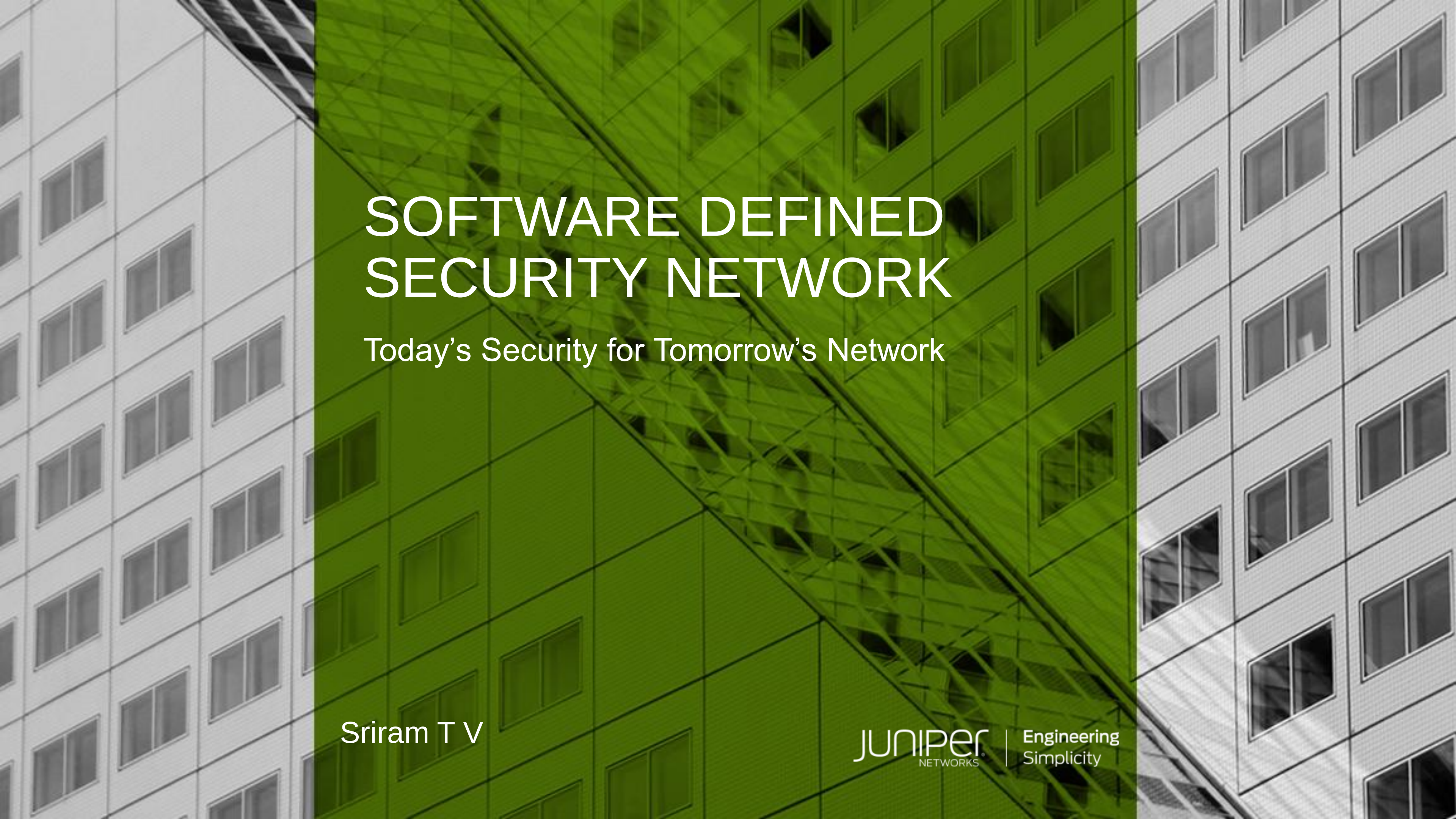


SOFTWARE DEFINED SECURITY NETWORK

Today’s Security for Tomorrow’s Network

Sriram T V

JUNIPER NETWORKS | Engineering Simplicity

TRENDS IMPACTING SECURITY

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

© 2018 Juniper Networks

CHANGING LANDSCAPE

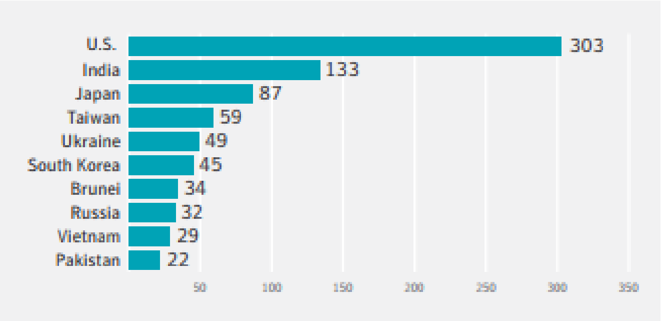
- Comprehensive security framework to address all aspects of cybersecurity with key focus on ***reducing the time to detect/mitigate an attack and operational complexity***
- Security is a ***key component of this transition to next generation infrastructure*** around Cloud, SD-WAN and Intent based networking systems.
- Security infrastructure should be able to ***protect the network from breaches, meet regulatory compliance and have proper controls in place***.
- Security solution should address the key challenges in datacenter and campuses around
    - ***User and workload protection*** based on risk profile and location
    - ***Threat detection and remediation***
    - Security ***analytics and automation***

© 2018 Juniper Networks

INTERNET SECURITY THREAT REPORT 2018 - SYMANTEC

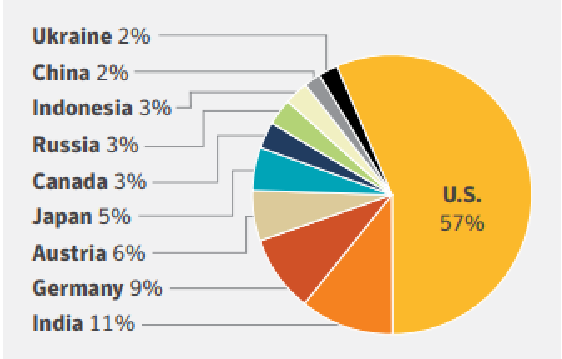
Top 10 countries affected by targeted attacks

Between 2015 and 2017, the U.S. was the country most affected by targeted attacks.



Top countries for mobile malware

Top 10 list of countries where mobile malware was most frequently blocked in 2017.



Internet Security Threat Report

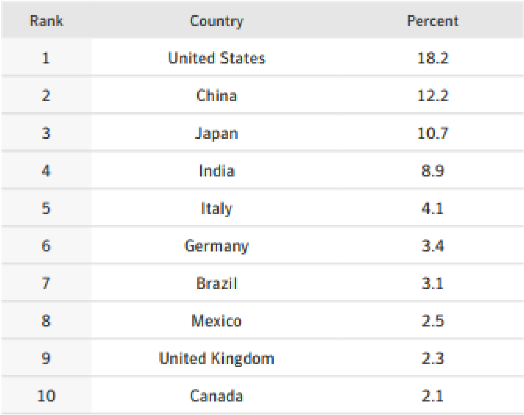
Volume

23

Symantec.

Ransomware detections by country

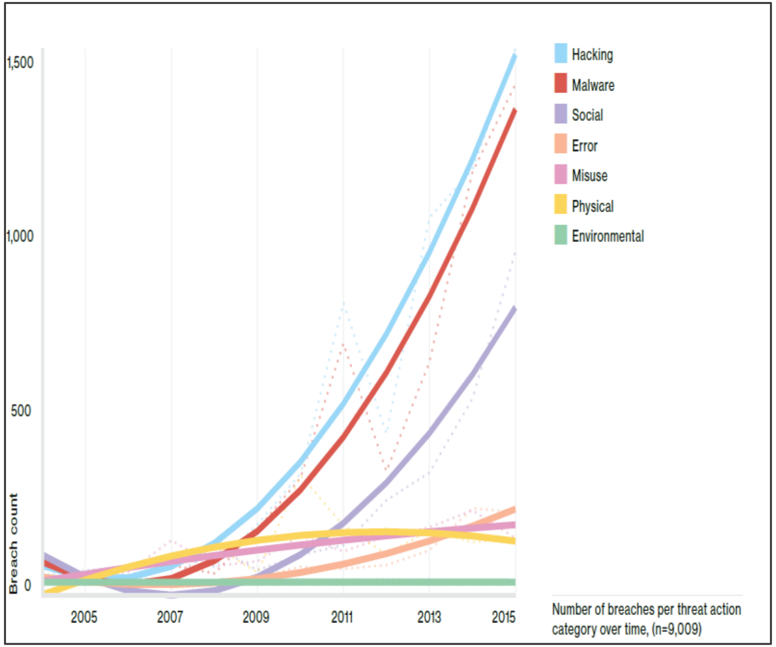
Typically, ransomware has been more dominant in countries with higher numbers of internet-connected populations.



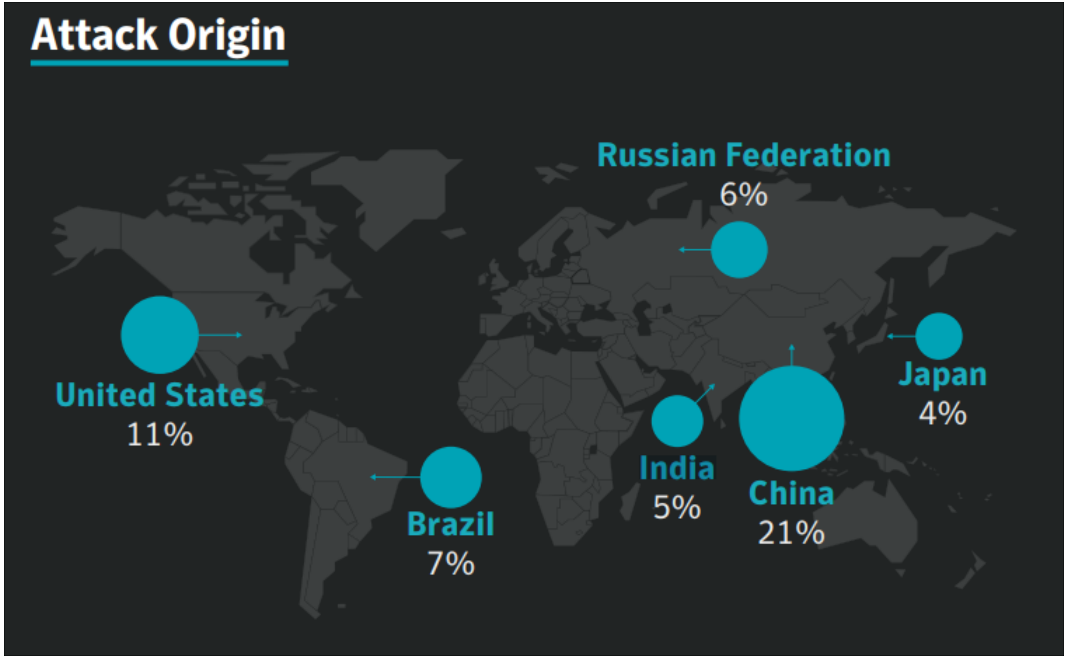
Rank	Country	Percent
1	United States	18.2
2	China	12.2
3	Japan	10.7
4	India	8.9
5	Italy	4.1
6	Germany	3.4
7	Brazil	3.1
8	Mexico	2.5
9	United Kingdom	2.3
10	Canada	2.1

© 2018 Juniper Networks

THREAT DEMOGRAPHICS



Number of breaches per threat action category over time, (n=9,009)



© 2018 Juniper Networks

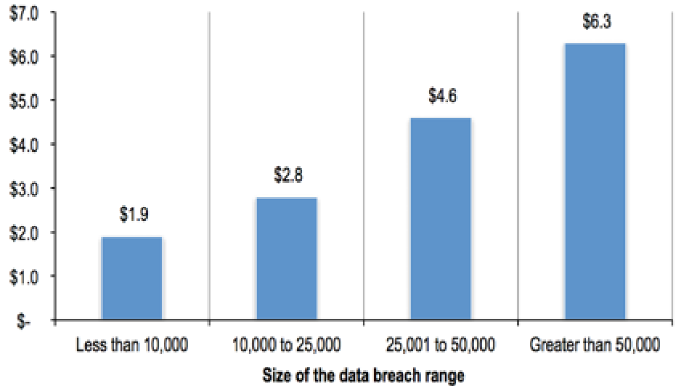
RISK & OPERATIONS

Average cost of breach is from US$ 3Mn

Top 3 root causes of the data breach

- Malicious Attack
- System Issues
- Human Error

Figure 10. Average total cost by size of the data breach
Measured in US$ (millions)



Operations Spend – $3 (Opex) / every $1 in network spend (Capex)

© 2018 Juniper Networks

SPECIALIZED SECURITY IS NOT SUFFICIENT

Intrusion Prevention

Endpoint Protection

Advanced Threat Prevention

Application Security

010101001010101
010111011011101
010110101001010
111001101110101

Data Loss Prevention

Perimeter oriented security

Limited Threat Visibility

Isolated security functions

Unco-ordinated Threat Intelligence

Multiple vendors and interfaces

Multiple Threat Scores

Manual co-ordination / enforcement

Poor Correlation & Resolution Time

© 2018 Juniper Networks

PARADIGM SHIFT

Hardware defined → Software/cloud defined

Perimeter → Pervasive

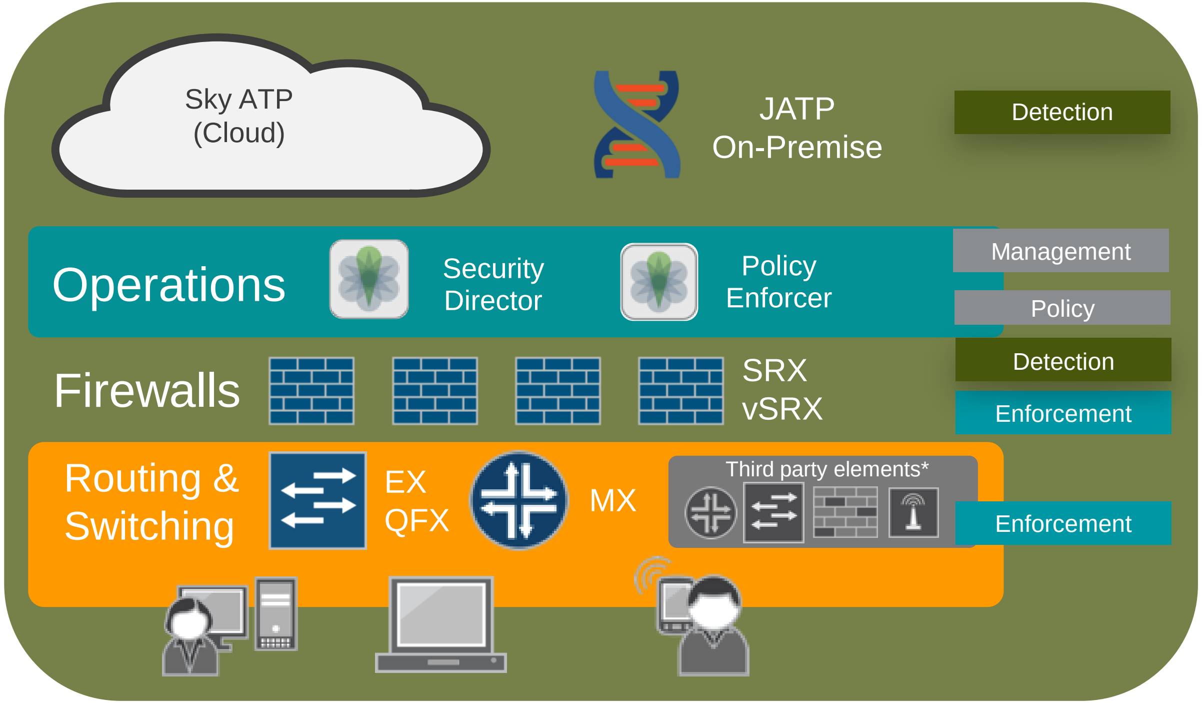
Manual enforcement → Automated

Configuration driven → Business driven

Closed ecosystem → Open framework

© 2018 Juniper Networks

SOFTWARE ENABLED SECURITY NETWORK (SDSN)



Detection

Cloud-enabled

Multi-vendor

Enforcement

Pervasive

Multi-directional

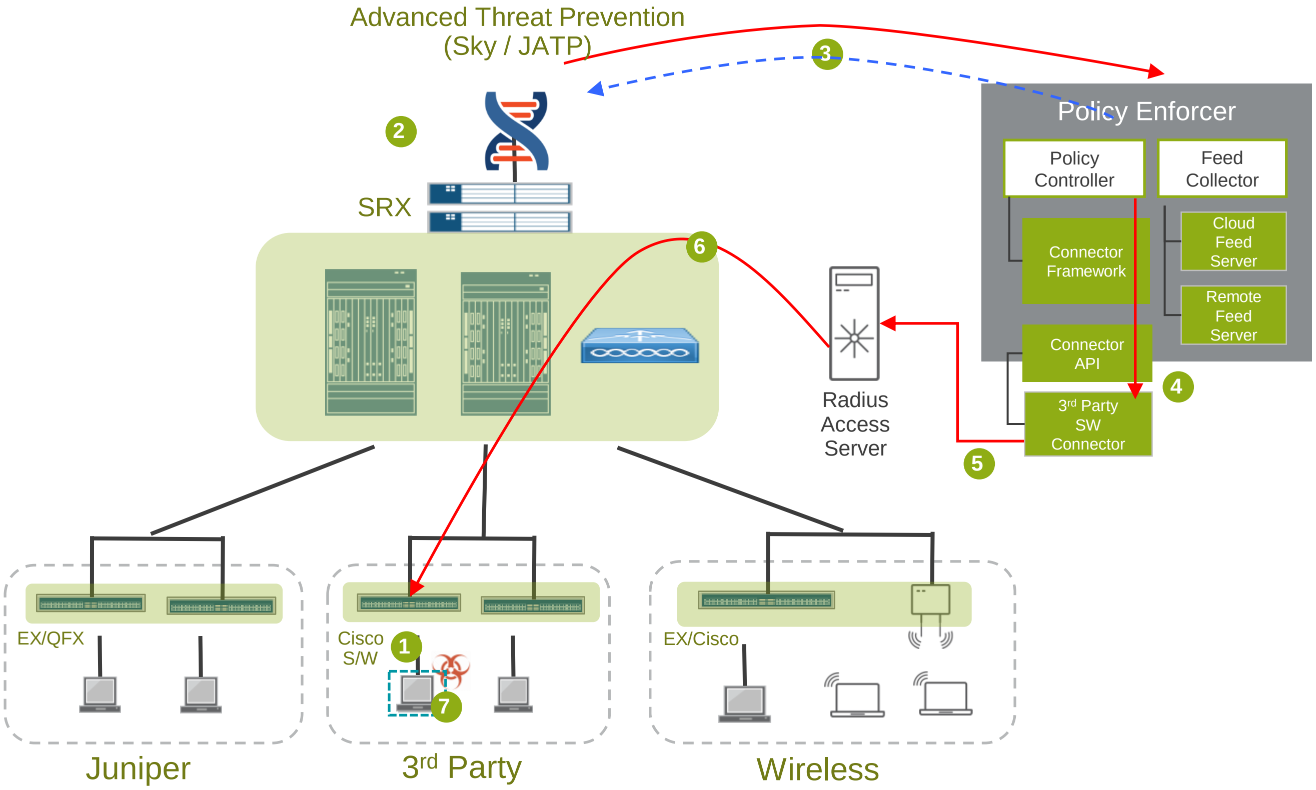
Policy & Mgmt

Automated

Intent Driven

© 2018 Juniper Networks

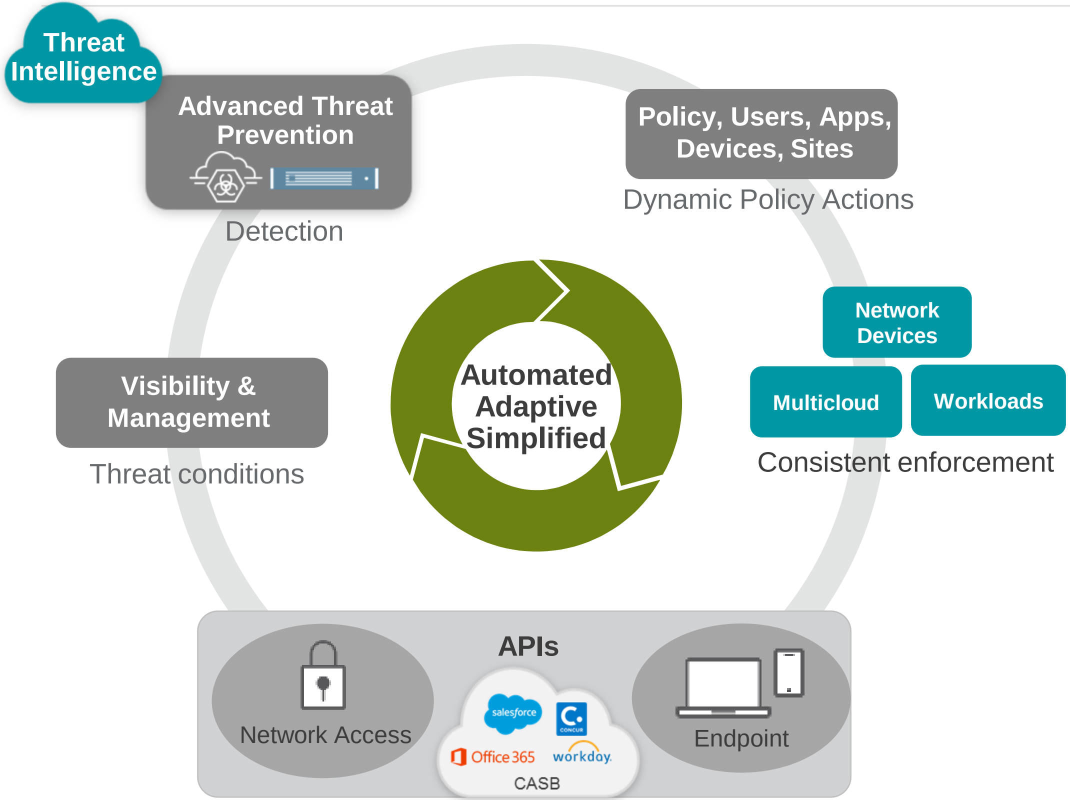
SDSN – TYPICAL CALL FLOW



1. End user authenticates to network via 802.1x or mac authentication
2. ATP detects End Point getting 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 End Point authenticated on.
8. Policy enforcer Communicates the end host details back to ATP

© 2018 Juniper Networks

UNIFIED CYBERSECURITY PLATFORM

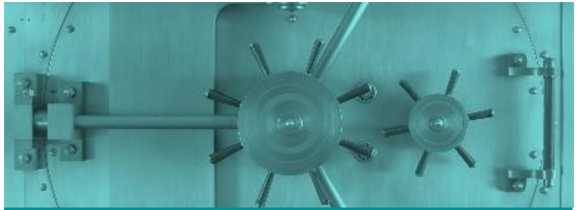


- Fast protection from unknown malware and advanced attacks
- Threat behavior analysis across threat lifecycle
- One touch automated enforcement and mitigation
- Unified visibility across traditional and multicloud environments
- Open architecture and suite of APIs
- Powered by Software Defined Secure Networking (SDSN)

© 2018 Juniper Networks

FUTURE PROOF STRATEGY FOR CYBERSECURITY

ANY NETWORK ASSET



Unified enforcement domain

ANY CLOUD

Consistent, automated defense across diverse environments

ANY VENDOR

Open ecosystem for threat intel sharing and integration

Unified cybersecurity platform powered by automation, machine learning and real-time intelligence

© 2018 Juniper Networks

SECURITY DOMAIN ECOSYSTEM

Endpoint

- Carbon Black.
- CROWDSTRIKE
- Symantec.
- McAfee

Firewall/SWG

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

SIEM

- splunk>
- JUNIPER
- IBM Radar
- ArcSight An HP Company

CASB

- netskope

NAC/Identity

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

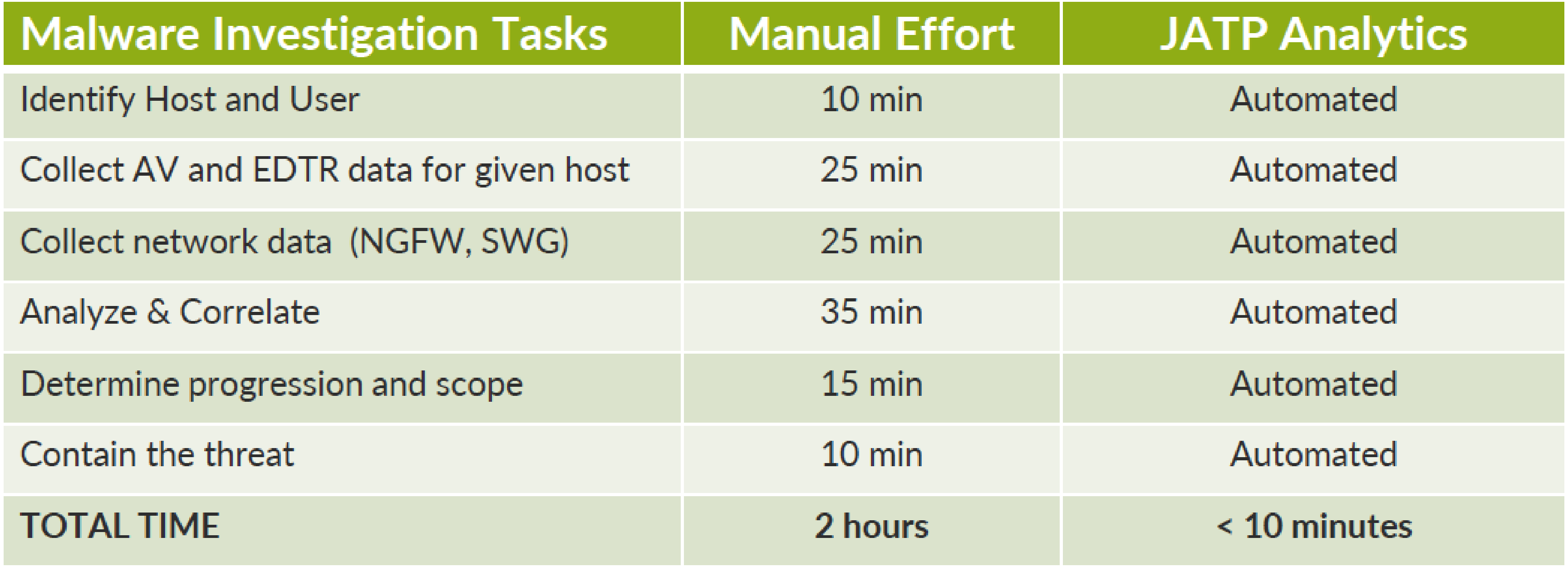
Other

- Gigamon
- riverbed
- DB NETWORKS
- exabeam
- Phantom
- CYBERSPONSE ADAPTIVE SECURITY

Ready to Deploy End to End Security Solutions

© 2018 Juniper Networks

AUTOMATION TO ACHIEVE PRODUCTIVITY GAINS



Malware Investigation Tasks	Manual Effort	JATP Analytics
Identify Host and User	10 min	Automated
Collect AV and EDTR data for given host	25 min	Automated
Collect network data (NGFW, SWG)	25 min	Automated
Analyze & Correlate	35 min	Automated
Determine progression and scope	15 min	Automated
Contain the threat	10 min	Automated
TOTAL TIME	**2 hours**	**< 10 minutes**

Japan customers said 4+ hrs!

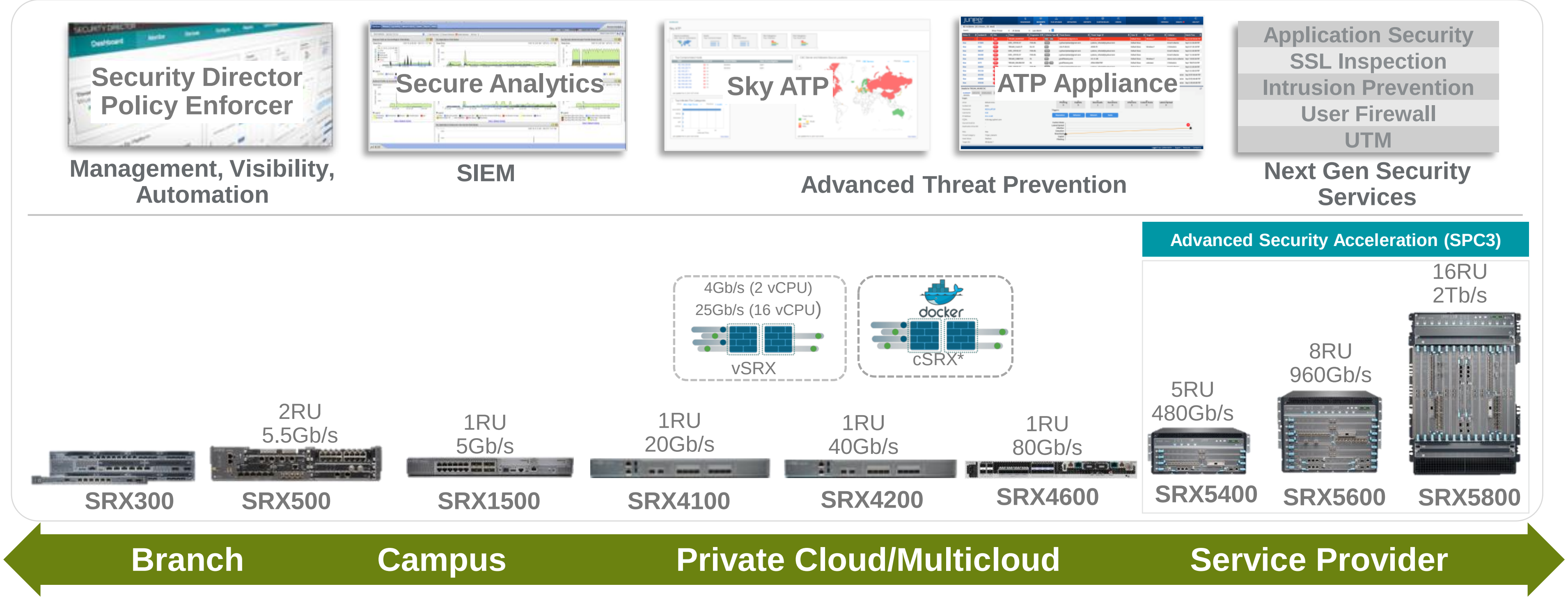
© 2018 Juniper Networks

WHY JUNIPER ?

- ✓ Juniper powers 60+% of world’s Internet transactions
- ✓ Top 130 service providers across the globe have deployed Juniper
- ✓ 6 out of 7 world’s largest stock exchanges use Juniper
- ✓ Top 5 social media properties run on Juniper
- ✓ Juniper secures more than 86% of US smartphone traffic
- ✓ Juniper powers the world’s largest enterprise networks, including 97 of Fortune Global 100

© 2018 Juniper Networks

COMPLETE SECURITY PORTFOLIO



Security Director
Policy Enforcer

Management, Visibility, Automation

Secure Analytics

SIEM

Sky ATP

ATP Appliance

Advanced Threat Prevention

Application Security
SSL Inspection
Intrusion Prevention
User Firewall
UTM

Next Gen Security Services

Advanced Security Acceleration (SPC3)

Beta*

© 2018 Juniper Networks

tsriram@juniper.net

© 2018 Juniper Networks