# Protecting The Backup: The New 3-2-1-1 Rule

Ransomware attacks are becoming so common that today's enterprises need to realize it is no longer a matter of "if" but "when" they are targeted. In a recent 2021 report*, tech market analysts IDC said their research shows that more than 90% of organizations have been attacked by malware/ransomware. More than 80% suffered a successful malware attack.

This requires a new mindset: preparing for inevitable breaches while also planning a way to return to normal operations as quickly as possible. For mid-market and enterprise customers, ransomware has changed the game—but new rules and new solutions can keep them ahead of the threat.

## The New Target: Backups

In their report, IDC identified the evolving threat to backup data. Cybercriminals know that attacking backup data first cuts off the enterprise from eluding an attack by restoring from uncompromised data. With backup data breached, they then move on to primary sources of data at the scale and pace they wish.

Ransomware organizations exploit flaws in detection systems to deliver their malware—and their methods are becoming more sophisticated. Typical of the cat-and-mouse game played out in cyber security is the way some monitoring software looks for unusually high I/O activity in disk drives to spot unwanted encryption. Ransomware gangs can respond by slowing the encryption. They also use the strategy of triggering an attack long after the breach, beyond the period of retention cycles.

The report notes that there are some key reasons why some enterprises fail at backup protection. Some do not prepare their recovery processes and plans well enough. Other are turning to a disaster recovery (DR) response. Unfortunately, according to IDC, few organizations are protecting all their application data, leaving them partially vulnerable to data loss.

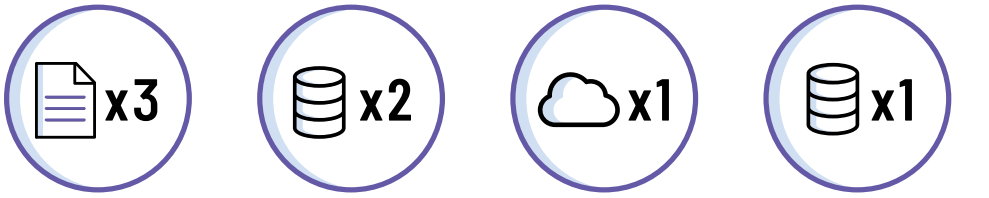
## Welcome To The 3-2-1-1 World

Many in IT may be familiar with the old "3-2-1" rule when it comes to data protection: Three copies of data (primary and two backups); two copies stored locally on two formats (NAS, tape or local drive); and one copy stored offsite (cloud or secure storage). But now due to the importance of protecting the backup, the new rule the IDC report recommends is 3-2-1-1 – with the extra "1" being immutable storage.

Immutability is a key element of successful ransomware protection. Immutability is when data is converted to a write-once, read many times format--which cannot be altered. Unlike data encryption, there is no key, so there should be no way to "read" or reverse the immutability. Immutability is also key when paired with other data protection elements, such as continuous data protection, which can capture data on each write at very quick intervals measured in seconds. If that data is then stored in immutable form, the customer can then have a "snapshot" of data which cannot be altered. Enterprises with the right technology and good restore and recovery practices can access unaltered data within minutes of a breach.

*IDC Perspective: To Thwart Ransomware, Protect the Backup First by Using Five Key Elements. 2021 IDC. https://cdn.idc.com/getdoc.jsp?containerId=US47666321

**Best practices in data protection now incorporate a 3-2-1-1 design:**




Create 3 copies of your data
(1 primary and 2 backups)

2 stored locally on at least 2 types of storage media
(local drive, NAS, tape, etc.)

Store 1 of these offsite
(secure storage, cloud, etc.)

1 copy on immutable storage
(on OneXafe appliance or in the cloud)

## New Solutions

There is no single silver bullet to kill the ransomware threat. A multi modal approach is still the best strategy. In the real world, VARs are often working with customers that have a mix of technology, solutions and vendors. Heavily siloed approaches can lead to the kind of gaps that cyber criminals can exploit.

The good news is that new technology and solutions can be mixed and matched to meet customer needs. At the intrusion detection and prevention phase, new solutions are using deep learning neural nets to detect known and unknown threats. In the response phase, some solutions use behavioral analysis to stop never-before-seen ransomware attacks. In the data protection and recovery phase, solutions exist that combine immutability and continuous data protection, such as the OneXafe 4400 series, a new addition to Arcserve.

## Focusing On Business Continuity

A continuum of solutions that covers the whole range of customer needs is difficult to find. Arcserve's recent merger with StorageCraft creates the kind of portfolio of solutions that give enterprises a clear path to business continuity. Whether it's an appliance-based solution that combines immutability such as the OneXafe 4400 series, or intrusion detection that uses neural net technology, such as, Sophos Intercept X Advanced, these are the kind of solutions needed to meet today's changing and evolving threats.

One thing is certain: the ransomware and malware threat to data backups is not going away. By focusing on business continuity, VARs can gain a seat at the table with clients when it comes to process, people and solutions. That's a key differentiator for VARs—and good for the customer as well.

# Take the Next Step

**Find out more at arcserve.com or contact us at +1 844 639-6792.**

## About Arcserve

Arcserve, a global top 5 data protection vendor, provides the broadest set of best-in-class solutions to manage, protect and recover all data workloads, from SMB to enterprise and regardless of location or complexity. Arcserve solutions eliminate complexity while bringing best-in-class, cost-effective, agile, and massively scalable data protection and certainty across all data environments. This includes on-premises, cloud (including DRaaS, BaaS, and Cloud-to-Cloud), hyperconverged, and edge infrastructures. The company's nearly three decades of award-winning IP, plus a continuous focus on innovation, means that partners and customers, including MSPs, VARs, LARs, and end-users are assured of the fastest route to next-generation data workloads and infrastructures. A 100% channel-centric organization, Arcserve has a presence in over 150 countries, with 19,000 channel partners helping to protect 235,000 customers' critical data assets. Explore more at arcserve.com and follow @Arcserve on Twitter.