



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

The background is a dark, deep blue space filled with numerous small, glowing particles in shades of purple, blue, and pink. Some particles are larger and more prominent, while others are tiny specks. In the upper left corner, there are several thin, white, curved lines that resemble orbits or paths. The overall effect is that of a complex, dynamic system or a futuristic digital environment.

Static AI Engine

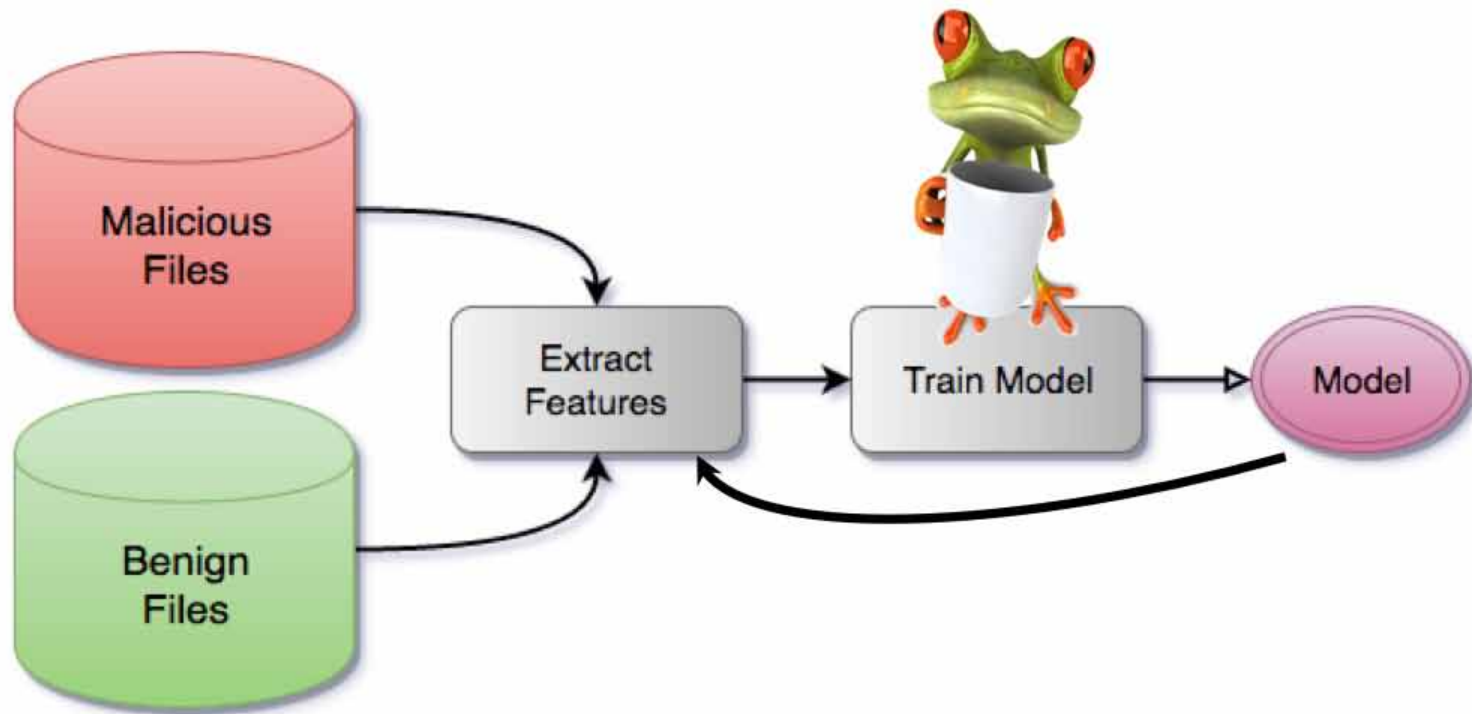
Problem



- 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 ...

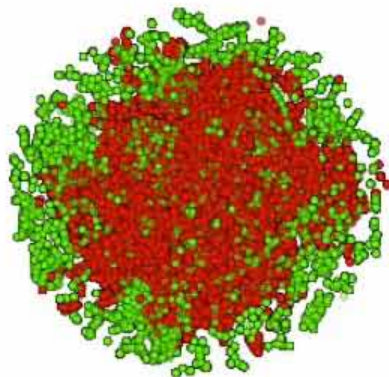


Complex Mathematics

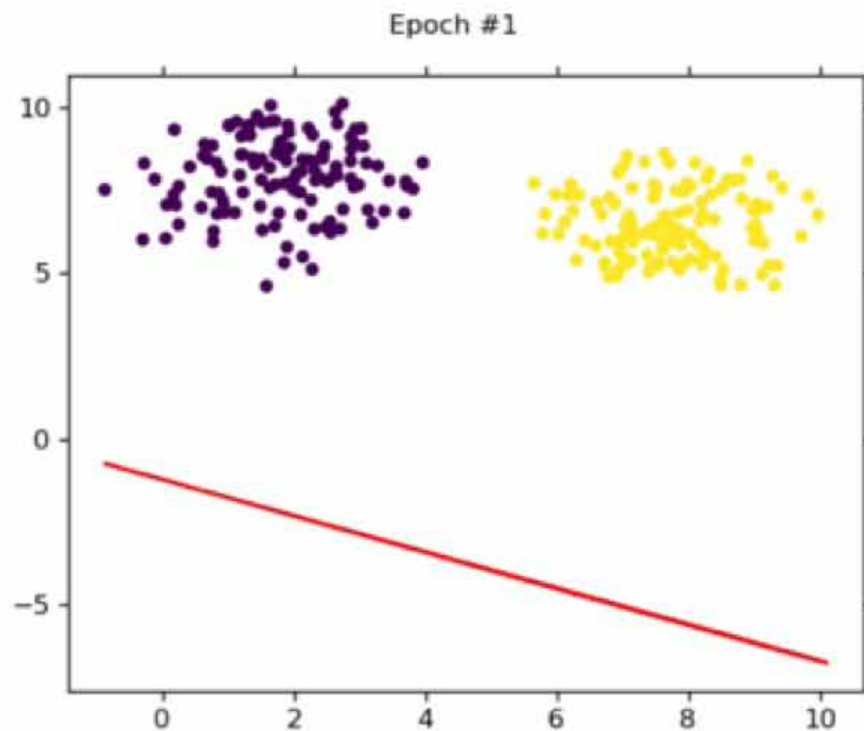
Handwritten mathematical notes covering various topics in quantum mechanics and complex analysis, including:

- Wavefunctions and Normalization:**
 - $\langle X | \Psi \rangle = \int \Psi^* X \Psi dx$
 - $\langle E | \Psi \rangle = \int \Psi^* H \Psi dx$
 - Normalization conditions: $\int |\Psi|^2 dx = 1$
- Probability and Expectation Values:**
 - $\langle X \rangle = \int X |\Psi|^2 dx$
 - $\langle E \rangle = \int \Psi^* H \Psi dx$
 - Variance: $\sigma^2 = \langle X^2 \rangle - \langle X \rangle^2$
- Complex Analysis and Derivatives:**
 - Derivatives of complex functions: $\frac{d}{dz} \left(\frac{z}{z^2} \right) = \frac{1 \cdot z^2 - z \cdot 2z}{z^4} = \frac{z^2 - 2z^2}{z^4} = \frac{-z^2}{z^4} = -\frac{1}{z^2}$
 - Integration: $\int \frac{1}{z^2} dz = -\frac{1}{z} + C$
- Diagrams and Plots:**
 - A diagram of a circle with a horizontal chord and a vertical line from the center to the chord, illustrating geometry.
 - Graphs of wavefunctions and probability densities.
- Other Mathematical Expressions:**
 - $\langle X^2 \rangle = \int X^2 |\Psi|^2 dx$
 - $\langle E \rangle = \int \Psi^* H \Psi dx$
 - $\langle X \rangle = \int X |\Psi|^2 dx$
 - $\langle E \rangle = \int \Psi^* H \Psi dx$
 - $\langle X \rangle = \int X |\Psi|^2 dx$
 - $\langle E \rangle = \int \Psi^* H \Psi dx$

Training a Model – The Real World



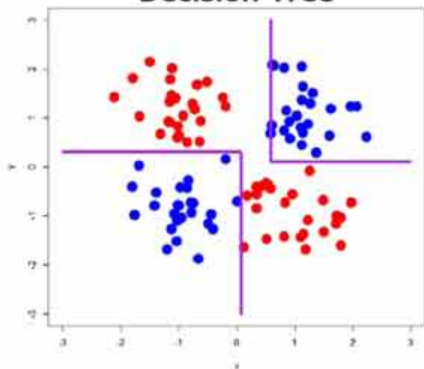
Training a Model - Simple Use-Case



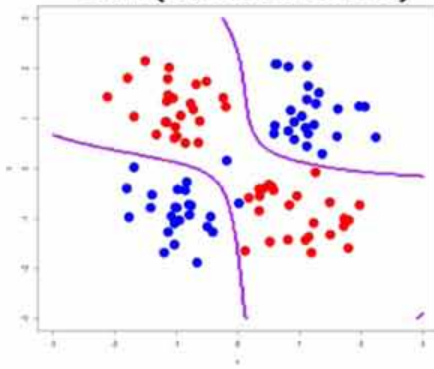
Machine Learning (ML) Classifiers

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

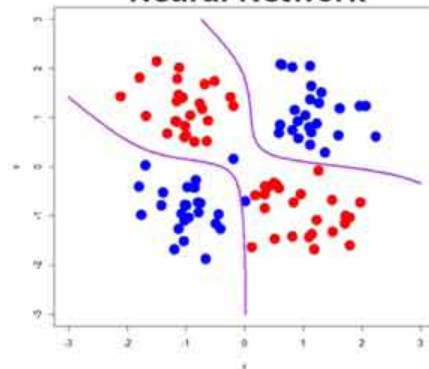
Decision Tree



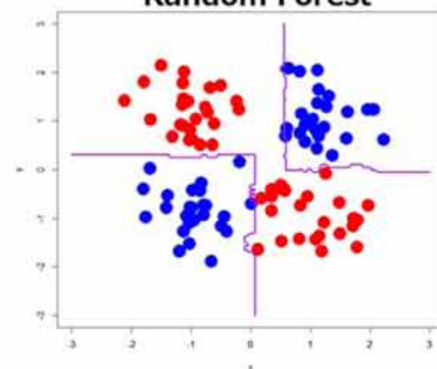
SVM (Gaussian kernel)



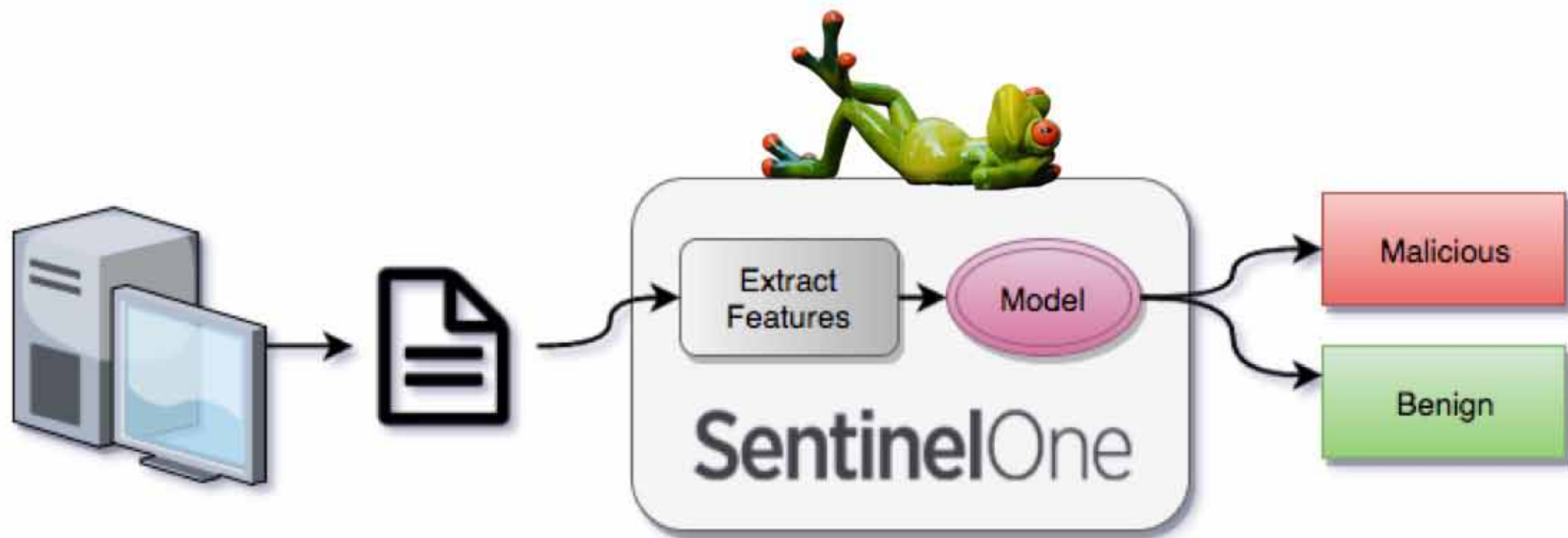
Neural Network



Random Forest



Our Solution



The background is a dark, deep blue space filled with numerous glowing particles and lines. In the upper left, there are several thin, white, tangled lines that resemble a complex network or a molecular structure. Scattered throughout the scene are many small, bright blue and purple dots, some of which are larger and more prominent, creating a bokeh effect. The overall aesthetic is futuristic and scientific, suggesting a digital or data-driven environment.

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

SVM-based classification

Supervised Learning

Running millions of files



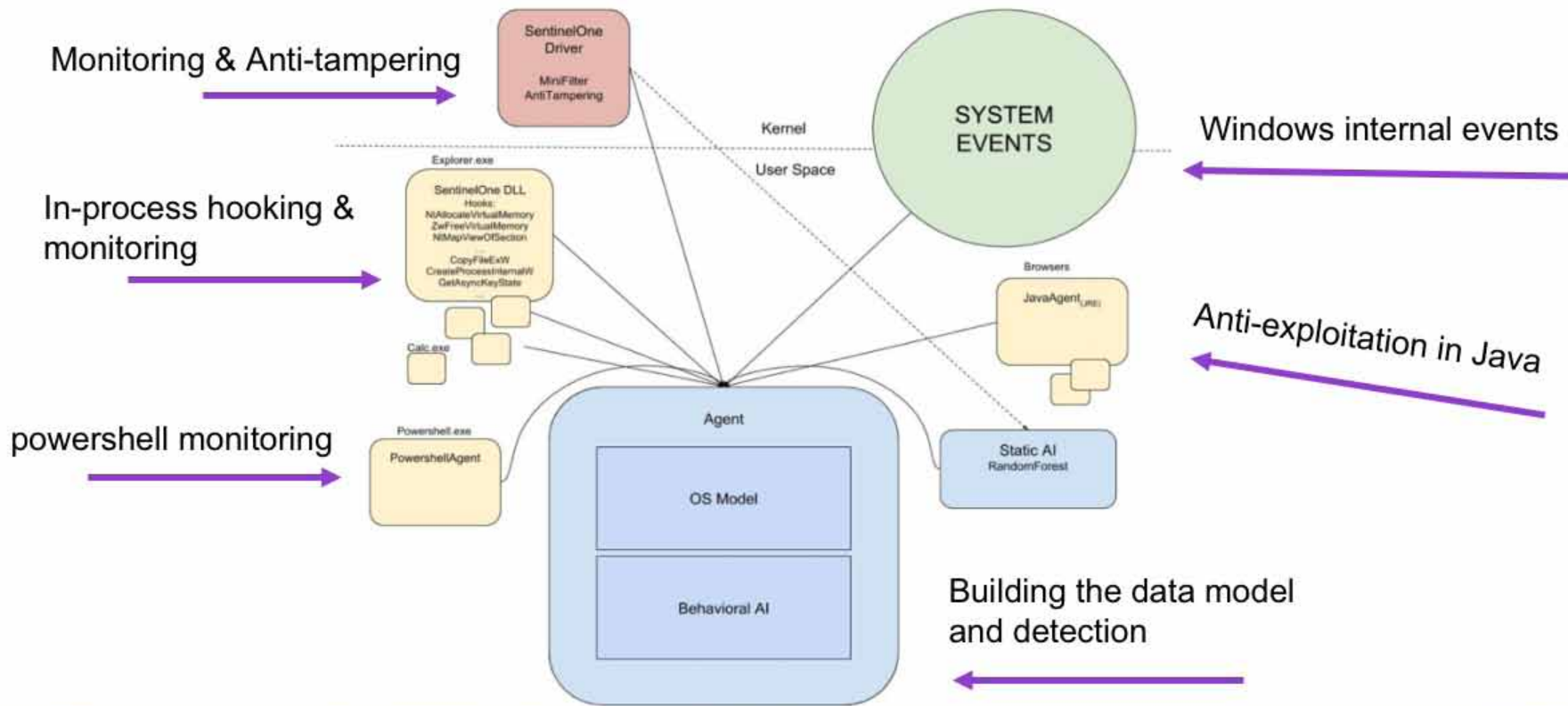
Monitoring OS-events and behaviors



Trained SVM



Architecture



What OS-Events are Collected?



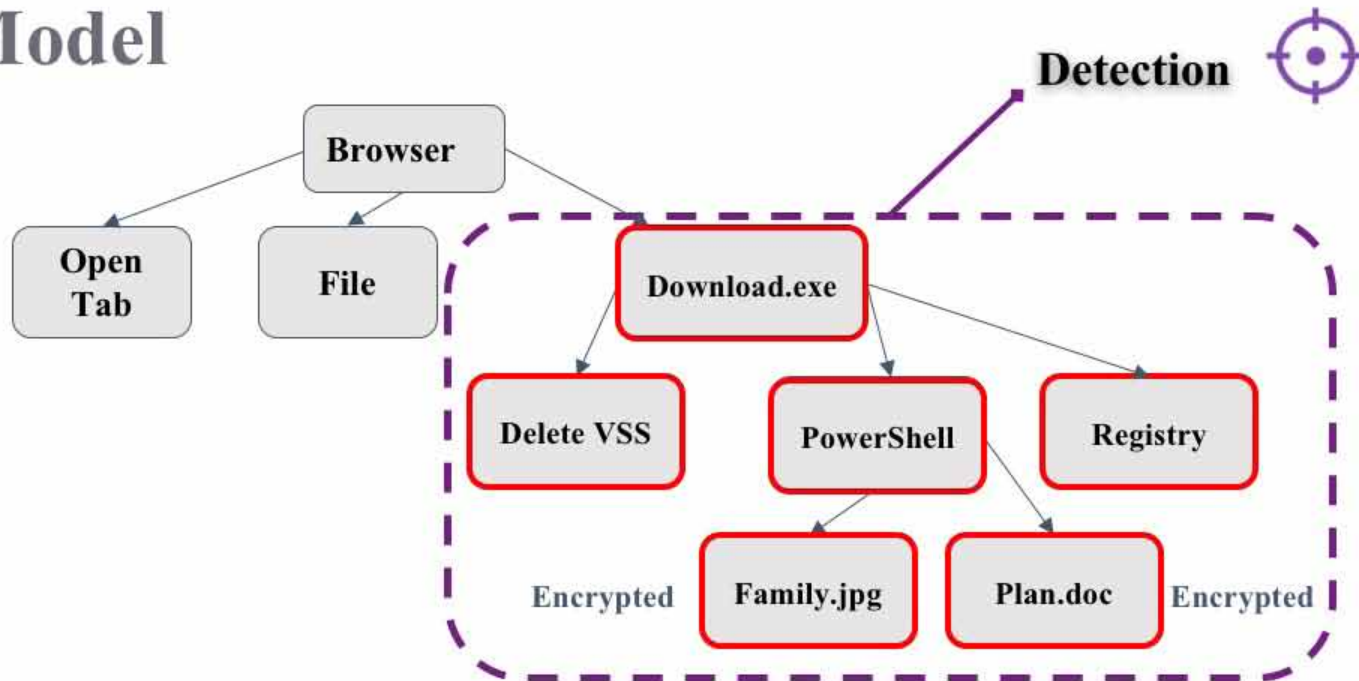
Detection Capabilities

- 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

The background is a dark, deep blue space filled with numerous glowing particles and lines. In the upper left, there are several thin, white, tangled lines that resemble a complex network or a molecular structure. Scattered throughout the scene are many small, bright blue and purple dots, some of which are larger and more prominent, creating a bokeh effect. The overall impression is one of a dynamic, energetic, and somewhat chaotic environment, possibly representing a complex system or a network of interactions.

Mitigation Approaches

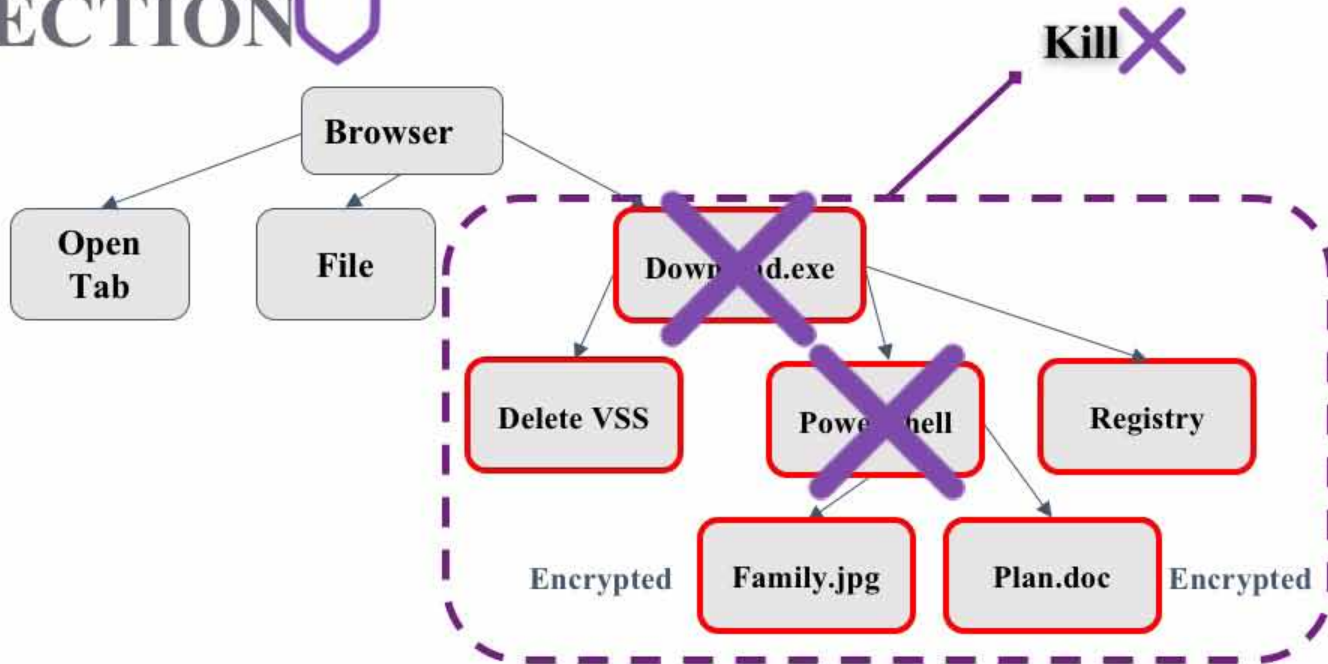
Data Model



SentinelOne unique data model capability

Enables Dealing with complicated OS flows (APC, RPC, Remote Threads etc.)

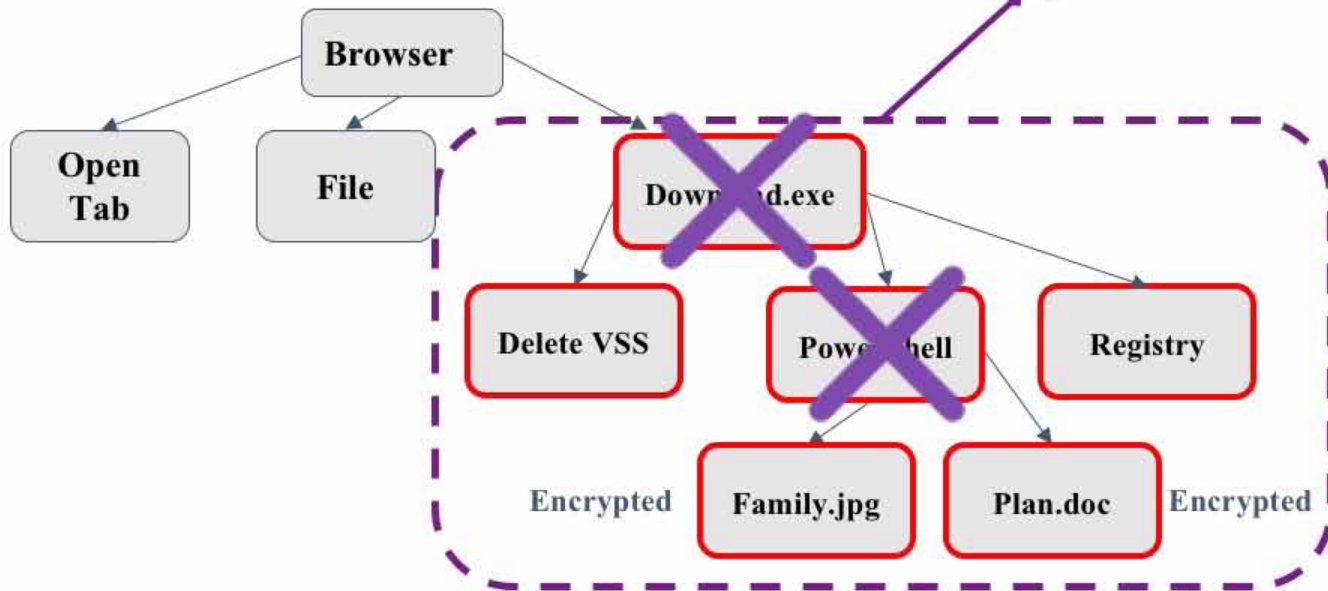
PROTECTION



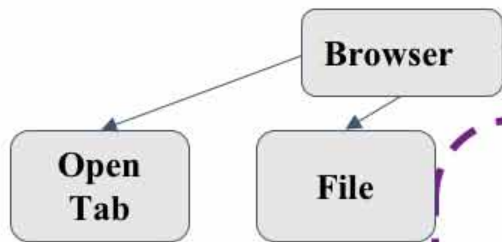
PROTECTION



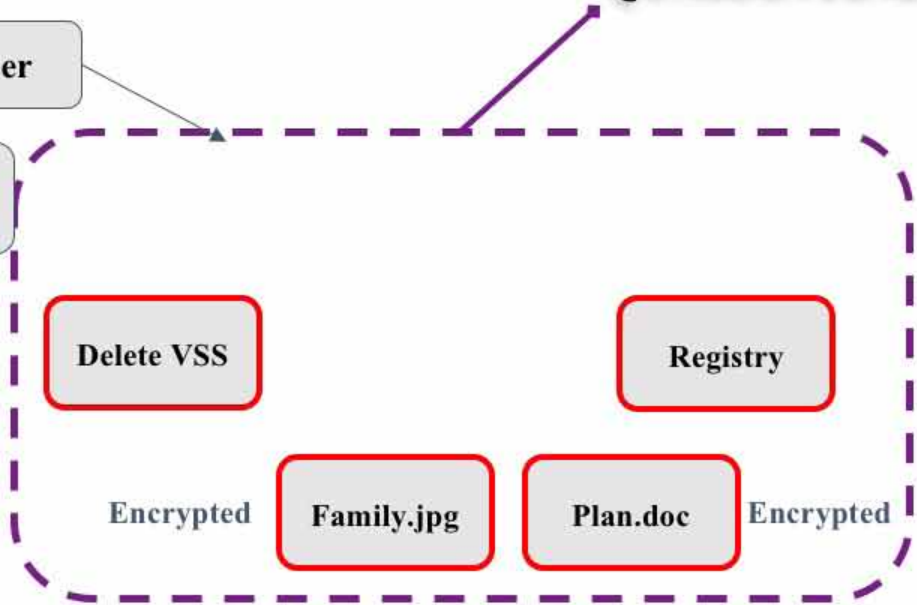
QUARANTINE



PROTECTION



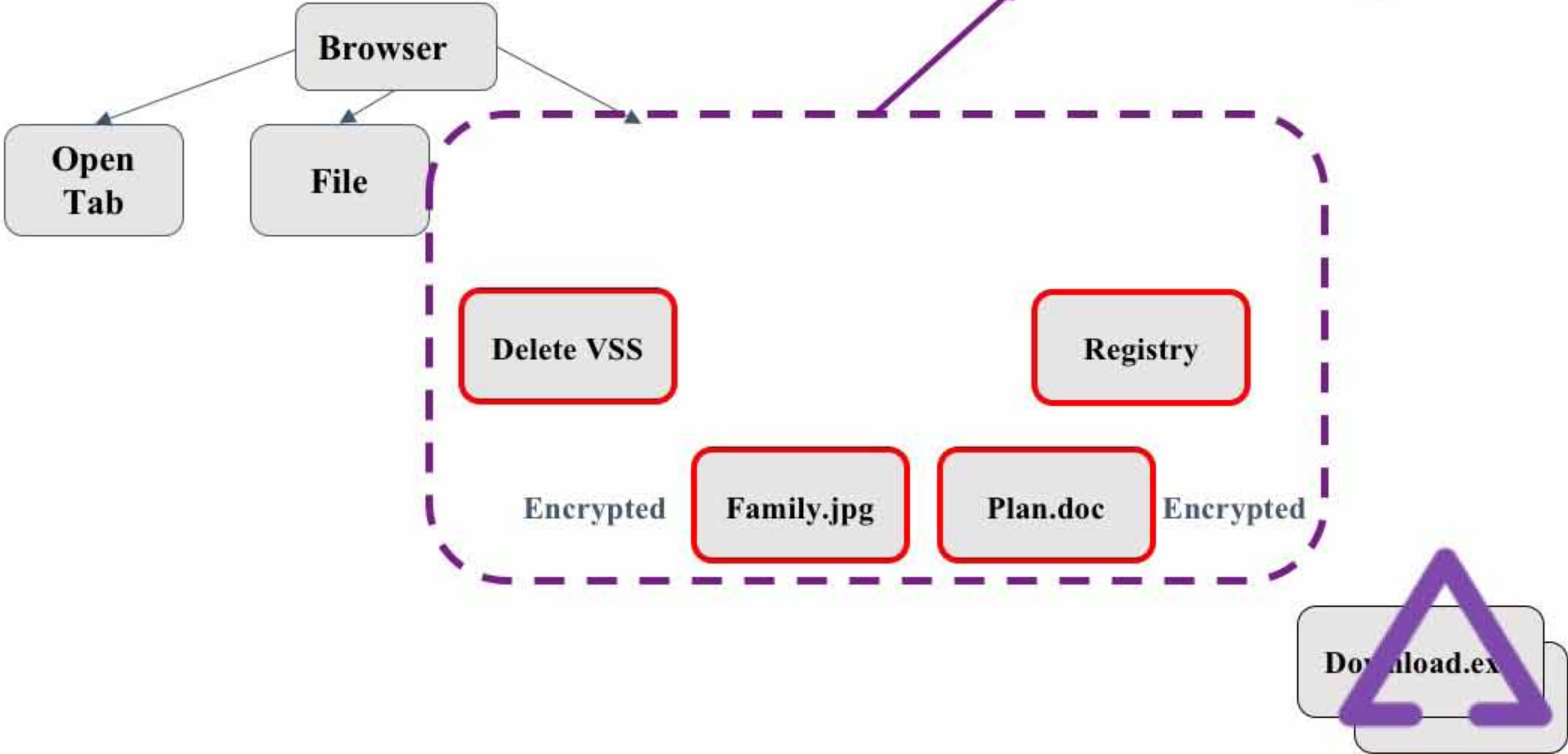
QUARANTINE



RESPONSE

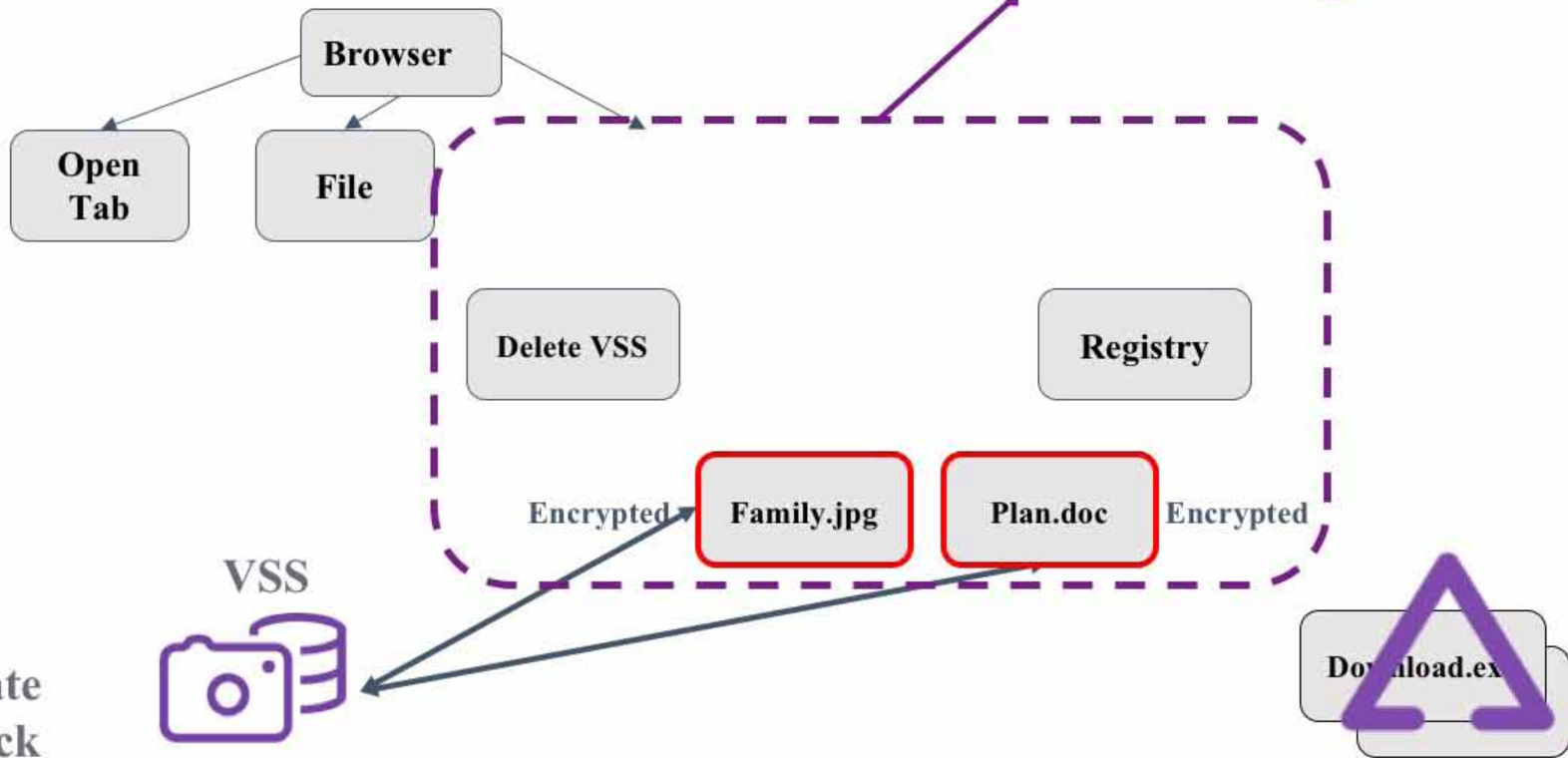


REMEDiate



RESPONSE

ROLLBACK



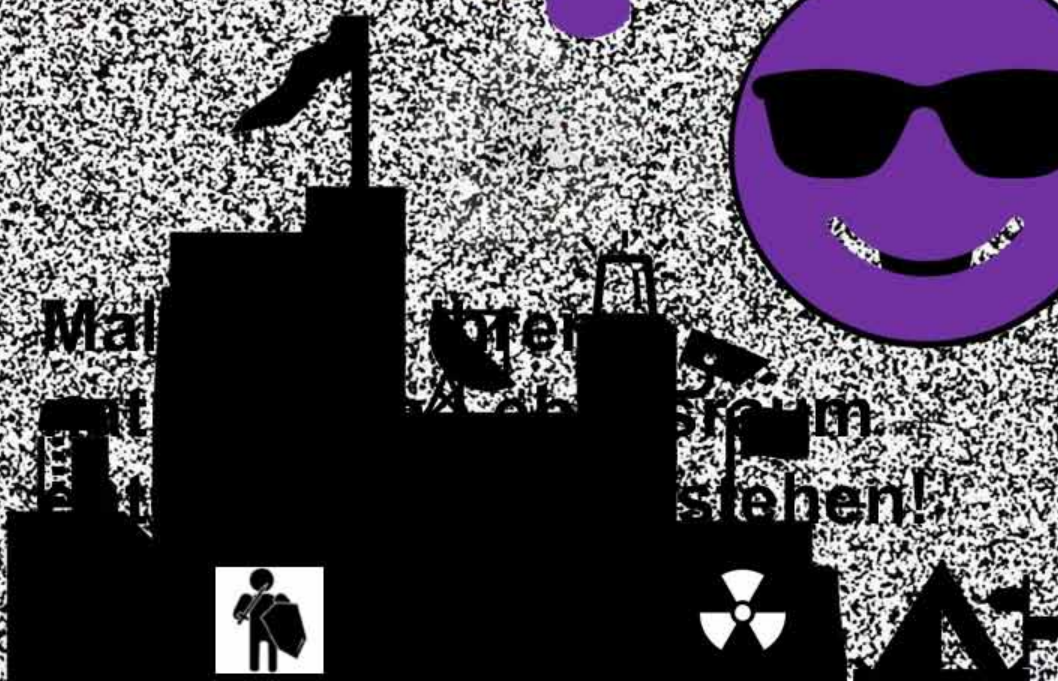
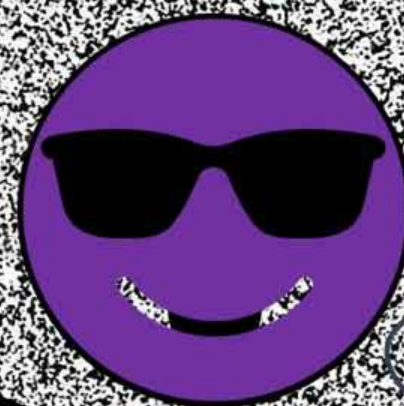
Accurate
Rollback



**Advanced
Endpoint
Protection**



SentinelOne



Mit 1-2% CPU auf dem Laptop!



Malware in ihrem natürlichen Lebensraum entdecken und verstehen!



Step by step...



BEFORE

Static AI

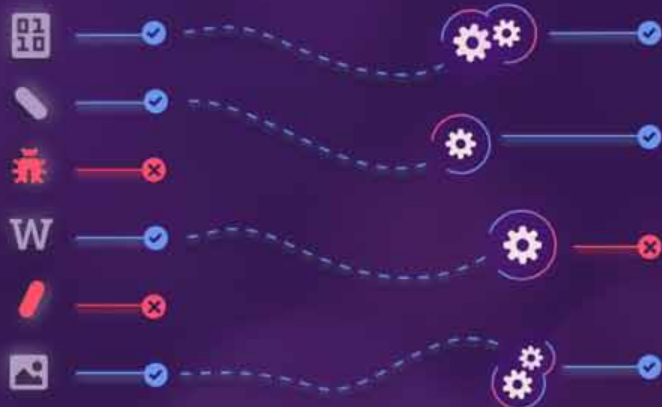
Prevent attacks
pre-execution



DURING

Behavioral AI

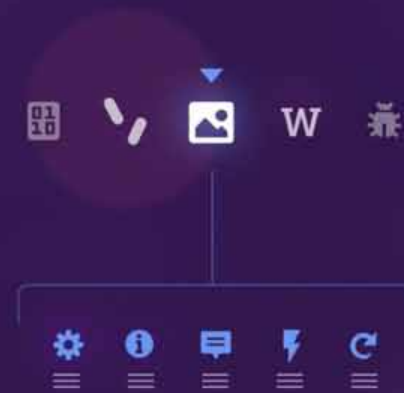
Constantly monitor and
map each running process
for incongruous behaviors



AFTER

Automated EDR

Automate remediation and
response...even rollback



Advanced Endpoint SECURITY



Endpoint Protection

Ein Agent!

Endpoint Detecton &
Response (EDR)

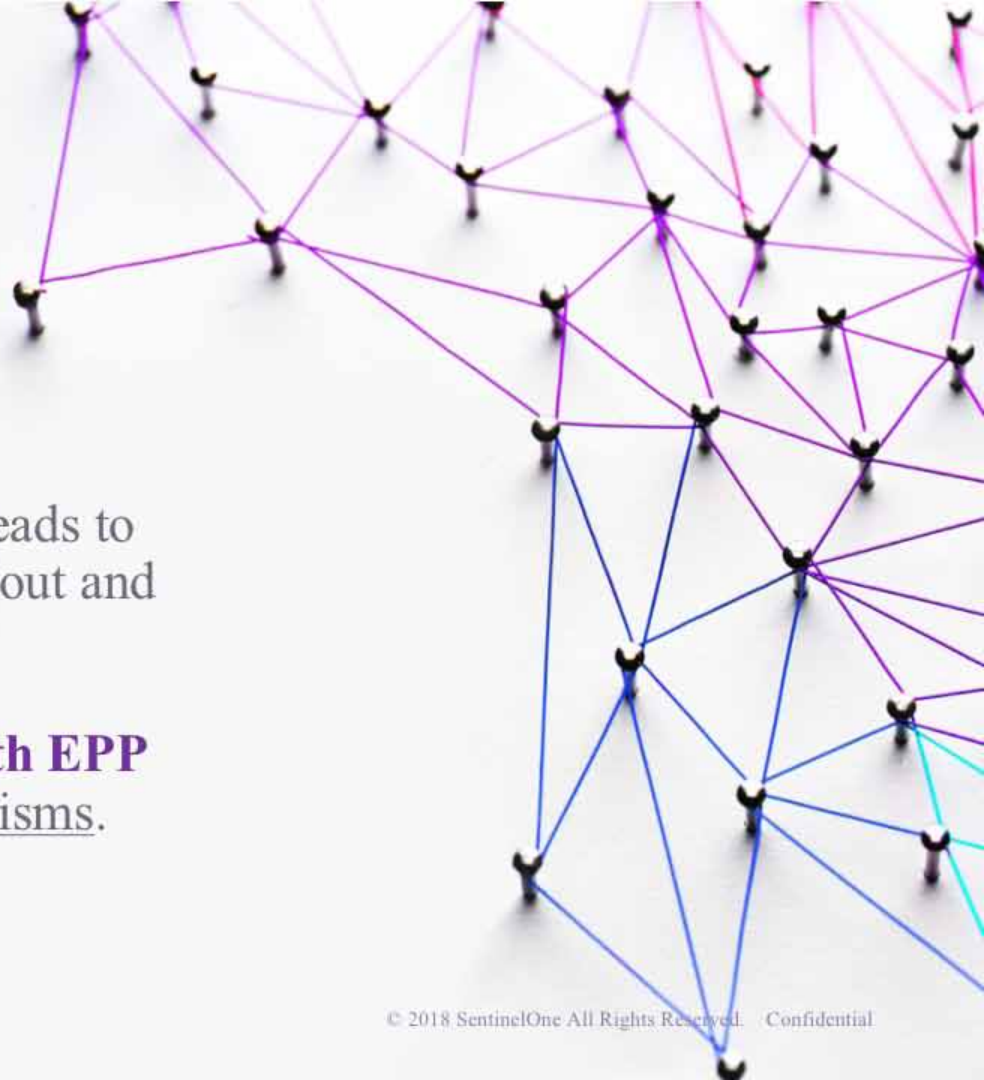
 SentinelOne™

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 maintenance (TCO).
- **Having EDR deeply integrated with EPP** leads to automated response mechanisms.



2x3 gute Gründe ...



Intelligenz auf dem Endpunkt



Ein schlanker Agent (Mac, MS, Linux)

Agent



Detect & Response (EDR)

Management



On premise, cloud oder hybrid



Mandantenfähigkeit



Integrierbarkeit (API)



... SentinelOne
einmal genauer
anzuschauen!

Live Demo!

Und jetzt?



SentinerOne™





Thank You