metallic™
A Commvault Venture

Three Must-Haves for Ransomware Data Protection

Cloud-based Backup Essentials for IT Professionals

Introduction

Ransomware 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, ransomware is here to stay, as evidenced by an increase of 41% compared to last year and surging price tags.[1] It is estimated that all corporations' losses to cybersecurity attacks run at the rate of one million dollars ($1m) 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.

Ransomware is growing in sophistication

Ransomware uses phishing spam and social engineering to access victims' resources. Attackers encrypt and deny access to critical and sensitive data, then demand a monetary payout before returning encrypted data to a usable format.

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.

For comprehensive coverage from today's threats institutions must proactively invest in preventative security 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 cyberattacks expected to reach an attack every 11 seconds in 2021[6]

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 will have paid a collective $20B in ransomware payouts in 2020 alone[7]

Costly downtimes. Business disruptions of any kind are expensive. And in today's digital centric 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 doubled to $283,000 in 2020[8]

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:

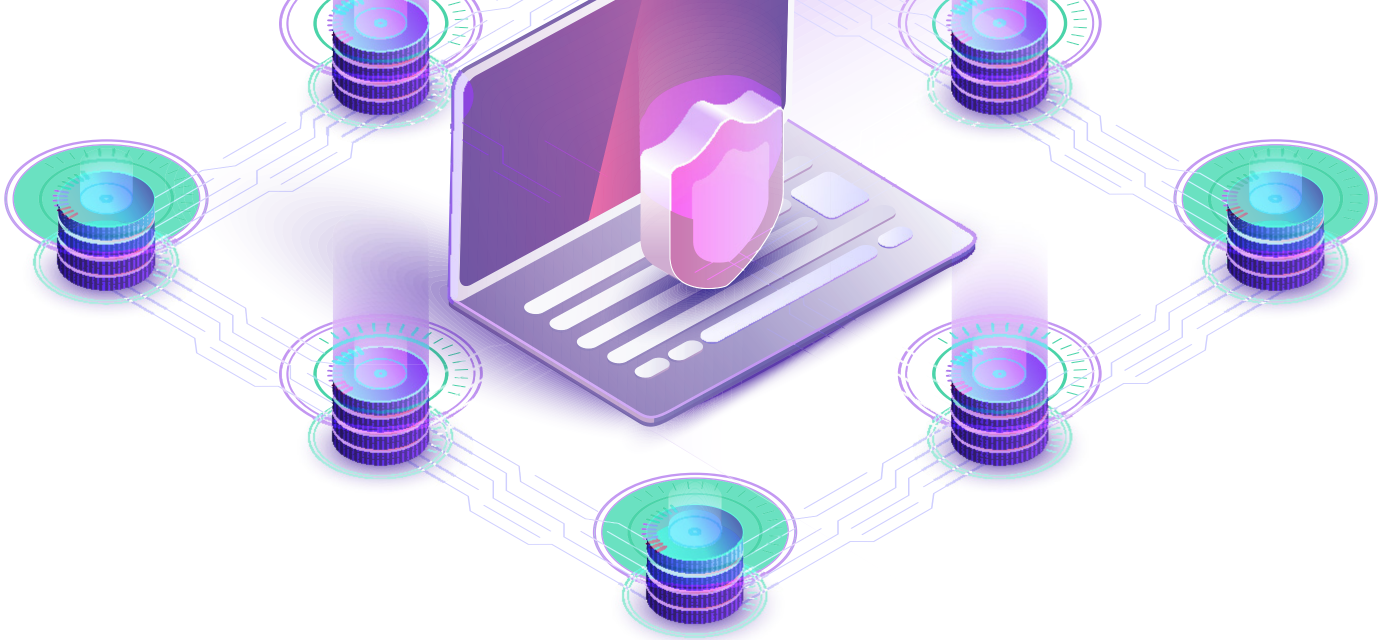
Cybercrime Activity

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 ransomware readiness

A robust security and data protection strategy falls within three main categories: denying unwarranted access to data, maintaining data integrity and enabling rapid recovery after a malicious attack. These three elements are essential in ransomware readiness, and deliver a multi-layered approach that proactively reduces risk of attack, but institutes best practices to effectively recover at scale.

Protection

Advanced security. Effective data protection starts with a strong foundation. Hardened security protocols, such as multifactor authentication, 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. Anomaly detection provides AI-powered capabilities that spot suspicious activity before ransomware can successfully penetrate data. By recognizing anomalies in file patterns, users and administrators are proactively notified of potential threats to production data

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 all establishes durability and performance as a critical component in the foundation of your backup solutions

Preservation

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 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 and bandwidth optimization eliminate redundancies while ensuring data copies are 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 allowing admins to restore their data even if they lose their production environment

Proven data protection, with Metallic

Metallic Backup-as-a-Service (BaaS), from Commvault, offers enterprise-grade data protection, with the simplicity of SaaS. Built on Microsoft Azure, Metallic offers trusted backup and recovery solutions with the durability, security, and scale of Azure. With broad-ranging coverage across apps, endpoints, on-prem and cloud environments, Metallic delivers a proven approach to data security for comprehensive coverage from deletion, corruption and ransomware attack.

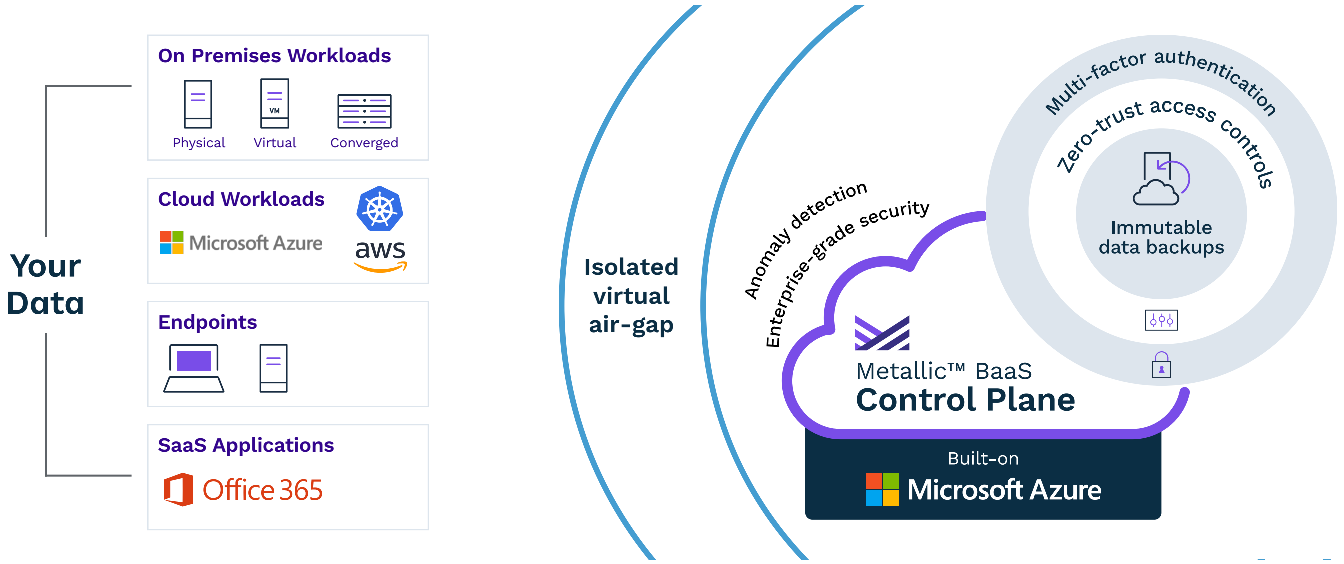
Ransomware protection. Metallic leverages a hardened, multi-layered approach to security. It provides robust controls to both protect and preserve data from external and internal threats, while ensuring data is highly available and recoverable

Hybrid cloud adoption. Hybrid is the new norm. And while there are many paths to the cloud, Metallic BaaS provides breadth of coverage across on-premises and cloud environments, helping secure your data, maximize your investments and adopt new workloads throughout your journey to the cloud

Data compliance. Metallic is purpose-built to keep you compliant and is capable of meeting internal requirements, retention SLAs, and prevailing local, global, regional and government data handling standards

How it works

A new and differentiated approach to Backup as a Service (BaaS)



Check out Metallic with a free trial today

Sources:

1. Entrepreneur.Com/article/349509
2. MarketWatch November 2019. “Microsoft security exec says passwords are bad for the planet.”
3: Thesslstore.Com/blog/ransomware-statistics/
4. EmsiSoft Malware Lab 2029. “State of Ransomware in the US, 2019 Report”
5. IDC June 2020. “IDC 2020 Predictions on Cloud and Edge Computing”
6. Thesslstore.Com/blog/ransomware-statistics
7. herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf
8. purplesec.us/resources/cyber-security-statistics/ransomware/