INFINIDAT
FEDERAL

SOLUTION BRIEF

InfiniSafe® Automated Cyber Protection: Reducing the Threat

Shrinking the threat window to avoid or try to prevent cyber attacks is more important than ever. No one solution can address every vulnerability, but having a highly flexible set of capabilities and options to protect a company's critical data assets is an important piece of a complex puzzle. **Remember: It is not a matter of if cyber attackers will strike, it's a matter of when.**

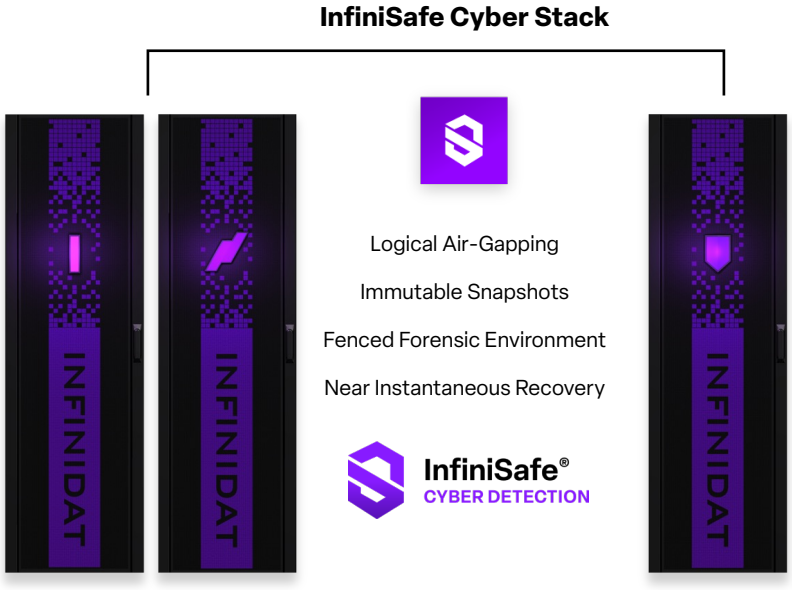
Prepare

Currently, most organizations protect data using traditional backup and recovery methods including deletable snapshots. Augment these methods with scheduled, timer-locked immutable snapshots and you have made incremental progress in securing your data. Unfortunately, scheduled events create wide gaps that make data vulnerable. The gap in time between these points is typically determined by the recovery point objective or RPO — a measure of how much data a business can afford to lose over a given time. If immutable snaps are done four times a day, that means up to a 6-hour RPO. Today, the amount of data that could be compromised in that time can ruin a business.

As a result, a more proactive process is necessary to protect data should something be suspected in the attack plane. Security monitoring teams can not react fast enough to protect data during cyber events that move at the speed of networks and compute. InfiniSafe Automated Cyber Protection addresses this. Leveraging real-time monitoring that exists within many company security operations centers and the speed of compute on any alert level, a security team may define a trigger to automatically and immediately create immutable snapshots on the storage environment thus reducing the risk of damaging data corruption, data deletion, data encryption, etc.

Every attack is about gaining information and leverage. Encrypting data, corrupting backups, and stealing information, create leverage. When attackers have leverage, they know it is likely that they will be able to extort you in some fashion.

Time is money — lots of money when it comes to cyber incidents. Companies are thrown into chaos when a cyber event of magnitude happens. The quicker you can ensure you have your data and that it is in a known good state, the quicker you get some, if not all, of your leverage back. We have all the mechanisms around us to help make cyber disasters easier to deal with,

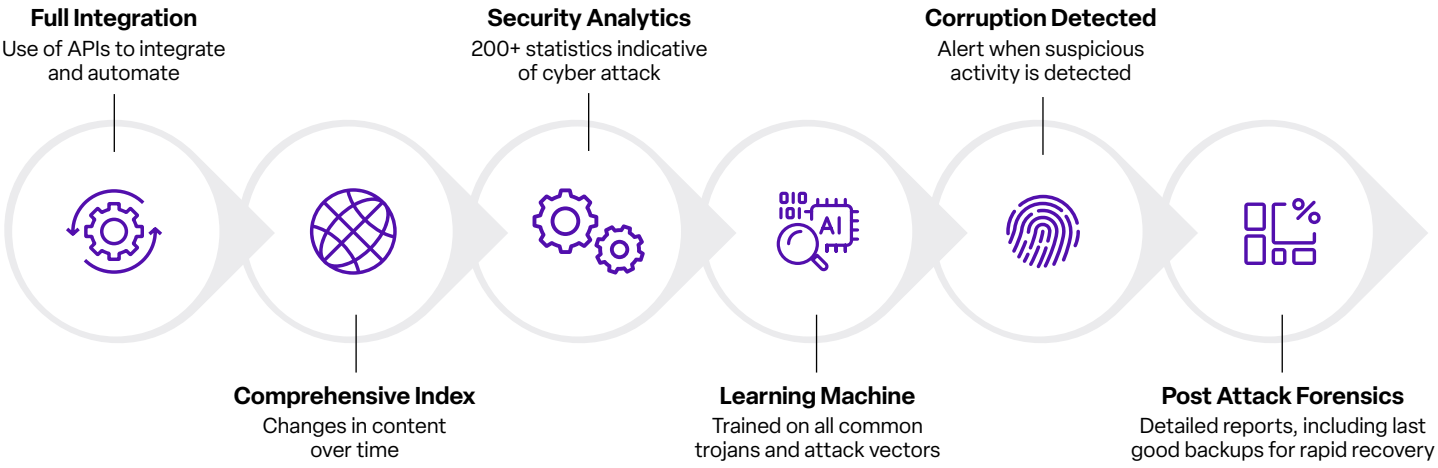


however, we must put the pieces of these solutions together and orchestrate the process, because attackers want to create chaos and not give you time to think.

Identify, Orchestrate, and Act

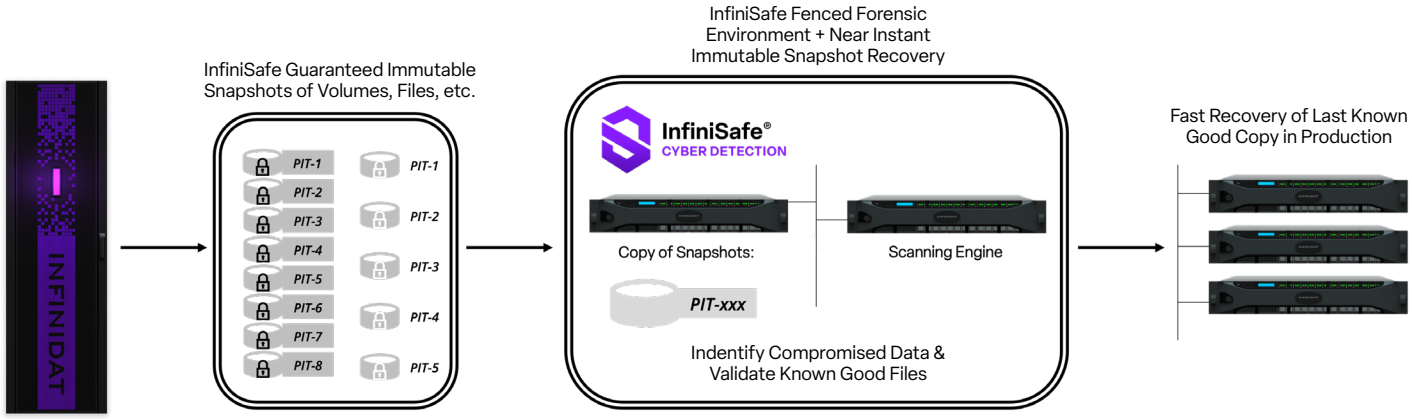
Today, companies have complex and multilayered environments that comprise many tools, monitoring systems, and processes. At the center, many have dedicated Security Operations Centers (SOC). Within the SOC, there are a number of applications designed for infrastructure security including many labeled as SIEM (Security Information and Event Management) and SOAR (Security Orchestration And Response) solutions. SIEM and SOAR environments are the center point of collection for most everything related to security as soon as an issue is detected. The next step is to create a well-defined and orchestrated process that is executed at the speed of compute without the need for slow human intervention. Sub-seconds matter and executing near-instantaneously is important to have a chance at limiting exposure.

How do we achieve this? Simple. For years now we have had our InfiniSafe capabilities available in our products. We have a powerful reference architecture for InfiniSafe for the InfiniBox family that is easily extended and orchestrated to be triggered by any event, anywhere. In this case, it could be triggered by a company's SIEM or SOAR environments. These application environments have extensible interfaces, via APIs or CLIs; tying them together with the well-defined InfiniSafe reference architecture provides a fully automated set of capabilities that can be orchestrated to proactively and quickly create immutable snapshots to protect your most critical primary data assets.



Validate the Data and Recover Quickly

InfiniSafe also has the ability to orchestrate the creation of a fenced forensic environment, a private clean network space apart from a possibly affected internal user network or systems. You can, and should have a dedicated set of resources outside of production to test and validate your data with the associated tools and software needed. InfiniSafe can then instantly present immutable snapshots of volumes or file systems to the fenced forensic environment, attach them, and utilize all the tools at your disposal to validate your data. We can help with that validation process as well, with powerful and insightful tools.



InfiniSafe Cyber Detection is an add-on solution to the otherwise no-cost components of InfiniSafe. InfiniSafe Cyber Detection performs deep scanning of block, file, and database stores by presenting InfiniBox and InfiniBox™ SSA immutable snapshots to a powerful AI-based scanning engine. The scanning is to validate data integrity and through AI-based machine learning, identify any malicious changes as a result of a cyberattack. More importantly, scanning uses more than 200 data points to determine which data may have been compromised with 99.5% accuracy. This level of accuracy and detail makes any additional forensics highly defined and easy to act on by minimizing any possible false positives because you need to be fast and accurate when dealing with a cyber event. Extending this functionality to InfiniSafe Cyber Detection requires the purchase of appropriate capacity licensing for scanning.

Summary

Bad actors create chaos and gain leverage over your most critical data assets if you are not prepared. Knowing the state of your data by proactively keeping it protected, beyond just scheduled events, is a key component to reducing the threat window, gaining back leverage, and thwarting those looking to extort you by compromising your data.

sales@infinidatfederal.com

INFINIDAT FEDERAL