Infinidat's Recovery-First Strategy to Fight Cyber-Attacks

Sponsored by Infinidat

Jean S. Bozman, Cloud Architects LLC
Srini Chari, Ph.D., MBA, Cabot Partners

February 2025

Innovative Data Protection Solutions Minimize Downtime Costs for Businesses

Cybersecurity is now the top-of-mind priority for business executives. The reason is clear: Cyber-attacks and ransomware threats inflict their worst damage by slowing business operations to a crawl. These threats often lurk undetected until they are discovered days or weeks later. By then, major damage has already been done to your business operations.

When cyberattacks hit, mission-critical applications are unable to support your business. Delayed discovery leads to millions of dollars in damage to the business. That's why planning for rapid data recovery from a cyber-attack is the first thing CXOs and business executives should consider when planning to avoid downtime.

Shrinking the "threat window" is key to reducing the damage from any cyber-attacks your company could experience each week, month, or year. Moreover, experience has shown that securing and validating your organization's critical data at the source is the best way to prevent damage to your business.

The best way to achieve quick recovery from a cyber-attack is to protect your data in its original state and isolate the "immutable snapshots" of that data, while validating that the isolated data is free of corruption.

Immutable snapshots are snapshots of enterprise data that cannot be changed. Later on, in the wake of a future cyber-attack, rapidly restoring your enterprise data with immutable snapshots will allow your business to resume normal operations – dramatically minimizing your company's downtime costs.

The conclusion is clear: Even with multi-layered security implementations, there is a major gap in most data-protection strategies. Enterprises are looking for innovative solutions that can quickly restore full production-level operations, returning the business to its pre-attack state.

The Real Cost of Downtime is Rising

The cost of downtime in a 24 x 7 x 365 world keeps rising– estimated to be $1 million ($USD) to $4 million ($USD) per incidence, as reported by widely published customer surveys[1] (See Figure 1).

Any downtime caused by an interruption in business processes – costs revenue and impacts the bottom line. It also affects the company's reputation, deepening the total amount of financial damage done by the attack.

Cyber-attacks cause major damage to businesses

Quick recovery minimizes cyber-attack damages

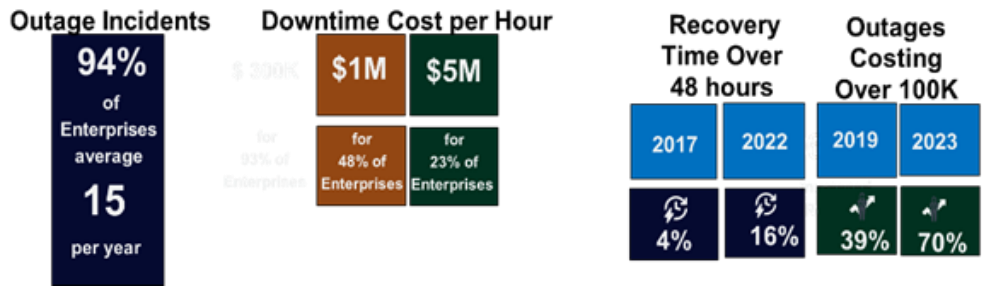[1] The Cost of Downtime: Outages, Brownouts & Your Bottom Line

Figure 1: The Rising Incidence of Outages, Costs of Downtime, and Recovery Time

There's no doubt that the frequency of cyber-attacks and ransomware attacks – freezing or deleting vital data – has been increasing in recent years.

Today's cyber-attackers are going after many types of data, including financial, medical, and personal identification (PII) data. Importantly, data corruption threatens business continuity – compromising the workplace and office systems that support all types of organizations. Downtime caused by cyber-attacks and corrupted data can disrupt your business operations for weeks or months.

Here are just a few mission-critical examples of cyber-attacks slowing or stopping normal business operations:

- Bank accounts become inaccessible to customers and depositors.
- Factory production lines come to a halt.
- Airlines are forced to delay or cancel scheduled flights during peak travel - often experiencing days to rebuild their normal schedule and to restore business operations.
- There are many more examples, reaching across every type of business organization and government unit, all the way around the world.

IBM, Siemens, Gartner, and IDC have each published reports showing how unplanned downtime threatens businesses, costing business and government organizations millions of dollars per incident due to unplanned outages. The data in these reports shows that customer-site downtime reduced revenues and profits, interfering with normal operations. Extended periods of downtime can damage a company's reputation for weeks or months, further reducing its financial results.

Each of these published reports has documented and published the financial impact of downtime based on actual revenues and customer surveys they conducted in CY2024 in the Americas, Europe/Middle East/Africa (EMEA), and Asia/Pacific, including Japan. According to these customer surveys, the good news is that downtime can often be avoided, resulting in many real-world business benefits (See Figure 2).
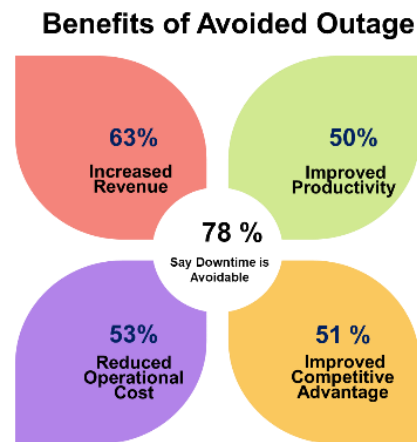

Figure 2: Majority of Customers Believe Downtime Can be Avoided, Yielding Business Benefits

CABOT PARTNERS
OPTIMIZING BUSINESS VALUE

Downtime costs are large and growing

Cyber-attacks harm several mission-critical business processes

Cyber-attacks hurt firms and cut profits, but they can be minimized

However, to combat data protection challenges and rising downtime costs, innovative solutions (often based on artificial intelligence/machine learning (AI/ML)) are needed (See Figure 3). These solutions must:

- Ensure accurate data replication via immutable snapshots of known, good data, supporting active and accurate business recovery.
- Isolate and proactively manage the process of data validation throughout the enterprise.
- Detect anomalies well beyond typical mechanisms for working with metadata and preventing data-entropy that could disrupt business uptime.
- Allow enterprises to act rapidly, with easy-to-use built-in automation/orchestration.
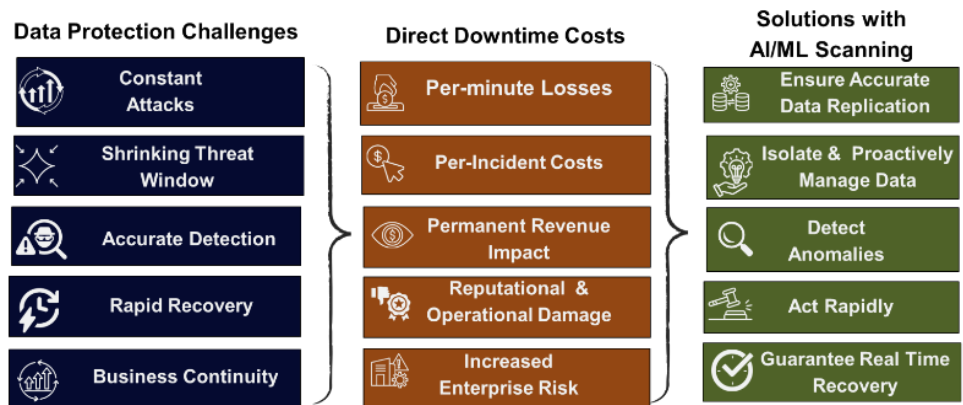- Guarantee real-time recovery to ensure business continuity.

Figure 3: Data Protection Challenges, Direct Downtime Costs, and Solutions

Infinidat's enterprises storage solutions offer more functionality than many customers see in their current data-protection and data-management software tools. The reason is clear: Infinidat provides an extensive set of capabilities with their InfiniSafe technology, many built in and optional advanced AI/ML scanning that prioritizes rapid recovery from data breaches. This scanning capability minimizes downtime costs and maintains seamless operations following a cyber-attack.

Infinidat's Next-Generation Data Protection and Recovery

Valuable time is lost when determining the full extent of data damage caused by a recently discovered cyber-attack. Recovery of data is achieved through quick and accurate detection of data attacks, ensuring that the process is automated. This approach enables the rapid restoration of the original data in its pre-attack, uncorrupted state – ensuring business continuity for the entire business enterprise.

Infinidat's InfiniSafe technologies include InfiniSafe Cyber Detection, the cybersecurity software that looks deeply within the data and validates its state. This validation process helps customers avoid the disruption caused by cyberattacks – providing strong data protection that is *cyber-focused* and *recovery-focused.* (See Figure 4).

The InfiniSafe software combines proactive data protection and a thorough data-validation process, enabling a quick recovery – and defeating the unwelcome element of surprise when a cyber-attack occurs. Otherwise, a cyber-attack's effects might linger

throughout an enterprise for days or weeks, long after the initial cyber-attack itself. During that lag time, customers would experience business-damaging delays while trying to find, identify, and replace the corrupted data stored throughout their enterprise.

Infinidat's solutions combine all the needed elements for rapid detection of cyber-attacks, providing the following;

- accessing immutable copies of known, protected data;
- scanning for threats to production data; and
- delivering quick and guaranteed recovery of enterprise data.

This rapid guaranteed recovery – often completed in less than one minute – works with volumes of any size by quickly restoring an immutable snapshot. Infinidat's overall enterprise architecture guarantees 100% availability for enterprise data, ensuring the protection of customers' mission-critical data.

Infinidat is partnering with Index Engines, a well-known cyber-detection specialist, to support continuous scanning of mission-critical data-sets. This combination of Index Engines' scanning software and Infinidat's Cyber-Security software yields real-world results, supporting rapid recovery from cyber-attacks – whenever they may occur.

Infinidat Supports a Wide Range of ISV Software Products

Providing broad support for customers' existing data-protection software is key to achieving business continuity. InfiniSafe software seamlessly connects with many of the most widely installed security and monitoring applications worldwide. These solutions include ISV software from Commvault, Hammerspace, Microsoft, Oracle, Red Hat, SAP, Thales – and many others.

From an analyst perspective, Infinidat's ability to work well with third-party software packages and APIs from systems companies preserves a customer's earlier investments in data protection and data management – while enhancing the overall business value of their enterprise data.
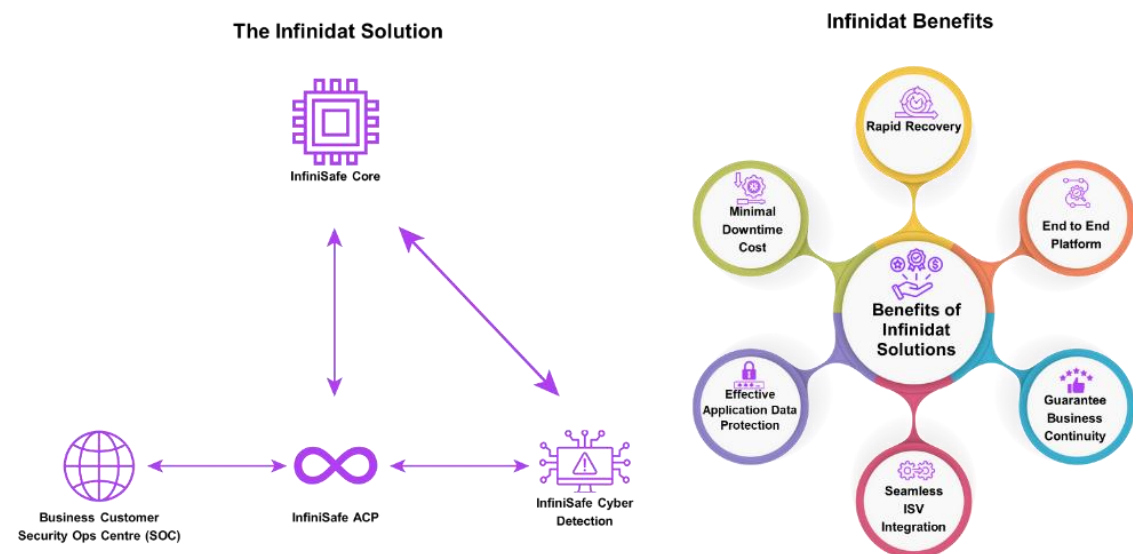

Figure 4: The Infinidat Cyber-Resilience Solution and its Benefits

The key ingredients (See Figure 4) in Infinidat's Cyber-Resilience solution are:

- **InfiniSafe Technology Stack** – InfiniSafe is a comprehensive and integrated solution that creates the foundation that protects data, and orchestrates the functions that enable finding instances of corruption, and restoring data to known, good data instances. Core functions of InfiniSafe are embedded in Infinidat's InfuzeOS, which is included with Infinidat's InfiniBox hardware systems. This provides immutable snapshots, logical and remote air-gapping, a fenced forensic environment, and guaranteed near-instantaneous recovery in less than one (1) minute – regardless of data-set size.
- **InfiniSafe Automated Cyber Protection (ACP)** – Filling the gaps, ACP augments scheduled immutable snaps (snapshots of enterprise data) that leave gaps, is critically important to reduce the threat window. ACP allows integration into other (third-party) security and monitoring tools. It activates the orchestration and the automation of a rapid response to cyber-attacks, filling data-protection gaps. It makes these near-real-time immutable snapshots available to be scanned for signs of a cyber-attack. That reduces the threat window by stopping the spread of data compromised by an attack. Quickly making "immutable snapshots" of the data for available for scanning and replacement ensures a quick recovery from cyber-attacks.
- **The AI/ML-enabled InfiniSafe Cyber Detection Scanning.** InfiniSafe scanning provides 99.99% accuracy in reporting cyber threats. It detects and analyzes changing data patterns, checking for data corruption, encryption/de-encryption, partial encryption, and more. It is trained to identify both known and unknown types of attack variants and leverages over 200 data points to determine the state of the data. InfiniSafe Cyber Detection is licensed by only the amount of data you need scanned and the length of the contract.
- **Taking a Pro-Active Approach to Enterprise Data Protection.** Taking a proactive approach to scheduling data snapshots – and automating the process of scanning your production data, InfiniSafe Cyber Detection completes the process. Customers know that they have clean copies of their data to recover. Recovery from immutable snapshots is guaranteed to be one (1) minute or less, resulting in rapid recovery from cyber-attack.

Infinidat's Customer-Centric Approach

The combination of these powerful capabilities is an important differentiator for Infinidat. Importantly, it works alongside market-leading backup-and-recovery software products on the market today – and these are already widely used inside customer's enterprises for daily backups.

Accurate detection within the enterprise data itself is key to the business recovery within your business organization. The vulnerabilities are clear, but data-protection software solutions vary in their effectiveness.

Bringing "immutable" data replicas that can be recovered within minutes of any cyber-attack and orchestrated immediately – allows data to be restored in near-real-time. These replicas protect file-formatted and block-formatted data with no disruption or performance impact on the application or workload. This approach (See Figure 5) is essential to rapid data recovery by accurately detecting and assessing cyber-attack damage.

Key parts of the Infinidat solution include a comprehensive technology stack, Automated Cyber Protection, AI/ML Scanning, and proactive data
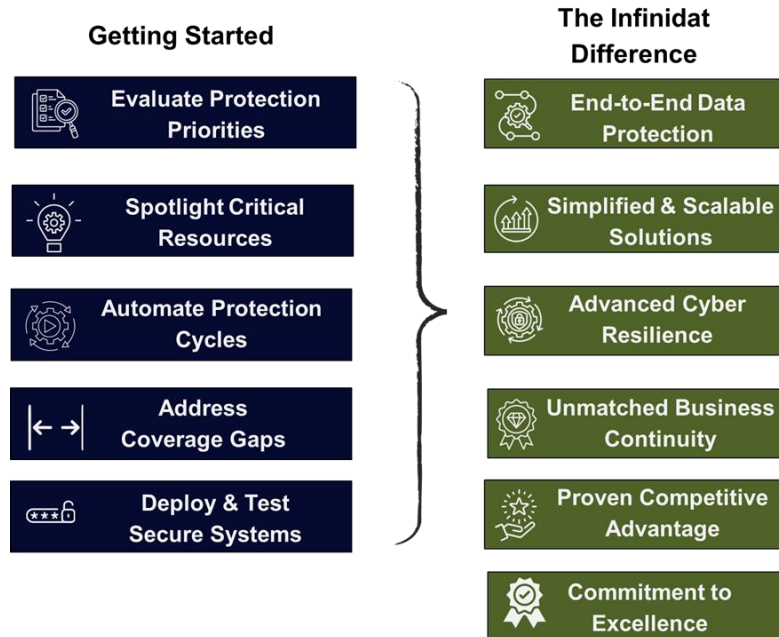
Data is restored in near real-time

Figure 5: The Infinidat Difference and Customer-Centric Approach

The Importance of Cyber-Resilience: Analysis

Companies become cyber-resilient when they clearly identify their critical data resources across their organization.

These resources become protected by using instant immutable data replicas, which are logically locally stored and/or replicated for further isolation. Any of these can be made available to an orchestrated "fenced" environment for validation and restoration within minutes of any cyberattack.

Infinidat leverages data isolation, data protection, and AI/ML-based scanning technology that detects compromised data using scanning technology that looks at the actual data and 200 other data points, and it restores the data within minutes of that initial attack.

The combination of these powerful capabilities is a differentiator for Infinidat. It goes beyond automated backup and recovery and works with the leading backup and recovery software ISV products.

We believe this is a pragmatic approach for customers because enterprises have been installing data-protection software solutions for many years – in their data centers and across multiple locations.

Infinidat's next-generation technology leverages advanced software capabilities and AI to protect data in block and file formats wherever they exist in an organization. The innovation here is the ability to rapidly detect, locate, and restore data, allowing organizations to resume normal operations in minutes rather than hours.

Customers can get started quickly and easily to benefit from the Infinidat advantage

Infinidat leverages data isolation, data protection, and AI/ML Scanning for rapid recovery to provide powerful capabilities beyond backup and recovery

Key Takeaways and Conclusion

There is a way to protect your business data – and to ensure 24 x 7 x 365 access to that data – no matter where it is stored in your company's data landscape. To achieve that goal, customers must find solutions that fit into a well-coordinated defense against cyberattacks and ransomware – worldwide and around-the-clock. Customers who adopt a thorough approach can detect and secure the data that is essential to protecting their data resources reliably and comprehensively.

Armed with the ability to restore access to mission-critical data within minutes of an attack, customers soon see that the benefits of this approach are clear: These customers are maintaining round-the-clock access to their mission-critical production data, and they're fending off attacks that would have the potential to corrupt their most vital data resources while damaging or halting their business.

In an environment that continually threatens to interrupt your business operations with cyber-attacks and ransomware, Infinidat's comprehensive approach to rapid recovery from cyber-attacks protects your enterprise data, ensuring business continuity throughout your entire organization.

Infinidat's comprehensive approach to rapid recovery from cyber-attacks protects your enterprise data, ensuring business continuity throughout your entire organization