

Global Cybersecurity Regulatory Frameworks and Your Enterprise Storage Infrastructure

Reduce Your Cyberthreat Exposure



Eric Herzog – CMO



Tim Dales – Product Marketing Manager

April 2025

Review: InfuzeOS - One SDS Architecture, All Platforms

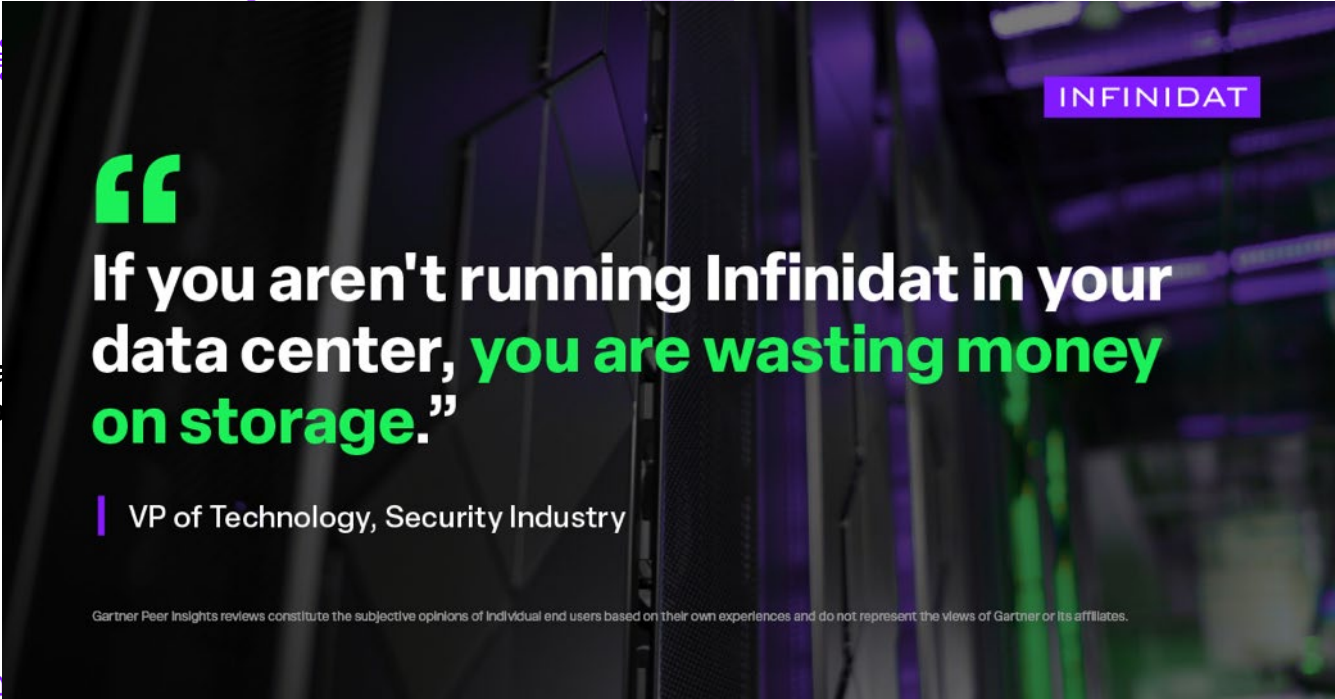
Use Cases:

- Performance-critical Apps
- Mission-critical Apps
- Business-critical Apps
- Containers
- Cyber Security
- AI/ML
- Analytics
- Big Data
- Business & Office Apps
- Data Warehouses
- HPC
- Hybrid Multi-Cloud
- VDI
- Virtualization

Guaranteed SLAs:

- Performance
- 100% Availability
- Cyber Storage Immutability
- Cyber Storage Recovery Time (RTO)

Lower TCO and Rapid ROI



Storage Suite

Broad-based Consolidation

100% Availability Guaranteed

Use Cases:

- Next Generation Data Protection
- Archive Backup
- Disaster Recovery
- Hybrid Multi-Cloud
- Instantaneous Recovery
- Long-Term Retention

Industry Acclaim: 2024



Outperformer - 2024 Radar Report for Primary Storage For Large Enterprises



InfiniBox™ SSA II Named One of Top 5 for Secure High-End Enterprise Storage



Six Time Gartner® Peer Insights Customers' Choice Award in North America



InfiniBox® and InfiniBox™ SSA a Leader - GigaOm Radar Report for Primary Storage v.5



CRN® Storage Vendor 100 for the Fifth Year in a Row



Capacity Storage Vendor of the Year Winner - Storage Awards - Capacity Storage Vendor of the Year



InfiniBox® and InfiniGuard® Named One of Top 5 2PB+ Cyber Secure Backup Targets in



Infinidat Named a 2024 CRN® Tech Innovator Winner for InfuzeOS™ Cloud Edition, and a Finalist for InfiniSafe® Cyber Detection



Eric Herzog - CMO of the Year 2024



Infinidat - Finalist for Infrastructure and Storage Manufacturer of the Year



InfiniBox® a Leader in 2024 Radar Report for Storage M



Eric Herzog - CMO to Watch 2024 by the CMO Alliance



InfiniBox® G4 "Best of Show" for "Most Innovative Hyperscaler Implementation"

Editor's Choice - Winner - Eric Herzog - Choice - Product of the Year - InfiniGuard - Runner-up - Best of Show - Performance, Backup and Optimization



Eric Herzog - 2024 CRN® Inclusive Channel Leaders



Steve Sullivan - 2024 CRN® Channel Chief



James 'JT' Lewis - 2024 CRN® Channel Chief - EMEA and APAC



Lynsy Marshall Top 100 Channel Marketing Leader - Channel Insider



Product of the Year Finalist - SSA Express



Infinidat named one of the World's Top 50 Marketing Teams



Lynsy Marshall CRN 2024 Women of the Year Finalist



One of 2024's 50 Coolest Software-Defined Storage Vendors



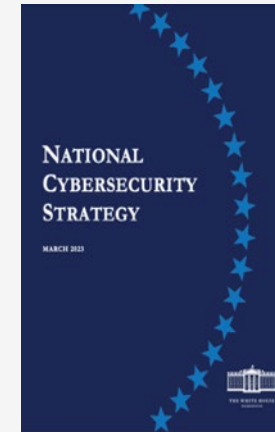
Eric Herzog 2025

Cyberattacks are Extensive and Expensive!

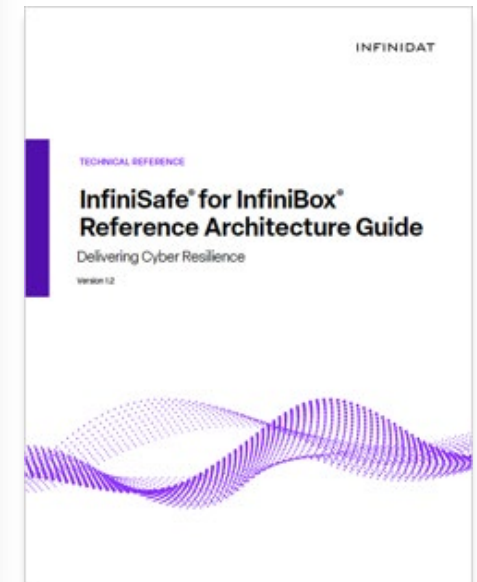
Headline News

World @ Business @ Finance @ Travel @ Sport @ Weather

- Cybercrime will cost enterprises **\$10.5 Trillion** in 2025
- Cyber security is the **#1 concern of CEOs globally** (PwC Pulse CEO survey, Oct 2024)
- US releases **National Cybersecurity Strategy v2** (Tighter compliance and cybersecurity reporting. EU Cyber Resilience Act in force, Dec 2024)
- Enterprises suffer **1,636 cyberattacks per week** (up 30% over 2024)
- Demand for cybersecurity experts exceeds supply! **27%** of jobs are vacant – **Skills Gap**
- World needs to cyber protect **200 Zettabytes** in 2025



InfiniBox™ SSA II Named
One of Top 5 Cyber
Secure High-End All-
Flash Arrays for
Enterprise Storage



Current State of NIST CSF 2.0

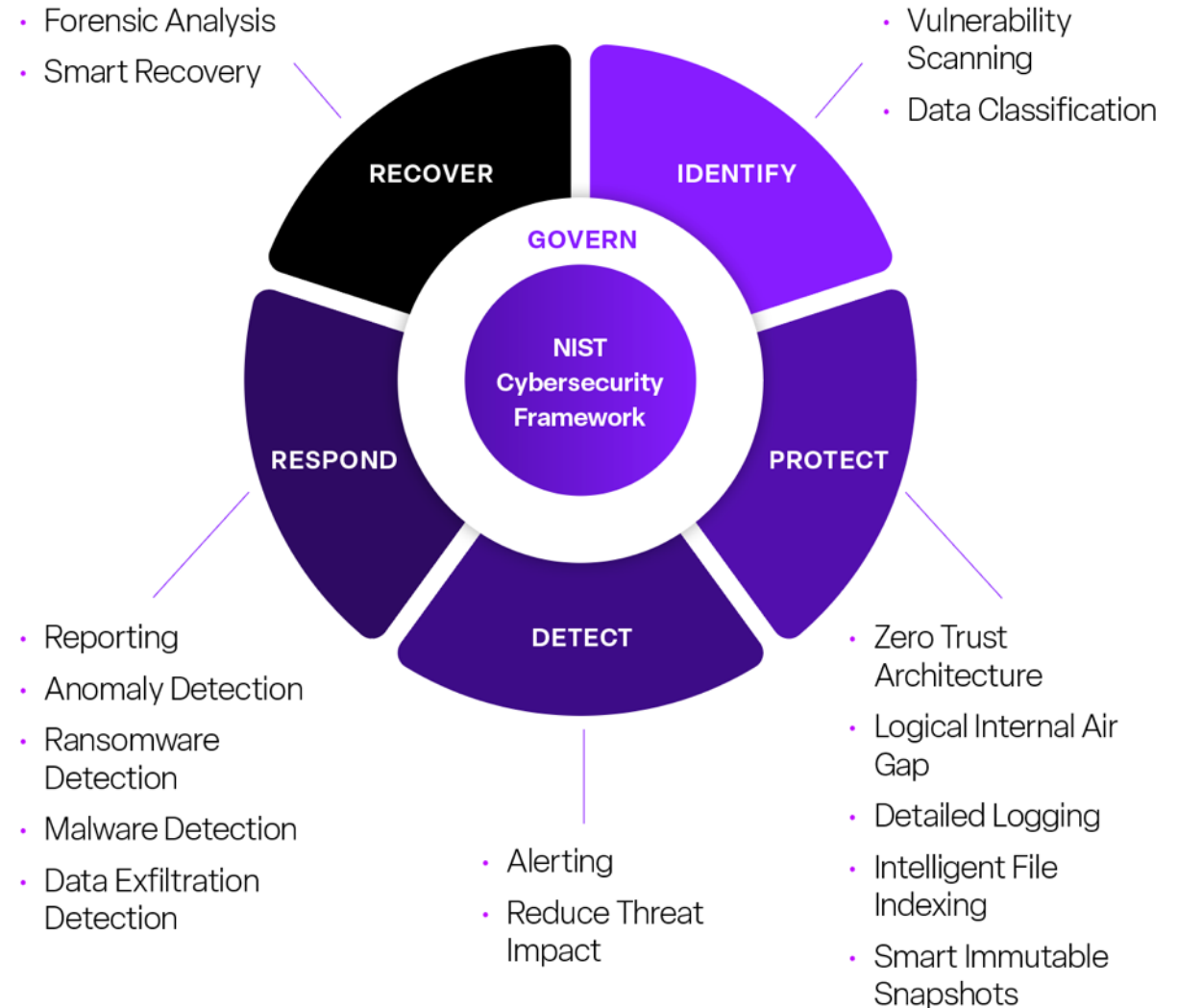
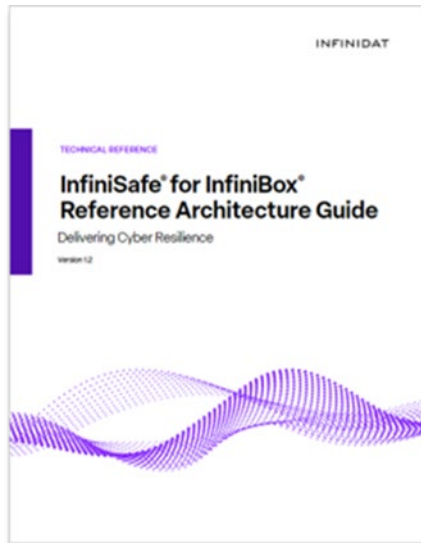
- Developed and published in 2014 to help organizations worldwide easily and effectively manage cybersecurity risk
- Most widely adopted security framework across all industries, worldwide
- CSF 2.0 (Feb 2024) update of this framework
- Adding the “Govern” function as a core function that informs how the other five functions are implemented



<https://www.nist.gov/cyberframework>

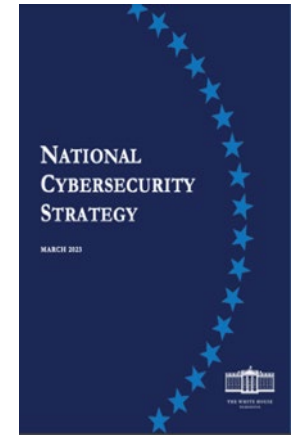
How Does CSF 2.0 Map to Storage?

- Cyber Storage Capabilities Mapped to the NIST CSF
- The InfiniVerse Cyber Resilience Services of InfiniSafe fulfills all the NIST CSF 2.0 core functions



Impact of Cyber Regulations Worldwide - USA

- National Cybersecurity Strategy Implementation Plan v2 (May 2024)
 - Introduces 31 additional initiatives, 6 additional agencies
 - Key Additions include:
 - Healthcare Sector Security
 - Education Facilities
 - Supply Chain Risk Management
 - Ransomware Mitigation
 - Software Security
 - Emerging Technologies
- Led by the **Office of the National Cyber Director (ONCD)** within the White House



Impact of Cyber Regulations Worldwide - USA

Regulation	Key Focus	Enforcement Agency
Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Guidelines	Cyber risk management for banks & financial institutions	FFIEC (Fed, OCC, FDIC, CFPB, NCUA, etc.)
SEC Cybersecurity Rules (2023-2024)	Requires public companies & investment firms to disclose cyber risks & incidents	SEC (Securities & Exchange Commission)
New York DFS Cybersecurity Regulation (NYCRR 500, 2017, Updated 2023)	Strict cybersecurity & third-party risk management for financial institutions	New York Department of Financial Services (NYDFS)
Federal Reserve's SR 21-3 (2021)	Risk management for third-party IT service providers in financial services	Federal Reserve



Impact of Cyber Regulations Worldwide - EU

- NIS2 - (Network and Information Systems)
- Directive aims for a high common level of cybersecurity across the European Union providing legal measures to boost the overall level of cybersecurity in the EU
 - Improve cybersecurity risk management
 - Introduce reporting obligations across sectors such as energy, transport, health, and digital infrastructure, starting into force in 2023.
- Member States had until 17 October 2024 to transpose the NIS2 Directive into national law
- 23 Member states (of 27) failed to comply – put on notice!
- As of March 2025 – 7 have fully transposed NIS2



Impact of Cyber Regulations Worldwide - EU

- **DORA - (Digital Operational Resilience Act)**
- Regulation aims to strengthen the IT security of financial entities such as banks, insurance companies and investment firms and make sure that the financial sector in Europe can stay resilient in the event of a severe operational disruption, like a cyberattack.
- Adopted on December 14, 2022, and entered into force on January 17, 2023
 - Compliance deadline: January 17, 2025
 - Legally binding
- Accompanying **Directive (EU) 2022/2556** – still being transposed
- National competent authorities within each EU member state are responsible for overseeing the implementation of DORA
 - For example: in Germany, the Federal Financial Supervisory Authority (BaFin) has provided guidance and resources to financial entities in aligning with DORA requirements



Impact of Cyber Regulations Worldwide - UK

- **UK GDPR and Data Protection Act (2018)**

- Requires organizations to protect personal data
- Breach notifications within 72 hours



- **NIS - (Network and Information Systems) 2018 Updated 2024**

- Across sectors such as energy, transport, health, and digital infrastructure



- **Product Security and Telecommunications Infrastructure (PSTI) Act (2022)**

- Consumer product security, IoT devices



- **Telecommunications Security Act (2021)**

- Strengthen cyber security in Telecom sector

- **National Cyber Security Center**

- Reduces risks to the UK by securing public and private sector networks
- Provides incident response



Impact of Cyber Regulations Worldwide - Japan

- **The Basic Act on Cybersecurity** (v 2022) - sets a basic policy for Japan's cybersecurity initiatives, clarifying responsibilities of the national and local governments, and creates a national cybersecurity strategy
- Working in conjunction is: **Basic Act on the Formation of an Advanced Information and Telecommunications Network Society**
- Creates the **National Center of Incident Readiness and Strategy for Cybersecurity (NISC)**
 - The country's central government agency responsible for cybersecurity policy, coordination, and incident response



Impact of Cyber Regulations Worldwide - Japan

- **Cybersecurity Guidelines for Critical Infrastructure**
 - Issued by NISC to protect finance, energy, healthcare, and telecom
- **Telecommunications Business Act** (Revised 2022)
 - Secure networks, report cyber incidents, foreign cyber threats
- **Financial Services Agency (FSA) Cybersecurity Regulations**
 - Regular cybersecurity audits and incident reporting
- **Industrial Cybersecurity Guidelines**
 - Issued by Japan's Ministry of Economy, Trade and Industry (METI)
 - Secure supply chains and IoT security



Infinidat Alignment with NIS2



27.12.2022

EN

Official Journal of the European Union

L 333/80

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Directive 2022/2555 – on measures for a high common level of cybersecurity across the Union

NIS2 Directive

- <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555>

Infinidat Alignment with NIS2



NIS2 - Article 21 - Cybersecurity Risk-Management Measures

Directive	Infinidat Approach
a) Policies on risk analysis and information system security	Our TAs can assist with policy formulation. Also, NIST Doc can help. NIST SP 800-209 (2020) Security Guidelines for Storage Infrastructure.
b) Incident handling	Preemptive incident handling with InfiniSafe, seamlessly integrates with data center-wide SIEM or SOAR cyber security software or a SOC.
c) Business continuity, such as backup management and disaster recovery, and crisis management	InfiniSafe Cyber Detection recovers known good data from a backup, ready for near instantaneous recovery - guaranteed. InfiniBox has comprehensive data replication capabilities for DR.
d) Supply chain security, including security-related aspects - the relationships between each entity and its direct suppliers or service providers	Customer specific.

Infinidat Alignment with NIS2



NIS2 - Article 21 - Cybersecurity Risk-Management Measures

Directive	Infinidat Approach
e) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	Customer specific. Our TAs can assist.
f) Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Professional Services can setup and test effectiveness.
g) Basic cyber hygiene practices and cybersecurity training	Customer specific. Infinidat can assist with the enterprise storage part of cyber hygiene and provide InfiniSafe cybersecurity training.
h) Policies and procedures regarding the use of cryptography and, where appropriate, encryption	We encrypt data at-rest by default. Support KMIP protocol. Integrate with Thales and IBM Guardium.

Infinidat Alignment with NIS2



NIS2 - Article 21 - Cybersecurity Risk-Management Measures

Directive	Infinidat Approach
i) Human resources security, access control policies and asset management	RBAC on the storage array. User permissions and access controls are compliant with NIST SP 800-209 (2020) Security Guidelines for Storage Infrastructure Section 4.3 - Authentication and Data Access Control. Also supported through AD / LDAP authentication. Support for CyberArk CPM, PSM and SSO using SAML2.
j) Use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Infinidat storage supports MFA from several vendors, including Okta, Cisco Duo and Microsoft Entra ID. Also, support for open standard SAML2.

InfiniSafe is Next-Gen Data Protection and Recovery

A Cyber Focused, Recovery First Strategy



InfiniSafe®

- InfiniSafe is recovery first focused!
- InfiniSafe is
- InfiniSafe is
- InfiniSafe Cyber Stack
Protection (

- InfiniSafe Cyber Stack

- Immutable snaps, Logical/Remote Air gaps, Fenced

Near instant recovery

Integration with SecOps (SIEM/SOAR)

Single Snaps

Point-in-time window

Immutable Snaps

For data validation

Protection

Protection rate

Ability to determine issue

Reporting

Status of your data

- Subscription Licensed

INFINIDAT

“
**Because we are concerned about cyber threats,
we use InfiniSafe. This is an excellent solution to
improve the cyber resilience of our storage.**”

CTO, Transportation | InfiniBox®

Gartner Peer Insights reviews constitute the subjective opinions of individual users based on their own experiences and do not represent the views of Gartner or its affiliates.



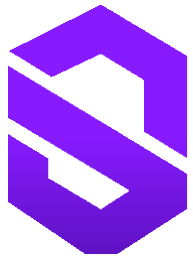
+



“On average, companies face about **22 days of downtime**, as reported by Coveware. However, some companies can be incapacitated for months...”

<https://www.xitx.com/2024/06/how-long-are-companies-down-after-a-cyberattack-understanding-ransomware-recovery/#:~:text=On%20average%2C%20companies%20face%20about,the%20attack's%20severity%20and%20complexity.>

InfiniSafe Cyber Stack



InfiniSafe[®]
CYBER DETECTION



LOGICAL AIR-GAPPING



IMMUTABLE SNAPSHOTS



FENCED FORENSIC ENVIRONMENT

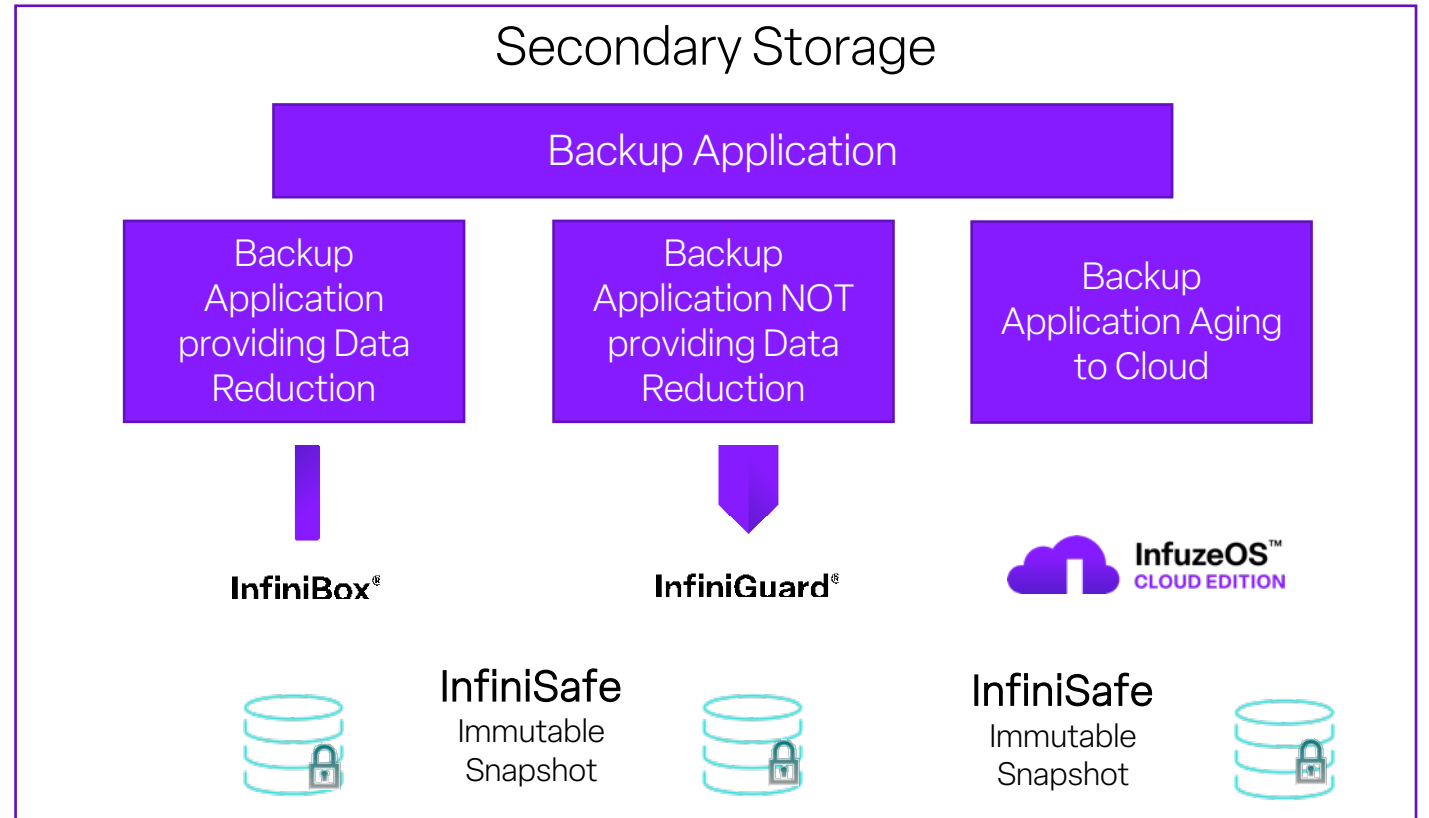
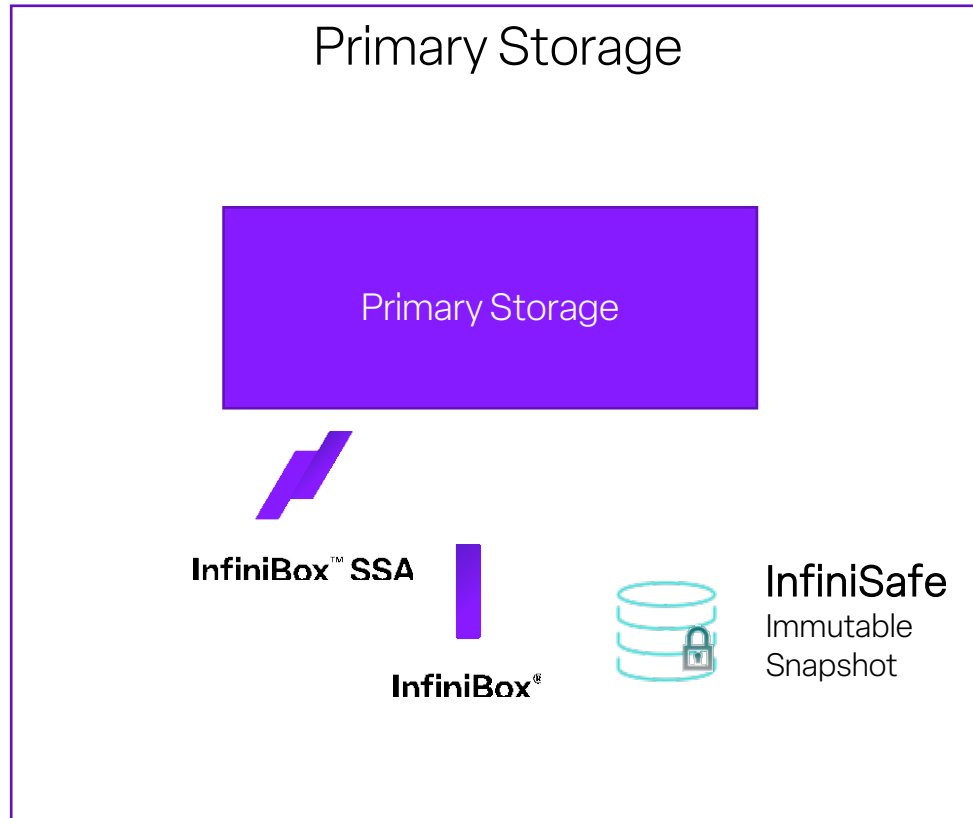


NEAR INSTANTANEOUS RECOVERY



AUTOMATED CYBER PROTECTION

Cyber Resilient Storage Enabled by InfiniSafe



InfiniSafe Cyber Storage Resilience Guarantees

- Guaranteed immutability of InfiniSafe immutable snapshots
- Recovery time guarantee of those immutable snapshots
 - Less than 1 minute for InfiniBox SSA II and InfiniBox
 - Less than 20 minutes for InfiniGuard
 - Regardless of immutable snapshot size

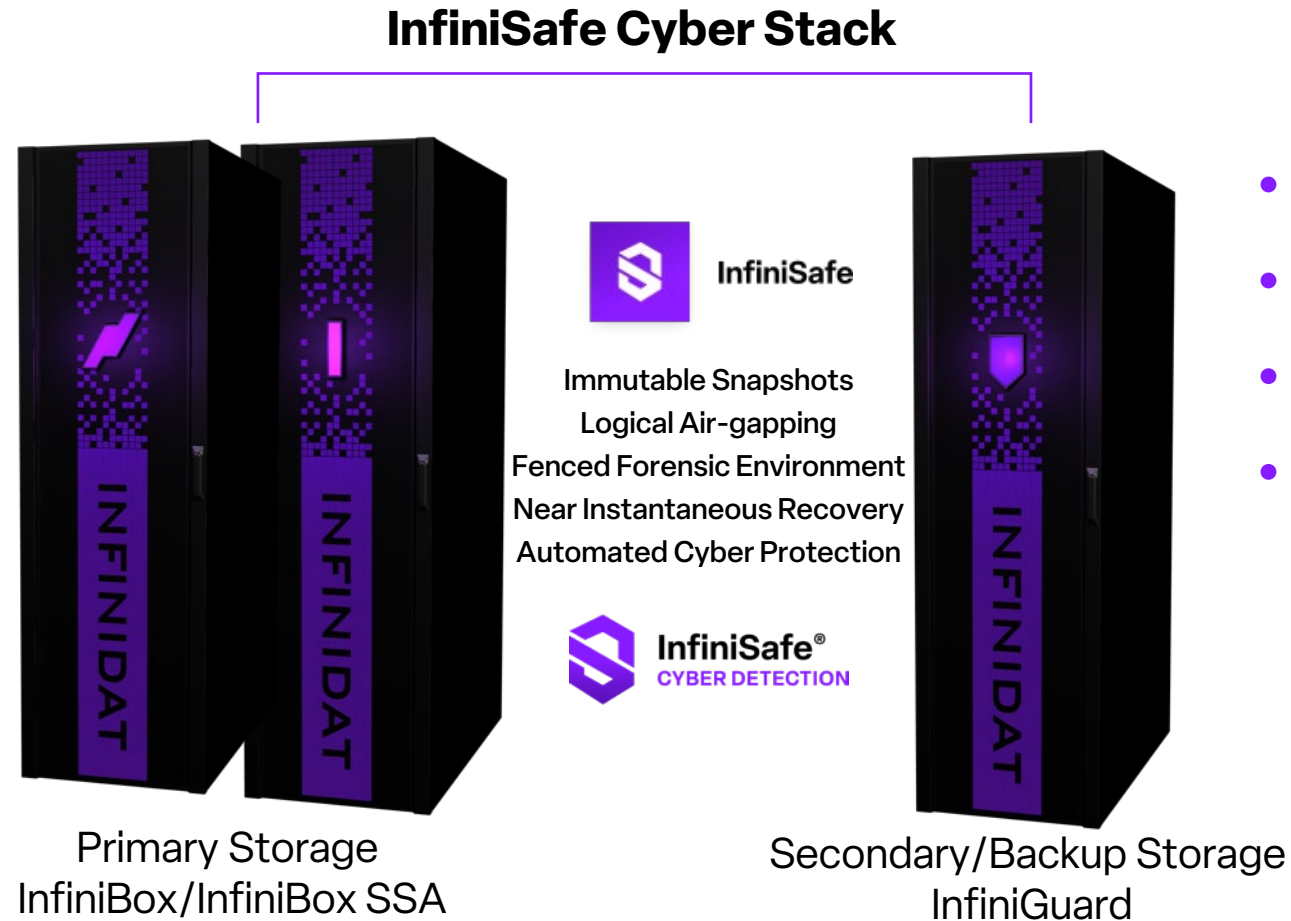
InfiniSafe Cyber Storage Resilience

- Immutable Snapshots
- Logical air-gapped protection
- Fenced forensic environment
- Near-instantaneous recovery of any size backup repository
- Seamless integration to cyber security software: InfiniSafe Automated Cyber Protection (ACP)
- AI-based scanning for cyber threats: InfiniSafe Cyber Detection

InfiniSafe – Same Functionality Optimized by Solution

Consistent Cyber Resilience

- Built into InfuzeOS
- Flexible Integration
 - Reference Architecture
 - API first integration methodology
- Guaranteed!
 - Immutability
 - RTO – 1 Min or Less



- Built Into InfuzeOS
- Purpose Built
- Fully Orchestrated
- Guaranteed!
 - Immutability
 - RTO – 20 Mins or Less

InfiniSafe Automated Cyber Protection



InfiniSafe®

Reducing the threat window!

- Data needs to be protected at the speed of “Compute”
 - Scheduling Immutable Snap is great, but leaves GAPS
 - Threat
 - Not
 - Trig

“Infinidat has carved out a very unique leadership position as the only storage vendor to offer an automated enterprise storage cyber protection solution that seamlessly integrates with cyber security software applications. Infinidat’s newly launched InfiniSafe Automated Cyber Protection (ACP) that easily meshes with the SIEM, SOAR or Security Operations Centers is exactly what enterprises need, to include enterprise storage as a comprehensive approach to combat cyber threats. This proactive cyber protection technique is extremely valuable, as it enables taking immediate immutable snapshots of data at the first sign of a potential cyberattack. This provides a significant advancement to ensure enterprise cyber storage resilience and recovery is integral to an enterprise’s cybersecurity strategy. ACP enhances an enterprise’s overall cyber resilience by reducing the threat window and minimizing the impact of cyberattacks on enterprise storage environments.”

Chris Evans
Founder and Principal Analyst
Architecting IT

- What is the difference between SIEM and SOAR?
- Both Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) are cyber-security tools that aggregate and correlate data from multiple sources to detect and respond to threats.
 - SIEM focuses on generating alerts from traditional infrastructure components,
 - SOAR takes in more data and automates the remediation and response process.

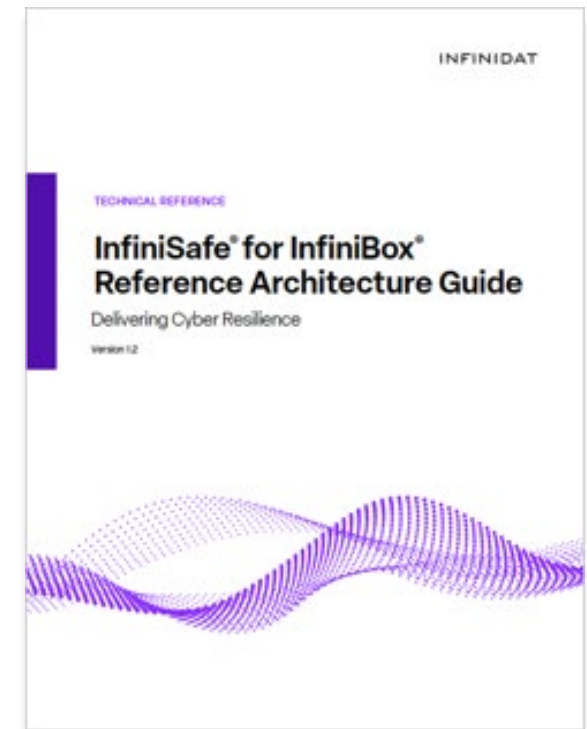
Source: <https://simonangling.com/what-is-security-orchestration-automation-and-response-soar/>





InfiniSafe ACP – Protection at the Speed of Compute

- Near Real Time – reduce the threat window!
 - Catch it as early as possible and reduce proliferation
 - Scheduled snapshots are proactive, but leave gaps
- API's and connectors are easily established to trigger immutable Snaps
 - Users determine the triggers from their SOC/SIEM/SOAR on what they feel are important events
 - Leverages generic syslog functions, can work even without SIEM/SOAR
- Immutable Snaps are Instant and have no affect on production!
- Can be orchestrated with InfiniSafe Cyber Detection scanning
 - Easily know if the data is good or compromised
 - End to End process automated – Reduces chaos in responding to an attack
- Time is MONEY.... Second/minutes can = \$\$\$\$Millions



InfiniSafe Ransomware and Malware Resistance

Cyber Detection Flexibility



Primary Storage

Volumes, App Workloads, Snapshots, VMware



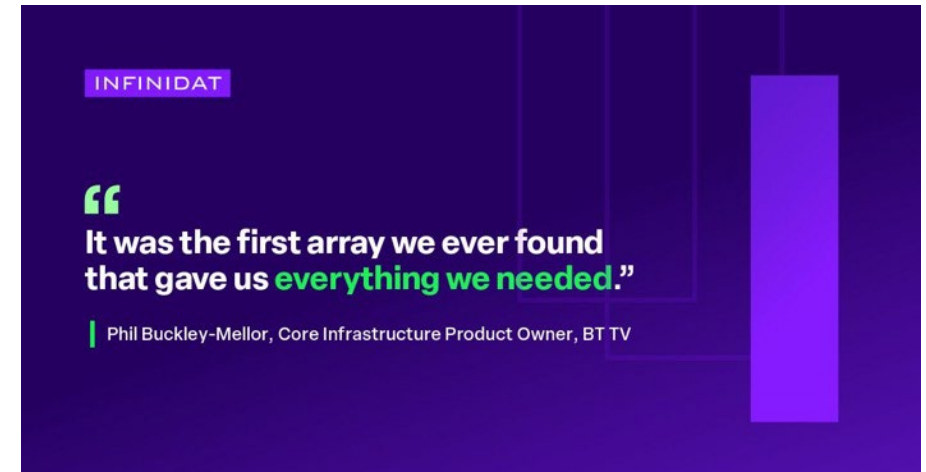
Databases

Oracle, DB2, SQL, SAP Hana, Cache, etc.



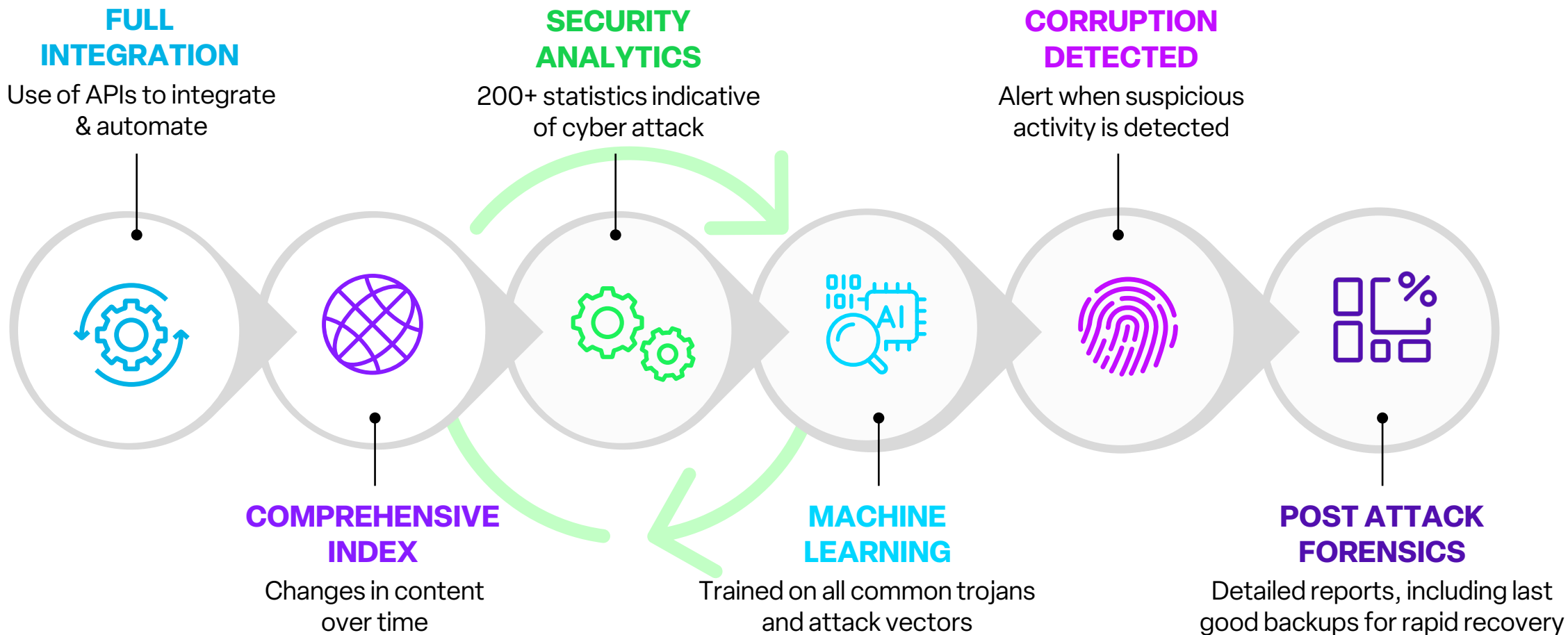
User Files

Contracts, Financial Docs, Intellectual Property, etc.



Cyber Detection Workflow

Analytics, Machine Learning and Forensic Tools to Detect and Recover from Cyberattacks



InfiniSafe Cyber Detection Early Warning System

- Multiple InfiniBoxes or InfiniBox SSAs replicate to one
- Cyber Detection offload “array” will scan all data files and tag any corrupted files, create forensic report
- Provides the intelligence needed to detect an attack

Multiple InfiniBoxes replicate to offload

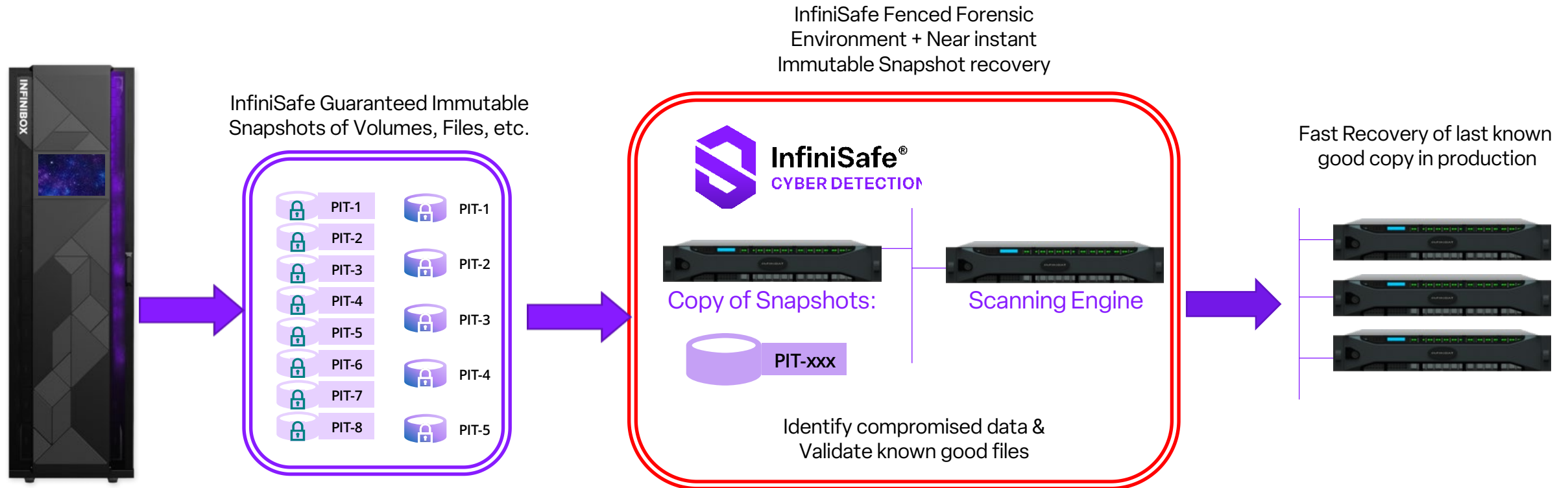


InfiniSafe Fenced Forensic Environment + Near instant Immutable Snapshot recovery



InfiniSafe Cyber Detection Solution

- Applications can validate immutable snapshots in Fenced Forensic environment
- Cyber Detection will tag any corrupted files, create forensic report
- Provides the intelligence needed to facilitate recovery



Cyber Detect Post Attack Dashboard

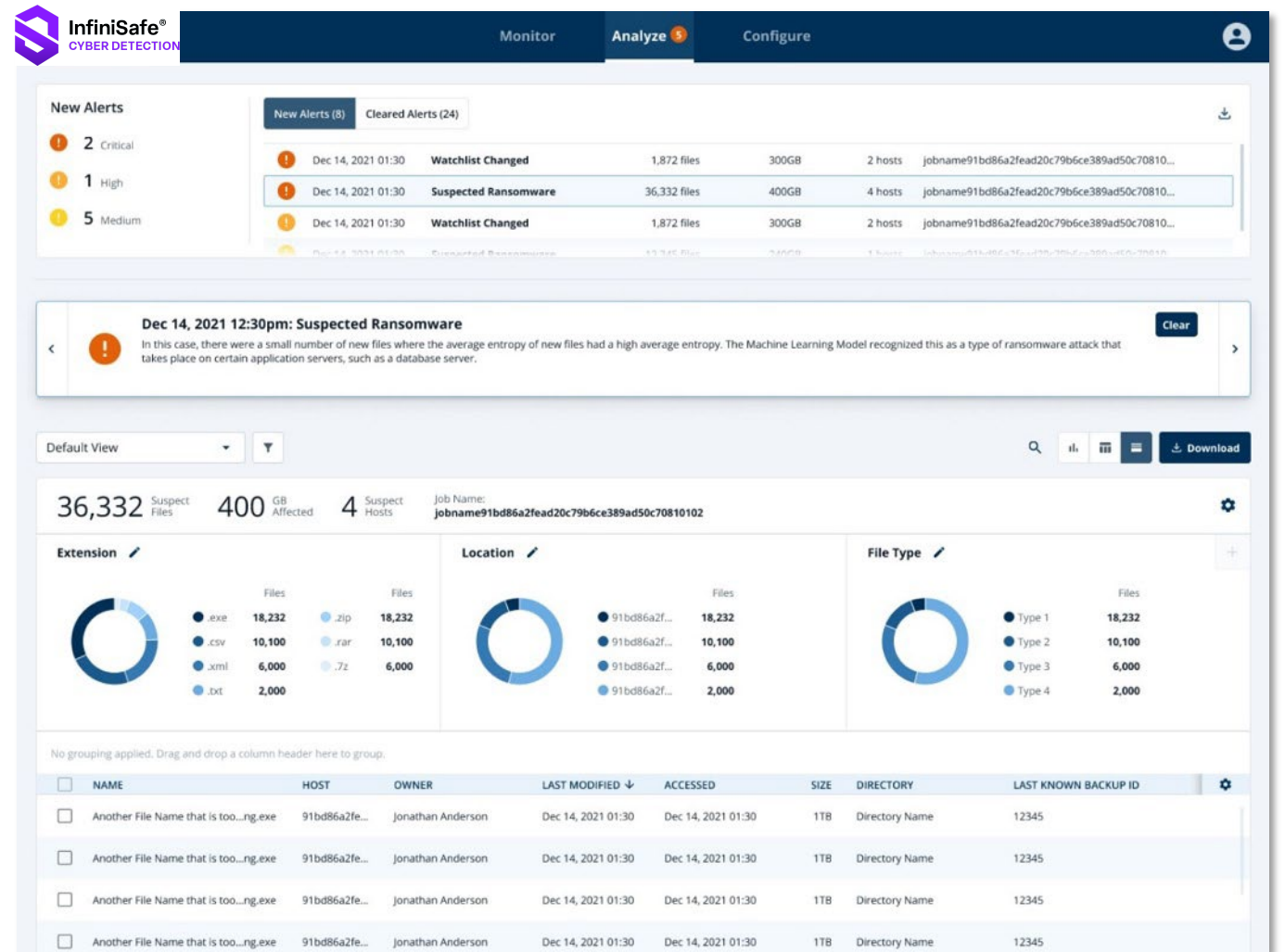
Improved user experience - More insight into data - Intuitive post attack workflow

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



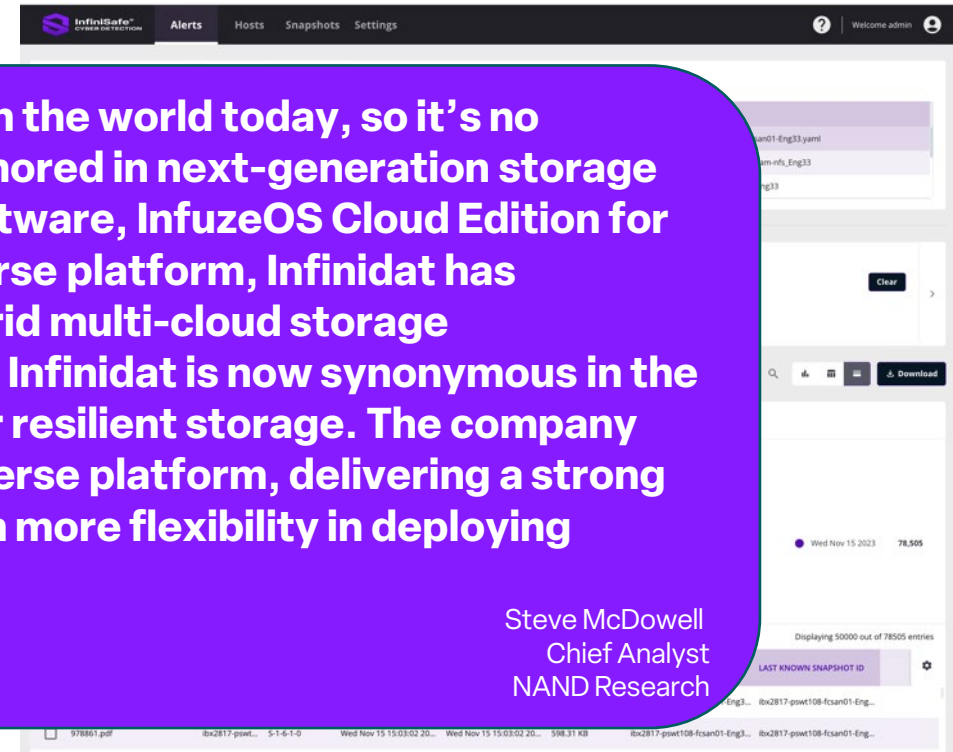
InfiniSafe Cyber Detection



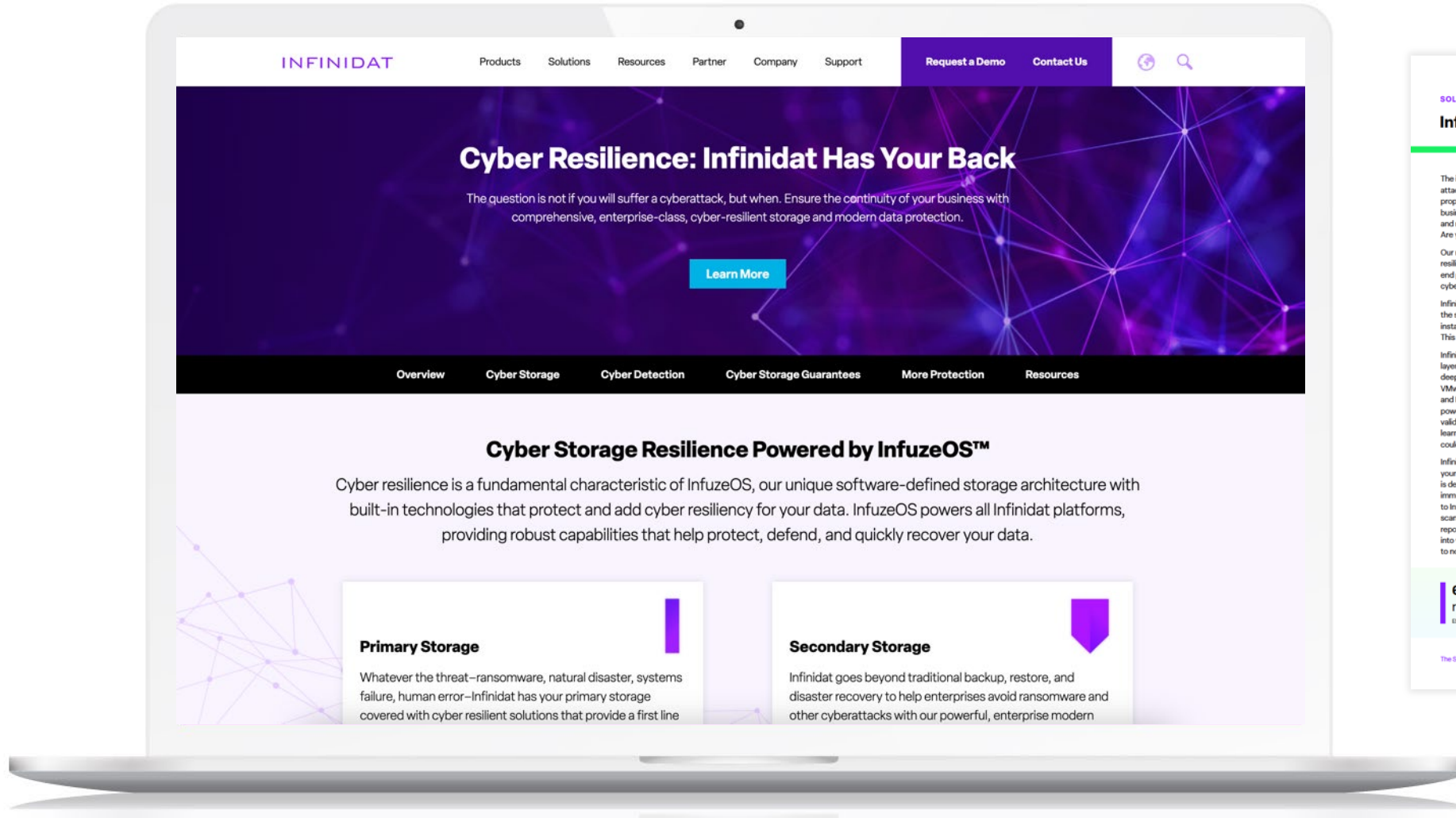
- Identify a VMware datastore to be scanned
 - Uses AI and ML technology to scan for malware
 - Warns of suspicious activity
 - Simplifies the process of identifying and isolating threats
 - 99% accuracy
 - Informs security operations

“Infinidat is one of the top enterprise storage companies in the world today, so it’s no surprise to see them launch compelling new solutions anchored in next-generation storage capabilities. With the new G4, the expanded InfiniSafe software, InfuzeOS Cloud Edition for Microsoft Azure, and all the enhancements on the InfiniVerse platform, Infinidat has solidified its position as a ‘go-to’ solution provider for hybrid multi-cloud storage infrastructures. It’s because of innovations like these that Infinidat is now synonymous in the enterprise with high performance and lower TCO for cyber resilient storage. The company is also making the right strategic investments in its InfiniVerse platform, delivering a strong Storage-as-a-Service offering that gives enterprises even more flexibility in deploying business-critical storage.”

Steve McDowell
Chief Analyst
NAND Research



Cyber Storage Resilience Web Page



<https://www.infinidat.com/cyber-resilience>

SOLUTION BRIEF INFINIDAT

InfiniSafe® Cyber Detection

The impact of cybercrime is expected to cost businesses 9.5 trillion USD per year.¹ Every 39 seconds, there is a new attack on the web.² The costs to a business include damage and destruction of data, lost productivity, intellectual property theft, personal and financial data theft, 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 only a matter of time before they have a cyberattack. Are you prepared?

Our next-generation data protection and recovery strategy is a cyber-focused, recovery-first strategy. The cyber resilience services of our InfiniVerse® platform provide direct support for extensive capabilities, giving you full, end-to-end protection, prevention, detection, and guaranteed recovery capability. Our InfiniSafe portfolio consists of the core cyber stack, InfiniSafe Automated Cyber Protection (ACP), and InfiniSafe Cyber Detection.

InfiniSafe Cyber Detection enhances Infinidat's core cyber stack resilience and response capabilities by enabling the security and IT teams to detect ransomware and malware attacks with up to 99.99% accuracy and enable near-instantaneous recovery of data from clean "known good" copies on the InfiniBox® and the InfiniBox™ SSA platforms. This gives you back leverage over your attackers.

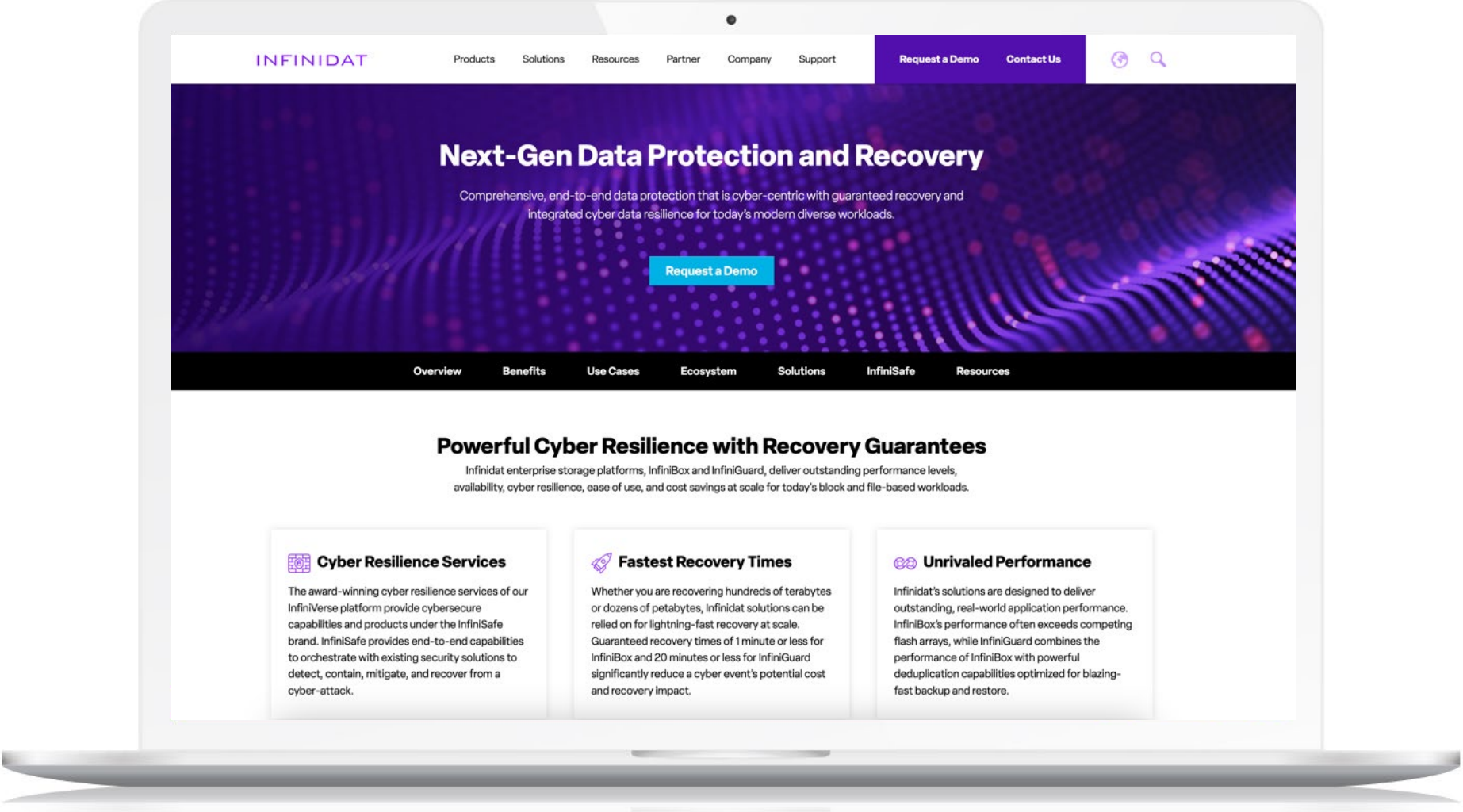
InfiniSafe Cyber Detection adds a level of data detection to the InfiniSafe cyber stack that surrounds the four main layers of the stack and deepens InfiniSafe's ability to detect cyber incidents. InfiniSafe Cyber Detection performs a deep scanning of block, file, databases and VMware datastores by presenting 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.

InfiniSafe ACP integrates directly with your security operations. When an attack is detected, it will automatically execute immutable snapshots and then present them to InfiniSafe Cyber Detection which will deep scan them and provide extensive forensic reporting to diagnose what data has been compromised and the nature of the compromise. This provides critical insights into 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.

65% of IT and cybersecurity professionals surveyed consider ransomware among the top 3 threats to their organization
ESG Report: 2023 Ransomware Preparedness

The Standard in Enterprise Storage

Next-Gen Data Protection and Recovery Web Page



<https://www.infinidat.com/next-gen-data-protection-and-recovery>

The End Users Have Spoken

InfiniBox Reviews
by Infinidat in
4.9 ★★★★★

InfiniBox
by Infinidat in Pri
4.8 ★★★★★

InfiniBox
by Infinidat in Data Center - Others
5.0 ★★★★★ 21 Ratings

INFINIDAT

“**InfiniBox SSA is an outstanding storage array.**”

Account Executive, IT Services | InfiniBox™ SSA

Gartner Peer Insights Customers' Choice 2025

Gartner Peer Insights Customers' Choice 2024 North America

Gartner Peer Insights Customers' Choice 2023

As of 25 Feb 2025

 **Thank you**