DBVISIT

ESTABLISHING A DEFENSIVE STRATEGY FOR RANSOMWARE

A DBVISIT WHITE PAPER

ORACLE | Partner

INTRODUCTION

With 4,000 ransomware attacks happening daily in the U.S. you can't read the news without seeing an article focused on the rapidly growing impact of ransomware. It has become a threat to businesses large and small and one that organizations must take seriously to protect themselves from potentially devastating consequences.

In recent years protecting mission critical data has become more challenging with increasingly sophisticated ransomware attacks now targeting database encryption and actively seeking to disrupt backups.

Your data is the heart of your business and losing access, even temporarily will affect business operations, customer experience and company revenues.

Unfortunately, many businesses are not prepared for today's more advanced ransomware that makes traditional protection, as well as backup and restore methods obsolete. With the increasing frequency and intensity of attacks, the new reality is that it is no longer a matter of 'if', but 'when' and 'how often'.

THE COSTS AND EFFECTS OF RANSOMWARE

What is ransomware?

Cybersecurity and Infrastructure Security Agency (CISA) defines ransomware as "an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid."

The average ransom paid by organizations in US, Canada and Europe increased from US $115K in 2019 to $312K in 2020 (171% increase year-over-year) [1]. Additionally, 46% of ransomware victims lost some or all of their core data, even after ransoms were paid [2].

Ransomware attacks are on the rise and show no sign of slowing down. Ransomware itself has become easier to access and deploy, especially with the rise in the ransomware-as-a-service (RaaS) model, allowing adversaries to utilize existing ransomware software for attacks. In addition, attackers are becoming more patient - prepared to take their time before attacking, thereby having greater effect, and demanding larger sums of money.

Advanced ransomware is now targeting backups - either by encrypting or removing them - making recovery more complicated or even impossible. Ensuring that backups or disaster recovery (DR) environments are protected and recoverable is critical. With ransomware attackers being more patient and malware residing inside environments for longer periods of time before being activated, this puts traditional backup strategies at some risk - malware could reside within the backup itself. This puts additional emphasis on ensuring that your recovery approach is robust.

At its core, ransomware is just another type of disaster that organizations need to account for when it comes to formulating a business continuity strategy. Although, ransomware presents unique challenges for business:

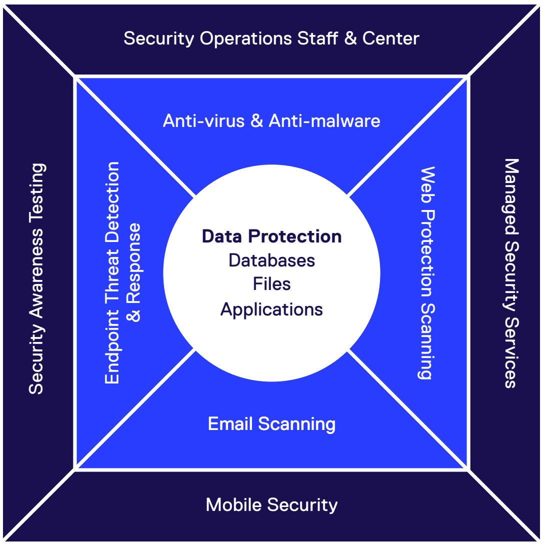
1. Public exposure of sensitive data
2. Financial cost if deciding to pay the ransom
3. Potential loss of data if unable to recover from backups or failure to get data back, even if the ransom was paid.

[1] Source: Palo Alto Networks | Unit 42 Ransomware Threat Report, 2021
[2] Source: Cybereason | ransomware, 2021

ESTABLISHING A DEFENSIVE STRATEGY FOR RANSOMWARE

No single tool exists that can protect you from a ransomware attack. Therefore, experts recommend establishing a multi-layered strategy that encompasses technology, people, and processes. This provides the best chance to reduce the risk of an attack, and in the case of a ransomware attack, gives you the best chance to successfully recover with minimal impact.

Ransomware Defensive Strategy


Security Operations Staff & Center
Anti-virus & Anti-malware
Security Awareness Testing
Endpoint Threat Detection & Response
Data Protection
Databases
Files
Applications
Web Protection Scanning
Managed Security Services
Email Scanning
Mobile Security

Education and infrastructure

The first layer of protection is centered around people and the underlying technology infrastructure.

Providing employees with security awareness training is an easy first step to help combat some of the traditional channels for attacks, such as weak passwords and phishing. This is the simplest and easiest thing to do and something that should be maintained on an ongoing basis.

Ensuring that relevant systems are patched and kept up to date for security concerns, is another area that should be addressed and continually reviewed. Attackers continue to exploit vulnerabilities that exist in software that was designed and built when ransomware was not prevalent. Establish procedures to patch systems and ensure they are kept up to date.

Active Monitoring and Detection

The next layer of protection is focused on active monitoring and detection capabilities that can [a] attempt to block intrusion, [b] detect malware and [c] alert when a breach has occurred. This includes areas such as;

1. Anti-virus and anti-malware
2. email scanning
3. web payload scanning
4. endpoint threat detection and response

Data Protection and Recovery

The final layer of protection in a multi-layered defensive strategy is ensuring that business critical data can be successfully recovered in the event of an attack. This makes recovery the most critical aspect, as it is your last line of defense. The detection and monitoring capabilities can minimize the risk, but you must be able to recover should the worst-case scenario occur.

According to a recent Cybereason research (Ransomware, 2021), Data Backup and Recovery was one of the top 5 technology investments implemented after a ransomware attack. Can you recover your business critical data if there was an intrusion? Have you tested it? Can you verify that it will work? These are all things that should be addressed before attackers get inside your company network. Recovery processes must be implemented and tested to reduce the time, cost and risk associated with recovering from a ransomware attack.

With attackers now targeting backups for encryption or even deletion, a critical strategy to ensure that data recovery is successful includes:

- Backups or standby environments are kept isolated from the primary - preferably off-site, air-gapped or on immutable storage. Companies that have on-premises primary environments are commonly electing to use cloud-platforms for the secondary DR environment.
- Test recovery procedures frequently to validate that recovery can be performed successfully.
- Use tools that automate the processes, to reduce risk of human error and time.
- Protect your secondary environments to ensure they are always available and secure. If secondary environments are breached, then recovery can be more challenging or even impossible.

DATA PROTECTION FOR DATABASES
THE CASE FOR A WARM STANDBY APPROACH

Databases present interesting challenges and have additional options when it comes to implementing a robust recovery strategy.

Recovering databases from backups can be a time-consuming process, as well as the inherent risk that the backup may be corrupted or otherwise unable to restore. Another, more robust approach, is to utilize a warm-standby database – one that is continually being kept up to date and verified. This reduces the risks that come with restoring databases from backups, as well as reducing the RTO and RPO times associated with recovery.

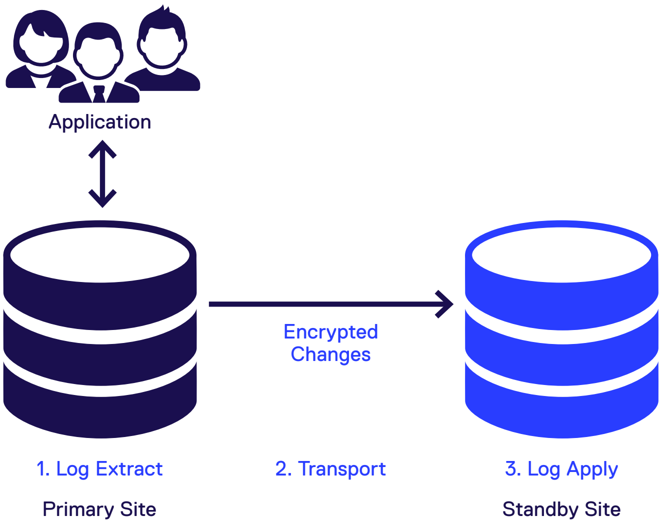
Dbvisit Standby™ falls into the data recovery section of a layered ransomware protection strategy. Standby automates the operational aspects of establishing, maintaining, and even failing over, a warm standby database. Standby provides additional capabilities to enable a robust recovery strategy, such as:

- A continuously validated database enables reliable recovery in the event of disaster, ransomware or malicious attack.
- Standby provides a secure network channel to transfer data between primary and secondary location, rather than relying on simple network sharing mechanisms such as NFS, which are inherently less secure.
- Built-in capabilities for Database Recovery testing, allowing organizations to test that their environment can be successfully recovered when needed.
- Ability to delay the application of transaction logs on the secondary database, by specifying a ‘time-lag’. This provides an additional layer of protection by providing a gap between when a transaction occurred on the primary and when it will be applied to the secondary.

See all features in our datasheet.

How it works

A simple implementation consists of one primary database and one standby database. The solution is built upon database logging mechanisms and physical replication technology to deliver a continuously updated and validated standby database. Read more on our website.



SUMMARY

To protect against ransomware, you need a well-conceived and layered approach that considers both prevention and recovery. An often-overlooked piece of the puzzle is the effective recovery of business-critical databases.

Why many are not prepared:

- Traditional backup and system protection tools are no longer enough.
- Sophisticated ransomware is now encrypting backups and targeting databases.
- For traditional backups, RTO is far too slow to be viable in the event of an attack.
- Continuous data protection and copying isn’t enough as those systems can copy the encrypted data assets before you can stop it.
- Other common types of DR, such as block copy replication, logical replication, or handwritten scripts, all have utility, but it’s essential to understand their limitations.

Concluding – Ensure you have a strong data recovery strategy

While a lot of focus is on preventing an attack, it is critical that companies have a robust, reliable, and tested data recovery strategy in place. It is the last line of defense and therefore must work, if called upon. When it comes to protecting an organization’s most critical data residing with a database, utilizing a warm standby database can reduce risks associated with traditional backup and recovery approaches, while offering excellent RTO and RPO performance.

To find out more about how we can help you protect your critical databases as part of a layered ransomware defense strategy visit www.dbvisit.com