Build *infrastructure resilience* to take the sting out of ransomware

How a proactive data recovery strategy helps to protect your business

Capgemini

Don’t let ransomware stop your business

When ransomware strikes, many organizations hit the panic button. Often, they don’t have a clear plan in place to recover all of their data rapidly. And even if they have a plan, they can’t be sure the data they recover hasn’t been infected.

While security leaders largely focus on threat prevention, IT leaders tend to concentrate on supporting the enterprise infrastructure. Recovering data after an incident falls somewhere between these two lines of responsibility, and it’s often entrusted to traditional backup solutions that offer inadequate protection in the modern threat landscape.

In many cases, the recoverability of clean data is untested, so organizations have no idea how much they’ll be able to recover. Without the infrastructure resilience to rapidly recover all data – and ensure it’s not been compromised – organizations are at risk of huge financial, reputational, and productivity losses. It’s a bad position to be in, especially on a day when teams across the organization are already in panic mode.

In 2023, there was a ***74% increase*** in the number of ransomware attack claims worldwide compared with 2022.

In this guide, we’ll explore the challenges ransomware creates for traditional backup strategies and outline a new approach to data recovery that helps organizations guarantee 100% recovery of clean data.

Traditional backup is no longer enough

Cyberattacks are becoming more sophisticated, with ransomware attackers often targeting backup images to neutralize organizations’ disaster response. In addition, AI-enhanced attacks and the ready availability of “ransomware-as-a-service” allow even inexperienced and unskilled attackers to cause enormous damage.

Soft ransomware targets are now the ***second biggest concern*** for risk executives and managers, after AI-enhanced malicious attacks.

A recent Gartner survey revealed that enterprise risk management leaders are increasingly concerned about ***“soft ransomware targets”*** In many organizations, these soft targets could include backups, which are often afforded less protection than production systems.

With AI and ransomware-as-a-service making it easier and cheaper to deploy attacks, there’s every reason for leaders to be concerned. “Similar to AI-enhanced malicious attacks, soft ransomware targets require minimal experience and cost to cause significant financial and reputational damage,” said ***Gamika Takkar, Director, Research in the Gartner Risk & Audit Practice***. “Ransomware-as-a-service lowers the barrier to entry for inexperienced cybercriminals who know just enough about how to attack and disrupt business operations, creating worse impacts than usual when attacks occur.”

Time to get proactive

The heightened threat of attacks has made many organizations adopt a proactive approach to cyber defense, but recovery measures are still mostly reactive. To mitigate the damage caused by modern cyberattacks, organizations need to be proactive about data recovery and infrastructure resilience.

Backup solutions offer cost-effective storage, but relying on them alone won’t make business-critical data easily recoverable. Organizations with a resilient infrastructure go beyond traditional backup by prioritizing three principles: data survival, data integrity, and rapid recovery with minimal data loss.

Building strategies and capabilities around these principles ensures these organizations can recover their data reliably and resume operations rapidly, reducing the impact of cyberattacks.

A proactive approach to data recovery and infrastructure resilience

Focusing on complete infrastructure resilience allows organizations to address regulatory compliance demands while providing robust ransomware protection across complex hybrid environments.

This approach has several key features that combine to ensure data is 100% recoverable after an attack, enabling organizations to avoid data loss and ransom payments:

Automated data recovery

By implementing recovery automation, organizations avoid the additional risk of making hasty decisions in the panic immediately after an incident. Instead, automated systems take the necessary steps to rapidly recover clean data. Meanwhile, teams follow clearly documented procedures to respond to incidents effectively and help the business recover as quickly as possible.

Regular testing of the recovery solution provides valuable peace of mind that clean data will be 100% recoverable. Granular recovery automation also helps organizations restore data efficiently and optimize resource utilization.

Zero trust data protection

A default setting of “trust nobody” is vital for preventing data loss and recovering clean data. Zero trust data security prevents organizations from restoring compromised files by analyzing backups and quarantining files that contain identified threats, mitigating the risk of additional damage after an attack.

This approach must be infrastructure-agnostic to safeguard data and applications across on-premises environments, public and private clouds, and SaaS platforms.

Immutability, air-gapping, and hardware acceleration

To expedite recovery, this proactive approach uses immutable backups that attackers can’t alter in any way and logical air gaps that isolate backups even if primary networks are compromised. This makes it easier and quicker to recover unaltered, clean data.

To restore data even faster after an attack, organizations can use specialized, low-latency hardware that eliminates much of the effort of restoring data from traditional backup appliances.

Threat hunting and data monitoring

Proactive data recovery also extends to threat hunting to Identify and mitigate risks in moving data with pattern learning and leverage the latest threat intelligence to stay ahead of attackers. Continuous threat and anomaly monitoring and sensitive data identification across on-premises, cloud, and SaaS environments also provides greater visibility of the organization’s data assets, wherever they reside or move.

Taking data recovery beyond traditional backup offers significant business value:

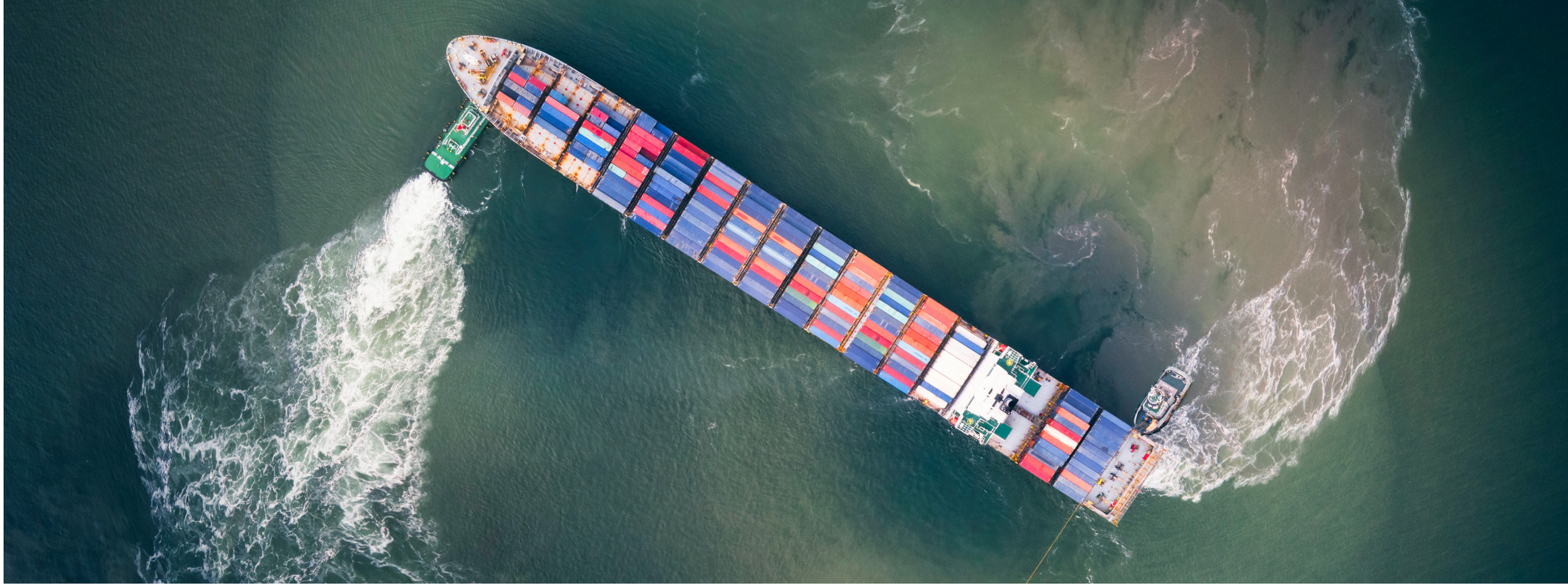
- More robust systems and a more resilient infrastructure
- Improved data and threat visibility across on-premises, cloud, and SaaS environments
- Strong governance and cohesive, efficient data restoration processes
- Streamlined compliance with global data regulations
- Faster recovery to minimize the financial and operational impact of attacks

Infrastructure resilience: key success factors

Shifting from reactive data recovery to a proactive approach to infrastructure resilience requires the right tools, technologies, and expertise. At Capgemini, we combine all these factors in our Data Recovery offer to help organizations build the infrastructure resilience to recover successfully from ransomware attacks.

Data Recovery offer combines our partners’ technology and the deep experience of our experts to help organizations establish effective recovery capabilities, processes, and governance protocols.

This offer supports compliance with numerous data regulations, including DORA, NIS2, PRA, FED, APRA, GDPR, and PCI-DSS. Importantly, it’s also infrastructure-agnostic, providing feature parity on a single, unified management system for all on-premises, private and public cloud, and SaaS environments.



To help organizations minimize the time and effort of building infrastructure resilience, our Data Recovery offer includes a range of accelerators:

Automated recovery tools – enabling organizations to recover data quickly and efficiently after a ransomware attack, helping minimize downtime and rapidly restore operations.

Data backup and recovery solutions – ensuring organizations always have secure, up-to-date backups of their critical data to minimize the operational impact of ransomware attacks.

Incident response framework – executing predefined processes and procedures to respond to ransomware incidents effectively and efficiently.

Advanced threat detection technologies – helping organizations identify ransomware attacks early and take proactive measures to minimize their impact.

Continuous monitoring and threat intelligence – keeping organizations informed about evolving threats and emerging trends to help proactively strengthen their defenses.

Training and awareness programs – educating employees about ransomware threats and giving them the knowledge and skills to recognize, prevent, and respond to attacks.

Create a more resilient infrastructure- and build an unstoppable business

As the threat of ransomware grows and attacks evolve, organizations must take proactive steps to protect themselves against data loss, operational downtime, financial losses, and reputational damage.

It's critical to move beyond traditional backup strategies that weren't designed to cope with modern ransomware attacks. By refocusing on infrastructure resilience, organizations can rapidly restore immutable backup copies of their data, minimizing downtime and data loss and eliminating the need to pay ransoms.

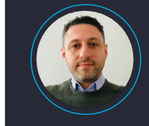
With infrastructure resilience – founded in proactive, automated data recovery –organizations can mitigate the impact of ransomware attacks, even as cybercriminals evolve their tactics in the future.

Next steps

To explore how a proactive approach to data recovery and infrastructure resilience can help you stay ahead of ransomware threats, ***get in touch with our experts***.

About the authors

Jordi Benet
Global Head for Data Center Transformation, Infrastructure Services, and Networks Service Line (DCT-IS-Network SL) Cloud Infrastructure Services



Izzet Biyikbeyoglu
Portfolio Lead for Data Center Transformation, Infrastructure Services, and Networks Service Line (DCT-IS-Network SL) Cloud Infrastructure Services

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided every day by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of nearly 350,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering, and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the future you want | www.capgemini.com

CIS_08.03.2024_SoumiBiswas

For more details contact:

infra.global@capgemini.com