RANSOMWARE PROTECTION

5 Top Ways
Scale Computing
Has You Covered

SCALE COMPUTING

"When people learn that an organization paid millions to resolve a ransomware issue, they assume that fixing it cost the company just the ransom. We found that ransoms alone account for less than 20% of the cost of a ransomware attack."

Larry Ponemon
Chairman and Founder of Ponemon Institute

Introduction

There are both pros and cons to the speed at which technology moves. While it provides increased employee productivity and fewer barriers to new business opportunities, the ever-increasing complexity of modern IT environments means safeguarding business-critical data becomes equally tricky.

Today, ransomware is one of the biggest cybersecurity threats impacting business and personal data. The volume of attacks is significant and may take various forms, presenting a unique set of challenges to IT staff tasked with defending against them. Understanding what data is at risk during a ransomware attack is the first and most critical step to preventing a large-scale disruption.

Businesses and their IT departments need easy, secure tools to get the most out of their data while keeping it safe as data volumes, infrastructure, and online threats continue to grow.

How can Scale Computing help? **Let's take a look.**

1 Clean, reliable backup

You may be able to restore your system without paying the ransom if you have a clean, reliable copy of your data. This has been an immensely effective strategy in the past. Still, the landscape has dramatically changed, as new ransomware strains specifically target backup agents, software, and files to deny users access to them.

Attackers increasingly use endpoints to enter primary environments and access backups before compromising production environments. Creating a multi-layered defense is necessary to protect your backups from ransomware attacks. And, access to backups must be simple, quick, and easy.

84% of enterprise data is now stored in the cloud.[1]

HOW SCALE COMPUTING HAS YOU COVERED

The concept of backup has evolved over the decades. Scale Computing integrates with third-party backup vendors you already know and trust to deliver different levels of unique storage subsystems (ie. Host-level and guest-level backups). You do not need to install an agent on guest VMs in order to perform host-level backups. Adding the virtual host to the Scale Computing appliance is as simple as selecting VMs to be protected.

The days of making traditional full and incremental backups should be over, with scheduling capabilities that are flexible enough to implement almost any backup strategy.

2 Immutable snapshots

Legacy backups are no longer sufficient. Enter snapshots. As the name implies, snapshots provide a quick "picture" of a server (including its files, software and settings) at a particular point in time. Generally, snapshots are instant and preserve a point-in-time state without moving or copying existing data at all. For this reason, most modern backup approaches go hand-in-hand with snapshot technology to provide a stable, unchanging point-in-time image with which to do a backup.

Immutable snapshots change your posture against ransomware and malware because they are fundamentally resistant to attacks. Instead of defending or protecting, they reduce the impact and spread of an attack by not being affected by it in the first place. Like the "write once read many" (WORM) method of data storage in which information, once written, cannot be modified.

HOW SCALE COMPUTING HAS YOU COVERED

Scale Computing's protects every virtual workload with snapshots so that you can recover in minutes in case of a ransomware attack. If you're hit by ransomware, you can simply revert to a previous snapshot and carry on.

Scale Computing's snapshots are immutable. This means they cannot be altered or deleted by their VM in any way. Full stop. Snapshot immutability means an admin can quickly respond to a ransomware attack by cloning a previous snapshot - taken before the malicious executable was deployed - create a new VM from that snapshot, and power it on. Cloning only takes a few seconds, which means recovery is incredibly rapid.

3 Replication

Virtualization can offer seamless replication, but many organizations don't properly back up their virtual machines. According to a Veeam survey, 68% of organizations needed to fully recover an application or VM due to an outage in the past year, but nearly half of the organizations protect less than half of their VMs with a recovery plan, and almost a quarter of them back up less than half of their virtual environment each day.

Some replication technologies may be susceptible to man-in-the-middle (MIM) cyberattacks. In cyber defense, multi-tiering your replication procedures is an excellent idea: built-in, encrypted at the cluster level, but also covered through third-party integrations where this is done simultaneously.

HOW SCALE COMPUTING HAS YOU COVERED

All Scale Computing software systems include a free, built-in feature for system-to-system replication at the per-VM level. System-to-system replication is designed to run continuously and transmit changes to a secondary system as quickly as possible, using the snapshot functionality as the base for VM changes.

Replication follows the snapshot schedule assigned to a VM and can replicate snapshots as often as every 5 minutes for solid recovery objectives.

4 Hyperconverged Infrastructure (HCI)

Hyperconvergence is an innovative way to simplify your IT operations and is more effective at protecting data than traditional systems. HCI pools resources into an infrastructure that can be managed with cloud-like ease for the entire stack (hypervisor, storage, etc.). Virtualization software turns many high-performing processors into multiple virtual machines with their own virtual processors, thus allowing each OS to run its own set of programs independent of other OS running on other processors.

A properly architected HCI solution radically reduces the attack surface by doing things like eliminating storage protocols, and not simply virtualizing SANs. Storage protocol-based attacks simply won't work with HCI infrastructure.

HOW SCALE COMPUTING HAS YOU COVERED

Some hyperconverged architectures, like Scale Computing, already withstand attacks simply because they eliminate legacy attack surfaces used by malware and ransomware bad actors. Scale Computing's true HCI integrates bare metal at all layers, such as the compute storage, virtualization, management layers, and data protection features, instead of traditional systems that combine these components from different vendors using open network protocols.

5 Security through integration

A patchwork of security tools also makes managing security more challenging and less effective. Data protection and cybersecurity must be combined to protect data, systems, and applications from the risk of cyberattacks.

Providing continuous measurement and protection for recoverability requires integrated tools to deliver active protection, anomaly detection, immutable storage, air-gapping, and multifactor authentication controls. The objective is to expose and remedy problems, validate the recoverability of the data and business applications, and improve security to reduce business risk with seamless protection.

And a security solution is only viable if it is resilient.

Ransomware annually costs large organizations $5.66 million. Of that, $790,000 accounts for the paid ransoms themselves.[2]

HOW SCALE COMPUTING HAS YOU COVERED

Avoid permanent loss of data by decreasing the attack surface.

Scale Computing is unmatched in architectural flexibility and native backup and recovery to avoid data loss. It integrates with leading advanced backup and proactive ransomware third-party software vendors, like Acronis, to take data protection to any level customers may need.

By tightly integrating its own data protection technology with that of Acronis to actively detect ransomware as it is deployed, Scale Computing is able to eliminate protection gaps and enable seamless remediation. There's no need to juggle multiple solutions.

Conclusion

It's impossible for an organization to completely prevent a ransomware attack. But, organizations can mitigate the most negative effects of a ransomware attack by improving their storage and data recovery systems in advance.

Ransomware can sit dormant for weeks, if not months. We get constant feedback from our customers that they sleep easier knowing Scale Computing's software and hardware solutions have native ransomware protection because we do things differently.

Customers around the world that have had ransomware attacks have been back up in minutes without having to pay a penny! They did not have to wait days or weeks to recover and get their business back up. Choosing Scale Computing and the data protection options it natively provides ensures your cyber defenses are working smarter, not harder.

If business continuity and ransomware protection are important to you, let's schedule a meeting to show you how simple and affordable it can be with Scale Computing.

"We had a bad ransomware event hit a client on a weekend. Because we had a Scale Computing cluster with an offsite replication server, we were able to roll back the servers to 1 hour before the ransomware event and get the server back to functional (along with plugging the opening that let the ransomware in and changing all the account access logins and passwords). So glad we had a Scale Computing cluster!"

Terecia Burgess
Q&S Solutions ("Terecia5538" via Spiceworks)

Sources:

[1] Cohesity, 5 Ways Ransomware Renders Backup Useless, January 2022

[2] Ponemon Institute, Cost of Phishing Study, August 2021

SCALE COMPUTING

CORPORATE HEADQUARTERS

525 S. Meridian Street - 3E // Indianapolis, IN 46225

P. +1 317-856-9959 // **scalecomputing.com**