

How to survive ransomware by mastering disaster recovery

The landscape of disaster recovery continues to undergo a significant transformation, driven by the increasing reliance on SaaS applications and the rising threat of ransomware. As part of this transformation, traditional disaster recovery methods are evolving into more comprehensive resilience strategies.

In a recent Keepit webinar, guest speaker Brent Ellis, senior analyst at Forrester, shared actionable advice for organizations to shift from a reactive to a proactive strategic position, focusing on securing systems to withstand various disruptions. This involves understanding where data resides and recognizing the unique risks associated with each location, requiring tailored protection strategies.



Here's a look at a comprehensive approach to data management and risk mitigation

Data location	Risk	Protection strategies
Data centers	Physical damage, theft	Secure facilities, regular backups
Cloud	Downtime, data breaches	Multi-cloud strategy, encryption
Silos	Access control issues	Centralized management, audits
Desktops	Loss, malware	Endpoint protection, backups
Mobile devices	Theft, data leaks	Mobile device management, encryption
SaaS environment	API exploits, outages	Third-party backups, continuous monitoring

Consider where your data resides

Data resides in various locations such as data centers, cloud environments, silos, desktops, mobile devices, and SaaS platforms. Looking ahead, there will be a growing integration of data into and generation by AI systems, which will require robust security measures to handle these emerging data flows effectively.

Recognizing risks

Different locations and systems, such as cloud versus on-premises, pose unique risks that require tailored protection and recovery strategies. These risks need to be identified and evaluated before risk mitigation can take place.

Evolution of disaster recovery

The focus is shifting from traditional disaster recovery to technology resilience, emphasizing proactive measures to ensure business continuity and making sure disruptions have limited impact on the business.

Focus areas for resilience

Understanding the risks associated with different data storage methods is essential for building resilience. Implementing and maintaining robust backup solutions is critical, including regular testing to ensure backups are effective and can be quickly restored when needed. Regularly testing and updating recovery plans ensures they can withstand disruptions such as ransomware attacks, which are continuously evolving.

SaaS resilience

SaaS environments present unique risks, due to the limited control over the underlying infrastructure. The shared responsibility model means organizations are responsible for protecting their data themselves.

To build a resilience strategy, organizations should consider using third-party backup services, offering additional layers of protection in an isolated environment separated from the public cloud.

“Generally, people expect their SaaS providers to back up their data, protect it and secure it. But as we’ve seen, that is not always the case. And when you think about SaaS, it’s not just one platform, it’s not just your data center, it’s not just your cloud environment. It’s a variety of different platforms that do different things for your environment. And each has a different way of protecting it and keeping it safe.”

Brent Ellis, Senior Analyst at Forrester

SaaS platform risks to consider in your disaster recovery planning

Risk	Solution
API exploits	Regular audits, stronger authentication
Shared platform vulnerabilities	Segregated, air-gapped backup location, e.g., with a third-party backup service
Cyber threats	Continuous monitoring, advanced threat detection, and incident response
Limited version retention	Implement comprehensive version control and retention policies
Role-based access control issues	Enforce strict RBAC policies, regular review, and adjustment of access privileges
Exfiltration threats	Encryption, network segmentation, and data loss prevention (DLP) tools
Malicious data changes	Implement immutability options, regular integrity checks, and audit trails
Accidental data changes	Regular user training, versioning, and undo capabilities
Platform misconfigurations	Regular configuration audits, automated compliance checks
Vendor dependency	Diversify vendors, implement robust exit strategies
Insufficient backup solutions	Ensure comprehensive backup plans, regular testing, and validation
Compliance and regulatory risks	Regular compliance audits, adherence to data protection regulations


How to create a SaaS resilience strategy

Building cyber resilience involves gathering knowledge about the SaaS platforms you use and understanding their risk profiles. Once you have done a risk assessment, you can decide how to mitigate that risk and develop a resilience strategy. This includes assuring that the security posture of these environments meets your needs and backing up data. It is vital to use immutable backups and set up isolated recovery environments, which ensure data integrity and quick restoration. Continuous scanning of backups is crucial for detecting threats, maintaining the overall integrity of data recovery processes.


Three important resilience measures

1. **Isolated recovery environments:** Dedicated spaces for secure data recovery
2. **Immutable backups:** Backups that cannot be altered by malware
3. **Continuous scanning:** Regular scans to detect and mitigate threats


Here at Keepit we:




Are specialized on SaaS data protection
We support a wide range of commonly used SaaS platforms, such as M365, Entra ID, Salesforce, and more. Our solution is purpose-built and specifically designed for protecting cloud SaaS data.



Deploy leading security measures
We deploy leading security measures, keeping your data safe in a fully air-gapped, separated environment with immutability by default and encryption both in transfer and at rest.



Are a completely independent backup provider
We maintain our own cloud infrastructure and our own data centers across the world. Vendor independence means you'll always have access to your data, even when disaster strikes.



Hold relevant security certifications
As your trusted cloud backup vendor, we're serious about the security of your data. Keepit holds both the ISO/IEC 27001:2013 certification and the ISAE 3402-II certification (audited by Deloitte annually).

Continue the conversation

Watch the on-demand webinar

[Watch it now](#)



keepit
Webinar: On-demand
How to survive ransomware by mastering disaster recovery
Featuring: FORRESTER
Brent Ellis
Guest speaker
Senior Analyst at Forrester

Keepit provides next-level SaaS data protection purpose-built for the cloud, by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience and future-proof data protection.

For more information visit www.keepit.com or follow Keepit on [LinkedIn](#)