eBOOK

Three must-haves for ransomware resilience

Data security essentials for IT professionals

Introduction

Cyber attack is an unwelcome reality in the digital universe and has been amplified due to the recent shift in remote work, distance learning and rapidly evolving workplace models. No one is immune from it, but everyone must protect against it. Many security experts compare protecting digital assets to securing a home. While that is mostly accurate, the one crucial difference is that cybercriminals don't just walk through your front door to steal your assets, they seep through your walls.

And unfortunately, cyber threats, like ransomware, are here to stay as evidenced by an increase of 41% compared to last year and surging price tags.[1] It is estimated that downtime associated with cyber attacks could cost businesses up to $9,000 per minute.[2] With the recent rash of attacks touching tech, retail, education, healthcare and government agencies, it takes a proactive approach to keep data safe from attack.

To mitigate risk and maintain business continuity, today's businesses require a multi-faceted and comprehensive data protection strategy for ransomware readiness, and a cloud-delivered data backup service is an essential part of that strategy.

ATTACKS ARE GROWING IN SOPHISTICATION

But what was once a lone wolf practice has emerged as a new network of digital organized crime. Bad actors not only understand your data's value but employ sophisticated measures and technologies to orchestrate their attack to more effectively mine for and exploit security loopholes. In other words, cybercriminals too are advancing their business practices.

From Phishing and Ransomware-as-a-Service, to zero-day attacks and supply chain breaches, cyber threats come in many shapes and sizes today[3]. But they all share one common goal: compromise your data. With encryption and exfiltration on the wise, attackers aim to extort your business, by denying access or damaging your data - on their way to a lofty monteary payout.

For comprehensive coverage from today's threats institutions must proactively invest in preventative data security and cyber response measures to keep data safe and recoverable from attack. Not only does this reduce the threat of exposure and liability for businesses but it instills a high level of business continuity in the face of ransomware and malicious attack, among other data loss threats.

PRICE TAGS ARE GOING UP

The impact of ransomware-triggered shutdowns is profound on the victim organizations, especially in the first year following the attack. The lasting adverse effects can drain revenue but also extend far beyond just monetary loss, often resulting in a loss of customers, negative harmful exposure and potential liabilities and lawsuits.

- **Accelerated cyberattacks.** Businesses must defend against an unbelievably high number of sophisticated cyberattacks—designed to just do more than just deny you access to your data. In fact, of ransomware attacks feature some form of exfiltration, encryption, and damage has increased 83%[4].
- **High payouts.** The more valuable the data, the higher the ransom. And as bad actors target sensitive and vital organizational data, price tags are surging. And ransomware victims have almost no maneuvering margin, often being forced to dispense lofty payouts to regain access to their data. In some instances, meeting a ransom doesn't always ensure access as bad actors maintain access to data even after ransoms are paid in full. In fact, it's estimated that businesses damages tied to ransomware will exceed $260 billion by 2031[2].
- **Costly downtimes.** Business disruptions of any kind are expensive. And in today's digital world, malicious attacks on data can be crippling. Without user access to mission critical financial, system, and customer data, outages can stop operations dead in their tracks and result in business and user liability. It is estimated that the average cost of downtime data security and cyber response measures[2].
- **Reputation damage.** Even when they survive a ransomware attack or other data breach, a company's reputation can be irretrievably harmed, with customers taking on a negative view of the brand and an overall loss of client loyalty. That is especially the case with ransomware attacks that shake the foundation of an organization and raise doubts about its ability to protect customers and their data.

RAISING THE THREAT LEVEL

Today's businesses face new internal and external factors which only further complicate how to properly safeguard data from cyberattack. You have new advancements in technology, making ransomware attacks even more dangerous and sophisticated than ever.

Compounded with internal conditions, such as fragmented data storage properties, new workload adoption, and the increase in remote work, organizations are tasked with security and managing their ever-growing data estate.

Threat #1

Data Sprawl and Silos

More data in more places introduce new vulnerabilities, especially with an increasingly remote workforce and rapid endpoint device expansion.

Threat #2

Cybercrime Activity

Ransomware attacks and other cybercrime is consistently growing to pace the expansion of technological advances and new tools.

Threat #3

Rapid Tech Advancements

New software applications and hardware platforms are being created and implemented faster than protective solutions can be developed.

THREE ESSENTIALS FOR CYBER SECURITY READINESS

A robust data security and cyber recovery strategy falls within three main categories: securing data, seeing threats sooner, and recovering fast. These three elements are essential in ransomware readiness, and deliver a multi-layered approach that proactively reduces exposure and the risk of an attack, but institutes best practices for effective cyber recovery at scale.

PROTECTION

- **Advanced security.** Effective data protection starts with a strong foundation. Hardened security protocols, such as immutability, advanced data encryption, and zero-trust user access controls prevent unwarranted access to systems and data. Leading solutions can also help prevent data loss by meeting stringent security standards and privacy standards (including ISO27001, GDPR and SOC 2).
- **Detection.** A key aspect of any cyber resilience platform is detection. Advanced AI-insights and early warning systems help spot threats sooner, before damage is done. This helps accelerate response with deep visibility into latent and ongoing threats so your business can anticipate threats, reduce exposure, and minimize potential damage.
- **Proven infrastructure.** Trusted data protection should be backed by cybersecurity experts and industry-leaders, which adhere to global, regional, government and industry compliance standards. This establishes durability and performance as a critical component in the foundation of your backup solutions.

OBSERVABILITY

- **Backup immutability.** While malicious attacks can encrypt business data in production environments, separate and immutable backups maintain a protected data copy that cannot be tampered with, altered, or deleted in the event of a breach. This isolation ensures ransomware that impacts production/system data cannot make the leap to also infect backups—as data backups live in a separate security domain and different format from customer environments.
- **Air-gapped service.** While isolated backups securely store copies of your data from bad actors, it is also imperative that your backup service (itself) remains air-gapped. This is a critical but often overlooked element, as both backup and restore operations should be separate and not susceptible to ransomware attacks that successfully penetrate customer environments.

RECOVERY

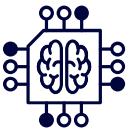
- **High performance.** Your solution should support rapid recovery of data. Features such as built-in deduplication, compression, clean rooms, malware scanning, and bandwidth optimization eliminate redundancies while ensuring data copies are uninfected and highly available for quick and reliable restoration. The fast recovery reduces costly downtime and helps meet recovery SLAs.
- **Speed and precision.** Granular search and flexible recovery options enable faster recovery with precision. A cloud-based control dashboard allows admins to restore their data even if they lose their production environment.

PROVEN CYBER RESILIENCE, FROM COMMVAULT®

Cmmvault Cloud, powered by Metallic AI, delivers the world's most advanced cyber resilience platform for your hybrid data. Now, businesses don't have to sacrifice. Get true data security and recoverability for wherever your data lives - for advanced protection from malicious attack.

SECURITY

All your data, secured everywhere, all in one cloud
No more costly workarounds and patchwork solutions. Commvault Cloud secures all your hybrid workloads—combining the power of the market's most innovative capabilities and unique architecture with cloud simplicity for all your data. This means complete visibility across your data for unified protection and recovery—from any location to any location.



INTELLIGENCE

Advanced AI, enabling next-generation capabilities.
Go beyond the backup to proactively stop ransomware in its tracks. Powered by Metallic AI, Commvault Cloud provides layered defense — minimizing the impact of cyberattacks with early warning and cyber deception, while accelerating recovery with comprehensive threat scanning, remediation, intelligent quarantining, clean recovery validation, and unparalleled recovery speeds.

RECOVERY

Your business, recovered with certainty, at scale
Unlike niche solutions that break down at scale, Commvault Cloud makes the world's fastest recovery predictable. That means your data is always secure and available, wherever it lives, with powerful AI-driven automation to verify clean recovery points, and unparalleled scaling to recover data faster than the competition, at a fraction of the cost.

1 Entrepreneur.Com, article, 349509
2 Pingdom Team, January 2023. "Average Cost of Downtime per Industry"
3 Sophos, 2022, "The State of Ransomware"
4 Steve Morgan, July, 2023, "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031"

To learn more, visit **commvault.com**

© 2023 Commvault. See here for information about our trademarks and patents. 10_23