

BLOCKWATCH

CLOUD INSPECTION AND IDENTIFICATION

DON'T TAKE CHANCES

BlockWatch (BW) delivers guaranteed results without the guess work. Our insightful out-of-the-box operations is what can keep your systems clean and trouble free from malware, worm or any form of trojan hack attack.

Using secure methods, not fuzzy or broken heuristics, BW out performs signature or traditional virus and malware systems.

BW is a high performance system that can process MANY MILLIONS of results and validation per minute, each result is a guaranteed finding, not a guess or a probability "score", don't be fooled into a false sense of security with inexact tools and techniques.

BLOCKWATCH FUNCTIONALITY

BW is a code scanner able to verify and perform integrity checks of cloud memory compartments and a data scanner which can extract fragment or partial data artifacts from cloud memory and networks.

- Protect server's from running any unknown/unauthorized code
- Detect access or use of data/documents

BW is an agentless cloud search tool designed to locate data and code inside of a cloud container.

BW has built in functionality for memory code integrity verification supporting security defense and monitoring. BW also enables a cryptographically secure search engine; able to locate data (and partial data matches) using secure methods, detecting confidential data access/disclosure within cloud containers.

USE CASES

DETECT USE OF SENSITIVE DOCUMENTS

MEMORY INTEGRITY CHECKING

DATA ASSURANCE

Cloud Data assurance steps	Define data set	hash sets are generated compiled into scan engine
	Scan for data	Virtual Containers Network traffic
	Report on detections	Identify data breeches

CLOUD SECURITY

System Integrity monitoring	Extract cloud memory	Agentless
		VM Platform agnostic
	Validate system	Detect ODAY malware unauthorized code

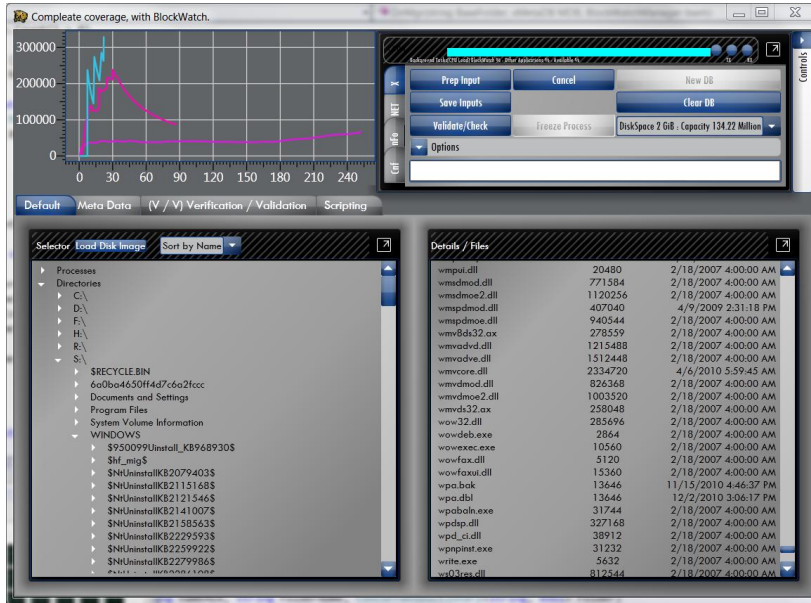
FEATURES

FEATURES	BENEFITS
Block/Fragment detection	Partial search results not just exact matches <ul style="list-style-type: none">• Document revisions or formats• Copies/data clones
Cryptographically secure search	Leverages secure hash algorithms to ensure security of search. <ul style="list-style-type: none">• No way to infer what is being searched for from analyzing the search without breaking (crack) the hash algorithm<ul style="list-style-type: none">○ Hash algorithm is configurable
Reads physical memory	Works with any cloud vendor Not Microsoft, VMware or XEN specific Works with physical systems
Very large input support	Can handle many GB/TB's of data
Python or Ruby scripting	Customize or use powerful API and developer features
Works from outside the guest	No BW code is open to attack. Agentless.

MANAGEMENT OF DATA SETS

HIGH PERFORMANCE transactions rates range from tens to *hundreds of thousands* per second.

Use either the WINDOWS UI or built in PYTHON and RUBY scripting.



VISUALIZATION

PROVABLE RESULTS; the visualization view illustrates where each detected artifact is located inside of a virtual container.

Zoom in to inspect data (each color is a unique detection).



High level inspection of data in a container.

