# DR in the Ransomware Age: Isolated Recovery, DRaaS and Embracing IT Resiliency

By Kasia Lorenc

Channel Partners™

JANUARY 2017 | US$25 | S020117

# DR in the Ransomware Age: Isolated Recovery, DRaaS and Embracing IT Resiliency

By Kasia Lorenc

JANUARY 2017 | US$25 | SO20117

Channel Partners™

# Table of Contents




Channel Partners™

# About the Author

**KASIA LORENC** has been working in technology and marketing for nearly a decade, most recently serving as the managing editor for Tom's IT Pro and Tom's Hardware, focusing on content strategy and development in business computing and computer hardware. In her previous roles, Lorenc pursued her passion for writing, technology and marketing, creating content for a variety of channels for the IT professional and developer audience. With strong ties to enterprise IT, she continues to write about cloud, security and mobility topics.

linkedin.com/in/kasialorenc
@kasialorenc

# DR in the Ransomware Age: Isolated Recovery, DRaaS and Embracing IT Resiliency

## ON FRIDAY, NOV. 25, 2016, THE SAN FRANCISCO MUNICIPAL TRANSPORTATION AGENCY WAS HIT WITH A

ransomware attack that forced the metro to shut down its affected ticketing systems, hang "Out of Service" signs and give away rides for free. The ransomware attacker demanded approximately $73,000, to be paid in Bitcoins, in exchange for a digital key that could decrypt the thousands of systems that were compromised. It seemed to be another episode in a depressing parade of hit-and-profit ransomware attacks.

Then, something interesting happened. SFMTA did not pay the ransom. Instead, the agency was able to contain the situation, shutting down and restoring its systems from backups.

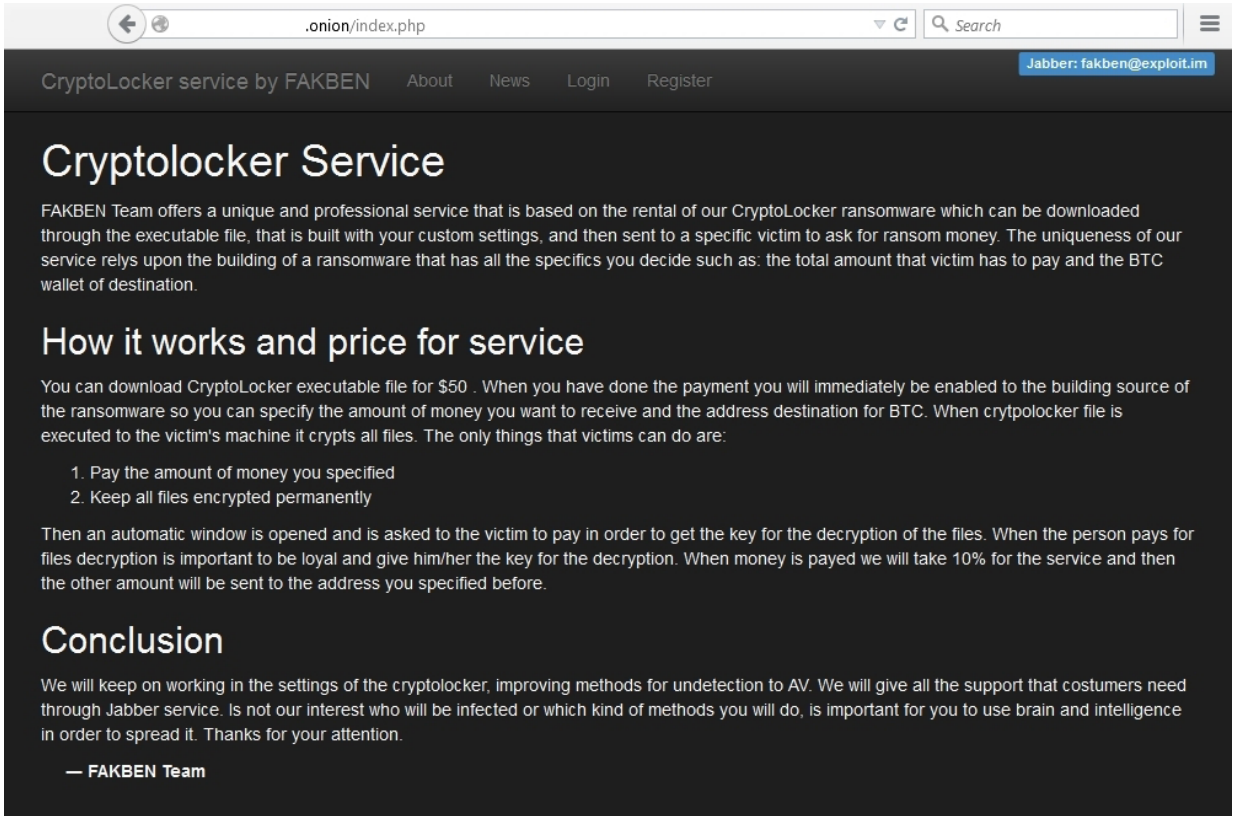
Unfortunately, not all organizations are that prepared. Without proper backup and disaster recovery (DR) procedures in place, many have no choice but to pay attackers to get their critical data back. Malwarebytes' international survey of 540 CIOs and CISOs, released in August 2016, revealed that nearly 40 percent of businesses were hit by ransomware in the last year, and more than 40 percent of the businesses affected were forced to pay sums ranging from $1,000 to more than $150,000.

What's more, the damaging effects of ransomware go beyond blackmail. Most businesses experiencing an attack will experience loss of revenue: San Francisco's Muni wasn't

able to charge customers and had to offer free rides before all systems were restored. Malwarebytes' survey shows that 60 percent of ransomware attacks took more than nine hours to remediate.

## Ransomware for Hire

Part of the reason for the rapid growth in these attacks is the rise in "ransomware-as-a-service." Malicious hackers can buy malware kits for a small fee or rent the code for a percentage of collected ransom. Check out the following offer for CryptoLocker ransomware.




Today, over 80 percent of cybersecurity professionals are concerned about ransomware, according to a report released by Check Point in December 2016. We're not sure what the remaining 20 percent know that the rest of us don't — Check Point predicts that there will be even more ransomware attacks in 2017 and that malicious hackers will find their way into cloud-based data centers. That will be a game changer, say experts.

"As more organizations embrace the cloud, both public and private, these types of attacks will start finding their way into this new infrastructure through either encrypted files spreading cloud to cloud or by hackers using the cloud as a volume multiplier," said Don Meyer, head of product marketing at Check Point.

Ransomware attacks are getting more complex, incorporating different techniques and technologies. The current motto guiding security seems to be: It's not a matter of *if* you get attacked by ransomware, but only a matter of *when*.

## Death and Taxes. And Ransomware

One reason ransomware has increased dramatically in the last few years is the rise of digital currencies. Bitcoins allow a much simpler, more efficient and anonymous way for attackers to get paid. Years ago, attacks were focused on obtaining intelligence — interested in the data itself. While that often is still the case, more recently malicious hacking has become a lucrative business, with attackers searching for easy targets.

Before advising customers to pay the ransom, be aware that paying not only doesn't guarantee that they'll get all of their data back; it could precipitate a repeat attack. There have been reports of ransomware attackers leaving behind malware, even after receiving payment, so they could demand a ransom from the company again.

"Simply paying the ransom to get your data back doesn't mean that you're no longer vulnerable," said Roland Fritz, president at Data Protection Advisors, a sales and consulting company that specializes in designing solutions that protect customer data from the moment it's created until it's deliberately destroyed.

Most security professionals today agree that protecting a business from a possible ransomware attack is no longer enough. Organizations must be prepared for the worst-case scenario. That means being able to wipe systems to bare metal start over.

### The best defense is a holistic approach that combines four pillars:

- **Security 101:** Anti-virus, vulnerability scanning, network protection and keeping all systems patched.
- **Education:** Training staff to spot phishing and avoid shady sites so that malware doesn't sneak in through an endpoint device.
- **Advanced Tech:** Customers that have the security budget should also look into heuristic analysis, which has the potential to detect previously unknown malware.
- **Disaster Planning:** This is absolutely essential. Generating full and regular backups of customer data — and ensuring that those backups themselves are protected — is crucial.

"There's a long list of things that IT departments are doing, and they're all good things, but everyone has come to realize that they can and may be attacked despite all of those preventative actions," Fritz told Channel Partners.

Once attackers find a point of entry and infect vulnerable systems, they immediately go after backups. That's common practice today, according to Fritz. He said attackers are getting smarter; they aim to identify not only where backups are, but how long they're retained. Once they're aware of the organization's backup retention period, they simply wait until it's over to demand a ransom.

The malware itself is becoming more sophisticated as well. Some variants are capable of penetrating the firmware of the hard drive, Fritz told us. So even if you wipe drives, the malware can propagate from the firmware, and oftentimes it's not even detectable. The only solution then is to stand up a new environment.

While most organizations will have some type of data backup in place, when it comes to recovering from a disaster such as a ransomware attack, it's important to understand the capabilities your disaster recovery solution providers afford customers. Protecting data that's being backed up is important, but you also need to take a close look at how the data is being stored.

## DR Done Right Demands Isolated Recovery Solutions

So how can you help customers defeat these ever-more-sophisticated ransomware attacks?

One key is to completely isolate backups from the production environment. Store them off-site, and hide them as much as possible from a potential attacker.

"The only way to recover is from a static backup copy from a known-good point in time," said Fritz. "And if the attacker is able to find it, because it's in the production environment and it's not isolated, then you're at the mercy of the attacker. The only thing that ensures recoverability is an isolated backup copy."

Providers including Sungard Availability Services now offer isolated recovery solutions that aim to put the static backup copy beyond the reach of an attacker. When evaluating these solutions Fritz advised partners to ensure that:

- The backups are stored in an off-site, locked-down and physically secured location that's separate from the customer's production facilities.
- Systems are replicated on a regular basis, and all connections are tightly controlled. Ensure that backups are completed at different times of day, to make it even more difficult for an attacker to penetrate a connection.
- Managed recovery capabilities are in place so organizations can quickly and easily test recoverability, which in turn gives customers a certain level of confidence in the solution. Make sure that you can stand up an interim production environment through an isolated backup service to keep the business running during the recovery process.

Fritz said the last item is critical because cleanup can take a while, and downtime is lost revenue.

"If you do need to recover and operate for some period of time because your production system has been infected and there's a massive cleansing operation in progress in the production environment, a prospective customer of this service would have the option to run production from the Sungard AS facility until his own production environment has been restored," he said.

An isolated recovery solution is essentially a complete new data center that holds a copy of the data without which you simply can't run your business, so that in case of a disaster, such as a ransomware attack, you can recover quickly. Although effective, it's a costly solution. Fritz said it's typically created for only a subset of the environment that's mission-critical to minimize cost.

However, he argued that when compared with the costs of cutting-edge preventative security tools, an isolated backup service can be a bargain.

"There's never been a better time than now to have high confidence in your backup," said Fritz. "Buy the security you can afford, but understand that you can and likely will be attacked sometime in the future. And the only recovery is from an isolated backup copy."

## DRaaS: Disaster Recovery Simplified

Another approach that's been steadily growing in popularity is disaster recovery-as-a-service (DRaaS), which offers multiple recovery points of a customers' data, all stored in the cloud. Data is encrypted at rest, and there are physical and logical isolations in place to minimize security breaches. Most DRaaS options offer flexible testing, automation capabilities and single-pane-of-glass management.

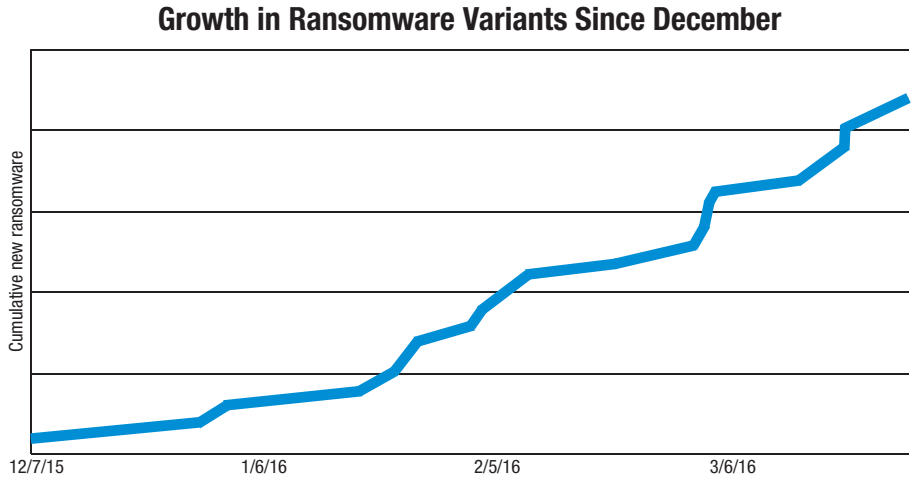
Today, there are several channel-focused DRaaS technologies to choose from, including Acronis, Datto, iland, Veeam and Zerto. Some offer just the DR software; you work with your choice of service provider. Others provide the software and the cloud service. Some will do either, depending on the partner and customer. For example, we spoke with Zerto, which provides just the software, and iland, which offers the cloud service integrated with Veeam and Zerto; we also spoke with Acronis, which offers both.

The cost of DRaaS will be more than that of doing just backups, but it's also much more cost-effective than traditional DR. It offers even SMB customers the ability to recover a full site and perform regular DR testing.

The main advantage of DRaaS is that a customer doesn't need the hardware, services, software or space to replicate a data center for the purposes of disaster recovery.

### Variation Is a Problem

One factor hindering security professionals is the rapid proliferation of new strains of ransomware.




Total new ransomware strains in the wild since December 2015.

Source: Proofpoint

IT pros who've been in the business for a decade or more remember the expense and complexity of standing up and maintaining a duplicate data center. Traditional DR can more than double the cost of a customer's operations, said Ron Hayman, chief cloud officer and COO at Avant Communications.

It's an expensive undertaking, which is why many companies haven't invested in proper DR environments. And even among those that do, many frequently don't do it right. Hayman has seen this firsthand: He's spent years working in the trenches, serving in vice president and director roles for IT organizations both large and small.

"DR is typically underfunded, and if it is funded, it's primarily to meet compliance requirements," he said. "It's also very hard to replicate."

Customer IT teams may not realize that there's now a dramatically better and less expensive way that still meets compliance demands.

Hayman's organization, Avant, is a master agent specializing in next-generation technologies such as cloud, colocation, connectivity, security and software. He said DRaaS is a growing area for Avant and for a lot of its partners.

DRaaS is the sweet spot between an expensive, traditional DR recovery site and doing just backups, which can be difficult and time consuming to use for recovery from ransomware. The biggest advantage, besides cost, is that DRaaS systems are managed by professionals who specialize in disaster recovery. This means customers have a much better chance of meeting their recovery time objective (RTO) and recovery point objective (RPO) requirements as compared to a traditional DR environment, where IT is more likely to underestimate the recovery time and not take into account possible obstacles, Hayman told us.

"You're taking it out of the hands of IT people who are good at their day-to-day jobs but don't have a lot of capability around disaster and backups, and you're putting it in the hands of organizations for whom it is their core business," he said.

DRaaS also offers the flexibility to test backups and the recovery process on an as-needed basis by simply renting the systems needed for trial runs. Unlike a physical data center, customers don't pay for the machines until they need to use them again, Hayman said. And some providers, like iland, offer failover and failback testing without restrictions at no additional cost.

## DRaaS for Virtual, Physical & Cloud-to-Cloud Recovery

To get a better sense of the current technology landscape, we sat down with executives from three of the top DRaaS providers: Acronis, Zerto and iland.

While iland offers a number of secure enterprise cloud services, it's best known for its DRaaS solution. Partnering with both Veeam and Zerto, iland has integrated DRaaS for physical and virtual workloads, both on-premises and in the cloud. We spoke with Dante Orsini, senior vice president at iland, to learn how the company combines best-of-breed technologies into a powerful cloud platform and a simplified offering that channel partners can take advantage of.

For organizations looking for a simple cloud backup solution, Veeam's Cloud Connect backup product makes it easy for partners or customer IT to get a backup copy off-site. VCC has built-in end-to-end encryption, so backup data is encrypted at the source, in flight and at rest.

"Veeam allows backup admins to be able to send backups off-site very easily," Orsini said. "It's all done over SSL, so they don't have to engage a network admin to set up a VPN [virtual private network]. And what we've done is simplified the model so it's just a per-GB charge — no cost for bandwidth, no cost for setup, no VM [virtual machine] charge."

For DRaaS, iland has partnered with Zerto to deliver an integrated solution. What makes Zerto unique, Orsini told us, is that it has moved replication into the hypervisor, which he said gives the solution an advantage. Customers gain affordable continuous data protection and are able to achieve RPOs of seconds, unheard of for small

and midsize businesses just a few years ago. What makes this possible is Zerto's Virtual Protection Groups (VPGs), which allow IT to protect individual applications or multiple VMs and virtual disks.

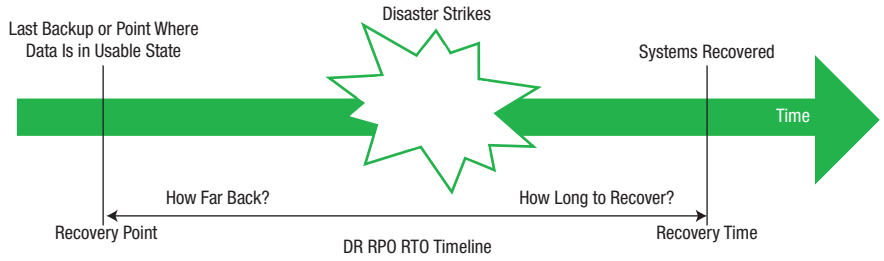
Additionally, everything is stored in a journal at the target site, Orsini explained, which allows for point-in-time recovery and up to 30 days of checkpoints.

"The journal capability really helps with ransomware in particular," said Orsini. "If something is lying dormant in the system, having the ability to roll back, like with a DVR, gives you a lot of flexibility."

When a partner combines that with a comprehensive backup strategy that goes beyond those 30 days they can position a customer for a successful recovery in case of an attack that can't be prevented, Orsini told us.

## How Much Loss?

Partners should sit down with customer IT teams and data owners and figure out the best balance between downtime, data loss and budget for each application. A payments database is a very different case from a mostly static website.




**Recovery Point Objective (RPO):**
Amount of acceptable data loss measured in terms of how much data can be lost before the business is too adversely affected.

- RPO indicates the point in time a business is able to recover data after a systems failure, relative to the time of the failure itself.

**Recovery Time Objective (RTO):**
Amount of systems downtime defining the total time of disaster until the business can resume operations.

- Quantifies how much data loss is acceptable without grossly adversely affecting the business due to lost business transactions data.

Source: Veeam

Orsini described another unique capability that involves running security scans on a DR copy so that the overhead of scanning doesn't impact the production environment. If the DR copy is affected in any way, the organization will have a heads-up and can address the issue in the production environment.

"It's too challenging and too risky to run that kind of testing nonstop in a production environment," he said. "But if you can do it on a copy, somewhere in the cloud, it gives you more flexibility to get to that ultimate answer of how secure you are."

It's clear that cloud technologies have come a long way in the last few years and continue to advance. As Orsini pointed out, DRaaS can be a substantial tool in the hands of a channel partner. On top of the ability to recover from any disaster, including a ransomware attack, iland's integrated cloud platform, and others like it, can offer a partner visibility into a customer's security, compliance and reporting posture, allowing for consultative services.

"When a partner is deploying an iland cloud, they're going to have very few line items, but they'll see a laundry list of value," said Orsini, "And when it's all integrated into a single pane of glass, it demoes very, very well."

## Beyond BC/DR: Embracing IT Resiliency

As the DR landscape continues to evolve, the conversation is changing from backups, disaster recovery and business continuity to creating resiliency — girding the customer's environment with continuous availability no matter what the circumstance.

"Where we see DR and ransomware intersect is really in the resiliency aspect," said Gil Levonai, CMO at Zerto. "Resiliency is the encompassing goal; to be resilient to whatever happens, to changes in power, human error and cyberattacks."

Levonai said achieving that involves preventative security measures alongside a resiliency strategy, which goes beyond backup and DR to minimize data loss. With continuous data protection, customers can restore from just 10 seconds before the ransomware infection happened, said Levonai, minimizing the impact of an attack.

What's more, the technology offers deep granularity options, in both time and scope of the recovery. A solution provider's IT can recover a single file, a single server, a group of servers or an entire site; likewise, you can have recovery points that are just seconds apart through Zerto's journal capability.

Zerto's solution allows organizations to replicate mission-critical data, and even entire environments. However, it's not for everyone; SMB customers in particular will find it overkill.

Smaller organizations can leverage other tools, like Acronis, which can work with businesses having just a couple of servers. John Zanni, senior vice president of channel and cloud strategy at Acronis, told us SMBs can work with an Acronis partner to define their needs and have a DR solution up and running fairly quickly.

Acronis, like Zerto and others, offers continuous data protection and resiliency capabilities, but with a different approach and set of technologies. Acronis collects data that needs to be backed up with a seeding device that's located on the premises, Zanni said. Customers have the choice to enable continuous data protection and set the frequency of replication. Backups are completed with Acronis' core backup technology; once a full image backup is complete, only changes are backed up. Like Zerto, Acronis offers deep granularity, so recovery can be set down to a single file — in fact, Zanni said Acronis was the first company to offer this functionality. Additionally, only corrupted files are recovered to speed up recovery time.

"The disaster recovery technology is in place where you have configured your applications or copies of your applications in the cloud," said Zanni. "Once again, defined by the customer, they can either be always-on and running, and then they

### Get out of Jail Free

Security providers Barracuda, Kaspersky and McAfee as well as AWS and law enforcement are collaborating on the **No More Ransom** initiative. The site offers a repository of keys and applications that can decrypt data locked by certain types of ransomware, including the popular TeslaCrypt.

pull the latest data from the seeding device and are current. Or they could be off and just need to be spun up, which can take anywhere from 15 minutes to an hour depending on the application."

Tied to the service is a set of runbooks and management capabilities that allow IT to point the Domain Name System (DNS) from an on-premises server to the one in the cloud, in case something goes wrong with a production system, Zanni said. For servers that are hot, this change happens instantaneously. Otherwise it takes 15 minutes to an hour.

Acronis' service includes a test mode, where IT can simulate a failure and run a recovery drill once or twice a month, just to make sure everything is configured properly. Acronis also offers the ability to define how backups are stored, offers a portfolio of solutions that go beyond DR and is committed to strong partner relationship.

"We made a conscious decision not to go direct but to go through partners so that the company that buys the solution is buying it from the same IT provider that they're used to and comfortable with," said Zanni. "And we provide the support services that are needed to make sure that our channel has everything they need to provide the level of service they want to provide."

## The Right Tools. The Right Strategy

When it comes to arming your customers against ransomware, it all comes down to having the right tools, the right infrastructure, the right approach and the right strategy in place.

Part of the strategy piece involves crafting a solution and processes that will allow IT to meet the organization's RTO and RPO objectives. Hayman said partners have a much better chance of meeting these requirements with a DRaaS solution rather than with a traditional DR site. Other important considerations include regulatory and compliance requirements and the unique needs of an organization. As always, budget will determine not only which tools and technologies are implemented, but also what data is being backed up and protected, and what RTO/RPO levels are realistic.

Finally, don't neglect end users. Backup services for endpoint devices is critically important, especially for ransomware, according to Hayman, because these are the systems that are most likely to get attacked. Partners should strongly advise customers to separate end-user data from the server infrastructure, because they'll typically have different policies, backup schedules and RTO/RPO requirements.

Today's DRaaS services take care of that, along with providing the necessary technical expertise and support. Distributors and master agents like Avant can provide the go-to-market expertise and support for channel partners looking to offer DR solutions to their customers as part of a comprehensive ransomware protection strategy.

"We continue to see DR as a very important service to offer customers; it's undersold in the market," Hayman said. "There's a great opportunity."