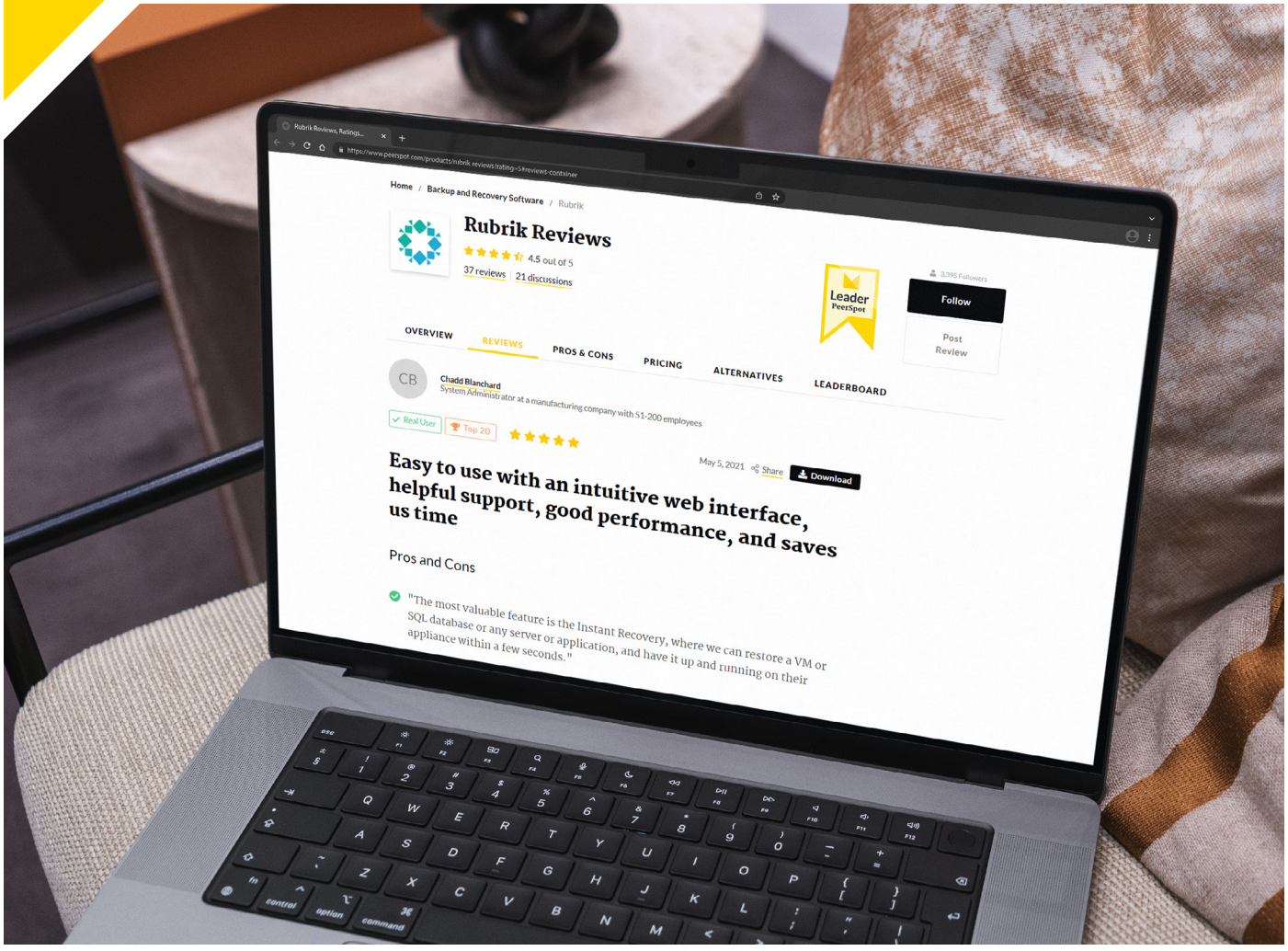
PeerPaper™ Report 2022

Based on real user reviews of Rubrik on PeerSpot

Top 10 "Must Haves" for Zero Trust Data Protection



PeerSpot

Contents

Introduction

The ongoing ransomware crisis is revealing deficiencies in legacy backup and recovery solutions when it comes to protecting data across the data center, public cloud, and SaaS applications. IT departments are turning to the Zero Trust model to protect data and ensure operational continuity. What goes into a backup and recovery solution that supports a Zero Trust security strategy? According to real users, who write about their experiences with Rubrik on PeerSpot, when selecting a modern backup and recovery solution one should look for 10 "must have" factors, including an "air gap," ransomware mitigation capabilities, immutability, scalability, and automation that span across on-premises and the cloud. The new solution must save time and money. Ease of use and ease of admin also count.

Except where noted, all the companies described in this paper have over 500 employees.

The Top 10 "Must Haves" for Zero Trust Data Protection

#1 - Air Gap
#2 - Ransomware Mitigation
#3 - Immutability
#4 - Ease of Use and Configuration
#5 - Cloud and Hybrid Cloud Capabilities
#6 - Automation
#7 - Scalability and Reliability
#8 - Speed of Recovery
#9 - Cost and Time Savings/Return on Investment (ROI)
#10 - Quality of Support and Service

The Evolution of Backup and Recovery

Backup and recovery operations date back to the very first uses of magnetic storage media in computing. The process used to involve the storing of wagon wheel-sized reels of tape in salt mines. Though the process grew more elegant as systems got increasingly sophisticated and storage media shrank, the basic "make a copy and store it somewhere safe" methodology remained essentially unchanged until the advent of widespread cloud adoption, starting about 10 years ago. Until then, most backup and restore solutions copied data onto dedicated physical solutions that were on-premises or in third-party hosting facilities.

The ransomware crisis, coupled with the increased complexity of cloud architectures, have put unsustainable pressure on legacy backup and restore solutions. Figure 1 offers a comparison of simplified reference architectures to show how things changed with the advent of multi-cloud, the edge and Software-as-a-Service (SaaS) solutions. While these new approaches to enterprise architecture enabled a more flexible and scalable backup option, they also opened up more vulnerabilities.

Very easy to configure

A ransomware attack can encrypt data in far-flung cloud-hosted assets and paralyze an organization in ways that were not previously possible. The Zero Trust approach to security, applied to backup and restore, mitigates this risk. By reducing the likelihood of unauthorized access to backed up data, the Zero Trust approach does a better job of protecting data than legacy backup and restore solutions.

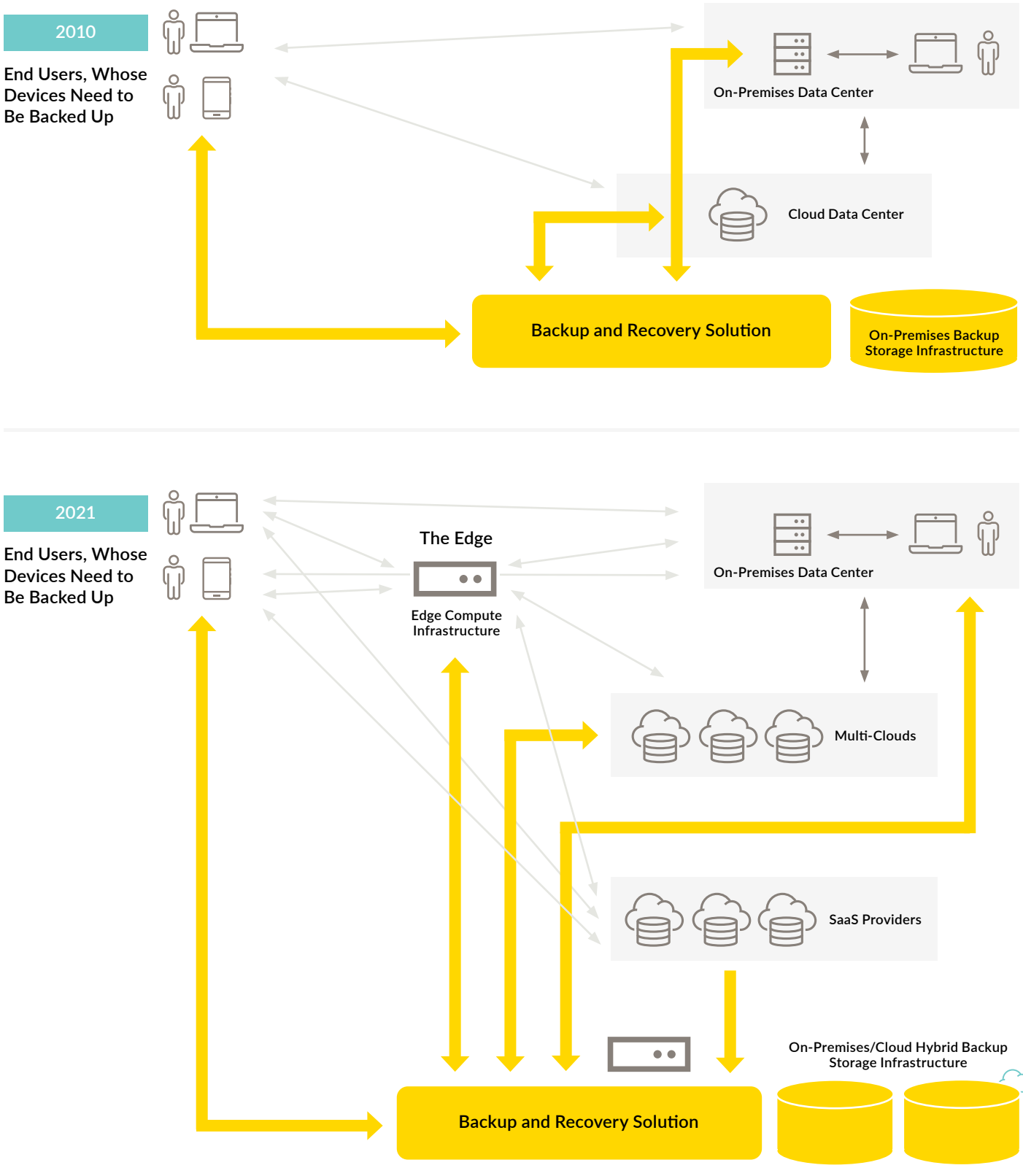


Figure 1 - The evolution of the modern enterprise toward hybrid clouds, the edge and SaaS, which complicate backup and recovery

Why Organizations Are Switching From Legacy Solutions

Ransomware has emerged as the most serious cyberthreat facing businesses and government agencies today. In the face of this onslaught, legacy backup solutions are proving to be deficient at protecting data. Ransomware response requires rapid data access and better backup security than legacy solutions were built for.

As a result of these conditions, backup managers are looking to move off of legacy solution. For example, an Assistant Vice President at a financial services firm remarked, “In our old system it took quite a bit of time, with indexing the files and trying to do a search.”

A Senior Systems Engineer at a university also shared, “We decided to switch because our system was way out of date, and in terms of performance, our backups were taking so long that we couldn’t actually complete them. The restore time was abysmal. It took days to restore if we needed a large chunk of data. The maintenance of it, in terms of the human capital, was intense. As I said, I was using at least 50 percent of my time per week just trying to make sure that the backups completed.”

Integration and platform-specific problems were also issues, as a Senior Systems Manager at a construction company found. Before Rubrik, his organization had used a competing product that they could not tie into VMware. This product's snapshot technology "was a continual failure," as he described. Even with the support of the vendor, they could not get it working without it causing infrastructure issues to their VMs.

Cost was a factor as well, with an IT Manager at a manufacturing company deciding to move off of his legacy solution, because, as he put it, "We realized simply upgrading it would have cost us quite a bit of money. The old solution we had was using a tape library to back up the data and it took too long to back up all the data on the tape." A Systems Architect at Cardtronics, a financial services firm, similarly switched from Commvault because of the cost of ownership. This user also had a negative support experience with the vendor—a factor that comes up in recommendations for selecting a modern backup solution.

Extremely efficient

The Top 10 "Must Haves" for a Zero Trust Based Backup and Recovery Solution

A Zero Trust focused backup and recovery solution for ransomware mitigation should offer the following "must have" characteristics:

#1 – Air Gap

For years, the allegedly best way to ensure data protection was to place digital assets in physically isolated systems. The so-called "air gap" meant that an attacker could not possibly access the data in question. The rise of cloud computing and pervasive internet connections has made the concept of physical air gap a lot harder to implement. Even when IT managers think they have an air gap in their infrastructure, they may be surprised to find a previously unknown external connection to their data.

A "logical air gap" is an alternative realization of this idea. Achieved through layers of protection and cryptographic techniques, a logical air gap like the one offered by Rubrik balances the right level of data isolation with rapid data access, offering faster recovery than a physical air gap like tape. The construction company Senior Systems Manager Employees spoke to this capability when he said, "We wanted to get to a state where our backups were protected against ransomware via immutability or air gapped backups, which we've now accomplished with Rubrik." They run a virtualized VMware environment.

> **"We wanted to get to a state where our backups were protected against ransomware via immutability or air gapped backups, which we've now accomplished with Rubrik."**
>
> Read review »

> "They were one of the first companies that offered proper ransomware recovery."
>
> Read review »

#2 – Ransomware Mitigation

Ransomware mitigation countermeasures are critical in backup and restore solutions. PeerSpot members discussed this in their reviews of Rubrik. A Systems Architect at a tech services company, for example, remarked, "A primary use case and where Rubrik was ahead of the pack, was ransomware attacks. They were one of the first companies that offered proper ransomware recovery."

"The feature that I have found most valuable from Rubrik is its protection against ransomware attacks," said a Technical Sales Engineer at a small tech services company. He added, "It is able to protect your data and you have the possibility from the backup to detect any abnormal behavior, like a ransomware attack."

A Head of Operations at the University of Reading similarly appreciated Rubrik's ransomware detection capabilities. He said that Rubrik "looks for anomalies in our backups and will trigger an alert if it sees something that is an abnormal amount of change." For instance, "That could be lots of deletes or modifications, compared to normal. Or it could be some VMs that have suddenly had a lot of folders added or deleted. It can detect when someone has gone in and deleted a substantial amount of data on a VM. If that's abnormal it will flag it and say, 'Well, you might want to investigate this."

#3 – Immutability

Vulnerability of data makes it advantageous to have a back-up that cannot be changed under any circumstances—a completely immutable backup, in other words. "The back-ups are immutable, and nobody can change them," said a Senior System Engineer at Thomas Jefferson University Hospital, a healthcare company. "You can't override them. You can't change anything in the backups once the snap-shot is taken. Our backup retention is 120 days. So, for 120 days, nobody can change that. When I take a snapshot of a server, if the next day we get hit with ransomware, I could shut that down. I can then just stand one up from the back-up that I took yesterday. They can't change anything that is already in the backup."

A System Administrator at a manufacturing company with more than 50 employees simply stated, "If you want peace of mind at night, immutable backups, cloud-native support, cloud DR support, all within a single solution with world-class technical support, Rubrik is the way to go." For a Director of Technology at a financial services firm with more than 200 employees, the immutability of Rubrik backups was part of their ransomware mitigation strategy. As he said, "We have not needed to use the ransomware recovery function but I know that Rubrik backups are essentially immutable. Even if an intrusion does happen, we'll be able to restore the data quickly."

A Software Administrator at a university offered a comparable perspective when he said, "We haven't had to recover from ransomware. However, in every test that we have done, we have been very happy with how it works and the concept of immutable backups. Once the data is backed up, it can't be changed."

> "It's just fantastic and intuitive. It's so easy to use."
>
> **Read review »**

"Rubrik's archival functionality is a no-brainer"

Read review »

#4 – Ease of Use and Configuration

A backup and recovery solution has to be easy to use. An insurance company Senior Network System Engineer put the matter in context when he said, "Rubrik's archival functionality is a no-brainer. It doesn't require a ton of thought. I don't have to over-engineer different policies to validate what I think it's doing. If it says it's doing it, it's doing it, and it's really easy to click a button and say, 'Now it's done.'" The Systems Architect at Cardtronics stated, "The ease of use is the most valuable feature. It is a very simple system compared to just about any other back up technology like Commvault or EMC Avamar." An IT Infrastructure Engineer at Shakespeare Martineau, a legal firm echoed this sentiment, saying, "It's just fantastic and intuitive. It's so easy to use."

Enabling people to manage their own backups is a natural, valuable aspect of ease of use. For example, the university Senior Systems Engineer leveraged Rubrik's multi-tenancy feature to allow another team within his organization to manage their own backups and only see their servers. He said, "They are able to only touch and change stuff for their own systems. In theory, that also gives them the ability to do their own restarts if they ever need to. Our previous system had really no way to handle that, so it's been pretty fantastic."

Regarding configuration, Shakespeare Martineau's IT Infrastructure Engineer characterized Rubrik as "very easy to configure" regarding its [VMware] vCenter connections. The financial services Assistant Vice President similarly noted, "The initial setup was really straightforward. From start to finish, from unboxing the product to setting it up, took us about half-a-day, through to getting our first full backup completed. The deployment itself only took about two hours and then, within three to four hours, we already had the first full backup."

"The initial setup was very straightforward. It was the easiest setup that we had on all of the systems that we had looked at before we bought them," said the university Senior Systems Engineer. "When we moved from our PoC to production, we actually handled the setup of the second brick when it came in. We didn't even need to engage their field engineers to help us. The deployment took about four hours."

Ease of management was what mattered to the insurance company Senior Network System Engineer. He said, "It takes the load off of vSphere or vCenter or any of our ESXi hosts. It makes things just a dream to manage." He further commented, "The design, from a user-experience standpoint, is really straightforward and easy to use."

"The design, from a user-experience standpoint, is really straightforward and easy to use."

Read review »

#5 – Cloud and Hybrid Cloud Capabilities

Enterprises that leverage the cloud need backup and recovery solutions that are aligned with cloud computing architectures. And, because almost every organization that operates in the cloud also has some on-premises infrastructure as well, a backup solution that works in a hybrid mode is also very useful.

This was the view of the financial services Assistant Vice President, who acknowledged that Rubrik offered a deployment model that is hybrid, where, as he said, "We have the solution on-prem, plus we back up to the cloud, on AWS." The construction company Senior Systems Manager added, "Due to Rubrik's ability to execute in protecting our on-premises assets in the data center, we decided to utilize Rubrik's Office 365 and AWS Cloud Native solution to protect our data in the cloud."

#6 – Automation

Automation is critical to backup and recovery success a modern enterprise confronting ransomware attackers. Automating backup and restore processes enables fast incident response and ensures that organizations stay protected. Relying on manual processes is not efficient, and it exposes the process to human error. The financial services Assistant Vice President spoke to these issues when he described Rubrik's automation capabilities. He said, "In general, day-to-day, it's made the administration of backups way easier. We went from having management of the backup system as full-time role for somebody to now being a role where we basically just look at the reports and make sure that everything is running correctly and smoothly. We don't have to constantly log in to the system and rerun jobs."

This user also shared about the importance of Service Level Agreement (SLA)-based policy automation as a criterion for selecting a modern backup and recovery solution. He said, "The SLA-based policy automation has made my life a lot easier because, on the administration side, things are way easier to manage. They're not as convoluted as other systems. Once I add a virtual machine to one of the SLA policies, it does its own thing and, at the end of the day, it's backing up stuff correctly. There's very little day-to-day maintenance that I have to do as an administrator."

"The SLA-based policy has had a positive effect on our data protection operations," said the university Senior Systems Engineer. "I'm going to be going even deeper into the automation part. It's going to be great to be able to just tag a machine in Virtual Center and its backups will be taken care of. That will help our process in terms of protecting machines that need to be protected and it will remove a step that people don't necessarily remember to do."

> **"In general, day-to-day, it's made the administration of backups way easier"**
>
> Read review »

> **"Rubrik has absolutely reduced the time we spend on recovery testing by about 75 percent."**
>
> Read review »

SLA-based policy automation streamlined data protection operations for the construction company Senior Systems Manager. He observed, "We have moved away from back-up windows and moved to letting the SLA policy actually determine when is the most efficient time to do backups. We apply the SLA based on business rules to certain artifacts or entities within our environment and let Rubrik run with it. It has been extremely efficient and has cut down on the operational overhead of managing backups."

Automation saves time or the equivalent by improving productivity. To this point, the university Senior Systems Engineer said, "Since I'm not spending as much time dealing with the backups or doing any sort of recovery, we have been able to actually work on other projects and other needs of the organization."

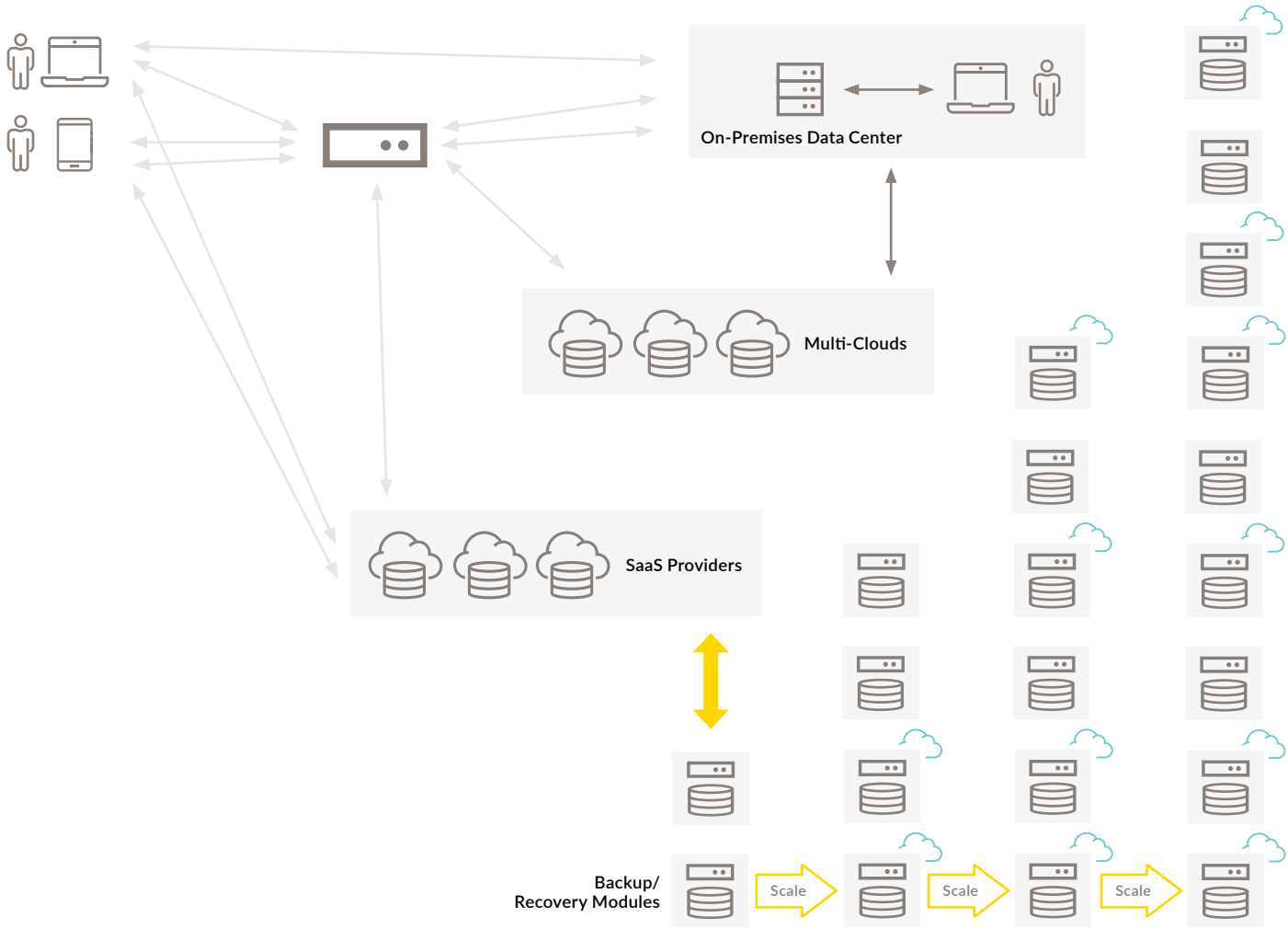
"Overall it has greatly reduced the time it takes to manage backups, again by 50 to 75 percent," said the financial services Assistant Vice President. "In terms of reducing downtime, I haven't really had to deal with any major crises, but for restores, it has also improved that tremendously, by 50 percent at least."

The Systems Architect at Cardtronics offered an example, saying, "With Live Mount I can instantly spin up a server for backup in less than two minutes. It takes 10 minutes to backup and it also takes under a few minutes to recover. With Avamar, these would take an hour or more." Shakespeare Martineau's IT Infrastructure Engineer simply stated, "Rubrik has absolutely reduced the time we spend on recovery testing by about 75 percent."

#7 – Scalability and Reliability

The data volumes covered by backup and recovery solutions seldom get smaller over time. Indeed, growth—often extremely rapid growth—is the norm. As a result, backup managers want solutions that can scale easily. The insurance company Senior Network System Engineer felt that a backup and recovery solution should have technical scalability, meaning it is consistent and stable and being able to improve and evolve. He added that scalability in backup and recovery "should allow your business to be driven in whatever direction it needs to go. It should be something that just works, and so far I've seen it just works."

Figure 2 - How an appliance-based modular architecture facilitates backup scalability.



Cut down on operational overhead

For the construction company Senior Systems Manager, value came from "the ability to just attach additional bricks [now called "appliances" by Rubrik] to scale-out capacity." Figure 2 shows this appliance-based modular architecture approach to facilitating backup scalability. The university Senior Systems Engineer said, "[Rubrik's] scalability is pretty simple. We had initially started off with our two Rubrik appliances in a replication pair, and then we needed to bring that replicated pair into the main system. I worked with support, decommissioned the replication target, got that brick reset, and then brought it into the cluster. That took just a couple hours, but that included the fact that I had to physically move the box. But it was extremely simple and, once it was in, it operated just as you would have expected."

Everyone in an organization is counting on the backup and recovery solution, even if they have no specific awareness of it. They'll definitely know if it doesn't work when they need it. Backup and recovery must be reliable. In this vein, the construction company Senior Systems Manager acknowledged that "the stability of the Rubrik solution has been extremely solid." He added, "In the two years we've owned the solution, we've had no downtime because of hardware or software failures."

The insurance company Senior Network System Engineer also found that "Rubrik is incredibly stable." He added, "I'm getting out of that mode of thinking with Rubrik, 'Well, maybe it won't work this time. Maybe it'll be down.' It's never been down, it's never been inaccessible. If I can't connect to it, I'm typing the URL wrong. That's it."

#8 – Speed of Recovery

PeerSpot members shared that fast recovery is a critical feature in a solution suited to ransomware response. This has long been a factor in selecting a solution. However, as experience with legacy systems has shown, not all back-up and recovery solutions can keep up with expectations. In this context, Shakespeare Martineau's IT Infrastructure Engineer observed that Rubrik's most valuable feature is the speedy restore. He said, "It helps in expediting RPOs and RTOs across our core applications."

For the university Senior Systems Engineer, the requirement emerged most significantly as the ability to return to production. He said, "While having your data is important, having the ability to return to production, within minutes of an issue - which means standing up the whole VM at a point in time - is way more important in today's world than it is to just have a copy of your data."

Greatly reduced the time it takes to manage backups

Other users shared quantitative measures of success in fast data recovery:

- "It's in the Exchange and database stuff that we've really noticed the difference. It's so much easier for the guys in support to recover single files, so the reduction in recovery time is as much as 85 to 90 percent." - Infrastructure Engineer at Shakespeare Martineau
- "We've had phone calls where they say, 'Hey, I need XYZ restored, or I need this entire drive restored, or I need this entire VM restored.' At the click of a button, five seconds later, it's back. It took longer for them to tell me what they needed back than it did to get it returned." - Senior Network System Engineer at an insurance company
- "It can recover the entire VMO database within five seconds."- CTO at a small tech services company
- "I was able to recover three machines in 15 minutes versus nine hours." - Systems Architect at Cardtronics

#9 – Cost and Time Savings and Return on Investment (ROI)

IT departments face relentless cost cutting pressure, and backup is seldom spared from such measures. IT executives thus prefer systems that contribute to greater economies in the department. As the construction company Senior Systems Manager said, "We're seeing about a 62 percent TCO [Total cost of Ownership] savings and 90 percent management time savings since switching to this solution. And we've reduced the data center footprint, which comes with operational overhead, by 75 percent since switching from Tivoli."

The university Senior Systems Engineer concurred, saying, "It does all of its processing of the deduplication and compression before it sends it off to the archive, which helps with our cloud costs. Before, we weren't doing anything to the public clouds. But the amount of storage that we're actually storing in AWS is a lot smaller than what it would have been if we had just done a normal copy-out."

A modern backup and recovery solution should have a favorable financial profile. Fast, compelling ROI is essential. The insurance company Senior Network System Engineer addressed this need when he said, "I believe our company has seen return on investment by going with Rubrik." In his case, ROI came from less time wasted on managing and deploying and supporting free or open-source software.

For the university Senior Systems Engineer, ROI arose out of avoiding hidden costs. He said, "With the lower amount of management time, I've been able to focus on doing a whole lot of other work." The financial services Assistant Vice President added, "We've seen ROI. Productivity has gone up because we're able to spend less time on daily operations for backups."

#10 – Quality of Support and Service

Good support is a non-negotiable characteristic of a preferred backup and recovery solution. Rubrik users commented on this aspect of their experience. The financial services Assistant Vice President said, "I've used technical support a few times and they've always been great, very responsive, including on weekends. They have even been proactive and have automatically opened up a ticket when they see something fail." Rubrik also fields a Ransomware Recovery Response team to help customers handle this uniquely serious threat.

"Tech support has been fantastic. They will bend over backward to help get solutions," said the university Senior Systems Engineer. "Since they have global support people, I'm not having to either patch a system in the middle of the day or having to change our backup windows. They have someone available after our backup window ends but before the beginning of our business day." The Systems Architect at Cardtronics had a comparable observation. He said, "Rubrik has the best vendor support that I've dealt with. They're probably the best. They're the most knowledgeable, they're the most respectful, they call a lot better, they will follow through to the end. Not like with VMware."

Conclusion

Ransomware is having a major impact on enterprise IT, with implications for backup and recovery. Older solutions are showing their limitations in the face of the threat. In their place, IT teams are turning to the Zero Trust model, which has the potential to make backup and recovery better at mitigating the ransomware threat. Selecting a backup and recovery solution that supports a Zero Trust security strategy is a process that requires looking at many system characteristics at the same time and aligning them with one's unique organizational requirements.

According to users of Rubrik on PeerSpot, the top 10 "must haves" include air gaps, ransomware mitigation, immutability, scalability and automation that span across on-premises and the cloud. Saving time and money are important, too, as are ease of use and administration. Solutions that meet these criteria will be poised to handle the increasingly challenging backup and recovery demands of the evolving modern enterprise.

About PeerSpot

PeerSpot (formerly IT Central Station), is the authority on enterprise technology. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

About Rubrik

Rubrik, the Zero Trust Data Security™ Company, delivers data security and operational resilience for enterprises. Rubrik's big idea is to provide data security and data protection on a single platform, including: Zero Trust Data Protection, ransomware investigation, incident containment, sensitive data discovery, and orchestrated application recovery. This means data is ready at all times so you can recover the data you need and avoid paying a ransom. Because when you secure your data, you secure your applications, and you secure your business.

For more information please visit www.rubrik.com and follow @rubrikInc on Twitter and Rubrik, Inc. on LinkedIn.