Solid Rock Solutions

RANSOMWARE PROTECTION AND RECOVERY SOLUTION

Solution Sheet

Your data is more valuable to you than to anyone else. That is why hackers are after your data: so they can sell it back to you. They want to prevent you from doing business, in effect holding your business for ransom. All it takes is one click by one employee on an attachment in an email personalized for them, designed to look genuine. That one click begins the process of locking down the employee's files. In short order, they are prevented from doing their job. Then it silently spreads to other desktops and servers on the network. If left unchecked, it will shut down your business in hours. Your valuable data will be encrypted and marked for deletion unless the ransom is paid. Most attacks also include a countdown timer, with portions of your business data deleted permanently as the clock ticks down and no ransom is paid.

If this has happened to you or a customer of yours, you are not alone. Ransomware attacks are succeeding on an unprecedented scale. With individual attacks netting anywhere from a few hundred to thousands of dollars, Ransomware netted over $325 million in 2015, and has already made over $200 million in the first half of 2016. In this environment, what can you do about it?

RANSOMWARE NETTED OVER $325 MILLION IN 2015, AND HAS ALREADY MADE OVER $200 MILLION IN THE FIRST HALF OF 2016.

Ransomware Protection and Recovery Solution

Datto is pleased to announce the industry's first Ransomware Protection and Recovery Solution (RPRS). Built on top of innovative new features in the Datto SIRIS, NAS, Backupify and Datto Drive product lines, this solution will detect a ransomware attack, and roll back systems to a point time time before the attack happened. This includes protecting files and folders anywhere on the network, on mobile devices, workstations, and in the cloud.

Here is how to take advantage of RPRS:

1. Ensure your systems and files are protected as soon as possible by deploying the SIRIS 3 Total Data Protection platform for all physical and virtual systems. Set a regular backup schedule.
2. Identify additional backup needs on the network, on mobile devices and in the cloud, and back them up using Datto NAS, Datto Drive and Datto Backupify.
3. When a ransomware attack starts, the attack profile is quickly detected, and an administrator is notified.
4. The administrator restores the affected system to a snapshot before the attack happened, erasing the attack.
5. If also infected, network file storage, mobile devices and cloud files are restored as necessary to prevent remnants of the ransomware from spawning a new infection.
6. Business resumes as usual. No ransom is paid, no files are lost, there is only a brief disruption, and it's over in a matter of minutes.

YOU NEED A WAY TO QUICKLY DETECT AND RECOVER FROM THE ATTACKS THESE EXISTING TECHNOLOGIES MISS. YOU NEED RPRS.

As with most disaster recovery scenarios, the best approach is to plan and prepare. While end user education and endpoint and perimeter protection solutions are critical components of such a plan, they alone are not enough. Most businesses already employ these solutions, and ransomware still gets through. To comprehensively protect your business, you need more than white and blacklists. You need a way to quickly detect and recover from the attacks these existing technologies miss. You need RPRS.

The Ransomware Protection and Recovery Solution is a collection of Datto products combined to protect businesses from the impacts of ransomware attacks. The solution includes SIRIS 3 detection, backup and recovery capabilities, as well as NAS 3, Backupify and Datto Drive to protect business data wherever it lives from ransomware.

SIRIS 3

The only sure way to resolve a ransomware attack is to restore the infected systems, effectively turning back the clock. SIRIS 3 with ransomware detection and point in time rollback, is designed to identify an attack, notify administrators, and recover from just these scenarios. Within minutes, it can be as if the ransomware never happened. Say goodbye to ransomware and other disasters, and hello to simple preventative measures provided by SIRIS.

Cloud Protected Services

Ransomware is often thought to be only an on-premises threat, but it does not stop there. No matter how hard you try to prevent it, someone's PC will get infected with ransomware. If the user syncs files with Google Drive or OneDrive, ransomware will lock files in the cloud too. Fix ransomware with a best in class SaaS backup solution and easily restore data to a point in time before your files were encrypted.

Datto NAS 3

Ransomware is not just a problem for endpoint and server systems, it will also affect all data stored on the network. Our network attached storage product, NAS 3 with NAS Guard can mount all of your network storage devices and automatically schedule and copy data to the local Datto NAS. This data is then backed up to the secure Datto Cloud, and available for restore at any time. Protect your existing network storage solutions from ransomware attacks with NAS Guard, available by the end of 2016 on the Datto NAS 3.

Datto Drive

Traditional file sync and share solutions are highly susceptible to ransomware attacks. Simply infect one user's computer, and files are then automatically synced amongst all devices - including mobile. Datto Drive is the only platform that natively protects against ransomware by taking complete backups of all files on the sync and share platform, enabling restore to before an incident. Erase the impact of ransomware on file sync and share with Datto Drive.

For more information please contact:
Angelo Vitale | President/Founder
Phone: 727-809-2009
Email: angelov@solidrocksolutionscc.com
Angelo A. Vitale | https://srscctek.com
5745 Main St., Suite 101, New Port Richey, Florida, 34652