PREVASIO

Zero Trust Container Analysis System

Key Benefits

Behavioral Analysis
leaves no chance to malware that easily evades other vendors' static scanners with a dynamic payload

ML-based Detection
provides generic detection for malicious ELF binaries, resistant to source code modifications

Agentless Approach
ensures no implants are embedded into container images

HTTPS Traffic Analysis
makes sure all traffic generated by containers is intercepted and inspected

Vulnerability Scan
reports any packages found to be vulnerable to any known, previously reported exploits

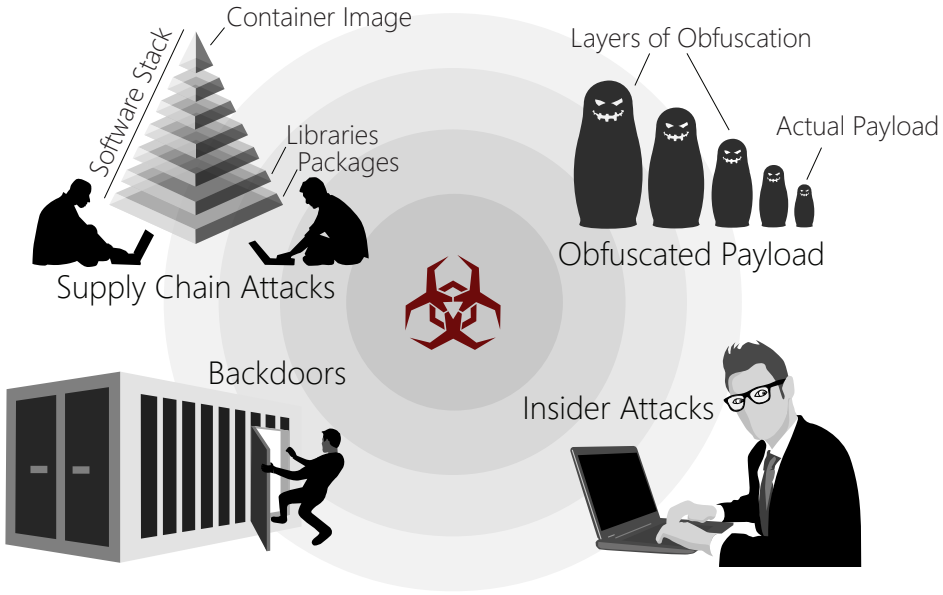
Automated Pen-Test
simulates attackers' actions while posing no risk to the production environment

System Event Graph
visually represents all kernel-level system events within a running container

The growing popularity of Docker containers exposes one fundamental issue with this technology: the lack of visibility of what actually happens inside the running containers.

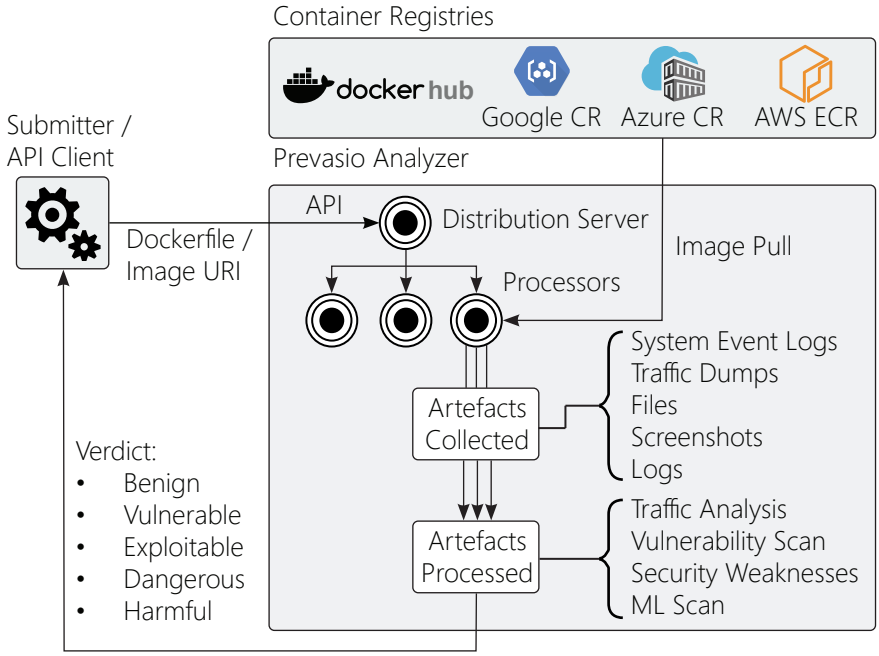
Without this transparency, containers largely stay what they are - the black boxes.

For example, malicious intent of a trojanized container can't be known until its payload is dynamically downloaded, compiled, and executed.



Prevasio's Solution to the Problem

In a controlled virtual environment of a network sandbox, container images are first built, and then executed, monitored, analyzed and pen-tested to determine if they are vulnerable, exploitable, or harmful.

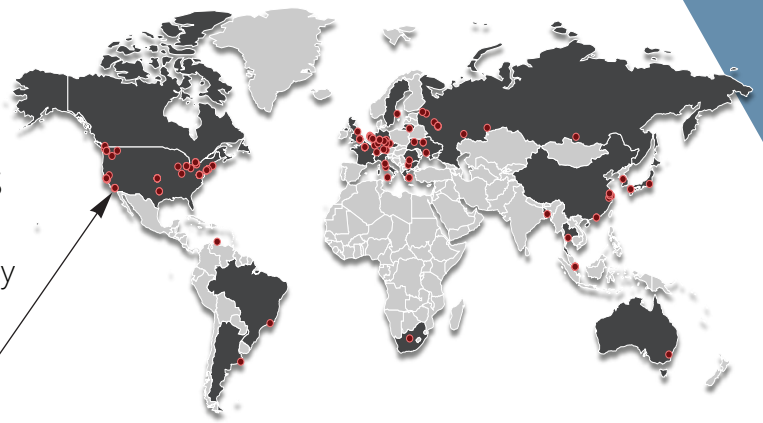


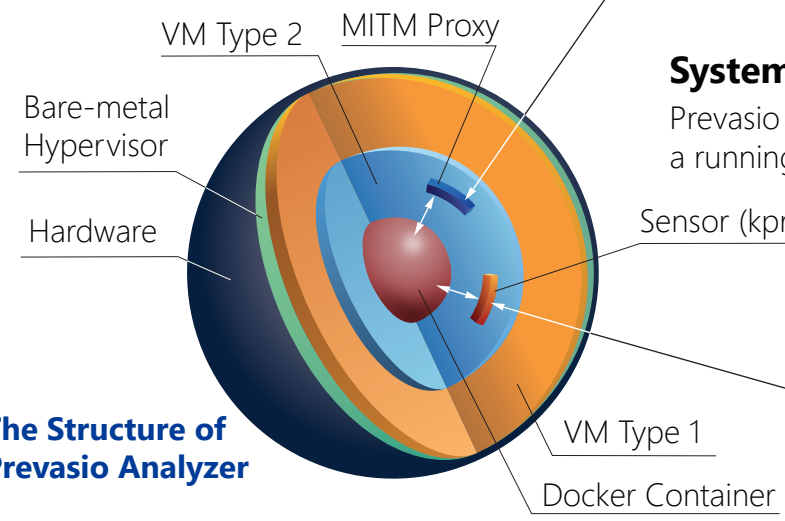
PREVASIO

Network Traffic Analysis

Prevasio intercepts and inspects all network traffic generated by containers, including HTTPS traffic.

SSL/TLS Inspection is enabled with a MITM proxy certificate being dynamically injected into and forcefully trusted by an analysed container.

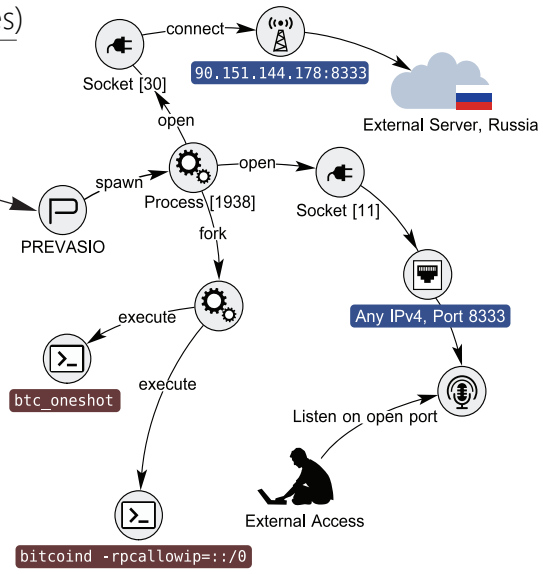




The Structure of Prevasio Analyzer

System Event Graph

Prevasio collects kernel-level system events within a running container, by using an external sensor.



No Massive Report Volumes: Single View For All Events

Any container-based activity, such as new file execution, or executed scripts within shells, are then correlated into a hierarchy and visually displayed in form of a force-directed graph. The graph allows to visually identify problematic containers and also quickly establish remote access points.

Automated Penetration Test

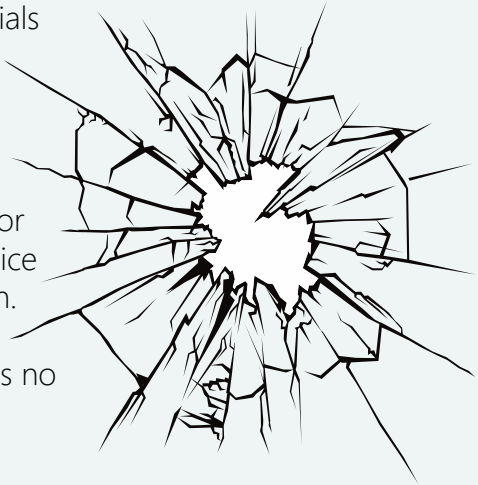
The Zero Trust model employed by Prevasio treats all containers as if they were internet-facing, and considers the entire network to be compromised and hostile. For this reason, it exposes containers to a full pen-test in accordance with the following cyber kill chain phases:

Reconnaissance | Discovery | Vulnerability Lookup | Exploitation | Scanning For Default Credentials | Brute Force Attack | Post Exploitation

Prevasio simulates attackers' actions, first trying to fingerprint running services, and then intelligently selecting and applying a range of pen-testing tools against them.

For example, if a service exposed by a container was identified as SSH or MySQL, the pen-test will perform a brute-force attack against that service in order to find weak credentials that would allow the attackers to log in.

As the pen-test is performed in an isolated virtual environment, it poses no risk to the production environment.



PREVASIO

ML Model: Resilience to Malware Modifications Due to Signatureless Approach

The following charts reveal scan results for 33 thousand malicious ELF executables.

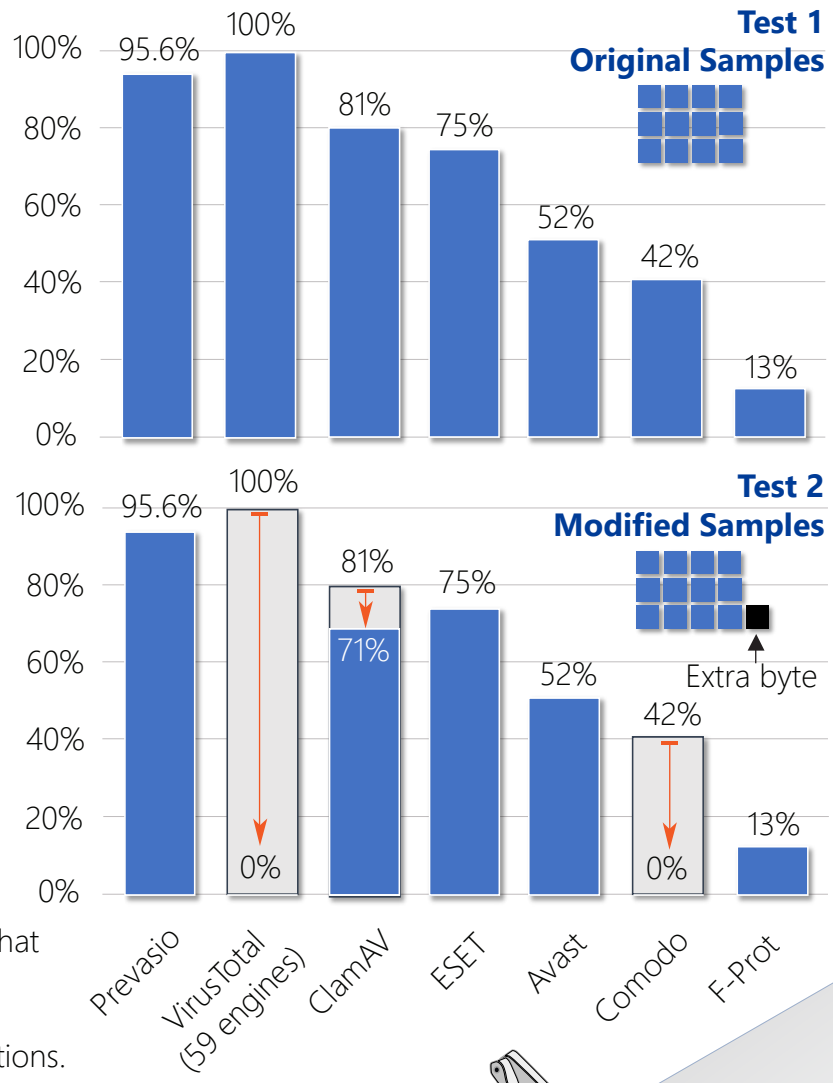
There were 2 tests performed: in the first test, the original samples were scanned.

In the second test, each sample out of the entire set was appended with one extra zero byte. The entire set was then scanned again.

In both tests, Prevasio's ML scanner has reached 95.6% detection at 0.1% False Positive Rate (on par with ClamAV's FPR).

The VirusTotal hash lookup has failed in the second test, as it contained no hashes of the modified samples.

Some AV vendors have demonstrated a reduction of the detection rate, revealing how much they depend on hashes.



Other tests conducted by Prevasio prove that Prevasio ML scanner demonstrates excellent resilience to substantial malicious source code modifications and re-compilations.