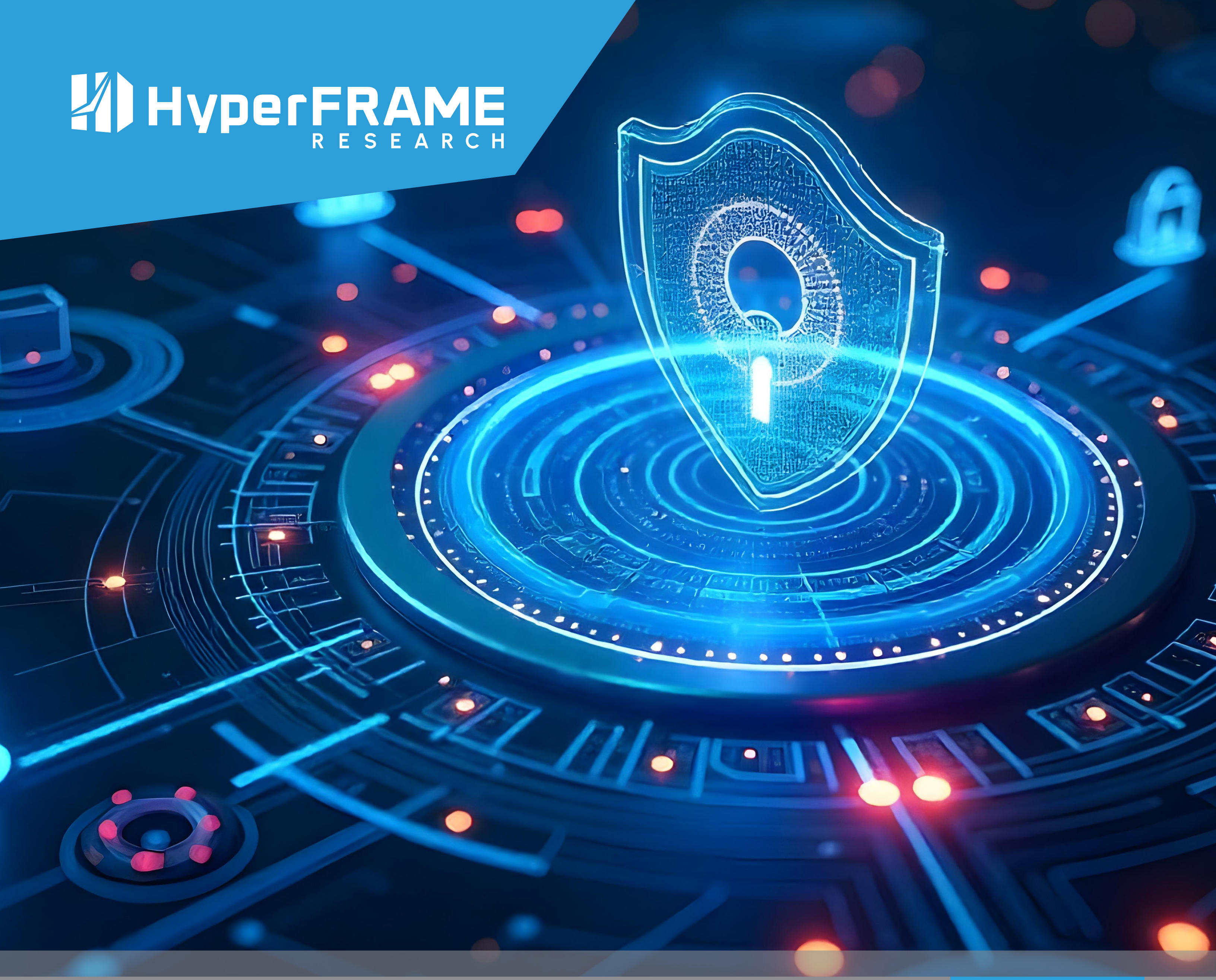


WHITE PAPER

InfiniSafe and the New Standard for Cyber Resilience: Sub-Minute Recovery and Compliance for Modern IT Infrastructure

Authors:
Ron Westfall
Analyst In Residence

Steven Dickens
CEO and Principal Analyst

JULY 2025

Executive Summary

Enterprise Chief Information Security Offices (CISOs) are grappling with a wide array of cybersecurity obstacles amidst a global landscape that is becoming more complex. Geopolitical tensions are driving a surge in sophisticated cyber threats, such as state-sponsored attacks targeting sensitive data and critical infrastructure. This growing complexity heightens the risks and demands innovative strategies to protect organizational assets. The rapid rise of AI-driven technologies introduces both opportunities and risks, with AI sharpening attacks by creating new vulnerabilities that outdated security systems struggle to counter effectively.

Stricter regulations, particularly in Europe and the U.S., are adding more demands to an already challenging role. CISOs must navigate these evolving compliance requirements while aligning with strategic business objectives, necessitating stronger collaboration with legal and executive teams. Legacy malware response systems, reliant on slow backups and reactive measures, are proving inadequate against modern threats. These outdated approaches result in extended disruptions, significant data loss, and increased exposure to ransomware, underscoring the urgent need for agile, real-time defense mechanisms.

A persistent shortage of skilled cybersecurity professionals further strains resources, leaving teams under pressure as they address multifaceted risks. Developers are taking on more security responsibilities, but the gap in specialized expertise remains a hurdle. To adapt, CISOs should invest in advanced tools to manage AI-related risks, foster cross-functional partnerships to meet regulatory demands, and prioritize training to build robust teams. Developing proactive, comprehensive incident response strategies is critical to counter both geopolitical and technological threats. By embracing innovation and collaboration, CISOs can strengthen their organizations' defenses, ensuring resilience and adaptability in this dynamic and increasingly volatile cybersecurity landscape.

Against this backdrop, enterprises are looking for solutions that address these requirements without bringing complexity and cost. Enter Infinidat InfiniSafe technology and Infinidat's next-generation data protection strategy. From our view, the Next-Gen strategy that InfiniSafe powers creates a highly automated and orchestrated cyber-recovery platform that sits on primary storage, continuously creates immutable snapshots on a scheduled basis and if augmented with a powerful capability to integrate with Security Operations Centers (SOC), Security Information and Event Management (SIEM), and Security Orchestration And Response (SOAR) tools to trigger protection the moment an alert fires. What this means is that Infinidat has found a simple but powerful way to reduce the threat window outside of just the storage environment. This is very important as much of a company's data exists on their solutions inside of company data centers around the world.

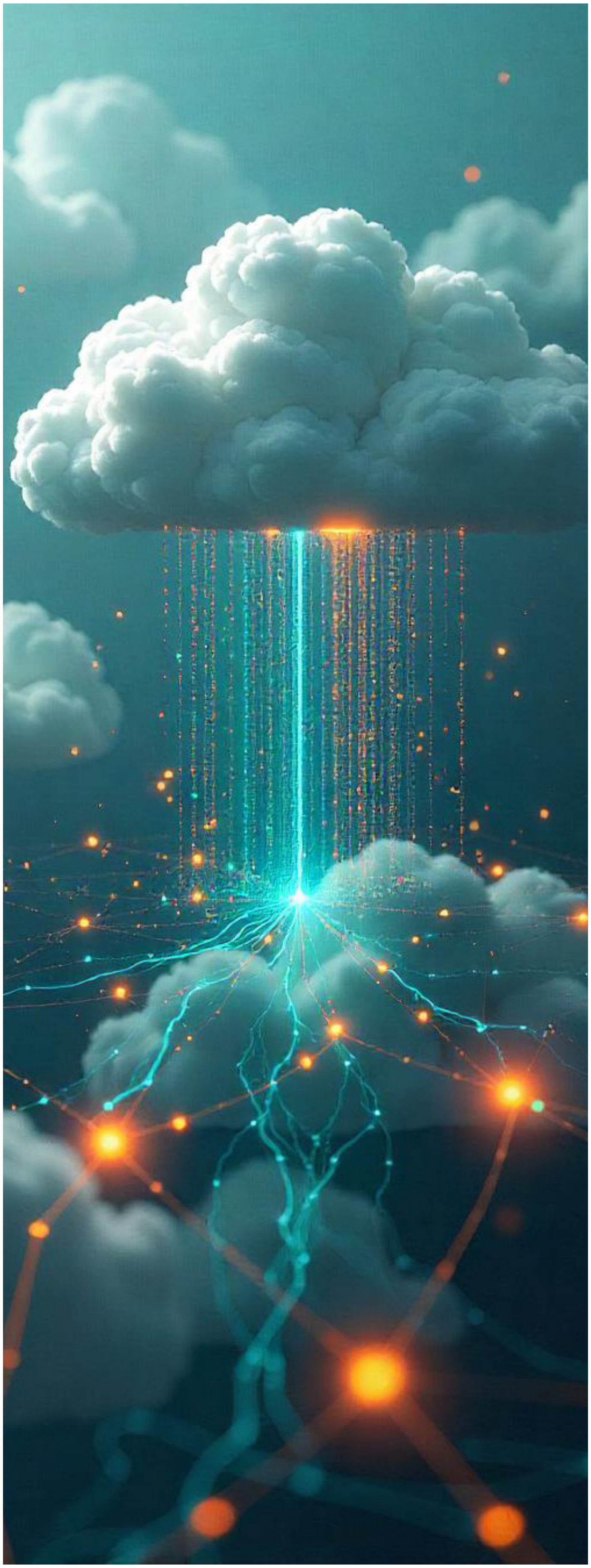
Most data storage products have no line of sight to what is happening in the broader security eco-system. From data protection through to data validation with their optional InfiniSafe Cyber Detection, Infinidat's next-generation data protection strategy delivers a cyber-focused, recovery-first approach. The emphasis being focused on rapid, verifiable recovery from cyberattacks using validated data in immutable snapshots. Add to this logical and remote air-gapping, and near-instantaneous restores. All fully Integrated InfiniSafe technology automates cyber protection and leverages AI-based detection to minimize threat windows and ensure business continuity across hybrid multi-cloud environments. What this means is you already have validated copies of your data prior to an attack and your teams won't waste time trying to determine that after the fact.

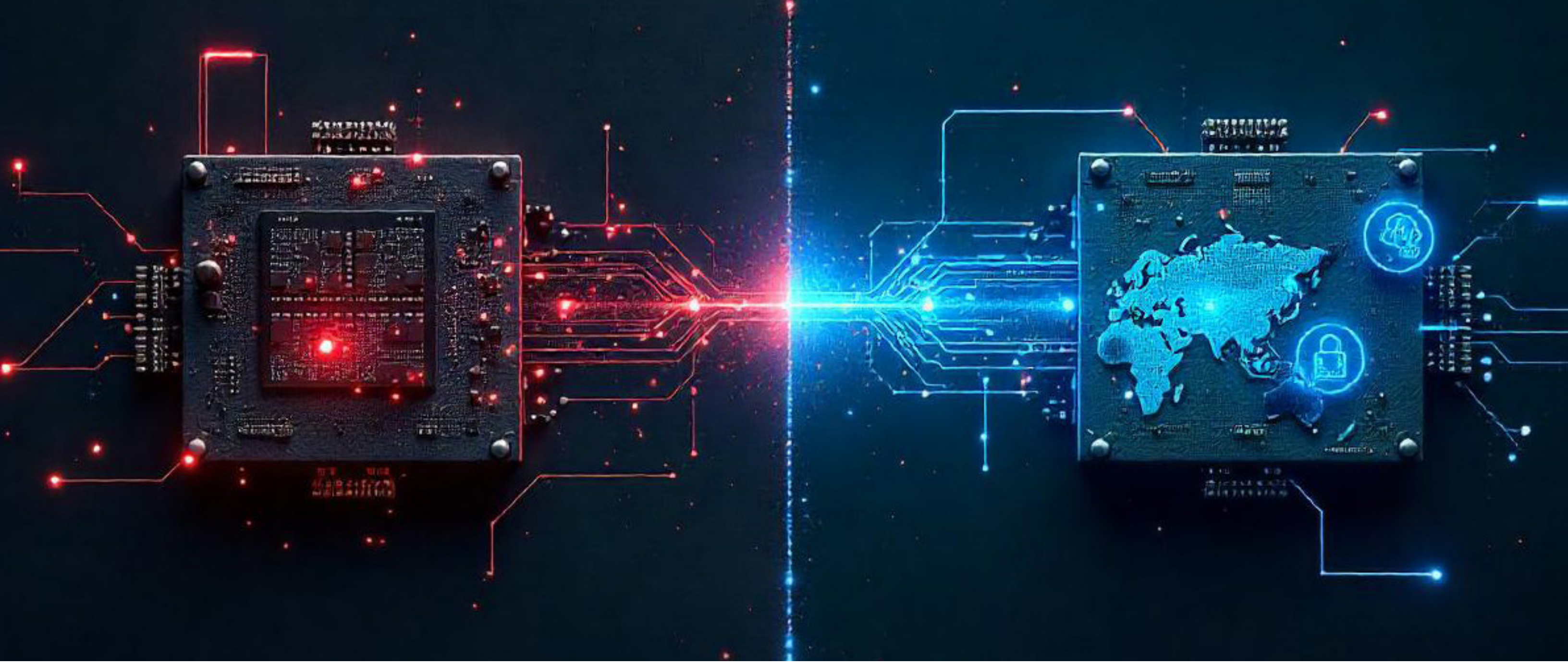
Once the security team confirms remediation, InfiniSafe's Service Level Agreement (SLA) restores full operations in under one minute, slashing the threat window and eliminating the need to consider ransom payments. The platform's sub-minute recovery, ecosystem compatibility, and automation translates into measurable ROI by preserving revenue, avoiding regulatory penalties, and sustaining user experience during otherwise catastrophic attacks.

Introduction: Top Cyber Challenges for Enterprise IT Infrastructure

In today's heterogeneous, hybrid, and multi-cloud IT landscape, CISOs are facing unprecedented pressure as cyber threats evolve in both frequency and sophistication. The reality is stark: it's no longer a question of if a cyberattack will occur, but when and how quickly it will strike. The rapid adoption of advanced technologies, particularly GenAI and other data-intensive workloads, has led to the dispersion of data across increasingly complex and distributed storage environments. This not only expands the surface area for potential attacks but also complicates governance and control. Specifically, cybercrime will cost enterprises $10.5 trillion in 2025.

Simultaneously, heightened geopolitical tensions and expanding regulatory demands are driving stricter compliance mandates, forcing enterprises to navigate a growing maze of local and international laws. Data security, sovereignty, and compliance are no longer back-office concerns - they are now strategic imperatives assigned executive-level accountability. Yet amid these challenges, organizations cannot afford to compromise on user experience or the pace of agile application development. The result is a high-stakes balancing act where security, speed, and scalability must coexist by design.





Call Out: Limitations of Legacy Malware and Ransomware Response Processes

Traditional malware response mechanisms are slow, disruptive, and often ineffective in minimizing operational impact. These legacy processes typically begin with anomaly detection - either by remediation tools or, alarmingly, through notification from threat actors after data exfiltration has occurred. Incident response then involves analyzing the entire primary data estate for signs of compromise, a time-intensive task.

Legacy ransomware response solutions often rely on manual processes and outdated detection methods, which can be slow and prone to human error, delaying recovery and increasing vulnerability. They typically lack comprehensive integration with modern SecOps tools, limiting automation and real-time threat response capabilities. Additionally, these solutions may not provide guaranteed recovery times or robust compliance with evolving regulatory frameworks, leaving enterprises exposed to greater risks and inefficiencies.

Recovery depends on identifying a viable backup, which is often outdated by 24 hours or more, followed by a rollback to this last known good state, leading to significant data loss and workflow disruption. In many cases, the operational and financial burden of this process compels organizations to consider paying the ransom, highlighting the critical need for modern, proactive, and real-time cyber resilience strategies.

Why InfiniSafe Integrated Capabilities Meet Top Enterprise IT Security Challenges

In today’s digital landscape, cyber attacks are inevitable, making it critical to shrink the threat window - the time between an attack’s initiation and its detection or mitigation. Today no single solution can address every vulnerability, but a flexible, multi-layered approach is essential to safeguard critical data assets. From our viewpoint, InfiniSafe offers next-generation data protection and recovery with a cyber-first, recovery-focused methodology, seamlessly integrated into storage solutions.

Its Cyber Stack features immutable snapshots, logical/remote air gaps, a fenced forensic environment, and near-instant recovery to ensure robust business continuity. The fenced forensic environment is particularly valuable, providing a clean, isolated network to test and validate data without risking further compromise. Immutable snapshots are presented here for analysis using specialized tools, ensuring data integrity before recovery. This orchestrated approach restores leverage to organizations, countering attackers’ attempts to disrupt and extort.

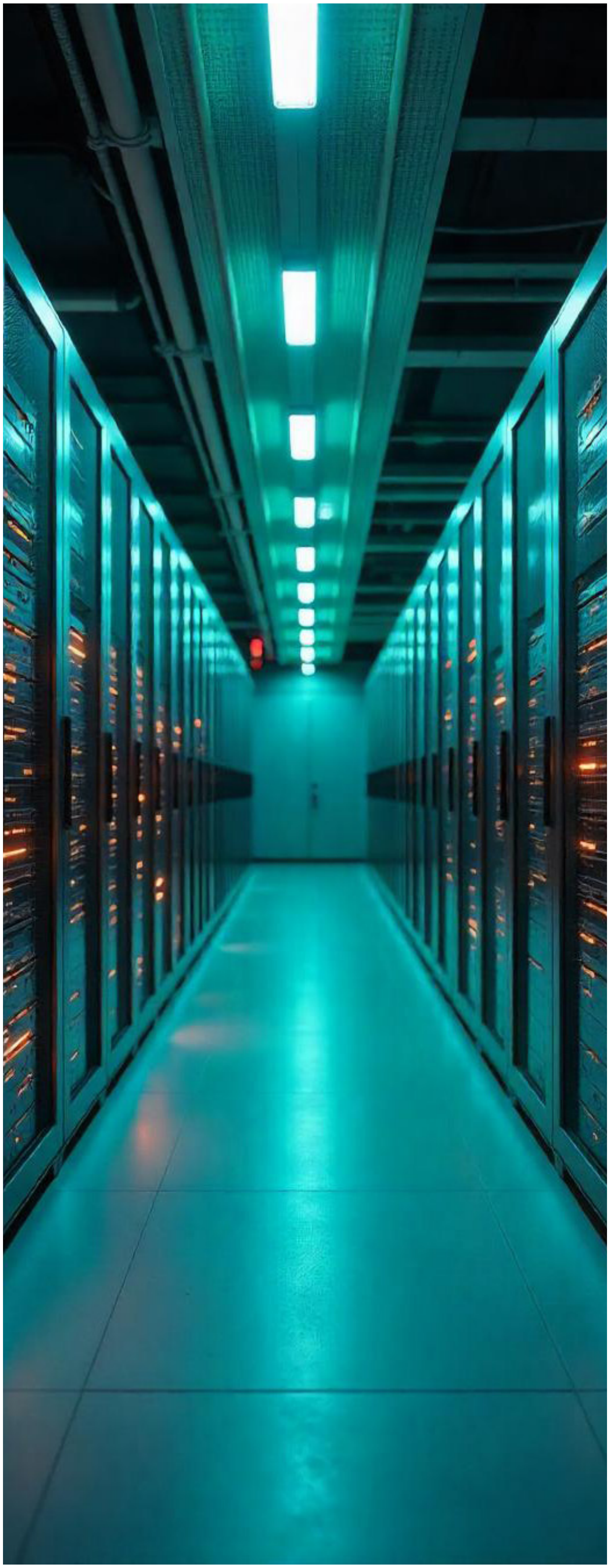
InfiniSafe Automated Cyber Protection (ACP) orchestrates integration with SecOps (SIEM/SOAR), automating threat response by triggering immutable snapshots, reducing the threat window, augmenting scheduled snapshots, and queuing data for validation. Additionally, InfiniSafe Cyber Detection provides a 99.99% detection rate, scanning over 200 data points for accurate, detailed reporting to assure data integrity, all available through a subscription-based license. This precision minimizes false positives, enabling rapid, confident responses. The solution also generates detailed forensic reports, identifying the last known good backups for quick recovery. While InfiniSafe's core features are included with Infinidat systems, Cyber Detection requires additional capacity licensing.

Traditional data protection relies on backup and recovery methods, such as deletable snapshots, which leave gaps in security including vulnerability to ransomware attacks. Scheduled immutable snapshots, locked for a set period, improve resilience but still expose data during intervals defined by the Recovery Point Objective (RPO). For instance, snapshots taken four times daily result in a six-hour RPO, during which significant data loss or compromise could cripple a business. Cyber attacks - whether encrypting data, corrupting backups, or stealing information - exploit these gaps to create leverage for extortion. As a result, modern threats move at network speed, outpacing human-led security responses.

InfiniSafe addresses this by leveraging real-time monitoring within SOCs. Using SIEM and SOAR systems, InfiniSafe enables automated, near-instantaneous creation of immutable snapshots triggered by suspicious activity. This reduces the threat window dramatically, minimizing risks such as data corruption or encryption. The solution integrates with Infinidat's InfiniBox storage systems through APIs or CLIs, allowing seamless orchestration with existing security infrastructure. This automation is critical, as attackers aim to create chaos, leaving little time for manual intervention.

Organizations with complex, multi-layered environments must integrate tools like SIEM, SOAR, and InfiniSafe to act at compute speed. By proactively creating immutable snapshots and validating data in a fenced environment, organizations can reduce exposure and recover swiftly. This approach not only protects critical assets but also disrupts attackers' ability to exploit vulnerabilities.

Overall, shrinking the threat window requires moving beyond traditional backup methods to proactive, automated, and integrated solutions like InfiniSafe. By combining real-time monitoring, instantaneous snapshots, AI-driven detection, and forensic analysis, organizations can mitigate cyber risks, maintain control over their data, and minimize the chaos and financial impact of attacks. As cyber threats evolve, such comprehensive strategies are vital to staying ahead of bad actors and safeguarding business continuity.



InfiniSafe Assures Accelerated Ransomware Recovery

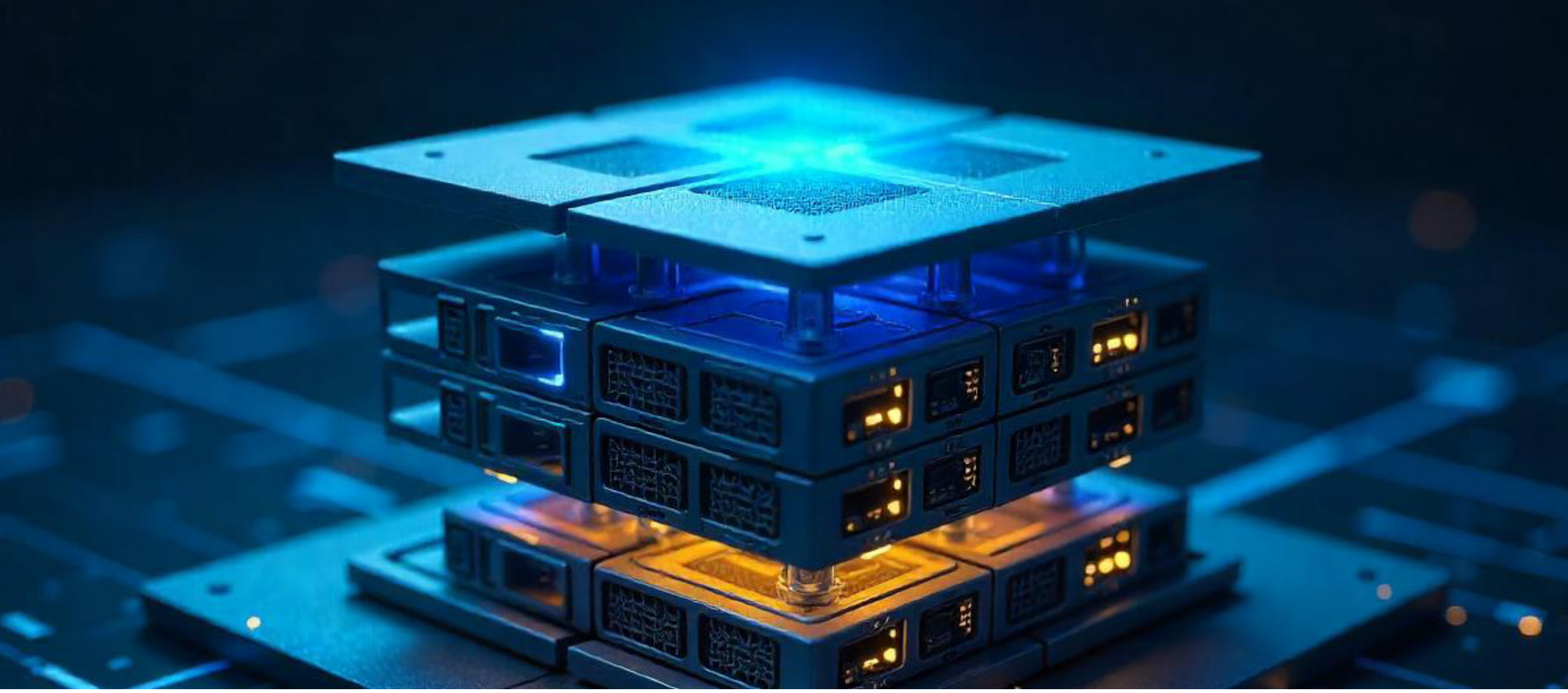
InfiniSafe offers a transformative approach to ransomware incident response, delivering sub-minute recovery through intelligent automation and integration. We identify that InfiniSafe SLAs that restore any size data set within one minute are a game changer. In stark contrast to legacy methods involving manual analysis and delayed restoration, InfiniSafe integrates seamlessly with a wide range of security tools through APIs and signaling mechanisms to detect real-time alerts.

It continuously and proactively generates immutable snapshots of the primary data estate, and through its centralized dashboard, surfaces potentially compromised datasets for review. Once a remediation decision is made, InfiniSafe's SLA ensures a complete data recovery in under one minute. This capability not only minimizes downtime and data loss but also significantly reduces the financial and operational costs typically associated with ransomware recovery.

InfiniSafe Cyber Stack: Enhances the Same Functionality for Optimal Performance

The InfiniSafe Cyber Stack, consisting of primary storage InfiniBox/InfiniBox SSA and secondary/backup storage InfiniGuard components, delivers the consistent cyber resilience that organizations demand today. The InifiBox/InifiniBox SSA solution is seamlessly integrated into InfuzeOS, offering enterprise CISOs a robust cybersecurity solution with flexible integration capabilities, including a reference architecture and an API-first methodology, ensuring adaptability to diverse systems.

Above all, it guarantees immutability and an RTO of one minute or less, providing unmatched protection and rapid recovery in an increasingly fractured global cybersecurity landscape. InfiniGuard, the purpose-built secondary/backup storage solution integrated into InfuzeOS, delivers fully orchestrated data protection with guaranteed immutability and a RTO of 20 minutes or less, ensuring enterprise CISOs can rely on robust, efficient, and secure data recovery in today's ultra challenging cybersecurity environment.



InfiniSafe: Differentiating Cyber Resilience through Instant, Intelligent Remediation

InfiniSafe redefines cyberattack remediation by delivering near-instantaneous recovery capabilities directly on primary storage, addressing key limitations of traditional backup and restore models. Unlike legacy solutions that rely on infrequent, manually triggered backups and often outdated secondary storage, InfiniSafe uses automated, frequently updated, immutable snapshots of primary data. These snapshots are securely indexed and unchangeable, enabling rapid identification of compromised data and informed recovery decisions. Key advantages include:

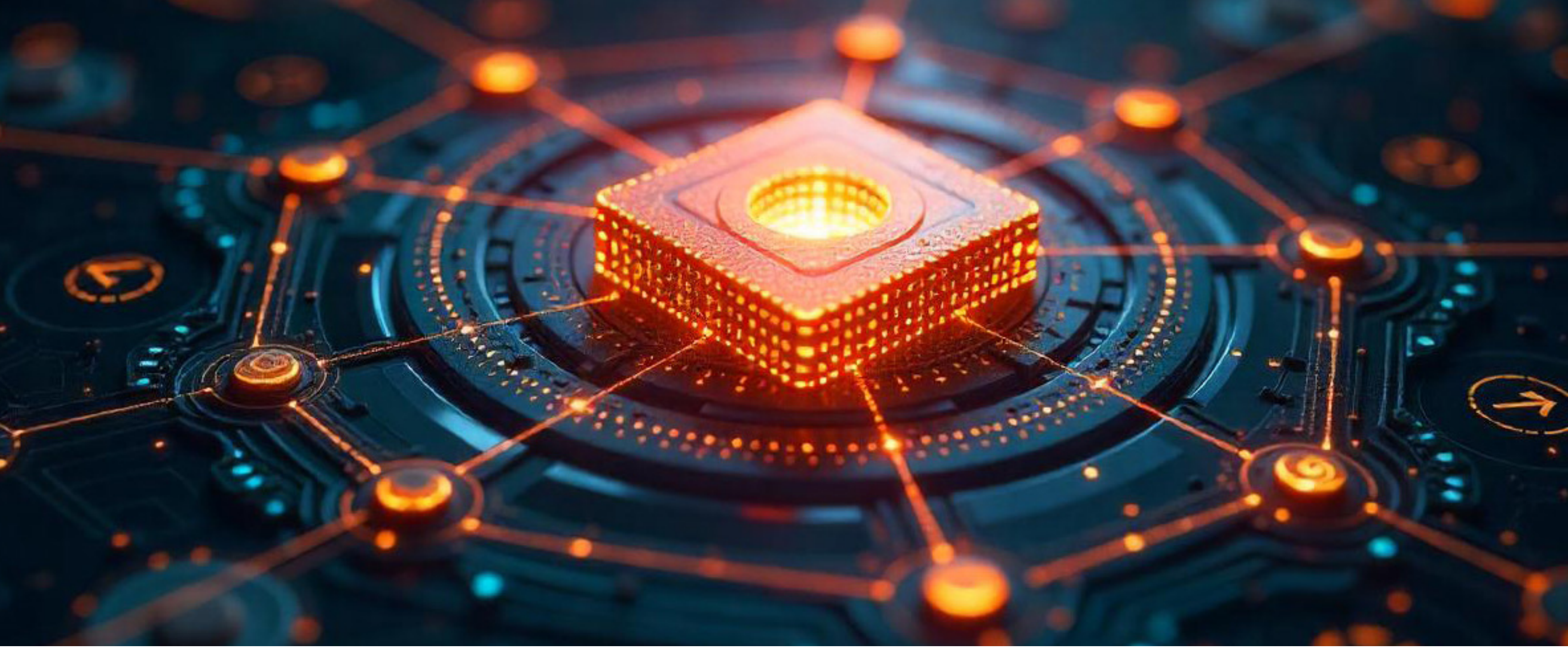
- **Primary Storage Remediation:** InfiniSafe operates directly on primary storage, eliminating the lag and complexity of restoring from secondary systems.
- **Ecosystem Compatibility:** Designed to integrate effectively with existing enterprise IT environments, InfiniSafe plays well with threat detection, data storage, and orchestration tools, enhancing overall cyber resilience.
- **Infrastructure Flexibility:** InfiniSafe operates on appliances provided either by Infinidat or certified third-party vendors, ensuring adaptable deployment across varied enterprise architectures.

Financial Impact: By shortening response times, preventing extended outages, and reducing reliance on ransom payments, InfiniSafe and Infinidat infrastructure offer a strong return on investment. They serve as a critical hedge against modern cyberattacks' operational and financial risks, enabling enterprises to maintain business continuity while minimizing data loss and reputational damage.

Regulatory compliance: In light of the globalization of threat vectors and attack surfaces, global legislators have passed legislation with which enterprises are required to comply. InfiniSafe enables enterprises to automatically and programmatically maintain full compliance at all times. Supported regulatory frameworks include:

- EU: DORA - (Digital Operational Resilience Act)
- U.S.: National Cybersecurity Strategy Implementation Plan v2 (May 2024)
- NIS2 - (Network and Information Systems)
- UK: GDPR and Data Protection Act (2018)
- Japan: The Basic Act on Cybersecurity (v 2022)

As a result, Infinisafe ensures enterprises consistently meet stringent legal and industry standards without manual intervention, reducing the risk of costly penalties and reputational damage. This capability streamlines compliance processes, saving time and resources while enhancing operational resilience and trust in data protection.



Looking Ahead: Strategic Considerations for Cybersecurity Platform Engineering

As the cybersecurity landscape evolves and the threat blast radius grows in sophistication and frequency, enterprises must evolve beyond the limitations of traditional malware response strategies that are slow, costly, and operationally disruptive. As data increasingly becomes the lifeblood of enterprises, especially as they look to embrace AI initiatives, where that data is stored is not only operationally vital, but also crucial to planning for cyber security posture assessment.

InfiniSafe's Cyber Resilience innovation track record underscores its commitment to pioneering cyber resilience, delivering the first cyber resilience solution for primary storage, the first guaranteed cyber resilience recovery, and the first guaranteed recovery time. It offers a comprehensive Reference Architecture for seamless ecosystem integration and features InfiniSafe Cyber Detection, which provides deep and accurate scanning and detection to ensure robust data protection. This puts InfiniSafe in the driver seat to deliver optimal outcomes for cybersecurity platform engineering.

Against this landscape, InfiniSafe delivers a paradigm shift in cyber resilience, enabling intelligent, automated, and near-instantaneous recovery directly on primary storage. With its sub-minute SLA, seamless integration across security ecosystems, and immutable snapshot architecture, InfiniSafe empowers organizations to respond to ransomware and other cyberattacks with unmatched speed and precision. By ensuring business continuity, minimizing data loss, and maintaining compliance in the face of rising regulatory scrutiny, InfiniSafe positions itself as a remediation tool and a strategic enabler of secure, scalable, and compliant digital transformation. For CISOs seeking to defend both data integrity and enterprise agility, InfiniSafe offers a timely and proven solution.

ABOUT HYPERFRAME RESEARCH:

HyperFRAME Research delivers indepth research and insights across the global technology landscape, spanning everything from hyperscale public cloud to the mainframe and everything in between. We offer strategic advisory services, custom research reports, tailored consulting engagements, digital events, go to market planning, message testing, and lead generation programs.

Our industry analysts specialize in rigorous qualitative and quantitative assessments of technology solutions, business challenges, market forces, and end user demands across industry sectors. HyperFRAME Research collaborates closely with your Analyst Relations, Product, and Marketing teams to build and amplify your thought leadership, positioning your expertise to enhance brand and product recognition. Through content that engages readers, viewers, and listeners alike, we ensure your voice resonates across channels.

CONTACT HYPERFRAME RESEARCH:

Steven Dickens
CEO & Principal Analyst | HyperFRAME Research

Email Address:

steven.dickens@hyperframeresearch.com

Telephone Number:

+1 845 505 1678

X: - @StevenDickens3

LinkedIn: Steven Dickens

BlueSky: Steven Dickens

CONTRIBUTORS

Steven Dickens CEO & Principal Analyst
HyperFRAME Research

Ron Westfall
Analyst In Residence

INQUIRIES

Contact us if you would like to discuss this report and HyperFRAME Research will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "HyperFRAME Research." Non-press and non-analysts must receive prior written permission by HyperFRAME Research for any citations.

LICENSING

DISCLOSURES

HyperFRAME Research provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

HyperFRAME
RESEARCH