ANALYST BRIEF
Sponsored by: Google Cloud

A complete cyber-recovery solution should provide security expertise, recovery guidance, and other services to organizations that don't have all the skills and resources to do it themselves.

Using the Cloud to Bolster Cyber-Recovery Strategies

July 2024

Written by: Johnny Yu, Research Manager, Infrastructure Software Platforms, Worldwide Infrastructure Research

Introduction

Cyberattacks in general and ransomware attacks in particular have become so pervasive, sophisticated, and destructive that it's no longer helpful to ask "When?" but rather, "How severe?"

An IDC survey found more than 90% of organizations acknowledged being attacked by malware, and of those, 87% said the attacks led to successful intrusion. While not all intrusions resulted in dire outcomes, in total, one-third of the respondents suffered an attack that blocked access to their data or key systems.

AT A GLANCE

KEY STAT

According to IDC research, 90% of organizations acknowledged being attacked by malware, and of those, 87% said the attacks led to successful intrusion.

The consequences of ransomware attacks are costly. Other than the price of the ransom itself, organizations suffer downtime, reputation and brand damage, productivity loss, compliance violations, and potential lawsuits. These costs add up, and for businesses that don't have a solid cyber-resilience plan, they can prove fatal.

The U.S. National Institute of Standards and Technology (NIST) has established a framework to help businesses build a strategy for cyber-resilience. It consists of five pillars: identify, detect, protect, respond, and recover. While organizations need to adequately address all five pillars, the sheer pervasiveness of cyberattacks revealed in IDC research highlights the importance of the "recovery" aspect of cyber-resilience. Because cyberattacks are inevitable, cyber-recovery must also be readily available.

Hallmarks of a Cyber-Recovery Solution

Data survival is foundational to cyber-recovery. A cyber-recovery solution needs robust and redundant backup to guarantee there is a clean copy of data to recover from. As some malware can lay dormant for long durations, the solution should store backups spanning multiple points in time to maximize the chances of having an uncompromised copy.

IDC research found that in nearly half of the cases, attackers will attempt to delete or corrupt backups to prevent victims from recovering. Therefore, a cyber-recovery solution must also include ways to store clean backup copies in a secure, immutable, and air-gapped environment. In addition, security capabilities such as malware scanning on the stored copies or requiring multiuser authorization to initiate the recovery process can be implemented as an additional layer of cyber-resilience.

With robust backup serving as its core, a cyber-recovery solution should include an isolated recovery environment (IRE), where backups can be recovered and verified. In a cyberattack scenario, it's important that data is first recovered to an IRE to test that the data is clean and valid. Only after that data is confirmed should production workloads use it.

Although backup and recovery fall into the data protection side of IT, cyber-recovery and the entirety of the NIST cyber-resilience framework depend on data protection and data security working in tandem. A cyber-recovery solution should therefore be integrated with security tools to allow for combined and effective responses from both IT and SecOps.

Last, a complete cyber-recovery solution should provide security expertise, recovery guidance, and other services to organizations that don't have all the skills and resources to do it themselves. IDC research found only about 30% of companies can fully recover on DIY efforts alone. Cyber-recovery requires extensive cyberattack knowledge, and because attacks evolve rapidly, it is difficult for organizations to maintain expertise.

How Cloud-Based Cyber-Recovery Aligns with Cyber-Resilience Needs

The cloud makes sense as the back end supporting a cyber-recovery solution. With highly scalable infrastructure that can be created and collapsed on demand, it is well suited for the IRE use case. Cloud-based IREs can support failover from production environments without requiring a physical secondary site for failover, and with organizations only needing to provision (and pay for) as much compute and storage as they need (and only when they need it). Network access to cloud-based IREs can be tuned as necessary to deliver levels of isolation aligned to security requirements.

In addition to the nature of cloud infrastructure, cloud service providers (SPs) themselves may have backup and recovery offerings that can be used as the foundation of cyber-recovery. Native tools found on cloud platforms may deliver robust backup capabilities, with features designed specifically to enable cyber-recovery.

Cloud SPs provide a platform to serve as a nexus for value-added integrations. This would allow security tools to integrate with native data protection capabilities on the platform, which is crucial to an effective cyber-recovery solution. This level of efficient integration extends to other valuable technology that could support the cyber-recovery use case, such as AI/ML.

Considerations

When implementing a cloud-based cyber-recovery strategy, organizations should take the following into consideration:

- **Prioritize cyber-recovery services to close skill and knowledge gaps.** While cloud SPs often offer many tools for building a solid cyber-recovery solution, it is important to find one that can offer services to make up for a lack of cyber-resilience expertise. Tools are always useful, but some organizations need expert guidance with implementation and best practices to effectively use those tools. More importantly, expert services allow organizations to keep up with evolving threats without devoting their own resources to maintaining cyber-resilience expertise.
- **Switching cloud SPs can be difficult.** Organizations that already have a cloud of choice or were locked into one due to other aspects of their infrastructure will have limited ability to use another cloud SP for their cyber-recovery solution. Therefore, it is important that organizations fully understand their cloud SPs' cyber-recovery offerings and how well they integrate with their own overall cyber-resilience strategy to build the best possible solution.

» **Data sovereignty must be maintained.** Organizations must ensure that compliance is maintained. As certain industries have strict rules governing how and where backup data is stored, organizations must carefully vet cloud SPs' offerings and configure for compliance where appropriate. Depending on cloud SPs' offerings and organizations' needs, using the cloud for cyber-recovery may not work for every situation.

Conclusion

Implementing the key elements of a cyber-recovery solution can minimize the impact of cyberattacks, and using cloud infrastructure to support cyber-recovery provides many benefits. IDC believes the pervasive nature of cyberattacks is driving organizations to actively pursue not only cyber-recovery but full cyber-resilience in accordance with the NIST framework.

Using cloud infrastructure to support cyber-recovery provides many benefits.

About the Analyst

Johnny Yu, *Research Manager, Infrastructure Software Platforms, Worldwide Infrastructure Research*

Johnny Yu is research manager within IDC's Worldwide Infrastructure Research organization and part of the Infrastructure Software Platforms practice. His coverage includes storage software, data replication, protection and archiving software, storage device management, and container data management.

MESSAGE FROM THE SPONSOR

Google Cloud delivers robust cyber recovery solutions, leveraging years of security expertise. Our centralized backup service (Google Cloud Backup and DR), and Backup for GKE efficiently protect critical data, secure backups against unauthorized deletion, and integrate with security tools to support threat detection. In addition, leveraging the Compute Engine (GCE), Kubernetes engine (GKE), and VMware engine (GCVE) services, Google Cloud also enables on-demand creation of isolated recovery environments (IREs), supporting forensics and recoveries into secure, trusted environments. Finally, Mandiant, now part of Google Cloud, offers specialized expertise and services to enable enhanced resilience and response.

To learn more, complete the Security & Resilience discovery assessment to receive customized guidance regarding best practices and relevant solutions, including services such as: Google Cloud Backup and DR.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com