


# THE SECRET TO WINNING THE WAR AGAINST RANSOMWARE

 **64%** of IT leaders #1 objective over the next 12 months is to improve data security for their organization.<sup>1</sup>

In May of 2021, one of the largest insurance companies in the U.S. agreed to a \$40 million payment to restore access to its systems following a crippling ransomware attack.<sup>2</sup> That eclipsed the highest ever attempted ransomware demand of \$30 million set only a year earlier. Make no mistake about it, ransomware is a war, and the stakes have never been higher. As in all war, there is growing collateral damage as hackers are now targeting critical infrastructure, stopping gasoline and jet fuel supply lines, shutting down hospitals and even disrupting food production.

## YOUR LAST LINE OF DEFENSE

In every war, there is always a last line of defense. They are the reserves which are thrown into battle at the very end to hold the line and save the day at all costs. When it comes to combatting ransomware encryption, that last line of defense is your backup system. Regardless of which malware strain you might fall victim to, your backup system can restore all the data that was lost during that frontal attack. It is the knight riding in on the white horse that restores your data, your applications, and the business operations that depend on them. The backup server today holds a new prominence within every enterprise. No longer should it ever be referred to as “just the backup server”.



The key to winning the war against ransomware is preparedness and that starts with properly securing your backup system.

## THE INITIAL BATTLE IS THE KEY

What you may not know is that there is a skirmish fought prior to the main battle. Before the initial ransomware attack begins, the perpetrators first target the backups. Their aim in this initial attack is simple, destroy your backup system. Whether that means deleting it, corrupting it, modifying or whatever, the attackers know that the one thing often standing between them, and a handsome payday is your backup system. That's why it must be protected. Ransomware organizations make it their business to understand how backup systems work. In many cases, they know the most popular vendors backup solution better than its customers.



While there are still amateur cybercriminals that rely on arbitrary phishing attacks to snag an unsuspecting victim, the more successful ransomware organizations don't blindly send an email with the intention of encrypting files minutes after they infiltrate a network. Instead, they perform reconnaissance, taking time to learn about your environment. One of the first objectives is to gain access to your backup system. They learn when your backup jobs run and where the data is stored. They can then determine the vulnerability of your backups. Your mission is to shut them out of these systems.

This isn't to imply you don't need a well-conceived multilayer cybersecurity strategy. You still need a next generation firewall solution to analyze, identify and eradicate known malicious or highly suspicious traffic from your network as well as other cybersecurity tools in your arsenal. A backup system will do little to remediate the aftermath of a data breach for instance. But regarding traditional ransomware encryption attacks, winning the initial battle may in the end, win you the war. In the classic book, *The Art of War*, the ancient Chinese military strategist, SunTzu states: "The supreme art of war is to subdue the enemy without fighting."<sup>3</sup> An impenetrable system is a big step to subduing a future ransomware attack. After all, these bad actors are like any other criminal. They want to get in, get out and move on to the next easy target.

## SECURE YOUR BACKUP SYSTEM WITH BEST PRACTICE SECURITY

We recently asked our subject matter experts in backup technology to create an outline of best practices to help organizations fully secure their backup failover systems. We will use Veeam in our examples, but many of these practices will apply to any modernized backup system on the market today.

### 1. Don't virtualize your backup system

Yes, by and large, there are huge advantages to virtualizing your servers, but there are some exceptions, and your backup server is one of them. Think about it. The bulk of your servers are virtual, which means the attackers are going to seek out your VM environment to encrypt the data stores. If you have a VMware environment, they will take out your vCenter server as well as the encompassing ESX servers. If your VM environment is out of commission, then so is your backup server. To shield

your backup system from your virtual environment you should consider installing Veeam Backup Replication (VBR) along with its SQL DB on a physical server. It should be hosted in an isolated zone along with strict firewall policies. Another option would be to host it in the cloud and have it connected through a VPN tunnel.

### 2. Don't join your VBR server to the active directory

Admin rights are the keys to the kingdom and the key to taking out your backups. There are so many ways to gain access to AD accounts. Once an AD admin account is compromised, the attackers have full uninhibited rights to your backups. Only use a local administrator account for your VBR that uses a 20-character complex password for maximum security.

### 3. Avoid RDP when accessing your backup server

Admins love to RDP into their servers. The problem is that if hackers have penetrated your network to do reconnaissance, you are opening yourself up by constantly connecting to your critical machines while they quietly observe. Hackers have a variety of methods to exploit RDP connections. That's why Veeam has offered its own remote console software for years that installs on your managing client device. The remote console should be the primary way that you always access the VBR. The only time you should ever remote into the actual server hosting your backup system is to manually run updates and patches.

### 4. Use multifactor authentication

Many companies use multifactor authentication for their O365 accounts, yet still rely solely on password protection for some of their most critical servers. If your backup system has MFA (which Veeam does) then use it. Passwords alone should never be relied on.

### 5. Don't disable the local firewall within your backup infrastructure

We've all done it. Before installing a software application, we aren't familiar, we disable the local firewall on the hosted server to make the implementation go smoother. We then get distracted and vow that 'someday' we will enable the firewall again. That someday often never comes, and if it does, it is often after an attack has already taken place. Take the time to



find out the required ports for your backup architecture and configure all involved local firewalls according to best practice.

## 6. Use a secure repository

For the same reasons why, you shouldn't use a VM as your backup server, you should use a separate repository to store your backup files. Don't backup your SAN and then store the backups on the same SAN. You should also refrain from using a NAS or Windows repository as these can be more easily exploited.

## 7. Create a recovery checklist

If hackers manage to take out elements of your infrastructure, then you will first have to rebuild it in order to restore your backups. This is where a recovery checklist comes into play. In case your DNS infrastructure is taken out or can't be trusted, you need to know the IP addresses of all your critical infrastructure components. If your vCenter is no longer accessible, you need to know the root passwords of your ESX servers. You should also not rely on a password manager running on a VM. In the event that someone either intentionally or inadvertently deleted your elements of your backup architecture, you need to know the location of your Veeam backup configuration database as well as the

passwords to your repositories. Because you don't utilize this type of information every day, its easy to forget.

## CONCLUSION

Sun Tzu also said, "Every battle is won or lost before it is ever fought." The key to winning the war against ransomware is preparedness and that starts with properly securing your backup system. That assumes you have a modernized backup architecture that can accommodate these best practices as well as additional proprietary features specifically designed to protect against ransomware. If you would like more information to win the battle before it is ever fought, contact our subject matter experts at WEI who can sit down with you, analyze your current backup environment, and suggest a course of action. WEI wants you to consider us as a valuable ally in this war that must be won.



## TALK TO WEI TODAY

**Contact the security experts at WEI to find out how you can win the war against ransomware hackers.**

### Sources:

1. IDG Research commissioned by WEI, January 2021.
2. CNA Financial Paid Hackers \$40 Million in Ransom After March Cyberattack - Bloomberg
3. Sun Tzu - Wikipedia

## ABOUT WEI



**WEI is an innovative, full service, customer centric IT solutions provider.**

**Why WEI? Because we care. Because we go further.**

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 30 years.



info@wei.com

www.wei.com

43 Northwestern Drive | Salem, NH 03079

800.296.7837