JUNIPER NETWORKS

Sky ATP Advanced Threat protection

Juniper’s Sky IS the limit!

Juniper Networks, April 2016

Santanu Ganguly <santanu@juniper.net>

An Evolving Threat Landscape

New actors, new threats, and new technologies means the threat landscape is constantly evolving.

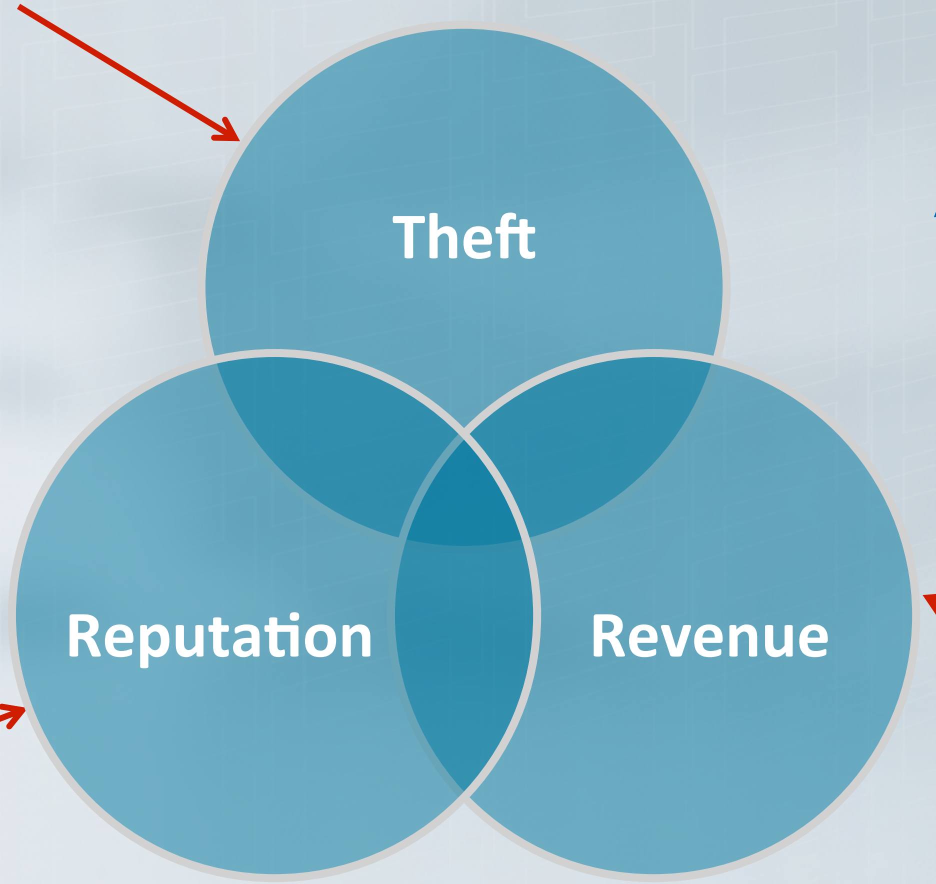
- State sponsored actors and targeted attacks change the landscape
- Attackers are constantly looking for, and finding, new vectors
- Security solutions need to be agile to keep up
- The impact of security breaches can’t be understated

The Head of Cyber of British Intelligence, in his first public, yet anonymous interview stated: “There are now three certainties in life: there's death, there's taxes and there's a foreign intelligence service on your system."

Impact of security breaches:

Target breach (2013)

Target Stolen Data: 110M Records



Ponemon Institute:

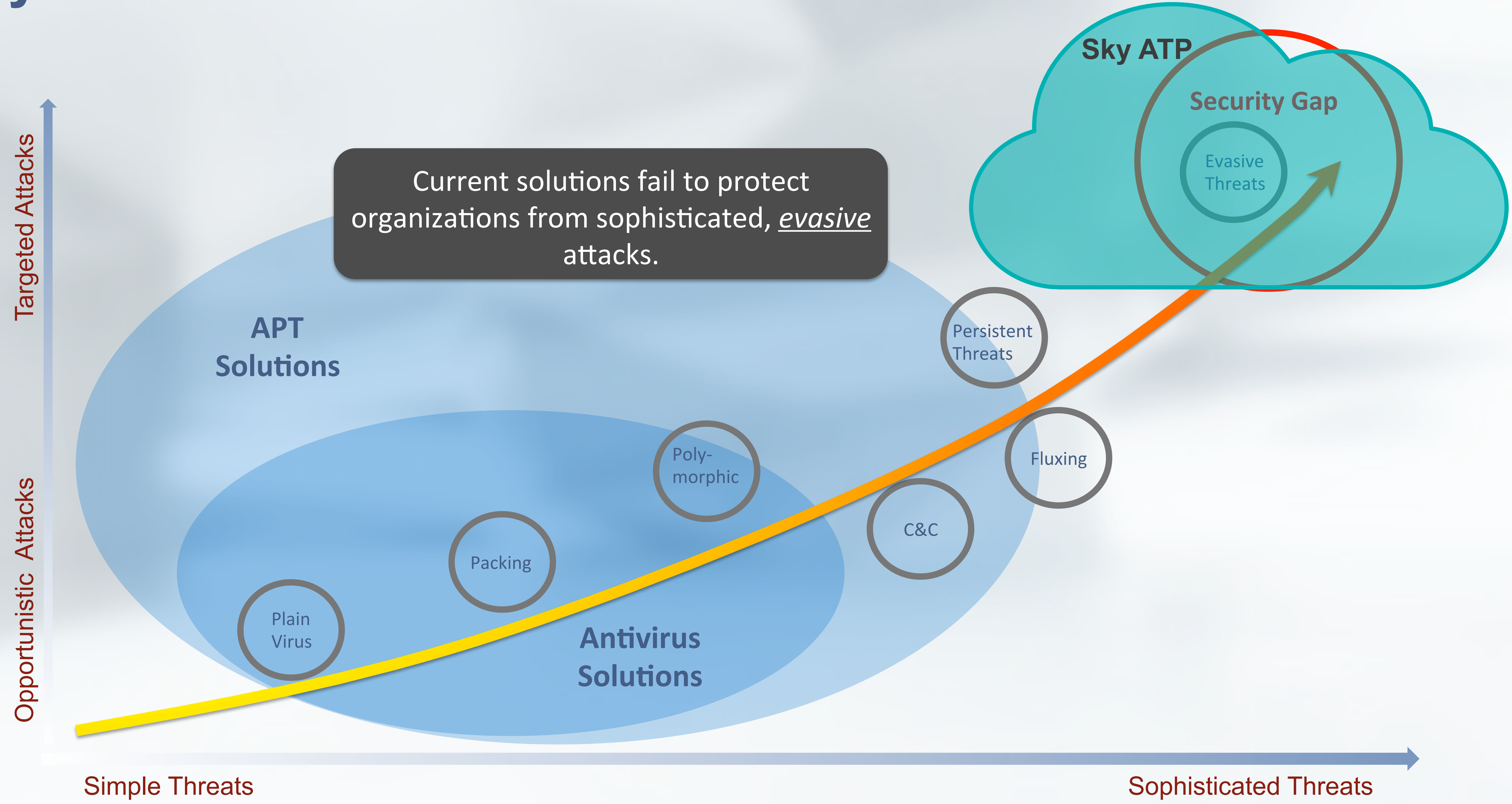
Average breach costs $214 per record stolen

A dozen lawsuits in progress, lost customers

Cost of the breach:

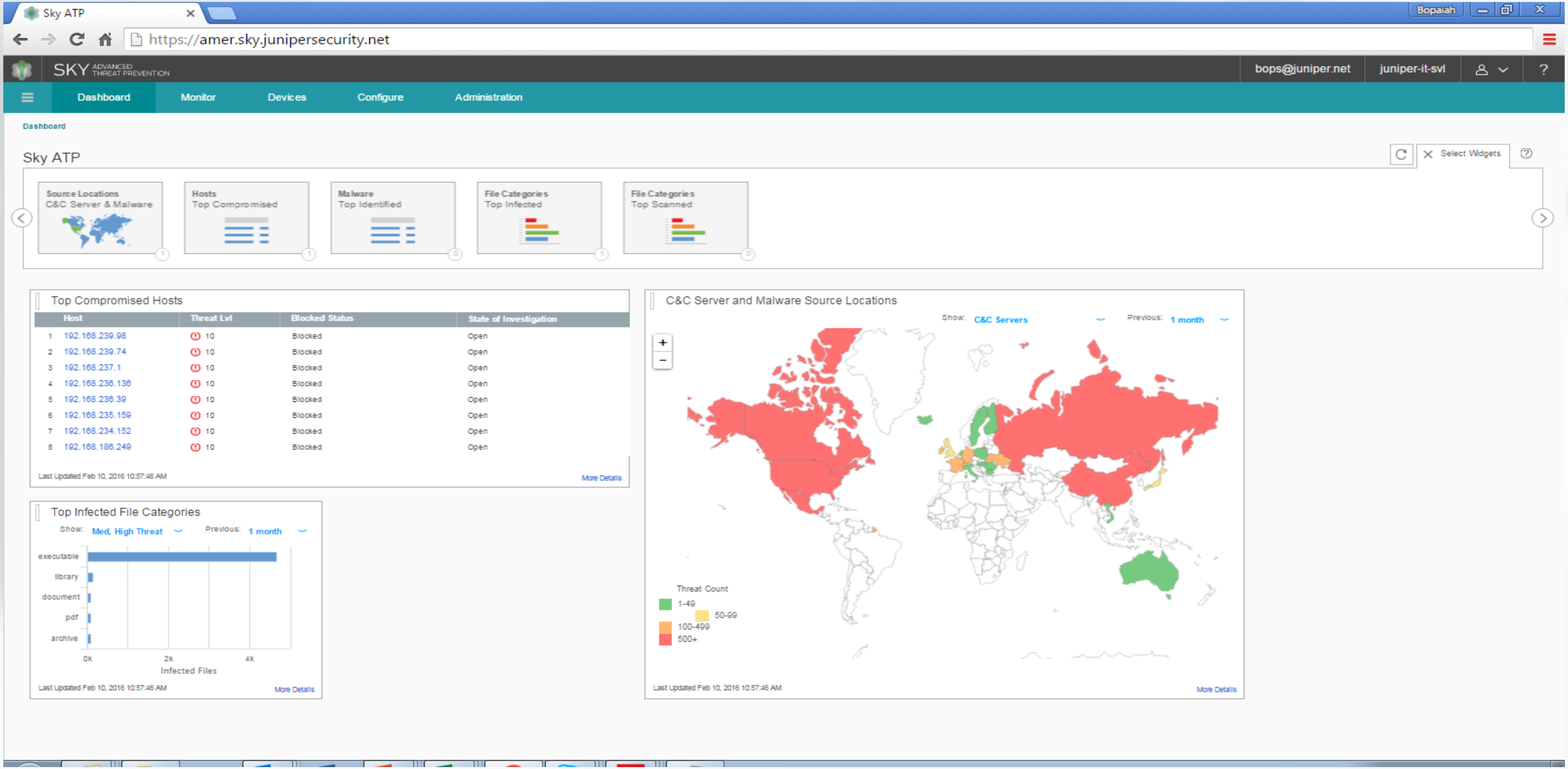
- Gross expense of $191M
- Net cost of $162M

Sky Advanced Threat Prevention to the Rescue



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

What is Sky Advanced Threat Prevention



Sky ATP

Top Compromised Hosts

	Host	Threat Lvl	Blocked Status	State of Investigation
1	192.168.239.98	10	Blocked	Open
2	192.168.239.74	10	Blocked	Open
3	192.168.237.1	10	Blocked	Open
4	192.168.236.136	10	Blocked	Open
5	192.168.236.39	10	Blocked	Open
6	192.168.235.159	10	Blocked	Open
7	192.168.234.152	10	Blocked	Open
8	192.168.186.249	10	Blocked	Open

Last Updated Feb 10, 2016 10:57:46 AM

More Details

C&C Server and Malware Source Locations

Show: C&C Servers

Previous: 1 month

Threat Count

🟩	1-49
🟨	50-99
🟧	100-499
🟥	500+

Last Updated Feb 10, 2016 10:57:46 AM

More Details

Top Infected File Categories

Show: Med, High Threat

Previous: 1 month

Last Updated Feb 10, 2016 10:57:46 AM

More Details

Why Cloud?

- Cloud environments are flexible and massively scalable
- A shared platform means everyone benefits from new threat intelligence in near real-time
- Security developers can update their defenses as new attack techniques come to light, with no delay to distribute the threat intel.
- On-site platforms offer lower efficiency, scalability, efficacy and agility.

The connection between the SRX and the Cloud is encrypted. Customer data exported to the Cloud is destroyed after analysis. Customer data is isolated to ensure privacy.

Sky Advanced Threat Prevention Architecture:

Sky components are divided between the SRX, embedded in Junos, and the cloud

- Components in Junos:
  - SecIntel Service
    - Receives feeds from the cloud
      - GeoIP
      - Command and Control
      - ***Infected Hosts***
  - Sky ATP Service
    - Passes incoming files to the Cloud for analysis
    - Enforces policies based on Cloud verdicts

Sky Advanced Threat Prevention Architecture:

Sky components are divided between the SRX, embedded in Junos, and the cloud

- Components in the Cloud:
  - Analytics
    - Malware analysis pipeline
    - C&C / Malware Event correlation
  - Threat feeds
    - Cascade – generating the C&C Feed
    - GeoIP – externally sourced
    - ***Infected Hosts*** – Generated by event correlation
  - Management
    - Web UI for all your management love and affection

Sky Advanced Threat Prevention

Infected Hosts:

The ***Infected Hosts*** feed allows automated quarantining and active responses to internal threats. This is an “Event Driven” feed, created in the Cloud based on what’s actively happening on a protected network.

Use Cases

Sky Advanced Threat Prevention Use Cases

Use cases across the deployment spectrum of SRX

A. Campus Edge Firewall

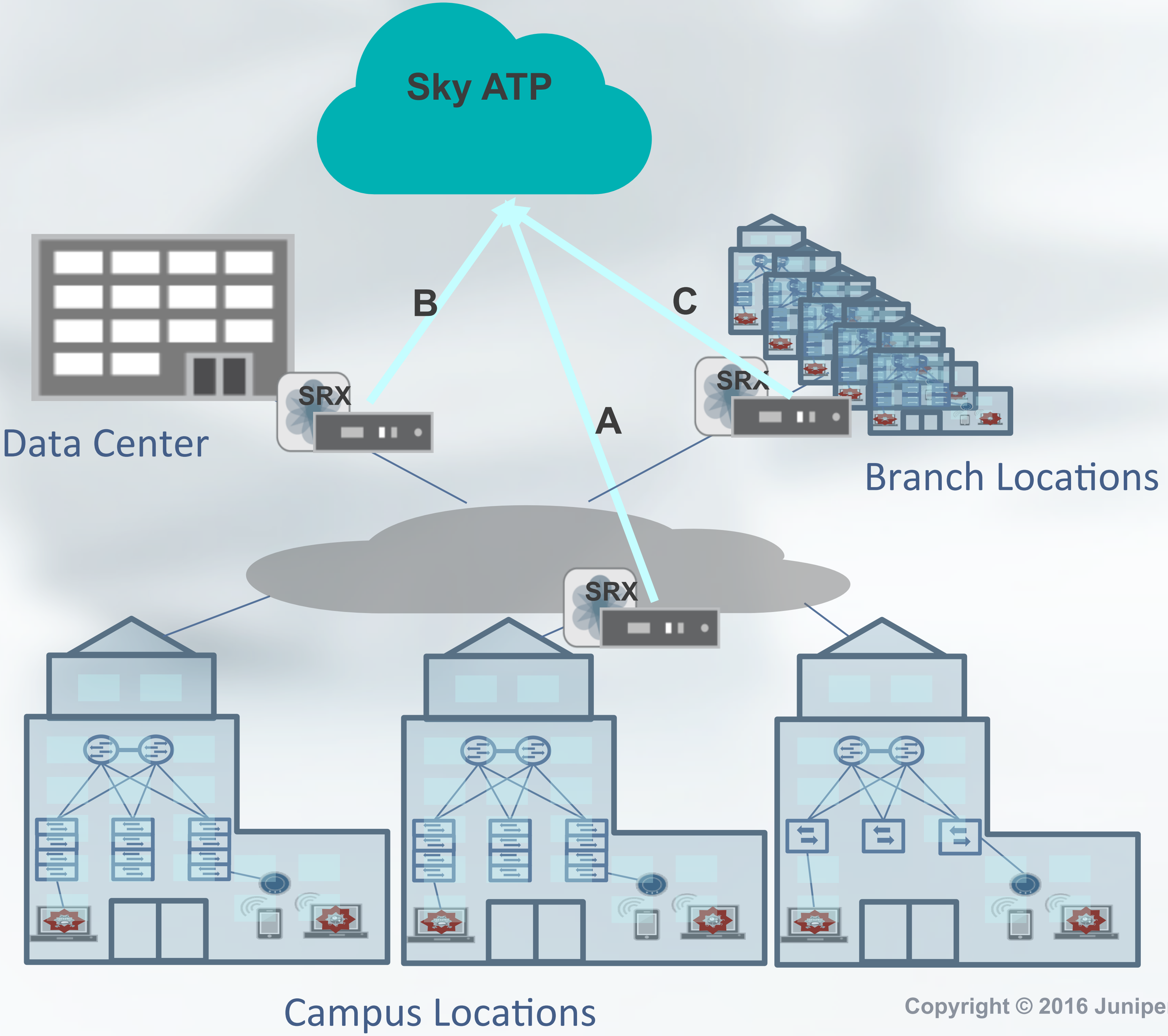
- **Protection of end user devices from files downloaded from the Internet**

B. Branch Router

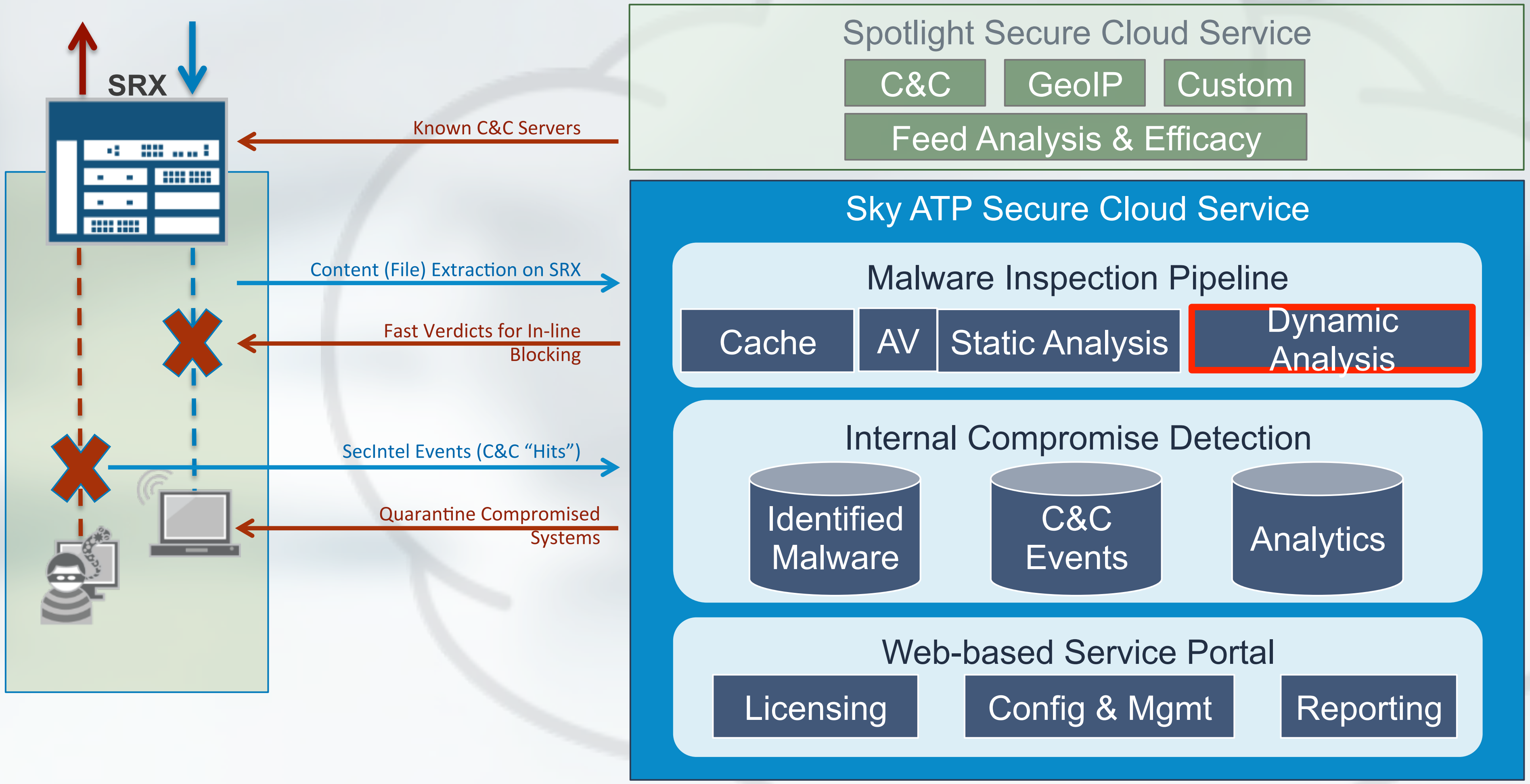
- **Protection for split-tunnel deployments**

C. Data Center Edge

- **Application protection from infected files**

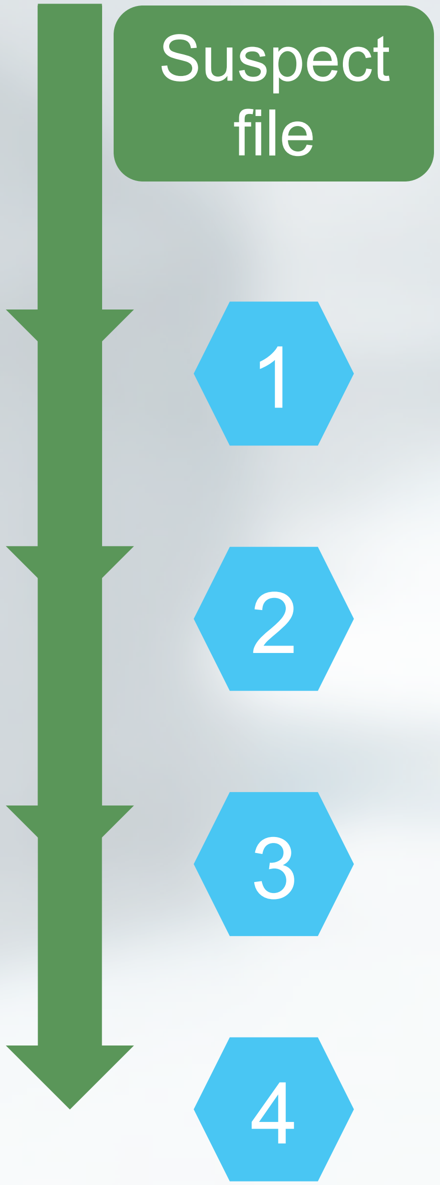


Sky Advanced Threat Prevention in action


SRX
Known C&C Servers
Content (File) Extraction on SRX
Fast Verdicts for In-line Blocking
SecIntel Events (C&C "Hits")
Quarantine Compromised Systems
Spotlight Secure Cloud Service
C&C
GeoIP
Custom
Feed Analysis & Efficacy
Sky ATP Secure Cloud Service
Malware Inspection Pipeline
Cache
AV
Static Analysis
Dynamic Analysis
Internal Compromise Detection
Identified Malware
C&C Events
Analytics
Web-based Service Portal
Licensing
Config & Mgmt
Reporting

The ATP verdict chain

Staged analysis: combining rapid response and deep analysis



Suspect files enter the analysis chain in the cloud

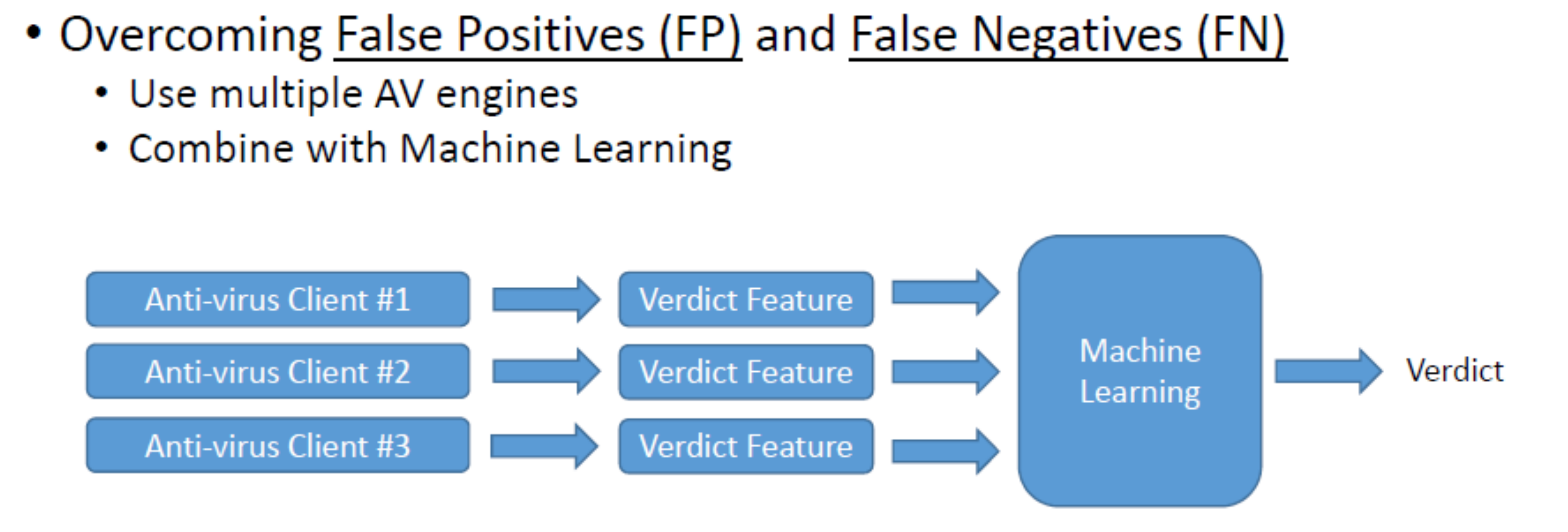
Cache lookup: (~1 second)
Files we’ve seen before are identified and a verdict immediately goes back to SRX

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

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

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

Anti-Virus: First Pass



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

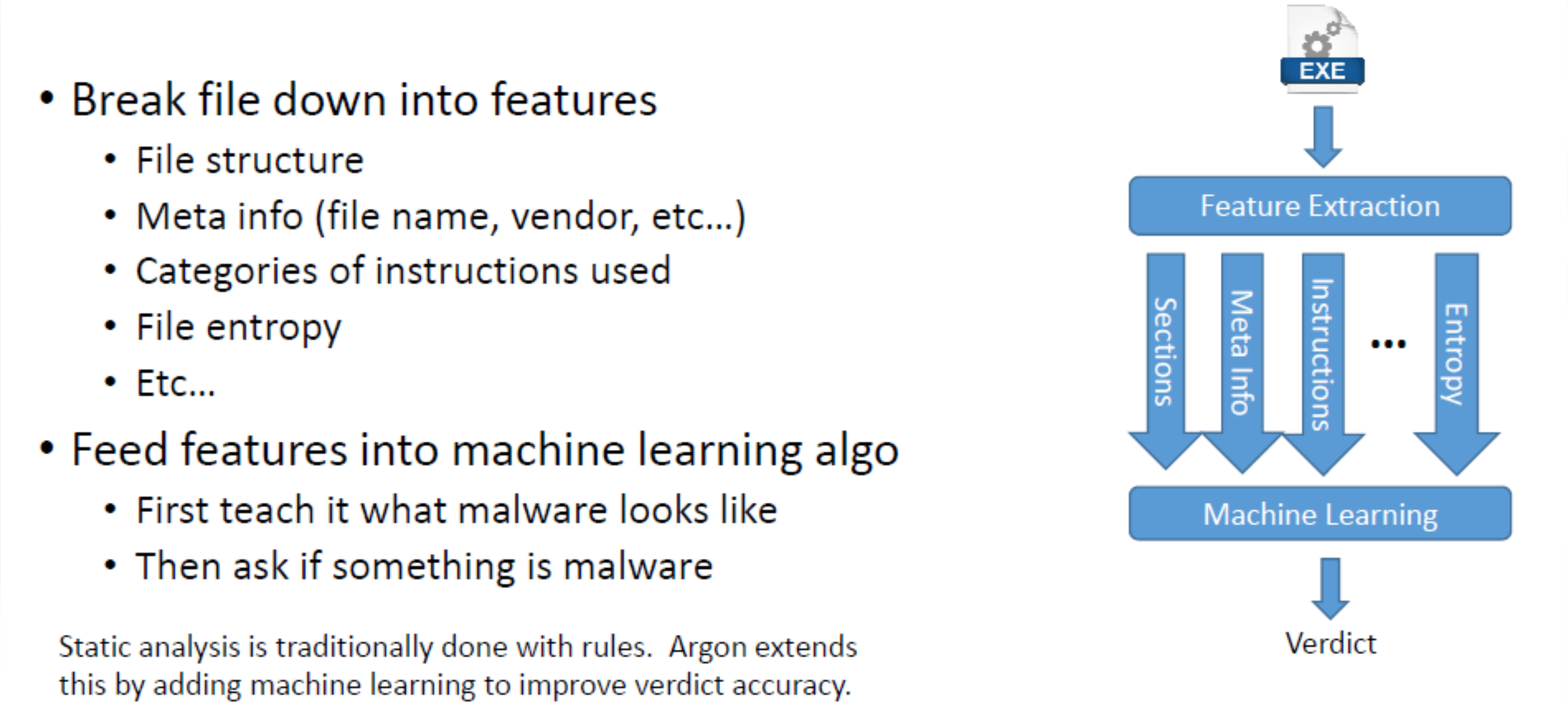
Anti-virus Client #1 → Verdict Feature →

Anti-virus Client #2 → Verdict Feature →

Anti-virus Client #3 → 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

At release: *Windows 7*
Future: Windows 8, 10, *Android, Linux, other.*

Sandboxing: Behavioral Analysis

Behavior analysis gives us a better understanding of what a suspect file is trying to do. Some behaviors are usually considered benign, while others may be benign, but are also seen in malicious programs. Still others are usually associated with attack behaviors. Some examples:

Hostile

Often Malicious behaviors

- Allocates large chunks of memory
- Unusually long sleep times (> 3 minutes)
- Execute a document exploit

Possibly Malicious behaviors

- Launches process in debugging mode
- Creates mutexes

Usually Benign behaviors

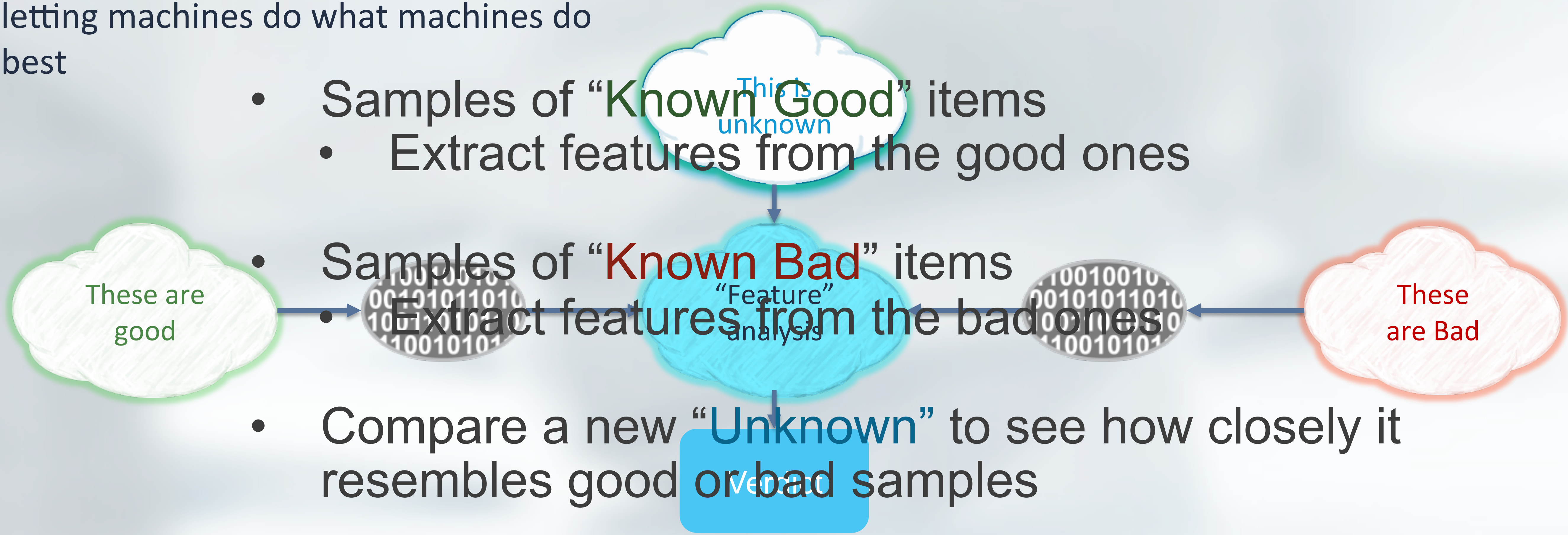
- Creates files in the user's directory

alyze hundreds of behaviors to reach a verdict.

Machine Learning

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

- Samples of “Known Good” items
  - Extract features from the good ones
- Samples of “Known Bad” items
  - Extract features from the bad ones
- Compare a new “Unknown” to see how closely it resembles good or bad samples



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.

Machine Learning algorithms build a feature set by looking at thousands of samples of known “Good” and known “Bad” examples. This gives a baseline for comparing unknown samples.

Summary

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) – *future*
- Cost-effective, non-intrusive solution with full network coverage

Summary

Leveraging the Cloud to provide efficacy and agility

- [illegible] at scale.

Thank You!