IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Data Centre and Virtualization

Taking Cyber Storage Resilience to the Next Level

Guy Kariv

Guy Kariv
Chief Technology Officer EMEA
Infinidat

Biography

Guy Kariv is Chief Technology Officer EMEA at Infinidat (https://www.ininfidat.com).

An industry veteran, Guy has many years of experience in various disciplines of the IT industry, ranging from primary storage and data protection to applications, cyber security and cloud.

As field Chief Technology Officer, EMEA, Guy is helping Infinidat's customers to transitions their storage infrastructure into modern, business driven, IT-as-a-Service operations, improving business agility while reducing operational overhead.

Guy blogs at https://www.infinidat.com/en/blog/

Keywords Cyber storage resilience guarantee, Storage innovation, Data protection, InfiniBox, IT infrastructure
Paper type Research

Abstract

In February 2022, Infinidat announced InfiniSafe®, its comprehensive cyber resilience[1] architecture, which covers both primary and secondary storage, providing four pillars of protection: immutable snapshots, logical air-gapping, a fenced forensic environment, and near-instantaneous cyber recovery. All of these features are an inherent part of InfuzeOS™, its core operating system that is the driving force at the heart of all its storage devices – the InfiniBox® and InfiniBox™ SSA primary storage solutions, as well as the InfiniGuard® secondary storage platforms. In this article, the author looks at how Infinidat has gone well beyond what most other storage companies provide with guarantees on the immutability of its snapshots and recovery times to create the first cyber storage resilience guarantee on primary storage in the industry.

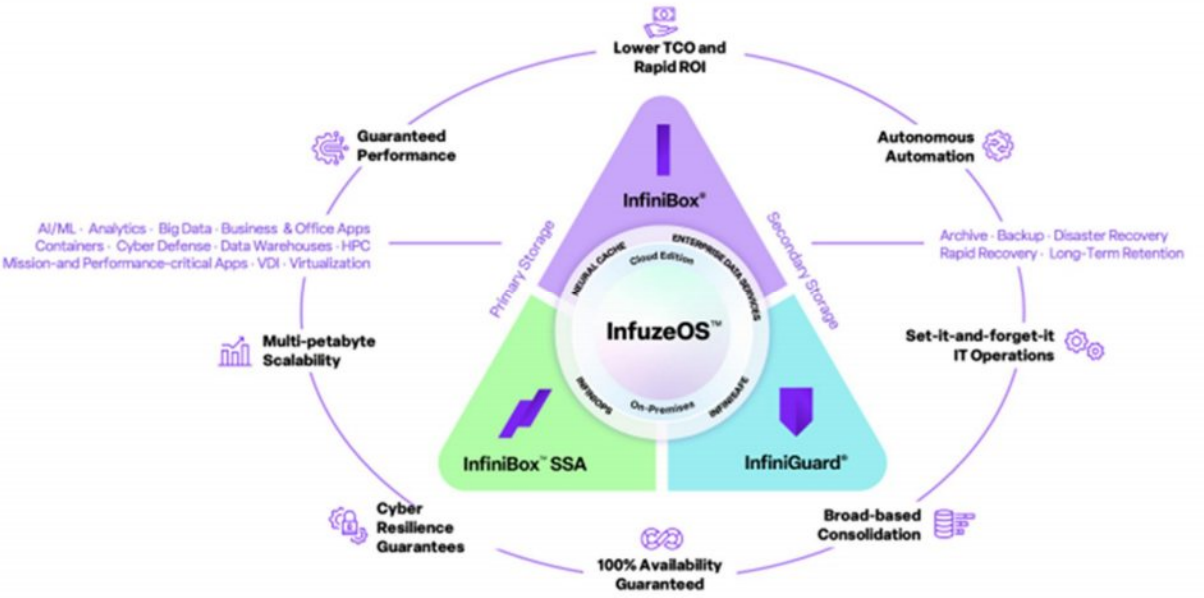
Introduction

Over the last decade, IT infrastructure vendors have been adding guarantees on their storage platforms that have definitively improved the ownership experience for enterprise storage, but they have always stayed away from the topics of performance and recovery time. With its new performance and cyber storage recovery guarantees, Infinidat is breaking new ground in these areas in ways that drive meaningful value for their enterprise customers.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Cyber resilient storage is among the most important and highly demanded requirements of enterprises today to ensure exceptional cybersecurity and combat cyberattacks across the entire storage estate and data infrastructure. In recent research, IDC found that 87% of organizations impacted by ransomware in the past year had to pay a ransom to recover their data. At Infinidat we help organizations avoid having to pay the ransom, yet still retrieve their data, uncompromised and intact, through rapid cyber recovery. By extending cyber resilience to our InfiniBox and InfiniBox™ SSA II enterprise storage platforms with the InfiniSafe Reference Architecture including our InfiniGuard® modern data protection and purpose-built backup platform, Infinidat can provide its immutability snapshot guarantee and the recovery time of immutable snapshots at one minute or less.



IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

One of the critical components of the InfiniSafe architecture is the fenced forensic environment, which provides the ability to spin up immutable copies of primary or backup data[2] in an isolated environment without affecting production operations. When we designed the fenced forensic environment concept, the idea was to provide the infrastructure that allows customers to validate the immutable, protected copies of data, which then enables the use of cyber forensic tools to detect possible ransomware and cyberattacks. It also provides an indication to the infiltration point in time, providing a clear understanding of the point in time, which is safe to recover to, in case of such an attack – referred to as the "last known good copy."

At the time of the initial release, InfiniSafe provided the core capabilities of the fenced forensic network, but we relied on external tools to do the actual scanning of data to come up with a known good copy of the data to execute the recovery. Our motivation at the time was to provide our customers the infrastructure needed to enable validation tools in a secure and fenced environment and evaluate the key requirements for validation and scanning tools together with our valued customers. The aim was to provide them with a tailored fit and (not generic) general-purpose signature-based tools, like antivirus, for example.

As InfiniSafe gained traction, with many of our enterprise customers already using it in production to protect their data, and with cybercrime soaring to new levels, coupled with a constant evolution of ransomware tools becoming more sophisticated with every passing day (see new ransomware attack release earlier this year, targeting vSphere VMFS datastores[3]), we came to understand that detecting and alerting of zero day attacks, where no known signature of the ransomware tool exists in the field, is of the highest value to our customers.

With that understanding in mind, it became clear that the next phase evolution of InfiniSafe would have to be driven by machine learning algorithms that can analyze previously unknown data patterns and make educated decisions based on entropy detection and multiple other data points, all resulting in targeted and timely alerts regarding suspected ransom infiltration into the customer data assets.

Being a leader in data classification algorithms, we set out to the task and today we are announcing the newest addition to the InfiniSafe family of technologies: InfiniSafe Cyber Detection.

InfiniSafe Cyber Detection is an add-on cyber storage software package, which as a best practice, is designed to run inside the fenced forensic environment on dedicated hardware. It uses sophisticated machine learning algorithms to scan data over time, generating a baseline score for the data patterns on the system and then detecting changes on those patterns in a specific point in time. Security and storage teams are alerted to a potential infiltration of a dormant ransomware attack, which is slowly corrupting the data overtime, waiting for the D-day to proverbially "drop the bomb."

While the above description is intentionally over simplistic, InfiniSafe Cyber Detection is, in fact, a very sophisticated piece of software that uses over 200 analytics that represent changes in value of the file content and metadata from one


IT for CEOs & CFOs is published by House of Words Media Limited.

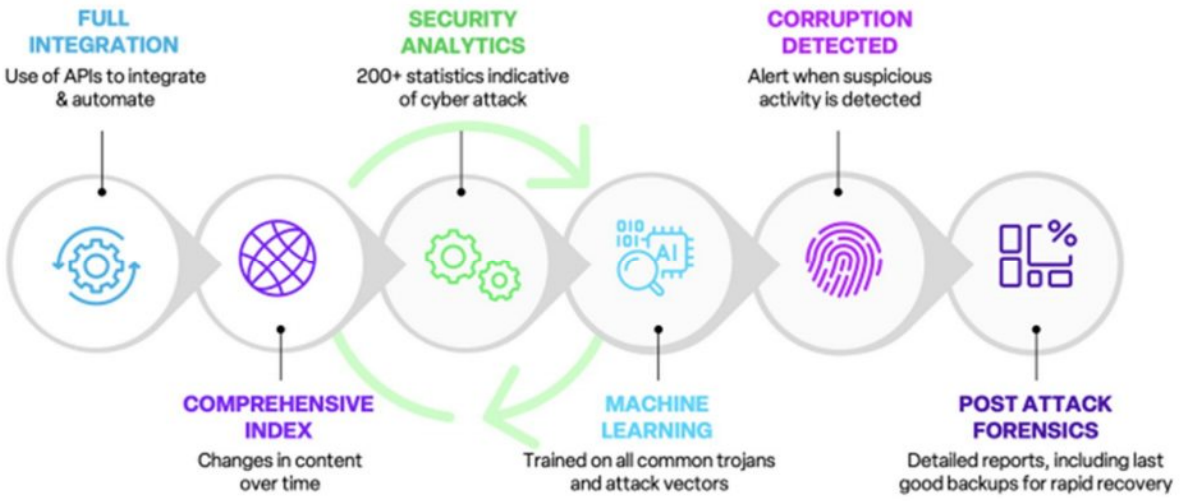
The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

observation to the next. These are then fed to machine learning algorithms in order to make probabilistic decisions regarding data integrity.

Dave Vellante, Chief Analyst, Wikibon noted why our new cyber detection product is significant: “Customer data shows that cybersecurity is the #1 priority for IT decision makers… The company has a history of combining technical differentiation with business value and the new InfiniSafe Cyber Detection system and InfuzeOS Cloud Edition appear to continue this pattern. Customers increasingly demand simplicity and cost savings that can directly impact the bottom line and Infinidat's latest announcement aim to do just that.”

Phil Godwin, COO and President, Clear Technologies sees Infinidat’s expansion with InfiniSafe Cyber Detection as a strong benefit to his enterprise customers: “Infinidat continues to expand its cyber storage resilience solutions by adding cyber detection capabilities for primary storage. Not only does Infinidat give us the solutions we need to click all our customers’ critical selection boxes, but the company is also solidifying its leadership in enterprise storage. Infinidat drives the right solutions for our enterprise customers' needs.”

The machine learning engine itself is trained using data sets representing many different pre- and post-attack environments, with all known ransomware variants and tuned to detect even slight anomalies in the data pattern, which was measured to be 99.5% accurate.

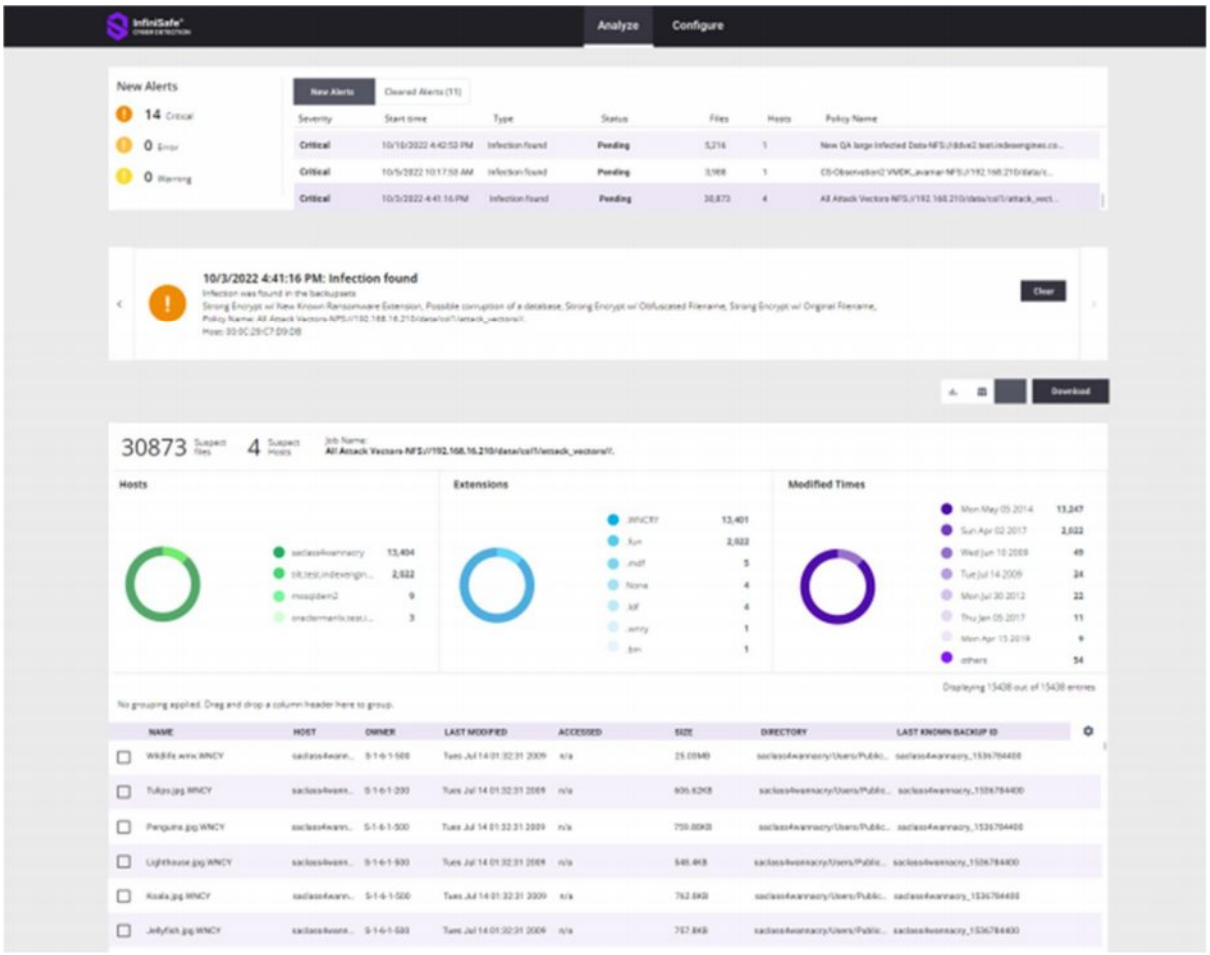


The indexer used to scan through the data is very robust, and, also, efficient, supporting the scanning and indexing of petabytes of data. Being the standard in enterprise storage, this makes it perfect for the petabyte-scale, enterprise-grade line of thinking[4], which is always at the heart of every Infinidat product. Additionally, the indexing processes are aware of the internal data structure of dozens of applications and datasets, enabling the solution to support a variety of enterprise-grade, mission-critical applications as well as secondary storage use cases.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Furthermore, the robust indexing engine makes it easy to drill down inside of storage resources provisioned on the storage systems and enables InfiniSafe Cyber Detection to provide comprehensive reports in case of a suspected ransomware attack that can point to infection, even at the single file level.



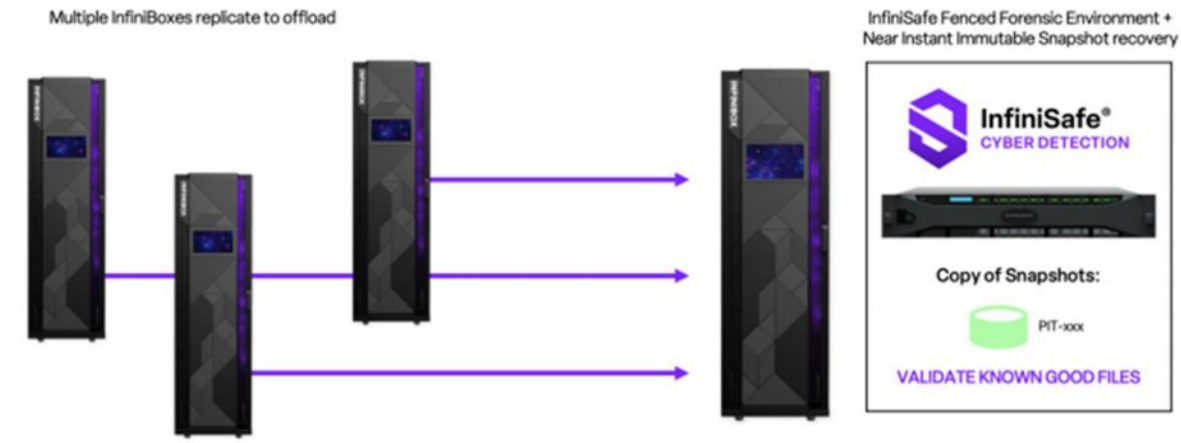
One critical component of InfiniSafe Cyber Detection is the automation[5] that is required to orchestrate the routine, day-by-day scanning of multiple storage resources in a petabyte-scale environment.

As we understand that such operations cannot be performed manually as it would generate an unacceptable management overhead, we made sure that our new cyber detection capabilities would take care of the entire process: starting by the creation of point in time copies of the customer data, protected and immutable by InfiniSafe[6], followed by securely mounting them in the fenced forensic environment, orchestrating the scanning process and all the way through generating timely alerts in case of a suspected ransomware attack. The scanning process can be performed on the production system, as InfiniBox and InfiniBox SSA storage platforms are highly efficient in creating and managing tens of thousands of penalty-free snapshot copies of data.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Alternatively, the process can be offloaded to a dedicated InfiniBox system located in an environment with elevated security and even scan data coming from multiple source systems in a fan-in topology.



In conclusion

As cybersecurity continues to be one of the top concerns of CEOs and senior leadership teams, Infinidat made it a priority to enhance its InfiniSafe cyber storage resilience solution portfolio with cyber detection. Infinidat is now one of the very few storage vendors to offer cyber detection on primary storage. Infinidat equips enterprises with stronger cyber storage resilience capabilities to counter cyberattacks against their data infrastructure in the face of increasing cyber threats.

InfiniSafe Cyber Detection is designed to help enterprises resist and quickly recover from cyberattacks. It provides highly intelligent deep scanning and indexing needed to identify potential issues. InfiniSafe Cyber Detection inspects the full breadth of files, applications, core storage infrastructure (such as volumes), and databases for

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

signs of cyber threats for primary storage environments, helping ensure all data that needs to be recovered has integrity.

InfiniSafe Cyber Detection uses advanced machine-learning models that provide 99.5% confidence in detecting cyber threats. This helps dealing with false positive/ negatives and greatly reduces the effort in any additional forensics. Over 200 points of determination are included, using content-based analytics that inspect inside files for even subtle signs of attack. The post-attack dashboard (with forensic report) details the last known good copy of the data for rapid, intelligent recovery.

InfiniSafe Cyber Detection will be available in the second half of 2023 with the initial release supporting both primary applications and backup uses cases running on InfiniBox and InfiniBox SSA II storage systems. It will focus on block volumes and file systems containing user data and mission-critical Oracle databases. There will then be a subsequent release to add support for InfiniGuard systems, as well as extending enterprise application support.

The new Cyber Detection addition to the InfiniSafe family of solutions will play a substantial role in our cyber resilience strategy for the upcoming years. This new technology is yet another testimony to Infinidat's commitment to securely manage enterprise-scale customer data, without compromise and with constant improvement and new functionalities that deliver the next level of cyber resilience.

Reference

1 https://www.youtube.com/watch?v=xq5ydg-Ggwc
2 Solution Brief - Stop Ransomware in its Tracks with InfiniGuard (r) InfiniSafe (r). Infinidat. Available at: https://www.infinidat.com/en/resource-pdfs/stop-ransomware-its-tracks-infiniguard-infinisafe.pdf
3 Abrams, L. (8 February 2023), New ESXiArgs ransomware version prevents VMware ESXi recovery. Bleeping Computer. Available at: https://www.bleepingcomputer.com/news/security/new-esxiargs-ransomware-version-prevents-vmware-esxi-recovery/
4 https://www.infinidat.com/en/solutions
5 https://www.youtube.com/watch?v=tOT6uXRJeys
6 https://www.itceoscfos.com/new-launches-for-infinidat