Cyber Recovery as a Service

Recover faster with with thoughtful immutability.

We've seen the aftermath of a successful attack when we were engaged after a cryptolocker hit the servers of a small business. Their backups were destroyed, meaning that they had to pay the criminals, and only then could the process of recovery begin. It cost them weeks of downtime and four times their annual IT budget to recover. There's a better way, and it's not always traditional Disaster Recovery (DR).

At Volta, our engineers work 24/7 to prevent, detect, and react to cybersecurity threats that are a constant pressure on our clients. There's nothing unique about the situation; if you have a connection to the internet, then you are a target. With the sophistication of attacks increasing, IT teams across the globe know their organizations will be attacked at some point. It's a matter of what protections will be in place when it happens.

When an attack gets through, Cyber Recovery saves you.

A Cyber Recovery strategy allows you to sidestep the effects of an attack and get back on your feet as quickly as possible. Volta provides Cyber Recovery as a Service (CRaaS) to take the painful task of backups off your plate with technology that also makes your data copies immutable and untouchable. An investment in cyber resiliency surfaces when organizations make the theoretical, mental shift from "if" we get hit by ransomware to "when" we get hit by ransomware. Cyber recovery is the best answer to the real world threat. If bad actors got through your cyber security program, how would you recover?

VOLTA CRAAS IS: **RAPID** | **ROBUST** | **RESILIENT**

Why is resiliency challenging?

1. BACKUPS STINK

Compliance auditing diligence is also exhausting. These are jobs that no one wants to do. Backups are a pain and you can never perform the job well enough. They're never 100% and no matter how hard you try, you can't make them 100%. What's more... You never use them. Well, hopefully you never use them. Everyone thinks they're not important until they're really, really important.

2. THE RANSOMWARE TIMEBOMB

One of the biggest challenges in data protection is ransomware that acts like a timebomb. You don't want to be in a situation where you have to restore, but when you do, you often restore the malicious code that has infiltrated your systems. It is critical that you figure out where the bomb is when you restore.

Unfortunately that presents another challenge since typical enterprise data is scattered across:

+ Data centers
+ Remote offices
+ Public clouds
+ SaaS applications

Volta's Answer. When our security staff engages on a restoration event the best practice is to restore to a sandboxed location or to alternate environments to test, scan, and remediate the ransomware threat before it re-enters your production environment. Our technology stack allows us to spin up critical pieces of your environment away from your production servers and find the right solution quickly and safely.

3. TRADITIONAL DR PITFALLS

The challenges of traditional DR have to do with rapidity; how quickly you can bring back your data. Timelines have changed. Data from a week ago is not as valuable as it once was and data from a month ago might be worthless. Organizations need RPOs and RTOs within an hour or two, and traditional DR doesn't have that capability the way a program focused on cyber resilience does. New capabilities should be a part of every organization's backup strategy, particularly Continuous Data Protection solutions for RTOs measured in minutes and next-gen protection that can act as both a secondary environment and sandbox during a disaster or attack.

4. AUDITS & INSURANCE

Three years ago, the only time Volta would hear about insurance audits was when one of our clients had been successfully attacked. Today, over half of our security engagements start from an audit. Initiatives typically placed on the backburner have now been accelerated into immediate demands. It's the new normal for organizations to undergo routine audits in order to meet new insurance requirements. This trend is causing everyone to rethink their cyber recovery strategy.

Volta's Answer: Volta is a consultative partner to our clients during and after their audits. We help identify, remediate, and respond to challenges and requirements that ensure success.

How we provide it.

RAPID

Keep your data relevant with a dedicated SOC team available to you 24 hours a day, 7 days a week. We take a personal interest in our customer's business and have the tools and personnel necessary to help organizations recover rapidly.

We have a targeted technology solution for CRaaS through Cohesity. We'll take on the task of backing up your VMs and your file server, which ensures that if your file server blows up, and can't be used, Cohesity will turn itself into the file server for as long as it takes to fix the hardware. It will rapidly serve up files to get your business running again.

The unique capability of our solution is a node-based architecture that provides sufficient compute power to spin up a critical subset of your virtualized environment so that testing, remediation, and restoration can begin. Then, when the team is satisfied that the virtual server is ready to be moved back to the production cluster, a seamless storage vMotion handles the move, letting you have an "Instant On" restoration for your Tier 1 systems.

ROBUST

Real protection from ransomware means you need immutability. The primary attack vector is compromised credentials, the higher the privilege the better. Without immutable protection, the attackers will always seek out your backups before they trigger the main attack. Immutability means that no matter the access rights they obtain, there is still a secure set of backup data they can't touch. Additionally, Volta provides a "2 man rule" as a service, where we can retain top level access to backup systems, preventing internal compromises or stolen credentials from having the necessary roles to wreak havoc.

Our targeted solution comes with an overarching control layer that aggregates normal alerts, like backup failures. We manage backups, monitor the control layer, and if something fails, we discover what went wrong and fix it. That could be simply restarting the backup, or if more thorough analysis is required, working with client teams to determine what is causing the failure. Volta provides biweekly or monthly reports of event failures and success, trending, and more.

RESTORED

Volta Recovery Assistance assures that if a client has an event, our team will assist with the recovery.

Restoration Services

+ Restoration of a VM upon request.
+ Volta will develop an isolated cloud environment where recoveries of backups can be hosted and tested for potential vulnerabilities before attempting full restore in the on-premises production environment.

Recovery Services - Disaster Response

+ Fast restoration to target production environment.
    + Dedicated engineers available until restoration of a VM(s) identified in the disaster event is restored.
    + VPN access to a remote DR facility will be required in order to complete the restoration.