arcserve®

Customer Case Study

Arcserve Helps MSP Save Client from Ransomware Infection

TruTech provides IT managed services to small and medium sized businesses in Northern California. Their services include everything from managing desktops, servers and networks to providing support with IT security and anti-virus management.

Tru Technical Partners

INDUSTRY:
IT Managed Service Provider

LOCATION:
Campbell, CA

SOLUTION:
Arcserve UDP Cloud Direct BaaS

PROBLEM

Ransomware virus infects client server and blocks business-critical data from being accessed.

SOLUTION

Client recovers quickly and avoids prolonged downtime.

RESULTS

TruTech demonstrates value of being MSP customer.

THE PROBLEM

Ransomware Infects Office Server

When one of TruTech's clients came to work and was unable to access any of their files, they knew something was seriously wrong. They couldn't resolve the problem on their own so they knew it was time to get in touch with their MSP. After some investigation, they realized that their systems were infected by the dreaded ransomware virus, CryptoLocker.

TruTech's investigation into the ransomware infection revealed how it spread to their client's system. An employee at the company had received an email from what they believed was a trusted source, since the scripting made it look legitimate. When that employee downloaded the attachment from the email, their computer and their files were infected. The virus then spread to the 160GB office server, resulting in their files being completely inaccessible and prolonged company downtime.

THE SOLUTION

TruTech Recovers Client Data from Arcserve UDP Cloud Direct Cloud Fast

Luckily for TruTech's client, the ransomware infected server was backed up with Arcserve UDP Cloud Direct BaaS. TruTech got in touch with Arcserve's support team to help get the client's business- critical data back.

> We were able to get back all the data we needed. – **Ben Rombaoa,** IT Manager

As soon as they had retrieved the customer's data from the Arcserve UDP Cloud, TruTech's team immediately went into action. The customer's retention policy went back seven days, and the ransomware files were not present in their Arcserve backup. The team then copied their data from Arcserve onto an external drive. The customer was able to access their files from the Arcserve UDP Cloud. As a result of the ransomware infection, the customer was down for three business days. Recovering all of their data took about eight hours total.

What is Ransomware?

Ransomware viruses often come through emails and infect a computer's files, systems, and even servers. They can remain dormant and undetectable for months at a time, so a user wouldn't even know that their system is infected until it's too late. The virus works by encrypting the files on a system so they become inaccessible to the user. The files are then held hostage by the hackers until the user agrees to pay the ransom in order to get access to their data back with a decryption key.

Ransomware Attacks on the Rise

Ransomware attacks are increasing in frequency significantly every year.

- **2,500 ransomware attacks were reported to the FBI in 2015i, costing victims $24 million.**
- **Hackers collected $209ii million just in the first three months of 2016.**

From hospitals, to businesses, to government organizations — anyone can become a victim of ransomware. And cyber criminals are notoriously difficult to catch or even locate. Emails containing the virus are also automatically sent out as spam in the thousands, making it very easy to cyber criminals to do — and increasing the chances of anyone having their files held hostage.

Sending backups offsite on a daily basis is an essential layer of security that can help protect your business critical data from such devastating cyber attacks. That is why having a solid data protection solution is critical in helping to prevent data loss — whether it's from a natural disaster, employee error, or hackers holding your data hostage.

THE RESULTS

TruTech Demonstrates Value of MSP to Customer

By getting in touch with TruTech, the business was able to begin the recovery process almost immediately. The value and major difference between being a managed service support customer versus break-fix support became clear due to the quick emergency support TruTech was able to provide. And thanks to Arcserve's WAN-optimized solution, they were able to retrieve all of the server data in less than 8 hours. "We were able to get back all the data we needed," said Ben Rombaoa, IT Manager at TruTech.

> Disaster recovery will become more important as cyber attacks keep going up.
>
> – **Ben Rombaoa,** IT Manager

Offsite Backups Keep Data Safe from Ransomware's Reach

Since ransomware spreads by infecting local servers, having a solution like Arcserve UDP Cloud Direct BaaS, which sends data offsite to the cloud is critical in keeping it safe from such an attack. According to Victor Cruz, Sr. Systems and Networks Engineer, "A great thing about cloud backup is having a reliable backup location outside the office. Disaster recovery will become more important as cyber attacks keep going up."

For more information on Arcserve, **please visit** arcserve.com