Dr.Backup™
data protection service

Is Your Antivirus Software Like an Old, Battle-worn, Set of Boxing Gloves…Ready to Go Down for The Count?

In its heyday, it fought the good fight. But today's opponents are faster, nimbler and don't play by the rules.

If you own or operator a business that relies heavily on traditional antivirus products to protect your workplace computers…

You're literally a "sitting duck" for the next cyber-attack!

Dr.Backup™
data protection service

Because it takes only one misstep, by one employee, to bring your business operations to a grinding halt.

Each day 500,000+ malware variants ("viruses") are reported worldwide. This includes "zero-day" exploits never seen before.

Under this load, traditional signature-based antivirus products simply don't have a chance.

Even newer artificial intelligence-based security can't adapt quick enough to prevent all cybercrime.

But you don't need to sit around waiting to get "knocked out."

Because now, there's a painless way to say GOODBYE to the threat of ransomware…and say HELLO to a less stressful computing experience!

Imagine not having to worry about a single unintended click, a malicious email attachment, or a moment of carelessness on the web…

Causing major data loss.

It's actually never been easier to protect YOUR business from a computer data breach…

Using the same technology that large commercial, municipal and military organizations worldwide are RUSHING to implement…

But at a fraction of the cost they will invest!

Dr.Backup
data protection service

The good news is:

Zero Trust Security Filters are now an integral part of the Dr.Backup *B3 Data Protection Service*.

And this powerful technology can be rapidly deployed in your workplace -- by data protection experts that businesses have trusted for over 20 years!

Here's how it works.

With your team's cooperation, our technicians remotely install a Zero Trust security agent on each of your Windows computers.

This generally takes 5 minutes per device.

After installation, these agents "watch and learn" the applications you use.

This learning process generally lasts 2-3 weeks.

The data being gathered helps to create "white lists" -- which are the foundation of Zero Trust protection.

Next, security filters are activated on your computers. This means that going forward, only previously registered applications can execute.

Should an attempt be made to start ANY application NOT in the security filters -- it will initially be blocked.

This ensures ***system integrity is preserved..***.

But a blocked application will cause a pop-up support form to automatically appear on the PC screen -- so the user has an option to request technical assistance.

In this way, security experts can help review, and if appropriate, add new applications to Zero Trust Security Filters in near-real time.

And in case you're wondering…

Windows updates and revisions to widely-used business software, are routinely updated in your security filters by our team.

This keeps computers safe – without creating an undue burden.

Over time, you'll gain confidence in the "trust nobody" approach to data protection…

And consider Zero Trust as an indispensable component of your computing infrastructure.

But hey…I already back up my data…isn't that enough?

EVERY DATA PROTECTION PLAN SHOULD ABSOLUTELY START WITH A RELIABLE BACKUP PROCESS…

Since NO security solution is 100% perfect.

And, the only way to retrieve data loss from fire, flood, theft, equipment failure and human error is using your backups.

Dr.Backup™
data protection service

However, Zero Trust is a NEW and DIFFERENT type of data protection.

It's a loss *PREVENTION* tool and the perfect *COMPLEMENT* to any backup service.

Think about it this way:

An ounce of prevention is worth a pound of cure when it comes to fighting cybercrime.

Using backups to recover data from a ransomware/malware attack is ALWAYS going to be a disruptive and time-consuming effort…

So why not avoid the pain and lost revenue caused by downtime?

Besides, even if you do restore your files…

"Bad actors" will likely upload your data to the "Dark Web" for sale.

Now, you run the added risk of exposing your trade secrets and customer information to the world…including your competition!

With Zero Trust Security Filters installed on all your PCs and Servers, you prevent the bad guys from running their ransomware encryption and extraction software.

This dramatically cripples their ability to victimize you!

Zero Trust Security Filters are the same technology we use internally to protect staff PCs – and now it can protect you too!

Dr.Backup™
data protection service

For more details…

Schedule your confidential call with a security specialist today!

https://drbackup.net/request-a-call-back/