EXHIBIT 14

UNREDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

JUNIPER NETWORKS

Sky Advanced Threat Prevention

Bopaiah Puliyanda

Product Manager

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

Trial Exhibit 88

Case No. 17-CV-05659-WHA

Date Entered: __________ By: ____________
Deputy Clerk

Juniper's Security Focus

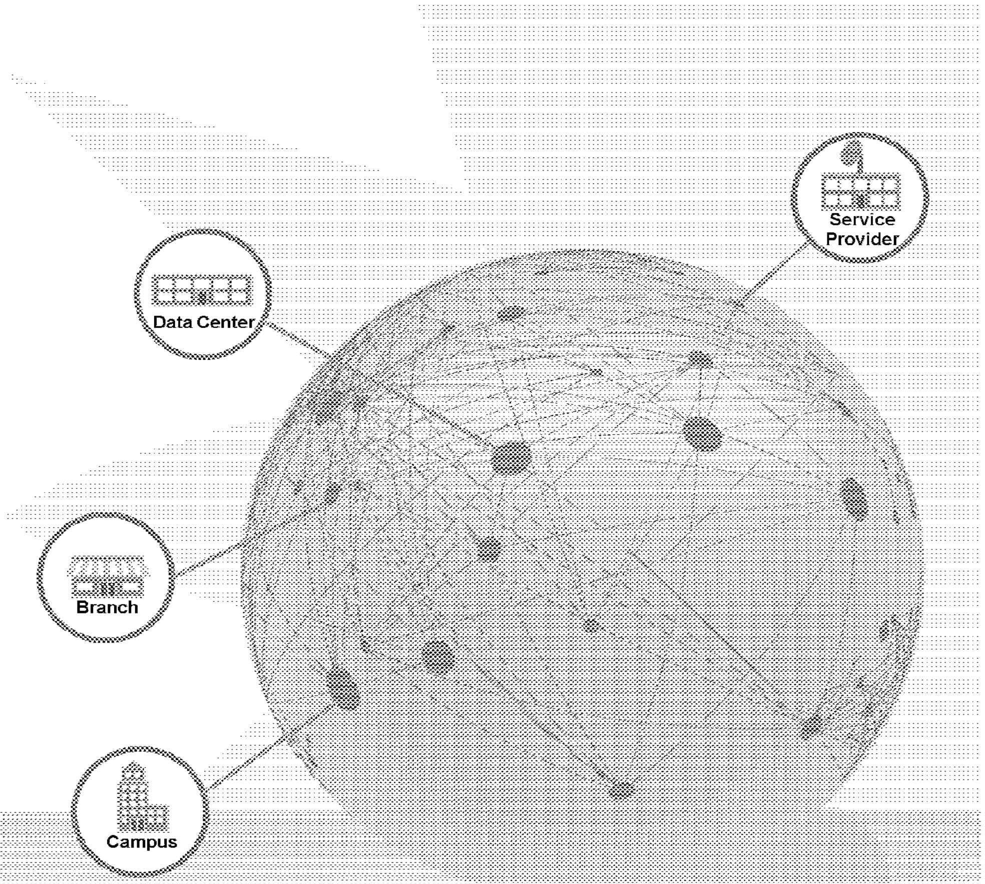
Software Defined Secure Networks

High Performance Platforms

Advanced Threat Protection

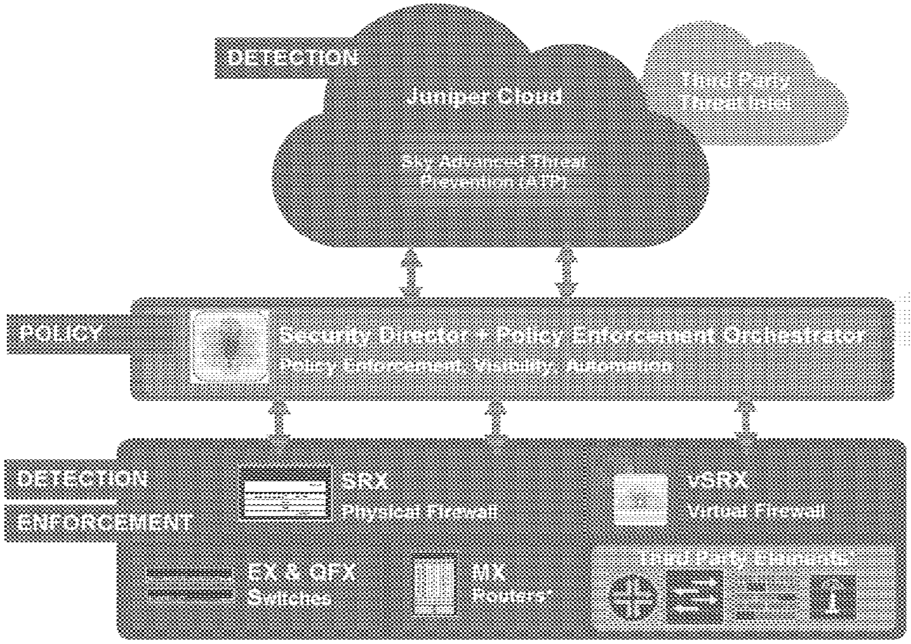
Central Management and User Experience

Automation and Operator Efficiency



Software Defined Secure Networks (SDSN)

Unified Security Platform



*Roadmap, subject to change

Detection

- Fast, effective protection from advanced threats
- Integrated threat intelligence

Policy

- Adaptive enforcement to firewalls, switches, 3rd party devices and routers
- Robust visibility and management

Enforcement

- Consistent protection across physical/virtual
- Open and programmable environment

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

Threats are Everywhere

Perimeter security isn't enough.
Malware walks in with your employee!
Stop Threats. Faster.

- Increasing sophistication
- Increasing variability
- Threats are already inside
- Keeping data secure throughout your network is key!

Speaker Notes for Slide 4

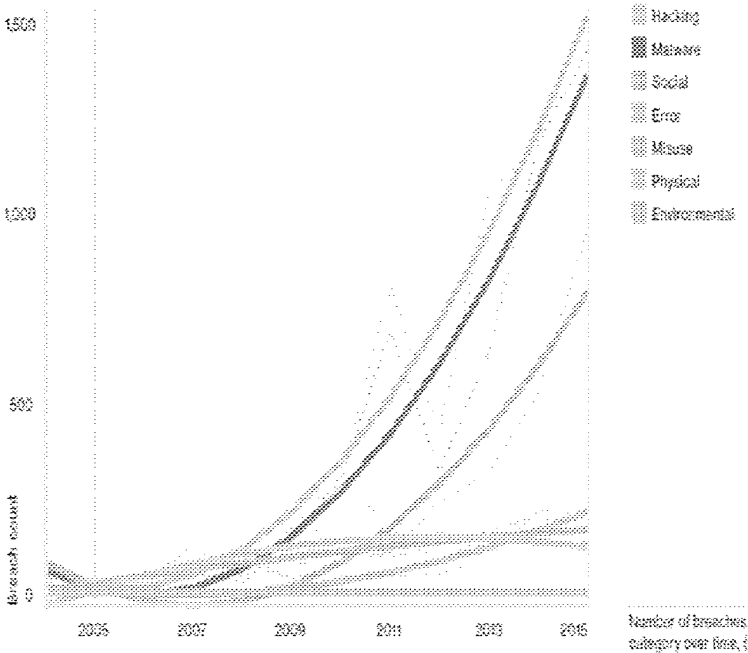
Outside your network, inside your network and between endpoints and the cloud apps your employees use. It's a zero trust world. (Zero trust can be the only security posture.)

Threats have changed. From phishing, anti-malware, and morphing executables to security hackers who infiltrate Enterprises to retrieve data for financial gain. The attacks are targeted, focused and use advanced persistent threats. And today, these attackers have the advantage of time on their side. Enterprises have the disadvantage of the complexity of their networks as well as organizational complexity working against them.

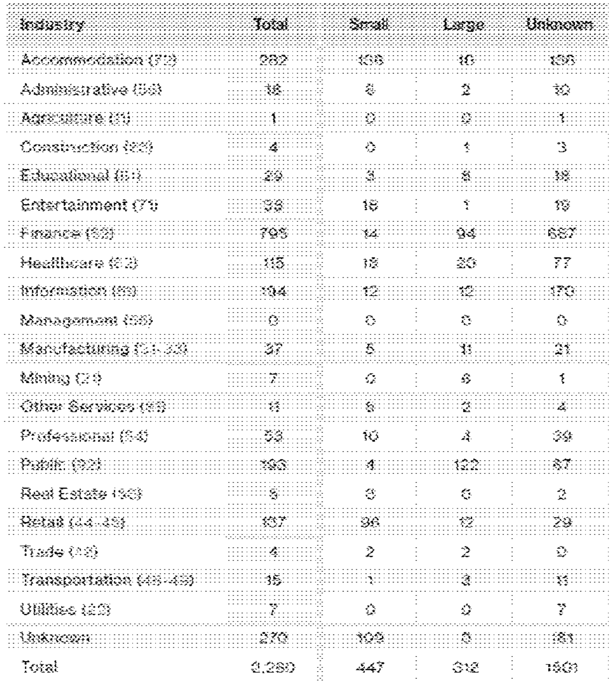
Attackers are also are increasingly able to socially engineer their way into your internal network. The variability of threats range from large, organized and systematic attacks to employees of a company who may have accessed public Wi-Fi or inadvertently clicked on the wrong link and as a result is now unknowingly infected with malware. They then spread the threat as their device connects directly within the network. The best (and only) security approach has to assume that threats are already inside your enterprise perimeter. And it must assume that new types of threats will pop up every day, which means your security approach needs to be more agile than ever and more decisive once a breach is found.

Security used to only need to be at the edge of your network. Now you have to secure at every point of access in your network, because it's not just the intruder trying to break in. The threat can now be your employee who has walked through your front door with malware on their device or an employee who was developing in a container and accidentally copied malware into his code. (And with the proliferation of BYOD and IoT, trying to secure endpoints is nearly impossible) Enterprise security posture today requires zero trust of anything entering or leaving the network.

Malware continues to dominate



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



Industry	Total	Small	Large	Unknown
Accommodation (72)	282	136	10	136
Administrative (56)	18	6	2	10
Agriculture (11)	1	0	0	1
Construction (23)	4	0	1	3
Educational (61)	29	3	8	18
Entertainment (71)	38	18	1	19
Finance (52)	795	14	94	687
Healthcare (62)	115	18	20	77
Information (51)	194	12	12	170
Management (55)	0	0	0	0
Manufacturing (31-33)	37	5	11	21
Mining (21)	7	0	6	1
Other Services (81)	11	5	2	4
Professional (54)	53	10	4	39
Public (92)	193	4	122	67
Real Estate (53)	5	3	0	2
Retail (44-45)	137	96	12	29
Trade (42)	4	2	2	0
Transportation (48-49)	15	1	3	11
Utilities (22)	7	0	0	7
Unknown	270	109	0	161
Total	2,260	447	312	1501

Small = organizations with fewer than 1,000 employees, Large = organizations with 1,001+ employees.

Number of security incidents with confirmed data loss by victim industry and organization size, 2015 dataset

Source: Verizon DBIR 2016 report

Speaker Notes for Slide 5

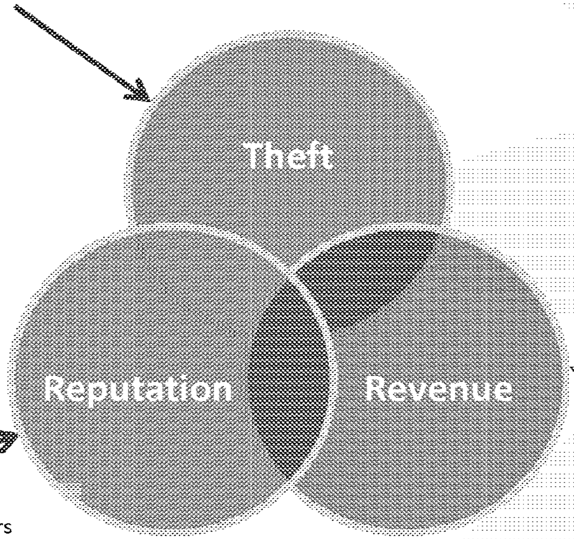
Impact of security breaches:

Target breach

Ponemon Institute:

Average breach costs $214 per record stolen

Target Stolen Data: 110M Records



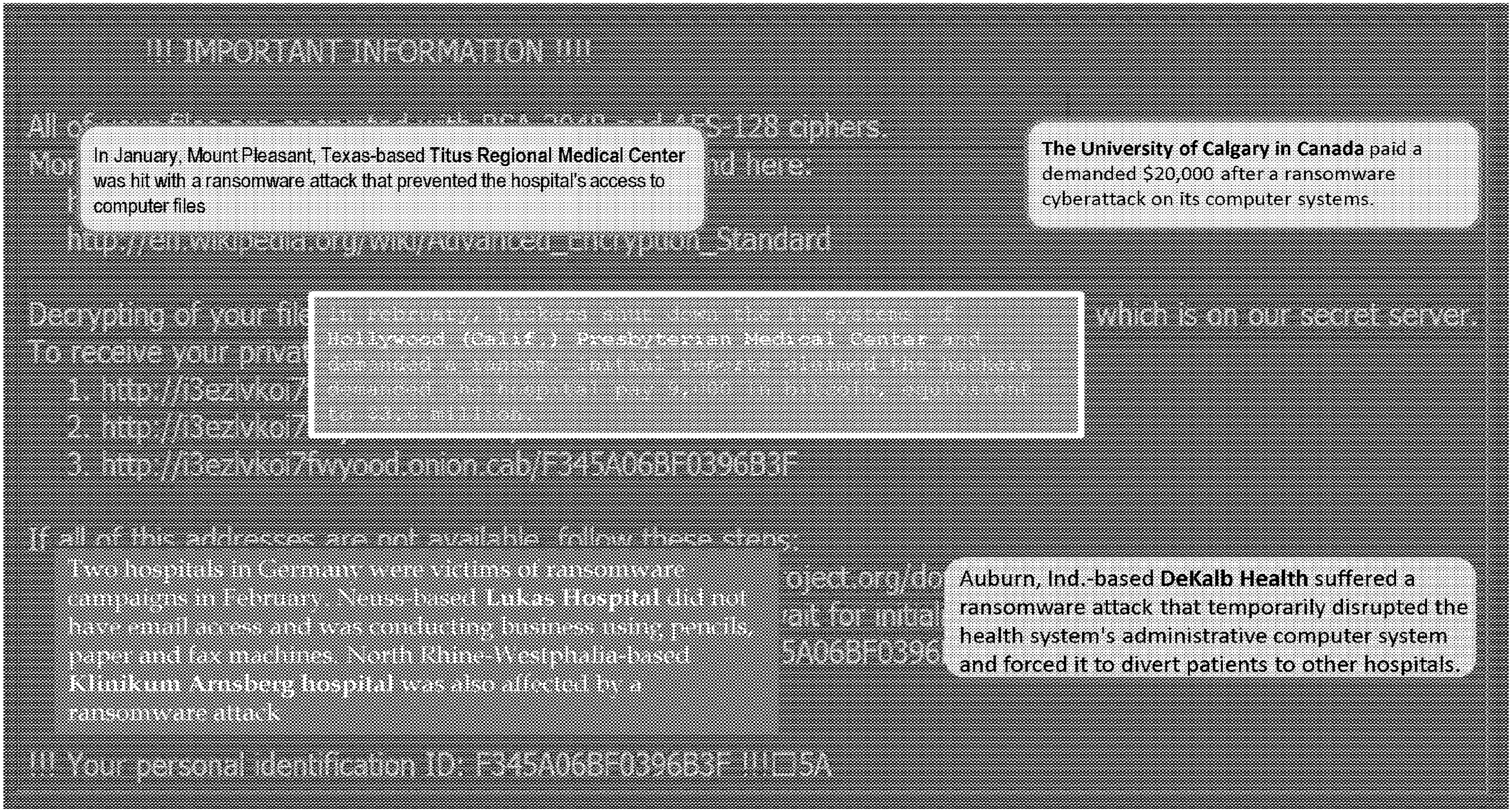
A dozen lawsuits in progress, lost customers

Cost of the breach:

- Gross expense of $191M
- Net cost of $162M

Speaker Notes for Slide 6

While the monetary cost of a breach is relatively easy to calculate the cost in reputation and public trust can be much greater, as well as more difficult to estimate. Several organizations have been target more than once, with huge costs in both financial and more ephemeral terms.



!!! IMPORTANT INFORMATION !!!!

All o … AES-128 ciphers.

Mor … nd here:

h

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your fil … which is on our secret server.

To receive your privat

1. http://i3ezlvkoi7

2. http://i3ezlvkoi7

3. http://i3ezlvkoi7fwyood.onion.cab/F345A06BF0396B3F

If all of this addresses are not available, follow these steps:

oject.org/do

ait for initial

5A06BF0396

!!! Your personal identification ID: F345A06BF0396B3F !!!□5A

In January, Mount Pleasant, Texas-based **Titus Regional Medical Center** was hit with a ransomware attack that prevented the hospital's access to computer files

The University of Calgary in Canada paid a demanded $20,000 after a ransomware cyberattack on its computer systems.

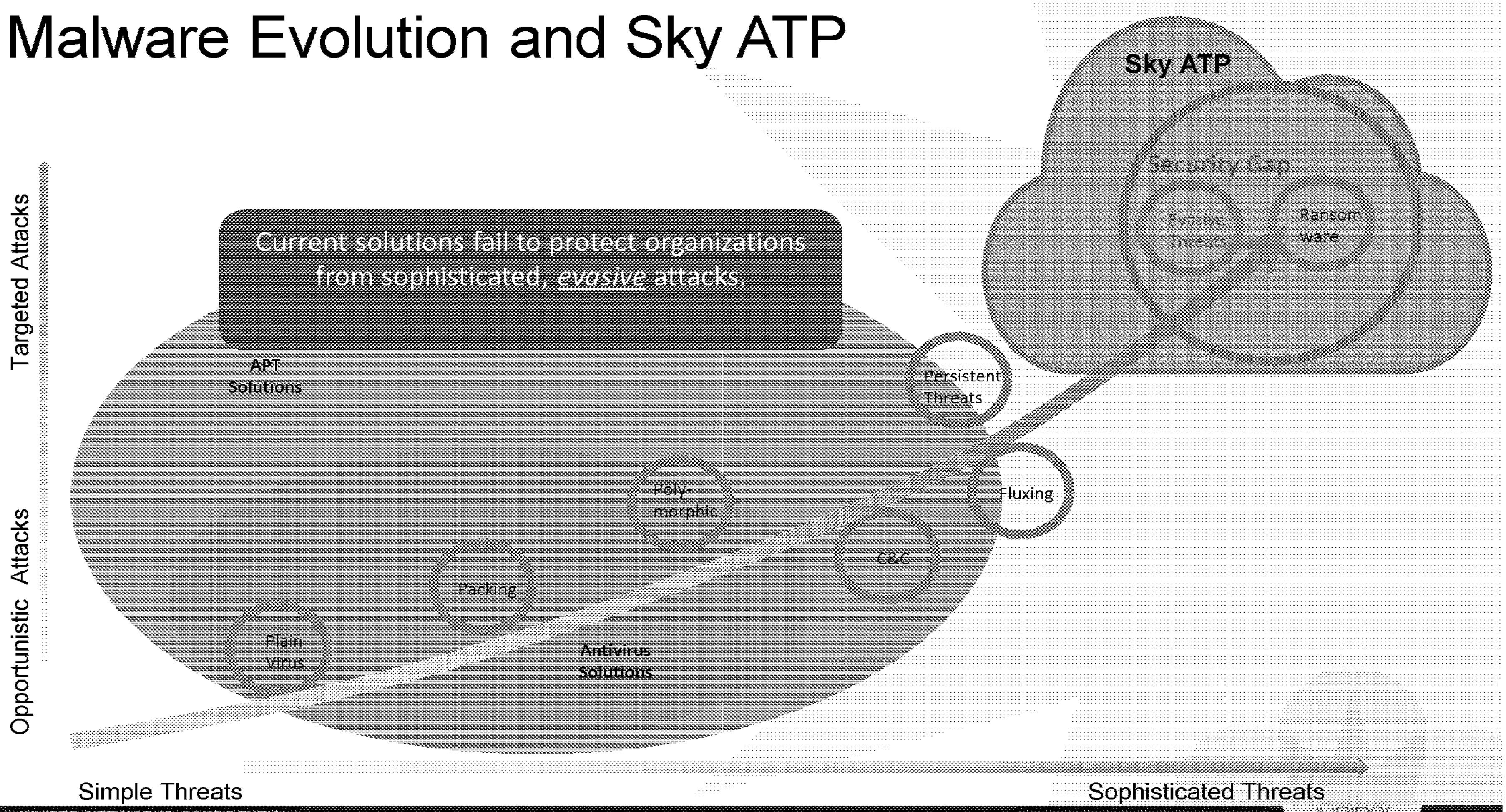
In February, hackers shut down the IT systems of **Hollywood (Calif.) Presbyterian Medical Center** and demanded a ransom. Initial reports claimed the hackers demanded the hospital pay 9,000 in bitcoin, equivalent to $3.6 million.

Two hospitals in Germany were victims of ransomware campaigns in February. Neuss-based **Lukas Hospital** did not have email access and was conducting business using pencils, paper and fax machines. North Rhine-Westphalia-based **Klinikum Arnsberg hospital** was also affected by a ransomware attack

Auburn, Ind.-based **DeKalb Health** suffered a ransomware attack that temporarily disrupted the health system's administrative computer system and forced it to divert patients to other hospitals.

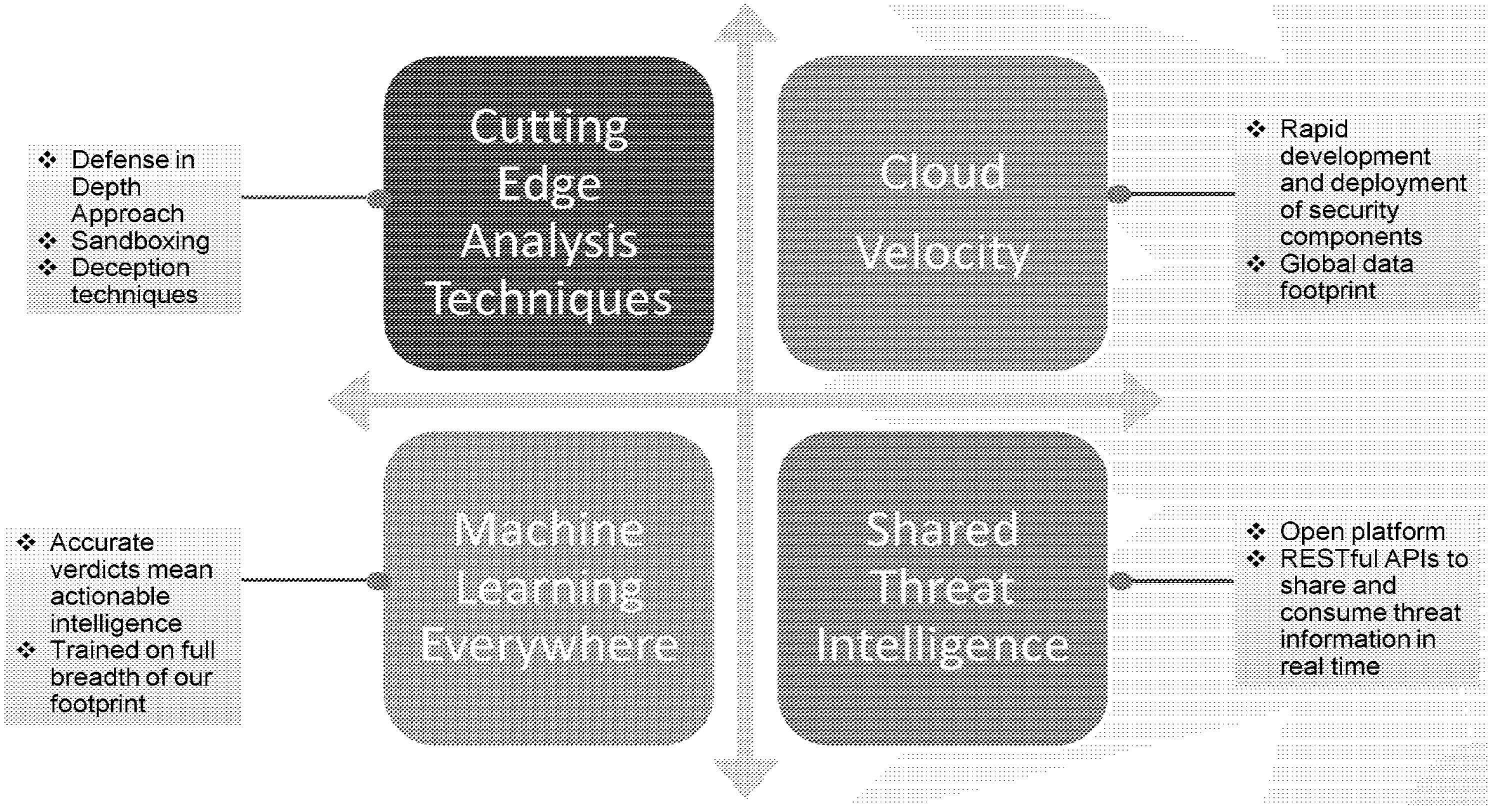
Speaker Notes for Slide 7

Malware Evolution and Sky ATP



Current solutions fail to protect organizations from sophisticated, *evasive* attacks.

Sky ATP Efficacy



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

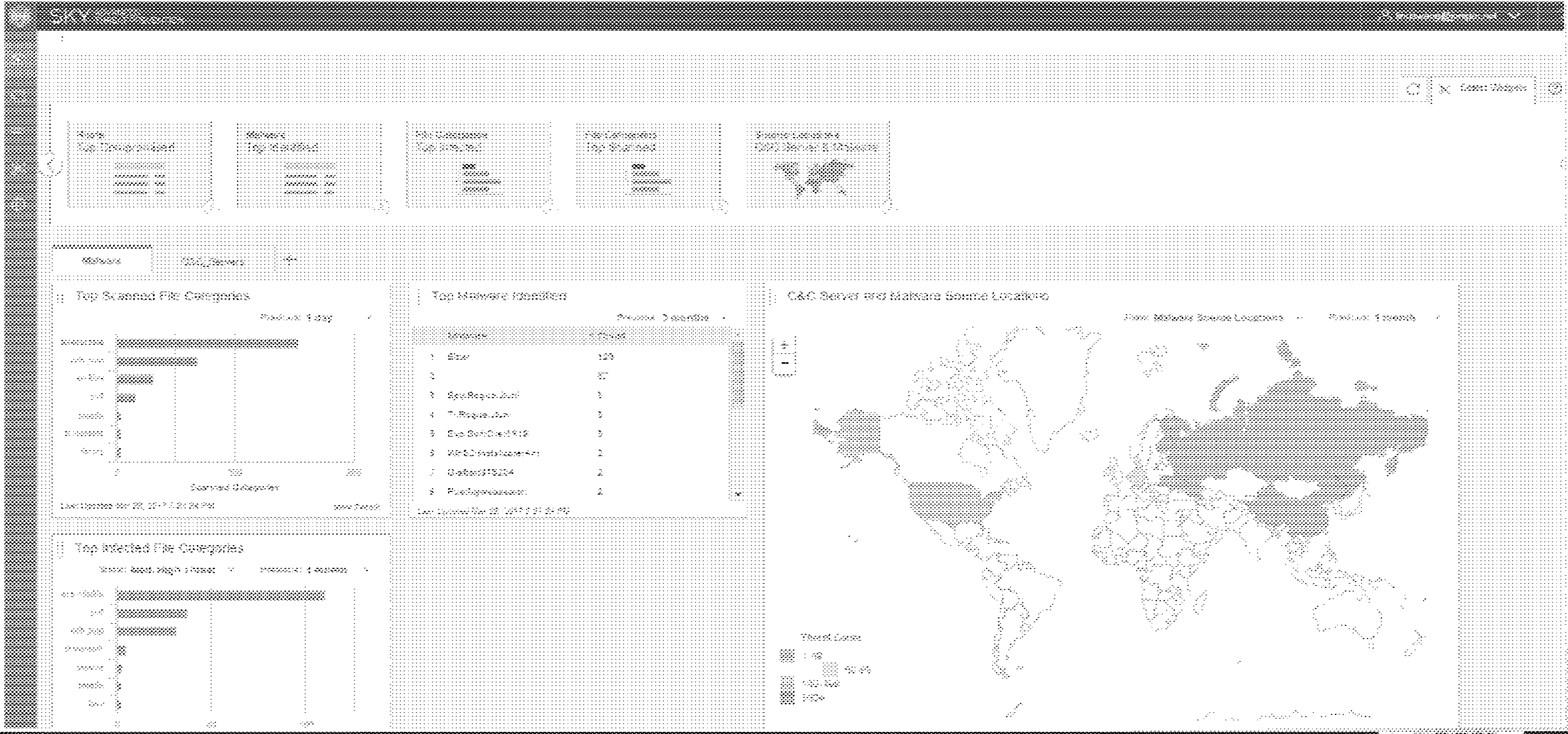
- Defense in Depth Approach
- Sandboxing
- Deception techniques

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

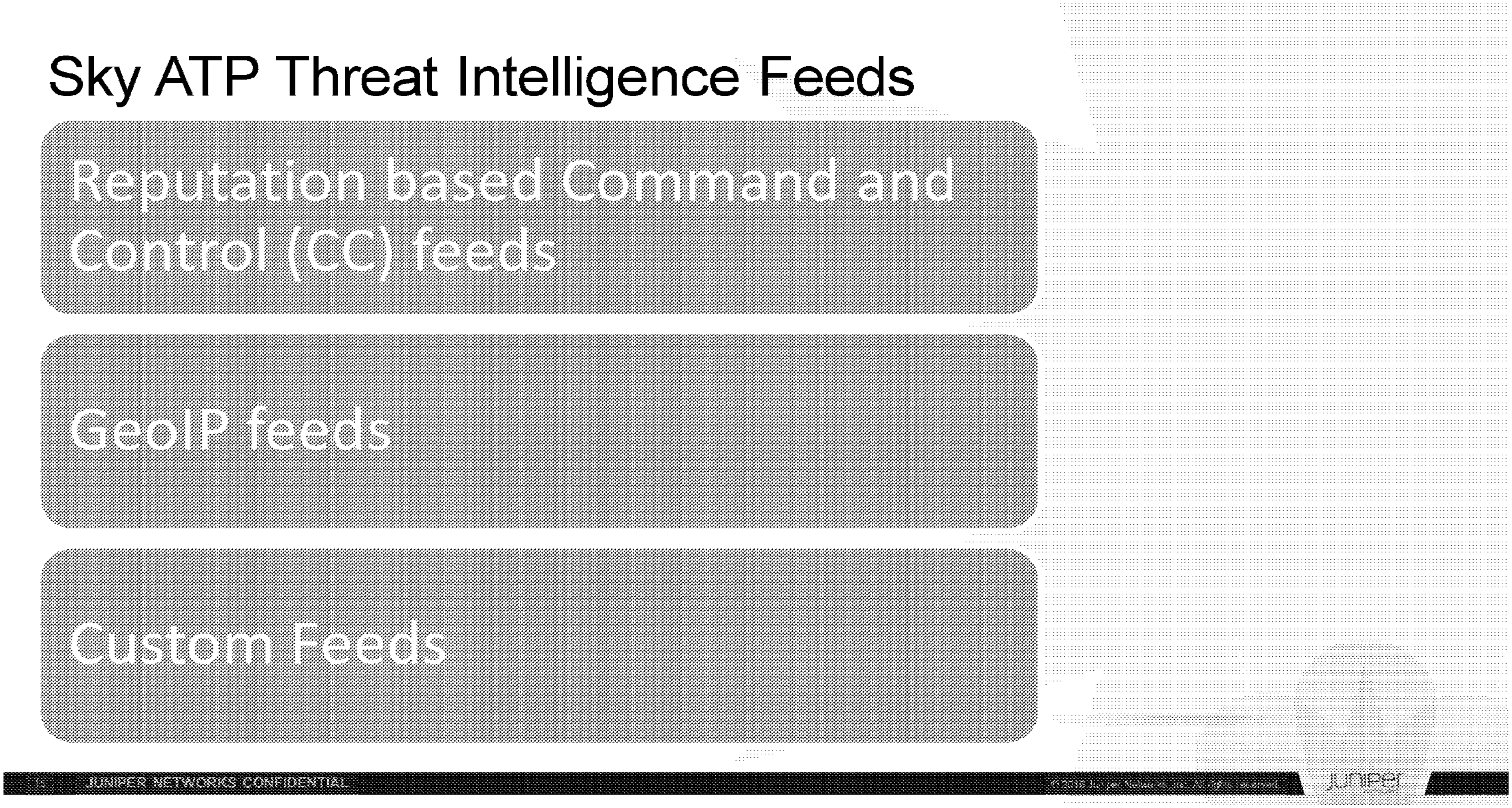
- Accurate verdicts mean actionable intelligence
- Trained on full breadth of our footprint

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

What is Sky Advanced Threat Prevention



Malware	Count
1 Eicar	120
2	87
3 [illegible]	3
4 [illegible]	3
5 [illegible]	3
6 [illegible]	2
7 [illegible]	2
8 [illegible]	2



Sky ATP Threat Intelligence Feeds

Reputation based Command and Control (CC) feeds

GeoIP feeds

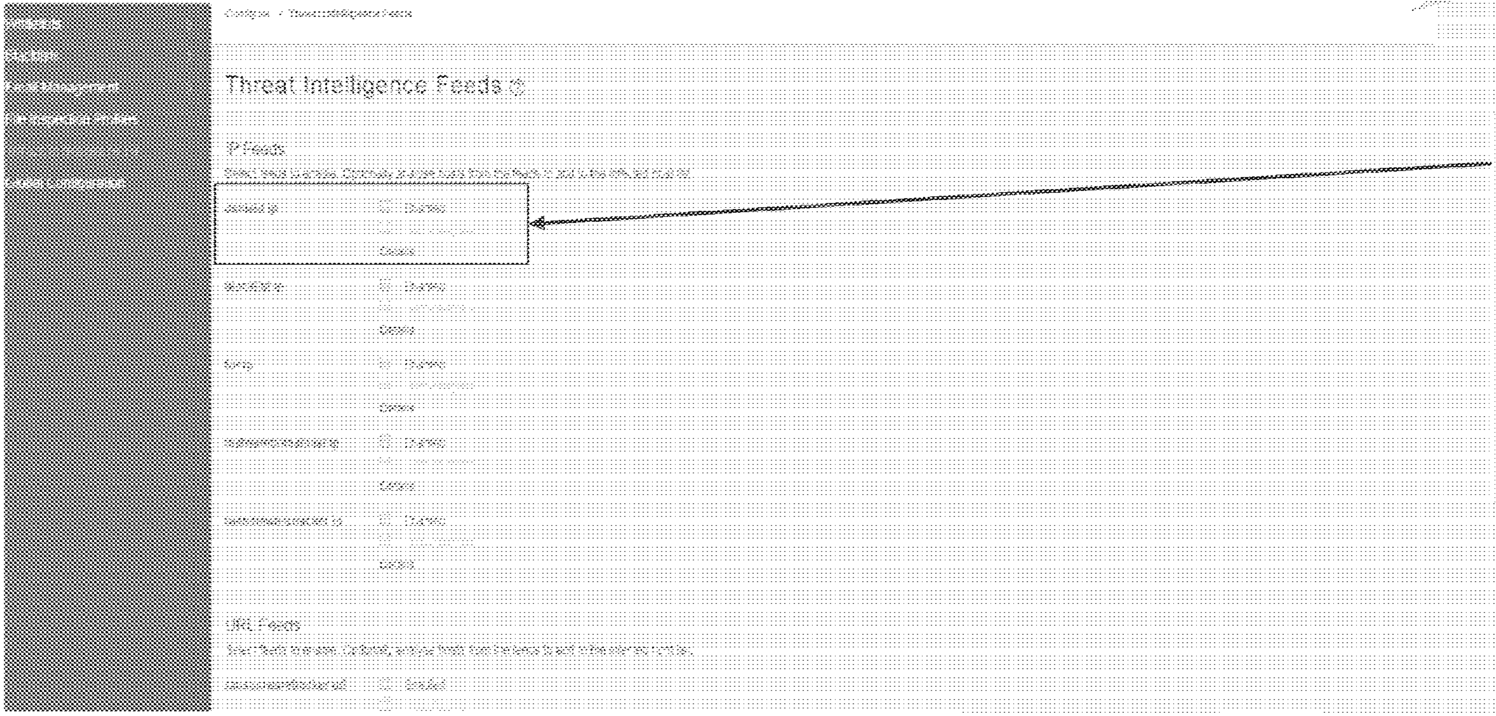
Custom Feeds

Command and Control feeds

- Derived from a global sensor network and malware sandnet
- 50 to 100K domain names and 350 to 500K IPs
- 13 different categories including Command and Control (CC), Drop sites, Spyware sites, P2P CC, Bitcoin related, ToR nodes, AbusedTLD
- Separate lists for IPs, URLs (FQDNs supported too)
- Updated in real-time and aggressively aged to reflect current conditions. Over 30% turned over every 3-4 weeks
- Threat scores (1->10). Scores driven by both volume and type of activity
- Data is based on multiple commercial sources as well as proprietary Juniper Sky ATP intelligence (we don't use open source data sources)
- Data quality is enhanced using additional network intelligence done by Juniper and a machine learning backend rescores all entries continually

Integrated open source feeds

New Feature

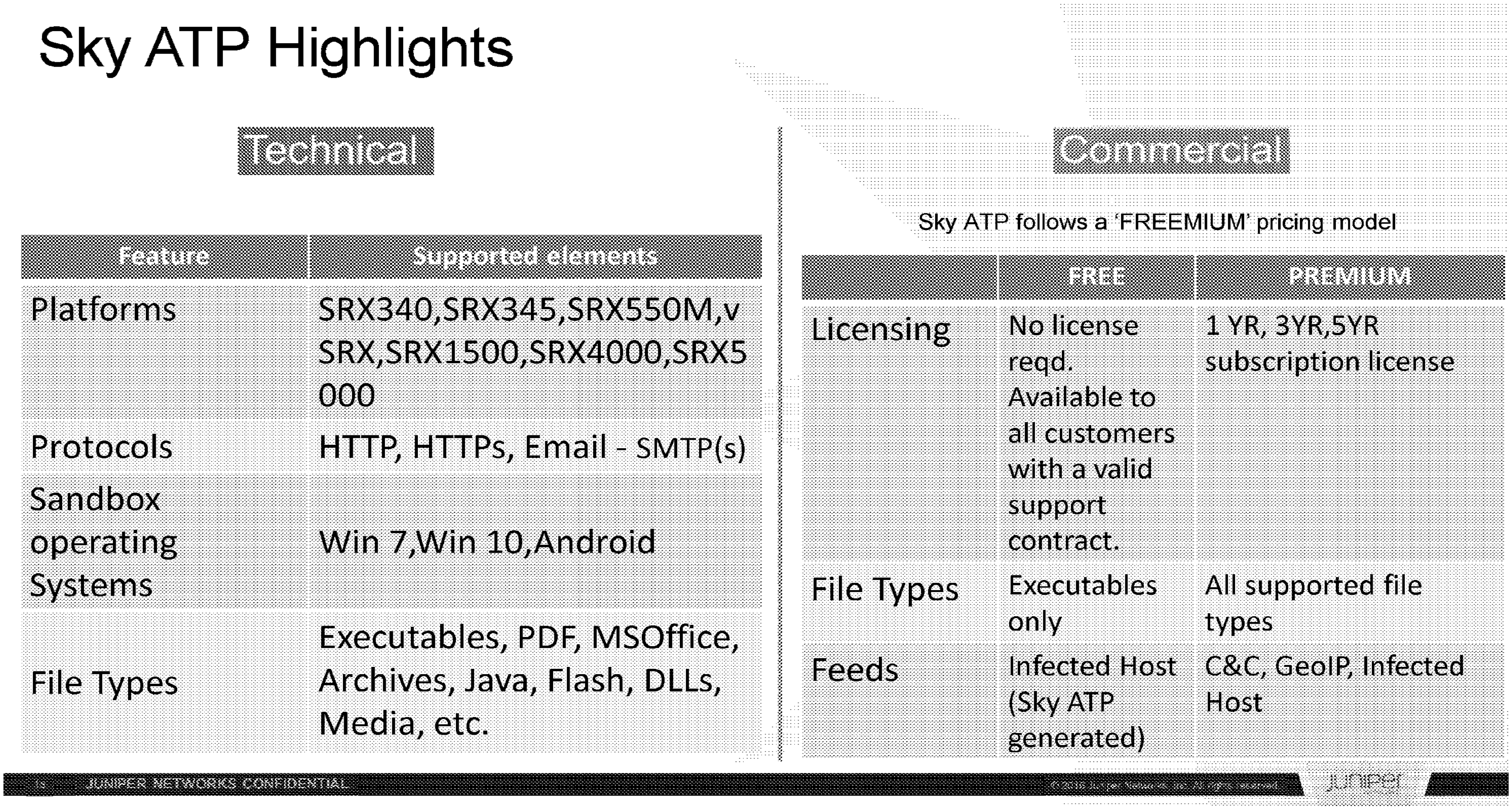


Threat Intelligence Feeds

IP Feeds

URL Feeds

- One click import of threat feeds from multiple sources
- Enforce on SRX firewall



Sky ATP Highlights

Technical

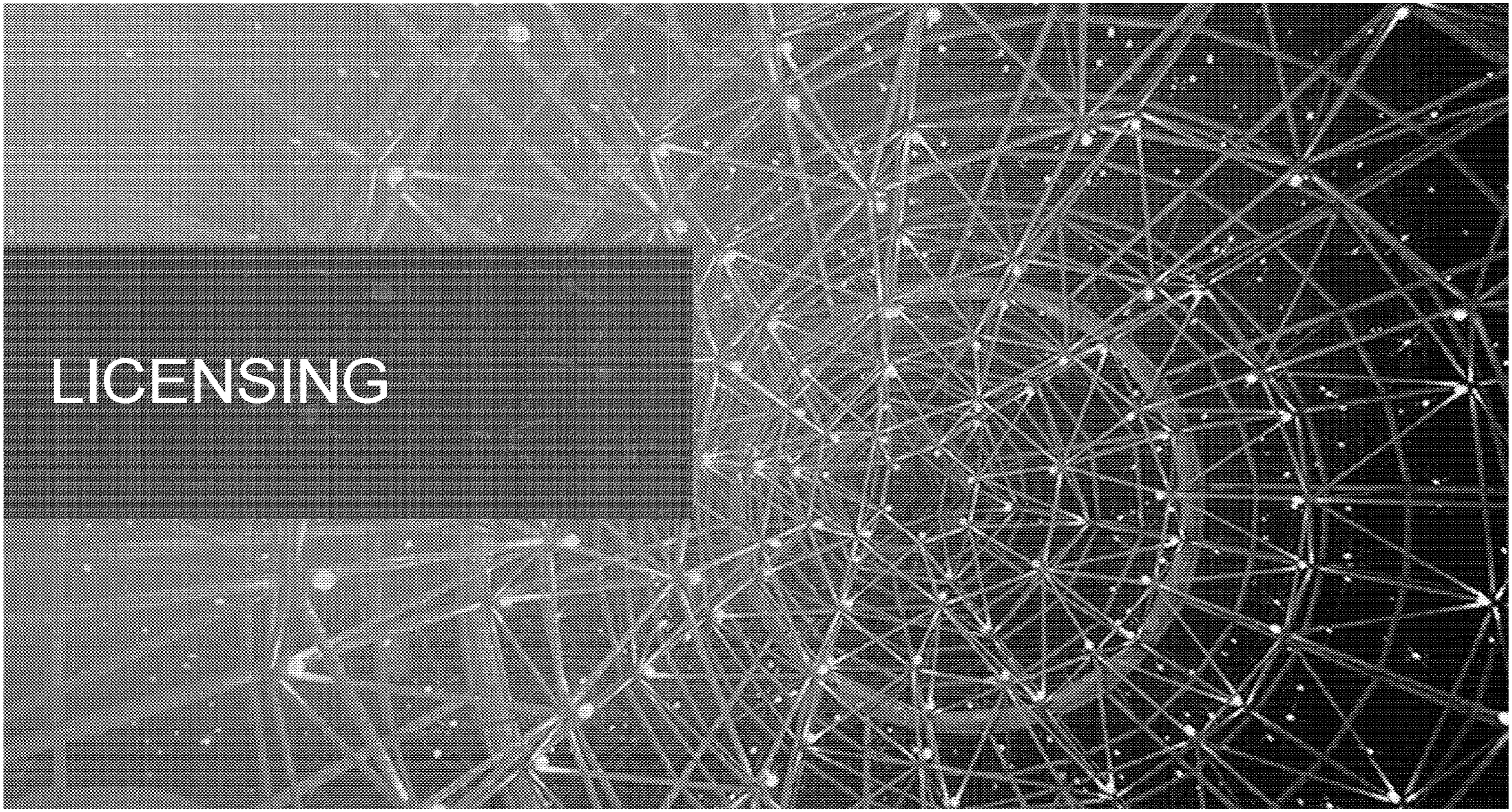
Feature	Supported elements
Platforms	SRX340,SRX345,SRX550M,vSRX,SRX1500,SRX4000,SRX5000
Protocols	HTTP, HTTPs, Email - SMTP(s)
Sandbox operating Systems	Win 7,Win 10,Android
File Types	Executables, PDF, MSOffice, Archives, Java, Flash, DLLs, Media, etc.

Commercial

Sky ATP follows a 'FREEMIUM' pricing model

	FREE	PREMIUM
Licensing	No license reqd. Available to all customers with a valid support contract.	1 YR, 3YR,5YR subscription license
File Types	Executables only	All supported file types
Feeds	Infected Host (Sky ATP generated)	C&C, GeoIP, Infected Host

JUNIPER NETWORKS CONFIDENTIAL



LICENSING

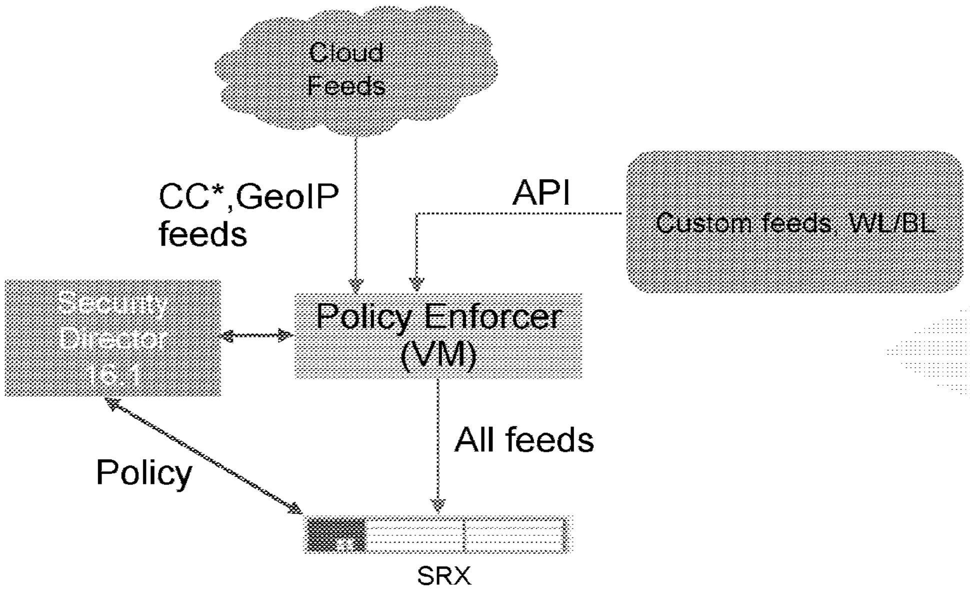
Licensing Model

- Sky ATP offers a “Freemium” model i.e. limited features for ‘FREE’, charge for other features
- 1YR,3YR and 5YR software subscription SKUs

FREE	BASIC	PREMIUM
• Available on any SRX – valid support contract reqd. • Processes executable file type only • No threat feeds	• Threat Feeds (CC, GeoIP, custom) included • Limited APIs • No anti-malware protection (executables are processed)	• Full anti-malware protection – all supported file types • Threat Feeds included • All APIs included • Infected host feed included

Spotlight Secure transition

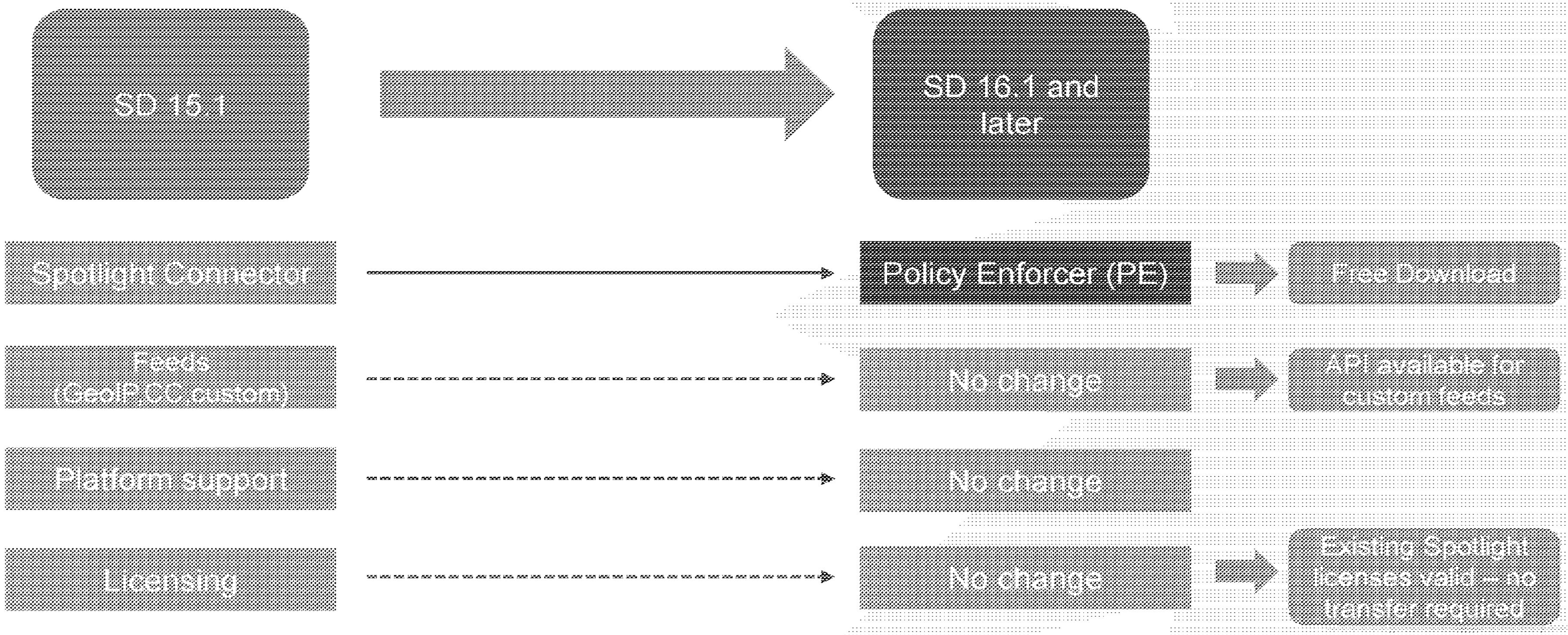
Spotlight Secure – Security Director 16.1



- ✓ Policy Enforcer is a new component effectively behaving as a 'connector'
- ✓ Non-SDSN mode sufficient for feeds

*CC = Command and Control

Transition components



SD 15.1

SD 16.1 and later

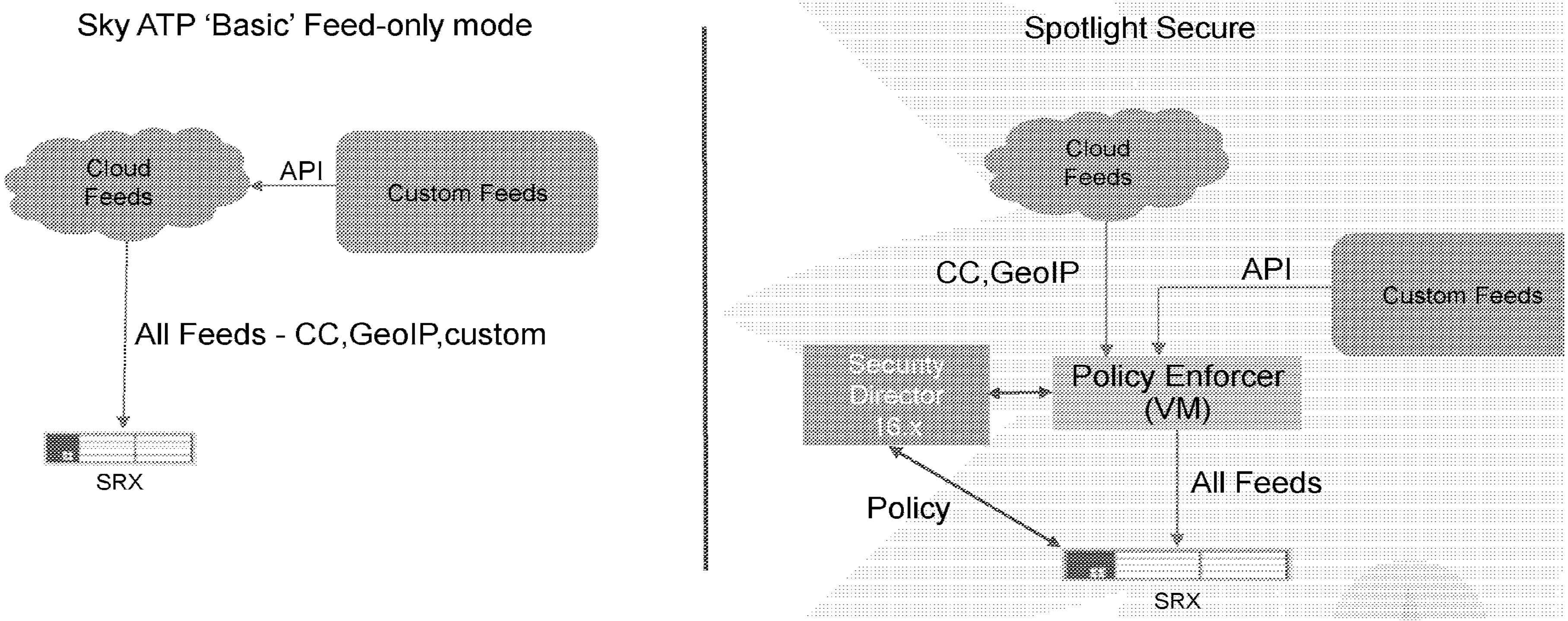
Spotlight Connector → Policy Enforcer (PE) → Free Download

Feeds (GeoIP,CC,custom) → No change → API available for custom feeds

Platform support → No change

Licensing → No change → Existing Spotlight licenses valid – no transfer required

Threat Feeds deployment models



Sky ATP ‘Basic’ Feed-only mode

Cloud Feeds

API

Custom Feeds

All Feeds - CC,GeoIP,custom

SRX

Spotlight Secure

Cloud Feeds

CC,GeoIP

API

Custom Feeds

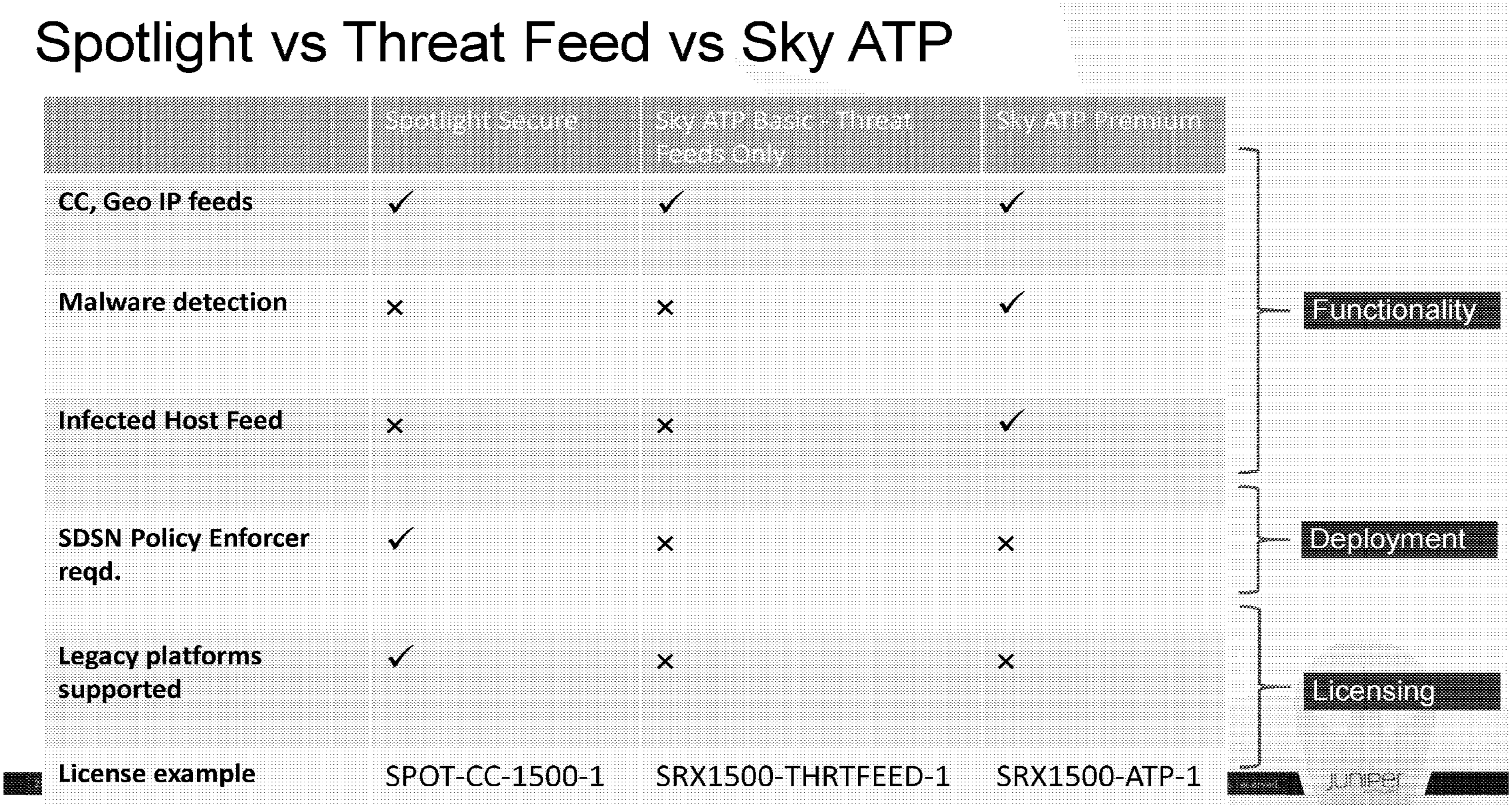
Security Director 16.x

Policy Enforcer (VM)

Policy

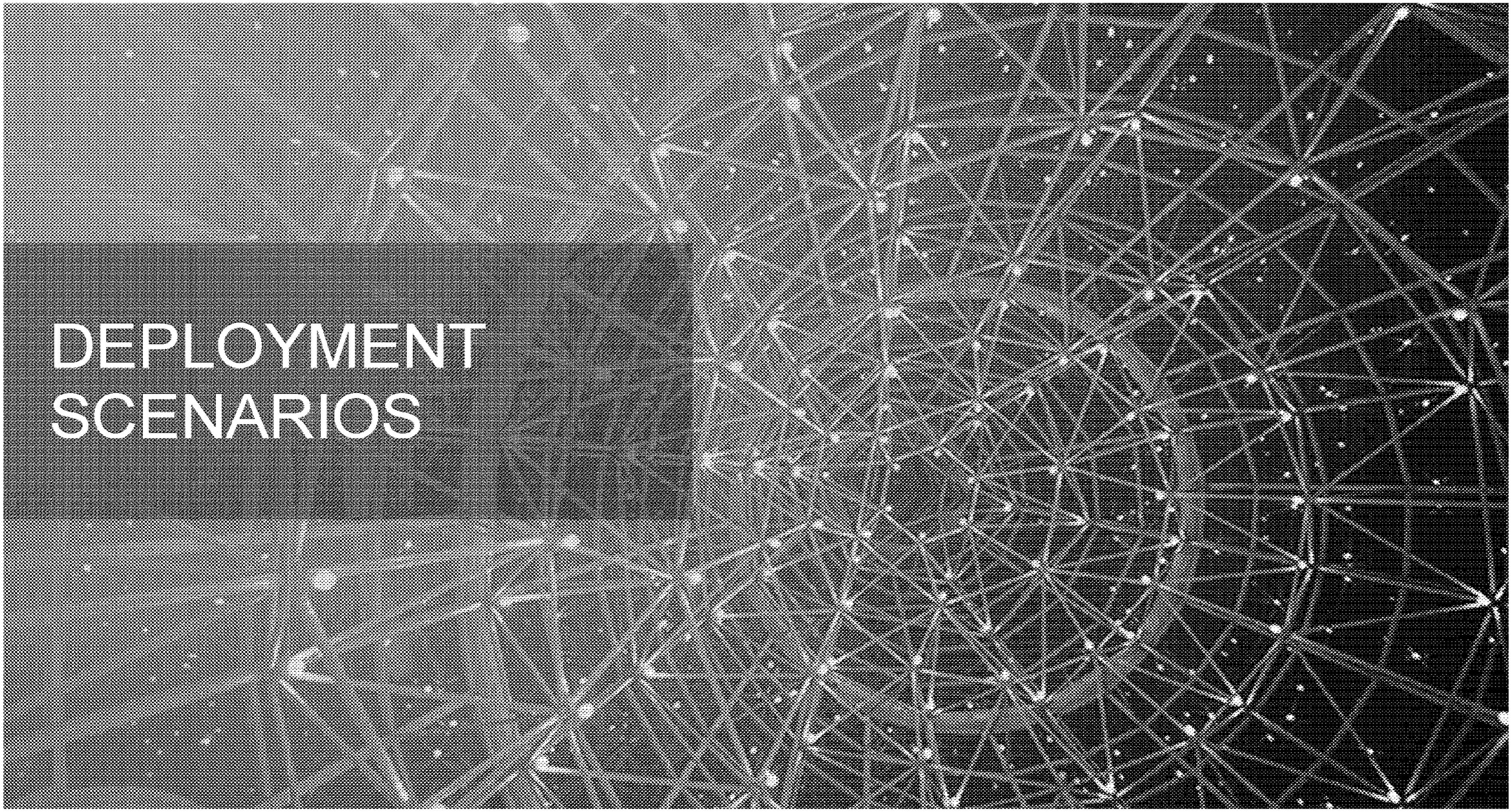
All Feeds

SRX



Spotlight vs Threat Feed vs Sky ATP

	Spotlight Secure	Sky ATP Basic - Threat Feeds Only	Sky ATP Premium	
CC, Geo IP feeds	✓	✓	✓	Functionality
Malware detection	×	×	✓	
Infected Host Feed	×	×	✓	
SDSN Policy Enforcer reqd.	✓	×	×	Deployment
Legacy platforms supported	✓	×	×	Licensing
License example	SPOT-CC-1500-1	SRX1500-THRTFEED-1	SRX1500-ATP-1	



DEPLOYMENT SCENARIOS

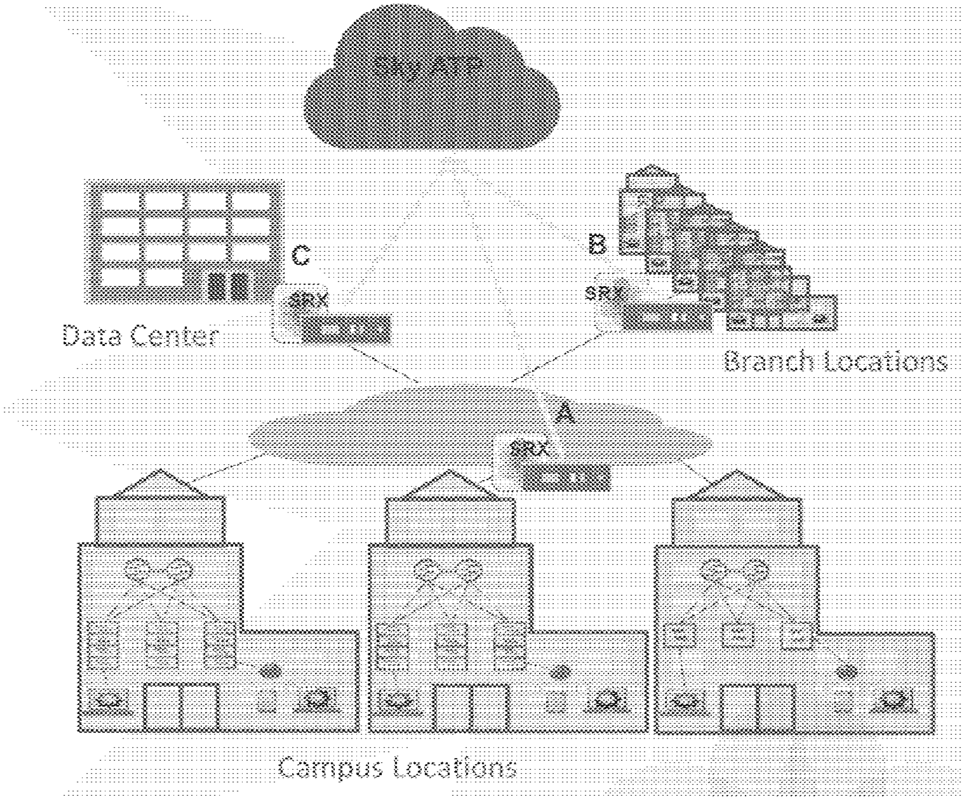
PLACES IN THE NETWORK

Use cases across the deployment spectrum of SRX

A. **Campus Edge Firewall**
- **Protection of end user devices from files downloaded from the Internet**

B. **Branch Router**
- **Protection for split-tunnel deployments**

C. **Data Center Edge**
- **Application protection from infected files**



FedRAMP:Sky ATP Cloud for US Federal/DoD

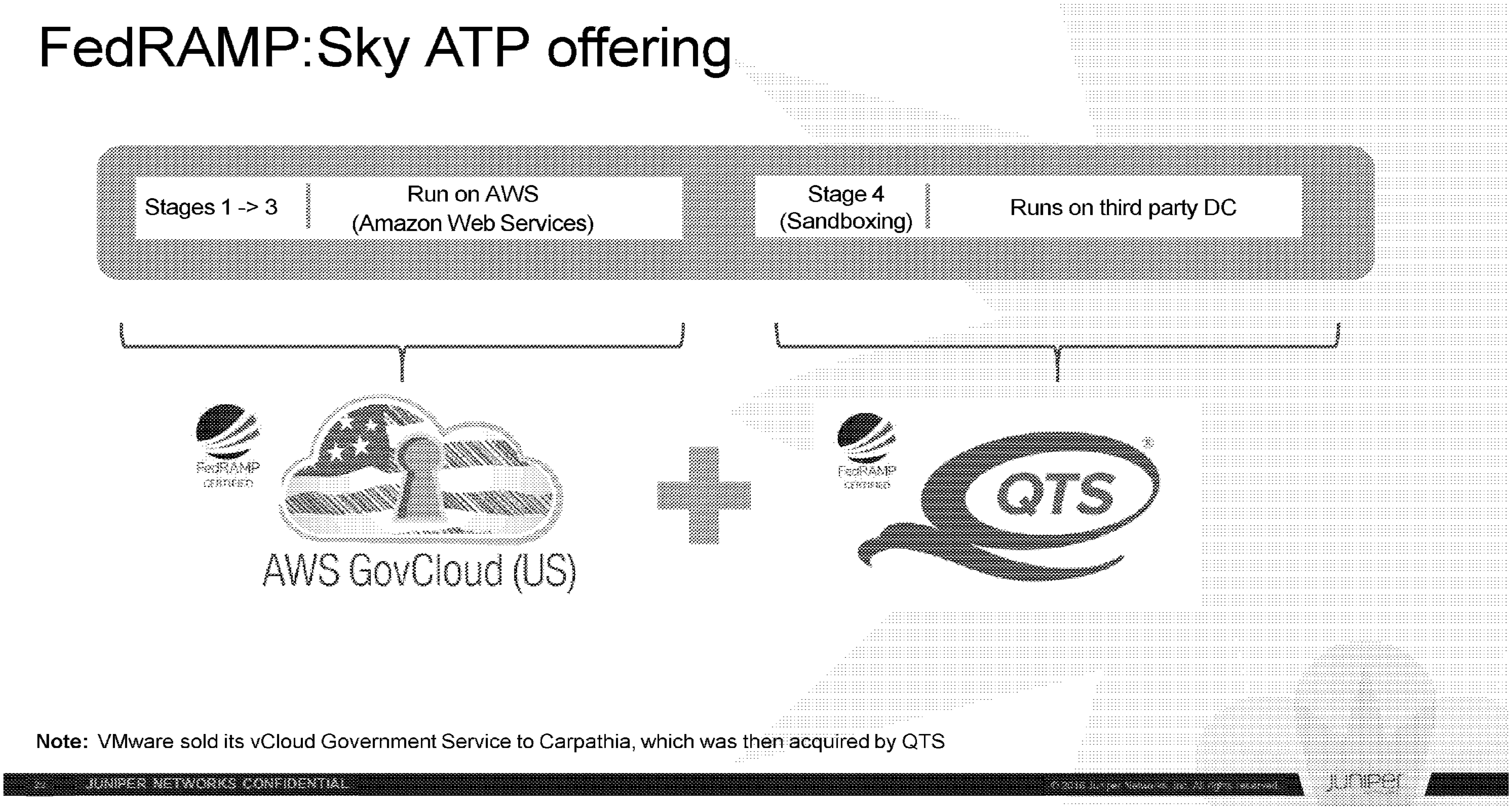
❑ FedRAMP = Federal Risk and Authorization Management Program

❑ Applicable to Cloud based services – part of the “Cloud-first” initiative announced in Dec. 2010

❑ CSPs undergo an extensive certification process to become FedRAMP certified: One of the most in-depth compliance exercise any organization can attempt

❑ Prior to FedRAMP, every Federal agency conducted its own risk assessment service for every procured Cloud service: resulted in redundancy

❑ CSPs that complete a FedRAMP assessment obtain an ATO (Authority to Operate) i.e. becomes eligible for procurement by Federal agency

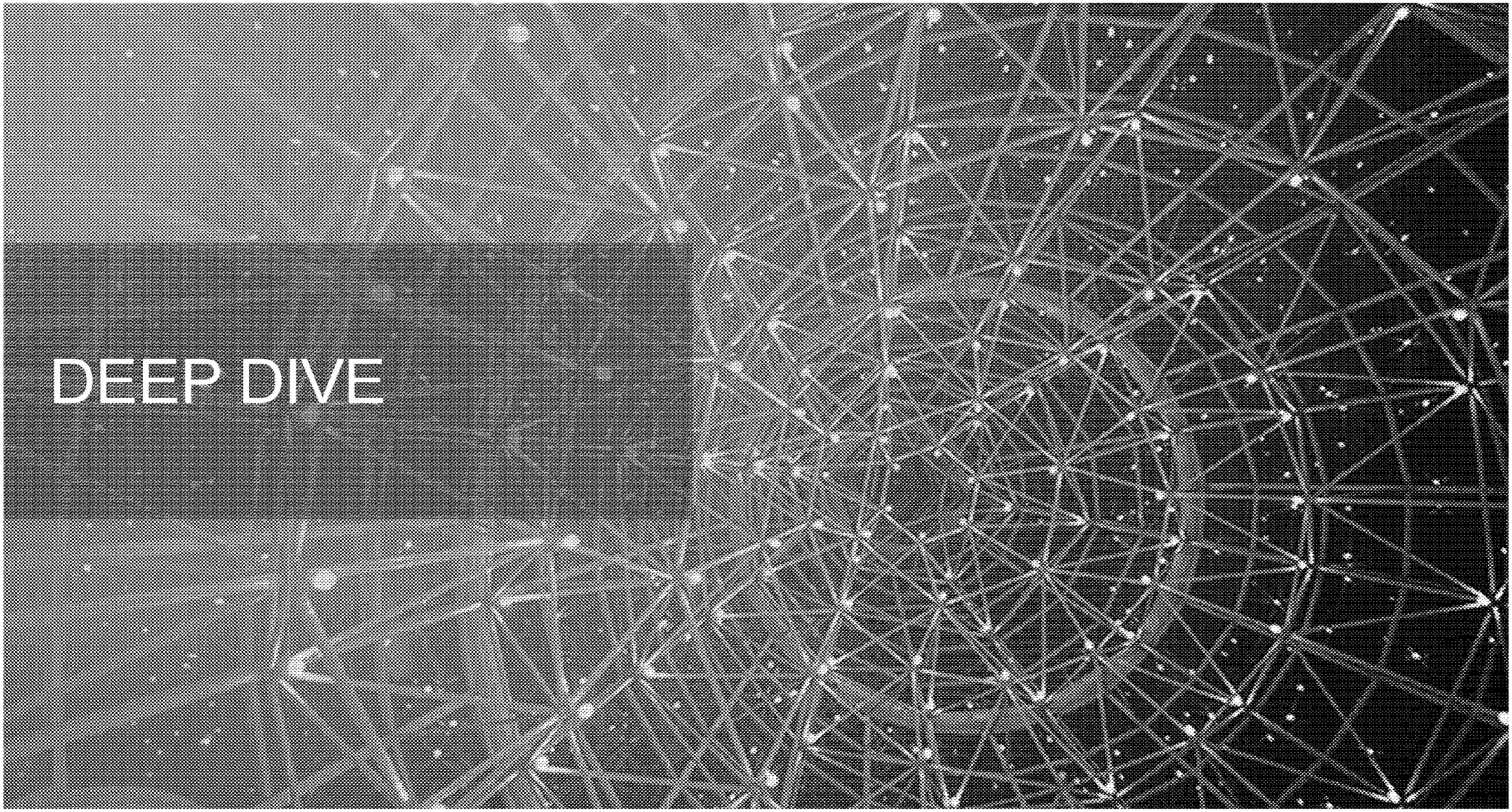


FedRAMP:Sky ATP offering

Stages 1 -> 3	Run on AWS (Amazon Web Services)	Stage 4 (Sandboxing)	Runs on third party DC

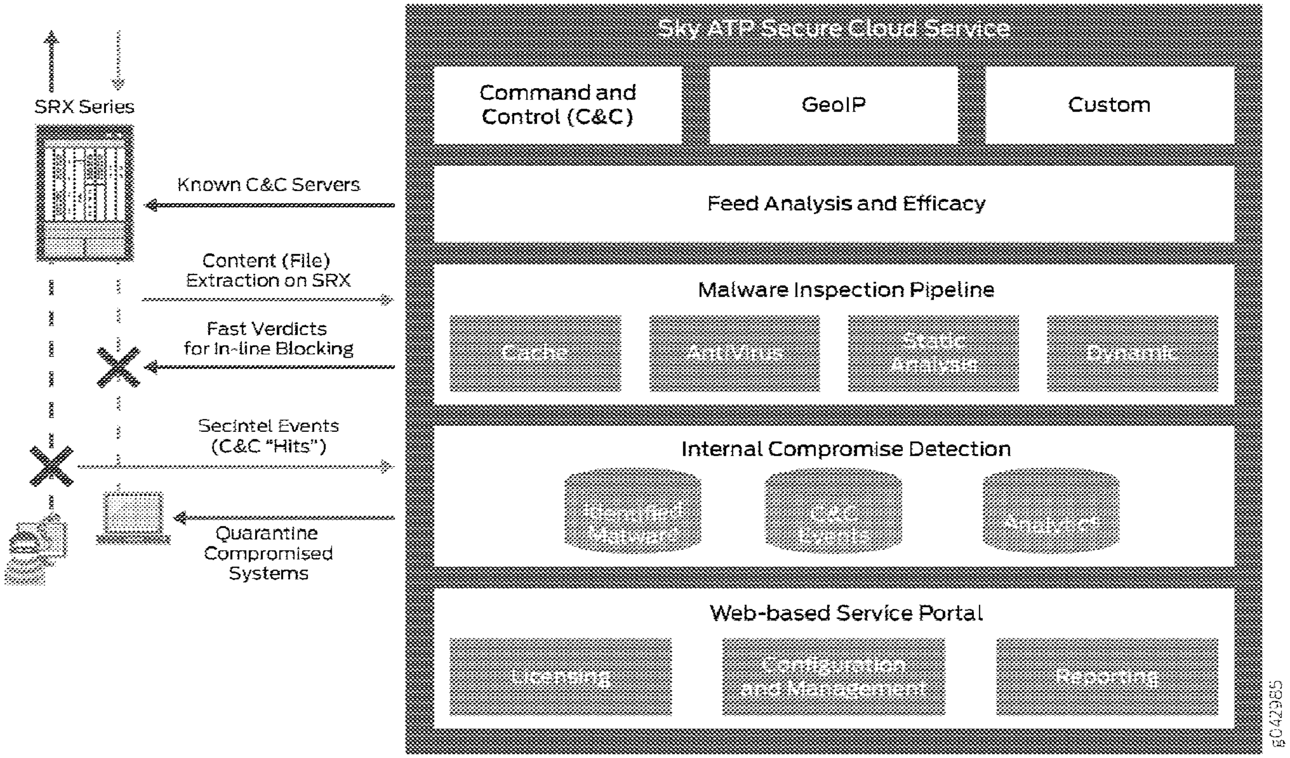
FedRAMP
CERTIFIED
AWS GovCloud (US)
FedRAMP
CERTIFIED
QTS

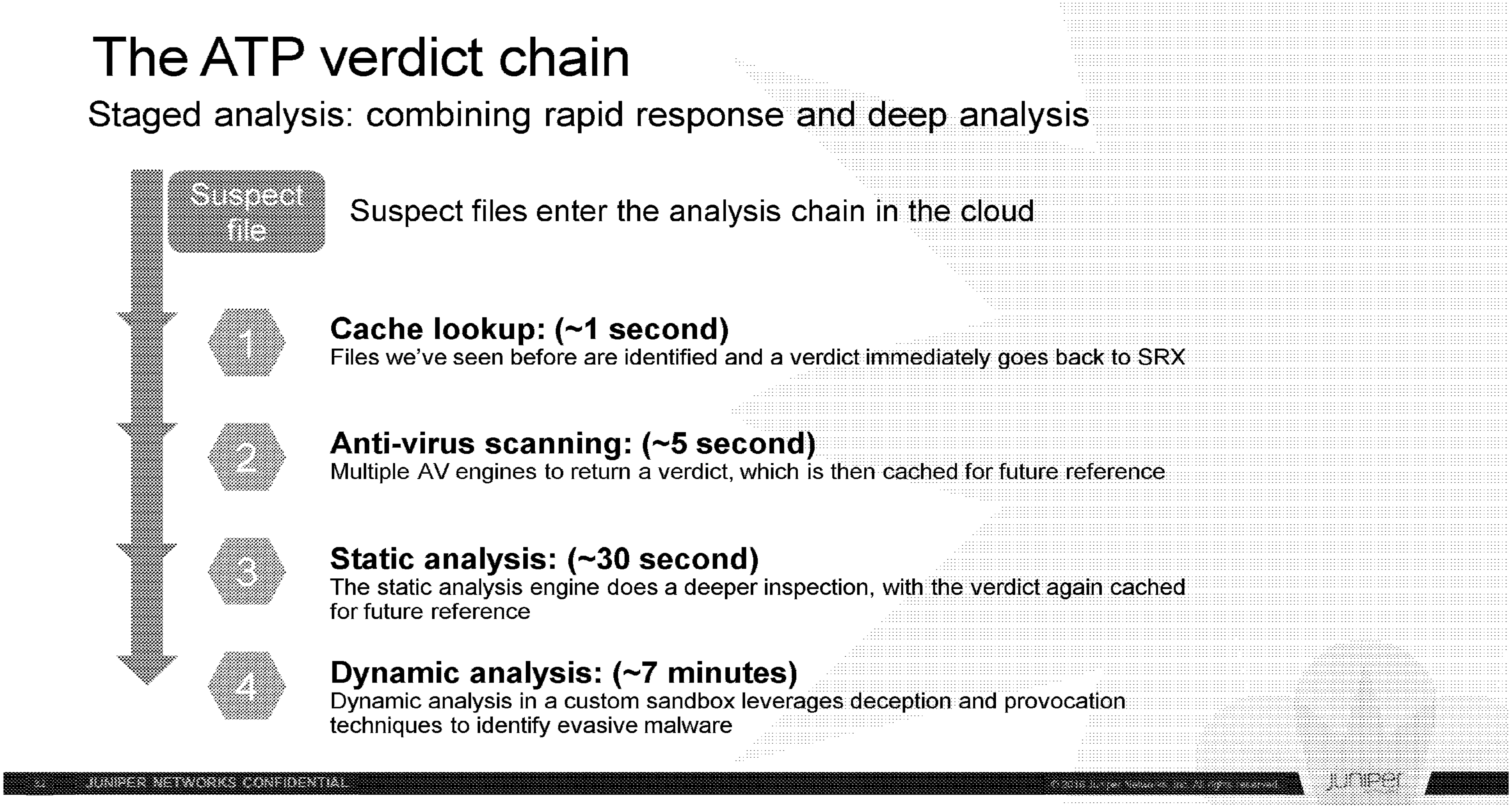
Note: VMware sold its vCloud Government Service to Carpathia, which was then acquired by QTS



DEEP DIVE

Sky ATP architecture





The ATP verdict chain

Staged analysis: combining rapid response and deep analysis

Suspect file

Suspect files enter the analysis chain in the cloud

1

Cache lookup: (~1 second)
Files we've seen before are identified and a verdict immediately goes back to SRX

2

Anti-virus scanning: (~5 second)
Multiple AV engines to return a verdict, which is then cached for future reference

3

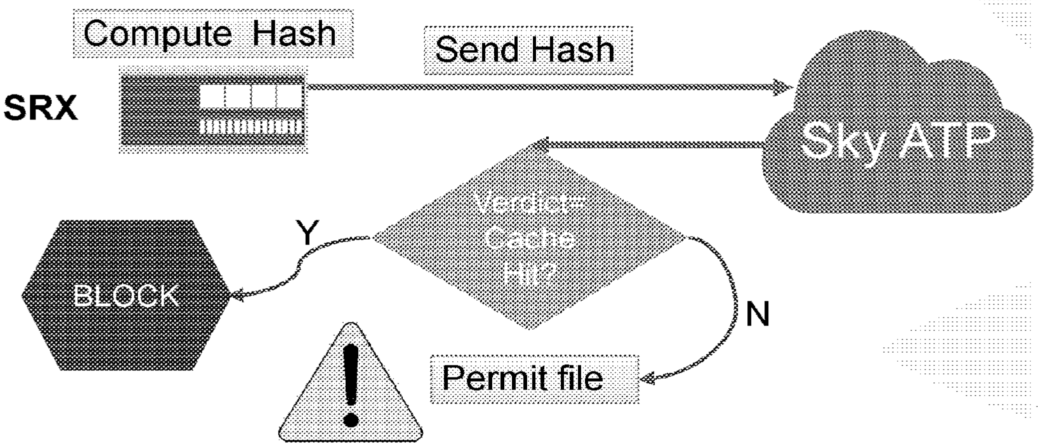
Static analysis: (~30 second)
The static analysis engine does a deeper inspection, with the verdict again cached for future reference

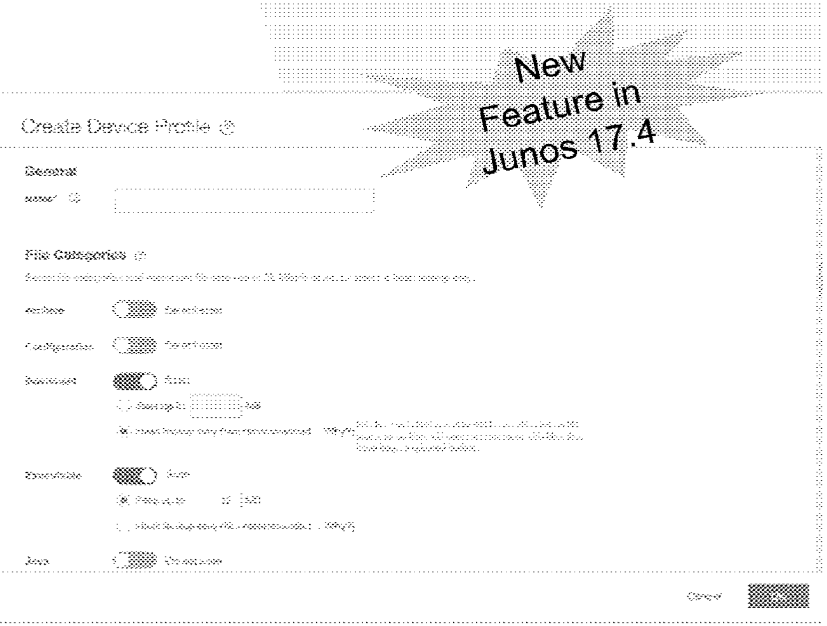
4

Dynamic analysis: (~7 minutes)
Dynamic analysis in a custom sandbox leverages deception and provocation techniques to identify evasive malware

JUNIPER NETWORKS CONFIDENTIAL

Private (hash only) mode

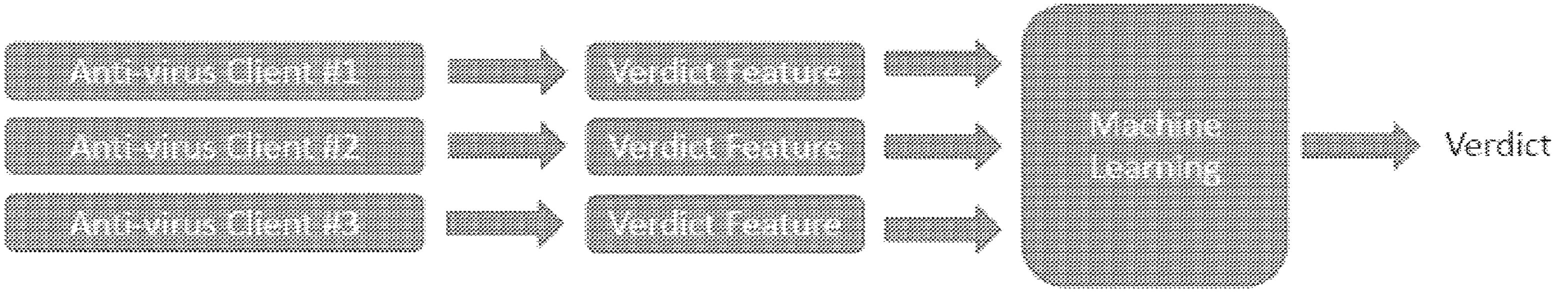




- Mitigate privacy concerns – protection level tradeoff. Position in RFPs
- No cache store/lookup on SRX – being evaluated
- Configurable by File Category
- HTTP 206 (Partial-Content) not supported – SRX cannot use disk to store file segments

Anti-Virus: First Pass

- Overcoming False Positives (FP) and False Negatives (FN)
  - Use multiple AV engines
  - Combine with Machine Learning



Anti-virus Client #1

Anti-virus Client #2

Anti-virus Client #3

Verdict Feature

Verdict Feature

Verdict Feature

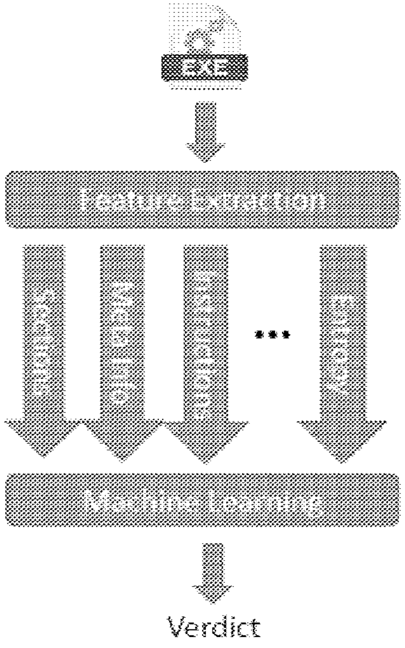
Machine Learning

Verdict

Static Analysis: Pulling apart the code

- Break file down into features
  - File structure
  - Meta info (file name, vendor, etc...)
  - Categories of instructions used
  - File entropy
  - Etc...
- Feed features into machine learning algo
  - First teach it what malware looks like
  - Then ask if something is malware

Static analysis is traditionally done with rules. Argon extends this by adding machine learning to improve verdict accuracy.

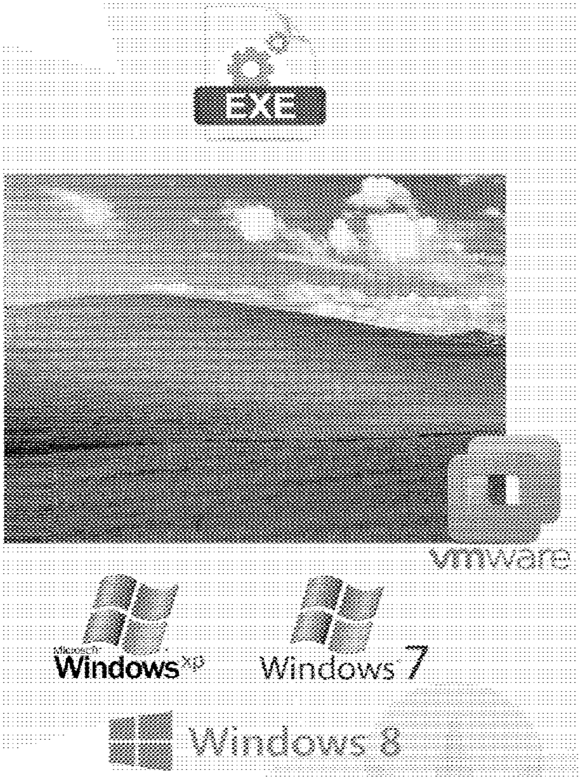


Dynamic Analysis: Sandboxing

Inside a custom Sandbox environment

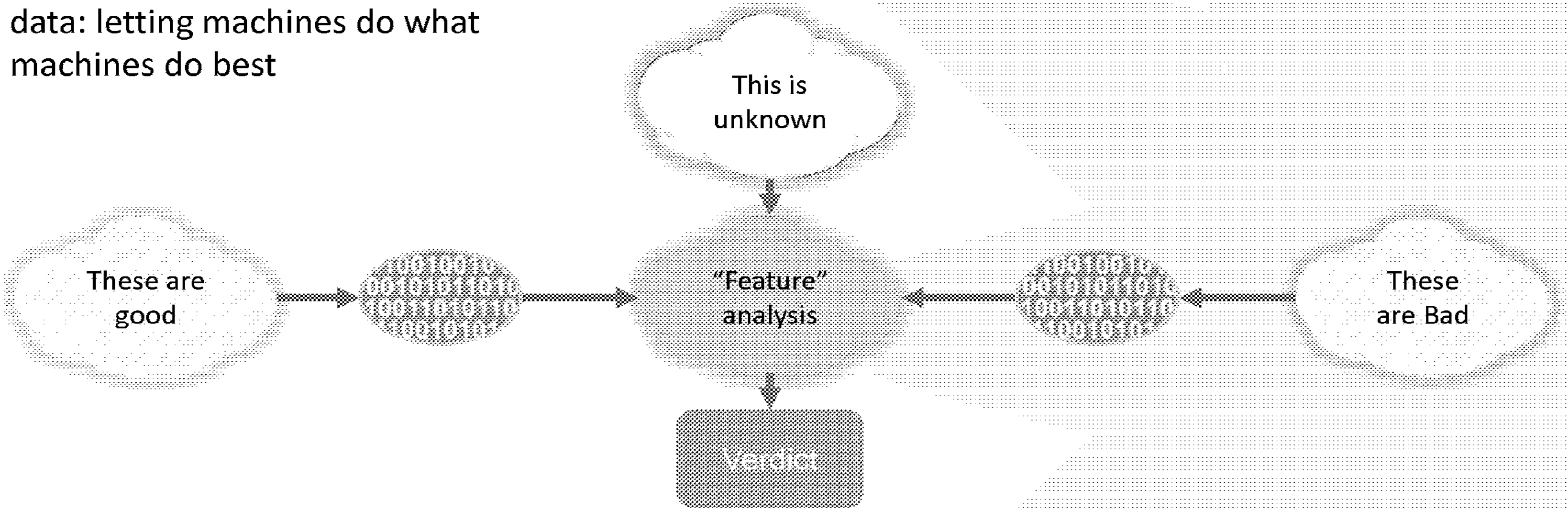
- Spool up a live desktop
- Hook into the OS to record everything
- Upload and execute the suspect file
- Apply Sky's Deception and Provocation Techniques
  - *The full run takes approximately 7 minutes*
- Download the activity recording for analysis
- Tear down the live desktop
- Generate a verdict with Machine Learning

Today: *Windows 7,Android*
Future: Windows 10, OSX,*other.*



Machine Learning

Digging through massive piles of data: letting machines do what machines do best



The final verdict is based on how much a new example resembles the known good or bad samples. By comparing many features across large data sets, we can deliver very accurate results.

Speaker Notes for Slide 33

Deception and Provocation

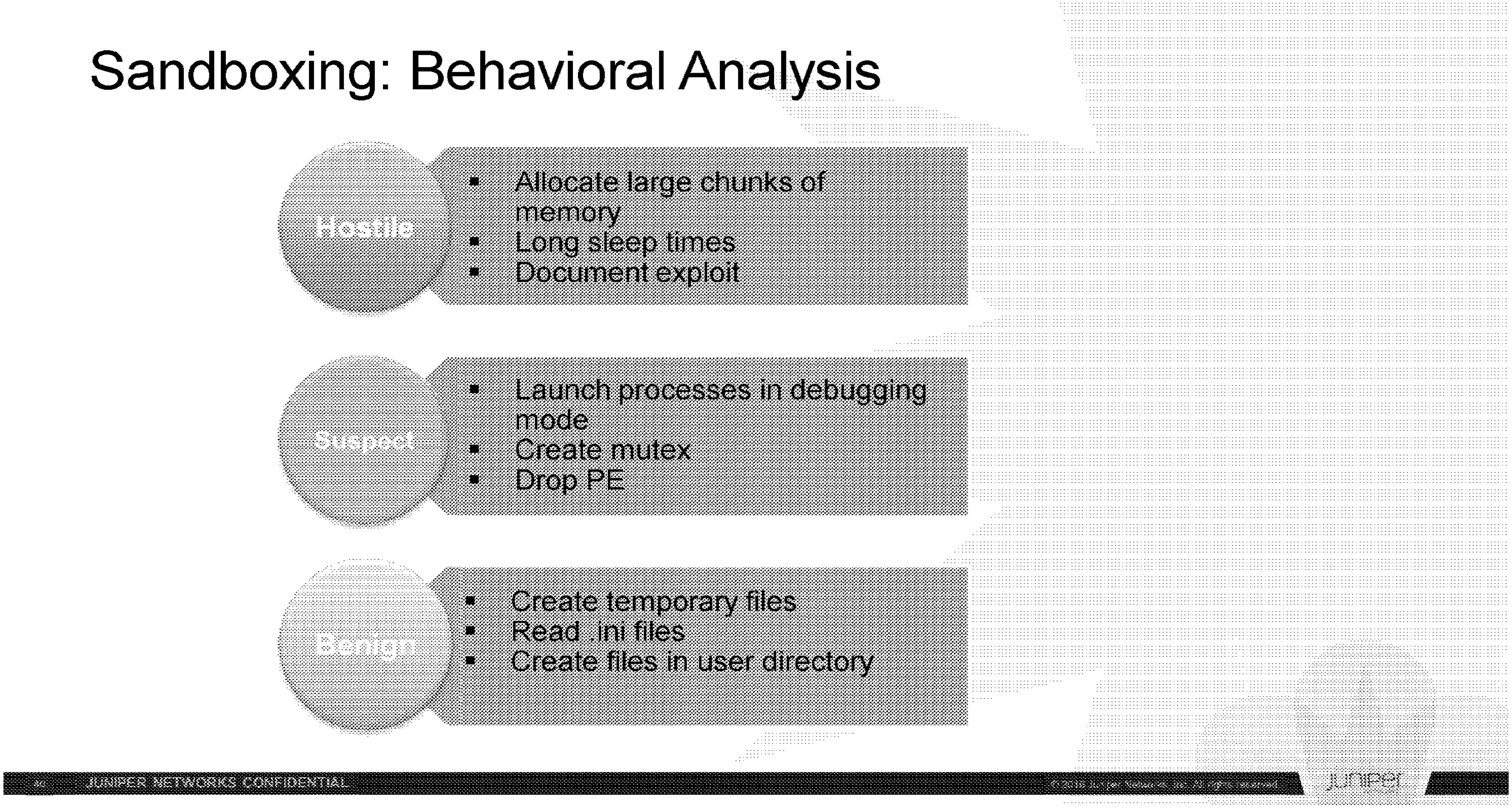
Provocation

Provoking Malware.

- Attach debuggers
- Run malware multiple times
- Actively interfere with malware operations
- Actively interfere with network communications

Juniper's Sky Advanced Threat Prevention looks for over 300 different malware behaviors and includes over 50 different deception techniques to provoke malware into revealing itself.

Deception: Convince it it's on a valid target to get a reaction
Provocation: Poke it with a stick and see how it reacts



Sandboxing: Behavioral Analysis

Hostile

- Allocate large chunks of memory
- Long sleep times
- Document exploit

Suspect

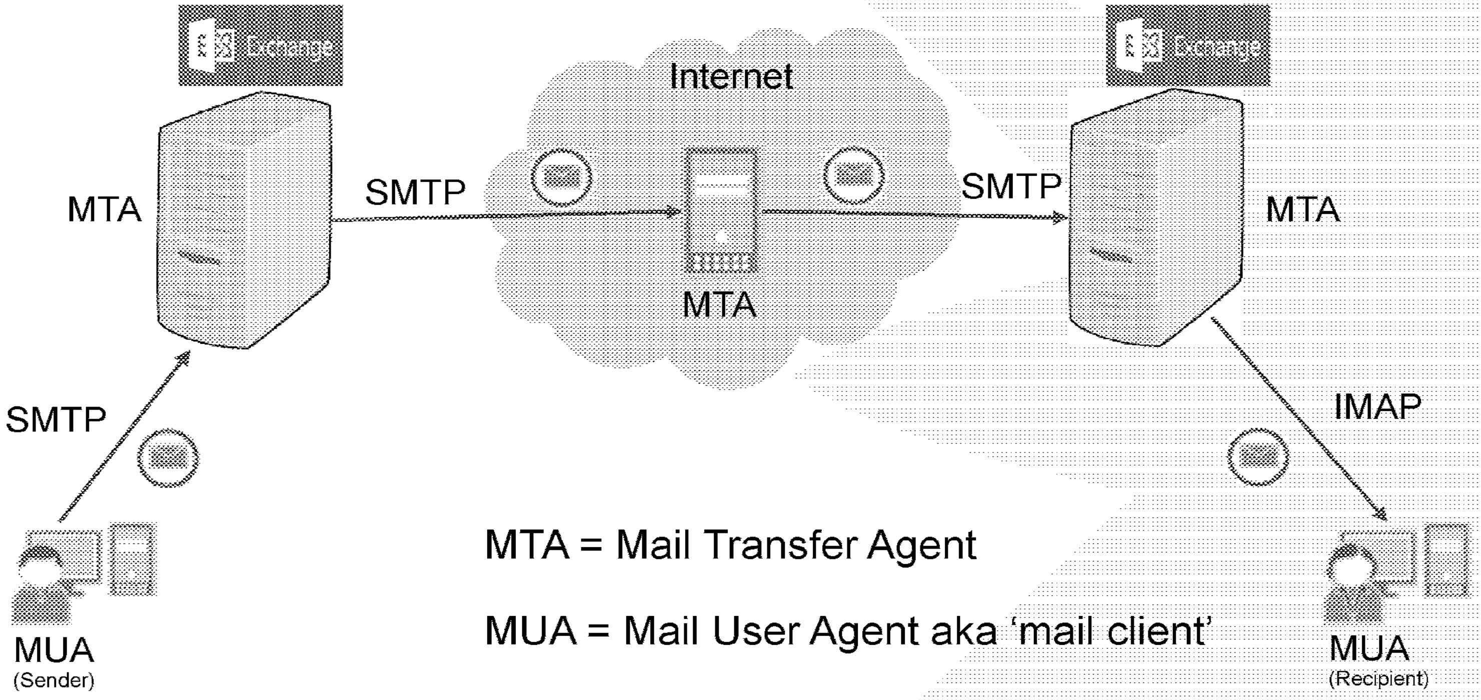
- Launch processes in debugging mode
- Create mutex
- Drop PE

Benign

- Create temporary files
- Read .ini files
- Create files in user directory

30 JUNIPER NETWORKS CONFIDENTIAL

Email – how it comes together

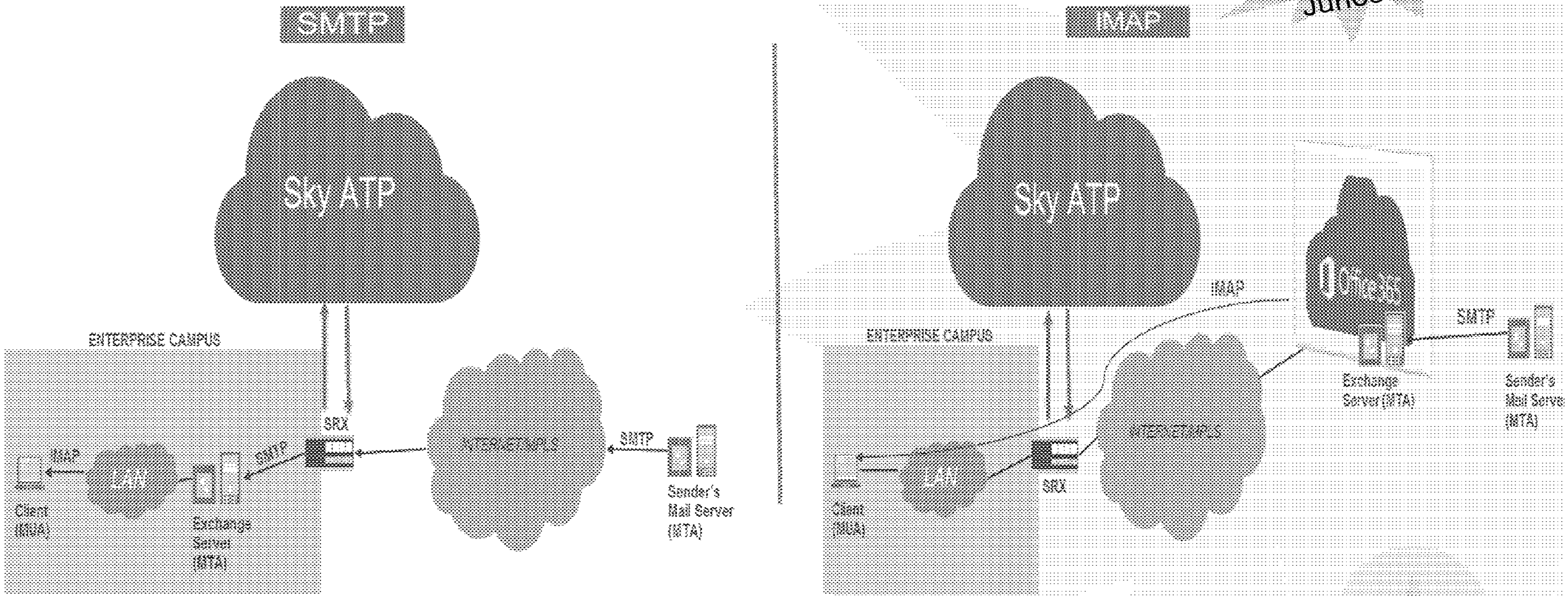


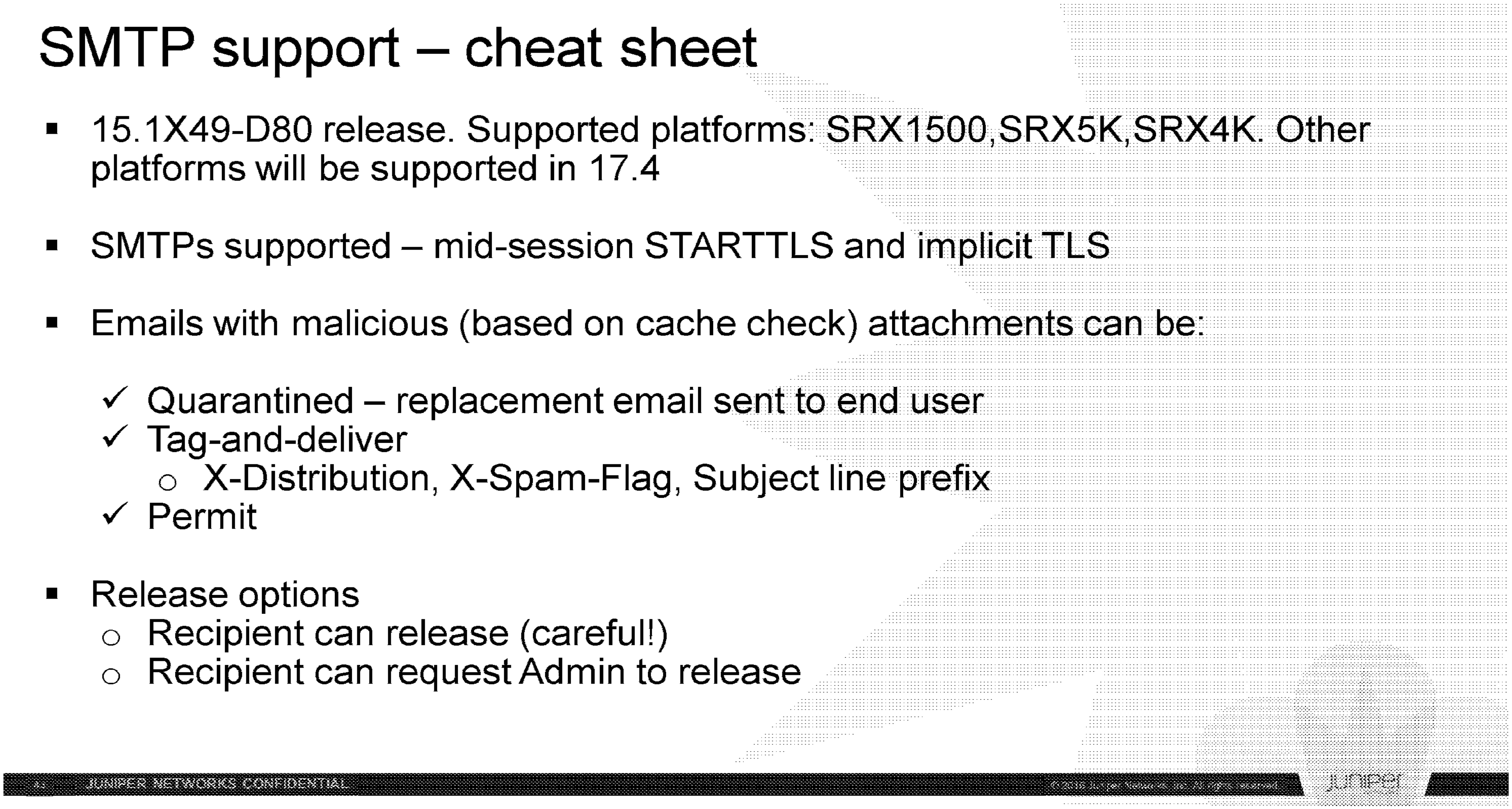
MTA = Mail Transfer Agent

MUA = Mail User Agent aka ‘mail client’

So what does this mean for Sky ATP?

New Feature in Junos 17.4

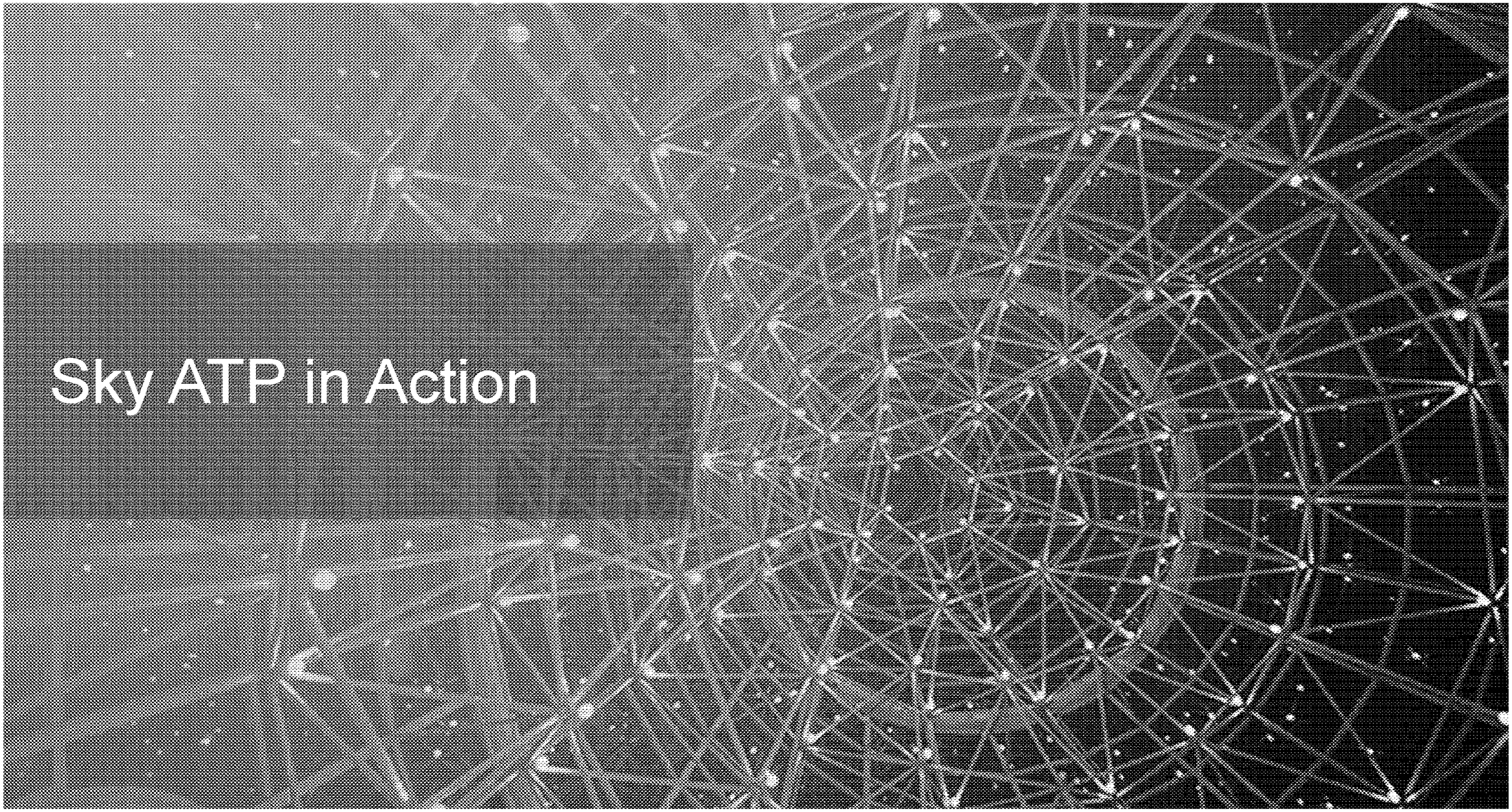




SMTP support – cheat sheet

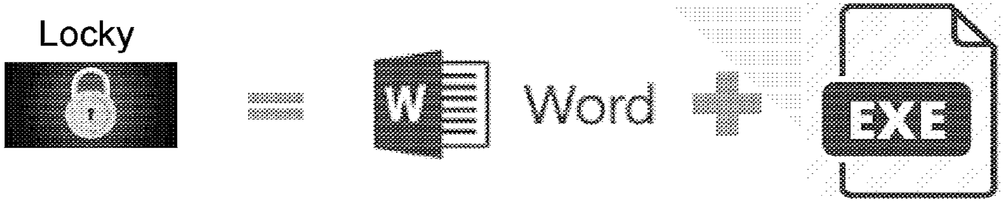
- 15.1X49-D80 release. Supported platforms: SRX1500,SRX5K,SRX4K. Other platforms will be supported in 17.4
- SMTPs supported – mid-session STARTTLS and implicit TLS
- Emails with malicious (based on cache check) attachments can be:
  - ✓ Quarantined – replacement email sent to end user
  - ✓ Tag-and-deliver
    - ○ X-Distribution, X-Spam-Flag, Subject line prefix
  - ✓ Permit
- Release options
  - ○ Recipient can release (careful!)
  - ○ Recipient can request Admin to release

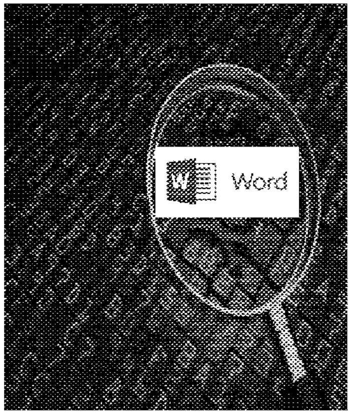
JUNIPER NETWORKS CONFIDENTIAL



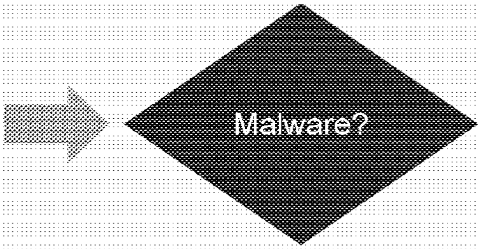
Sky ATP in Action

Sky ATP in Action: Detecting Locky

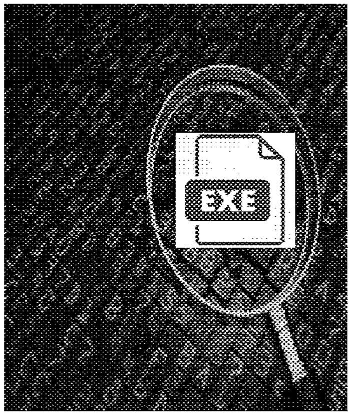




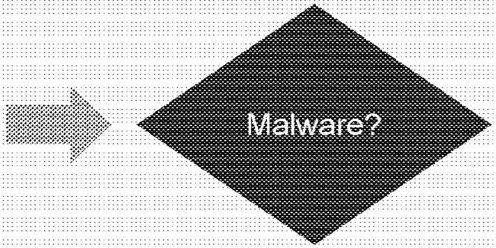
Traits seen in 'Locky'	Good documents	Malicious documents
Document has macros	0.9%	84.4%
No title	6.6%	50.2%
Single paragraph document	7.5%	45.3%
Obfuscation function calls found	< 0.1%	39.6%
Code Page 1251 Windows Cyrillic (Slavic)	varies	27.6%



Sky ATP in Action: Detecting Locky

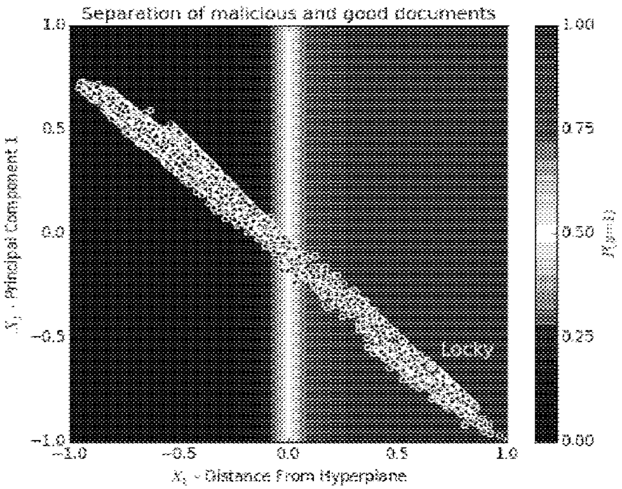


Trait	Good applications	Malware
Accesses hosts file	21.8%	49.5%
DNS resolution	27.4%	50.4%
Excessive sleep calls	43.6%	67.1%
DNS resolution of many domain names with many failures	0.2%	12.2%
Generates new code (typically unpacking or expanding shellcode)	2.4%	9.7%
Posts data to a webserver	1.7%	3.9%
Creates PE files with a name already existing in Windows	< 0.1%	1.9%
System process connects to network	0.2%	1.1%



Sky ATP in Action: Detecting Locky

File	Features Examined
Locky Word Document	~216,000
Locky Executable	~20,000,000



Sky ATP in Action: WannaCry

The origins

Exploits Windows SMB (Server Message Block) vulnerability

Vulnerability originally discovered by NSA and codenamed ‘Eternal Blue’

NSA did not inform Microsoft (why bother right?) but was made public by Shadow Brokers dump leaking classified NSA tool kit

Following leak by Shadow Brokers, Microsoft issued patch (MS17-010) but patch application takes months, sometimes years

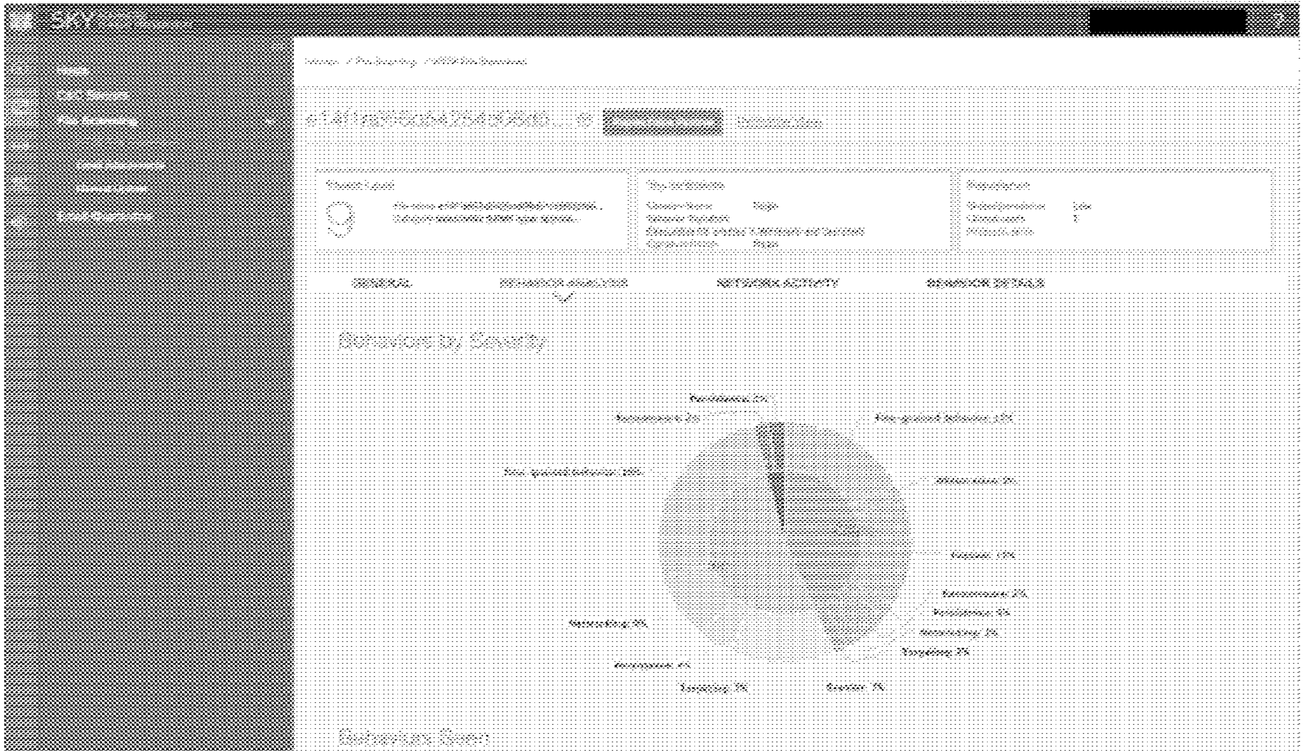
Threat vector

Possibly Email (phishing) or HTTP, not definitely known

Kill Switch

The malware starts by attempting to connect to: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Aborts if attempt succeeds.

Sky ATP in Action: WannaCry mitigation

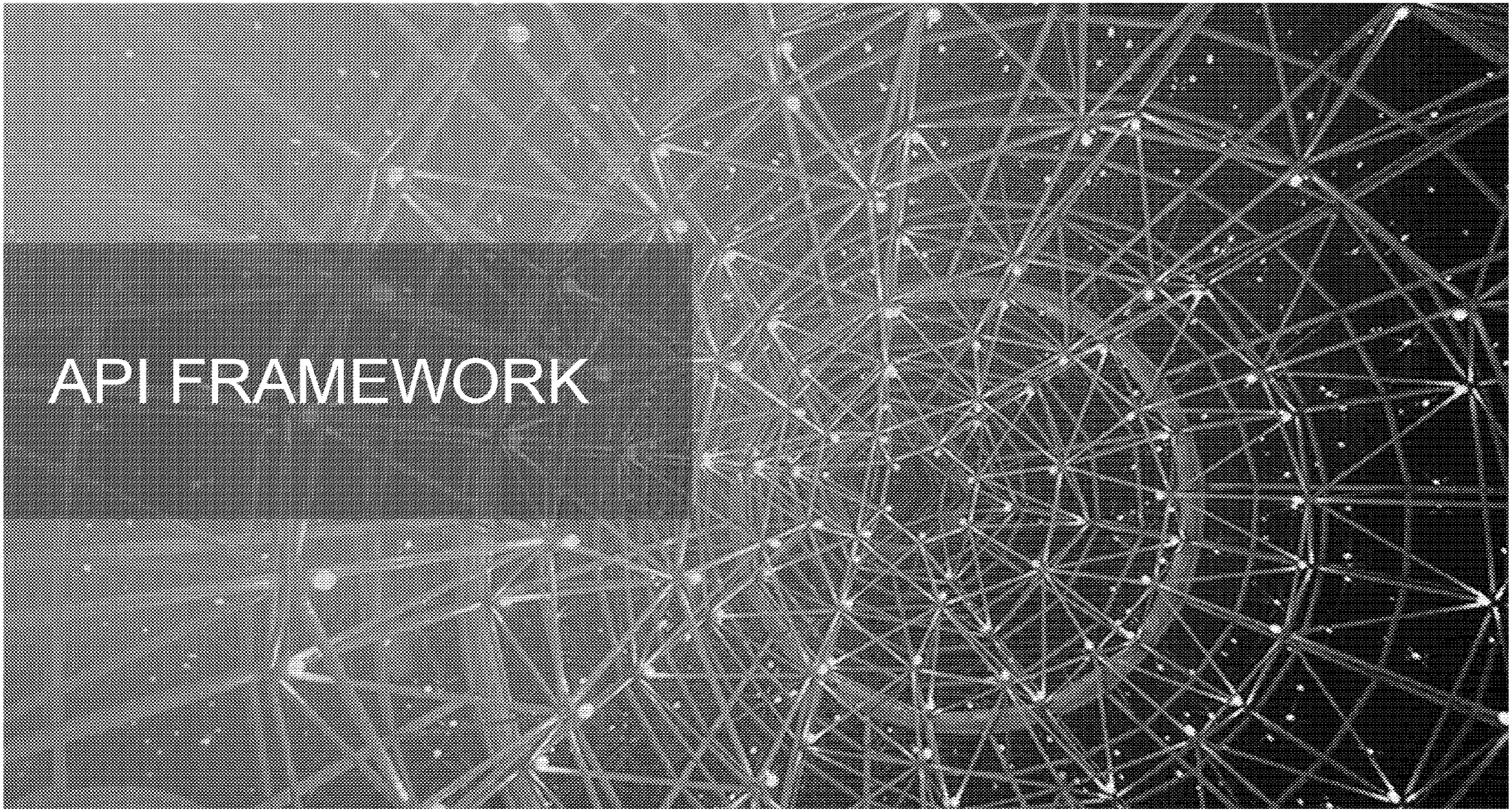


[redacted]

- 24 unique samples examined as of 5/12
- 30 seconds time to detection

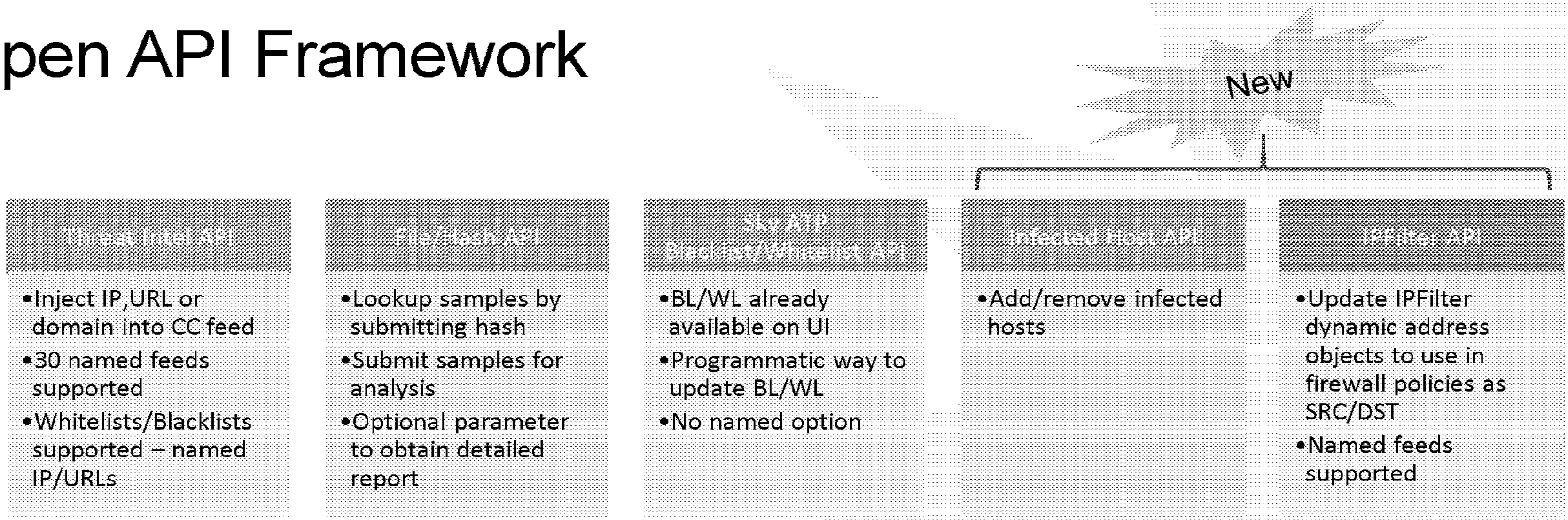
Sky ATP in Action: WannaCry mitigation

[redacted]



API FRAMEWORK

Open API Framework



Threat Intel API
- Inject IP,URL or domain into CC feed
- 30 named feeds supported
- Whitelists/Blacklists supported – named IP/URLs

File/Hash API
- Lookup samples by submitting hash
- Submit samples for analysis
- Optional parameter to obtain detailed report

Sky ATP Blacklist/Whitelist API
- BL/WL already available on UI
- Programmatic way to update BL/WL
- No named option

Infected Host API
- Add/remove infected hosts

IPFilter API
- Update IPFilter dynamic address objects to use in firewall policies as SRC/DST
- Named feeds supported

❑ RESTful API – standard methods include POST,PATCH,GET,DELETE

❑ Supports a Swagger API specification in JSON format. APIs conform to a standard called the OpenAPI Initiative. Programmers can interact with both APIs using auto-generated code

❑ Application token required to interact – generated per Sky ATP realm

Juniper Security Alliances

CASB

netskope

CipherCloud
Trust in the Cloud

Cloud App Security

- *Cloud App risk mgmt.*
- *Visibility & Control*
- *Cloud malware & threat protection*
- *Extend security policy*

Access Security

ForeScout

aruba
a Hewlett Packard Enterprise company

Access Security

- *Context-Based*
- *BYOD Onboarding*
- *Role-based Network Access Assignment*
- *NAC / Access Policy Enforcement*

Endpoint Security

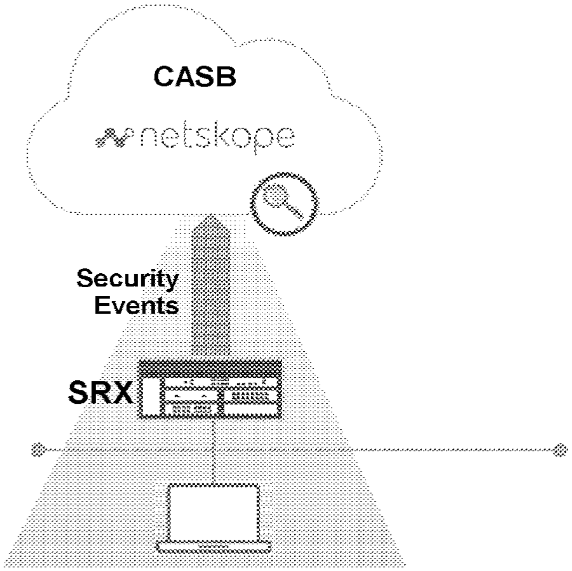
CARBON BLACK
ARM YOUR ENDPOINTS

Endpoint Protection

- *Continuous Policy Enforcement*
- *Discovery of all end-points*
- *Vulnerability and Patch management*

Ready to deploy comprehensive security solutions

Shadow IT Discovery



Customer Benefits

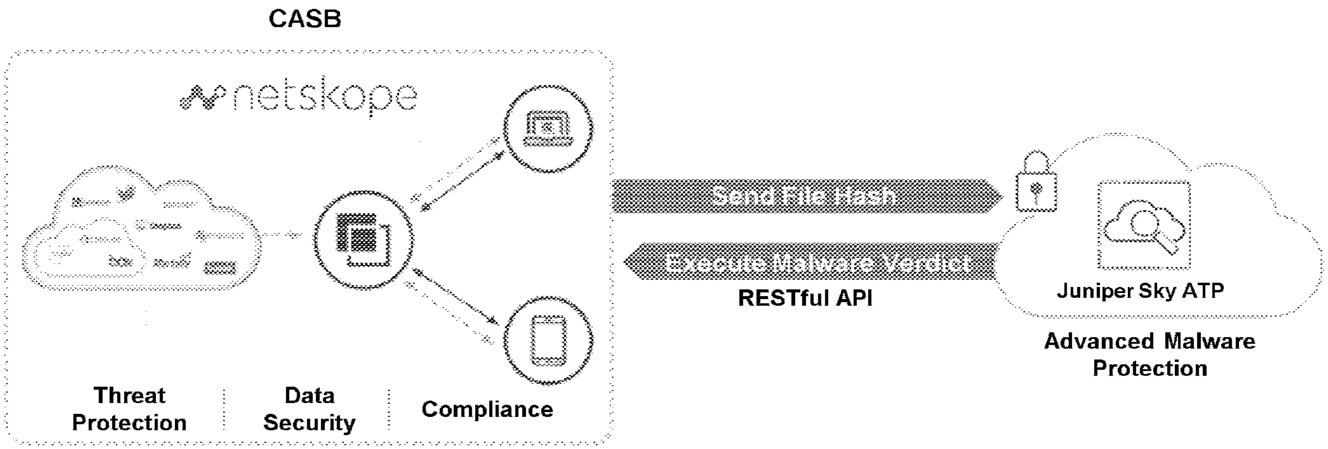
- Enterprise customers will have visibility to Cloud Applications
- Enterprise Policy can be extended to Cloud Applications

Use case

Available Now

- SRX Firewall sends syslog feed to Netskope Active Platform
- Netskope digests log information and provides visibility into Users, Applications and Compliance.

Advanced Threat Protection



Customer Benefits

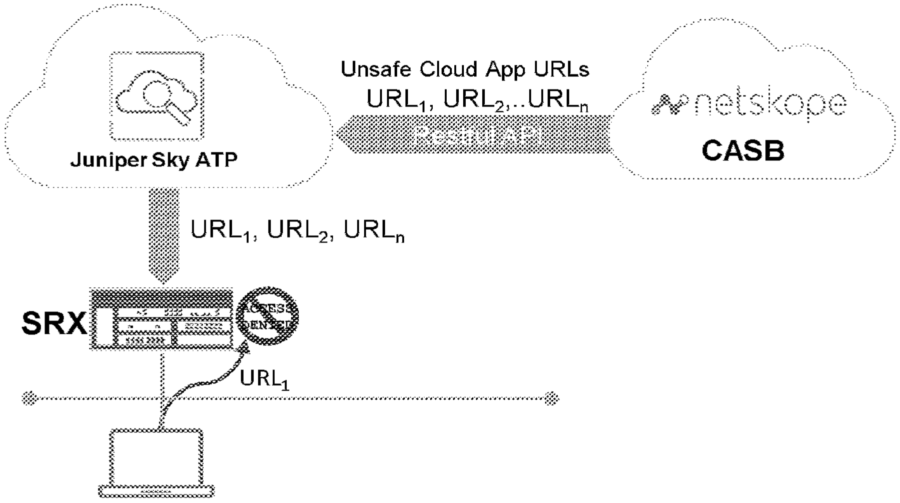
- Threat Protection extended to Cloud Apps
- Advanced Malware protection via Sky ATP
- Data Security extended to Cloud Apps
- Enforce compliance on Cloud data

Use case

Available Now

- Netskope will send File Hash to Sky ATP for malware identification
- Sky ATP responds back to Netskope with appropriate verdict

Threat Intelligence Sharing



Customer Benefits

- Enhanced security through Cloud Threat intelligence sharing
- SRX becomes 'Cloud App Aware' and enforces policy control

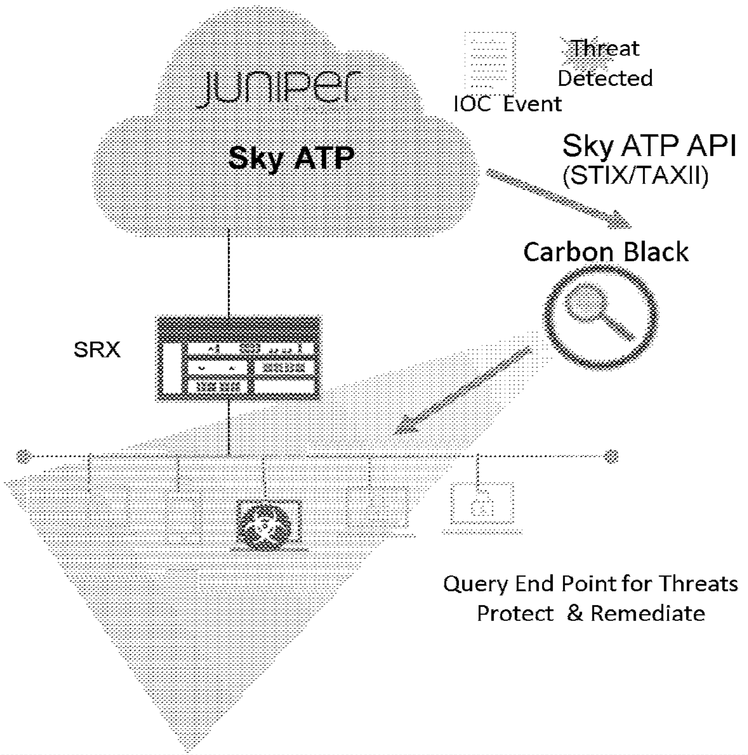
Use case

Available Now

- Netskope feeds URL verdicts to SRX
- SRX will block user access to destinations specified in URL feed

Threat Intel Sharing from SkyATP

THREAT INTEL: FROM SKY ATP To Cb



Use case workflow

Planning 4Q2017

- Sky ATP shares IOC with Cb Response
- Cb Response detects & reveals compromised endpoints network-wide
- Operator or auto remediate action taken on endpoint using Cb Response

Benefits

- Secures the network from vulnerabilities and risks from Malware and Compromised Hosts
- Offers a highly simplified, scalable solution for large deployments

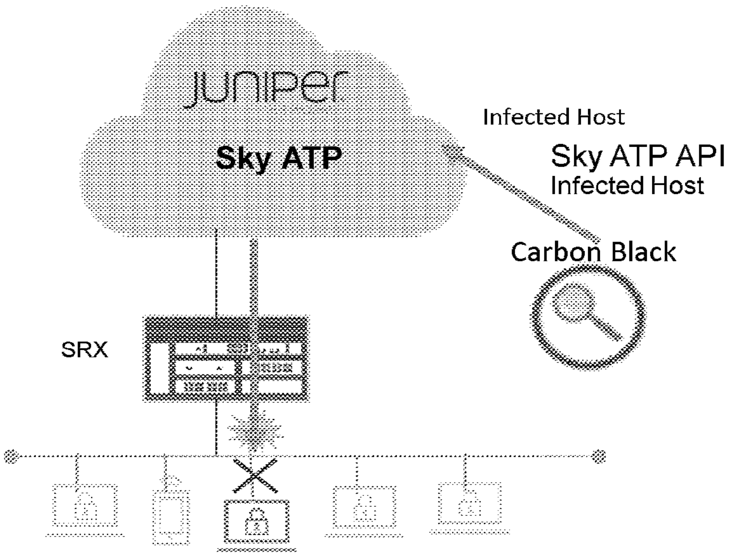
Speaker Notes for Slide 52

THREAT INTEL: FROM SKY ATP To Cb

10+ IOCs that include File Hash, File Name, IP address, malicious URLs & more
more
API

Infected Host Report from Endpoint

INFECTED HOST INTEL: FROM Cb TO SKY ATP



Use case workflow

Planning (3Q2017)

- Cb Response & Cb Defense observe malicious end point behavior, send Infected Host (IP address) to Sky ATP
- Sky ATP adds IP to Infected Host list and communicates to SRX
- SRX blocks traffic from Infected Host

Benefits

- Secures the network from vulnerabilities and risks from Compromised Hosts

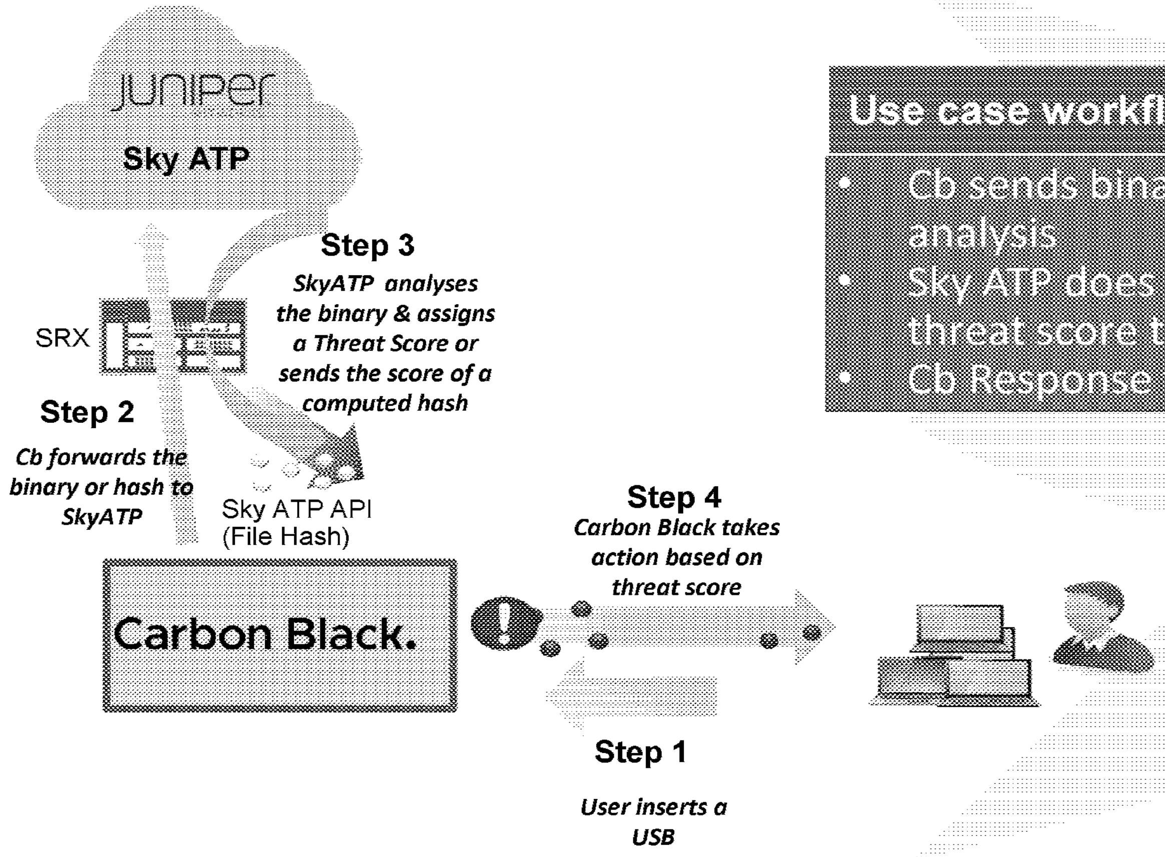
Speaker Notes for Slide 53

In this solution, we are receiving INFECTED HOST INTEL: FROM Cb TO SKY ATP

Note CB has near realtime capability of detecting infected end points.

We are using Sky ATP API (RESTFul API) for IH

Malware Detection & Remediation


Juniper
Sky ATP
SRX
Step 3
SkyATP analyses the binary & assigns a Threat Score or sends the score of a computed hash
Step 2
Cb forwards the binary or hash to SkyATP
Sky ATP API
(File Hash)
Carbon Black.
Step 4
Carbon Black takes action based on threat score
Step 1
User inserts a USB

Use case workflow

Planning Future

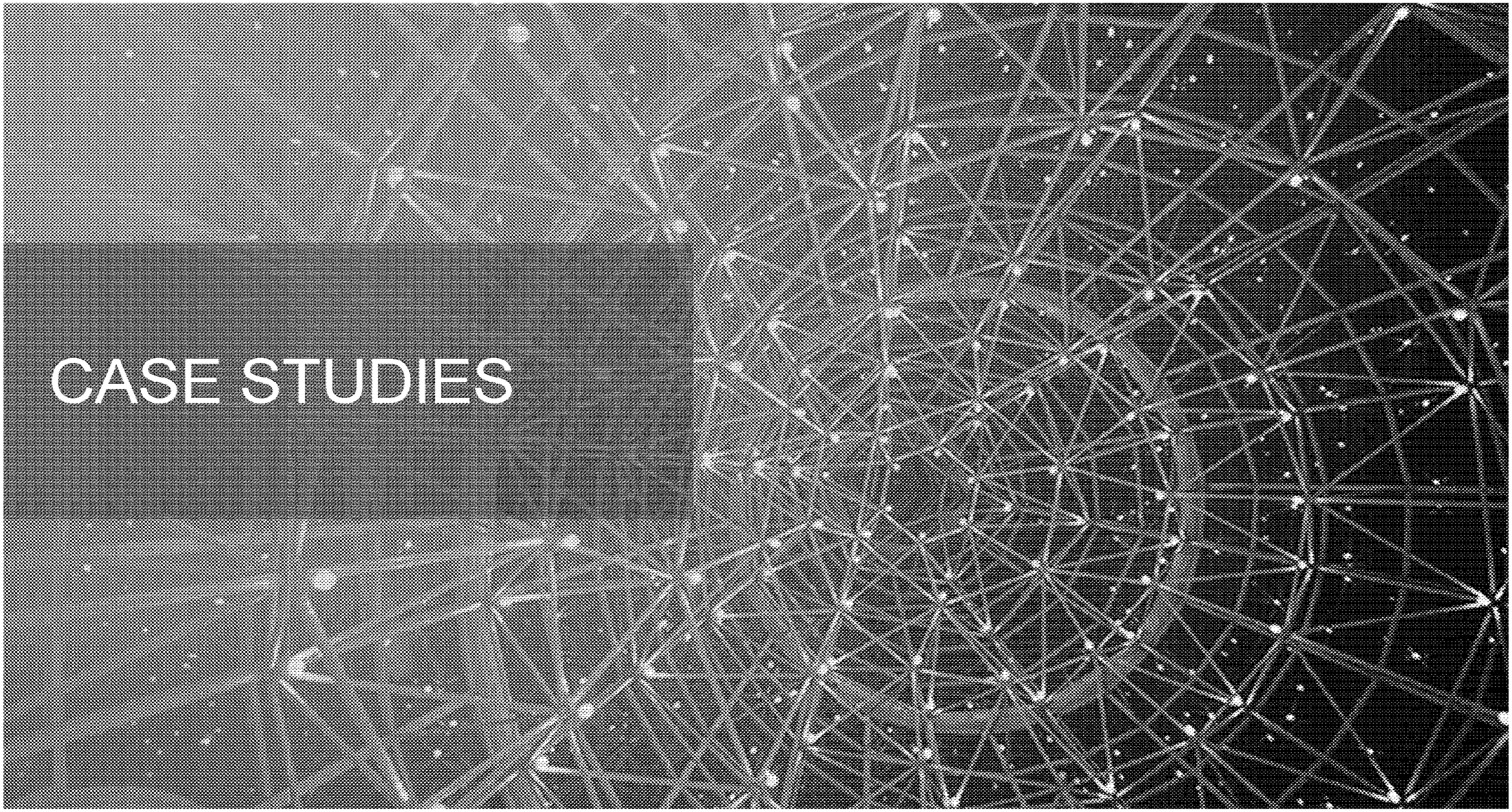
- Cb sends binary file or file hash to Sky ATP for analysis
- Sky ATP does malware assessment and assigns a threat score to the file
- Cb Response takes actions: isolate host, bans file

Benefits

- Malware analysis of unknown threat objects & remediation

Speaker Notes for Slide 54

Specially useful in the off-line devices , that go On-net and are infected.



CASE STUDIES

Case Study: Malware detection at scale

- Sky ATP deployed in TAP mode on SRX5600 by ISP in North America – primarily serving educational institutions
- Ingress and egress traffic inspected. Inline blocking not enabled
- 7 day period in March 2017

535,302
Total Files Processed

55,629
Unique Files

142
Files Determined to be Malware

69%
Discovered Malware was Previously Known

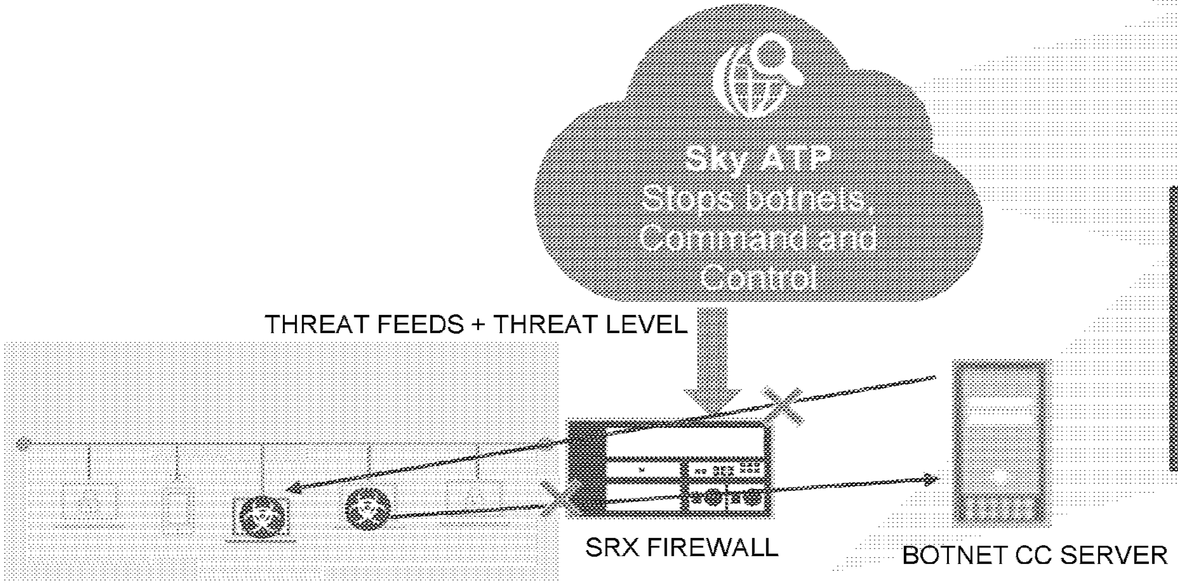
31%
Discovered Malware was previously unseen

Outbound high risk CC connections: 843,346 (1 day)

Case Study: Botnet detection with Sky ATP feeds

- Large IT consulting and managed IT service provider wanted a robust edge protection solution for its campus and branch offices
- Existing desktop and server based AV solutions not detecting advanced threats

Solution: Juniper SRX1500 + Sky ATP



Sky ATP
Stops botnets, Command and Control

THREAT FEEDS + THREAT LEVEL

SRX FIREWALL

BOTNET CC SERVER

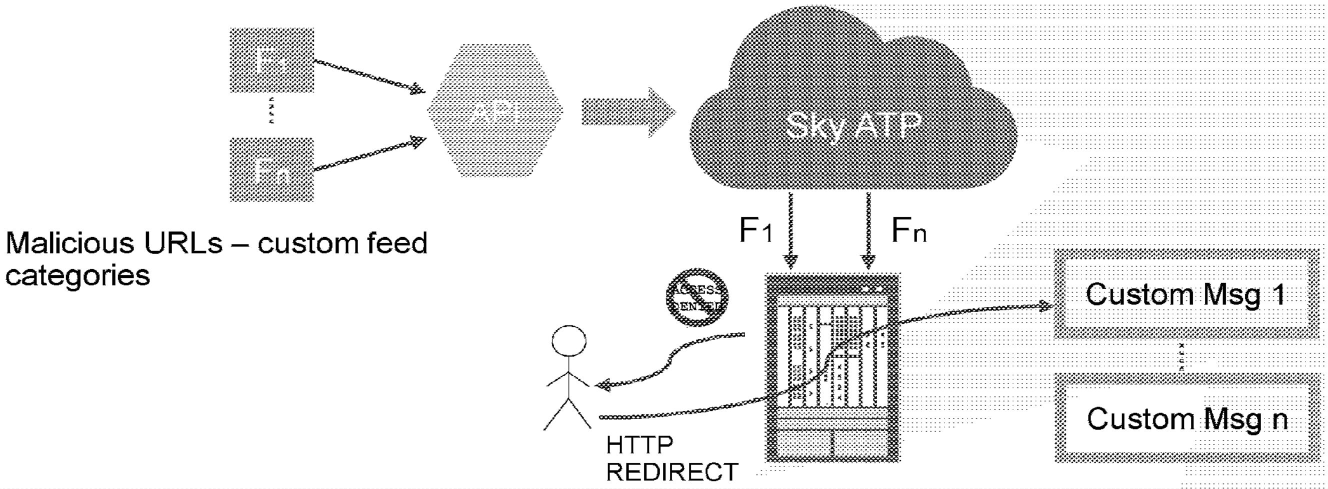
> "After less than a day with Juniper Sky, we knew about threats that we had never seen before." – **Senior IP solutions architect**

JUNIPER NETWORKS CONFIDENTIAL

Case Study: Automated enforcement with API

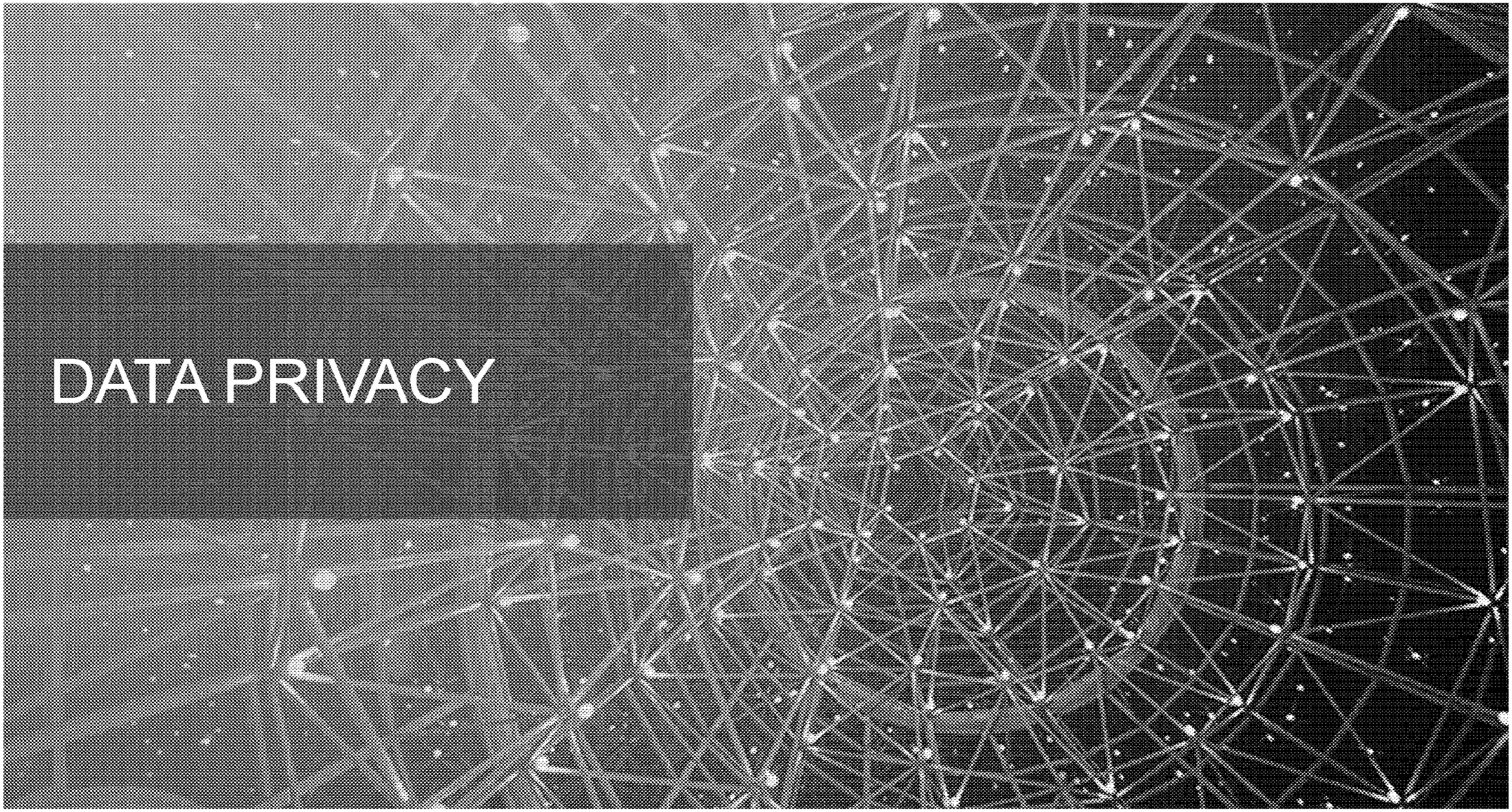
- Major Service Provider in LATAM has to comply with government regulations that require blocking access to questionable content – pedophile sites, gambling, etc.
- New sites/URLs constantly being added so needs dynamic programmatic solution to update firewalls. Also requires ability to redirect to web portals
- 40Gbps IMIX, 600K cps, 100-150M sessions

Solution: Juniper SRX5800 + Sky ATP



Malicious URLs – custom feed categories

JUNIPER NETWORKS CONFIDENTIAL

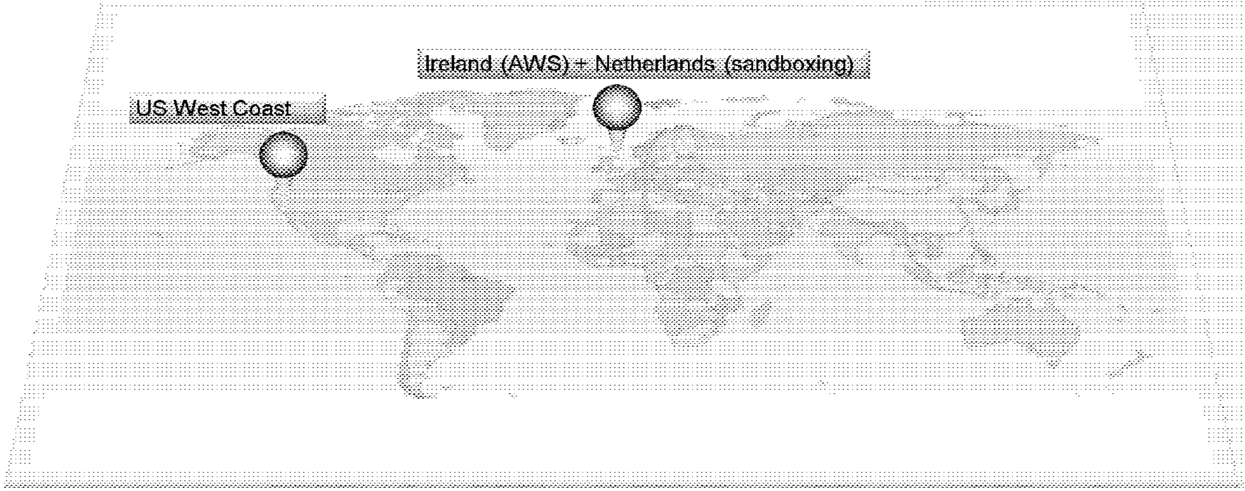


DATA PRIVACY

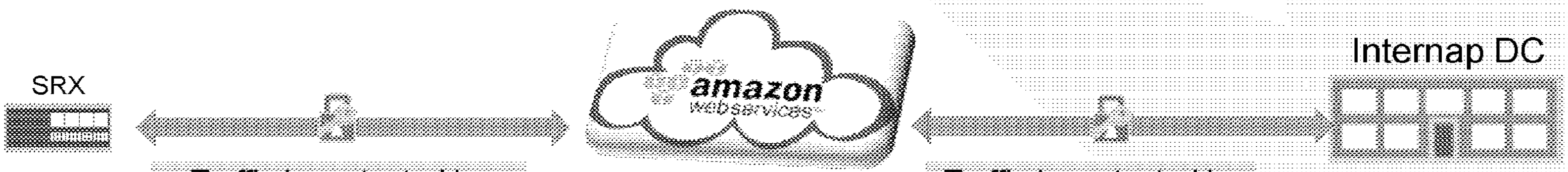
Sky ATP cloud – geo locations

Stages 1 -> 3 | Run on AWS (Amazon Web Services)

Stage 4 (Sandboxing) | Runs on third party (Internap) DC



Sky ATP Security and Privacy



Traffic is protected by TLS

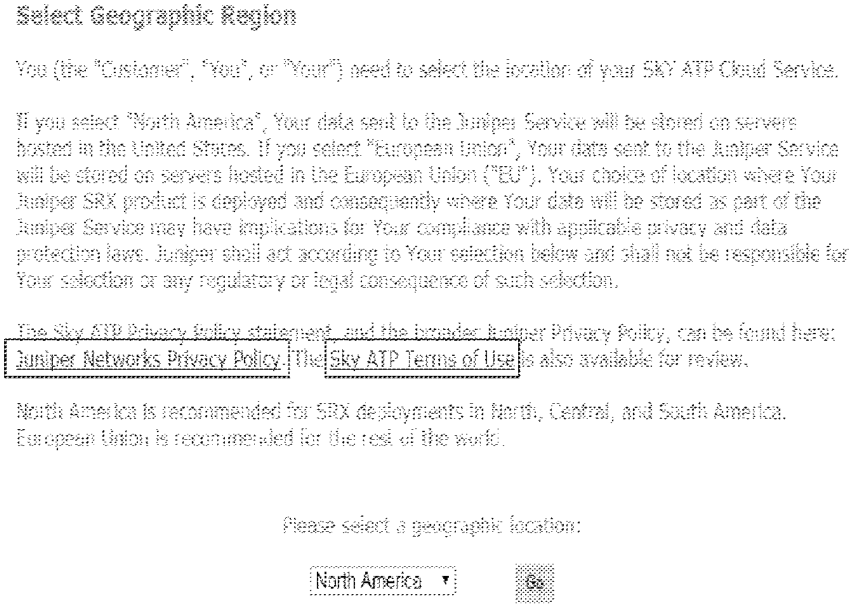
- Customer data is separated to ensure privacy
- Files are destroyed after analysis – only meta-data is maintained
- Executables are saved for 90 days for analysis and then destroyed

Traffic is protected by TLS

Sandboxing VMs and customer files are destroyed after analysis – typically 6-7 minutes

Sky ATP Security and Privacy

https://sky.junipersecurity.net



Select Geographic Region

You (the "Customer", "You", or "Your") need to select the location of your SKY ATP Cloud Service.

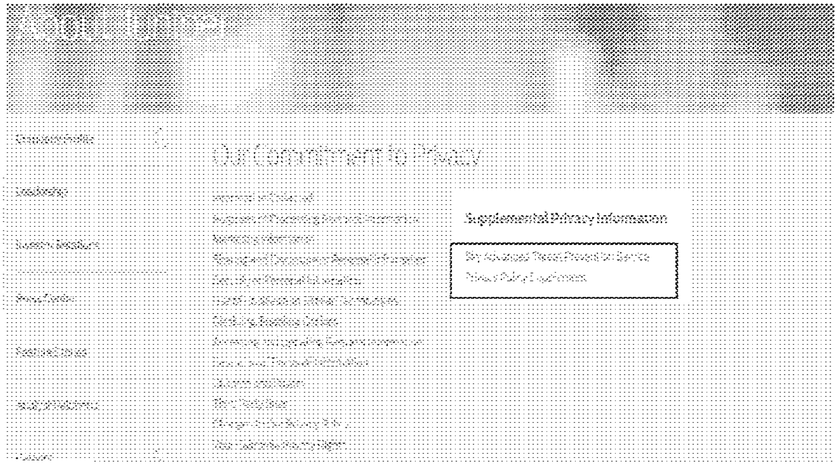
If you select "North America", Your data sent to the Juniper Service will be stored on servers hosted in the United States. If you select "European Union", Your data sent to the Juniper Service will be stored on servers hosted in the European Union ("EU"). Your choice of location where Your Juniper SRX product is deployed and consequently where Your data will be stored as part of the Juniper Service may have implications for Your compliance with applicable privacy and data protection laws. Juniper shall act according to Your selection below and shall not be responsible for Your selection or any regulatory or legal consequence of such selection.

The Sky ATP Privacy Policy statement, and the broader Juniper Privacy Policy, can be found here: Juniper Networks Privacy Policy. The Sky ATP Terms of Use is also available for review.

North America is recommended for SRX deployments in North, Central, and South America. European Union is recommended for the rest of the world.

Please select a geographic location:

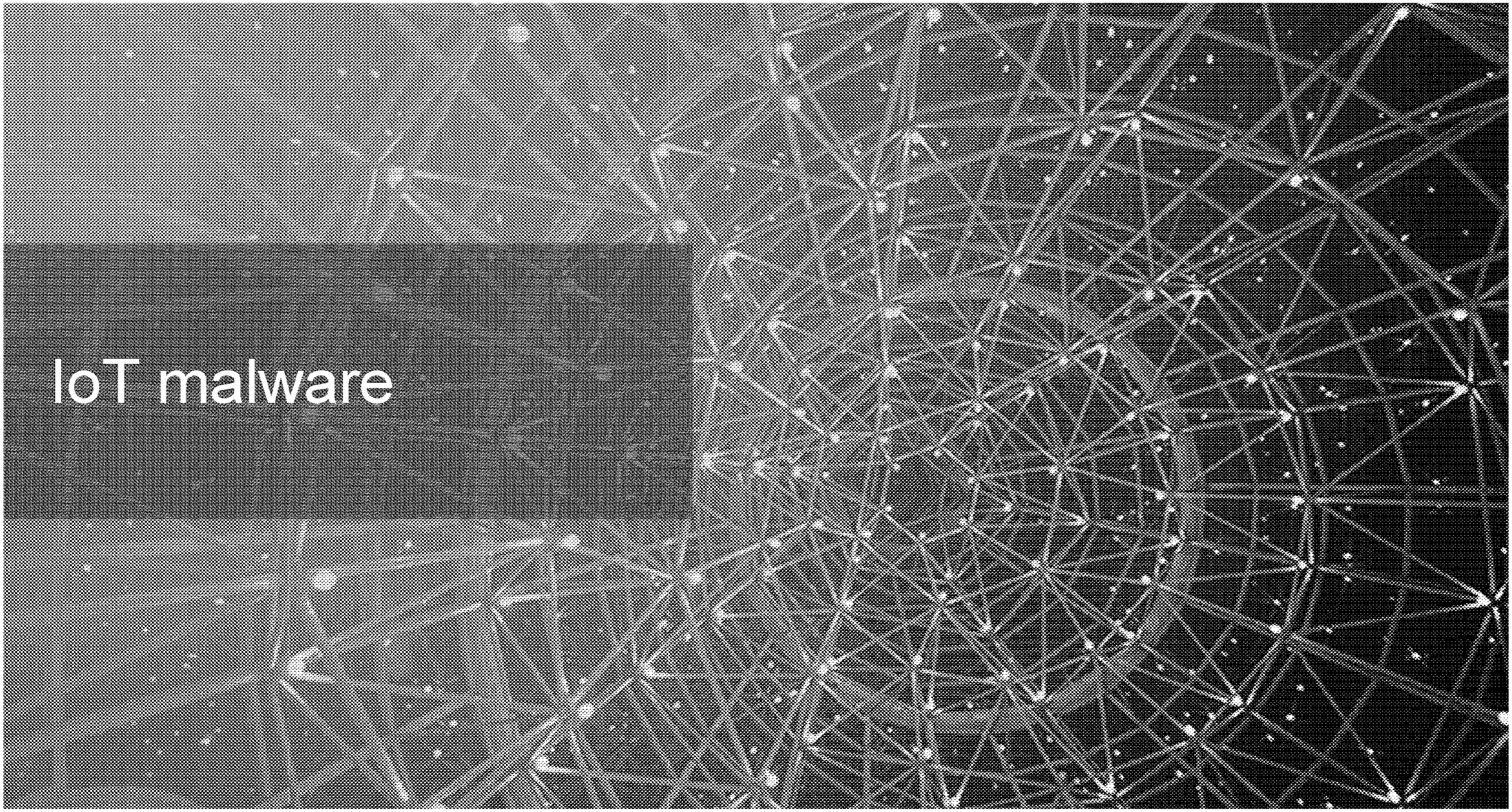
North America ▾ Go



Our Commitment to Privacy

Supplemental Privacy Information

Sky Advanced Threat Prevention Service Privacy Policy Supplement

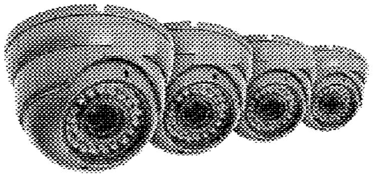


IoT malware

Real world examples of IoT malware / ransomware

- Thermostat ransomware[1]

- Amazon cameras malware[2]

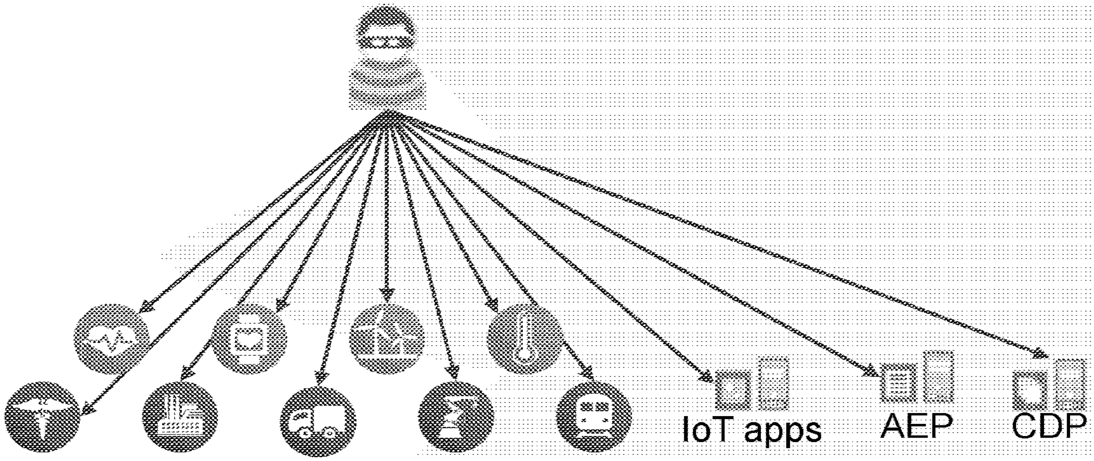


- Jeep remote control[3]

1. http://motherboard.vice.com/read/internet-of-things-ransomware-smart-thermostat
2. http://www.securityweek.com/malware-found-iot-cameras-sold-amazon
3. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Getting ransomware and malware into IoT networks

- DNS spoofing
- Default passwords
- Phishing attacks



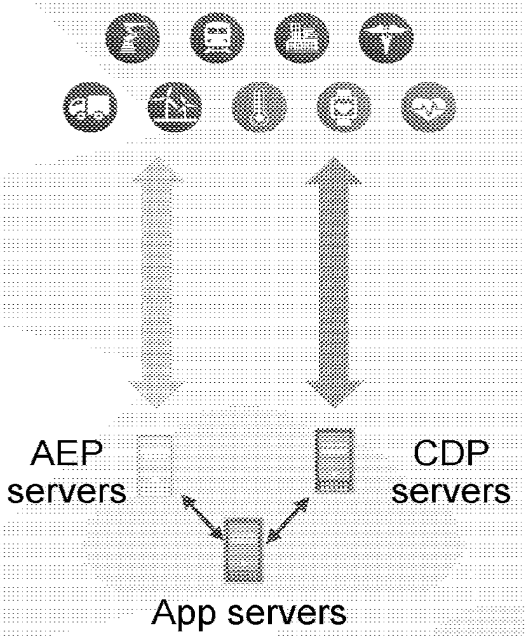
Both IoT devices **and** IoT application servers / supporting servers

Targets for IoT ransomware and malware

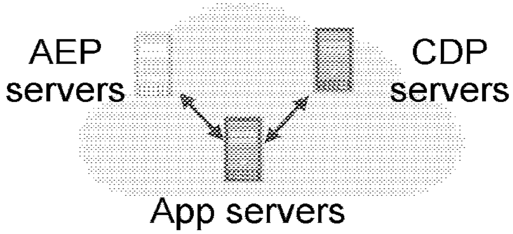
IoT devices

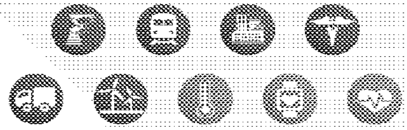
IoT application servers

- IoT application servers
- Application Enablement Platforms
- Connected Device Platforms



IoT specific Advanced Threat Detection





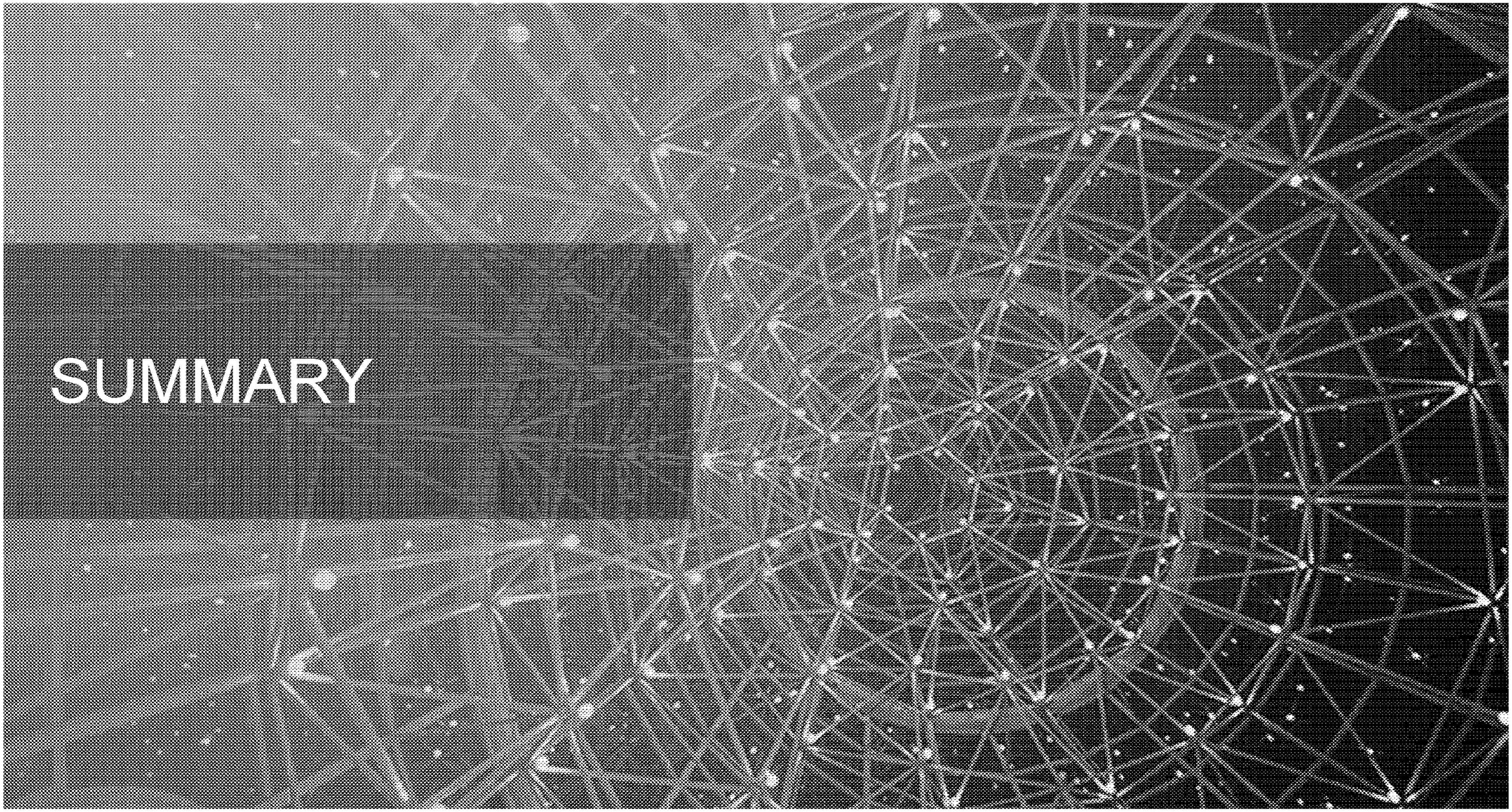
IoT servers

- Based on Windows or Linux
- Juniper Policy Enforcer can stop East-West propagation

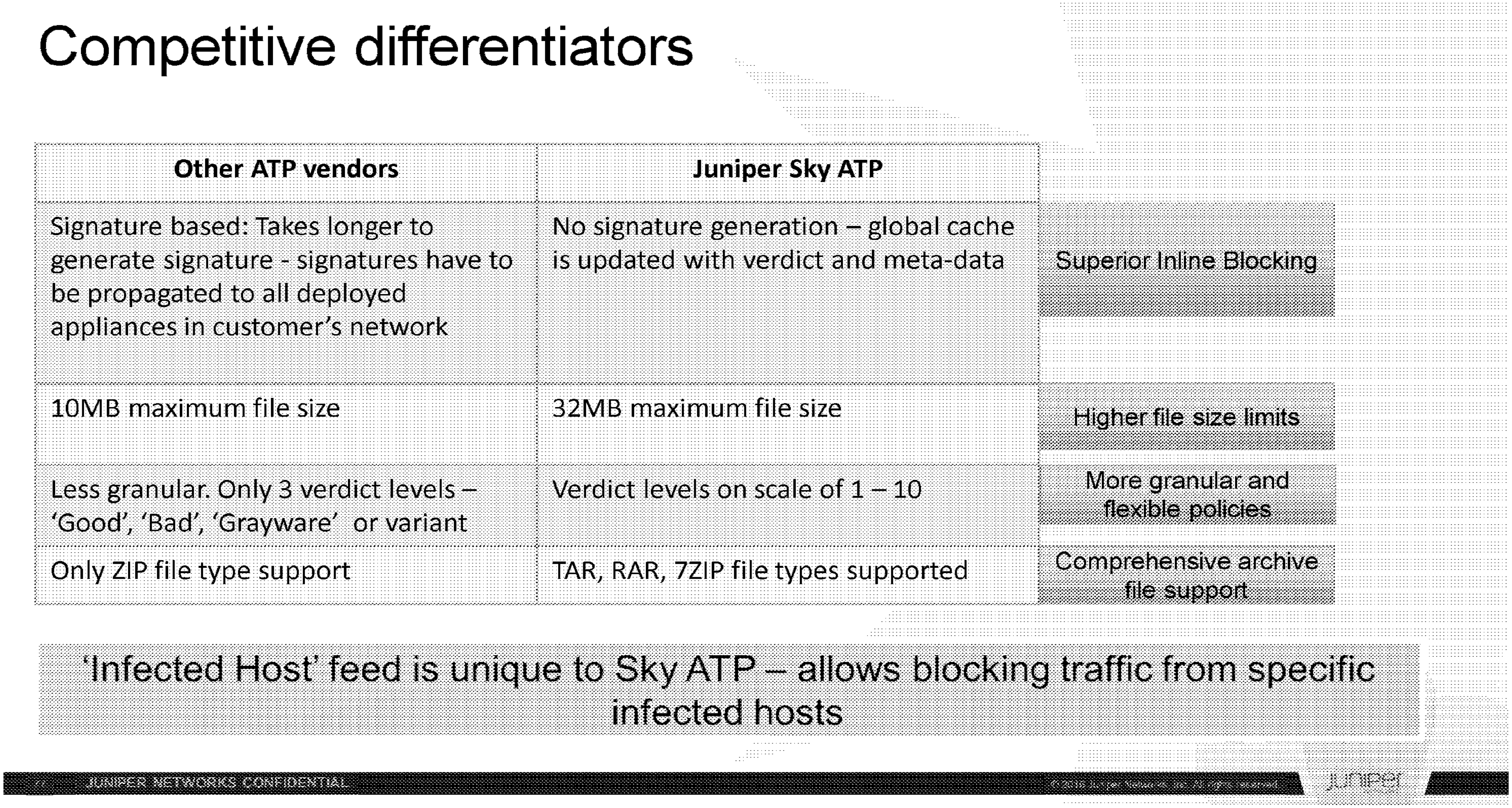
IoT devices

- Many are Linux based
- Sky ATP: static and dynamic analysis for IoT malware
- Will be tailored for specific devices / applications

SkyATP supports 3rd party detection integration



SUMMARY

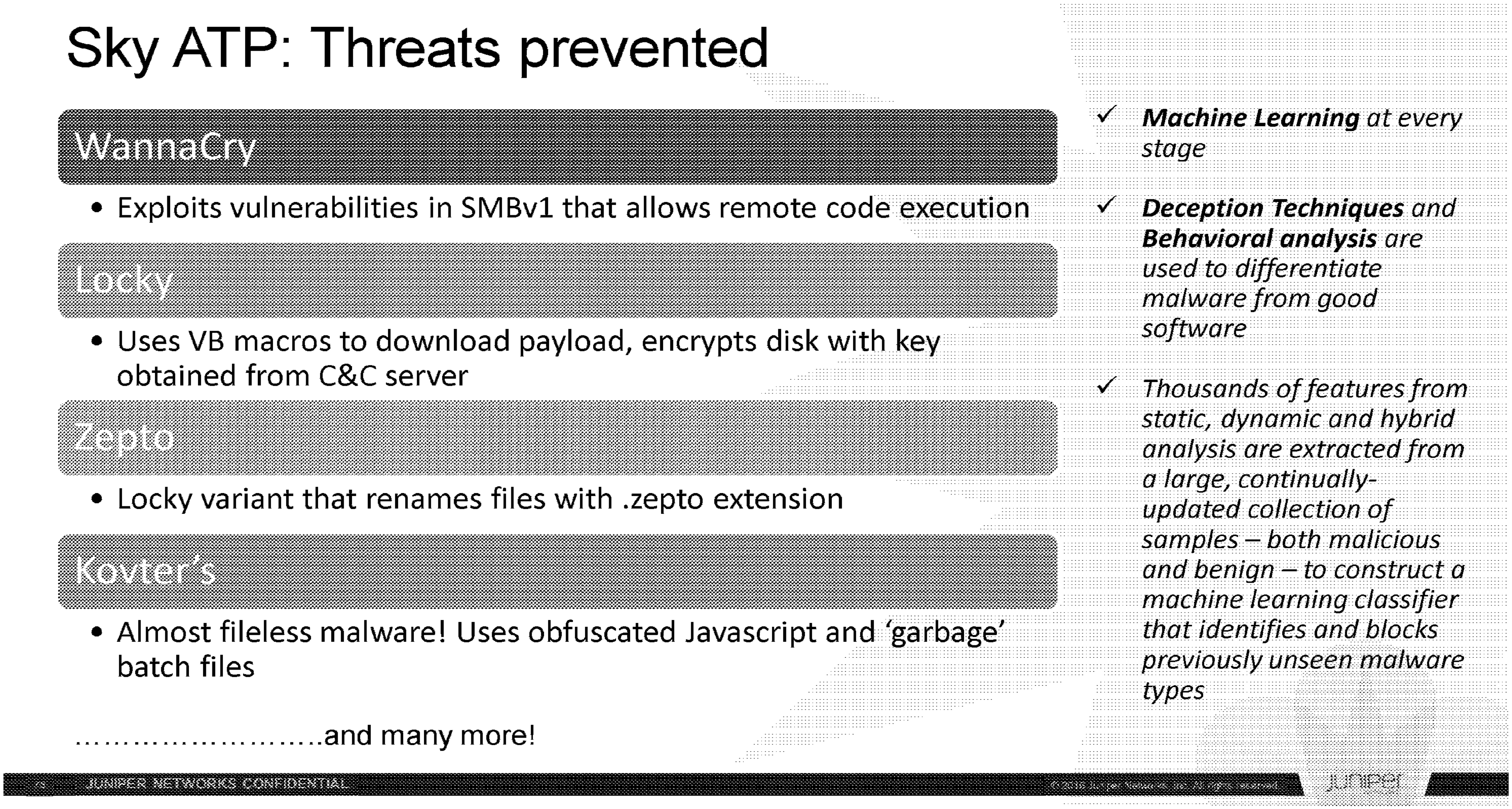


Competitive differentiators

Other ATP vendors	Juniper Sky ATP	
Signature based: Takes longer to generate signature - signatures have to be propagated to all deployed appliances in customer's network	No signature generation – global cache is updated with verdict and meta-data	Superior Inline Blocking
10MB maximum file size	32MB maximum file size	Higher file size limits
Less granular. Only 3 verdict levels – 'Good', 'Bad', 'Grayware' or variant	Verdict levels on scale of 1 – 10	More granular and flexible policies
Only ZIP file type support	TAR, RAR, 7ZIP file types supported	Comprehensive archive file support

'Infected Host' feed is unique to Sky ATP – allows blocking traffic from specific infected hosts

JUNIPER NETWORKS CONFIDENTIAL



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*

JUNIPER NETWORKS CONFIDENTIAL

How is Sky ATP Different?

- High Efficacy, Scalable and Tightly integrated solution
  - Distributed sensing and enforcement on SRX (no additional sensors)
  - Actionable Intelligence
  - In-line blocking to prevent zero-day infections from getting in
  - Unique deception & provocation techniques to counter evasive threats
  - Advanced machine learning
- Support for different types of analysis targets
  - Multi-platform executable and application support
  - Exploits and malicious content embedded in documents (MS Office, PDF)
  - Dangerous web applications (Java, Flash)
- Cost-effective, non-intrusive solution with full network coverage

Thank you