arcserve®

How Data Protection Modernization Helps You Defend Against Ransomware, Malware, and Other Data Disasters

Table of Contents

Data Protection Modernization: Why Your Business Needs to Adapt

Data is the backbone of any modern business, and it's more critical than ever to ensure your data is always protected and available. However, as technology evolves, traditional data protection methods have become outdated and less effective.

Gartner predicts that by 2023, 65 percent of the world's population will have its personal information covered under current privacy regulations, compared to only 10 percent in 2020. Meanwhile, the amount of data is expected to reach 175 zettabytes by 2025, a 61 percent CAGR. With this explosion of data, traditional data protection methods can't keep up with more stringent data privacy requirements.

Data protection modernization ensures your business can keep pace with ever-evolving technologies.

Modernization Eliminates the Need to Rip and Replace

Traditional data protection methods often require a complete overhaul of your organization's infrastructure to adapt to new threats as they appear. That's a costly and disruptive process. With data protection modernization, you can update and enhance your systems without the need to rip out and replace them, so you can continue using your existing procedures and processes. That saves time and money.

So, what should you do to modernize your data protection, backup, and disaster recovery efforts? Here are several vital steps that you can take:

Assess and Update Your Data Protection Strategy

Scrutinize your current data protection systems, processes, and infrastructure. Identify any areas that may be lacking or need improvement and put a plan in place that closes gaps that may expose vulnerabilities. Once you clearly understand your current landscape, develop a plan for modernizing your data protection efforts that align with your specific business needs and goals. That includes setting recovery time objectives (RTOs) and recovery point objectives (RPOs) that ensure your business will survive any disruption and get back in operation quickly.

Invest In Modern Data Protection Solutions

One of the essential steps in data protection modernization is investing in modern data protection solutions like Arcserve Unified Data Protection (UDP). Arcserve UDP protects your physical, virtual, and cloud-based workloads. With its comprehensive feature set, Arcserve UDP gives you a wide range of data protection, backup, and disaster recovery capabilities, including data deduplication, encryption, and easy disaster recovery testing.

Continuously Monitor and Improve

Data protection is an ongoing process. Once you've put modern data protection solutions in place, it's crucial that you monitor and improve your data protection efforts continually.

Working with a managed services provider (MSP) can relieve limited and overburdened IT teams of the time and effort involved with keeping doing so. They can also keep your systems current while bringing specialized expertise to enhance your cyber defenses and strengthen your data resilience.

Arcserve's modern data protection solutions, combined with our technology partners' expertise, help you navigate this evolving landscape, giving you a flexible and cost-effective way to protect your critical data. You'll find a list of Arcserve expert technology partners, including MSPs, here. To learn more about Arcserve solutions, check out our on-demand demos.

More Vice Society Ransomware Attacks in the News: 7 Ways to Ensure Your Data Is Safeguarded and Resilient

The Vice Society ransomware gang made headlines again. In late December, threat researcher SentinelLabs posted that the well-resourced ransomware group has adopted a new custom-branded payload in recent intrusions, dubbed "PolyVice." The story notes that Vice Society is selling similar payloads to other groups, which implement a robust encryption scheme using NTRUEncrypt and ChaCha20-Poly 1305 algorithms.

While Vice Society was once considered a threat mainly to large organizations—it was behind the damaging attacks on Colonial Pipeline and JBS meat processing in 2021—the group (and those that buy its ransomware) now targets just about every size and type of organization. Last September, we wrote about the Vice Society's involvement with the attack on The City of Palermo, Italy. More recently, its name has surfaced in attacks on a fire department in Victoria, Australia, and multiple schools in Gloucester, U.K.

Sophisticated Attacks Demand Unstoppable Defenses

Vice Society is just one of many sophisticated ransomware groups that would love to break in and steal your data. And they have plenty of tricks up their sleeves, from phishing to exploiting vulnerabilities in your hardware and software to gain access to your data.

While there isn't anything you can do to stop the attacks from coming your way, there are concrete actions you can take today. These ensure your defenses are as strong as possible and your data is always recoverable whether a ransomware attack, hardware failure, human error, or natural disaster hits you.

1. Keep Everything Up-to-Date

Patches and updates are crucial to closing vulnerabilities in your organization's software and hardware. But overwhelmed IT teams need to move fast to beat the bad guys to the vulnerabilities. So put a program in place that ensures patches are installed on receipt, and your systems are regularly reviewed to ensure everything is current.

2. Implement Robust Authentication and Access Controls

According to the Verizon 2022 Data Breach Investigations Report, the human element drives breaches, with the the two leading causes being stolen credentials and phishing—fake emails designed to steal private information by

masquerading as a trusted entity. Fight back by using multi-factor authentication (MFA) and role-based access controls (RBAC) to ensure that anyone requesting access to your networks and data is who they say they are.

3. Educate Your Employees

In this post, we shared eight ways employees can help reduce the risk of ransomware. That's a great place to start. Most importantly, train everyone, from the C-suite down, to spot malicious emails and websites and the steps they need to take when encountering something suspicious.

4. Update Your Disaster Recovery Plan

Nothing would be worse than to have a disaster strike only to find the plans you made for dealing with it are out of date. So dust off your disaster recovery plan and ensure it's current and supports your overall business objectives. That includes verifying that your RTOs and RPOs meet those needs. Then test your plan—regularly—so you know you can quickly recover no matter what comes your way.

5. Back Up Your Data to Immutable Storage

Even if you do everything we've listed above, all it takes is one click on a malicious link by an employee to let ransomware in and lock up your data. That's where immutable backups give you a last line of defense.

Solutions like Arcserve OneXafe use a file system based on an immutable object store, with every object written only once. These objects can't be altered or deleted, even by an admin. Any changes made to your file system result in the creation of new objects. And OneXafe continuous data protection (CDP) takes low-overhead snapshots every 90 seconds. So not only can you be sure that your immutable backups are always secure, but you can also return to a recent point in time following a disaster and recover entire file systems in minutes.

6. Consider Ransomware Insurance

The National Association of Insurance Commissioners reported that insurers wrote about $6.5 billion in direct written premiums in 2021, a 61 percent increase from the prior year. The report also notes that insurers have responded to a tough market where losses paid to customers exceeded projections, driving up premiums. These statistics tell us that companies are getting smart and paying the premiums, no matter how high, to cover what they now recognize as the potentially massive costs of an inevitable attack.

Insurers will likely require that you put effective data protections in place before you are underwritten. That's good because, while you'll be forced to invest more in modern data protection solutions, you'll also be able to rest assured that any losses you incur are covered.

7. Get Help From Ransomware Experts

Choose an Arcserve technology partner to help you select the best data resilience, protection, backup, and disaster recovery solution for your organization. Our partners bring deep expertise and experience to every client engagement. And check out our on-demand demos to see for yourself the robust data protections that Arcserve solutions deliver.

3 Steps Every Organization Should Take To Defend Against Wiper Malware

Wiper malware is an alarming threat to your organization's data. Unlike ransomware, which can encrypt and disable your files until you pay a ransom, wiper malware aims to delete your data permanently and cause as much destruction as possible. Once it infects your system, it will make your data completely unrecoverable. This type of malware is hazardous because there is no possibility that you can recover by paying a ransom.

Wiper malware has grown more common in recent years, with several high-profile attacks making headlines. The destructive WannaCry attack in 2017, which affected hundreds of thousands of computers worldwide, is believed to have been a wiper attack. Other recent notable wiper attacks include Olympic Destroyer, which targeted the Winter Olympics in South Korea in 2018, and ZeroCleare, which targeted the energy and industrial sectors in the Middle East in 2019. Even the infamous Sony Pictures hack was a wiper attack.

It's Not Just Criminal; It's Cyber Warfare

Today, wiper malware is a cyber warfare weapon. As the conflict between Russia and Ukraine continues, Ukraine has seen a withering barrage of wiper attacks. Recently, researchers at Fortinet reported that cybercriminals deployed wiper malware against other countries. In the first half of 2022, seven new wiper variants were used in campaigns against private, government, and military organizations. Indeed, there have been wiper malware attacks in 24 countries other than Ukraine, with some of these attacks targeting critical infrastructure using disk-wiping malware.

One of the fundamental challenges in dealing with wiper threats is that they're very often difficult to detect and contain. Unlike other forms of malware—which usually make their presence known—wipers erase all traces of themselves once they have completed their destructive work. That makes it difficult for IT security professionals to respond to these attacks and prevent them from spreading.

Your organization must implement robust, multilayered security measures, including regular backups of critical data to defend against wiper threats. It's also essential to maintain a strong security posture and be alert to signs of a potential wiper attack.

Here are three steps your organization can take to minimize your risk of falling victim to these destructive attacks.

1. Back Up Your Data

The importance of backing up your data can't be overstated when defending against wiper malware. While backups can't prevent an attack, they provide a lifeline for restoring data compromised by wiper malware—or any other type of attack.

By properly managing your backups, you can ensure copies of your data are stored separately from your production systems. Should wiper malware, ransomware, or any other malware strike your active IT environment, you can turn to your backups—stored on an immutable storage solution—for restoration. Not only is restoring from backups more cost-effective and faster than paying a ransom to recover data, but it's likely your only recourse in a wiper attack.

2. Follow the 3-2-1-1 Rule

A 3-2-1-1 data-protection strategy is a best practice for defending against malware, including wiper attacks. This strategy entails maintaining three copies of your data, on two different media types, with one copy stored offsite. The final 1 in the equation is immutable object storage.

Let's break down the advantages of the 3-2-1-1 strategy.

By maintaining multiple copies of your data, you can ensure that you have a backup available in case one copy is lost or corrupted. That's imperative in the event of a wiper attack, which destroys or erases data permanently, causing as much destruction as possible.

Storing your data on different media types also helps protect against wiper attacks. For example, you might keep one copy of your data on a hard drive, another at a cloud-based storage service, and the third on a removable drive or tape. This way, if one type of media is compromised, you still have access to your data via the other copies.

Keeping at least one copy of your data offsite—either in a physical location or in the cloud—gives you an additional layer of protection. If a wiper attack destroys onsite copies of your data, you'll still have access to your offsite backup.

The final advantage is immutable object storage, where continuous snapshots are taken of your data every 90 seconds, ensuring that you can quickly recover it even during a wiper attack. This next-generation data security tool helps safeguard your information and protect it from loss or damage.

3. Air Gap Your Networks

Air gapping is an efficient and effective method for protecting backup data against wiper attacks. There are two types of air gapping: physical and logical. Physical air gapping involves disconnecting a digital asset from all other devices and networks and physically separating that asset from your secure network and any other computer or network. You can store backup data on media such as tape or disk, then completely disconnect these media from your production IT environment.

Logical air gapping, on the other hand, relies on network and user-access controls to isolate backup data from the production IT environment. Data is pushed to its intended destination, such as immutable storage or a custom appliance, via a one-way street and can only be managed or modified through separate authentication channels.

The beauty of air gapping is that it renders your data virtually invisible to wiper malware attacks, making it nearly impossible for the bad guys to compromise your backups.

Final Takeaway

The increasing spread of wiper malware in the wild is a stark reminder of the dangerous landscape organizations face when protecting their data. A solid, well-managed data backup and recovery plan is the key to ensuring your data is secure in the face of today's growing threats. No matter what tactics cybercriminals may use to disrupt your access to your data, a robust backup and recovery plan will keep your data secure.

Get expert help building your defenses and deploying a data resilience strategy by choosing an Arcserve technology partner. To learn more about Arcserve products, check out our on-demand demos.

How to Protect Your Business From Ransomware at the Edge

It's rare for an enterprise to meticulously organize its data in a single data center. The need for redundancy, performance, compliance and business continuity has resulted in most enterprises having multiple data centers. One global IT survey found that 33 percent of respondents said their company operates between three and five owned or collocated data centers.

While multiple data centers can create complexity, remote office/branch office (ROBO) environments—often essential to growing a business—bring even more challenges. Keeping these edge environments secure from ransomware isn't easy because you'll rarely have technical staff on hand, and these offices may be far from your primary data centers.

So what can you do to keep your edge ROBO environments safe from ransomware when that's the case? Here are four tips for IT admins to help stop ransomware everywhere in your organization.

1. Start With Ransomware Prevention

As with all of your data centers, start by ensuring you have basic ransomware prevention measures in place. That can include firewalls, spam filters, anti-malware, and antivirus tools. Be sure all software is kept patched and up to date. And consider buying ransomware insurance or increasing your coverage to include new locations.

Most importantly, ensure your remote employees understand how to recognize and react to potential ransomware attacks. That includes spotting risky emails and phishing scams that could result in a ransomware attack and the steps they need to take if an attack is successful.

2. Create a Strategy for Remote Backup and Recovery

It isn't always possible to protect remote networks from ransomware. That's where a robust backup and recovery strategy makes all the difference by ensuring your business can get back up and running if your systems get locked down.

You also need to establish recovery objectives—your RTOs and RPOs—for each location. How much data can a particular location afford to lose (RPO)? How much downtime is acceptable (RTO)? You need to deploy solutions at these locations to meet these objectives and protect your data.

3. Understand ROBO Data Protection Essentials

Once your goals are set, it's time to choose the best solution based on these ROBO essentials:

Flexible Backup

The solution should back up virtual and physical machines, store those backups locally, and easily replicate them to the cloud.

Recovery Options

You need options when recovery is required. Your selected solution should give you flexible, fast recovery options that make it easy to recover your data locally at the ROBO site or from the cloud, depending on a disaster's severity.

Remote Management

You likely have multiple remote offices or branches, and each may have its own capabilities and recovery objectives. Your solution should include effective management tools that your IT team can use to handle each location's unique requirements from anywhere. And it should allow your admins to remotely deploy different policies in different locations.

4. Choose Appliances to Support Advanced Disaster Recovery

Backup appliances are often used at ROBO sites that don't have resources or technical staff to manage servers. That lets admins deploy backup and disaster recovery solutions without the need to be onsite. Anyone from the branch can plug in the device and connect it to the internet.

From there, your admins can remotely protect data by setting up backup schedules and retention policies. If a hardware failure or minor disaster strikes, your admins can use the device for instant failover. And because you can replicate data from the appliance to the cloud, a ROBO location can even spin up its entire site in the cloud should a big disaster bring it down.

Don't Be Ravaged By Ransomware

ROBO environments are particularly vulnerable to data loss and downtime because they lack technical staff onsite to keep their systems humming. Add in the growing threat from ransomware, and admins have their work cut out for them. Fortunately, backup and disaster recovery appliances like Arcserve OneXafe make it easy for admins to prevent data loss, even when they can't be onsite.

To get help ensuring your data is protected even in ROBO environments, talk to an expert Arcserve technology partner. And be sure to check out our free on-demand demos.

Need Answers?

Arcserve is always here—standing by and ready to help.

arcserve®

+1 844 639-6792

arcserve.com