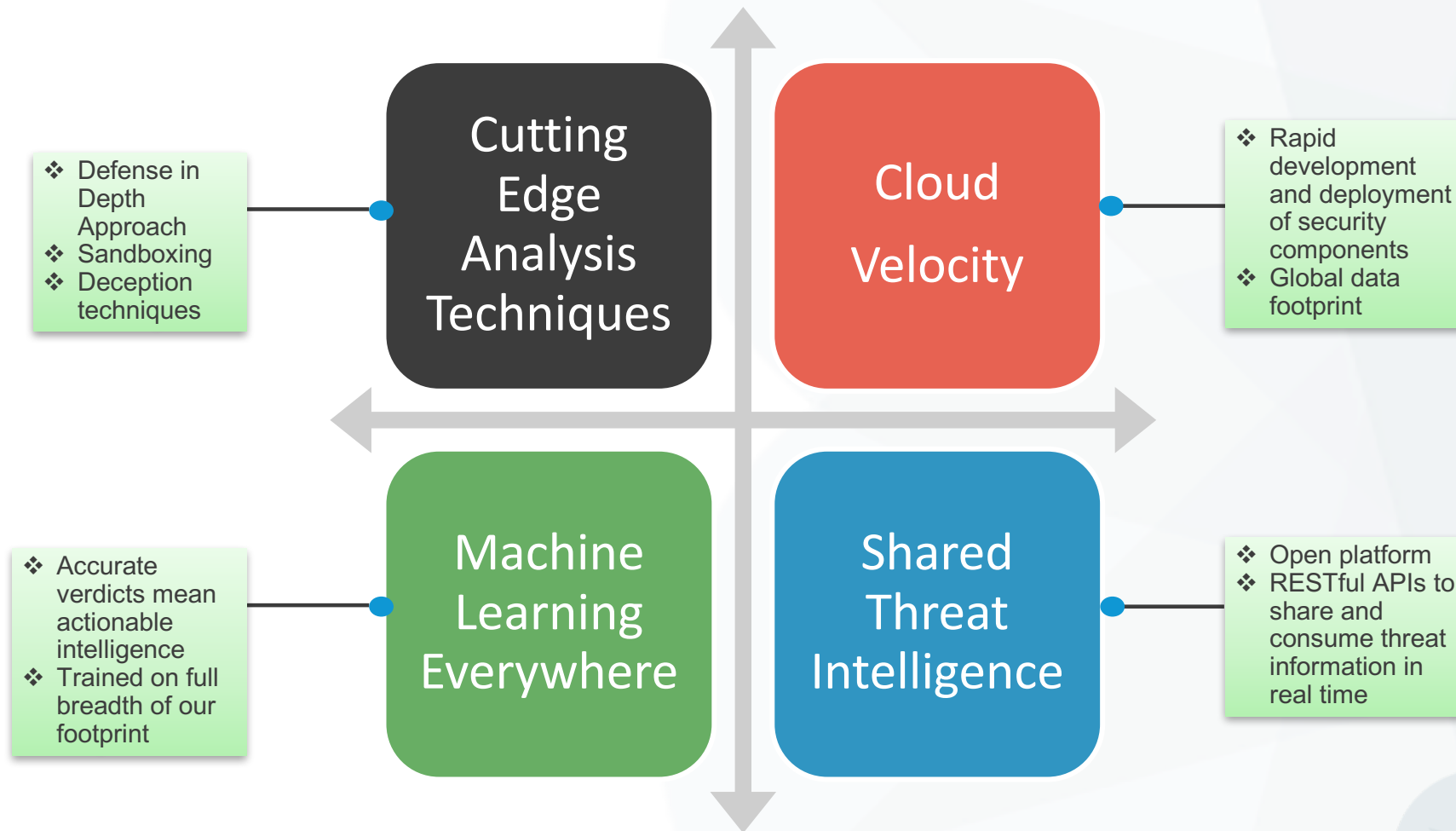
## Key Features

- Email support: SMTP, IMAP (Comprehensive email support)
- Threat Intelligence sharing: STIX/TAXII/Cybox, Yara
- API ecosystem: Infected Host APIs to integrate with third-party vendors along with custom feed API

## Customer Benefits

- Email bound malware prevention ability allows customers to fence off one of the largest threat vector- 70% malware comes through email
- Rich API ecosystem that enables shared Threat Intelligence Pool to identify and prevent malware quickly and effectively

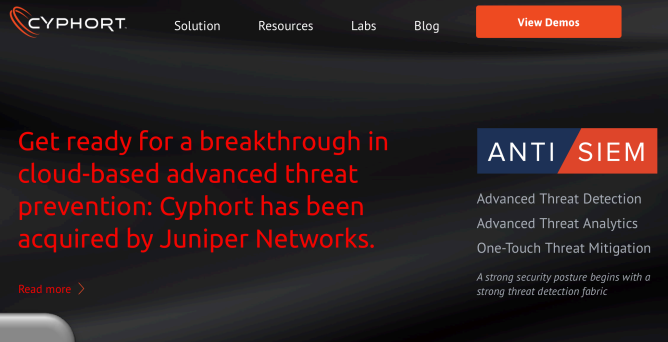
# Sky ATP Efficacy





# Juniper Announces Intent to Acquire Cyphort

Acquisition will extend the reach of Juniper Sky Advanced Threat Prevention.



2 Advanced Threat Analytics

ANTI SIEM

1 Advanced Threat Detection

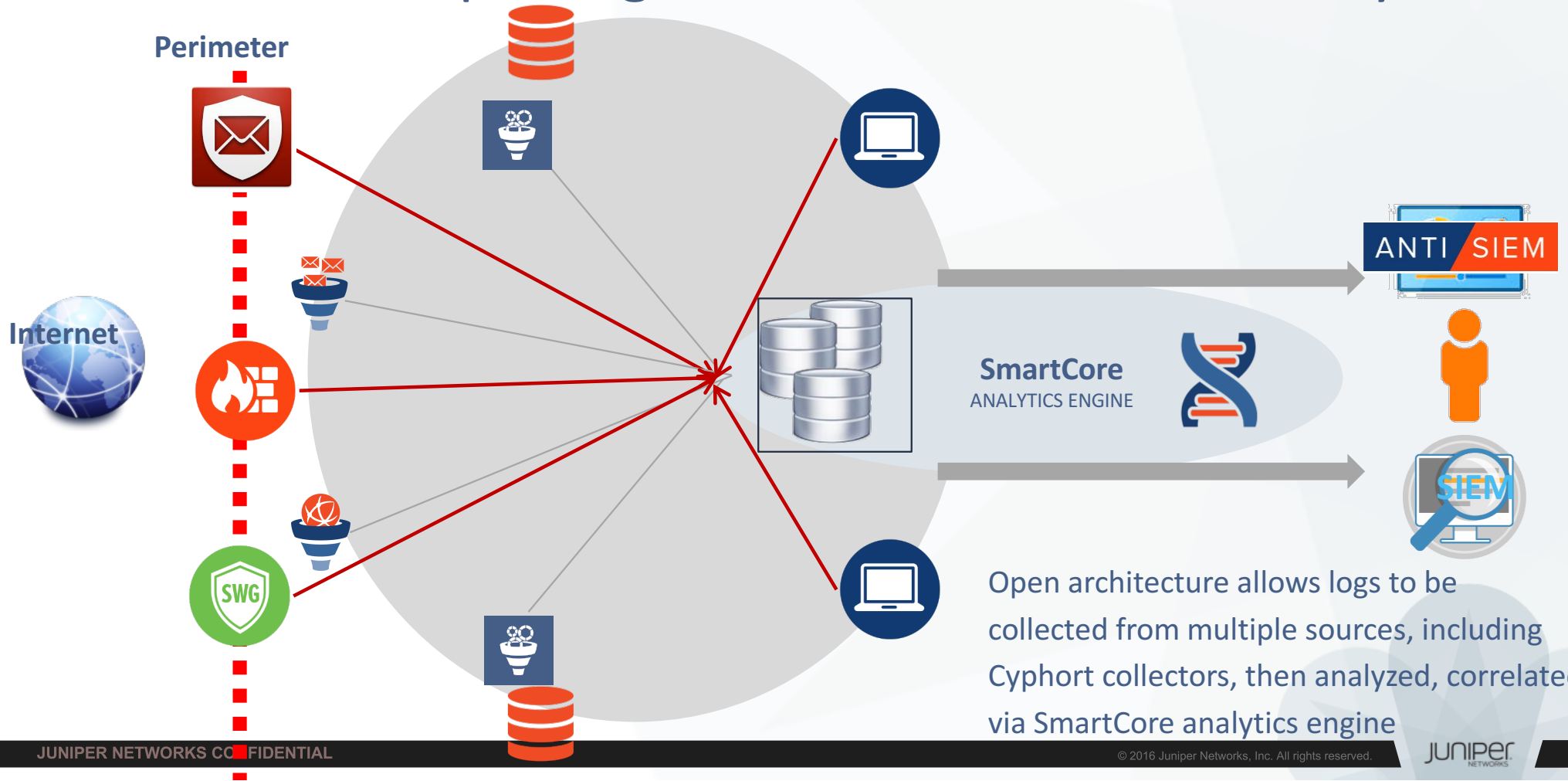
3 One-Touch Threat Mitigation

1 **Detection:** Discover threats that bypassed the 1<sup>st</sup> line of defense. Signature-less detection technology continuously analyze web, email and lateral spread traffic.

2 **Analytics:** Improve productivity and accelerate SOC/IR response. Events from multiple security tools correlated into an identity-based, timeline view of prioritized security incidents.

3 **Mitigation:** One-touch mitigation controlled by SOC/IR. Automated policy updates of security tools to isolate infected endpoints and strengthen in-line tools against future attacks.

# Native Detection, Open Ingestion Means Powerful Analytics



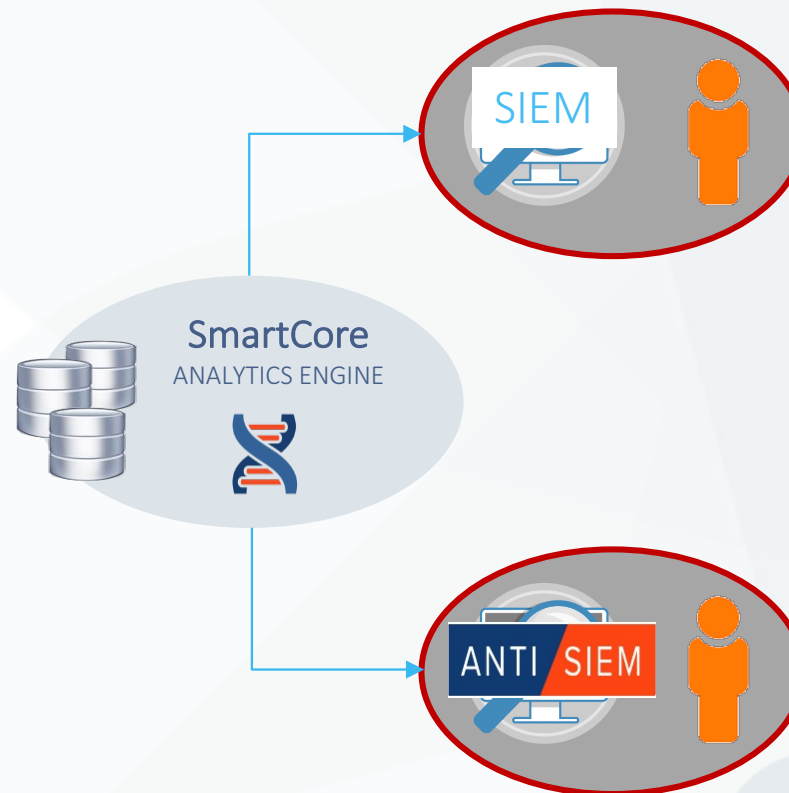
## Advanced Threat Analytics – Flexible Deployment

- **Works with your existing SIEM**

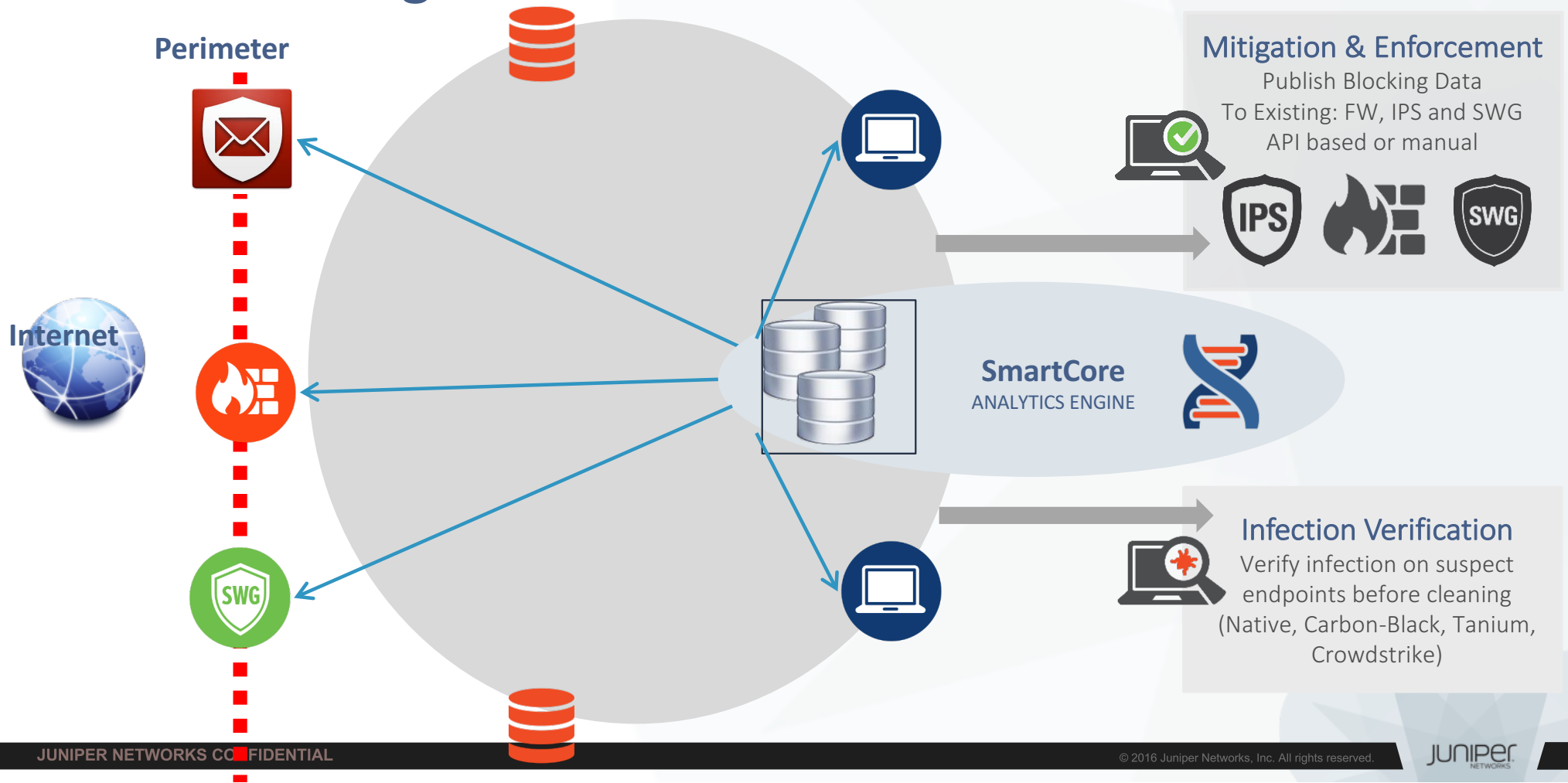
Leverage your SIEM platform and data feeds in combination with SmartCore analytics to strengthen security posture and accelerate incident response

- **Works as a stand-alone SIEM**

Anti-SIEM threat detection and analytics engine delivers all the values of a traditional SIEM – with less cost, noise, complexity, and wasted time.



# One-Touch Mitigation for IR Teams





### 3 Quilt - Technology Security Vendor Ecosystem

Endpoint



CARBON BLACK  
CROWDSTRIKE  
intel Security  
Symantec  
CYLANCE  
TANIUM

Firewall/SWG



Check Point SOFTWARE TECHNOLOGIES LTD.  
BLUE COAT  
Infoblox  
CISCO  
FORTINET  
JUNIPER NETWORKS  
SONICWALL  
paloalto NETWORKS

SIEM




splunk  
IBM  
hp ArcSight

CASB



skyhigh  
netskope

NAC/Identity



BRADFORD NETWORKS the smart edge  
Pulse Secure  
Hewlett Packard Enterprise aruba  
PFU a Fujitsu company

Other



Gigamon  
riverbed  
exabeam  
NETWORKS  
Phantom  
CYBERRESPONSE

All Incidents (359 shown, 359 total)

Search:  Show Threat  All Zones  Last 3 Months  [CSV](#)

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector	Date & Time
New	5428	MAX	TROJAN_MIUREF.DC	XP+DL+EX	Web LOG	582330430-6.idgro mo.ru	NICK-LAPTOP	Default Zone	Windows 7	2 Collectors	Apr 18 07:03:04 P DT
New	5272	LOW	TROJAN_LMN.DC	PHS+DL	EMAIL LOG	prince@gmail.com	dave@cydevel.com	Default Zone		2 Collectors	Apr 10 11:55:53 P DT
New	5270	MAX	TROJAN_WALDEK.DC	DL	Web LOG	greatfilesarey.asia	JOSH-DESKTOP	Default Zone	unknown	2 Collectors	Apr 10 09:07:01 P DT
New	5271	MAX	TROJAN_REXEC.CY	DL+EX	Web	horsebrasil.tv.br	BOB-DESKTOP	Default Zone	Ubuntu Linux	demo next x collector	Apr 10 09:05:07 P DT
New	5269	MED	VIRUS_VIRUT.CY	DL	Web	greatfilesarey.asia	RAJ-DESKTOP	Default Zone	unknown	demo next x collector	Apr 10 08:05:02 P DT
New	5264	HIGH	WORM_CRIDEX.CY	DL	Web	greatfilesarey.asia	CATHY-LAPTOP	Default Zone	unknown	demo next x collector	Apr 10 02:16:42 P DT

### Details for TROJAN\_LMN.DC

[SUMMARY](#) [PHISHING](#) [DOWNLOADS](#) [EXTERNAL SOURCES](#)

Actions

**Target:**

Zone: Default Zone  
 Incident Id: 5272  
 Hostname: DAVE-LAPTOP  
 Username: dave  
 IP Address: 10.1.1.190  
 FQDN: dave.eng.cyphort.com  
 Source Email ID: prince@gmail.com  
 Destination Email ID: dave@cydevel.com  
 Email Message ID: 58c6eb39.07cf620a.118ed.8a64@mx.google.com

**Progression:**



**Triggers:**

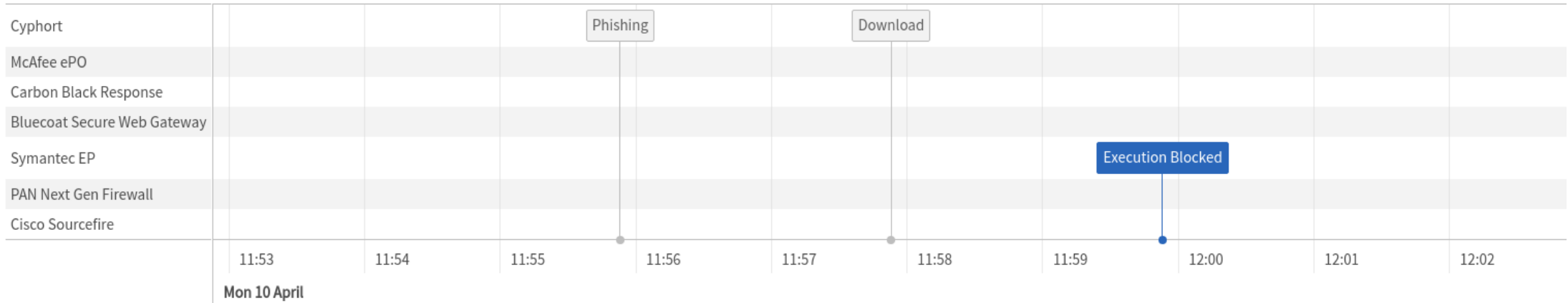
[Reputation](#) [Behavior](#) [Network](#) [Static](#)

[Operations](#)
[Research](#)
[System](#)
[Collectors](#)
[Events Timeline](#)

Hostname: 

 Select Vendor(s)

Timeline for Hostname : DAVE-LAPTOP



Details for TROJAN\_LMN.DC

[SUMMARY](#)
[PHISHING](#)
[DOWNLOADS](#)
[EXTERNAL SOURCES](#)

Actions

**Target:**

Zone: Default Zone  
 Incident Id: 5272  
 Hostname: DAVE-LAPTOP  
 Username: dave  
 IP Address: 10.1.1.190  
 FQDN: dave.eng.cyphort.com  
 Source Email ID: prince@gmail.com  
 Destination Email ID: dave@cydevel.com  
 Email Message ID: 58c6eb39.07cf620a.118ed.8a64@mx.google.com

All Incidents (359 shown, 359 total)

Search:  Show Threat  All Zones  Last 3 Months  [CSV](#)

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector	Date & Time
New	5254	MAX	EXPL_OFFICE.CY	PHS+DL	EMAIL	cyphsampletest@gmail.com	cydemo_infected@cydevel.com	Default Zone		Email Collector	Apr 8 11:55:50 PDT
New	5253	HIGH	WORM_DORKBOT.DC	DL	Web	greatfilesarey.asia	sj_demo_129	Default Zone	unknown	demo next x collector	Apr 8 08:22:41 PDT
New	5252	HIGH	SUSP_MCSWEEPER.CY	DL	Web	Infographiste.com	10.1.1.199	Default Zone	MacOS Macintosh X 10.9.0	demo next x collector	Apr 8 08:05:06 PDT
New	5251	HIGH	TROJAN_Pincav.CY	DL+IN	Web LOG	newwolfs29.mezoka.com	RITA-PC	Default Zone	Windows 7	2 Collectors	Apr 8 04:08:33 PDT
New	5250	HIGH	TROJAN_YONTOO.DC	DL	Web	oldcodehomeas.is-a-photographer.com	10.1.1.199	Default Zone	MacOS Macintosh X 10.6	demo next x collector	Apr 7 20:05:06 PDT
New	5249	HIGH	WORM_CRIDEX.CY	DL	Web	greatfilesarey.asia	sample_129	Default Zone	unknown	demo next x collector	Apr 7 12:54:00 PDT

### Details for TROJAN\_Pincav.CY

[SUMMARY](#) [DOWNLOADS](#) [INFECTIONS](#) [EXTERNAL SOURCES](#)

Actions

**Target:**  
 Zone: Default Zone  
 Incident ID: 5251  
 Hostname: RITA-PC  
 Username: rita  
 IP Address: 10.1.3.103  
 FQDN: rita.eng.cyphort.com  
 Source Email ID: -  
 Destination Email ID: -  
 Risk: High

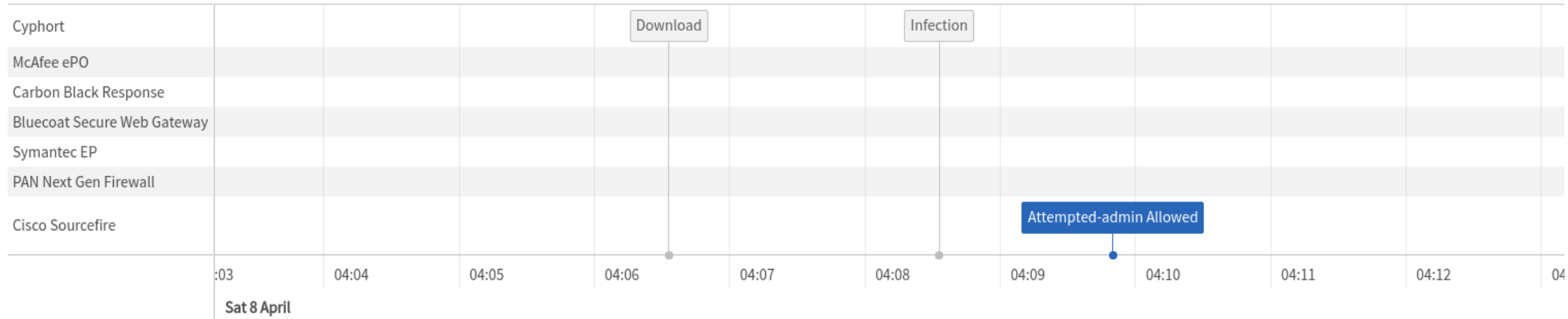
#### Progression:



#### Triggers:

[Reputation](#) [Behavior](#) [Network](#) [Static](#)

Timeline for Hostname : RITA-PC



Details for TROJAN\_Pincav.CY

[SUMMARY](#)
[DOWNLOADS](#)
[EXTERNAL SOURCES](#)
[INFECTIONS](#)

**Target:**

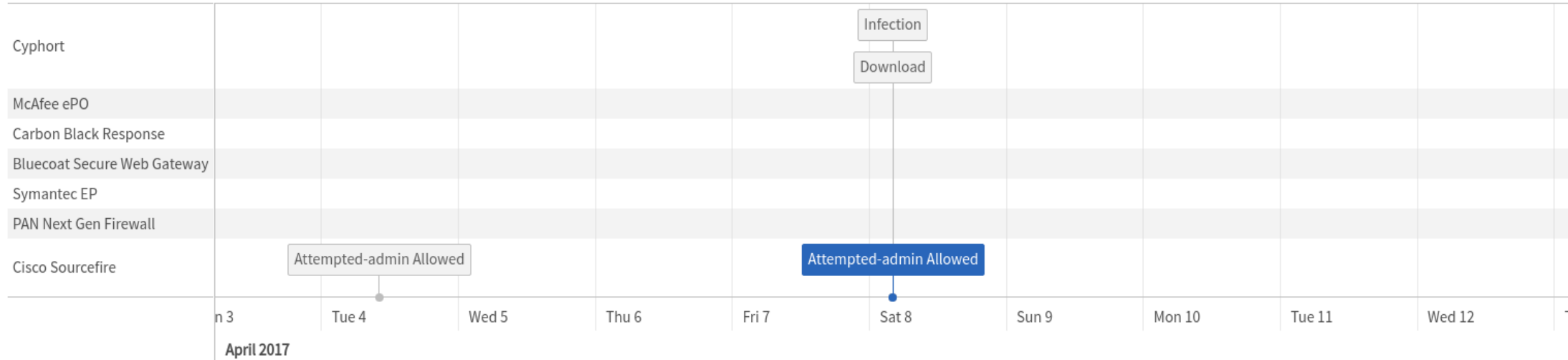
Zone: Default Zone  
 Incident Id: 5251  
 Hostname: RITA-PC  
 Username: rita  
 IP Address: 10.1.3.103  
 FQDN: rita.eng.cyphort.com  
 Source Email ID: -  
 Destination Email ID: -  
 Risk: High

[Operations](#)
[Research](#)
[System](#)
[Collectors](#)
[Events Timeline](#)

Hostname: 

 Select Vendor(s)

Timeline for Hostname : RITA-PC



Details for TROJAN\_Pincav.CY

[SUMMARY](#)
[DOWNLOADS](#)
[EXTERNAL SOURCES](#)
[INFECTIONS](#)

**Target:**

Zone: Default Zone  
 Incident Id: 5251  
 Hostname: RITA-PC  
 Username: rita  
 IP Address: 10.1.3.103  
 FQDN: rita.eng.cyphort.com  
 Source Email ID: -  
 Destination Email ID: -

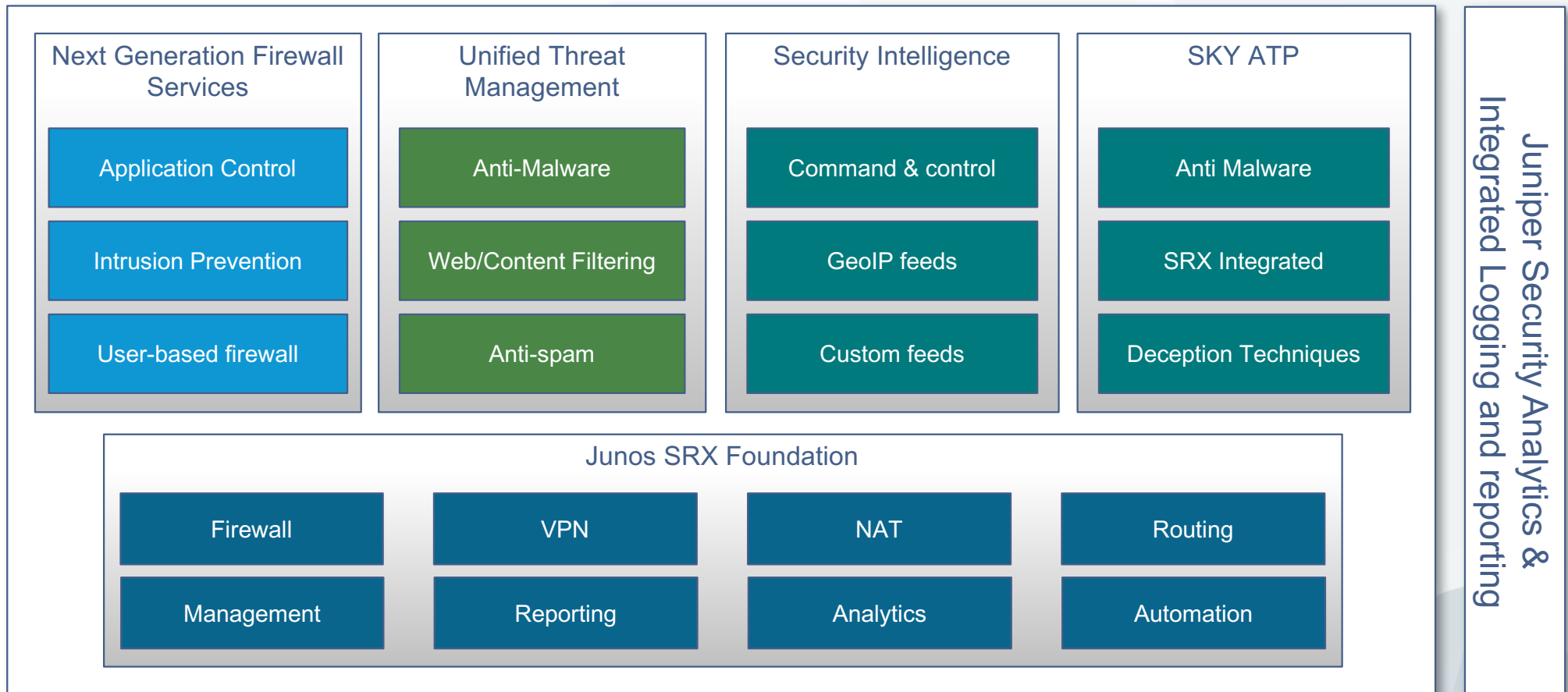




# SECURITY SERVICES

---

# Security Services: Physical and Virtual SRX



# SRX Unified Threat Management (UTM)



## Antivirus

- Sophos Live Protection against Trojans, Viruses, Phishing Attacks
- Reputation-enhanced capabilities

## Antispam

- Multilayered spam protection from security experts
- Protection against APTs

## Web Filtering

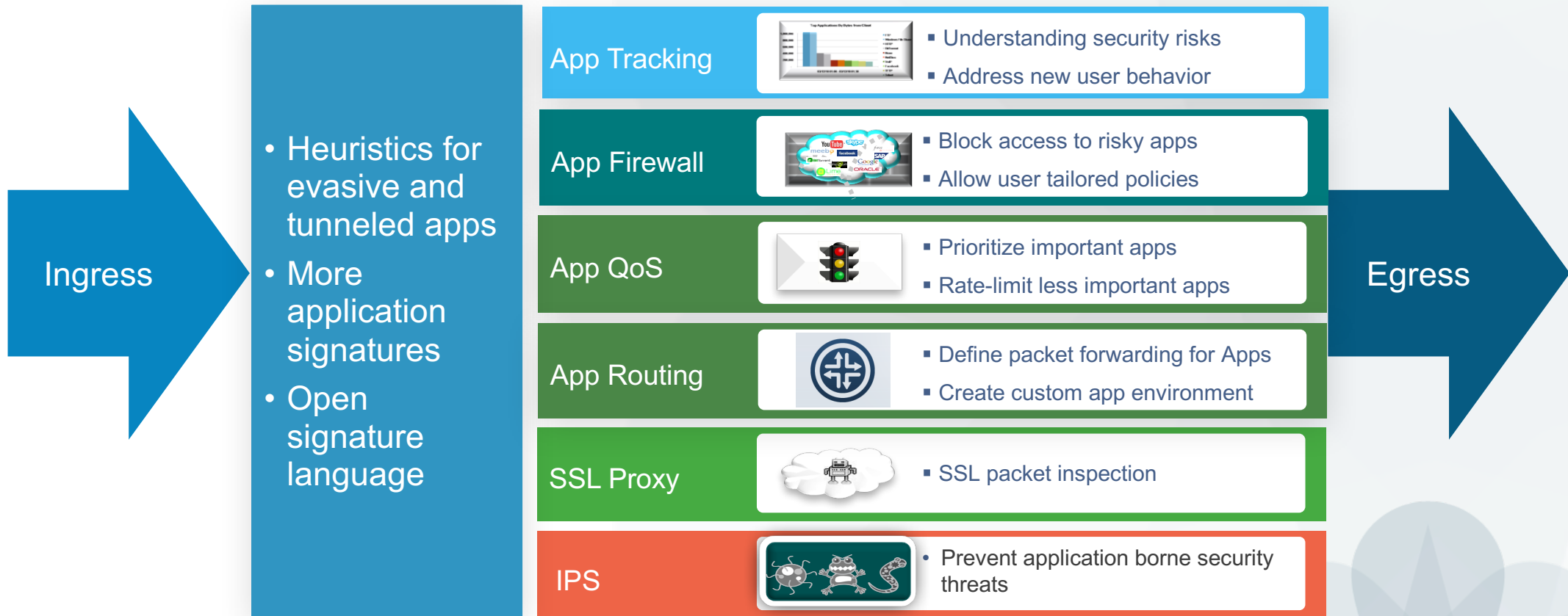
- Block malicious URLs
- Prevent lost productivity
- Websense TSC with more than 140 categories

## Content Filtering

- Filter out extraneous or malicious content
- Maintain bandwidth for essential traffic

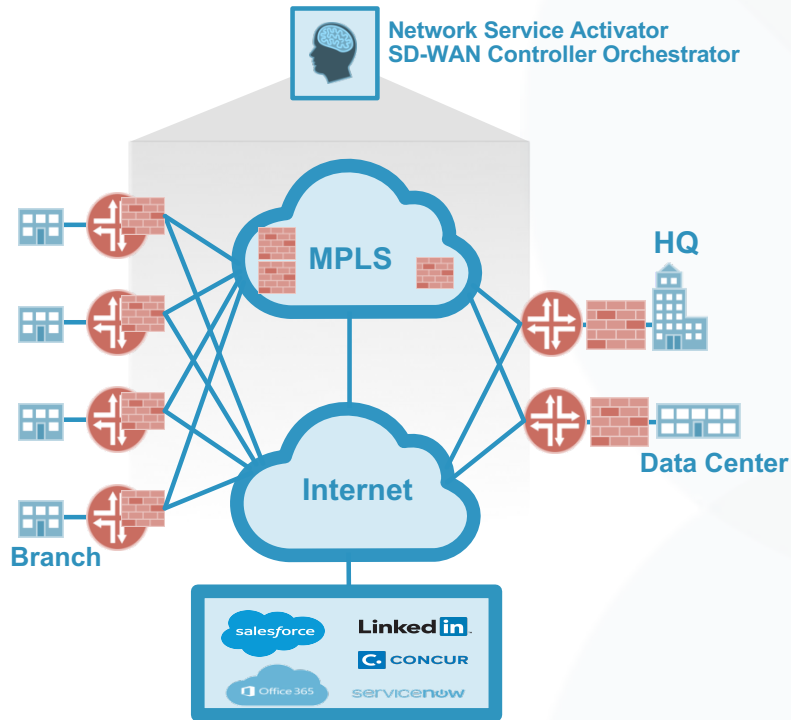
Subscription Based Software Services for a Turnkey Fully Integrated Offering

# Next Generation Firewall Services





# SD-WAN



## SD-WAN Highlights

### Must support multiple WAN connections

MPLS, Internet, LTE etc.

### Can do dynamic path selection

Allows for Application based load sharing across WAN links

### Provides simplified WAN management

Support zero-touch provisioning & unified security & routing policy

### Must support secure VPNs

Support flexible VPN deployments options with Auto VPN, Group VPN

## Key Features

- Integrated LTE MPIM
- Application based routing phase-II
- Phone call home client on SRX3xx / SRX1500
- Application QOE
- Ephemeral commit (policy changes without formal commit)

## Customer Benefits

- Enable customers to reduce WAN spending by incorporating cost-effective broadband and LTE links into the WAN
- Dynamic WAN path selection and load-balancing WAN traffic across multiple links based on the application, user and its performance
- Significant reduction in operation cost by provisioning remote branch office without truck rolls and on-site expertise



# Security Director

Dashboard

Firewall Policy

Threat Map

Events and Logs

Application  
Visibility



Automate Operations

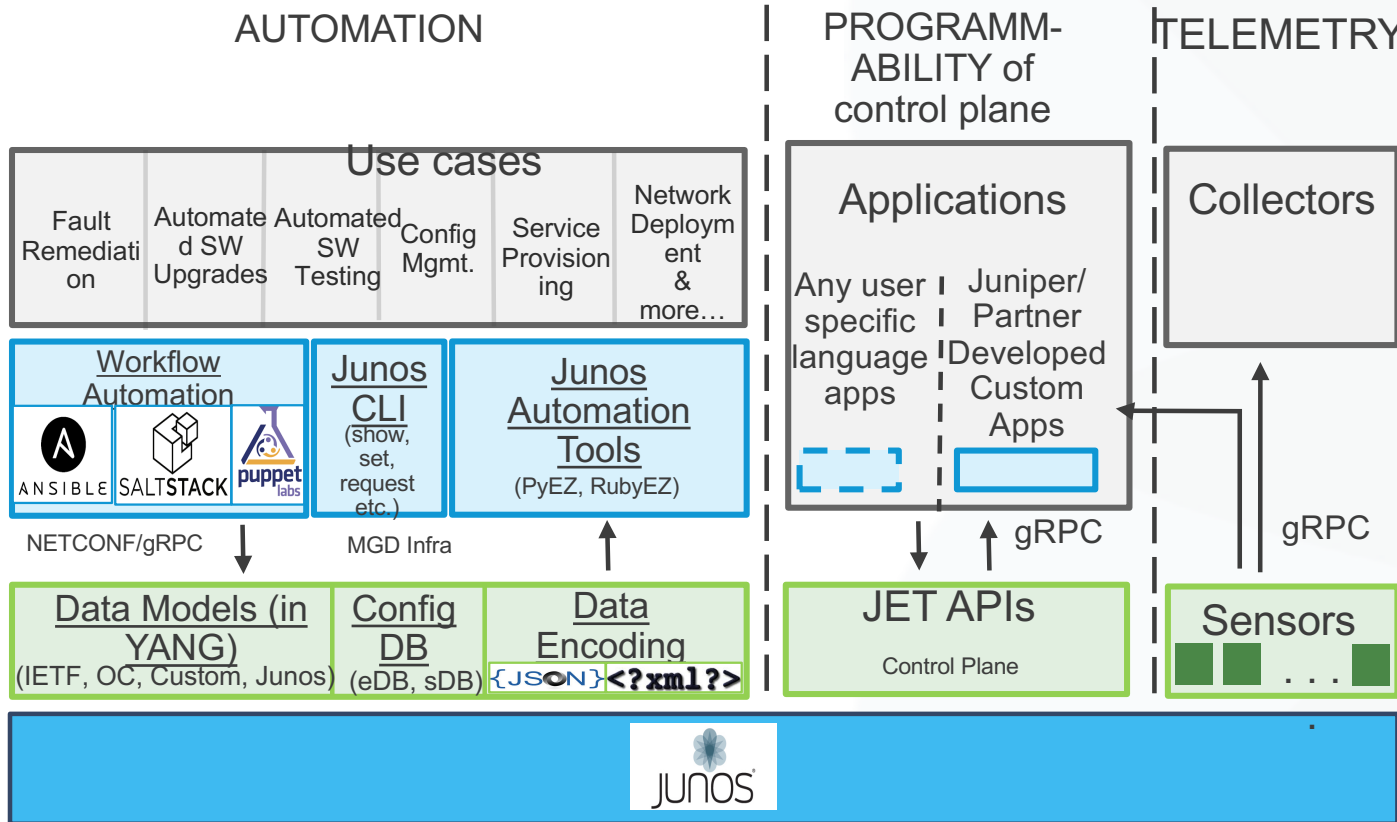
Auto Rule Placement

Reduce Effort By 20x

Reduce User Error

Improve Response Time

# Junos Automation Tools– Unrivaled Flexibility



Automation is a huge differentiator for Juniper  
 Infra built with Automation over 20 years

No other vendor has such a long history with automation  
 We have a Rich stack & continuously investing in enriching our portfolio

- Manual tasks are automated using infra in green showing capabilities exposed on Junos devices like data models/yang. We support many flavors, more agile so user can use any language.
- Config DB: Ephemeral DB provides faster commit times
- Data encoding formats to modify script outputs directly to JSON or XML (no conversion needed)
- Usecases can be done via CLI or workflow automation tools or via networking specific tools like RubyEZ, PyEZ-juniper developed on github.

## Programmability of control plane

South/north bound APIs for many functions like Firewall, routing, interface, manageability, Class Of Service.

- Junos extensibility toolkit –JET is the brand for ongoing work on APIs.
- gRPC is transport protocol
- Write a custom app in any language
- Juniper also builds User writes code against APIs

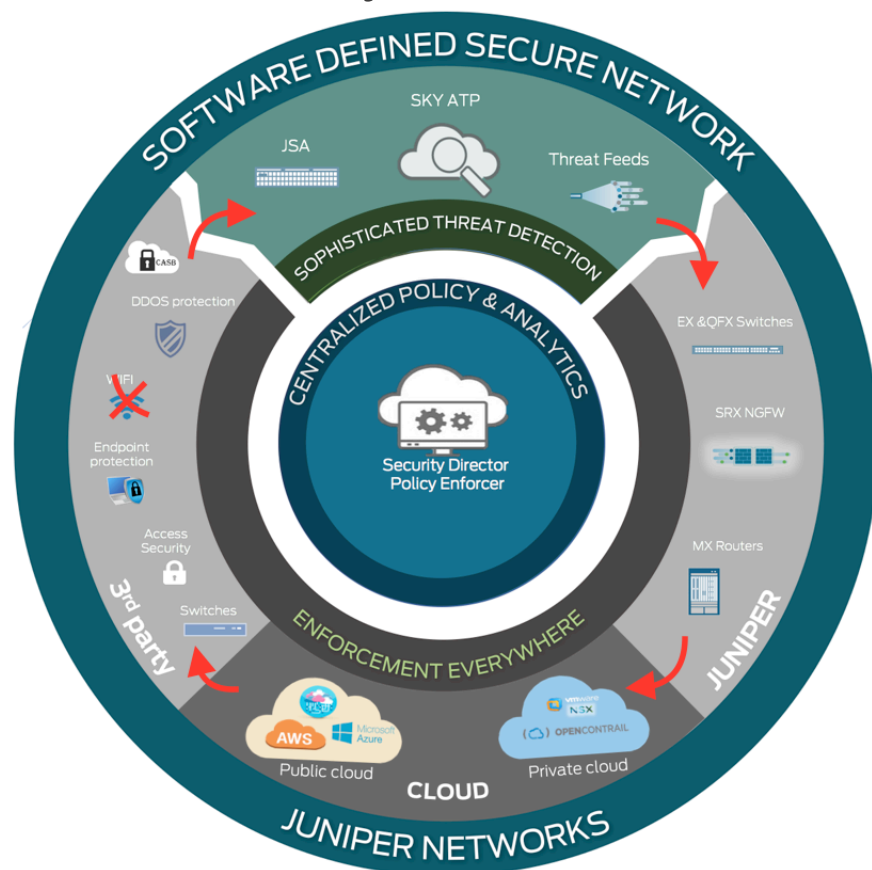
## Telemetry

Control + data plane on junos device support telemetry

- Collector is application sitting on mgmt. server running ansible or anything doing mgmt. activities..
- Specify in application sources of telemetry/JUNOS devices.
- Enable telemetry on junos, add target IP address of collector & server to listen to sensors on control+data plane on junos device.
- Feature enabled via CLI, controller, Ansible or anything user uses. Transport is gRPC and junos devices push data to server in specified encoding.
- High resolution Insights & Fine Grained capabilities & integrates with any type or number of open source tools & databases

# Software Defined Secure Networks (SDSN)

## Unified Security Platform



### Detection

- Leverage entire network and ecosystem for advanced threat intelligence and detection

### Policy

- User intent based policy model
- Consistent policy enforcement across multiple enforcement domains
- Robust visibility and management

### Enforcement

- Utilize any point of the network including firewalls, switches, routers, 3<sup>rd</sup> party devices, SDN and public cloud platforms as a points of enforcement

***Network as a single enforcement domain - Every element is a policy enforcement point***



**Thank you**