AI and Endpoint Protection

Matthias Canisius
matthias.canisius@mac.com

September, 2018

Detection Flow – High Level

Known Malware
As written to disk

Static AI
ML-based detection (On-write and on-access)

Behavioral AI
ML and Logic driven detection
of any executed attack

Threat Hunting and IR
Full context real time search for IOC

Reputation → Static AI → Behavioral AI → Deep Visibility

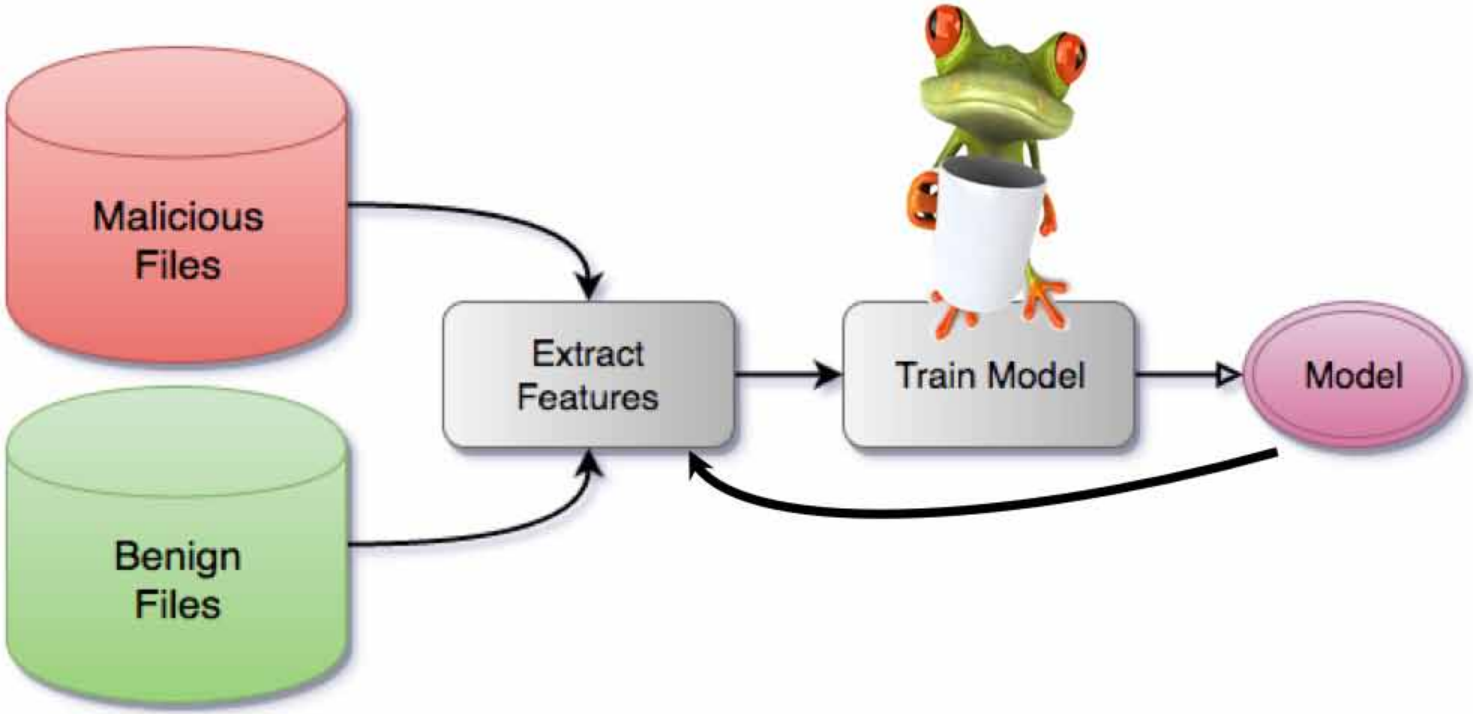
- Ransomware
- Lateral Movement
- Active Content (Docs)
- Interactive sessions
- Frameworks
- Exploits
- File-less Attacks

Static AI Engine

Problem

- Classify file as malicious / benign
- Do it fast for pre-execution, < 100ms
- Detect unseen / novel malware

Machine Learning Overview



Data Set

- Millions of malicious / benign files
- Constantly acquiring more from variety of sources
  - Threat feeds
  - Software distribution sites
  - Problematic software

Feature Extraction

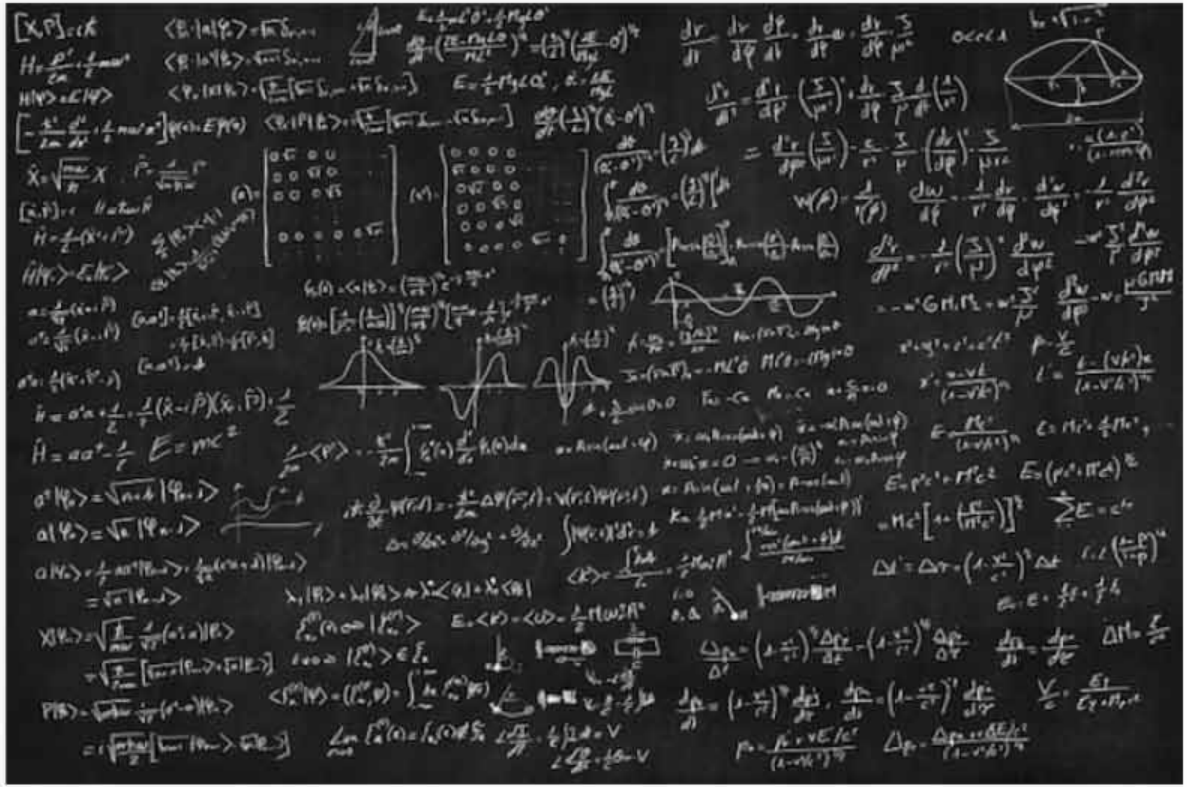
PE Features

- Number of sections
- Imports
- Exports
- Opcodes
- Section entropy
- Crypto constants
- Many more …

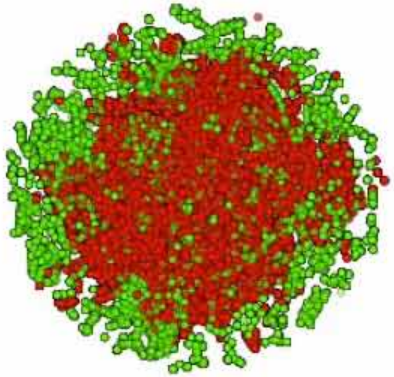
Macro Features

- Code entropy
- Comment entropy
- Uses CallByName
- Uses Xor operator
- Uses Shell
- AutoExec methods count
- Many more …

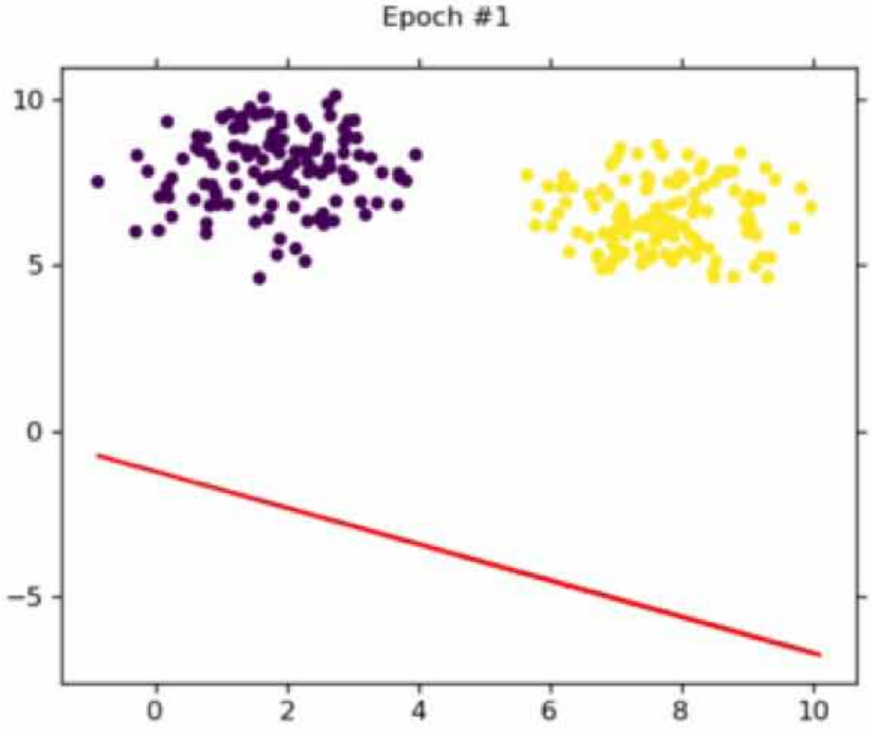
Complex Mathematics



Training a Model – The Real World

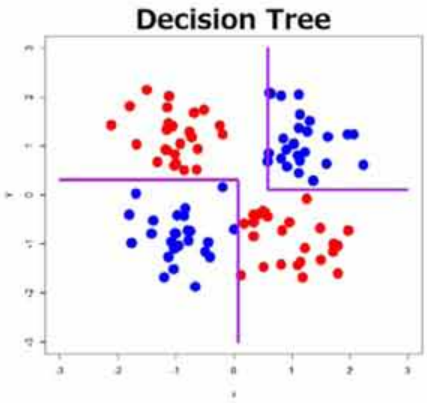


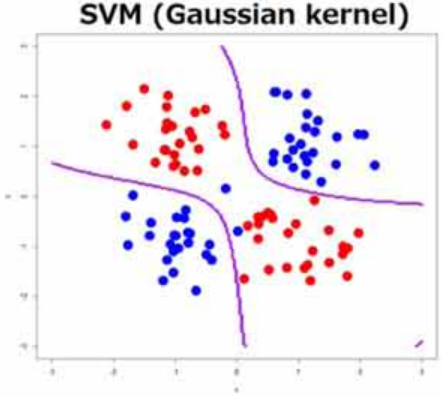
Training a Model - Simple Use-Case

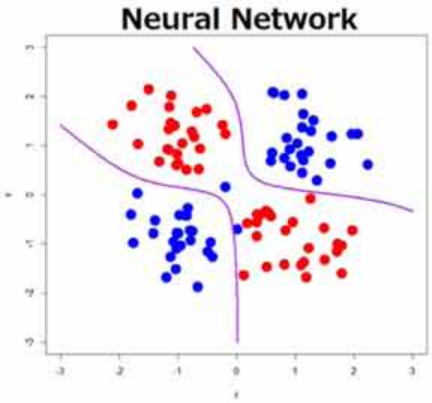


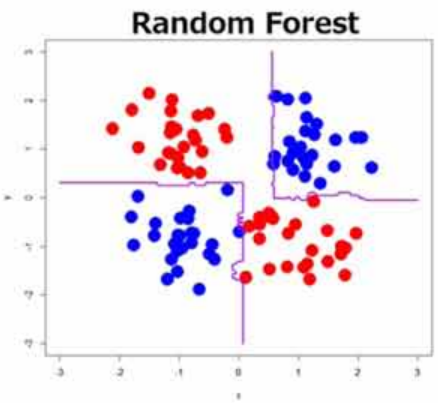
Machine Learning (ML) Classifiers

It's a classification challenge: Malware yes or no!

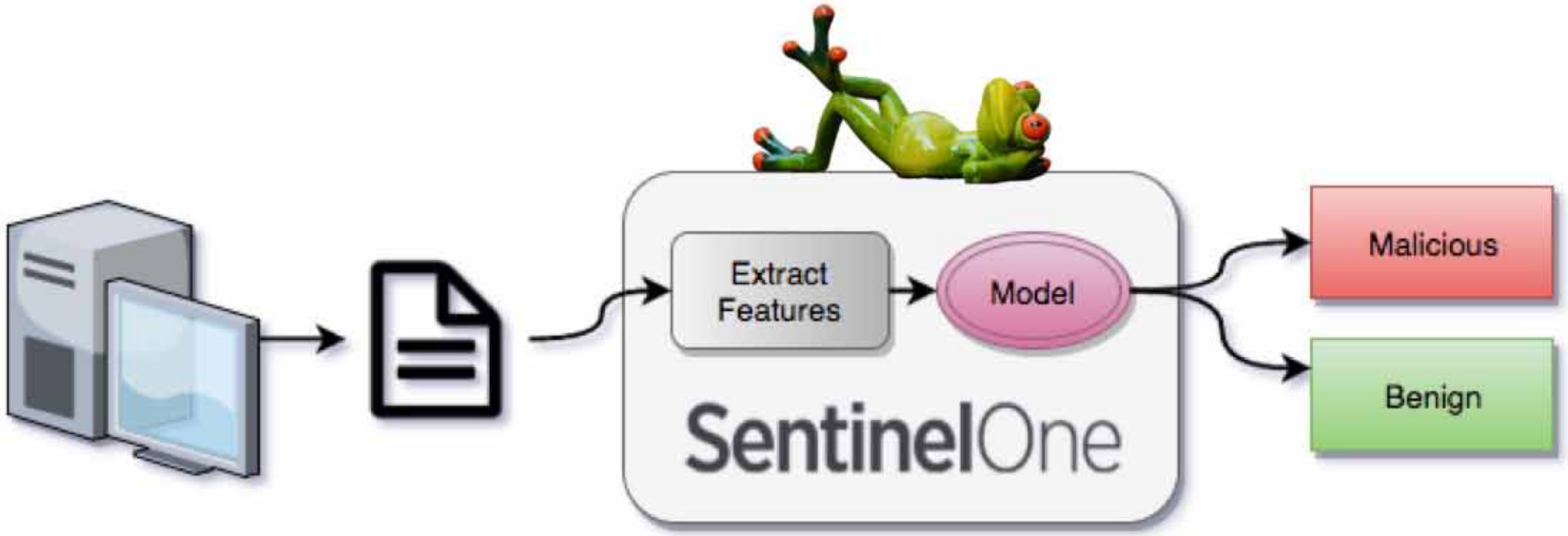








Our Solution



Behavioral AI Engine

Problem

- Classifying execution context to either threat or benign based on its behavior while running

- Monitors OS events
  - Many (hundreds)
  - Windows-Internal
  - Some undocumented

- Linking between behavior to maliciousness

Behavioral AI Engine

Behavioral Logic

Monitoring atomic OS-events

Translating to broader behavioral context

Classification based on observed behavior

- Injections
- Ransom behavior
- Persistency
- Remote Shell
- Exploit
- Lateral movement

Supervised Learning

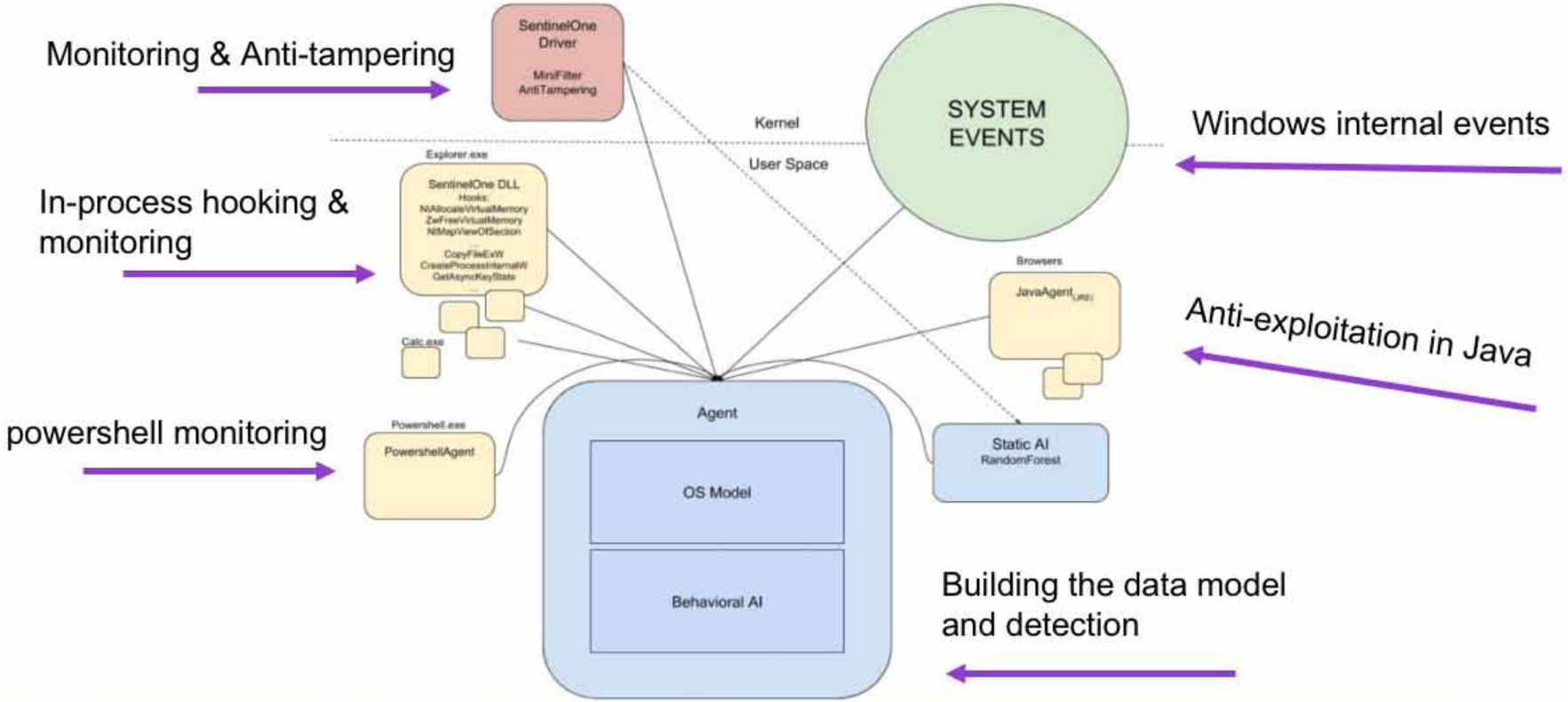
Running millions of files

Monitoring OS-evens and behaviors

Trained SVM

SVM-based classification

Architecture



What OS-Events are Collected?

SentinelOne

Detection Capabilities

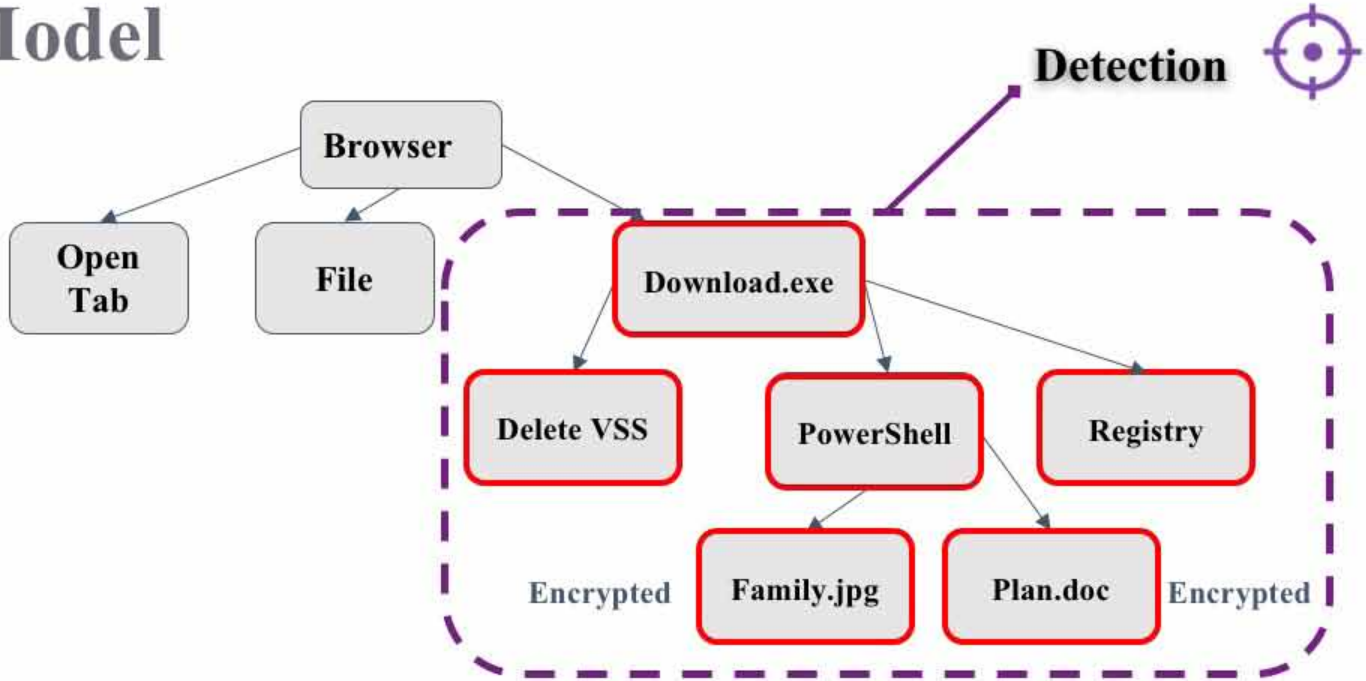
- System manipulations
  - UAC bypass
  - Code injections
  - Persistency
  - Ransom behaviors
  - Information stealers
  - Passwords stealing
  - Keyloggers
  - Remote Shell
  - Lateral movements
  - Process Hollowing
  - Anti debug / Anti VM
  - Doppelganger
  - Hiding attempts

- Known Attack frameworks
  - Meterpreter
  - Empire
  - Shinobot
  - Koadic
  - Mimikatz
  - Powersploit
  - PowerUp

- Exploits
  - Stack Pivot
  - Java exploits
  - Shellcodes
  - Sandbox escape
  - Malicious documents
  - Privilege escalation exploits
  - ROP

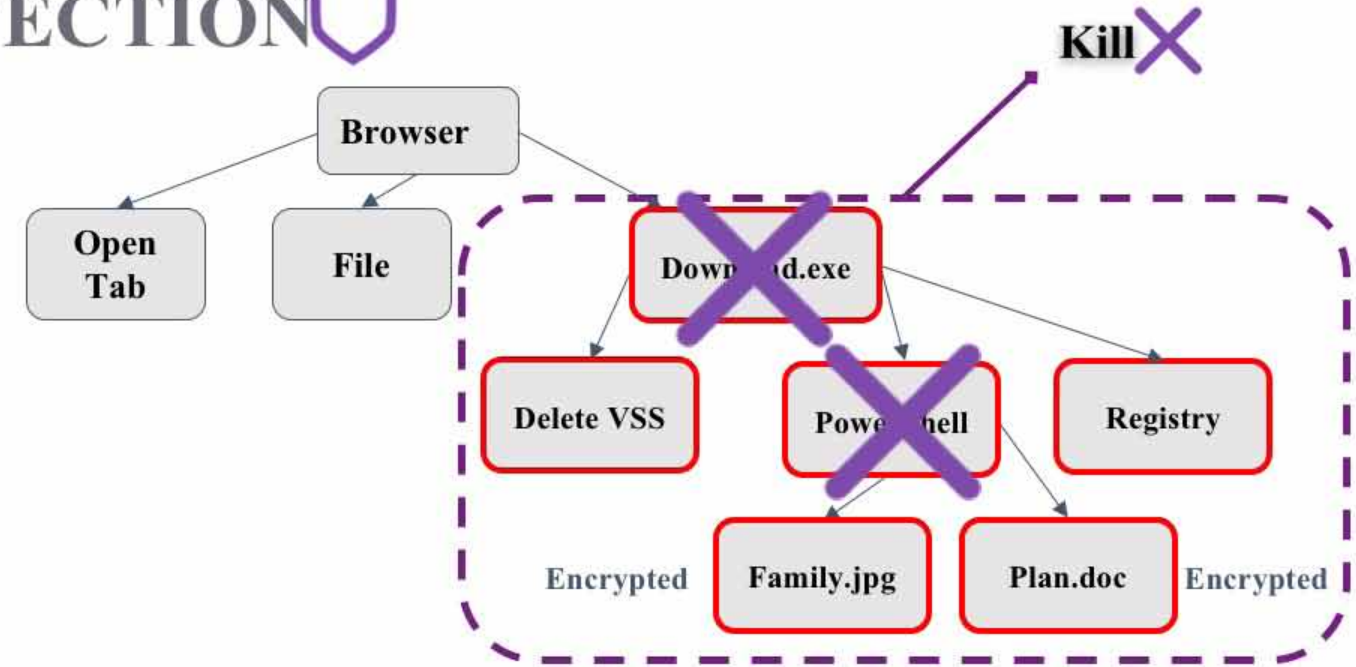
Mitigation Approaches

Data Model

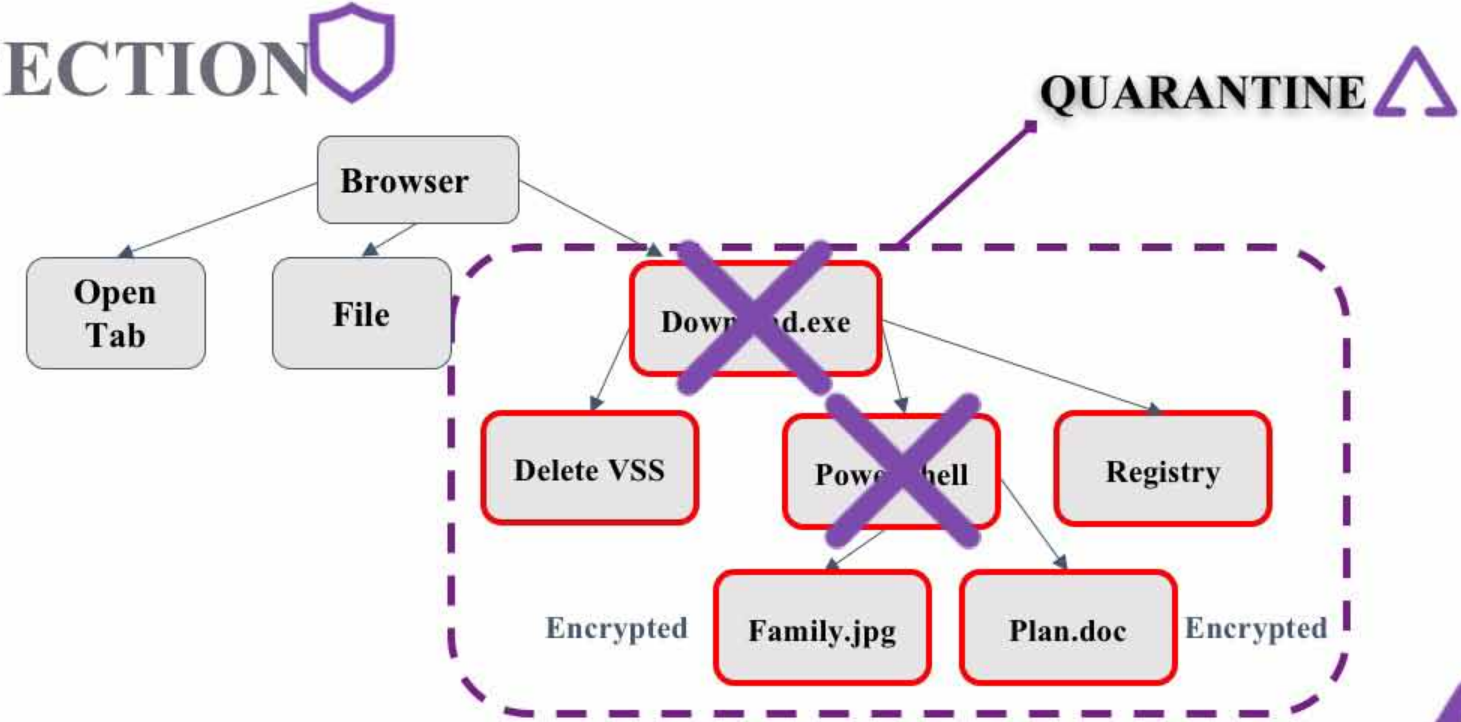


SentinelOne unique data model capability
Enables Dealing with complicated OS flows (APC, RPC, Remote Threads etc.)

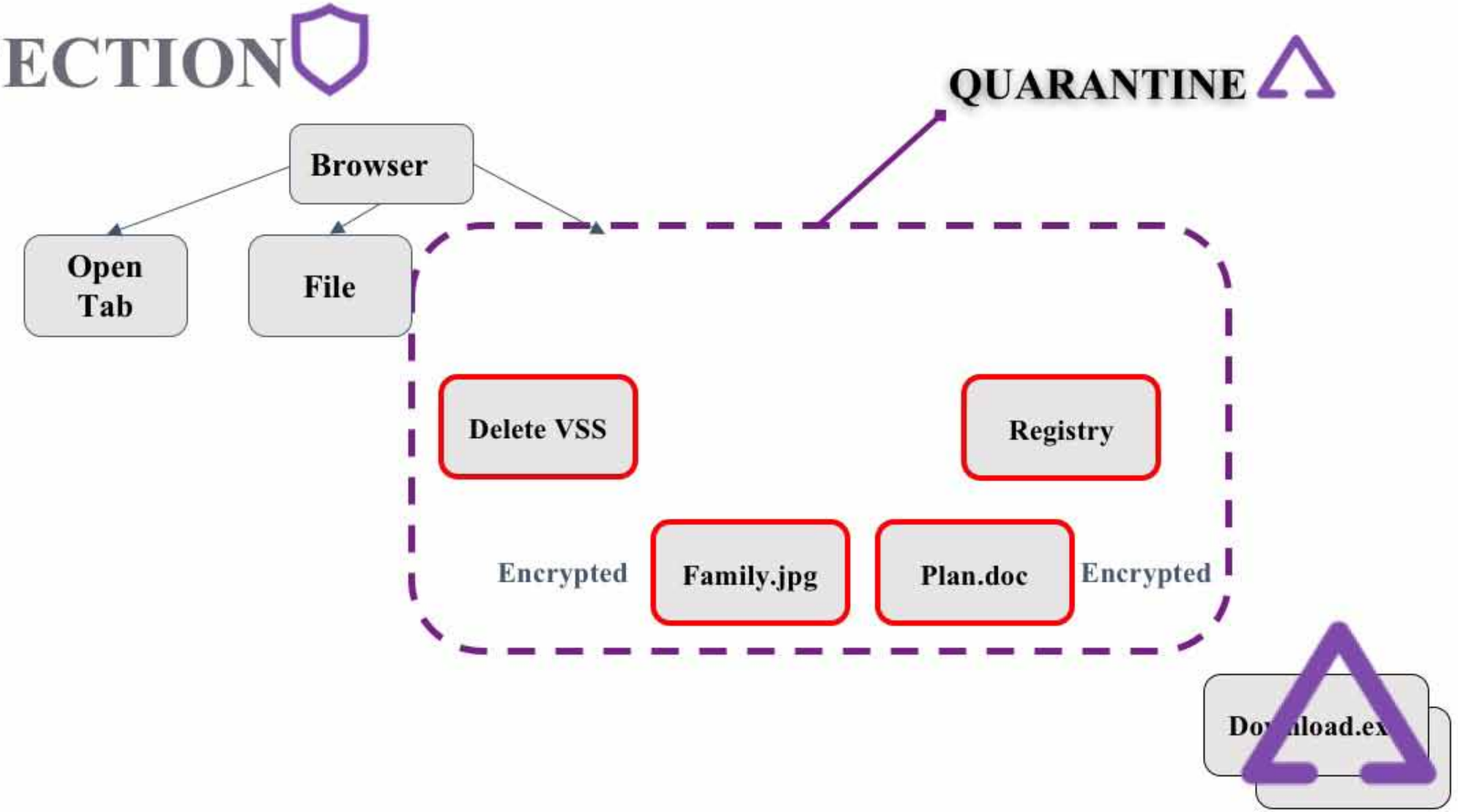
PROTECTION



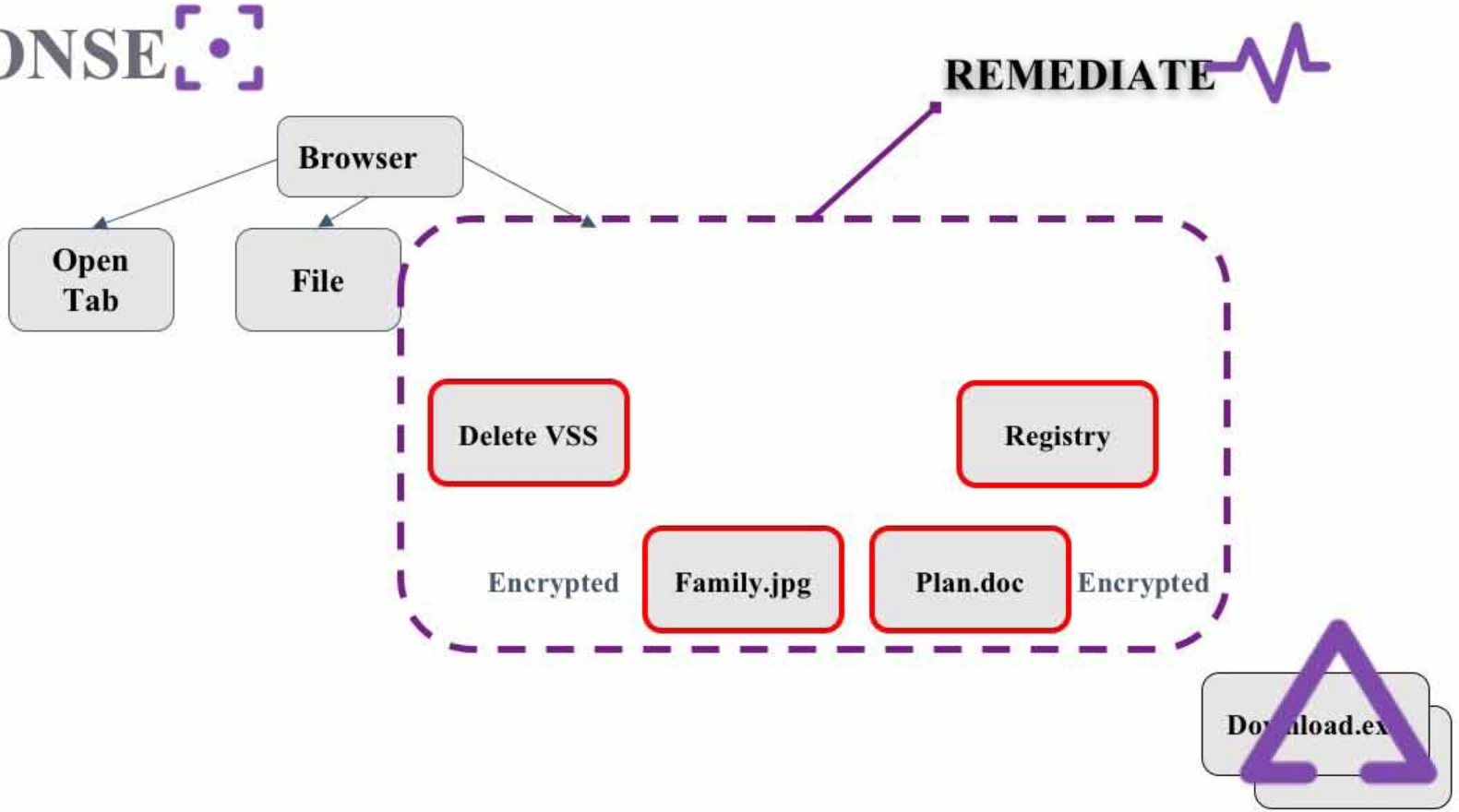
PROTECTION



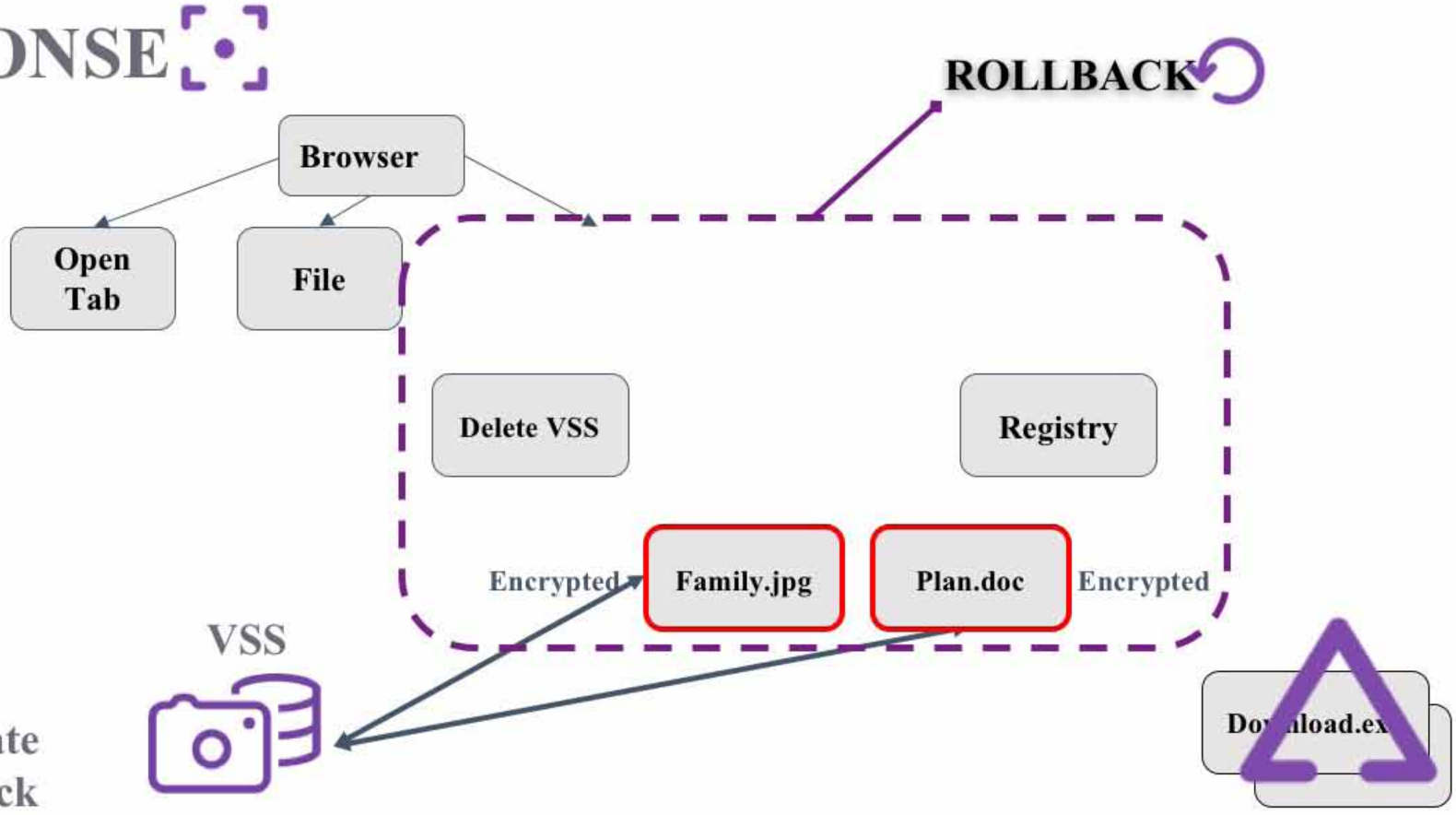
PROTECTION



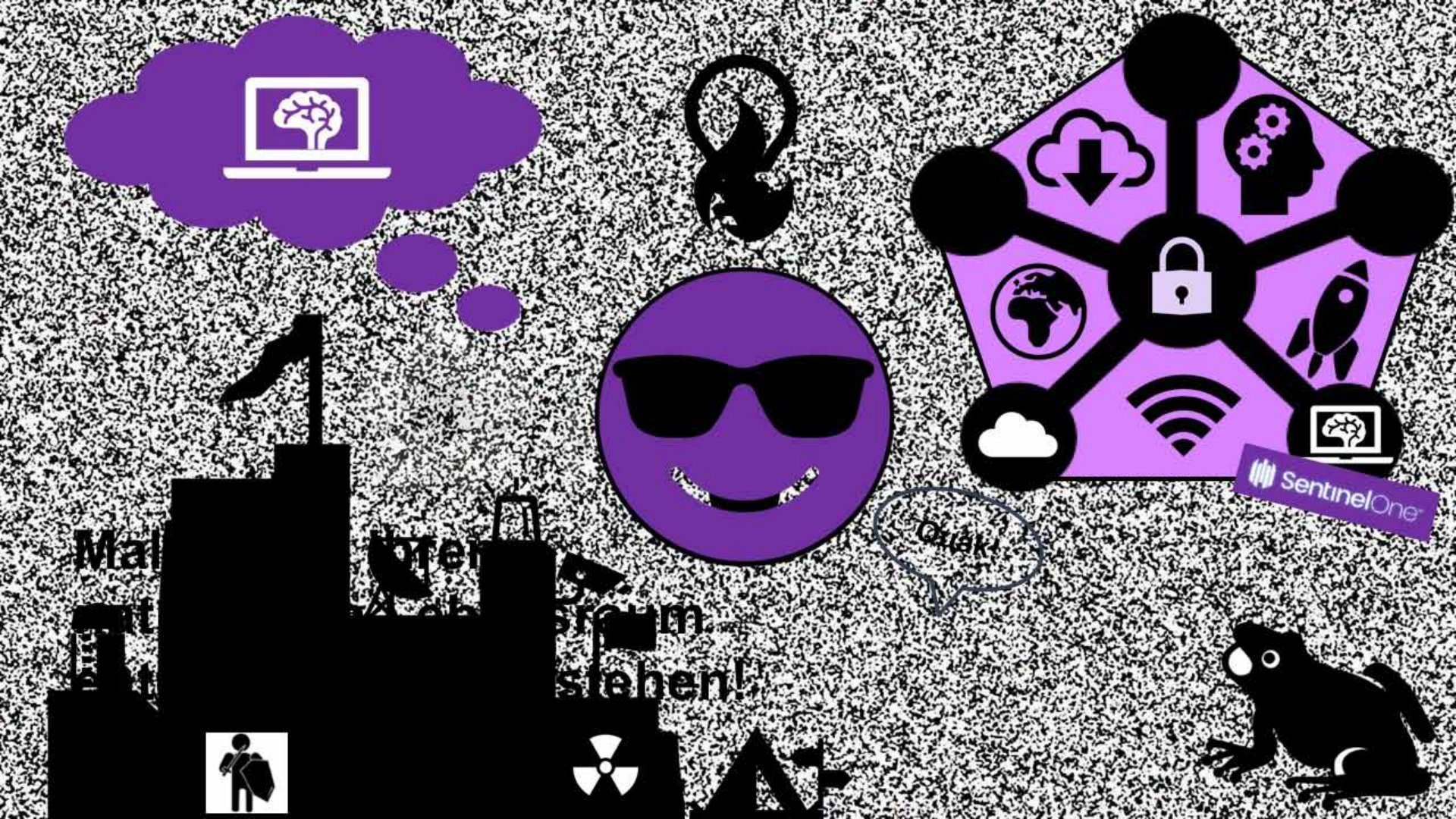
RESPONSE

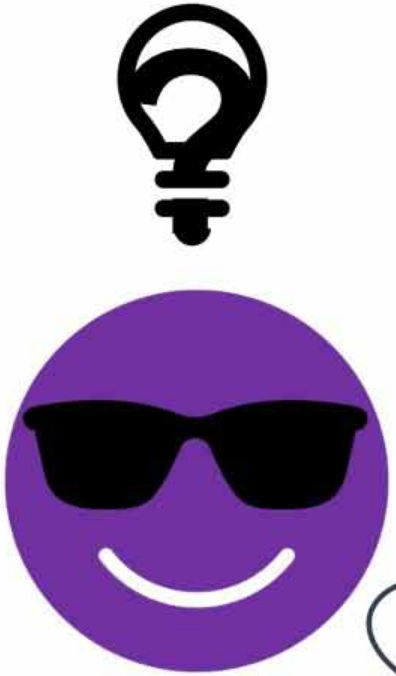


RESPONSE




SentinelOne™
Advanced
Endpoint
Protection


SentinelOne
Quak!



Malware in ihrem natürlichen Lebensraum entdecken und verstehen!

Step by step...

SentinelOne

BEFORE

Static AI

Prevent attacks pre-execution

DURING

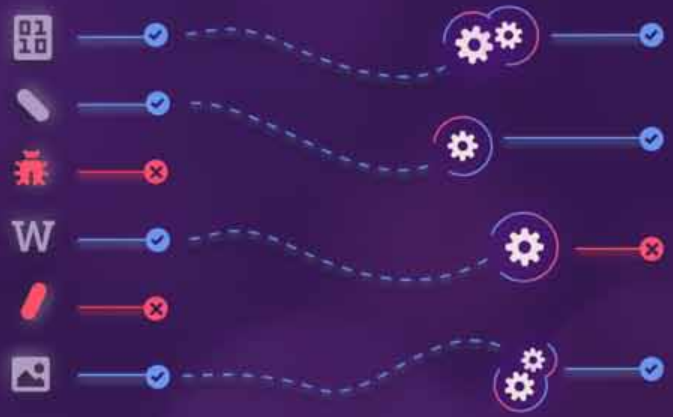
Behavioral AI

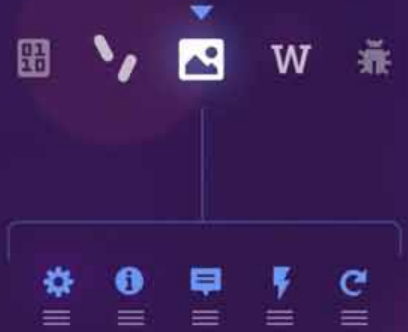
Constantly monitor and map each running process for incongruous behaviors

AFTER

Automated EDR

Automate remediation and response...even rollback





Advanced Endpoint SECURITY

Endpoint Protection

Ein Agent!

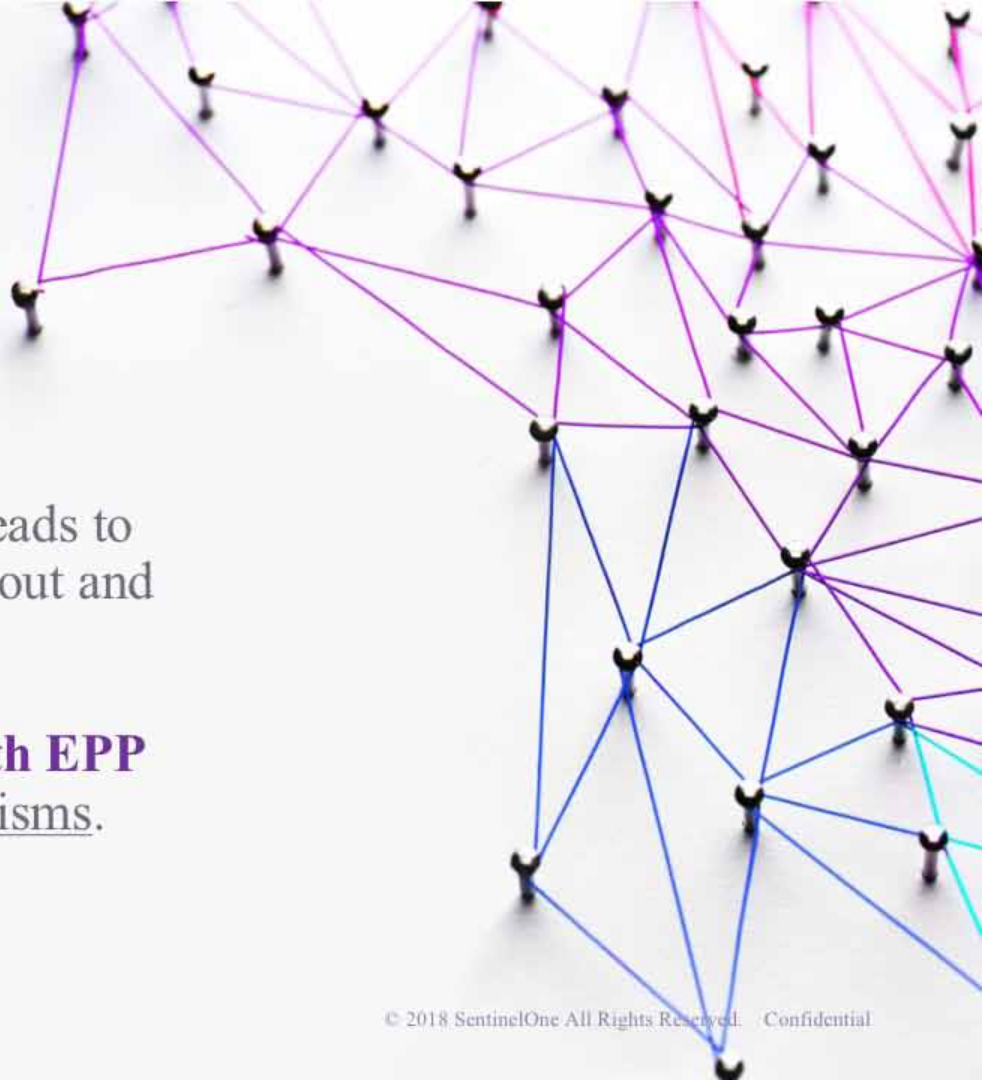
Endpoint Detecton & Response (EDR)

SentinelOne

Vigilance Automated SOC Services

Why ONE solution?

- **Strong Protection** leads to less incidents and lets the SOC focus on real advanced threats.
- **Having EPP + EDR in one agent** leads to less operational overhead, easier rollout and maintainance (TCO).
- **Having EDR deeply integrated with EPP** leads to automated response mechanisms.



2x3 gute Gründe ...

Agent

- Intelligenz auf dem Endpunkt
- Ein schlanker Agent (Mac, MS, Linux)
- Detect & Response (EDR)

Management

- On premise, cloud oder hybrid
- Mandantenfähigkeit
- Integrierbarkeit (API)

... SentinelOne einmal genauer anschauen!

SentinelOne


Live Demo!
Und jetzt?
SentinelOne™


SentinelOne™
Thank You