SOLUTION BRIEF

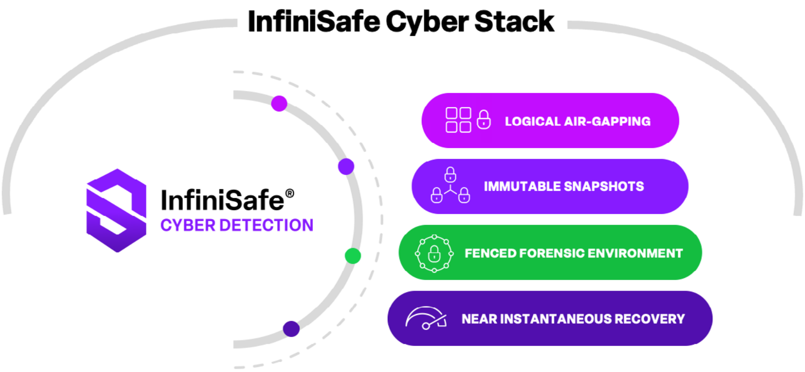
InfiniSafe® Cyber Detection

The impact of cybercrime is expected to cost businesses 8 trillion USD$ per year.[1] Every 39 seconds, there is a new attack somewhere on the web.[2] The costs to a business include damage and destruction of data, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, etc. Along with the post-attack disruption to the business, you have forensic investigation, detection and restoration of hacked data and systems, and loss of trust and reputation. Most security and IT teams feel that it's a matter of time before they have a cyberattack. Are you prepared?

InfiniSafe technology provides a multi-layered cyber stack for the creation of cyber storage resilient environments with the InfiniBox® and InfiniBox™ SSA platforms.

The introduction of InfiniSafe Cyber Detection, enhances Infinidat's cyber storage resilience and response capabilities by enabling the security and IT teams to detect ransomware and malware attacks with up to 99.5% accuracy, and enable near instantaneous recovery of data from clean "known good" copies on the InfiniBox and the InfiniBox SSA platforms.

InfiniSafe Cyber Detection adds a level of data detection to the InfiniSafe cyber stack that surrounds the four main layers of the stack and deepens the ability of InfiniSafe to detect cyber incidents. InfiniSafe Cyber Detection performs a deep scanning of block, file, and database stores by presenting InfiniBox and InfiniBox SSA immutable snapshots to powerful AI-based scanning engines that will validate their integrity and, through machine learning, identify any malicious changes that could indicate a cyberattack.



When an attack is detected, InfiniSafe Cyber Detection provides forensic reporting to diagnose what data has been compromised and the nature of the compromise, and provides critical insights to where the compromised data originated. Then, using the power of InfiniSafe technology, the user can quickly recover to normal business operations, once they have identified a known good copy of the data.

InfiniSafe Cyber Detection uses a combination of over 200 full-content-based analytics that inspect the content of files and data, not just metadata. Powerful machine learning algorithms will tell you the type of variant that was used to corrupt the data with 99.5% accuracy, helping companies protect their business-critical infrastructure and content without a waterfall of false positives, so you can focus on real areas of concern and address issues quickly.

> "**79%** of organizations report that **ransomware preparedness** is one of the top five overall **business priorities** in the eyes of their executive team and/or board of directors."
>
> Enterprise Strategy Group Research Report, The Long Road Ahead to Ransomware Prepareness, June 2022

Detection

Analytics and machine learning detection

Forensics

Forensic reports to diagnose and identify the ipact of the attack

Recovery

Reports on the last good version of files to streamline the recovery

If data corruption is identified, InfiniSafe Cyber Detection provides the necessary forensic tools to diagnose, identify, and help recover affected assets. InfiniSafe Cyber Detection reports on files that were impacted and the forensic findings can be investigated by your security and software teams and any issues can be eradicated as needed with their tools. Then any compromised data can easily be replaced with the last known good version to ensure business operations return to normal with minimal downtime. InfiniSafe Cyber Detection is an add-on option to our core InfiniSafe technology and is a subscription-based license. InfiniSafe Cyber Detection is a post-attack product that is focused on data resiliency in the InfiniSafe cyber stack and does not replace ransomware and malware prevention best-practices and traditional threat management products on the server, application, and networking part of the overall cyber security strategy.

Detection

InfiniSafe Cyber Detection uses full-content analytics on all the protected data. This deep awareness is the only way you can be confident that your data has integrity and that cyber criminals are not circumventing your data analytics tools, hiding their tracks, and covertly corrupting your data.

Much like our neural cache machine learning, InfiniSafe Cyber Detection is infused with powerful and deterministic machine learning. Combining 200+ analytics – over 20x as many as competitors – with data observations that get more intelligent over time with more observations. The machine learning is trained on thousands of ransomware, malware, and trojan infections to find unusual patterns of behavior and distinguish user activity vs ransomware, while minimizing false positives and negatives.

Forensics

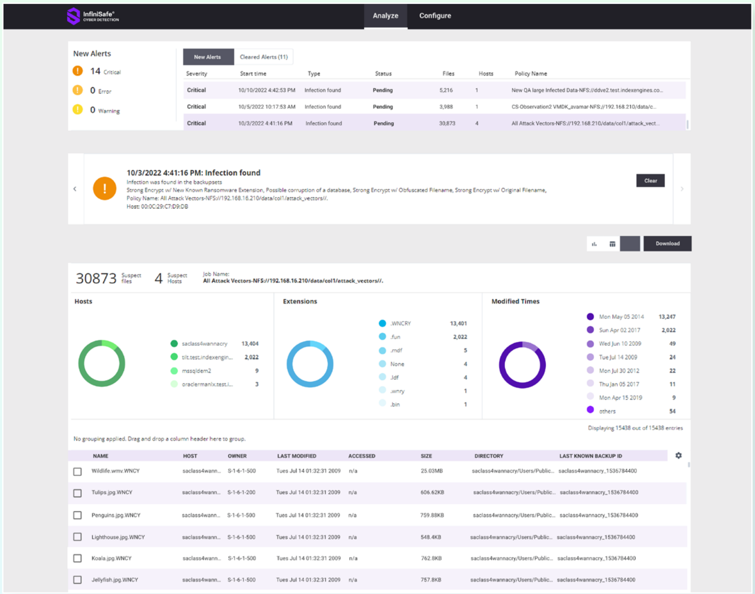
When data is corrupted, InfiniSafe Cyber Detection generates a list of the corrupted files. Corrupted files are tagged and forensic reports are created to diagnose and identify the impact of the attack and provide the intelligence needed to facilitate recovery.

Alerts organized by severity

New details on suspect corruption

Customizable, dynamic charts to drill down into details of the attack

List of corrupted files that can be downloaded



Severity	Start time	Type	Status	Files	Hosts	Policy Name
Critical	10/10/2022 4:42:53 PM	Infection found	Pending	5,216	1	New QA large Infected Data-NFS://ddve2.test.indexengines.co...
Critical	10/5/2022 10:17:53 AM	Infection found	Pending	3,988	1	CS-Observation2 VMDK_avamar-NFS://192.168.210/data/c...
Critical	10/3/2022 4:41:16 PM	Infection found	Pending	30,873	4	All Attack Vectors-NFS://192.168.210/data/col1/attack_vect...

10/3/2022 4:41:16 PM: Infection found
Infection was found in the backupsets
Strong Encrypt w/ New Known Ransomware Extension, Possible corruption of a database, Strong Encrypt w/ Obfuscated Filename, Strong Encrypt w/ Original Filename,
Policy Name: All Attack Vectors-NFS://192.168.16.210/data/col1/attack_vectors//.
Host: 00:0C:29:C7:D9:DB

30873 Suspect files 4 Suspect Hosts Job Name: **All Attack Vectors-NFS://192.168.16.210/data/col1/attack_vectors//.**

Displaying 15438 out of 15438 entries

No grouping applied. Drag and drop a column header here to group.

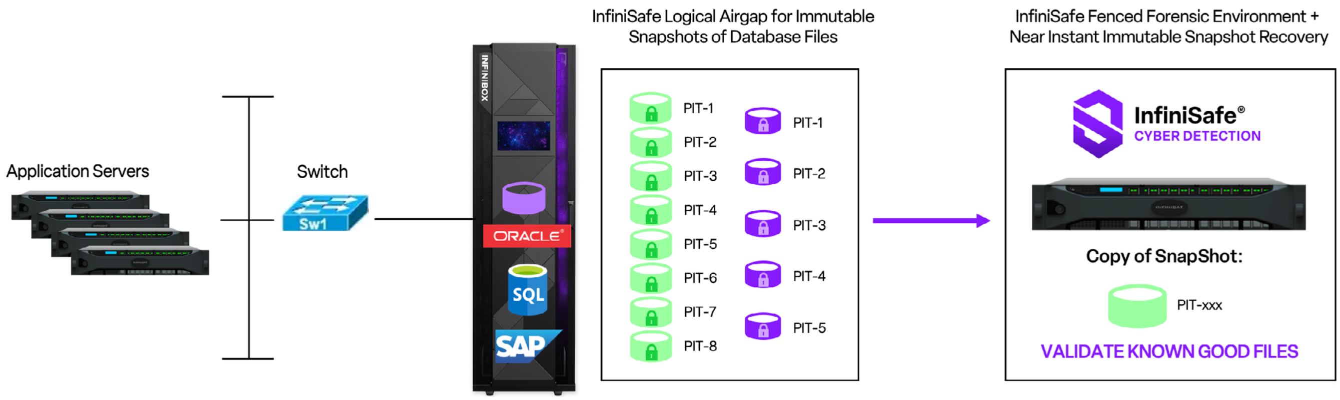
	NAME	HOST	OWNER	LAST MODIFIED	ACCESSED	SIZE	DIRECTORY	LAST KNOWN BACKUP ID
□	Wildlife.wmv.WNCY	saclass4wann...	S-1-6-1-500	Tues Jul 14 01:32:31 2009	n/a	25.03MB	saclass4wannacry/Users/Public...	saclass4wannacry_1536784400
□	Tulips.jpg.WNCY	saclass4wann...	S-1-6-1-200	Tues Jul 14 01:32:31 2009	n/a	606.62KB	saclass4wannacry/Users/Public...	saclass4wannacry_1536784400
□	Penguins.jpg.WNCY	saclass4wann...	S-1-6-1-500	Tues Jul 14 01:32:31 2009	n/a	759.88KB	saclass4wannacry/Users/Public...	saclass4wannacry_1536784400
□	Lighthouse.jpg.WNCY	saclass4wann...	S-1-6-1-500	Tues Jul 14 01:32:31 2009	n/a	548.4KB	saclass4wannacry/Users/Public...	saclass4wannacry_1536784400
□	Koala.jpg.WNCY	saclass4wann...	S-1-6-1-500	Tues Jul 14 01:32:31 2009	n/a	762.8KB	saclass4wannacry/Users/Public...	saclass4wannacry_1536784400
□	Jellyfish.jpg.WNCY	saclass4wann...	S-1-6-1-500	Tues Jul 14 01:32:31 2009	n/a	757.8KB	saclass4wannacry/Users/Public...	saclass4wannacry_1536784400

The post attack dashboard: improved user experience, more insight into data, intuitive post-attack workflow.

Recovery

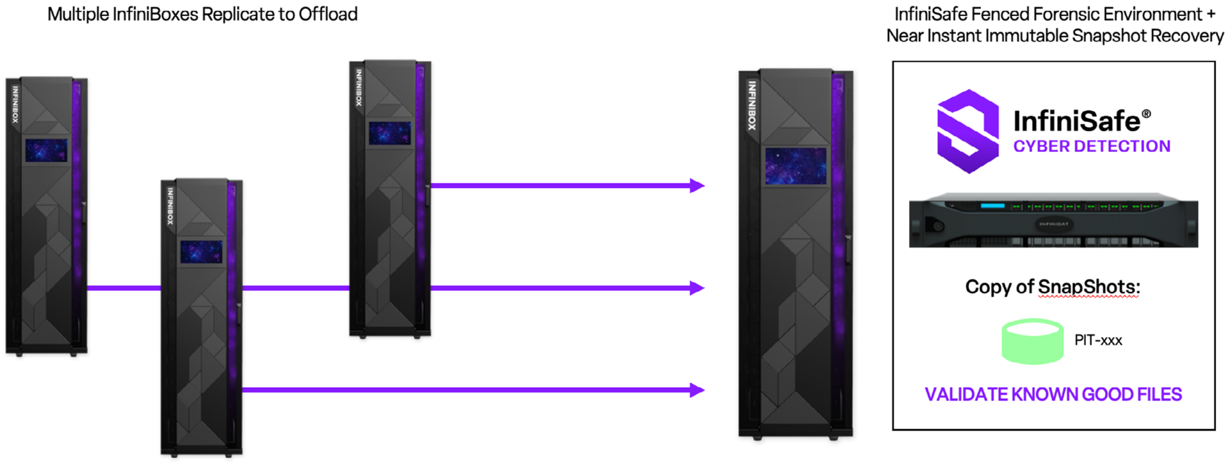
Finally, InfiniSafe Cyber Detection will report on the last good copy of a file or backup when the backup copy resides on an InfiniBox or InfiniBox SSA. It will know where the corrupt data is, where the last good version of the data is, and what snapshots or backup sets the data was in to streamline the recovery process.

Use Cases: Block, File, and Database Cyber Detection


Application Servers
Switch
Sw1
INFINIBOX
ORACLE
SQL
SAP
InfiniSafe Logical Airgap for Immutable Snapshots of Database Files
PIT-1
PIT-2
PIT-3
PIT-4
PIT-5
PIT-6
PIT-7
PIT-8
PIT-1
PIT-2
PIT-3
PIT-4
PIT-5
InfiniSafe Fenced Forensic Environment + Near Instant Immutable Snapshot Recovery
InfiniSafe®
CYBER DETECTION
Copy of SnapShot:
PIT-xxx
VALIDATE KNOWN GOOD FILES

Enterprises using the InfiniBox or InfiniBox SSA for mission-critical database applications, can be assured when using InfiniSafe cyber stack technology with Cyber Detection, that they can take frequent immutable snapshots to validate their integrity and, through machine learning, identify any changes that indicate a cyberattack. InfiniSafe Cyber Detection will determine any issues and report on known good copies of data for near-instantaneous recovery with InfiniSafe.

Cyber Detection Array


Multiple InfiniBoxes Replicate to Offload
INFINIBOX
INFINIBOX
INFINIBOX
INFINIBOX
InfiniSafe Fenced Forensic Environment + Near Instant Immutable Snapshot Recovery
InfiniSafe®
CYBER DETECTION
Copy of SnapShots:
PIT-xxx
VALIDATE KNOWN GOOD FILES

Enterprises using multiple InfiniBox or InfiniBox SSAs can replicate data to a designated Cyber Detection Array, in a fenced forensic environment, using native Infinidat replication tools. The Cyber Detection Array will scan all data files, tag any corrupted files, and create a forensic report. This configuration provides enterprises with the intelligence to detect a cyber attack.

Malicious ransomware and malware incidents continue to disrupt critical services and businesses from energy pipelines to schools and hospitals. The total economic losses from ransomware and malware attacks continue to climb. Implementing an effective cyber detection strategy can mitigate your enterprise's exposure and ensure rapid recovery.

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[2] https://techjury.net/blog/how-many-cyber-attacks-per-day/

sales@infinidat.com

INFINIDAT