EBOOK

Amplify Data Security and Recovery on Azure with Zero Trust

Table of Contents

Enhancing Data Security on Microsoft Azure

Organizations worldwide turn to Microsoft 365 to support and empower their employees with industry-leading collaboration and productivity solutions. For this reason, cyber criminals heavily target the valuable, business-critical data being hosted in Microsoft 365 applications. Sophisticated ransomware attacks and other cyberthreats look to disrupt your business and hold data that is often unrecoverable.

Assessing the Increasingly Sophisticated Threat Landscape

As organizations continue to innovate and introduce new technologies to propel their business forward, new risks and opportunities for cyber criminals continue to surface. Additionally, the rise of hybrid and remote work present organizations with new challenges such as providing secure access to sensitive data.

Some ransomware trends currently impacting organizations include:

- **Enterprise Threats:** The number of organizations impacted by ransomware increased to 102% between 2020 and 2021,[1] and global ransomware costs were expected to reach $20 billion in 2021[2].
- **Financial Exposure:** The average ransomware recovery cost was $1.85 million in 2021, more than double the cost in 2020[3].
- **Low Risk for Attackers:** Anonymous cryptocurrency transactions enable extortion of huge ransoms, as there is little chance of getting caught.

Ransomware attacks exponentially increased during the COVID-19 pandemic and are continuously evolving to cripple businesses. Organizations urgently need data security solutions that enable advanced threat detection, rapid recovery, and data protection operating on a zero trust model.

[1] Check Point Research, The New Ransomware Threat: Triple Extortion, May 2022

[2] Cybersecurity Ventures, Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021, October 2019

[3] Dark Reading, Ransomware Recovery Costs Near $2M, April 2021

How Can You Fortify Your Cybersecurity?

Whether you're working in a multi-cloud or hybrid cloud environment, your data needs to be secure, discoverable, and always accessible. Simplifying data backup and recovery enables your workforce to reduce daily management and manual tasks to confidently focus their efforts elsewhere. When ransomware attacks hit your business, the options are limited to paying the ransom and risk affecting your reputation or attempting to recover.

Data storage in immutable archives enables data resiliency that is crucial to accelerating ransomware recovery without suffering high costs. Immutability ensures the integrity of data backups and enables your business to stay protected against even the worst attacks.

This is why Rubrik Zero Trust Data Security™ has combined an immutable filesystem with a zero trust cluster design in which operations can only be performed through authenticated APIs.

Maximize Your Data Security with Zero Trust

As ransomware attacks continue to threaten organizations worldwide, and across industries, IT teams are turning more to Zero Trust Security models. Applying a Zero Trust Security approach to Microsoft Azure provides an added layer of protection with the methodology that assumes risk from every device, user, and application.

The expansive landscape of cyber threats, including ransomware, can impact any business. Phishing attacks are a common method for cyber criminals to gain credentials and infiltrate privileged systems that can impact your recoverability from a ransomware attack.

71% of Microsoft 365 deployments have suffered an account takeover on average seven times in the past year.[4]

However, a Zero Trust Security approach requires additional user verification steps that reinforce your cybersecurity posture and protection of valuable company data. Ensure your data is always available, immutable, and locally air-gapped with permissions and access that are strictly enforced to maximize your data security.

[4] Guardian Digital, Microsoft 365 Account Takeover: How to Defend Your Deployment, November 2022

Strategically Approach Data Protection and Recovery with Rubrik

Our extensive experience with helping customers combat ransomware alongside our long-standing relationship with Microsoft has made us a first-choice partner for ransomware remediation. In fact, we're so confident in our solution that we've backed our technology with a first-in-the-industry ransomware recovery warranty of up to $5 million for Rubrik Enterprise and Cloud Vault.

Additionally, integrations with the Microsoft 365 suite, including Azure Sentinel, give customers comprehensive coverage and the confidence of knowing their data is protected from even the worst ransomware attacks. Our integration with Microsoft Sentinel allows organizations to conduct deeper and faster investigations, prevent malware reinfection, and quickly recover from ransomware. You can reduce the vulnerabilities and gaps in your data security with Rubrik to enable enhanced data protection on Microsoft Azure.

However, these words hold little weight without hearing directly from our customers about the benefits realized by their organization.

Helping the Colchester Institute Avoid a Crippling Security Breach

Education institutes have been the highest targeted vertical of ransomware attacks as they're hosts to vast amounts of research data, PII, and more. In 2021, the Colchester Institute became a part of this statistic, finding that all admin accounts had been disabled.

Although a ransomware attack such as this would be detrimental to most, Rubrik worked in partnership with KHIPU Networks to help Colchester instantly recover with zero data loss. With just one click, Colchester was able to return to the most recent clean copy to avoid a crippling security breach.

> **"Rubrik safeguarded our backups. Due to it's native immutability, 100% of our backups were protected against corruption and deletion."**
>
> – Ben Williams, IT Services Manager, Colchester Institute

Additionally, Colchester was able to analyze the impact of the attack and identify anomalies as well as determine exactly which files were affected. With first-hand experience of a ransomware attack, Colchester has now encouraged other institutions to reevaluate their disaster recovery solution and consider upgrading to Rubrik.

Enhancing Plymouth’s Ransomware Disaster Recovery

Plymouth, like many organizations, had security measures to prevent cyberattacks such as endpoint protection, email security, and more. However, without a comprehensive disaster recovery plan Plymouth left a critical gap in their cybersecurity. A ransomware attack exposed this gap and left their IT team scrambling to restore affected systems.

Backed by our native immutability and ransomware recovery, Plymouth was able to recover over 50 servers within 48 hours. Working alongside the Rubrik IT team, Plymouth was able to develop a full recovery plan and minimize their damage with $0 paid in ransom.

> **“The Rubrik Ransomware Recovery Warranty offers us a new level of protection and sense of stability that goes beyond traditional means of data security found in the industry.”**
>
> – Rama Arumugam, IT Manager, Plymouth Inc.

Working with Plymouth throughout the entire process, Rubrik ensured a best-in-class recovery to keep their business running smoothly with confidence.

Get Started with Rubrik on Azure Marketplace

Rubrik offers preferred Microsoft solutions meaning you can decrement your Microsoft Azure Consumption Commitment while protecting your most valuable data on Azure.

View Rubrik on Azure Marketplace

rubrik

Zero Trust Data Security™