


Kaspersky Non-Signature detection techniques

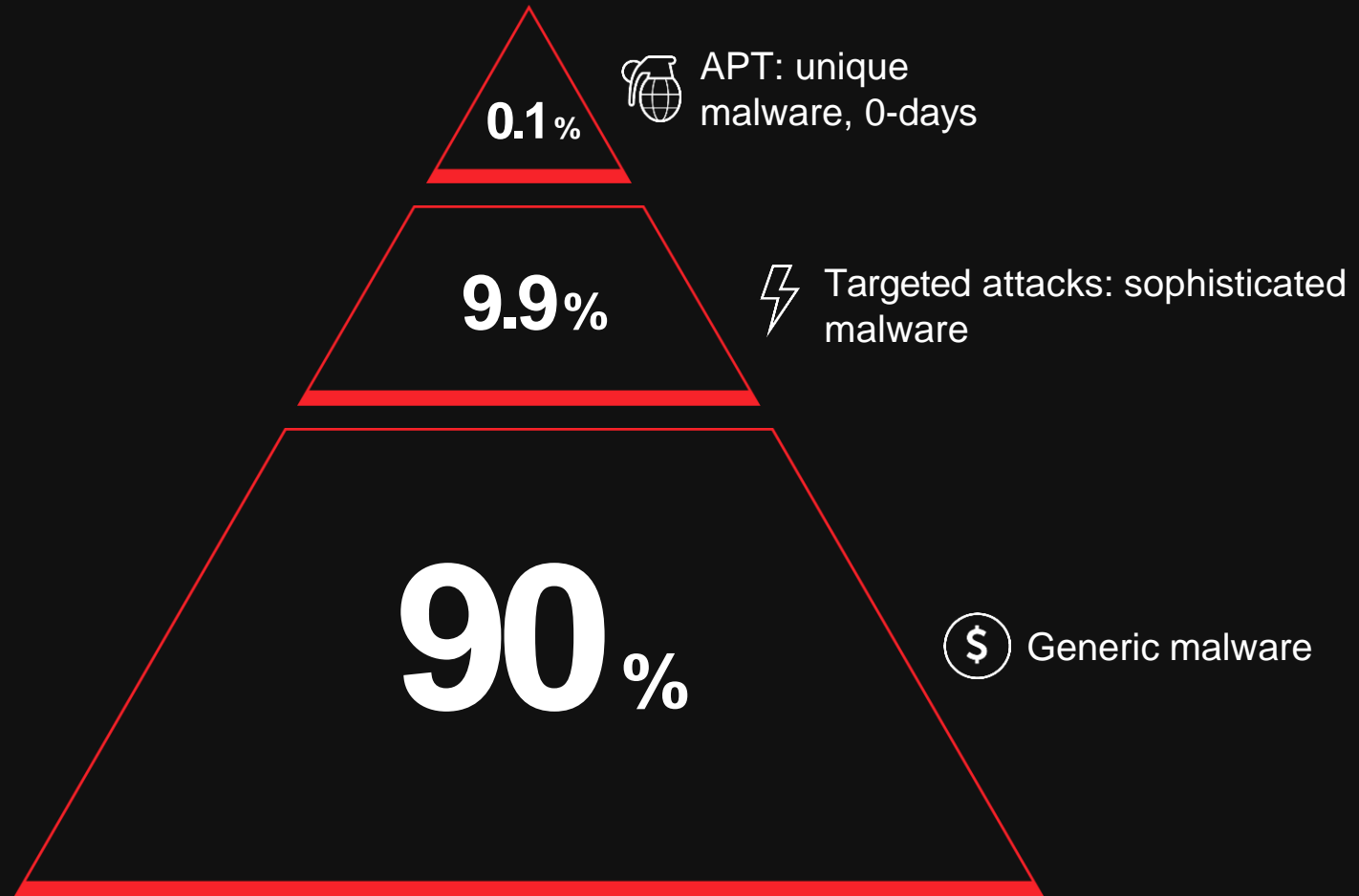
Alexey Malanov, malware expert, Anti-Malware Research



ANTIVIRUS SOFTWARE
1987-2014

I AINT DEAD YET!

Threats Today



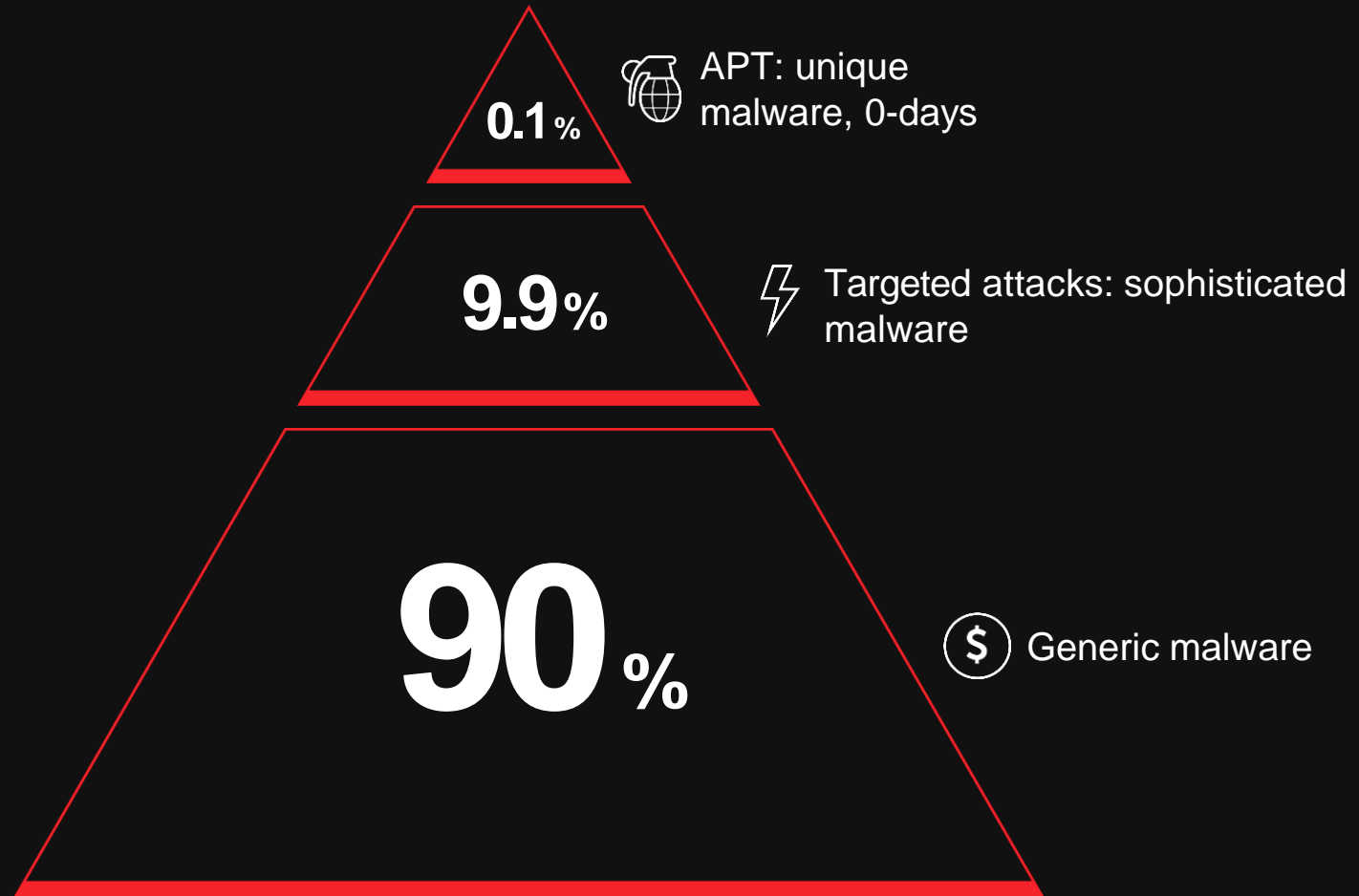
MULTILAYERED PROTECTION ON ENDPOINT

Threats are trying to pass

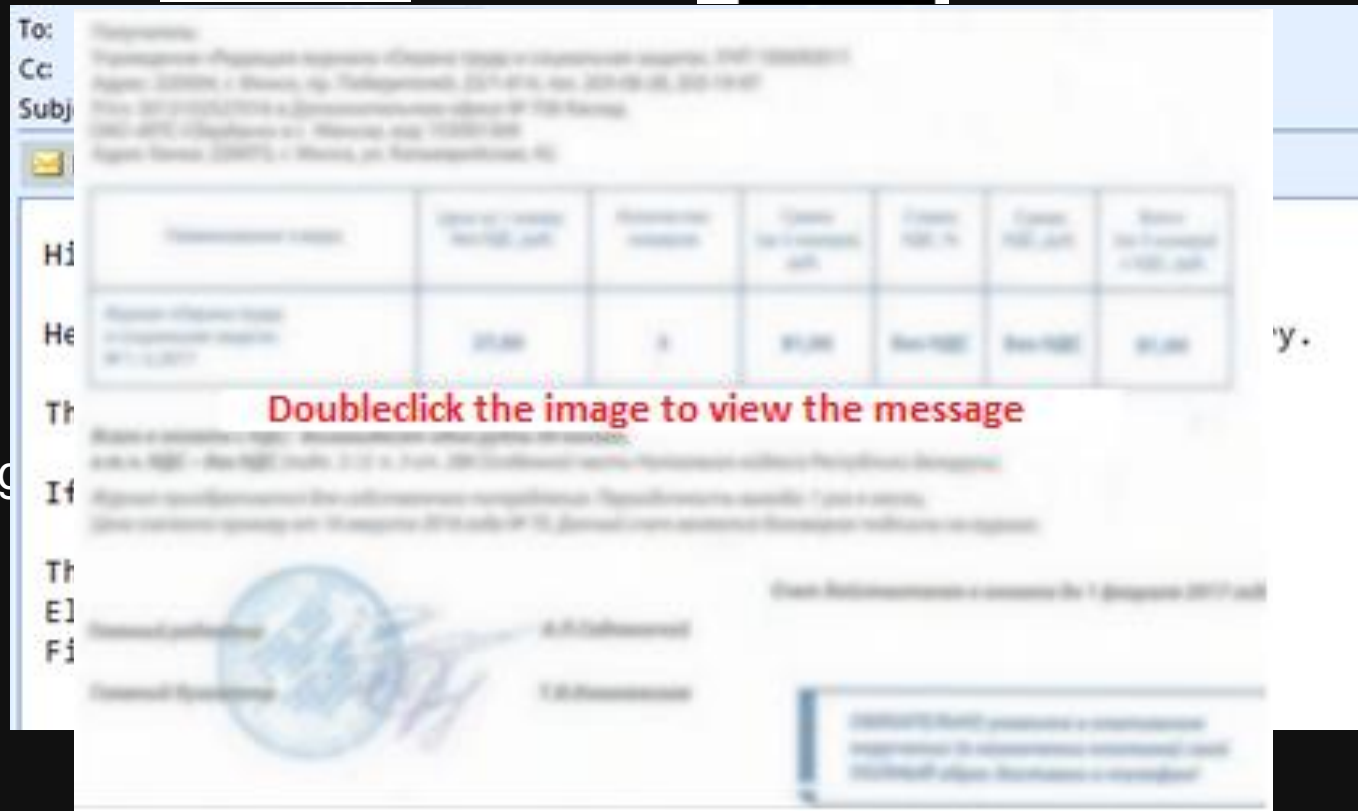


Targeted attacks

Threats Today



Modus Operandi Common ransomware infection (Trojan-Ransom.Win32.Scatter)

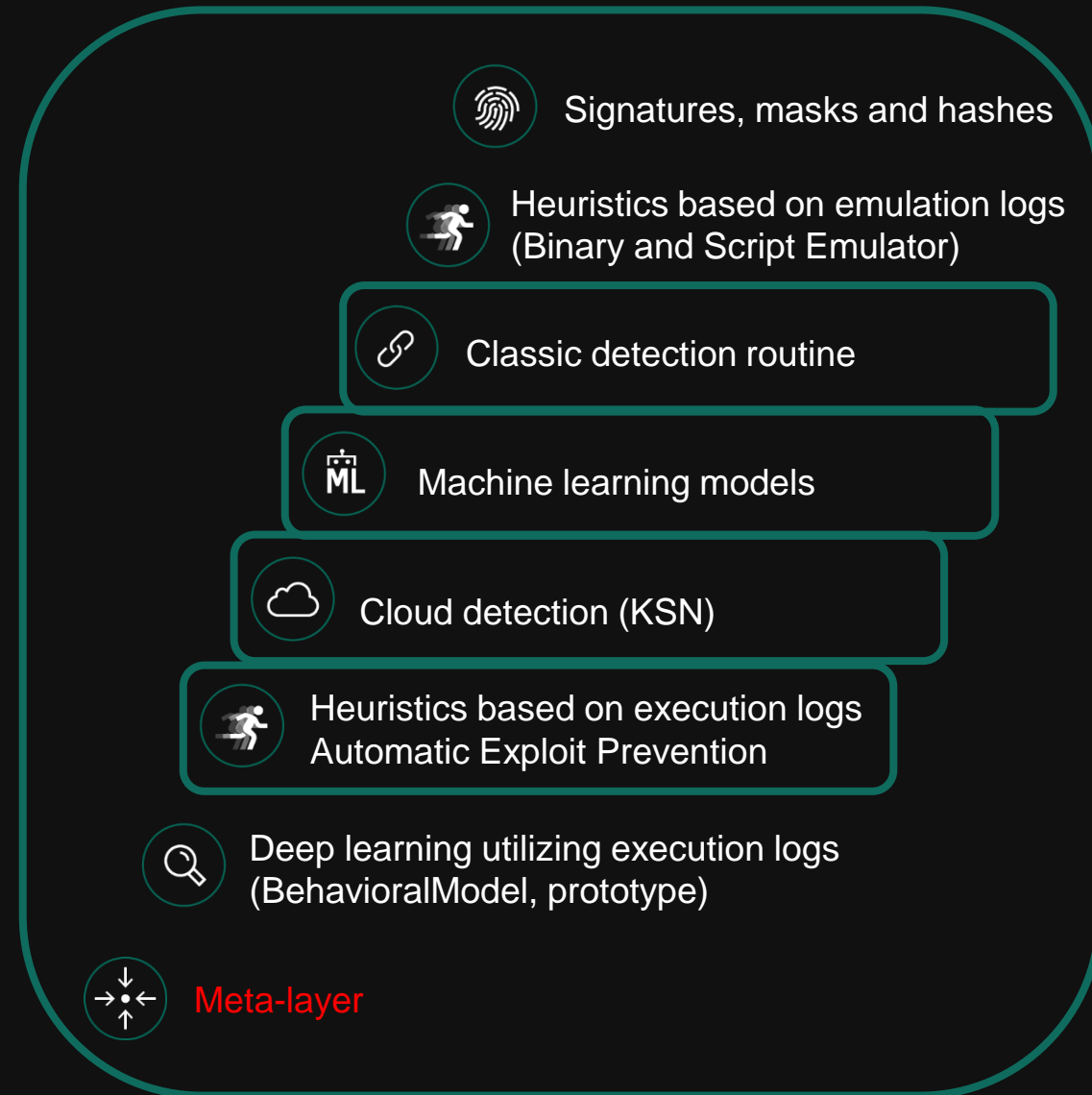


GnuPG

ate tool to encrypt files

META-LAYER – LAYERS SYNERGY

- Doc file with script inside arrived in email – channel is analyzed
- Legitimate file (GnuPG) downloaded – reputation and digital signature analyzed
- Connecting to C&C – domain reputation is analyzed
- The script and doc were never met before – files reputation is analyzed
- Script is obfuscated – ML-models say script is not bad, but not normal
- Deleting backup copies – not usual but still legitimate



FULL-SCALE DETECTION

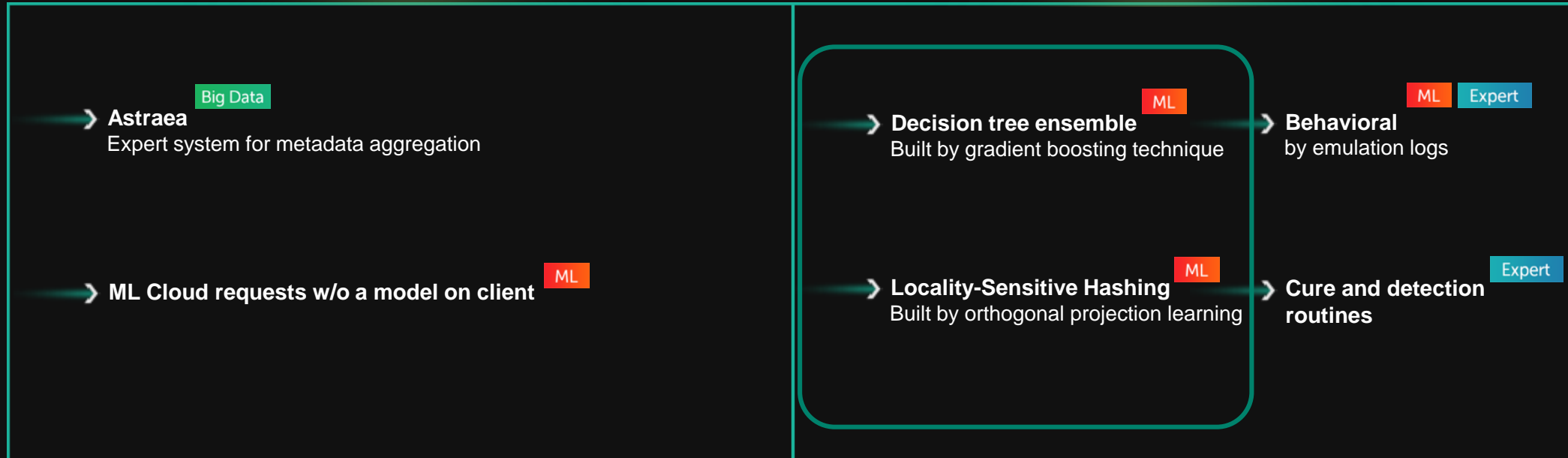
- A file was detected on execution stage in certain circumstances
 - Cloud detection (Kaspersky Security Network)
 - Accurate detection in bases
 - Emulator-based algorithmic procedure
 - ML models in bases
 - Cloud ML-detection
 - Behavioral model

Multilayered Machine Learning

Kaspersky Multilayered Machine Learning

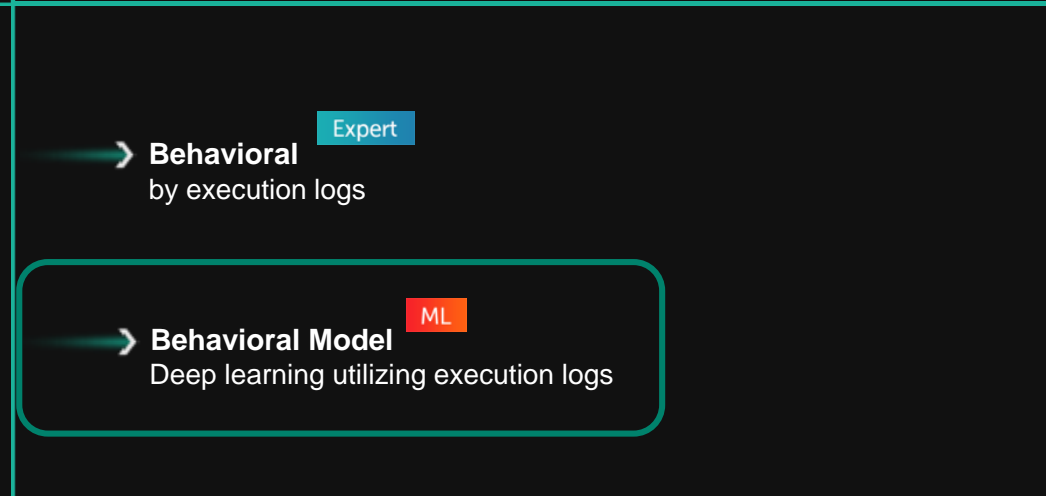
IN CLOUD

ON CLIENT



PRE EXECUTION

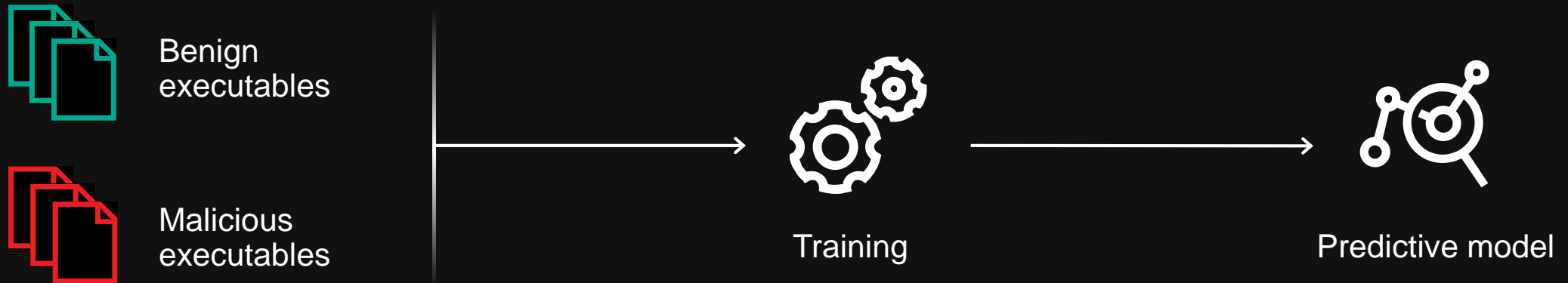
- ML** — Content is generated automatically by machine-learning techniques
- Expert** — Content is generated by experts
- Big Data** — Suspicious files' metadata from millions of endpoints collected and processed



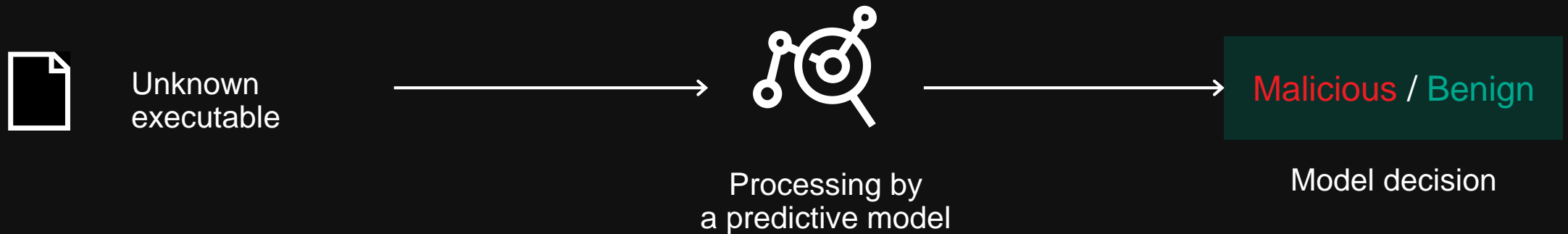
POST EXECUTION

Machine Learning: principles

Training phase



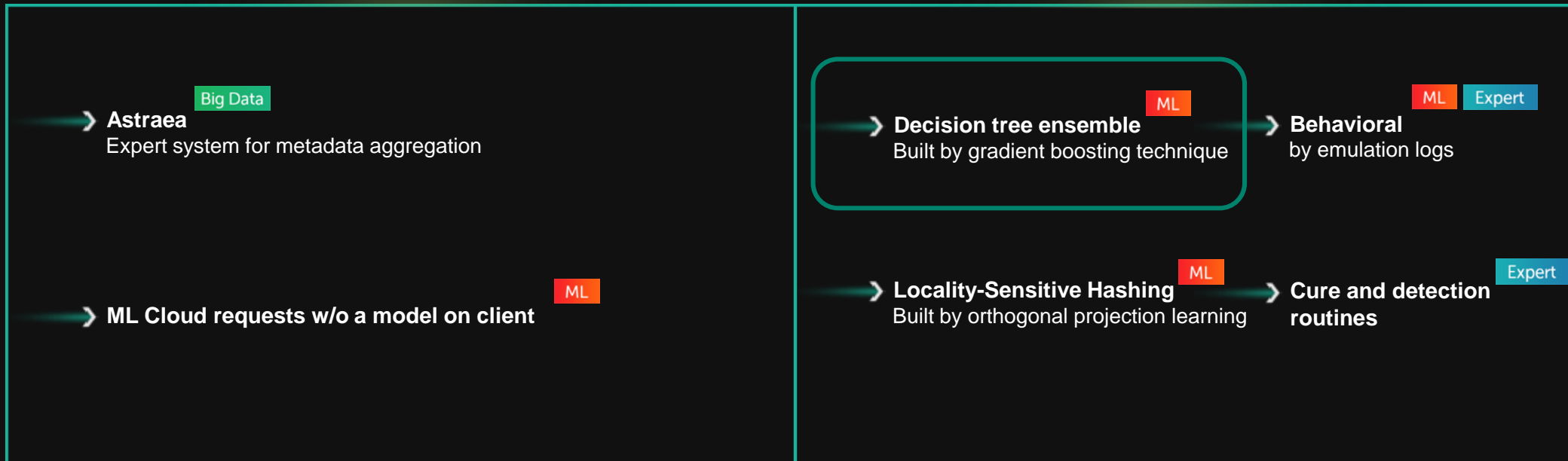
Protection phase



Kaspersky Multilayered Machine Learning

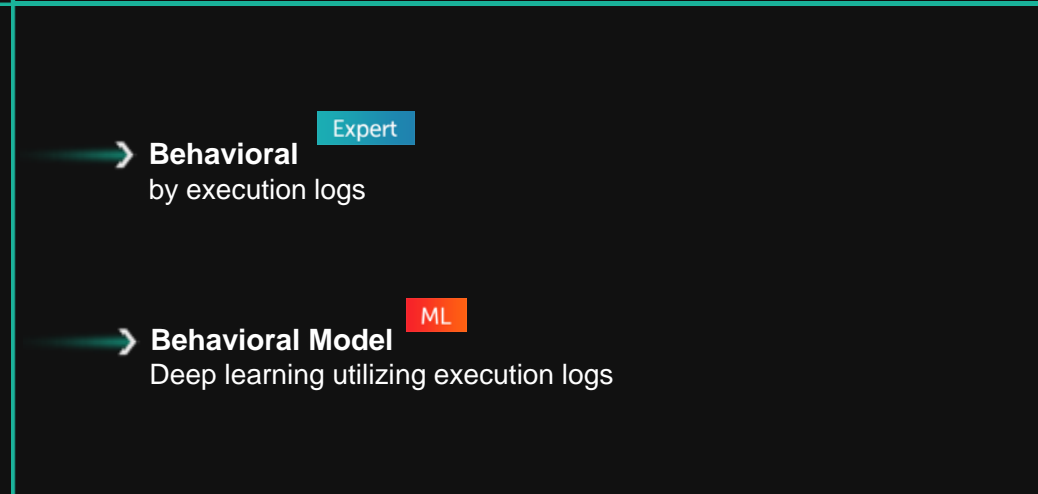
IN CLOUD

ON CLIENT



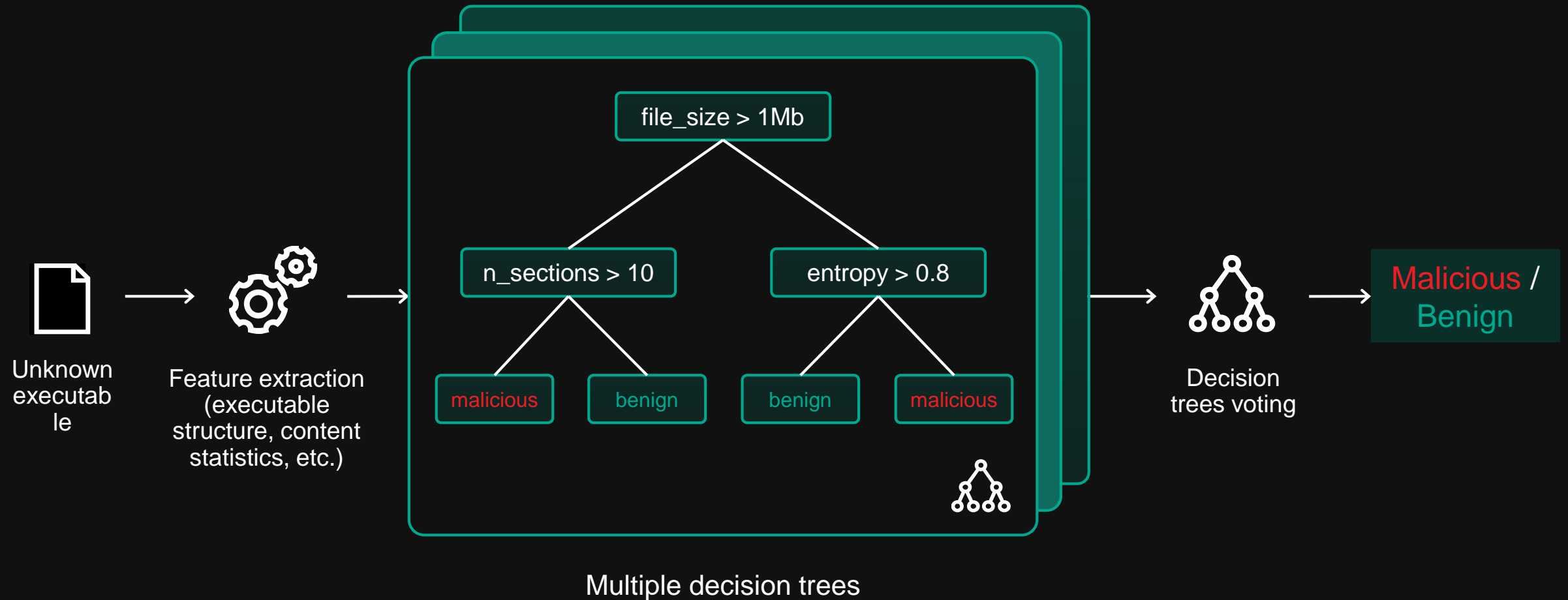
PRE EXECUTION

- ML** — Content is generated automatically by machine-learning techniques
- Expert** — Content is generated by experts
- Big Data** — Suspicious files' metadata from millions of endpoints collected and processed



POST EXECUTION

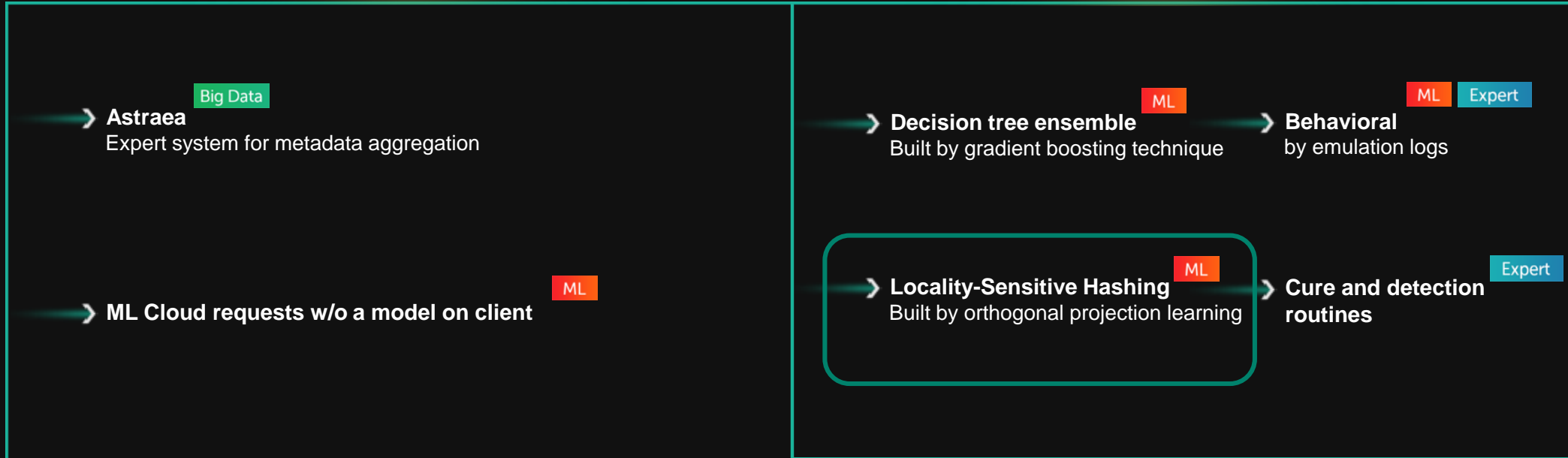
Machine Learning: decision tree ensemble



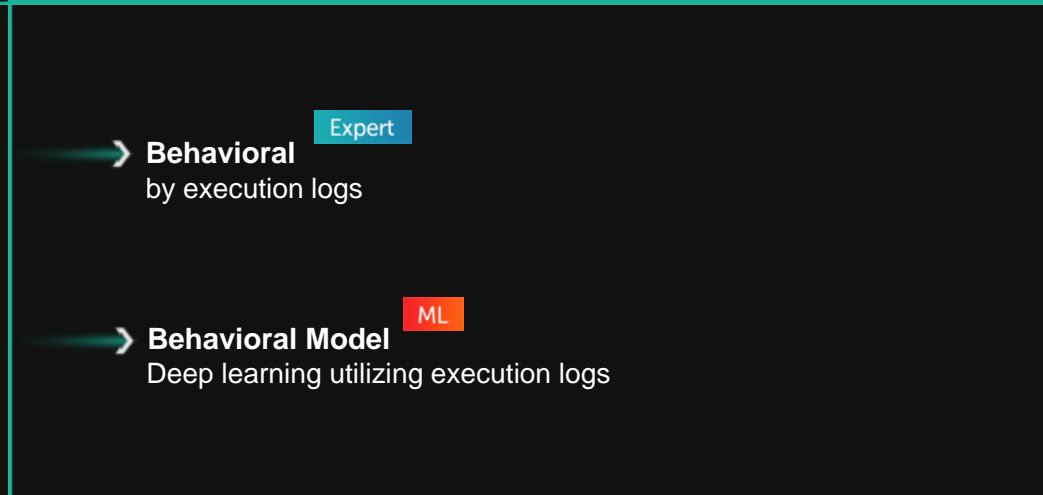
Kaspersky Multilayered Machine Learning

IN CLOUD

ON CLIENT



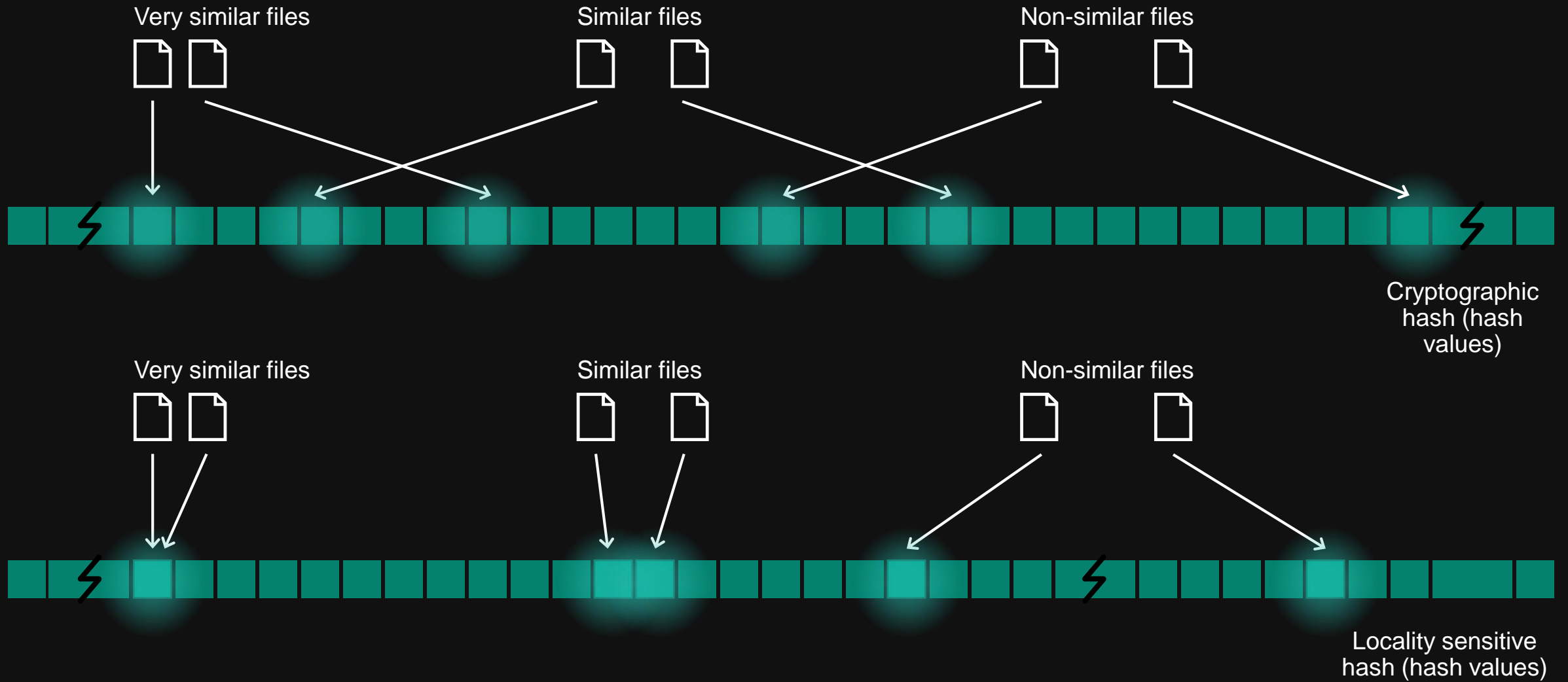
- ML** — Content is generated automatically by machine-learning techniques
- Expert** — Content is generated by experts
- Big Data** — Suspicious files' metadata from millions of endpoints collected and processed



PRE EXECUTION

POST EXECUTION

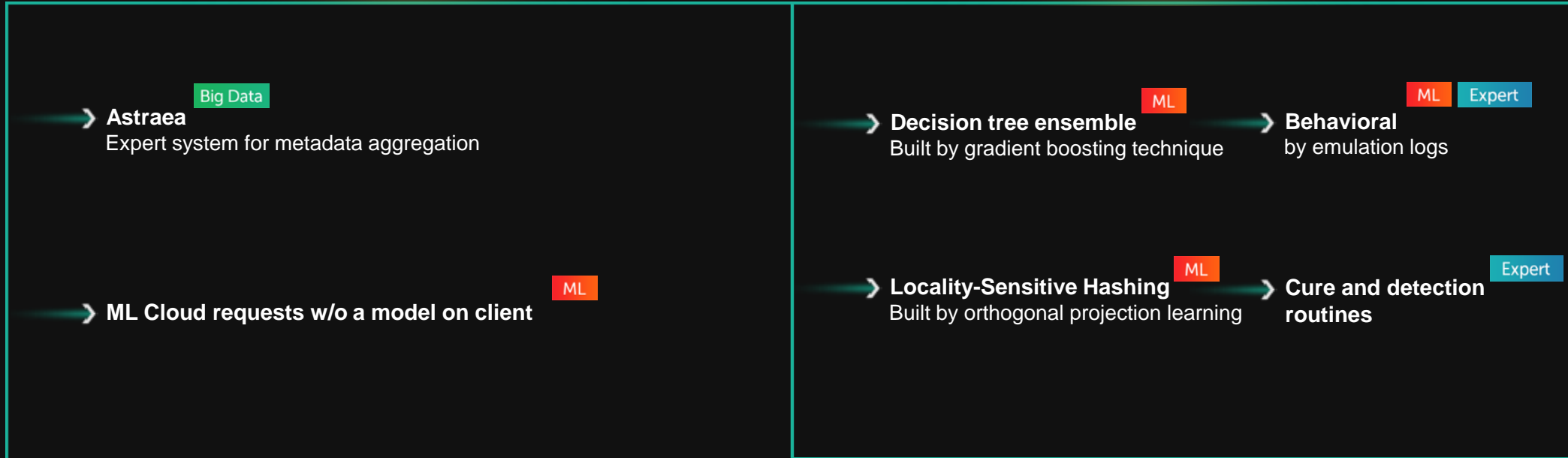
Machine Learning: locality sensitive hashing



Kaspersky Multilayered Machine Learning

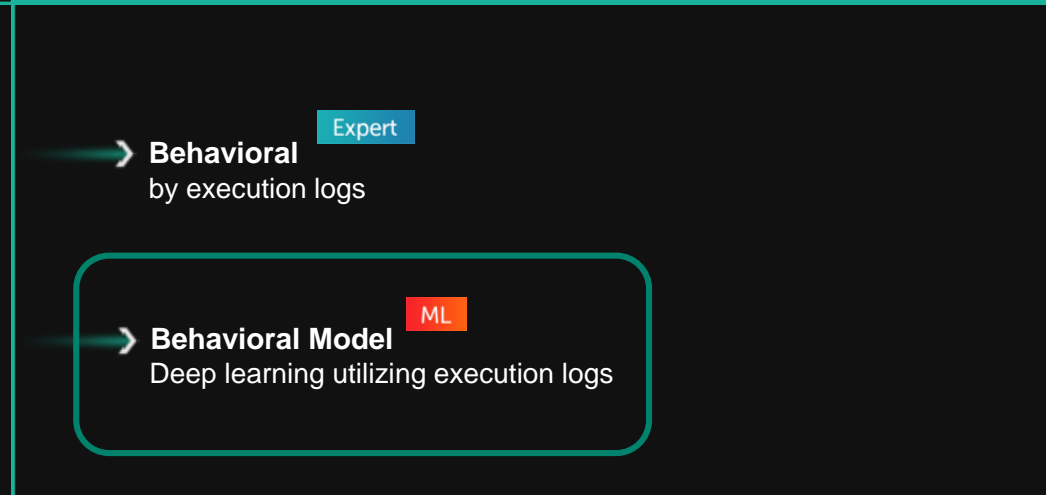
IN CLOUD

ON CLIENT



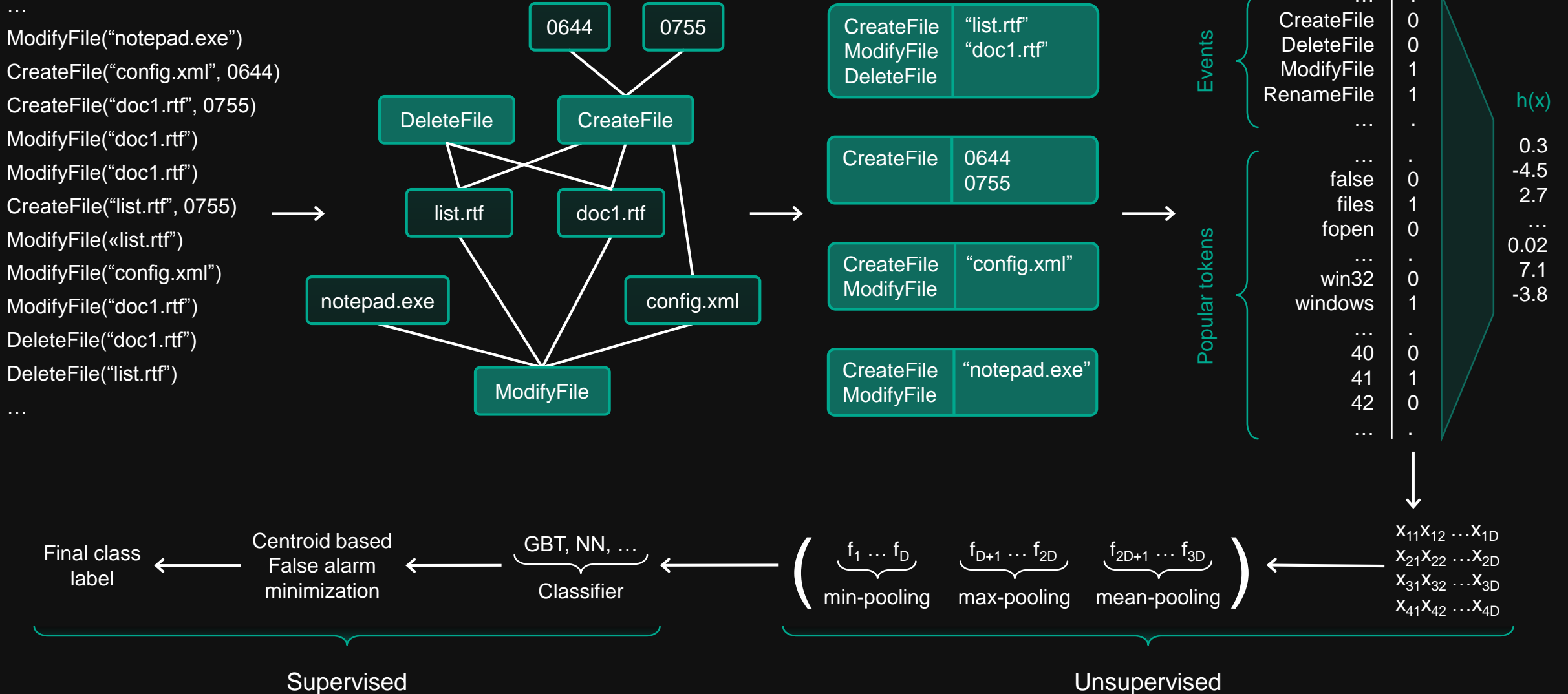
PRE
EXECUTION

- ML — Content is generated automatically by machine-learning techniques
- Expert — Content is generated by experts
- Big Data — Suspicious files' metadata from millions of endpoints collected and processed



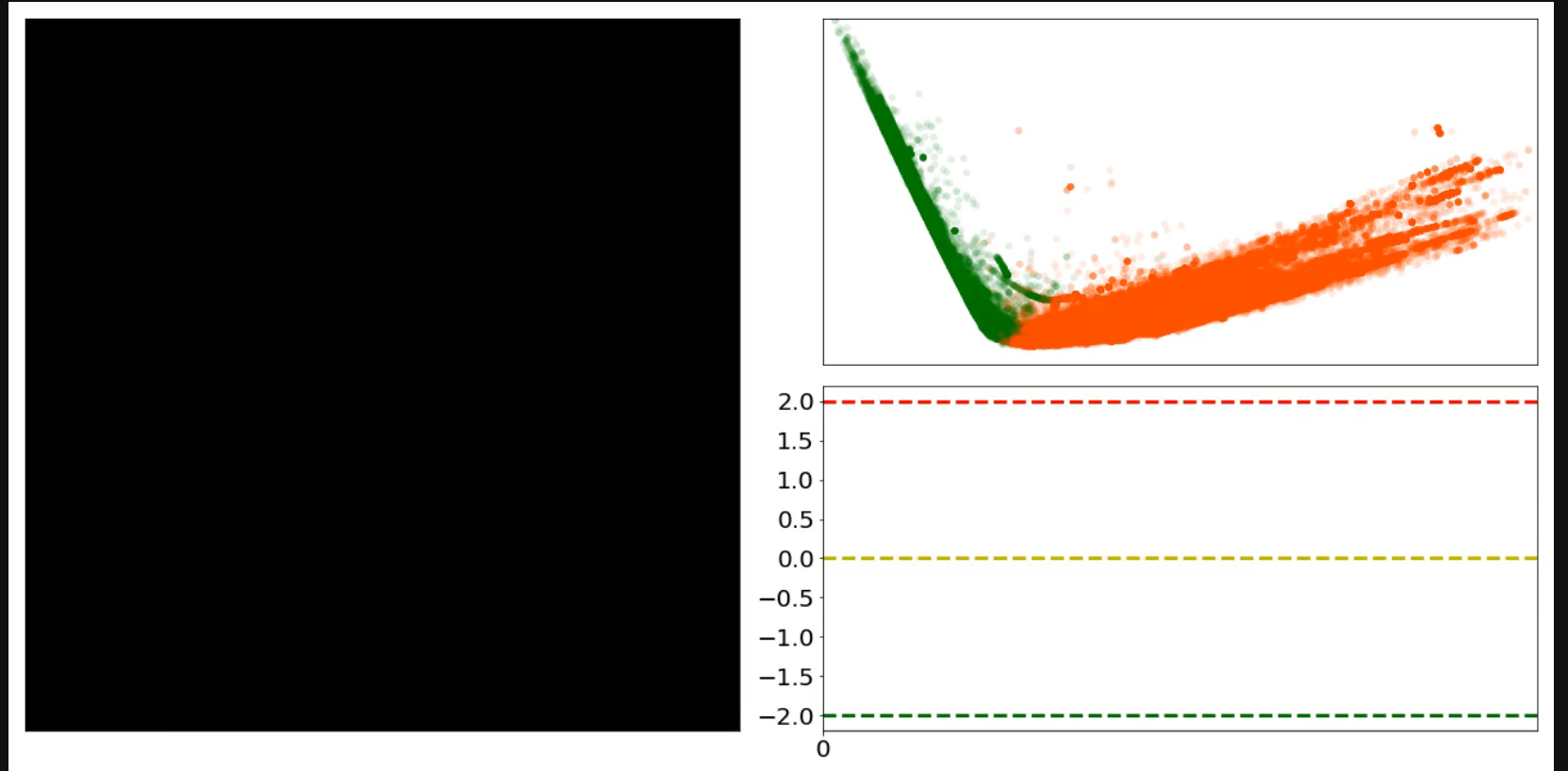
POST
EXECUTION

Machine Learning: behavior model pipeline



Behavioral Model in Action

- The Model is fed by process activity
- When the Model has reached an optimum level, it starts detecting
- level, it starts detecting
- Actions are rolled back



Fileless attacks

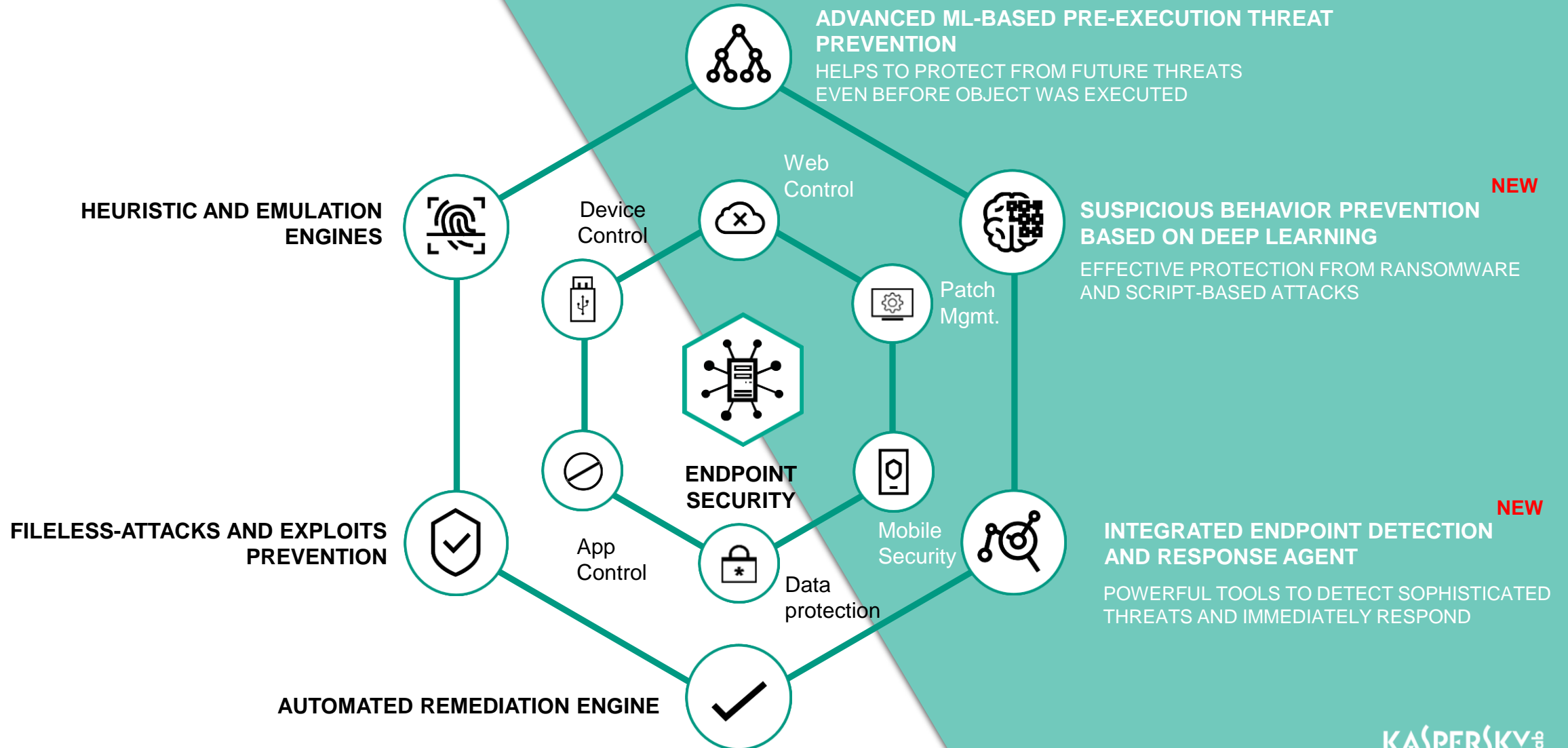
Typical Fileless Malware (RickyBobby APT from WikiLeaks Vault7)



- Victim has a task in Windows Scheduler
- Every 4 hours PowerShell script is executed by OS
- Script extracts DLL and loads it directly to memory

- Our product
 - Analyzes PowerShell script behavior
 - Notices executable being [System.Reflection.Assembly]::Loaded
 - Notices origin of such activity
 - Protects the user














Kaspersky Endpoint Security 11 + Detection + Response



ADVANCED CYBERSECURITY TECHNOLOGIES

Next Generation technologies and Multi-Layered approach form the foundation of our high-profile solution to protect consumer and business from any type of cyber attacks

www.kaspersky.com/TechnoWiki

 Machine Learning in Cybersecurity ML-based technologies are used in both products and infrastructure.	 Kaspersky Anti Targeted Attack Platform (KATA) Kaspersky Anti Targeted Attack Platform (KATA) protects against targeted attacks.
 Behavior Based Protection Behavior Monitoring with Memory Protection provide the most efficient way to protect against advanced threats and zero-day malware.	 Automatic Exploit Prevention (AEP) Automatic Exploit Prevention (AEP) protects against malware that takes advantage of software vulnerabilities.
 Fileless Threat Protection Fileless threat does not store its body directly on disk and requires special attention from security solutions	 Ransomware Protection Ransomware protection on both delivery and execution stages by technologies from Multi-layered protection stack
 Multi-layered Approach to Security Multi-layered approach allows effective protection against different types of malware.	 Big data - The Astraea Technology Expert system Astraea produces detection of malicious objects through processing of big data
 Anti-Rootkit And Remediation Technology The technology detects active infection by rootkit programs and remediates systems from this type of infection.	 Kaspersky Security Network (KSN) The Kaspersky Security Network (KSN) processes cybersecurity-related data and ensures fastest reaction time to new threats
 Emulator Code emulation for malware detection in Kaspersky Lab solutions	 Sandbox Running on premise, in the cloud and in Kaspersky Lab infrastructure.
 Online banking - the Safe Money technology Safe Money technology protects online critical operations.	



Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY 