The Backup and Disaster Recovery Security Toolkit

Quorum®

1-Click Instant Recovery

WHEN BREACHES HAPPEN, AND THEY WILL, THE FIRST CASUALTY IS TRUST.

Your customers lose their trust in you; your staff may lose trust in their leadership. After a big enough attack, especially one involving an aftermath of regulatory fines and a damaged brand, you may never really trust in the sanctity of your applications, servers and data again. Especially if the disaster affected your backups and ability to recover.

Yet secure backup and disaster recovery is within reach. Backup and Disaster Recovery (BDR) isn't always a first thought when IT leaders architect their security programs. But it s the last line of defense when all else falls to the invaders sacking your system. Perimeter security is all well and good; but when criminals take over your system, your backups may be your last hope for recovery   and in some extreme cases, your organization s survival.

Attackers know this, and many will head straight for your backups to kneecap any hope you have of recovery. Yet many IT teams fail to secure their backups like the valuable insurance they are. Instead they leave them vulnerable and unprotected, sabotaging their own future recovery.

Taking budget away from BDR to strengthen the perimeter can be a dangerous move for this reason. If a ransomware attack hits, or a natural disaster floods the primary and redundant datacenters, the survival of your backups will determine your fate.

The good news is that just as advanced BDR solutions have accelerated RTOs, they have also made it easier than ever to safeguard your entire backup and disaster recovery ecosystem.

RELYING ONLY ON BACKUP TAPES

For a long time, “backup” was almost synonymous with “tape.” IT teams took for granted that any kind of recovery meant they would have to retrieve tapes from an offsite location   and sometimes even wait for the tapes to be shipped to them.

In today’s always-on world, that kind of downtime is a death sentence for any organization that wants to be respected by its workforce and customers. Too many companies have raised the BDR bar with near-instant cloud solutions that make flawless continuity a reality. So why do so many teams still rely on backup tapes? Often they think they can protect physical backups more easily than virtualized replicas of their environment.

In reality, backup tapes can be more vulnerable than a cloud solution. Theft is always a possibility, as is any kind of transportation incident. They’re also liable to become corrupt or lost, or destroyed by an electrical fire, an earthquake, a flood or other natural calamity.

Yet the real security gap often occurs at the end of the tape or disc lifecycle; when the organization does not legitimately and thoroughly destroy the backup, sensitive data can be vulnerable for exploitation.

SLOW RECOVERY

Long delays in recovery are probably the top complaint in the BDR world. But speed isn t just about convenience—it’s about security.

Ransomware is one of the most obvious examples. If your attackers kidnap your data and take down your systems in a demand for money, you only have a short window in which to outplay them. Failover quickly and you can ignore their demands. But if recovery is hours (or even days) away, and you’ve got mission-critical systems that must be up, your team may be forced into paying the ransom   an act which often invites future attacks.

> **SPEED ISN T JUST ABOUT CONVENIENCE   IT S ABOUT SECURITY.**

A WEAK OR NON-EXISTENT RESPONSE PLAN

The “People—Process—Technology” mantra applies to backup and disaster recovery as much as anywhere else, yet most teams focus only on the technology. Your response plan whether you re trying to staunch a cyberattack or rescue a datacenter from a hurricane is all about your processes and your people. Fail to map out how you ll recover and who will help you do it, and you will be creating an enormous security gap.

Think of the panic or confusion that can set in when a security event happens. Your team needs to move fast in a cohesive, organized fashion. There’s no time for reminders or long explanations, which is why you need a documented plan that spells out who needs to be contacted, who is responsible for failing over and other decisions. If you’re using a hybrid solution with on-premises backups and cloud replicas, which is the priority? How can you stop an attack in progress while maintaining uptime? How can you ensure your backups will meet peak performance requirements? Do enough people understand how to operate your failover system?

Many epic disaster stories are epic precisely because a plan was nowhere to be found. The team assumed an outside attack was the biggest risk, but didn’t plan for human error; data was stolen en route to the cloud because they didn t adopt appropriate encryption. A good plan can mitigate the damage of even a drastic security event, and help the team panic less while accomplishing more. And of course the plan must be tested regularly to ensure its efficacy.

ASSET AMBIGUITY

Years ago, not knowing where your most valuable data was would have sounded absurd. Today, the explosion of applications and systems, and the complex ways in which they interact, means that many teams may have a misguided idea of what deserves top shelf protection.

Smart recovery is tiered recovery. By dividing your assets into groups **critical, important** and **back-burner**—you'll not only create a more cost-effective storage strategy but you ll ensure that your most valuable systems, apps and data get the strongest protection and the fastest recovery. Take a thorough look at your BDR ecosystem and decide how you can best protect your assets and position them for secure and immediate recovery.

SMART RECOVERY IS TIERED RECOVERY.

A COMPLICATED RECOVERY PROCESS

IT leaders often begin a disaster recovery program with the idea of keeping it streamlined and simple. Gradually they add more and more point solutions, until their BDR tech stack is made up of different vendors and processes that add up to a slow and laborious process. Other teams invest in leading solutions that involve a dozen or more steps simply to failover.

In a time of crisis, failover needs to be as simple as possible—ideally just a click. If intense training and cheat sheets are required simply to spin up a working replica of your environment, you ll need to guarantee the trained people are around and available whenever the crisis hits   and even then they may fumble the process. A simple failover process that anyone can execute is the key to a secure recovery.

> **IN A TIME OF CRISIS, FAILOVER NEEDS TO BE AS SIMPLE AS POSSIBLE IDEALLY JUST A CLICK.**

INSECURE BACKUPS

Leaving your backups unprotected is like insuring your house and leaving it unlocked. You re sabotaging your own recovery.

Criminals will find a way to your backups, particularly if they're intent on holding your information hostage. That's why your backups, in whatever form you're storing them, merit the same sophisticated security controls as your primary environments. Poor authentication controls or weak encryption key management can easily creep in as your data grows and your BDR system becomes more complex.

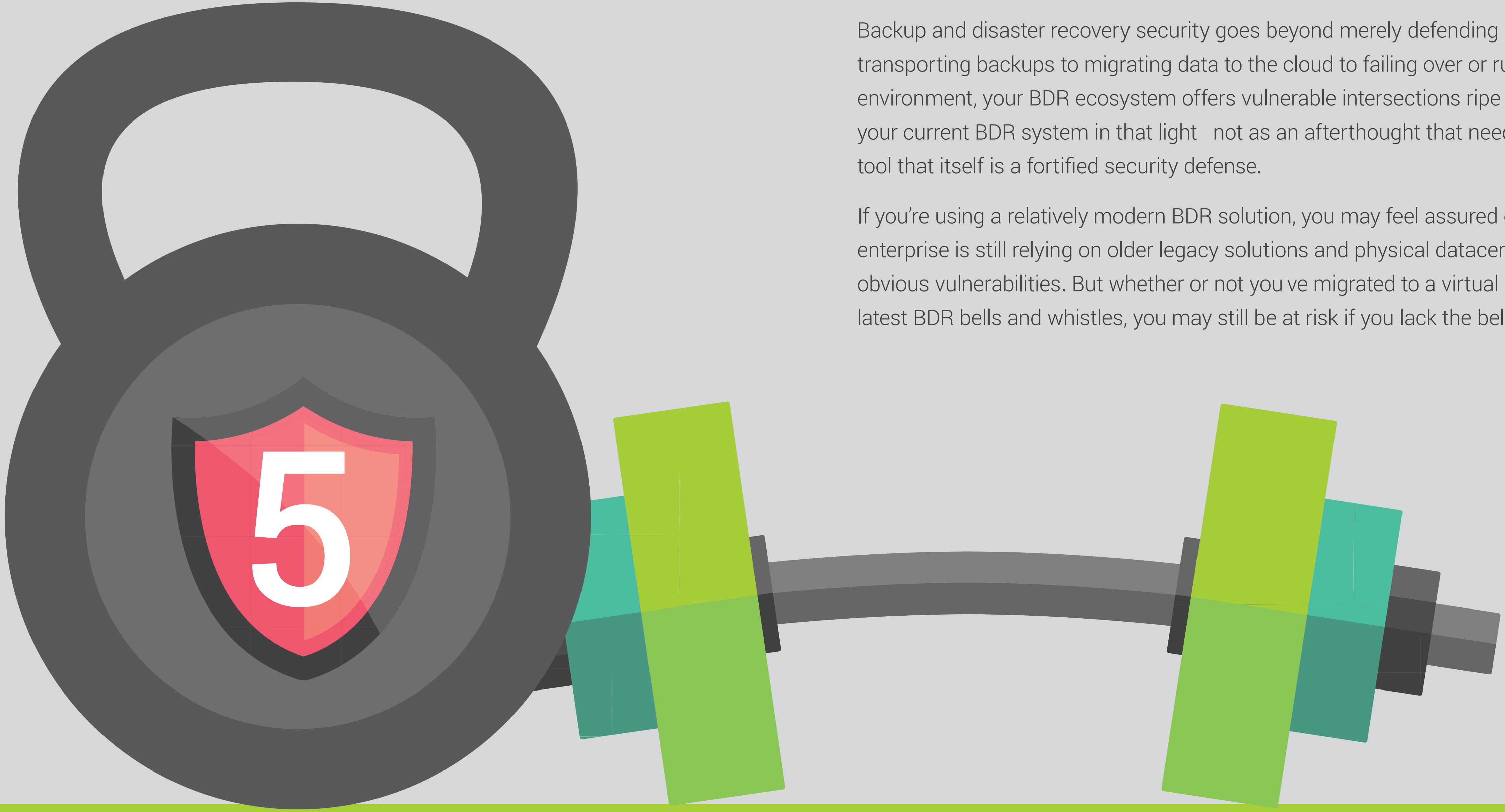
CRIMINALS WILL FIND A WAY TO YOUR BACKUPS, PARTICULARLY IF THEY RE INTENT ON HOLDING YOUR INFORMATION HOSTAGE.

AN INCOMPATIBLE SOLUTION OR PROVIDER

To many IT leaders, the “right” solution or provider is the one with the best reputation at the right price point. But even a leading name in the BDR space can leave your team with unexpected blind spots if you don t do your due diligence in determining their security capabilities.

This is especially true if you’re moving data offsite and into the cloud. The cloud can provide secure backup and disaster recovery, but you must detail who s handling which responsibility, and ask about encryption, compliance certification and their reliability track record. Ask if their data centers have on-site security and if they use multi-factor authentication. Many top BDR providers haven’t taken sufficient steps to secure their virtual environments.

MANY TOP BDR PROVIDERS HAVEN T TAKEN SUFFICIENT STEPS TO SECURE THEIR VIRTUAL ENVIRONMENTS.



THE 5 CRITICAL BDR TOOLS FOR STRENGTHENING SECURITY

Backup and disaster recovery security goes beyond merely defending backups. From transporting backups to migrating data to the cloud to failing over or running a replica environment, your BDR ecosystem offers vulnerable intersections ripe for malfeasance. Evaluate your current BDR system in that light not as an afterthought that needs to be secured, but as a tool that itself is a fortified security defense.

If you're using a relatively modern BDR solution, you may feel assured of your security. If your enterprise is still relying on older legacy solutions and physical datacenters, you may be aware of obvious vulnerabilities. But whether or not you ve migrated to a virtual infrastructure with all the latest BDR bells and whistles, you may still be at risk if you lack the below five tools.

TOOL #1: INSTANT RECOVERY

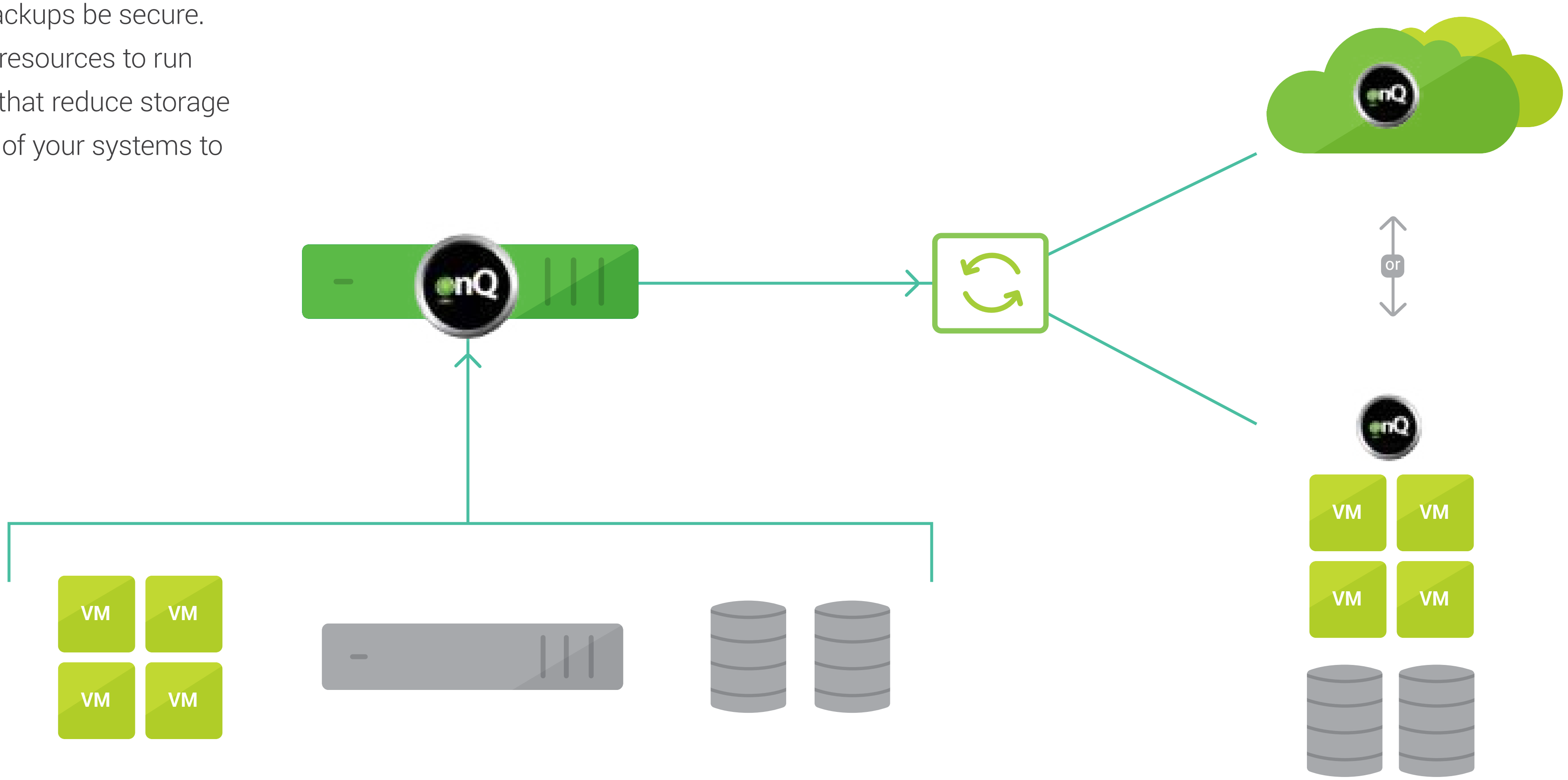
While long periods of downtime are still the norm for some organizations, near-immediate recovery is available with the right solution. Virtual clones of your environment can be spun up in minutes after any site, system or storage failure   not only for virtual production servers but for physical as well. Snapshot-based backups that replicate your server image, applications and data, with incremental backups at the frequency of your choice, make backing up faster as well—cutting down on data transmission time.

TOOL #2: REDUNDANCY

Despite the cloud s ascendancy, physical datacenters aren t going away. In fact, the two can work together by partnering local backups with the immediacy of virtualized solutions. Adopting a hybrid cloud configuration can help you get the most out of your existing investments while enjoying the peace of mind that comes with multiple replicas of your most critical assets. If your local backups fail, your virtual clone can step in and vice versa   so you are covered no matter which type of disaster strikes.

TOOL #3: ADVANCED SECURITY CONTROLS

IT leaders with a cavalier attitude toward BDR often fail to surround their backups with the right protection. In fact, each individual virtual network that connects to the DR recovery node should be isolated by a dedicated firewall. Any data centers hosting your applications should offer Tier 1 architecture and be certified with PCI, HIPAA & SOC 2. Only in that kind of well-guarded and stable environment will your backups be secure. Also important: solutions that won t rob your other resources to run failover workloads. Look for deduplication features that reduce storage and network bandwidth requirements. You want all of your systems to perform at their best.



TOOL #4: A UNIFIED, SECURITY-SMART SOLUTION

While most teams are familiar with the chaos that comes with using too many solutions and too many vendors, few think of it as a security issue. But the more tools you add into the mix, the more likely the resulting configuration is to have some security gaps. Look for one BDR solution that does it all, with user-friendly installation and configuration that you can handle without a specialized team. Also be sure that the support team is internal and staffed by engineers with first-hand knowledge of the solution. Those engineers will spot potential security loopholes; a vendor's third-party call center will not.

Ask your vendor detailed questions about their security protocols. Ask how they meet HIPAA, PCI and other compliance regulations, and how they handle data migration, cloud tenancy and remote access. Discuss in detail the plan for transitioning some of your in-house security responsibilities to the cloud provider if necessary. One solution that can remove many security burdens: a reputable Disaster Recovery as a Service (DRaaS) solution that liberates you from tech refreshes, datacenter maintenance and other demands.

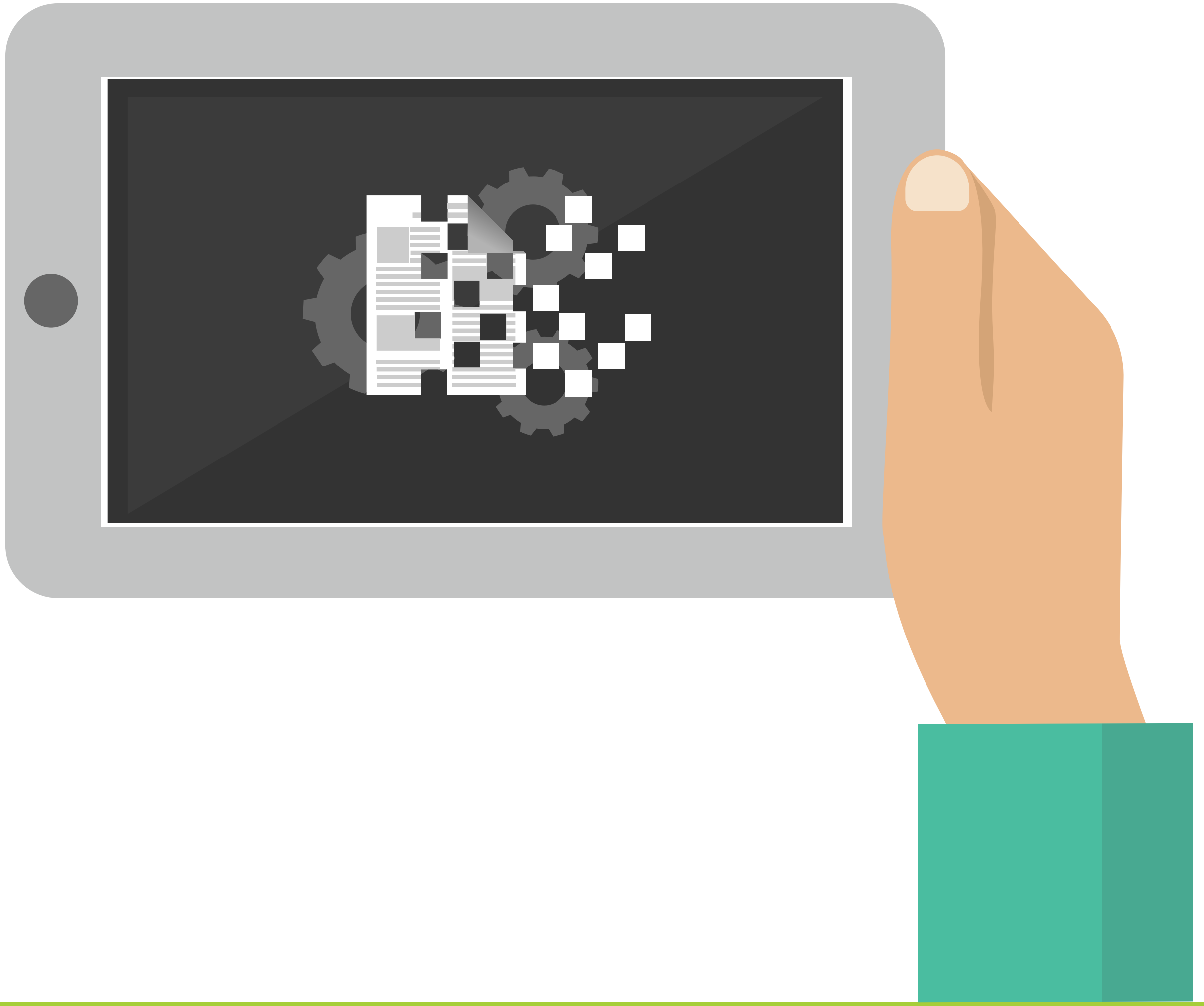
TOOL #5: ENCRYPTION

If BDR is a last line of defense, the last line of the last line is encryption. Even if criminals successfully steal your backups, encryption disguises the data from their unauthorized eyes. While the backups may still be gone, HIPAA and other regulatory institutions will often lessen certain financial penalties or exempt the breached organization from notification laws. These laws can require teams to notify customers, state and credit agencies to report a breach   but encrypted data will fall under most states' Safe Harbor laws, letting your team off the hook from a costly and humbling notification experience.

If you're curious what BDR encryption looks like, any backup stored in the cloud should pass through a 128 bit AES encrypted session over a 256 bit AES VPN tunnel before leaving your network; the data should be encrypted again while at rest in the cloud. Any link used to connect or upload your data should be secured through SSL or other protocols as well.

Typical methods for rendering data unreadable include encryption algorithms like AES, Blowfish, RSA and 3DES, truncation, index tokens and pads, and one-way hashing. But skilled cryptography must be paired with other security protocols as well, such as restricting access to encryption keys, protecting transmission over open networks, using best practices for wireless networks, and cracking down on transmission of sensitive data over email, chat and other casually used technologies. A weakness in any of these areas could open a door to loss and violation.

Is encryption an easily mastered skill? No, but the protection it offers your data, servers and applications is invaluable; another reason that finding the right vendor can unlock a new level of BDR security.



SECURING YOUR RECOVERY

As backup and disaster recovery solutions grow more advanced, many IT leaders grow nervous over their ability to protect their backups both onsite and in the cloud. Security is within reach, but it s the combination of your plan, your processes and your technology that will ultimately determine the sanctity of your assets. Luckily the same solutions that offer the fastest recovery also offer the most powerful protection. Evaluate your BDR solutions based on security as well as speed and efficiency, and you'll protect your data in every way that matters.

Quorum®
1-Click Instant Recovery