zensar

Ransomware and Backup

Making backups ransomware-ready

An RPG Company

A ransomware cyberattack occurs when malicious software denies a user or business access to a computer system or data. Ransomware attacks happen for many reasons, including reputation damage, extortion, and service disruption for different gains.

The malware spreads through phishing emails or visits to malicious websites. Usually, there is a demand for payment for the affected files to be unlocked.

Ransomware attacks have experienced a resurgence, with recent attacks focused on the international healthcare, local government, and education sectors.

The year 2021 can be called the year of data breaches caused by ransomware.

Ransomware attacks severely impact businesses and can lead to production disruption, sensitive data leaks, costs associated with remediation, recovery, potential ransom payment, litigation, and reputation damage. The rise in people working from home and the extensive use of VPNs have also contributed to a considerable surge in cybersecurity threats.

Joseph Blount, CEO of Colonial Pipeline Co., told The Wall Street Journal that he authorized a ransom payment of $4.4 million because his executives were unsure how badly a ransomware cyberattack had breached systems and how long it would take to return to regular operations.

Many such ransomware attacks prompt the question of what if?

Are organizations prepared to deal with these challenges? What is the right way to recover from a ransomware attack? How proactive can an organization be? What can be done to mitigate the situation?

Key findings

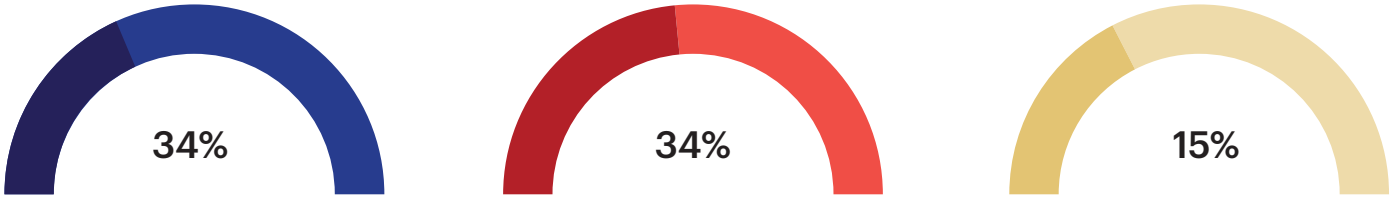


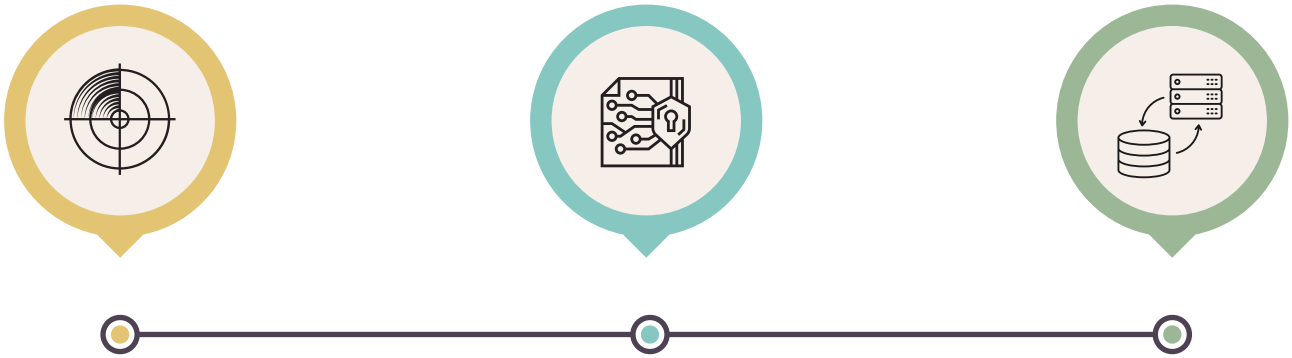
Figure 1: A robust backup strategy

As per the HHS Cybersecurity Program report, 44 percent of ransomware recovery involved backups to restore data. This gives us hope that if we have a good backup strategy with the right infrastructure, we have a fair chance to recover from ransomware attacks.

Figure 2: The 3-2-1 backup

The United States Government recommends the 3-2-1 backup in a US-CERT (United States Computer Emergency Readiness Team) paper. This strategy is an industry standard today. The 3-2-1 backup recommends the following: there should be three copies of data, on two different media, with one copy offsite. The offsite backup should be isolated from the production network.

How Backup Can Help to Protect Your Organization Against Ransomware



Detecting Attacks

Early detection of ongoing data encryption activity and scanning for inactive malware

Protecting the Backup System

Protection of backup repositories, catalogs, job definitions and administrator consoles.

Recovering From Attacks

High-perfomance, safe, orchestrated recovery from attacks

Figure 3: A multi-targeted approach

As indicated in the Gartner study above,
an organization needs to take a multi-targeted approach to deal with ransomware attacks.

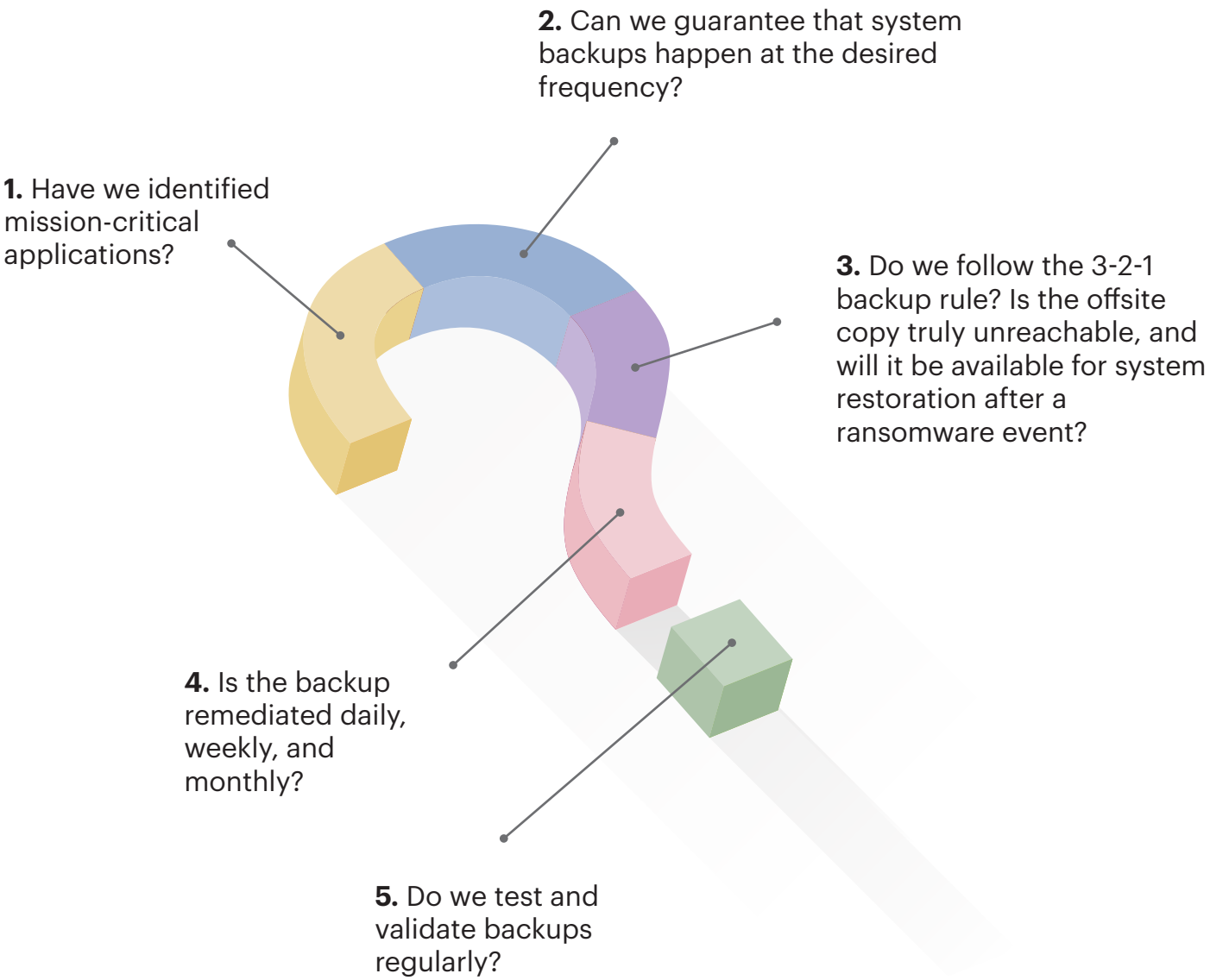
Mitigating security breaches

Here are a few key points to follow to mitigate security breaches:

Holistic review of the backup infrastructure

As the first key finding mentioned, a solid backup routine is the best defense against a ransomware attack.

These are the questions organizations should ask themselves:



Immutable backups

Immutable backups are backups that cannot be altered. This can be done at different backup levels.

Backup software companies such as Rubrik are never available in a ReadWrite state to the client. All applications and data ingested by Rubrik are stored immutably. This is true even during a restore or live mount operation. Since overwrites cannot happen, even infected data later ingested by Rubrik cannot affect existing files and folders.

Immutability can also be achieved at the storage level. Immutable copies of data can be created from an application writing to an MTree on data domain using retention lock.

Air gap and vault implementations

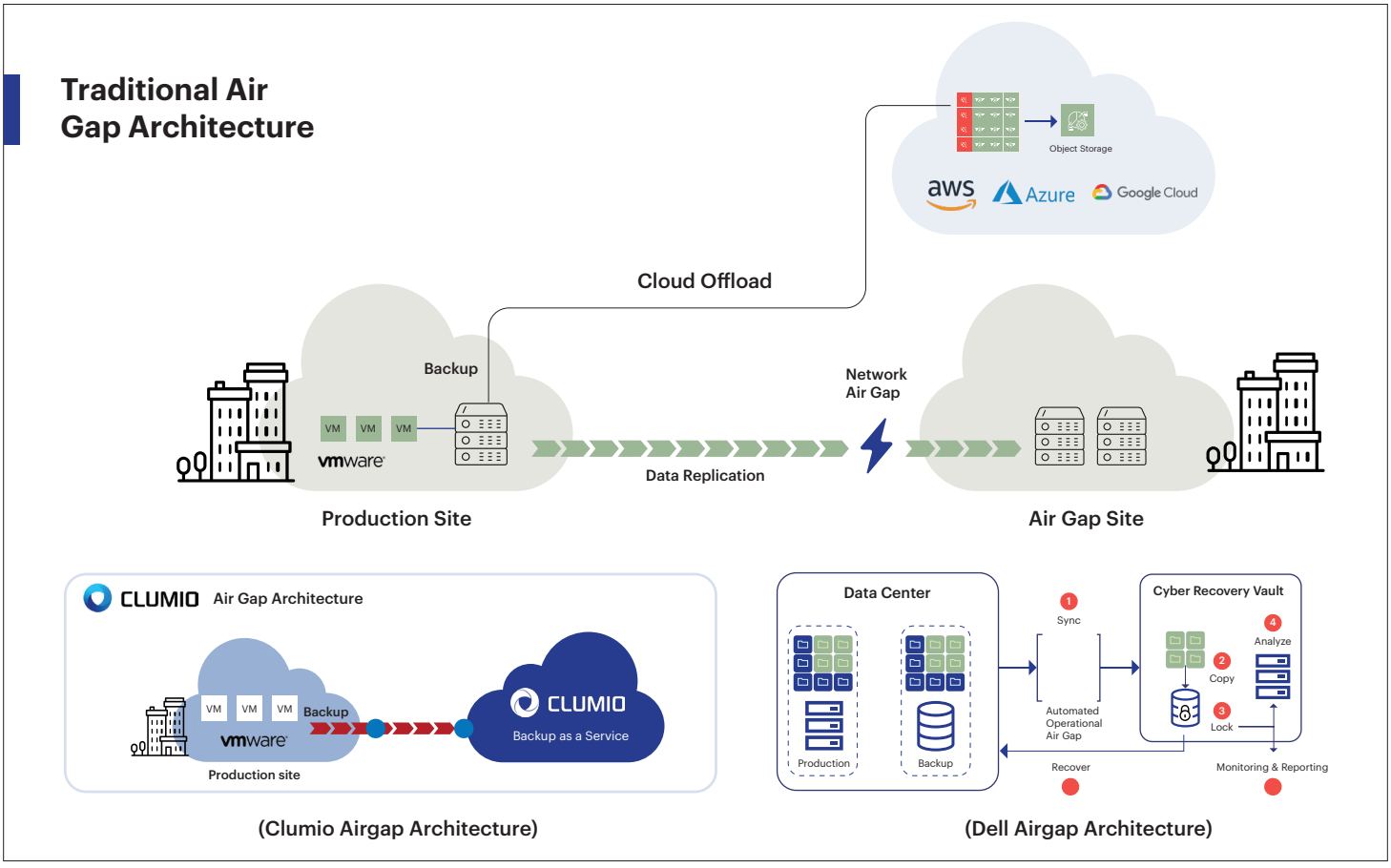


Figure 4: Traditional air gap architecture

Air gap refers to a physical air gap between onsite and offsite backups. With machine learning, air gap identifies and monitors suspicious activity while scheduled automated workflows securely copy data from production to the isolated environment. This helps monitor threats in real-time and vault out the backup copy to prevent it from being accessed. Once a baseline is set, any backup time or schedule irregularities can indicate ransomware infiltration.

Several companies, including Veeam, Dell, and Clumio, now offer their solution version.

Maintenance of systems

System maintenance is an integral part of the overall solution. Companies need to ensure that they are up-to-date on the patches, OS levels, and security vulnerabilities associated with the systems.

User education

One of the most overlooked aspects of cybersecurity is user education. Organizations should educate end-users on the proper security protocols and measures to prevent a ransomware attack. Social engineering and phishing techniques target all vulnerable employees. Hence, obtaining a good level of security demands a shift in the traditional mindset of the employees.

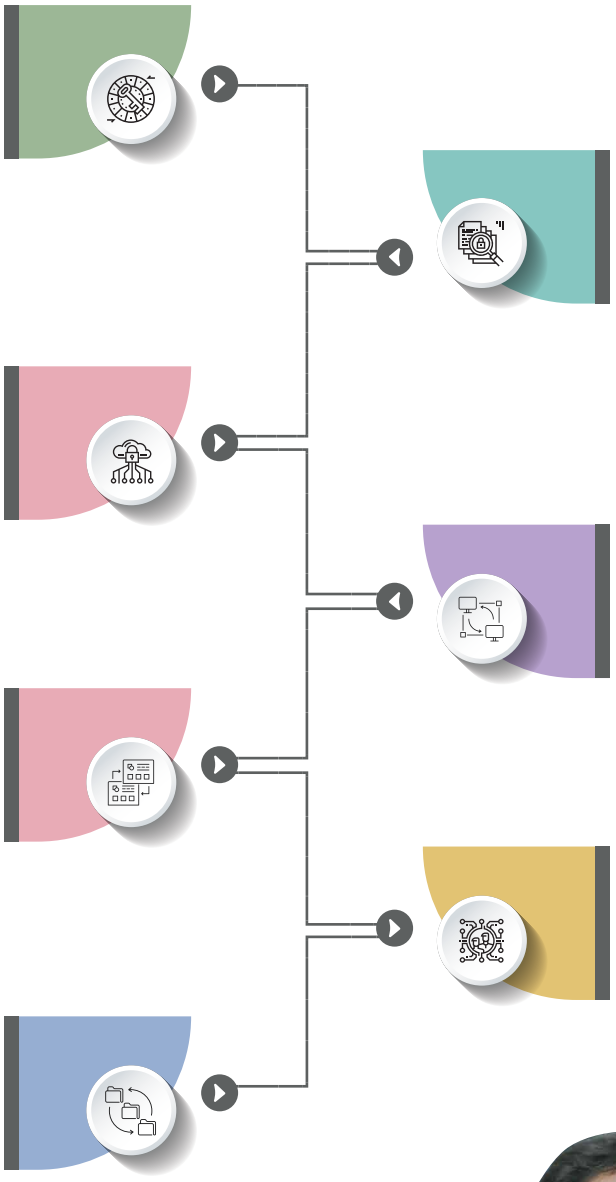
The Zensar advantage – how we can help

Help you evaluate your ransomware preparedness with compact and precise steps to achieve the security goals of your organization

Analyze current security patch strategy, and help create one, if required

Evaluate the relevant regulatory and legal guidance for ransomware in your operating environment

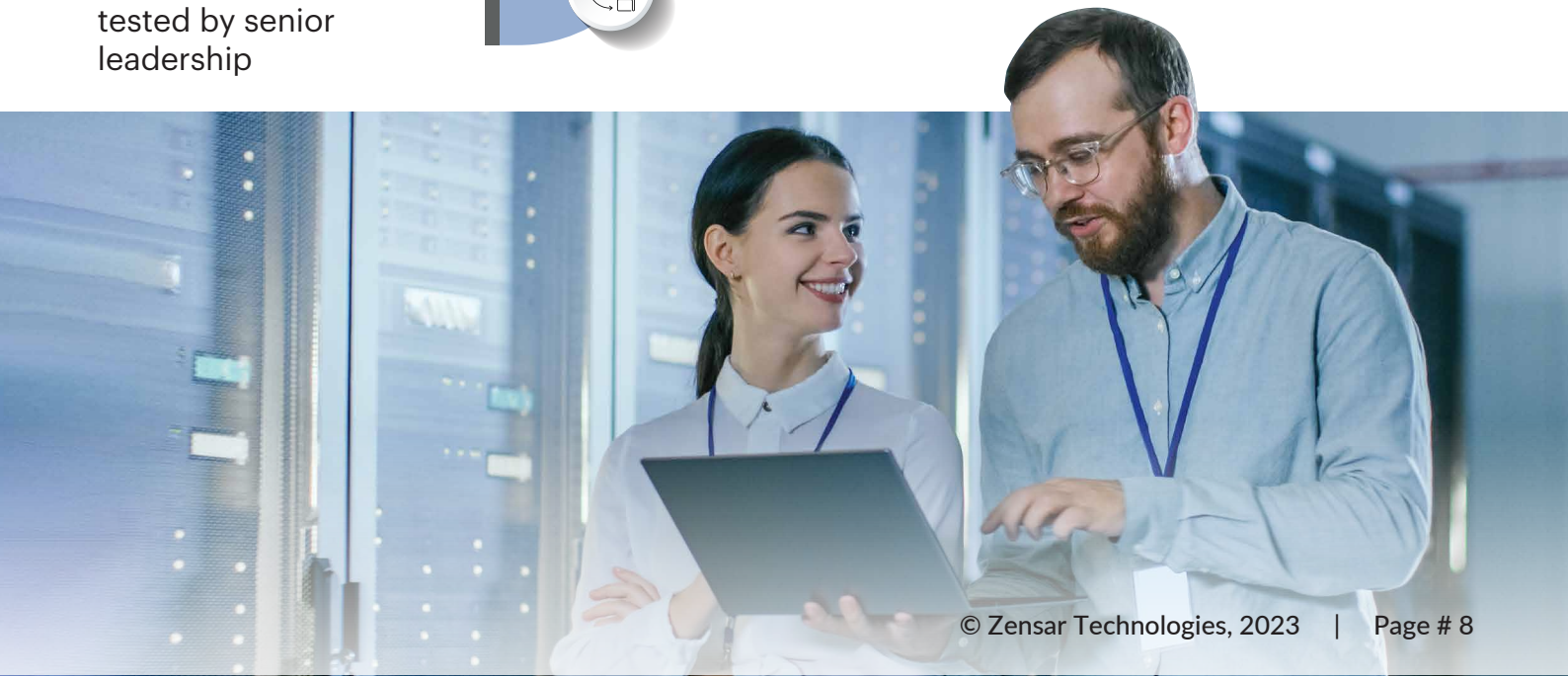
Provide ransomware-specific incident response plan, tested by senior leadership

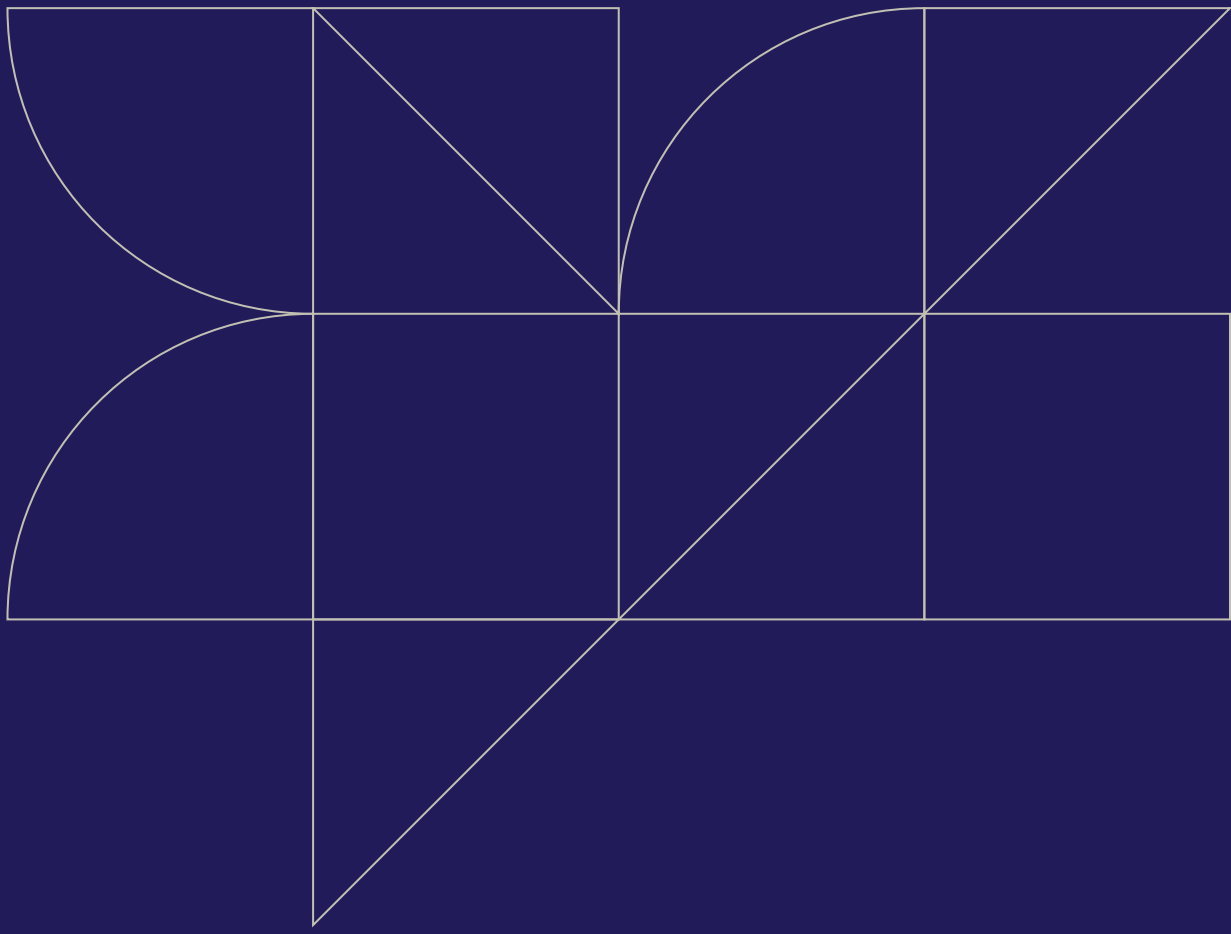


Analyze the backup infrastructure, including software and storage used, protocols, and schedules to ensure daily backups and remote backup copies

Develop a testing plan for remediation, testing restore, and validity of backups, and suggest any transformation, if necessary

Educate employees on cybersecurity and different tactics used for ransomware attacks





zensar

An RPG Company

We conceptualize, build, and manage digital products through experience design, data engineering, and advanced analytics for over 145 leading companies. Our solutions leverage industry-leading platforms to help our clients be competitive, agile, and disruptive while moving with velocity through change and opportunity.

With headquarters in Pune, India, our 11,500+ associates work across 30+ locations, including Milpitas, Seattle, Princeton, Cape Town, London, Singapore, and Mexico City.

For more information please contact: velocity@zensar.com | www.zensar.com