Juniper Sky Advanced Threat Prevention

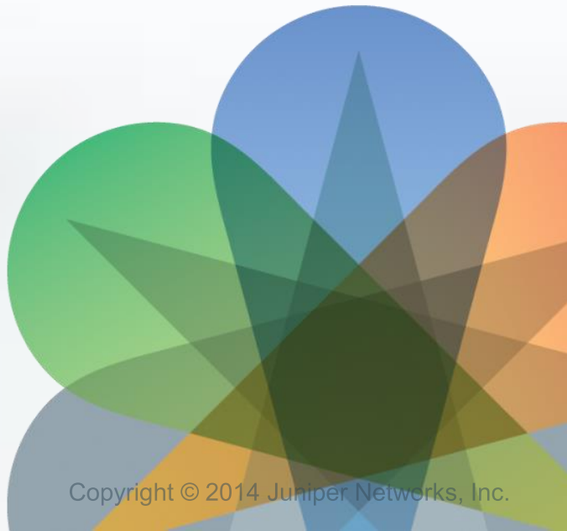
The evolution of malware threat mitigation

Nguyễn Tiến Đức
ntduc@juniper.net

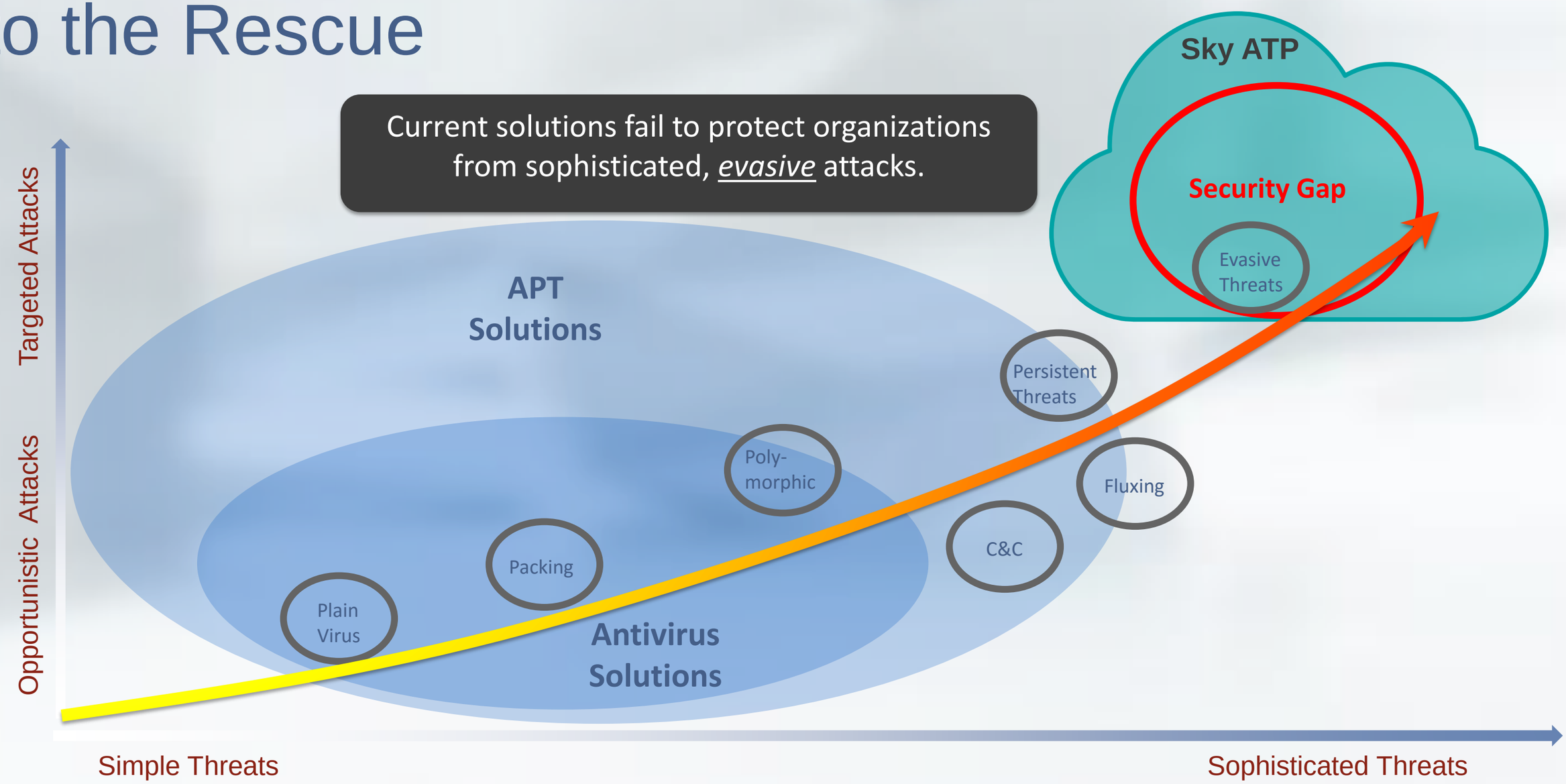
An Evolving Threat Landscape

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

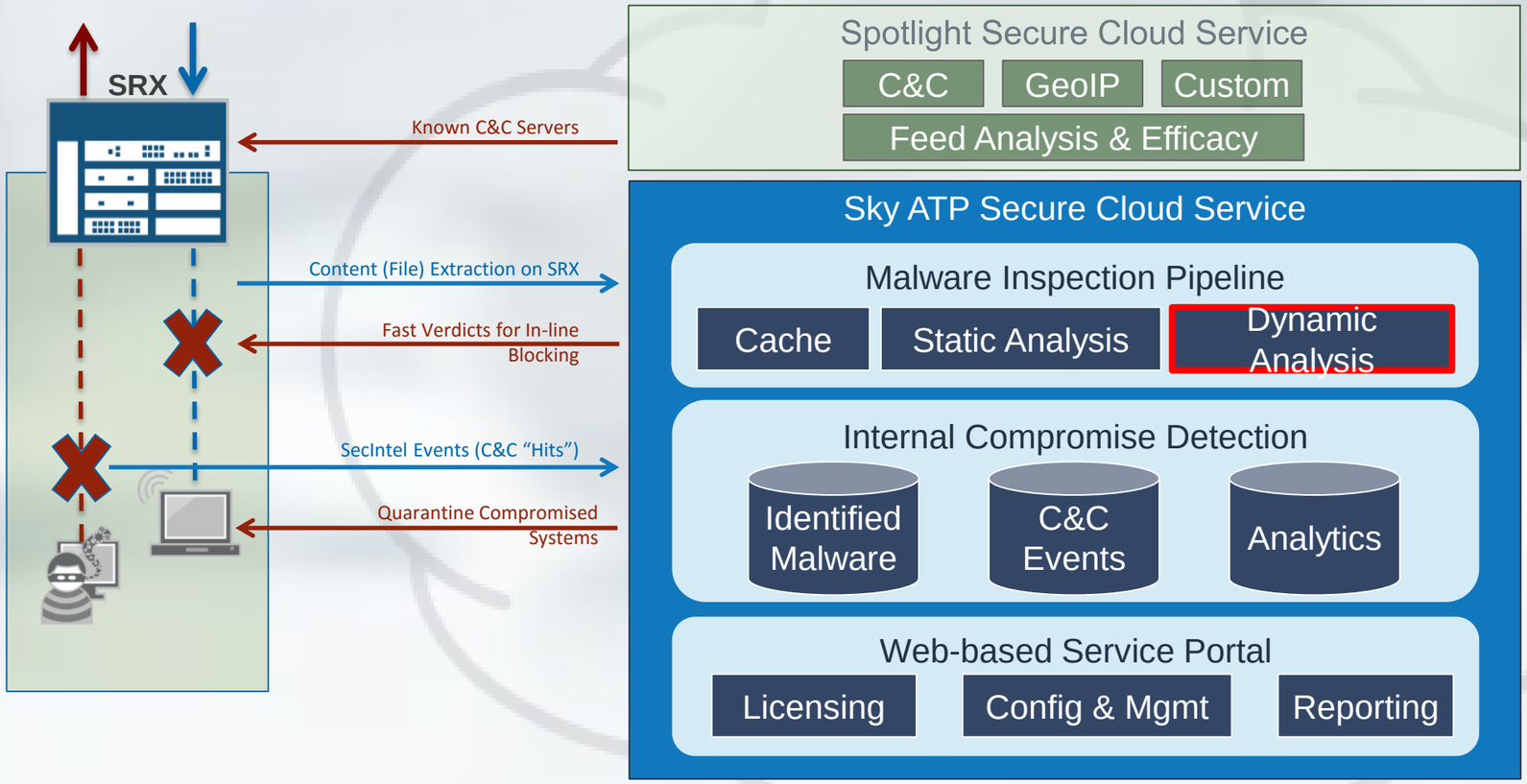
- State sponsored actors and targeted attacks change the landscape
- Attackers are constantly looking for, and finding, new vectors
- Security solutions need to be agile to keep up
- The impact of security breaches can’t be understated



Sky Advanced Threat Prevention to the Rescue



Sky Advanced Threat Prevention Architecture:



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

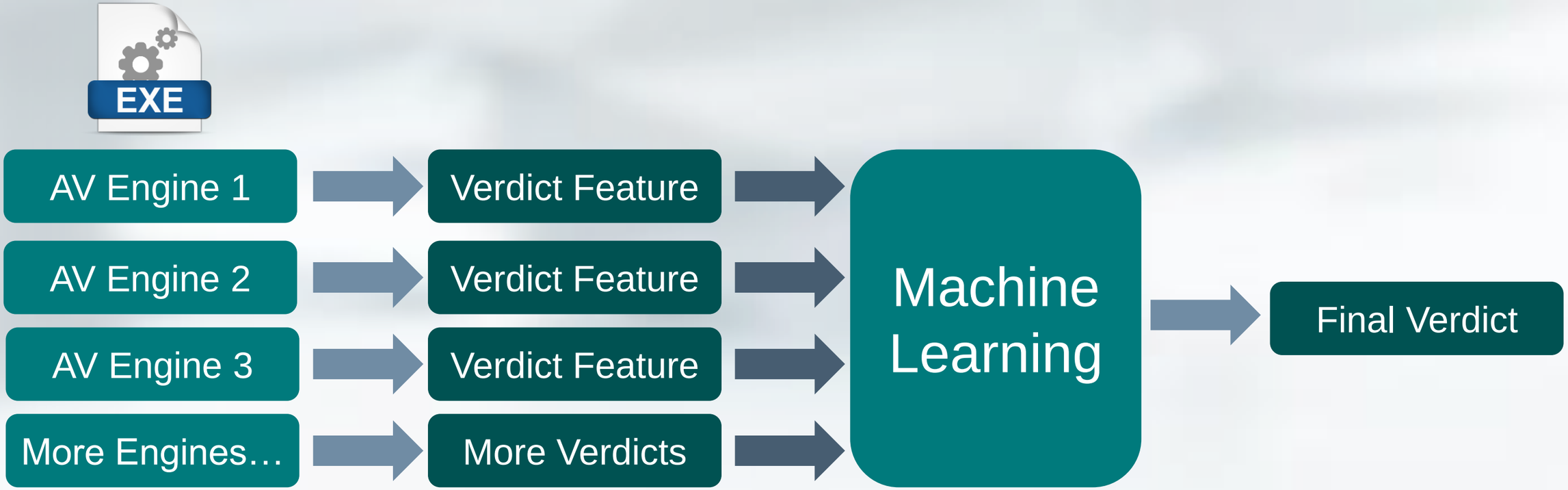
Static analysis: (~30 second)
The static analysis engine does a deeper inspection, with the verdict again cached for future reference

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 Positive (FP) and False Negative (FN) results

- Run samples through multiple AV engines
- Leverage Machine Learning to improve veracity



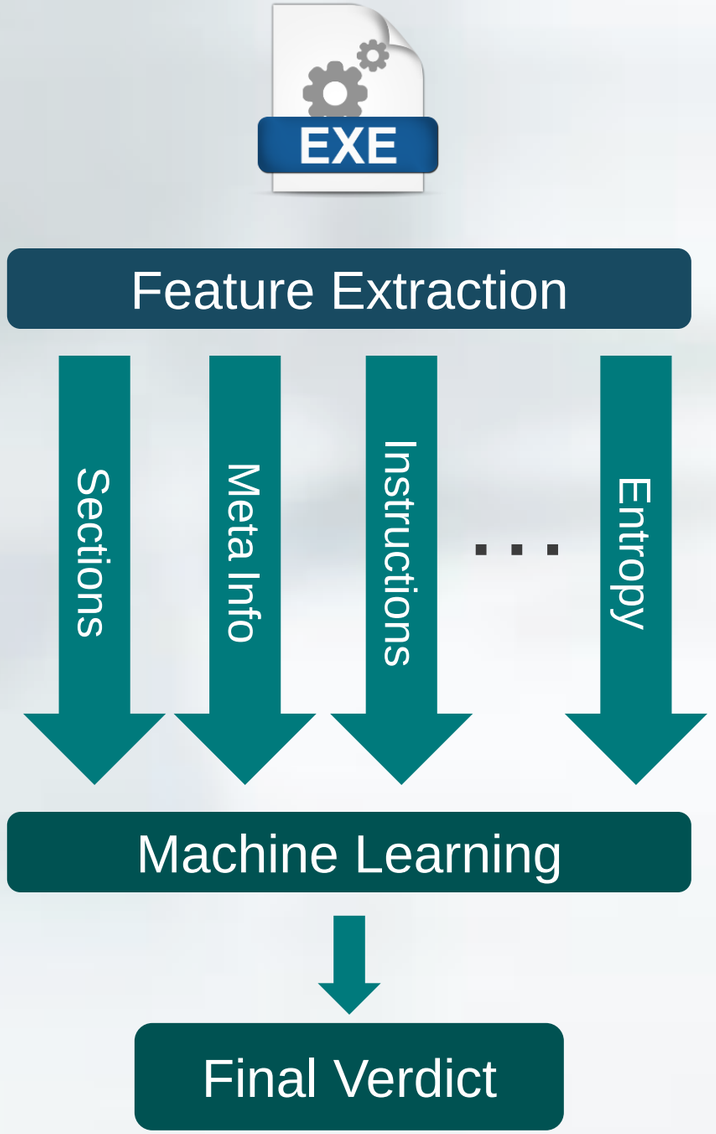
Static Analysis: Pulling apart the code

Break the file down into “features”

- File Structure
- Meta Info (vendor, filename, etc.)
- Instruction categories used
- File entropy
- Etc. . . .

Use Machine Learning to identify what features are associated with Malware and what are associated with Benign applications.

Finally, generate a verdict based on how much “Like” Malware a sample looks



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: *OS X, Linux, Android, iOS*

Deception and Provocation

Deception
Provoking Malware.

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

At FRS, Sky Advanced Threat Prevention will look for over 300 different malware behaviors and will include over 50 different deception techniques to provoke malware to expose 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

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

alyze hundreds of behaviors to reach a verdict.

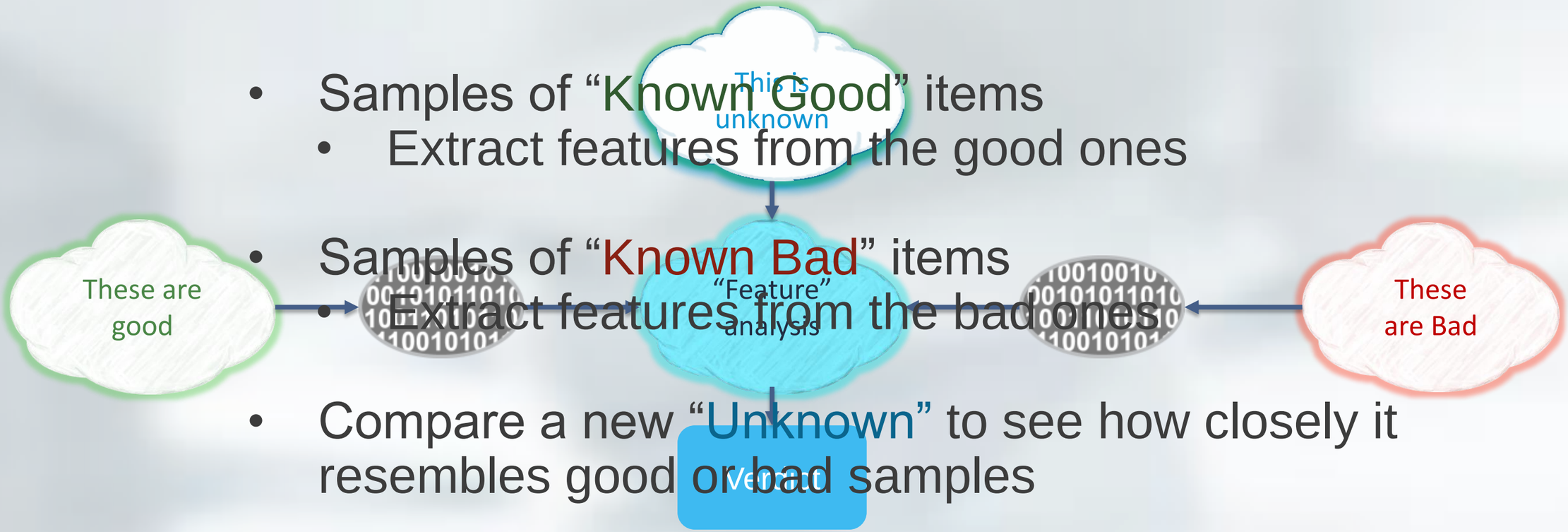
Often Malicious behaviors

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

directory

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 a new example resembles the known good samples of examples. By comparing "Bad" features across large datasets, we can deliver very accurate results.

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.

- CLOUD-BASED AND SCALABLE
- ZERO DAY THREAT PROTECTION
- INTEGRATES WITH SRX SERIES NEXT-GENERATION FIREWALLS
- INLINE BLOCKING
- UNIQUE DECEPTION AND PROVOCATION TECHNIQUES

and provocation techniques.

Thank you