ITRMS

Protecting against ransomware attacks and preventing lasting damage with NeuShield Data Sentinel

Ransomware has become one of the biggest threats in cybersecurity over the past few years, from large companies and city governments to even the smallest of organizations; no one is immune. Traditional ransomware protection is often ineffective in stopping new or unknown attacks, resulting in devastating impacts on the victim organization. Recovery from an attack is also becoming increasingly difficult. While victims may try to pay to recover their files, there is little guarantee that it will work. Meanwhile, traditional security and storage methods don't provide the ability to quickly and effectively restore lost data as a result of an attack.

About ITRMS

Founded in 1985, ITRMS, is a managed service provider (MSP) based in Southern California, specializing in providing businesses focused IT consulting and IT support solutions for small to mid-sized organizations. ITRMS' customers are typically companies with several servers and 10 to 20 clients, that have critical IT needs but do not have their own IT support function. In addition to IT support services, ITRMS provides a broad range of other services including, SEO, web design and disaster recovery. Through a variety of service offerings, ITRMS empowers clients to be successful, by leveraging technology to help achieve their business goals.

When we spoke with David Macias, President of ITRMS, he shared from personal experience two ransomware attacks on both his own organization and a client, before discovering NeuShield and the NeuShield Data Sentinel product.

After experiencing the ransomware attack on his client, Macias began researching for solutions but

was frustrated to find that the primary players in the space did not have a solution he felt was adequate. Luckily, just days after the attack on his client Macias participated in a webinar where he learned about NeuShield.

After meeting with NeuShield and getting a demo of the product, he was convinced that the NeuShield Data Sentinel product was one-of-a-kind and the solution he needed. Sealing the deal for Macias was the fact that NeuShield was able to demo their product using some of the actual ransomware code that Macias had saved during the attack on his customer. He described the

experience as, “truly incredible to see NeuShield in action and to see that if I had this solution during the recent attack, it would have been a simple one click restore of everything back to normal.” NeuShield quickly became his go to solution for ransomware protection for his own organization and his clients. “After seeing how effective it is and how easy it is to recover with NeuShield, I began to recommend it to all of my clients. NeuShield Data Sentinel truly lives up to its claims and performs just as it is designed to.”

Firsthand Experience with the Threat of Ransomware

David Macias has experienced the upsetting and frustrating reality of ransomware firsthand. As a seasoned, tech-savvy, IT professional David was not immune to the increasingly sophisticated attacks. In the course of supporting one of his clients, he found his network infected with ransomware. Luckily, he was able to quickly recognize the issue and limit the damage to his network and connected workstations, but even the quickest of reactions can’t prevent the significant damage inflicted by ransomware in a matter of seconds after infection. As Macias explained, the moment he discovered his network had been infected and his data encrypted by the ransomware, “I saw it happening right in front of my eyes, within 20 seconds three terabytes of data were encrypted. Just like that.”

In another experience, Macias remembers getting a call early one morning from a client that was confused and concerned that he couldn’t access his server. Macias immediately initiated a remote session and saw the hacker had compromised a remote desktop port and could see the ransomware actively attacking the network and the connected workstations. By the time network cables could be disconnected the server was completely encrypted along with several workstations.

The ensuing recovery from these attacks was difficult. Fortunately, in both cases the encrypted data had been appropriately backed up and protected. However, in his client’s experience, the ransomware had encrypted the full drive, even the recovery partition. In that scenario, no amount of backups will solve the need to start from scratch and painfully rebuild everything from backups. This is a long and tedious process that can take weeks to months, depending on the circumstances.

If there is one thing Macias learned from these experiences is that recovering from a ransomware attack is a long, tedious and costly process. A process he never wants to go through again. Macias tries to educate his clients about the potential cost of a ransomware attack, but finds that many companies don’t appreciate the potential magnitude of the impact and they are overwhelmed by all of the different preventative up-front costs in IT security. Macias views it as insurance and an investment that can save many multiples of the service’s cost. He says “the overall feeling that I get from a lot of clients that haven’t seen it firsthand, is that they will worry about it when it happens. That's a very dangerous mindset. If you consider all of the potential costs, from time and resources to rebuild and lost sales or operational costs from downtime, ransomware

protection is an investment that will have tremendous ROI."

The Solution

Cybercriminals show no signs of slowing down and attacks are getting more and more sophisticated by the day. The only way that companies can protect themselves from the full array of cyber-attacks is to deploy a 3-point solution. According to Macias, "there are three key elements to cyber defense. First, we use intelligent anti-virus and anti-malware systems to detect and stop known malware and viruses. Next, we ensure that clients have an appropriate backup solution and disaster recovery plans to protect against an earthquake, fire or other disaster. Finally, NeuShield is the critical line of defense against ransomware, that together with the other points, creates a full-proof defense. The key feature of NeuShield is the ability to restore things back to the current state, with a simple click of a button. Without this capability, ransomware protection will fall short and will result in the need to spend hours to weeks recovering from backups. Ransomware is increasingly intelligent and is encrypting the boot record, which damages the entire system and you have to start from scratch."

Macias continued, "in today's world where ransomware is more and more common, companies both large and small need to have the ability to recover from an attack, quickly and easily, without the need to go to the backup system and perform a lengthy restore. NeuShield provides the quickest and easiest recovery and even has added cloud capabilities which gives you additional flexibility and also enables management from my central location without having to be onsite, which is essential for a managed service provider."

Traditional ransomware protection focuses on detection and blocking malware and viruses, but unless these systems have a 100% detection rate, which is increasingly rare with the growth of targeted zero-day attacks, there will still be ransomware that goes undetected and the traditional solutions will fall short. NeuShield solves this issue from a different angle, that isn't dependent on keeping pace with the new attacks that are developed daily. Instead, NeuShield's Data Sentinel makes an attacker believe they have access to a computer's original data files, but they are in fact only seeing a mirror image of them, which enables Data Sentinel to fully recover data, regardless of how or why it was changed. Even the most advanced Fully Undetectable (FUD) or zero-day ransomware doesn't stand a chance against NeuShield Data Sentinel, which provides true protection against these attacks with the ability to get back up and running, quickly, easily and without lasting damage to the system or data.

The NeuShield solution achieves this level of protection through the following features:

File and Data Protection, leveraging NeuShield Mirror Shielding™ to protect files, ensuring that you can instantly recover important data from any ransomware attack. In addition, it leverages Data Engrams™ which allow organizations to view and rollback to previous versions of a file. This ground-breaking technology does this without any additional disk space nor impact on endpoint performance.

Disk and Boot Protection, by monitoring the boot portion of the drive and raw disk access, NeuShield prevents ransomware and malicious programs, such as NotPetya, Bad Rabbit, and Shamoon, from taking over the boot process and stops wiper malware from erasing all data on the hard drive.

One-Click Restore, which makes it easy to undo the damage of a ransomware attack, allowing users to quickly regain access to the computer and files, where traditional security and storage methods fail. NeuShield removes known and unknown threats, restores systems back to a known good state, as well as recovers encrypted and corrupted operating system files.

Key Benefits for ITRMS and its Clients

After deploying NeuShield Data Sentinel at ITRMS, as well as at the client that suffered the ransomware attack, Macias has recommended NeuShield to all of his clients, “NeuShield gives you peace of mind that if something was to happen all you have to do is click a button and like magic you are back up and running.”

In addition to the superior features, Macias has found the support and collaboration with NeuShield to be superior to other companies, “NeuShield has been incredibly helpful, has given me a tremendous amount of council and their customer support has been A+.”

Finally, Macias has appreciated the ongoing development and enhancements to the product: “They have continued to improve their software, including the ability to do total restores from the cloud. The cybercriminals never stop and NeuShield is improving their product and staying up to date with the current needs in the market.”

Macias feels that when working with his clients that he has a partner in NeuShield that he can recommend with complete confidence, “Now I go to sleep every night with total peace of mind that if something happens everything is protected and I'll be back up and running in a matter of seconds without any worry that anything was compromised.”

About NeuShield

NeuShield, Inc. provides Managed Service Providers (MSPs) and IT managers with the perfect solution to ensure all their PCs and servers are fully protected against ransomware and other threats that could impact their business. NeuShield’s award-winning Mirror Shielding™ technology enables you to recover your data instantly, without relying on backup or rollback, from any kind of corruption, deletion, or encryption due to cyber threats. Your data will never be held hostage again. For more information on NeuShield, please visit http://www.neushield.com