Zero Data Loss: Peace of Mind in the Ransomware Era

Alexei Balaganski

January 25

Oh, how time flies! Can you believe that we've been living with ransomware for over a decade already? Sure, a pedantic historian could explain that the first occurrences of malware encrypting files and asking for a ransom to restore access were recorded all the way back in 1989. Yet, it took another couple of decades for IT infrastructures and cryptocurrencies to evolve to a stage when ransomware truly became profitable and turned into a major risk with global impact.

The public probably experienced it for the first time in 2013, when the CryptoLocker ransomware was able to infect over 250,000 systems and netted its creators over $3 million in ransom payments. By 2017, strains like WannaCry and NotPetya became notorious for causing billions in damage around the world, with the latter showing the true weaponization potential of ransomware. In fact, NotPetya's creators were not even interested in collecting ransom, they just wanted to cause long-lasting damage to their victims.

And ever since, the entire world has been living under the constant fear of a ransomware attack. For many organizations, it has become the existential threat number one, surpassing all other known cybersecurity risks. It's the combination of immediacy, unpredictability, and the severe consequences of even a single attack that makes it so scary, amplified even further by the lack of a single comprehensive solution to reliably prevent them in the future.

A proper strategy for ransomware prevention must include a broad range of measures, proactive and reactive, technology- and process-based, covering a multitude of attack vectors. These include everything from e-mail and web monitoring to endpoint detection and response to network security and identity governance. And yet, for most victims, the most viable scenario of surviving a ransomware attack is not to prevent it, but to contain the damage, restore their disrupted processes, and recover business-critical data as quickly and painlessly as possible…

With this realization, now is the right time to stop thinking about ransomware as malware that just encrypts or steals your files. In fact, it does much more direct and indirect damage than that – and to start thinking of new tools to augment your existing anti-ransomware toolkit. This is especially relevant for backup and disaster recovery. For example, a lot has been written recently about immutable backups as a crucial factor for ransomware resilience. It is a well-known fact that modern ransomware specifically targets backup locations to make the recovery more difficult, but are you sure that you are even doing your backups properly in the first place?

Recently, I attended a presentation of Zero Data Loss Recovery Appliance, Oracle's specialized solution for backing up mission-critical databases. While I was familiar with the product already, I was somewhat surprised that the company now positions it as a premier solution for ransomware protection. Wait, what? Do ransomware groups even consider relational databases a viable target? And isn't Oracle's own Autonomous Database with all its built-in security control supposed to be 100% resilient against these attacks anyway? However, the more I was thinking about it, the more sense it all started to make.

First, not even the most hardcore Oracle customers have all their data stored in the Autonomous Database, which is, after all, a managed cloud service. For many industries and applications, sensitive data has to stay on premises at all times. Second, even when the database itself is managed by a service provider, their responsibility does not extend to protecting the integrity of the customer's data. And finally, ransomware attacks specifically targeting databases (relational and NoSQL) are not unheard of, especially when targeting specific high-profile victims! In the end, having a secure, reliable, and high-performant solution for backing up business-critical data from enterprise databases does make a lot of sense, since it can substantially speed up recovering from a ransomware attack.

Zero Data Loss Recovery Appliance (Recovery Appliance) is an engineered system for comprehensive data protection of Oracle databases, ensuring backup immutability, continuous validation, and rapid recovery without data loss, even in the event of a ransomware attack. It integrates natively with Oracle databases to consistently validate backup data, detect anomalies, and enforce retention policies, offering recovery up to the last sub-second before a data loss incident. The appliance supports flexible deployment architectures, including air-gapped Cyber Vaults, to enhance data protection and resilience. By consolidating incremental backups into space-efficient virtual full backups, Recovery Appliance minimizes recovery time while maintaining the highest data integrity and security standards.

Since the appliance is built on Oracle Exadata engineered system that customers leverage today for running the most critical enterprise Oracle databases, it inherits the underlying platform's performance, scalability, and availability characteristics. And since it natively supports all the internal data structures and protocols of an Oracle Database, it offers unique capabilities that no third-party, especially file-based, backup tool can provide. It can operate in "incremental forever" mode, only capturing small data changes in real time during backup but will reassemble ("materialize") them into a consistent full copy on the fly when needed for restoration.

Of course, all the backup copies stored by the appliance are immutable, but in addition to that, they are continuously validated for recovery integrity, down to the transaction level. Whenever you need to restore data, you can have peace of mind knowing that it will be free from any tampering or anomalies, whether caused by ransomware or other data compromise, encryption, or corruption scenarios.

To boost the level of security and compliance even further, while still meeting the RTO/RPO requirements, it is possible to deploy the appliance in an "air gap" configuration, further separating backup copies from production data. Whenever a full physical isolation is impossible or impractical, the combination of ZDLRA's security features (immutable backups, end-to-end encryption, strict access controls, integrity checks) with network segmentation provides a strong level of "logical air-gapping" consistent with NIST best practices.

Recently, Oracle announced **Zero Data Loss Autonomous Recovery Service**, a cloud-native, Oracle managed counterpart of the on-premises appliance. It offers the same capabilities but in the cloud; in fact, the service is available in all clouds currently partnered with Oracle: Azure, GCP, and AWS. Cloud backups also have a significant advantage of being natively distributed across multiple availability zones, so they remain available even if a zone goes offline. It is even possible to quickly restore a backup to a different region or tenant to deal with catastrophic failures – not just ransomware but natural disasters, like earthquakes or tornadoes.

The company is now working on integrating these two offerings to support hybrid deployments in the future. But even now, according to Oracle, the Recovery Service is projected to become their largest cloud service by total storage volume.

So, will it really protect your organization from ransomware attacks? I'm afraid that asking this kind of question is misleading and even somewhat dangerous. There is simply no single tool or technology that can provide complete protection, given the broad range of vulnerabilities and threat vectors that can be exploited by malicious actors. What it can offer though is a turn-key solution for a specific kind of risk – a risk of losing access or compromising your critical sensitive data.

In a world where ransomware evolves faster than defenses, solutions like Oracle's Recovery Appliance are not just useful tools – they're lifelines, turning catastrophes into recoverable incidents and keeping your business resilient when it matters most.

If you're looking for more information about Oracle's solution, check the links below:

Zero Data Loss Recovery Appliance Product Home

Zero Data Loss Autonomous Recovery Service Product Home

Oracle Backup & Recovery Technologies Blog Central

Oracle Backup & Recovery AskTOM Office Hours

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.