Executive Brief: Cloud Daddy Secure Backup

Modern Data Protection Requires a Holistic Approach

CONTENTS

INTRODUCTION

For the last half century, backup and disaster recovery planning has largely involved contingency planning for coping with physical disasters. Such disasters may include anything from a fire to a hurricane. As varied as physical disasters may be, they're all similar in that they pose a direct threat to the physical data center. This is an important distinction, because the focus on physical disaster has shaped disaster recovery planning for decades.

More recently however, the threat landscape has shifted away from physical disasters to man-made cyber disasters. Although the potential for physical disaster can never be completely eliminated, IT professionals realize that their organizations are far more likely to suffer data loss as the result of a ransomware attack than because of a physical disaster such as a fire.

Ransomware is serious business. It has the potential to cause loss of life. The notorious WannaCry infection crippled hospitals and medical facilities across Europe, preventing at least some patients from receiving emergency medical care.

The Exploding Ransomware Threat

In recent years, ransomware attacks have caused significant financial loss, data loss, and possibly even loss of life. Recently, the huge medical company LabCorp was seriously impacted by ransomware, https://bit.ly/2mtccLe, potentially exposing health records, patient data, and other personal information. These attacks naturally raise the question of why ransomware has been so effective. After all, organizations around the world collectively spent an estimated $7.13 billion on backup and recovery products and services in 2017, and yet remain seemingly ill-equipped to handle a ransomware infection. This phenomenon needs to change because cybercrime is projected to cost the world $6 trillion annually by 2021 – up from $3 trillion in 2015.

One factor that makes it so difficult for organizations to recover from a ransomware attack is reliance on legacy backup technology. For decades, data backup solutions focused solely on protecting on-premises resources. Although most current data protection solutions do offer cloud capabilities, the cloud protective features are commonly "bolted on" to a legacy product. In doing so, the protection of cloud resources may be treated as an afterthought. Consequently, such a tool's ability to protect cloud resources may be inferior to its ability to protect resources residing on-premises.

Today it's common for organizations to take a cloud first (or cloud only) approach to deploying new workloads. It therefore stands to reason that the only way to protect these modern cloud workloads against threats such as ransomware is to use a backup solution specifically designed to protect cloud resources.

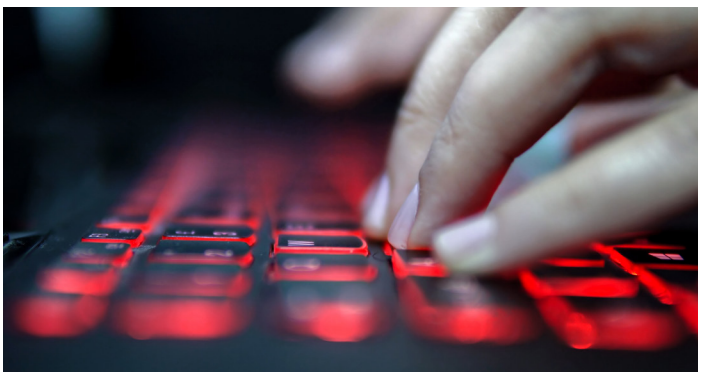
> The threat landscape has shifted away from physical disasters to man-made cyber disasters

One of the main reasons ransomware has been so damaging is that backup and disaster recovery systems have often been engineered around the idea of protecting critical systems against natural disasters, rather than man-made ones.

A typical disaster recovery plan is based on the idea that an organization's primary data center could become incapacitated as the result of a disaster, and operations would therefore need to be transitioned to a secondary data center or perhaps a public cloud operating in a different region. In order to achieve this objective, data is replicated to the standby facility on an ongoing basis.

This approach works really well for ensuring the organization's ability to remain online after a natural disaster. The ongoing synchronization process ensures that at most, only a few minutes' worth of data will be lost. The problem, however, is that the same synchronization engine that protects data from a natural disaster can also propagate the damage caused by a ransomware infection.

When ransomware encrypts data, the system that's being attacked is blissfully unaware that the action is malicious. The encryption process is interpreted as normal modification of the data. Because the disaster recovery system is designed to protect any newly-created or recently-modified data, the now-encrypted files are synchronized to the cloud or to the backup data center, which means that the secondary copy of the data becomes encrypted too.



It remains undeniably important to replicate workloads to other regions. However, replication alone is inadequate. If an organization is to protect against ransomware, it needs a way of rolling its systems back to an earlier point in time.

Most IT pros understand the importance of disaster recovery testing. Without proper testing, an organization has no way of knowing for sure whether or not its disaster recovery plan will work in times of crisis. The problem is that recovery tests are commonly limited in scope. An organization may, for example, test its ability to fail over to another region, but neglect to test its ability to roll its systems back to an earlier point in time. As such, the organization's ability to recover from a ransomware attack remains unknown.

> Modern cyber disasters such as large-scale ransomware attacks have clearly demonstrated that backup, security, and infrastructure management capabilities are most effective when intertwined with one another

In addition, backup, security, and infrastructure management have always been historically siloed. When they don't work together, it's easy for things to be missed, due to the greater complexity silos introduce to an infrastructure. This is ineffective in today's world, where modern cyber disasters such as large-scale ransomware attacks have clearly demonstrated that backup, security, and infrastructure management capabilities are most effective when fully integrated with one another. Consider that a ransomware attack is at its core a security incident – and while a restore operation may be necessary, security measures are also required to keep the attack from spreading throughout the organization's infrastructure.

Modern Data Protection Requires a Holistic Approach

IT pros today commonly have two primary goals – to keep the organization secure, and to provide the kind of agility that can support the organization's digital 3 transformation efforts. The thing that both of these goals have in common is that they're all-encompassing. An IT pro can't simply purchase a security product and consider the organization secure. Security must be implemented at every layer of the organization.

The same thing holds true for agility. While the cloud has given organizations unprecedented elasticity, true agility can only be achieved if the supporting infrastructure can take advantage of that elasticity. This is why it's so important to tightly integrate security and infrastructure management capabilities into an organization's data protection efforts.

> While the cloud has given organizations unprecedented elasticity, true agility can only be achieved if the supporting infrastructure can take advantage of that elasticity

Agility, Security, Protection

Cloud Daddy leverages the AWS Infrastructure to give you just that: agility, security and protection for today's environment, serving modern applications and keeping companies safe from the scourge of ransomware and other threats.

Take your data protection to the next level with the world's most secure backup/disaster recovery incorporating AI alerting, mal/ransomware detection and more into one interface.