

5

Ways You Can Kick Ransomware to the Curb for Good in 2022.

Stop losing the battle with ransomware in 2022. We'll show you how it's done.

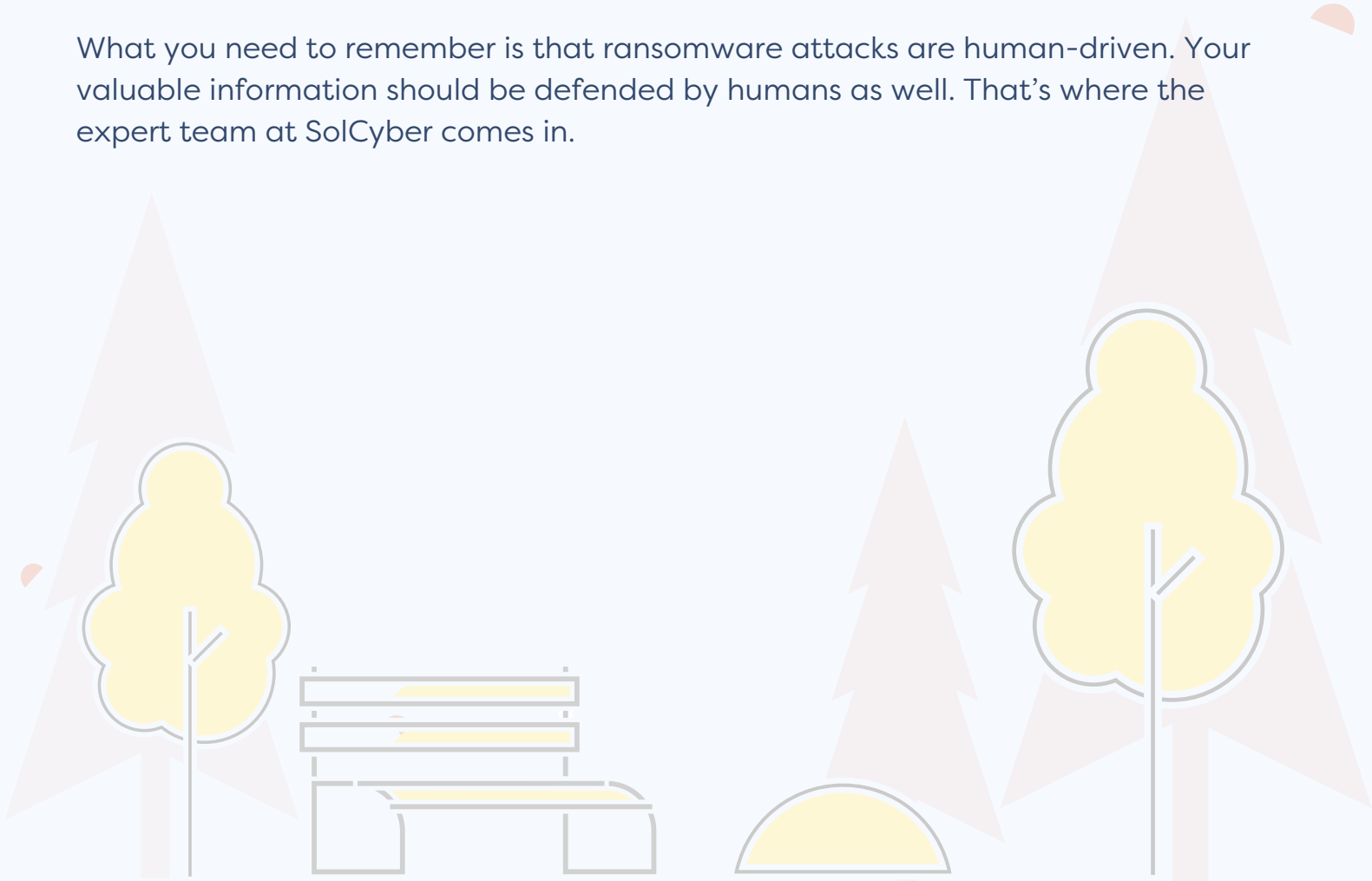


You know the problem. You've seen the stats. And you are probably as tired of hearing about it as we are. So how about we try and make it go away in 2022 together.

Unfortunately, it is still here now, and you can't just eye-roll your way out of this one and sweep it under the rug. So let's get proactive and nip these attacks in the bud.

The fact is, ransomware attacks are **becoming the primary threat to most organizations**. Your cyber security provider must have a plan of action for defending against ransomware attacks.

What you need to remember is that ransomware attacks are human-driven. Your valuable information should be defended by humans as well. That's where the expert team at SolCyber comes in.



Check The Facts — Ransomware Is Coming For You

Think ransomware isn't a threat to your organization? Think again. Take a little gander at these numbers...

- **60% of small businesses** close up shop after being hit with a cyber attack.
- **37% of organizations** were affected by ransomware attacks in 2021, **54%** of whom said the cybercriminals succeeded in encrypting their data.
- The average ransom paid by mid-sized organizations was **\$170,404**.
- The average bill for rectifying a ransomware attack, including downtime, people time, device cost, network cost, lost opportunity, ransom paid, etc. was **\$1.85 million**.
- The average downtime a company experiences after a ransomware attack is **21 days**.

The proof is in the pudding if the pudding is the livelihood of your organization. Protect your neck or lose it! Metaphors gone wild, the threat is real. And what you're currently doing to safeguard your business probably isn't enough.

Why The Current Choices Won't Cut It

Sadly, there's no silver bullet for ransomware protection. A firewall and endpoint protection just isn't going to cut it anymore. What you need is a combination of better controls, a breadth of technologies that work together, and active detection and response.

Does such a thing exist?! It does. We'll get to that in a minute. Patience!

The problem is, most of today's vendors will try to sell you technology and expect you to operationalize it. News flash! It ain't working. There will be gaps in your protection, and ransomware attackers are savvy enough to find them.

Today's ransomware attacks are human-driven, meaning there is a real person behind the keyboard who is an expert at hacking your data and holding it for ransom. These people know how to seek out vulnerabilities within your highest-impact resources. The result could be catastrophic to your business.

In response, you need a human on your end with the expertise to match. The good news is such humans exist with a beast of a tech suite behind them.

You don't have to settle for partial security. You shouldn't need to try and figure out the complexities of cyber security on your own or hire a team to help you. You just need SolCyber.

Consider The SolCyber Approach

We just said it, but it bears repeating: Patching together a solution is way too complicated to figure out on your own. You'll waste tons of your valuable time and budget trying to make all the pieces fit and will inevitably end up with gaps in your security. It's not your fault — it's really complex!

What you need is an end-to-end approach to ransomware from a single provider. Say hello to the modern MSSP — SolCyber.

SolCyber offers the perfect blend of technology and human care. The service includes a ready-to-integrate tech stack and a knowledgeable team to manage the system.

Our curated set of technologies will help prevent, detect, and respond to advanced threats across the entire kill chain. The SolCyber platform extends beyond just technology, it includes protection for your weakest link — your employees. And it's not just a one-time fix — you get a continuous assessment and feedback to improve your security posture over time.

With traditional/DIY cyber security options you:

- Focus only on endpoints but leave gaps in visibility where attackers can sneak past.
- Need to have the right people in place to make it work. See also: hiring full-time IT/cyber security staff – they're expensive!
- Stress about your security. A lot. Circle back to constant nagging insecure questions like "Is it even working?! Did I do it right?!" Answer: Probably not!

With SolCyber, you get to enjoy:

- Included next-generation technology
- A simple, predictable per-user pricing model
- Better value, better service
- Peace of mind. Yes, it's working 24/7. Have a question about something? A real, knowledgeable human will answer the call

Reasons You Need SolCyber

- Save yourself/your company a hell of a lot of time and money
- Deliver some actual return on your investment in the form of unparalleled security and service
- Incredibly fast, cost-effective security (see the theme here?)
- Range of extended services to fit your unique needs
- Real-time visibility, no blind spots, and continuous updates

This list could be endless but we'll cut it off here for now. Want more? Talk to a member of the SolCyber team and we'll walk you through our incredibly fuss-free solution.

The SolCyber Promise

No silver bullets, no BS, just amazing security, approachable humans, and incredible value.

Let's work together and in 30 days, you'll be ransomware resilient.

Get protected today

Need any help or
have any questions?
Fire away!

