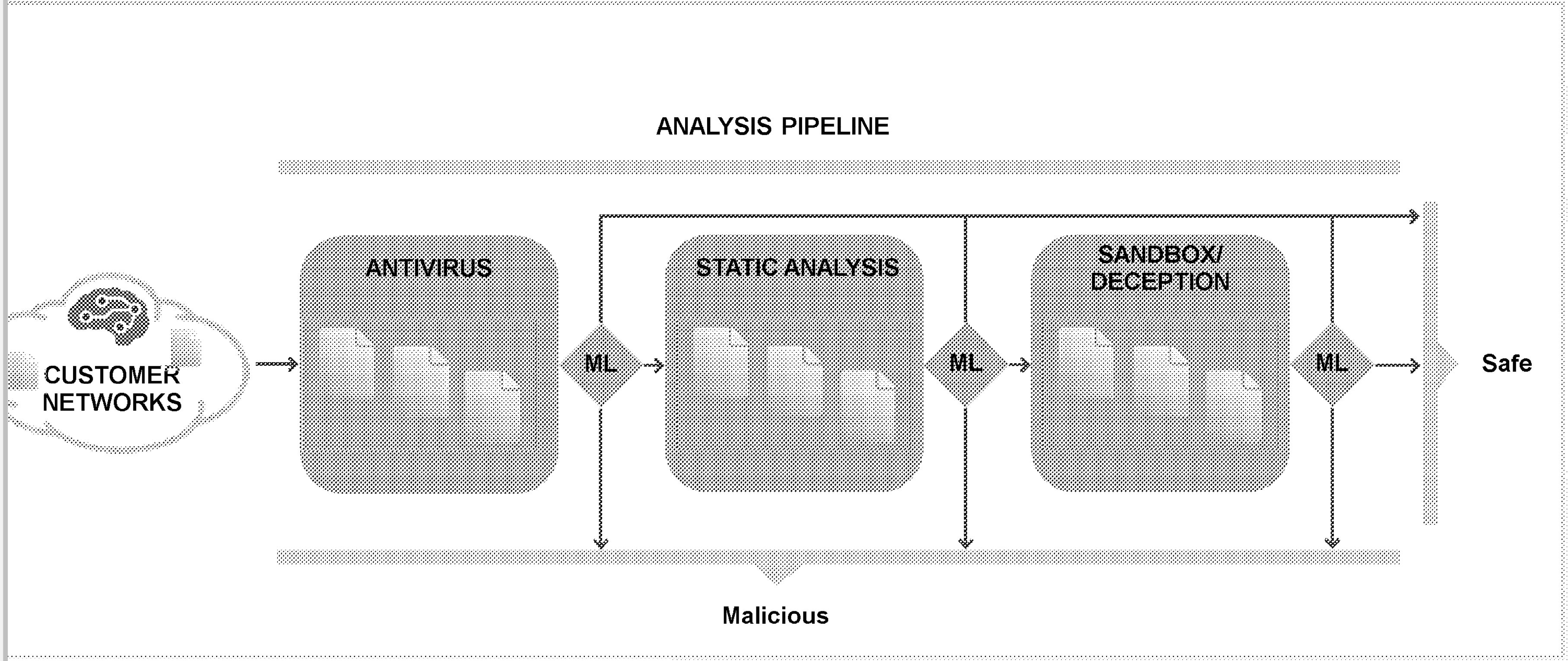
Sky ATP Analysis Pipeline



peaker Notes for Slide 1

), how does Argon use ML? What classification decisions are we making?

ssentially we want to decide, for each sample, whether it's malicious or not. We accomplish this by funneling samples through rgon's ANALYSIS PIPELINE. As samples flow through the pipeline, we process them in a number of ways to generate metadata hich helps us to classify the samples.

urrently samples can be analyzed by an antivirus adapter, two static analysis adapters, and a sandbox+deception adapter. Based on e metadata generated by these adapters our ML models form an estimate of the probability that a given sample is malicious.

owever, it costs us more the longer a sample remains in the pipeline since the latter stages take more time to compute, so we build L models which can try to classify a sample at each stage where new metadata is available. At each stage the VERDICT ENGINE ll basically say, "this is safe; stop scanning", "this is malware; stop scanning and block it", or "not sure; continue analyzing the imple."

Adapter flow

- The different 'adapters' produce results of varying fidelity.
- In order to deliver verdicts with high efficacy we build statistical models (ML) to interpret and combine the results at different stages of the analysis pipeline.
- This also allows us to optimize our resource usage: if we have enough evidence that a file is either malicious or benign at some intermediate stage of the pipeline we can '**early exit**' and save the cost of full analysis.

Antivirus Medley: all submitted file types

- Every submitted sample gets the AV treatment.
- We have a relatively simple model to interpret the results from 6 engines; the result is more or less that if a sample hits a couple trusted AVs (or several less trusted AVs) then we believe that it's malware.
- **Early exit**: If a sample is identified to be malicious by the AV adapter, further processing isn't strictly necessary.
- However, we may continue to analyze the sample in order to obtain more information either to inform the customer of the malware's behavior or for purposes of internal efficacy tracking/improvement.

Static Analysis: win7 exe; pdfs; doc[x]

- We use both internally-developed static analysis (fast) and vendor-sourced static analysis (slow, exe only)
- The results of the analyses are evaluated by ML models to determine (1) if a sample is so obviously malicious or benign that we can stop scanning it, or (2) if we should proceed to sandboxing.
- **Early exit**: If a verdict can be confidently determined at this stage, we may either mark the sample as 'done' or proceed to sandboxing anyway in order to collect additional information.
- We collect a large amount of information, including things like "this executable appears to contain code to make API calls secretly", or "this document contains obfuscated VBA”, but we do not provide this information to the customer.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**