



# Prepare Now or Pay Later

Shield Data & Secure Continuity With  
Data Protection Services (DPS)



Companies that proactively deploy security AI and automation save an average of

**\$3.8 million**

to recover from a cyber breach, compared to companies that do not.<sup>1</sup>

## After a Cyber Attack, You Don't Want Just To Survive. You Need To Thrive.

Data Protection Services (DPS) help mitigate the operational impact of cybercrime. With DPS, you get:

- Not just protection; minimize or eliminate downtime & data loss to ensure continuity
- Centralized monitoring & management to streamline risk mitigation & regulatory compliance
- Modernized & automated IT to ensure 24/7/365 coverage



# Be Prepared. Cybercrime is Everywhere.

You probably know your way around town pretty well. But it helps to have a map handy to guide you to shortcuts and detours when you come across a roadblock. A good map on hand keeps you moving when the going gets tough. When it comes to cyber security, the path has never been tougher, as organizations in every type of industry are running into mounting cyber challenges – and too often are driving blind.

**600%**

Increase in malware attacks during COVID-19 pandemic.<sup>2</sup>

**4,000**

Number of ransomware attacks reported daily in the United States.<sup>3</sup>

**4%**

Of IT decision-makers believe ransomware attacks are too sophisticated for their teams to handle on their own.<sup>4</sup>

**Only 1 in 10**

Companies proactively address cyber risk reduction.<sup>5</sup>

**16 days**

The average amount of time it takes an organization to restore networks following a ransomware attack.<sup>6</sup>

**\$6 trillion**

Projected global cost of cybercrime in 2021.<sup>7</sup>

Many industries we all rely upon are everyday cybercrime targets, including:

- Insurance & finance
- Telcom
- Manufacturing
- Healthcare
- Defense Contractors
- Local governments & first responders
- Schools and colleges
- Utilities

# Cybersecurity Myths vs. Facts

Think you're cyber secure? Let's separate some common assumptions from reality.

**MYTH** I'm safe! I have backup data.

**TRUTH** Backup data is much more vulnerable than popularly believed and may be locked up as part of a ransomware attack.

**MYTH** My operation is protected! I have all sorts of cybersecurity in place.

**TRUTH** You're interconnected to many third-party vendors and remote workers who may not be. How are you monitoring and securing them?

**MYTH** I have cybersecurity insurance; it'll cover everything!

**TRUTH** Insurers may balk at covering full financial losses, especially if you're not following best practices. Plus, how long can you afford to have an operational disruption?

**MYTH** We have an IT department. They can handle it themselves.

**TRUTH** IT departments are overworked, understaffed, and can use the assistance of specialized teams and tools. Think regular army + special forces.

These questions can help you start the cybersecurity discussion at your workplace. Questions to ask include:

- Do you understand the cybersecurity threat environment and what value you create is at risk?
- Are you struggling with understanding or meeting cybersecurity best practices or compliance requirements?
- Can you afford to suffer substantial downtime and operational disruption?
- When was the last time you had an objective third-party assessment of your organization's IT teams, processes, and technology?

# The Katalyst/Rubrik Team: Data Protection Services That Keeps Out Attackers & Keeps Up Operations

Cybersecurity is a team game. Just like Katalyst can team up with your team, we partner with Rubrik, a leader in zero-trust security and data immutability. Their know-how & tools effectively protect data from ransomware, natural disasters, and operational failures. That means your backup data is safe and can be easily accessed when you need to restore operations following a cyberattack quickly.

The Katalyst/Rubrik team gives you: challenges – and too often are driving blind.

- **Zero-trust for any circumstance by Rubrik**
  - No end-around for access; solid digital checkpoints at every step
- **No lockouts; 100% data immutability**
  - Absolute data accessibility to protect your operations, not just your assets
- **A recovery blueprint**
  - Not just protection, but a plan to quickly recover from attacks
- **One view to manage everything**
  - Centralized monitoring of threats, defenses, and compliance, all in one place
- **Simplicity and scalability**
  - Easy to use, deploy in less than 1 hour, and works with clients of all sizes
- **Lower Total Cost of Ownership (TCO)**
  - Savings of 20% or more over 3-5 years



# Protection and a Promise: The Rubrik Ransomware Recovery Warranty

With the rapid growth of ransomware attacks, enterprises all share the same concern: “If we get hit by ransomware, can we recover?” In an industry first, Rubrik, The Zero Trust Data Security™ company, announces a Ransomware Recovery Warranty of up to \$5 million for Rubrik Enterprise Edition.<sup>8</sup> This warranty will be available for customers running Rubrik’s Enterprise Edition and working with a Rubrik Customer Experience Manager (CEM) to ensure security best practices are in place. The warranty will cover expenses related to data recovery and restoration in the event that Rubrik is unable to recover protected data in the event of a ransomware attack. By partnering together we will reach the highest standards of data security excellence.

# At Your Ready: Katalyst's Team, Tools, & Talent

Our Katalyst team is ready to help you sort through these issues and find the solutions that fit your needs, wants, and budget. Katalyst provides the awareness, ability, and analytics that keep your operations protected and productive.

## See How Katalyst's Data Protection Services Can Help You Stop Cybercrime & Secure Continuity

<sup>1</sup> <https://www.ibm.com/security/data-breach>

<sup>2</sup> <https://www.businessinsider.com/top-un-official-warned-of-cybercrime-spike-during-pandemic-2020-5>

<sup>3</sup> <https://www.cloudwards.net/cyber-security-statistics/#Sources>

<sup>4</sup> <https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.aspx/>

<sup>5</sup> <https://www.mckinsey.com/featured-insights/coronavirus-leading-through-the-crisis/charting-the-path-to-the-next-normal/companies-play-catch-up-on-cybersecurity?cid=other-eml-alt-chr-mck&hlkid=a008fe8db58443a3a547fff12fe6f154&hctky=12639660&hdpid=82b5ffc0-412a-4d2d-bcdd-2ff5e649ce9>

<sup>6</sup> <https://www.zdnet.com/article/ransomware-attacks-are-causing-more-downtime-than-ever-before/>

<sup>7</sup> <https://cybersecurityventures.com/annual-cybercrime-report-2020/>

<sup>8</sup> Terms and conditions apply. Refer to warranty agreement for more information.