



# Ransomware

## Response and Recovery

The pandemic has created new routes for threat actors to exploit security vulnerabilities. Now it's easier than ever to disrupt your business and extort ransom.

### Top Ransomware Defense Challenges:

- Organized ransomware groups are ramping up attacks
- Actors are constantly refining their attack skills
- Businesses are lacking resilience



### What can you do now?

- Never ignore the basics of security hygiene
- Test and validate security defenses
- Be clear on how to restore operations swiftly
- Collaborate so everyone knows how to work cohesively
- Prepare. Be ready for any incident



### You've been attacked – What's next?

1. Isolate compromised servers

2. Identify and analyze the intrusion and impact

3. Report the incident to concerned legal authorities

4. Discard the malware

5. Analyze the compromised data

1

2

3

4

5



6

7

8

9

10

6. Restore data from the most recent backup

7. Conduct forensic analysis for potential entry points

8. Plug the identified security loopholes

9. Learn from experience

10. Strengthen security posture

### Are you geared up?

**Contact us** to find out what you can do to be resilient to ransomware!