CyberFortress™
The Recovery People

cyberfortress.com
855-223-9322
sales@cyberfortress.com

PROTEK
PROACTIVE I.T. SUPPORT

Customer Case Study

How an IT services company experienced a devastating ransomware attack, but still retained 95% of its clients

Protek is a Utah-based IT services company that provides a complete, outsourced IT department for small-to-mid-sized businesses. From phone and PCs to security and cloud apps, Protek handles it all. Most of its clients are in the construction and associated industries and have anywhere from 10 to 200 computers.

At 9:53 A.M. on February 4, 2019, Protek was hit by a devastating ransomware attack that encrypted nearly all its clients' data and distributed the malware to more than 1,700 machines. Protek was the first and one of the largest of hundreds of managed services providers (MSPs) to be similarly hit. It was a particularly hard blow for CEO and founder Eric Woodard, because he and his team prided themselves on the strength of its security practice.

While many MSPs targeted had security shortfalls, Protek's defenses were superior. They used multi-factor authentication, next gen firewalls and anti-virus technology. All software was updated at least once a week. Security information and event management (SIEM) patrolled for udpeculiar behavior, with threat hunting software on the lookout for malware.

Yet, though Protek had gone above and beyond in taking measures to safeguard clients, one of its vendors had not. Their software had an undetected hole which cybercriminals were able to use to get around Protek's advanced defenses.

The Department of Homeland Security believes the attackers were a Russian organization that operated much like a business. They were in and out of Protek's systems within 30 minutes, leaving millions of encrypted files and a ransom note in their wake. Months later, the hackers announced they had made $2 billion from their campaign and were retiring.

Company: Protek

Location: Sandy, Utah

Website: proteksupport.com

Business: Providing a complete, outsourced IT department to SMBs

Challenge: Protek was hit by a devestating ransomware attack, and its DRaaS / BaaS provider was unable to restore the company's data

Solution: Veeam Backup & Replication delivered by CyberFortress as a service

Benefits: CyberFortress demonstrated the ability to spin up 200-300 servers from backups. Additionally, recovery is 75% faster than before, and requires just five clicks as opposed to 30 minutes of a skilled tech's time.

cyberfortress.com
855-223-9322
sales@cyberfortress.com

Left in the lurch by their former BaaS/DRaaS provider

At first, Woodard wasn't too worried, because he'd contracted with a backup-as-a-service (BaaS) and disaster-recovery-as-a-service (DRaaS) provider to protect both his clients' data and his own. Their service level agreement (SLA) covered situations exactly like this one. But when he called his provider to request that they spin up between 200 and 300 servers, they responded that the most they could do was a dozen and it would take a week.

Woodard had no choice but to wire the $92k ransom in Bitcoin to the criminals because he knew he wouldn't be able to get backups. Then, he and his team had to wait until the weekend before finally receiving the encryption key. To Protek's horror, it didn't work at first, but an email to the cybercriminals' equivalent of customer service got the issue resolved quickly. Ironically, the criminals apologized for the mistake.

But even though the key worked, decryption proved to be a laborious process. The ransomware could encrypt 75 million files in just four hours, while it took one hour to decrypt just 1,000 files. Protek had to write scripts to run 50 decryptors at a time per computer. For two months, they worked around the clock to retrieve their client's data.

Transparency pays off to retain 95% of clients

One would think a disaster of this magnitude would cause clients to leave in droves, but that's not what happened. In fact, Protek retained 95% of its clients, thanks to the firm's transparency and communication.

Woodard and his team met with each client in person, explained exactly what happened, the consequences of the attack and the measures Protek was taking to retrieve their data. They then followed up with nightly emails, while holding frequent conference calls, ensuring clients were up to speed on the situation at all times.

"To be honest, we've got an even stronger relationship with a lot of our clients now"

- ERIC WOODWARD

"They appreciated our transparency and know how committed we are to ensuring that this never happens again."

"We switched from the product we were on to Veeam with a backup repository at CyberFortress"

"Once our data was in the system, we did some tests comparing our old solution to the new one, because we had both products on every system."

cyberfortress.com
855-223-9322
sales@cyberfortress.com

CyberFortress provides a proven BaaS / DRaaS solution

A big part of its plan to handle the situation required finding a new BaaS and DRaaS provider. Woodard and his team evaluated the software solutions on the market and decided that Veeam was the best option, thanks to its ease-of-use, reliability and flexibility.

But in addition to an enterprise grade product, Protek needed a provider to deliver it, one who was versed in Hyper-V. When Woodard asked some Veeam executives at an Ingram Micro conference for a recommendation, they introduced him to CyberFortress.

CyberFortress is a global provider of highly available and secure cloud data protection solutions, including Disaster Recovery (DRaaS), Backup (BaaS) and Microsoft 365 Backup and Recovery. They are also hypervisor agnostic.

Woodard required that CyberFortress be able to:

- Demonstrate that it can spin up 200 to 300 servers from backups within a week;
- Provide a written guarantee with a strong SLA; and
- Store reliable backups in a secure, dependable data center

Protek was impressed by CyberFortress' capabilities and expertise.

"The combination of CyberFortress and Veeam was 75% faster to restore, and it took just five clicks to complete versus 30 minutes of a highly skilled tech's time. CyberFortress is now backing up all our on-prem servers. Having the peace of mind that backups are occurring behind the scenes, that we can recover quickly in the event of disaster - and that CyberFortress is standing behind us every step of the way - is a huge comfort."