Ransomware isn't going anywhere. Be prepared.

Ransomware attacks have become so common that it's only a matter of time before cybercriminals target your organization. The end goal of an attacker is simple—prevent you from accessing your mission critical data and systems and then demand payment to restore access. Losing access to your data and IT systems means losing control of your business. Your entire business can grind to a complete halt in hours. Are you prepared?

Protecting against a ransomware attack requires a multifaceted defense strategy that covers and supports multiple layers of infrastructure. Each layer of infrastructure requires its own unique level of protection — endpoint, server, and network, along with backup and disaster recovery.

Begin Your Assessment

Our ransomware readiness assessment is based on the NIST Cybersecurity Framework,an industry standard approach you can follow to assess and protect your organization's data. The assessment looks at your cybersecurity preparedness, taking into account organizational discipline (people, policies, processes) as well as technology. We'll look at proactive areas to help you identify, protect, and detect, as well as reactive areas to help you respond and recover in the event of an attack.

Identify: Are you aware?

Having an easily-accessible inventory of your IT estate is critical to understanding your attack surface and where vulnerabilities may lie. Without this, you may miss a vulnerable system or platform that creates a breach you never saw coming.

Protect: Are you secure?

Understanding your current protection level can help define the holes in your security posture and what needs to be implemented to close those gaps. From staff training to credential management and network security, our assessment helps you discover your strengths and vulnerabilities.

Detect: Are you watching?

If you were under attack, how would you know? Our assessment will determine what monitoring capabilities you have and what's missing to make sure you're getting the full picture of threats, no matter where your workloads are, as fast as possible.

Respond: **Are you ready?**
It's not just about the technology. Having the right processes and plans in place can ensure that you'll be able to recover quickly. We'll dive into what your response plans are and where you can enhance them to make sure you respond to an attack most effectively.

Recover: **Are you resilient?**
If the worst happens, you need the ability to recover quickly and completely.
A ransomware attack is the most likely disaster an organization will face and your recovery capabilities need to be able to bring your critical assets back. We'll work with you on what capabilities you have and what can help you recover quickly.

Our Three Step Plan

We created a three-step methodology that helps you to understand the state of your ransomware readiness, develop a plan to accomplish your organizational goals, and take action in a deliberate and self-paced manner. Once you understand your current estate, you're ready to align your security goals with the business and then act.

1

Assess

- Take stock of your current posture
- Identify gaps in protection and opportunities for improvement
- Understand your risk

2

Align

- Mitigate risk with immediate remediation opportunities
- Review short- and long-term strategies for reaching your desired state
- Prioritize and plan

3

Act

- Architect remediation solutions
- Implement changes and solutions deliberately
- Continually reassess in the face of changing threats

Expedient offers award-winning cloud solutions and managed services, including best-in-class disaster recovery, security and compliance, and more.