INFINIDAT

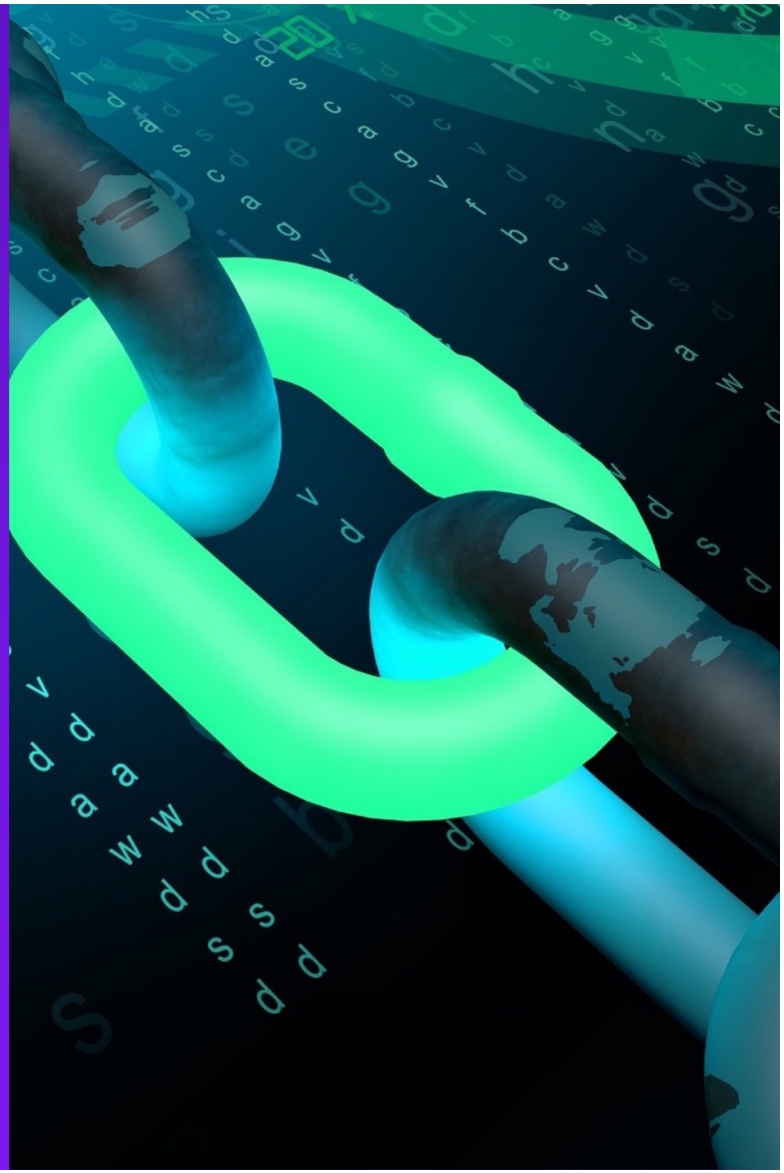
The Standard in Enterprise Storage

Strategies for Cyber Storage Resilience in an Era of Rampant Cyber Attacks

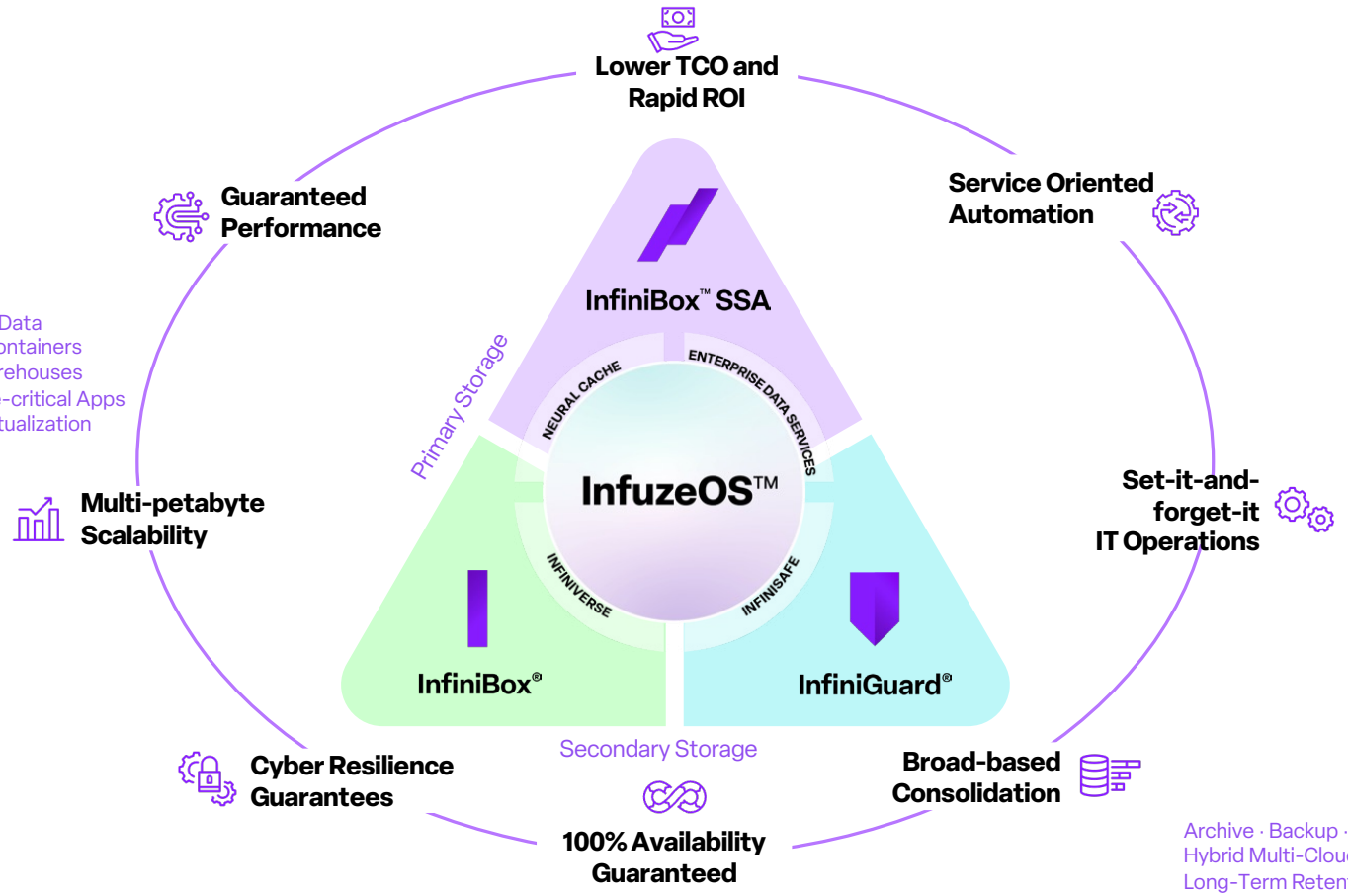
Eric Herzog
CMO
Infinidat
November 2024

eherzog@Infinidat.com

@zoginstor



Review: InfuzeOS - One SDS Architecture, All Platforms



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

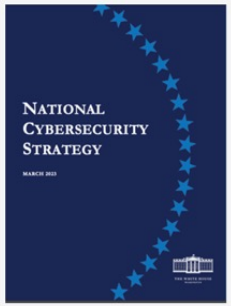
Archive · Backup · Disaster Recovery
Hybrid Multi-Cloud · Rapid Recovery
Long-Term Retention

Cyberattacks are Extensive and Expensive!

Headline News

World ◎ Business ◎ Finance ◎ Travel ◎ Sport ◎ Weather

- Cybercrime will cost enterprises $9.5 Trillion in 2024[1]
- Cyber security is the #2 concern of CEOs globally (Fortune Magazine, June 2023)
- US Securities and Exchange Commission adopts new rules on "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" by public companies (July 2023)
  - Item 1.05 Form 8-K due four business days after a public company has a material cybersecurity incident
    - UnitedHealth Group – Q1 '24, MGM Resorts International – Q4 '23
- US announces National Cybersecurity Strategy (Mar 2023)
- EU moves forward with Cyber Resilience Act (Dec 2023)
- Enterprises suffer 1,258 cyberattacks per week
- Global cybersecurity spending will exceed $1.75 Trillion cumulatively by 2025



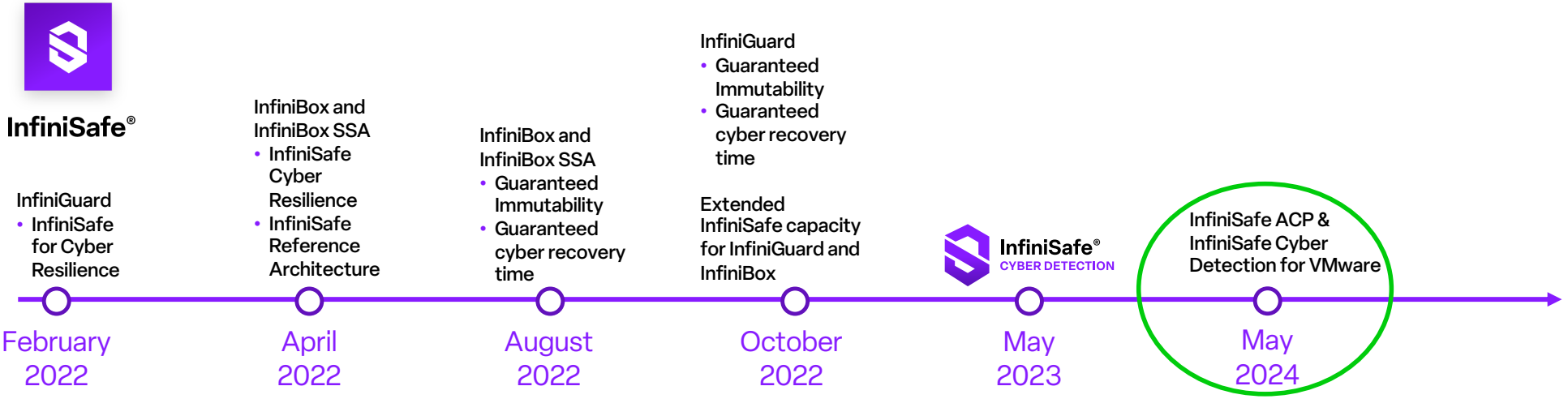
1 https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond

InfiniSafe Cyber Resilience Innovation Timeline

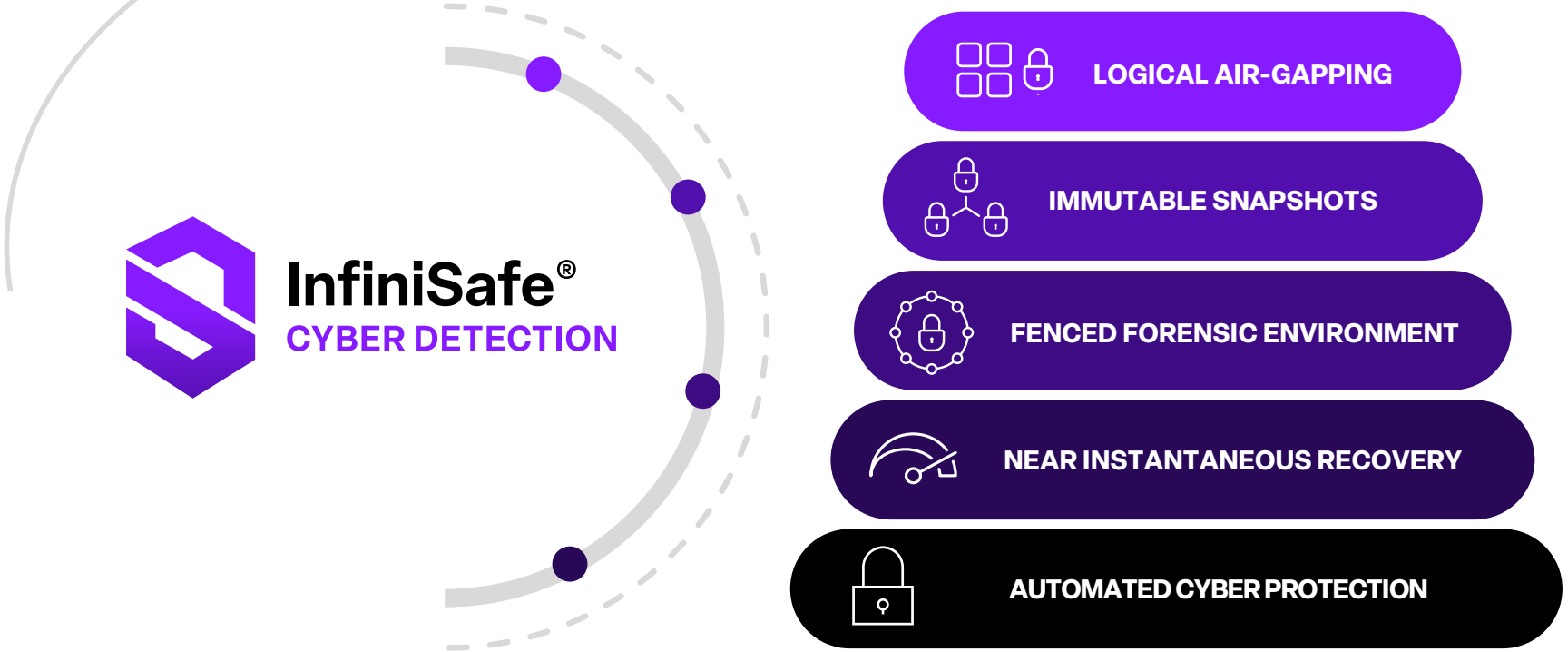
Commitment to delivery of cyber resilience innovation

- First cyber resilience solution for primary storage
- First guaranteed cyber resilience recovery
- First guaranteed cyber resilience recovery time
- Comprehensive Reference Architecture for ecosystem integration
- InfiniSafe Cyber Detection – Deep and Accurate Scanning/Detection



InfiniSafe Cyber Storage Resilience

InfiniSafe Cyber Stack



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

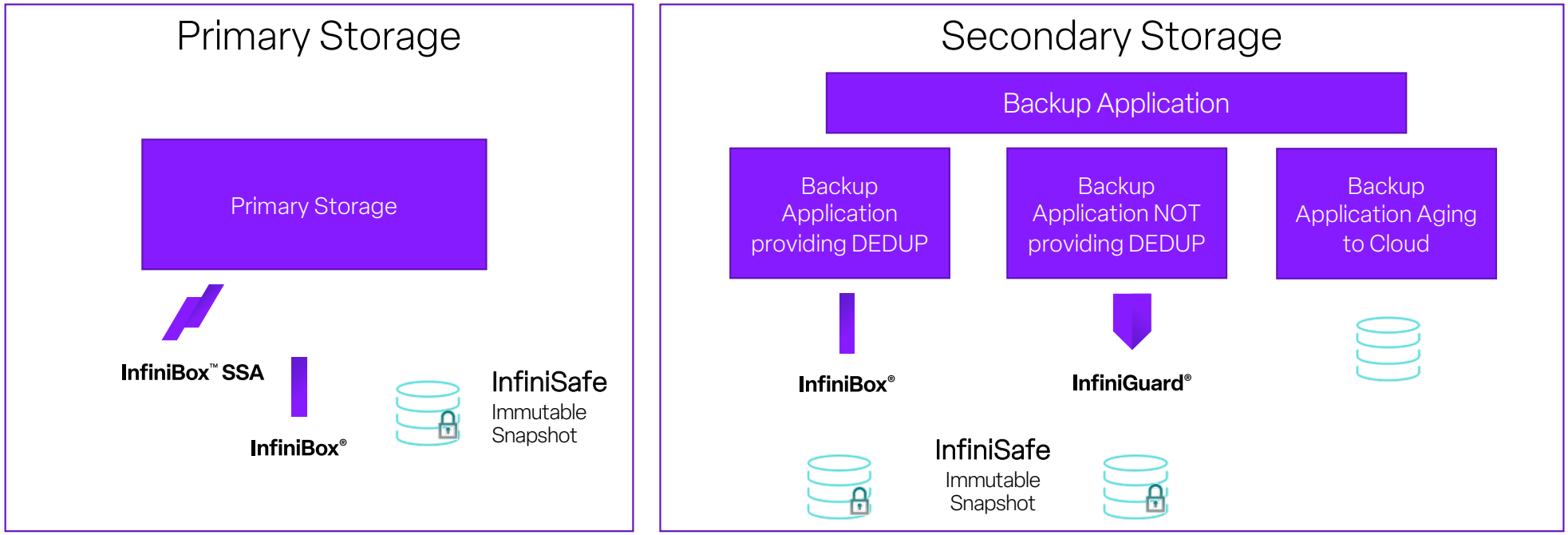
InfiniSafe Cyber Stack

Primary Storage
InfiniBox/InfiniBox SSA

Secondary/Backup Storage
InfiniGuard

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

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 that 20 minutes for InfiniGuard
  - Less than 1 minute for InfiniBox SSA II and InfiniBox
  - Regardless of immutable snapshot size

InfiniSafe Cyber Storage Resilience

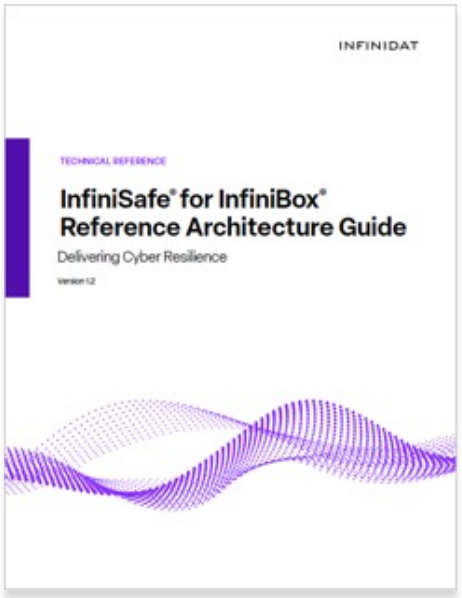
- Immutable Snapshots
- Logical air-gapped protection
- Fenced forensic environment
- Near-instantaneous recovery of any size backup repository

InfiniSafe Automated Cyber Protection

Reducing the threat window!

- Data needs to be protected at the speed of “Compute”
  - Scheduling Immutable Snaps is great, but leaves GAPS
  - Threats happen all the time and some are more critical than others
  - Not all threats attack all data, but will try to isolate important data
  - Trigger from standard syslog
    - SIEM and or SOAR environments supported via syslog
      - Security Information and Event Management software (SIEM)
      - Security Orchestration, automation and response (SOAR)
      - Direct integration possible

InfiniSafe®



- 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

InfiniSafe®

- 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

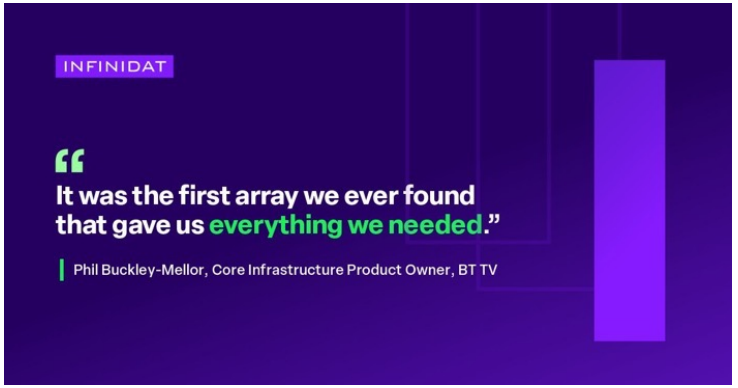
Cyber Detection Flexibility

InfiniSafe®
CYBER DETECTION

Primary Storage
Volumes, App Workloads, Snapshots
VMWare Datastores

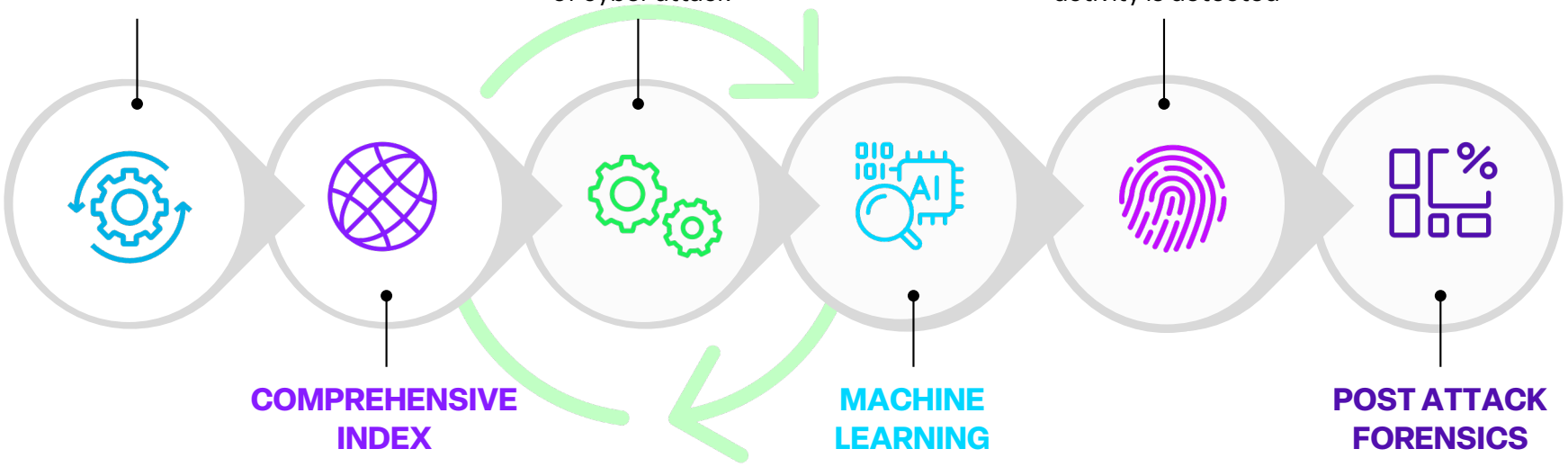
Databases
Oracle, DB2, SQL, SAP Hana, Cache, etc.

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

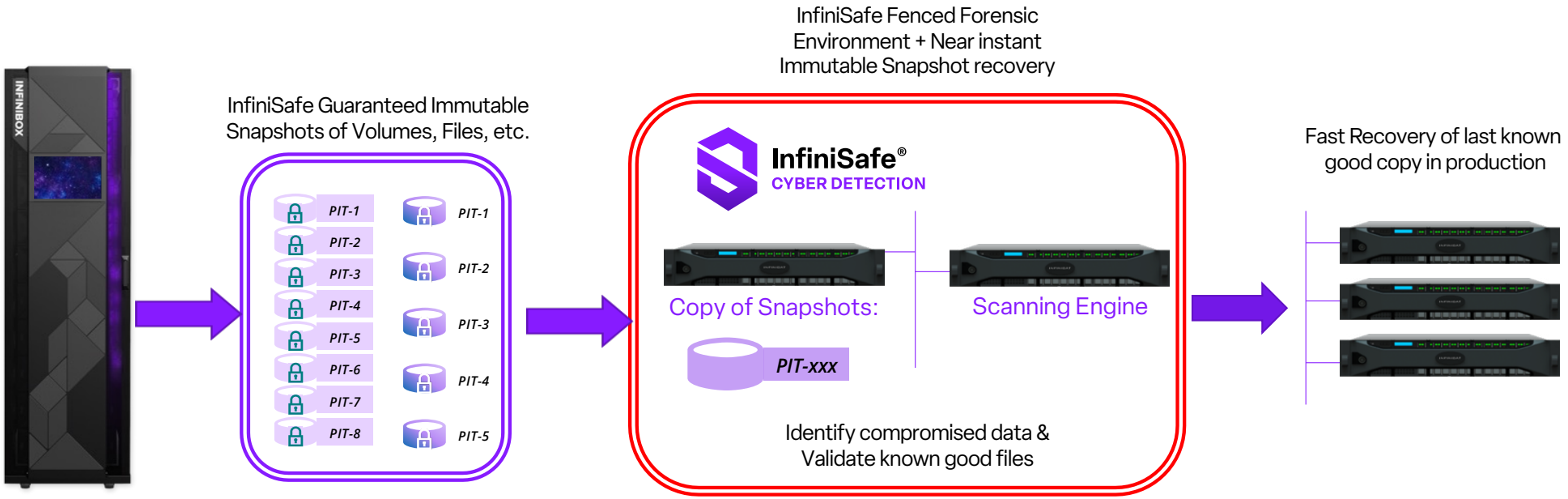
Multiple InfiniBoxes replicate to offload

InfiniSafe Fenced Forensic Environment + Near instant Immutable Snapshot recovery

InfiniSafe Cyber Detection Solution

InfiniSafe® CYBER DETECTION

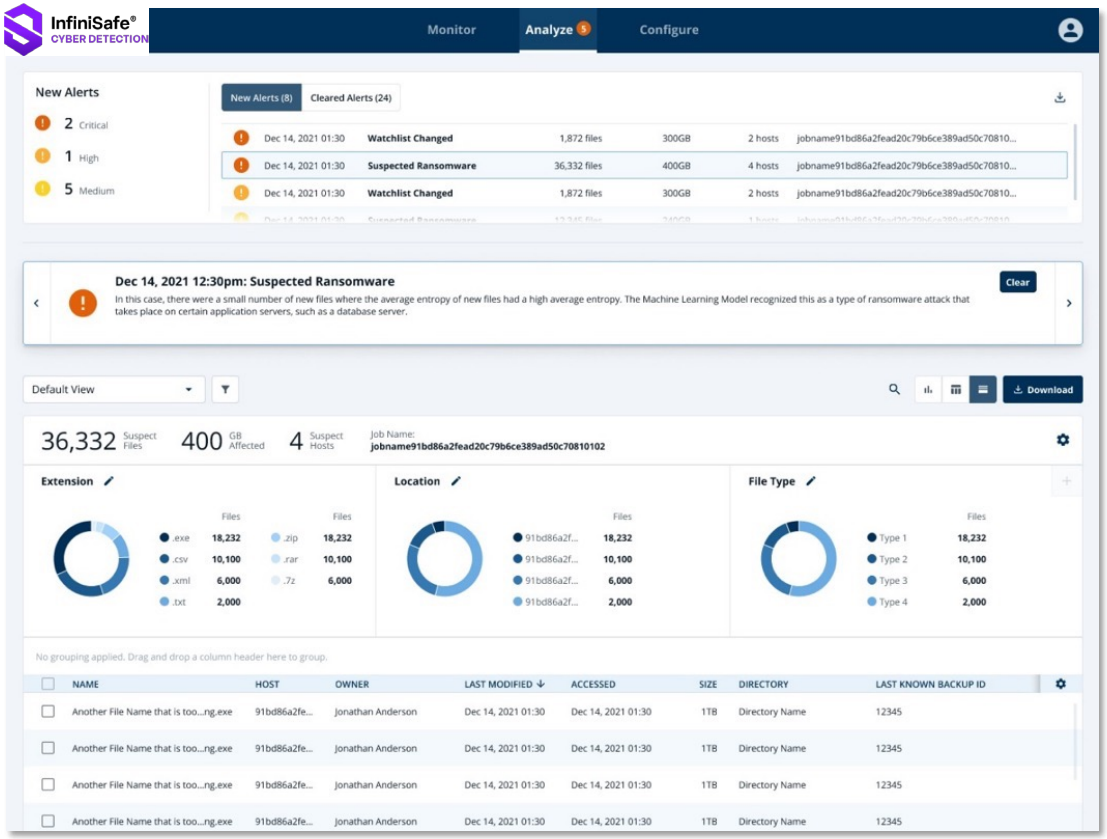
- Applications can validate immutable snapshots in Fenced Forensic environment
- Cyber Detection will tag any corrupted files, create forensic report
- Provides the intelligence needed to facilitate recovery



Cyber Detect Post Attack Dashboard

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

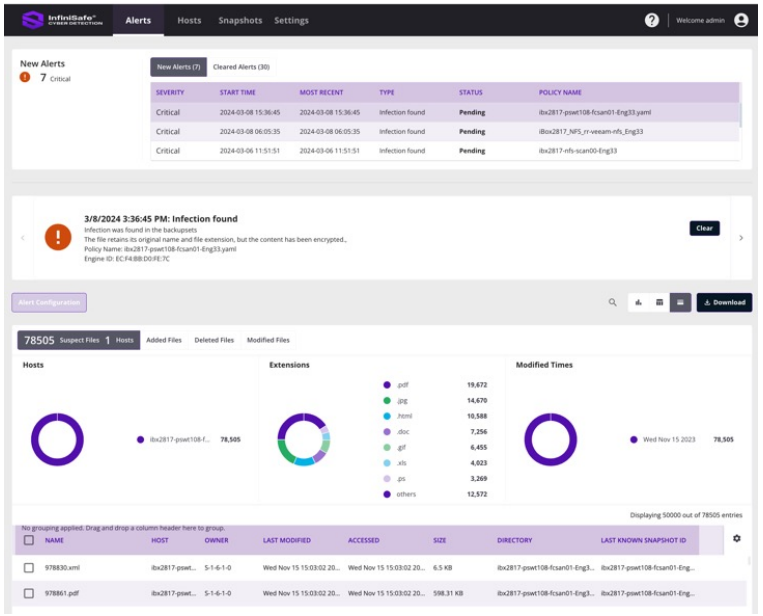
- Alerts organized by severity
- New details on suspect corruption
- Customizable, dynamic charts to drill down into details of the attack
- List of corrupted files that can be downloaded



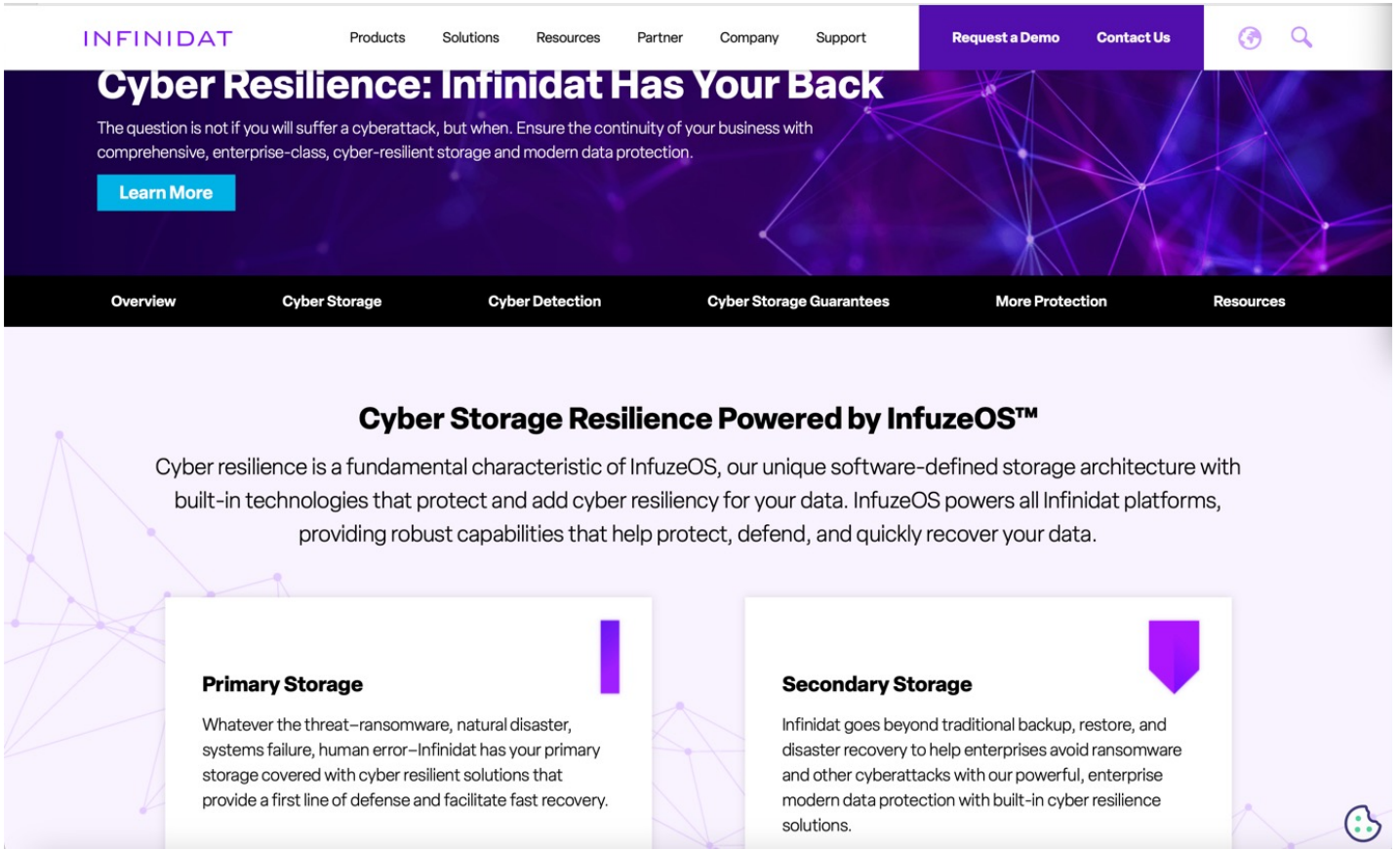
InfiniSafe Cyber Detection

InfiniSafe®
CYBER DETECTION

- Identify a VMware datastore to be scanned
  - Uses AI and ML technology to scan for malware, ransomware, and other cyber anomalies
  - Will scan all VMs in the datastore by default
    - Immutable snaps are scanned – Best practice
  - Simple to exclude any VMs not needed to be scanned
  - 99.99% effective
  - Integrated reporting with data center-wide cyber security software or your Security Operations Center though APIs

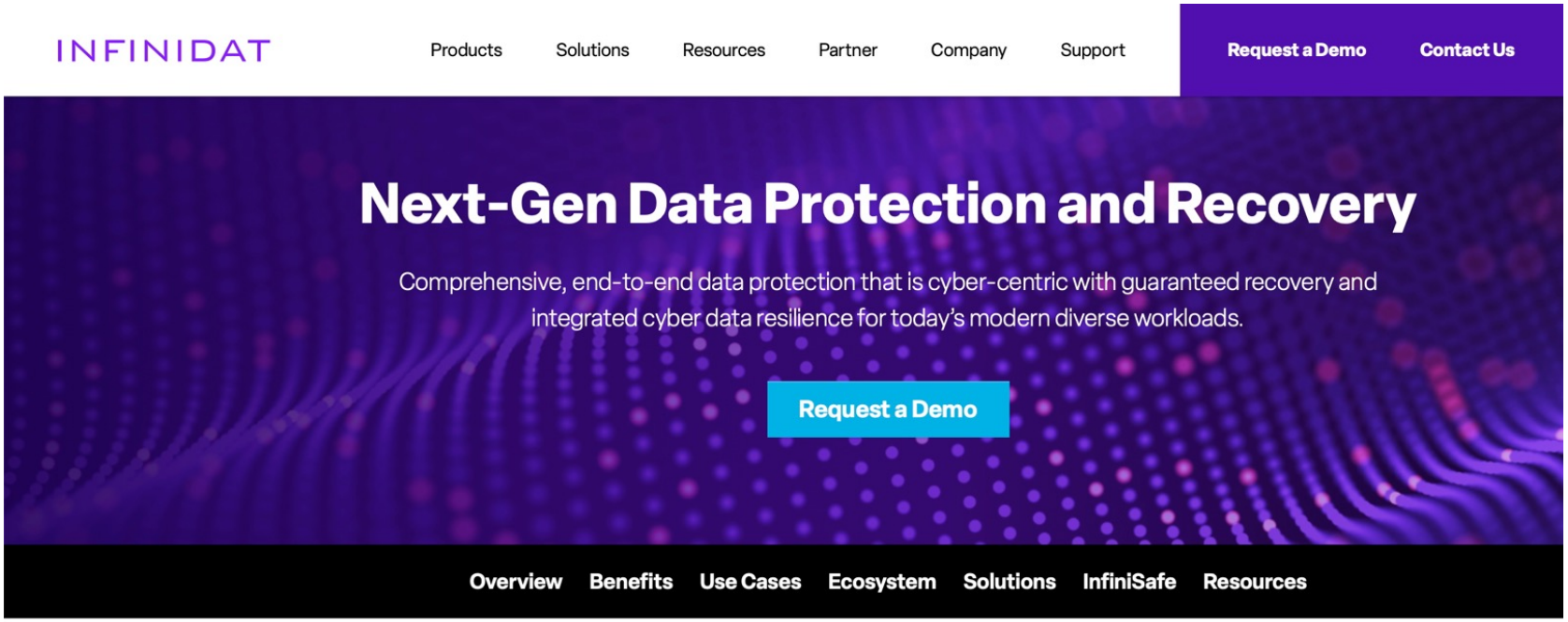


Cyber Storage Resilience Web page



https://www.infinidat.com/en/cyber-resilience

Next-gen Data Protection and Recovery Web page



Powerful Cyber Resilience with Recovery Guarantees

Infinidat enterprise storage platforms, InfiniBox and InfiniGuard, deliver outstanding performance levels, availability, cyber resilience, ease of use, and cost savings at scale for today's block and file-based workloads.

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

INFINIDAT

THANK YOU!

InfiniSafe®

CYBER DETECTION