Commvault

eBOOK

FIGHTING RANSOMWARE

UNDERSTANDING TEAM ROLES AND RESPONSIBILITIES

CONTENTS

03 Being prepared

04 It's going to take a village

08 Layered defenses

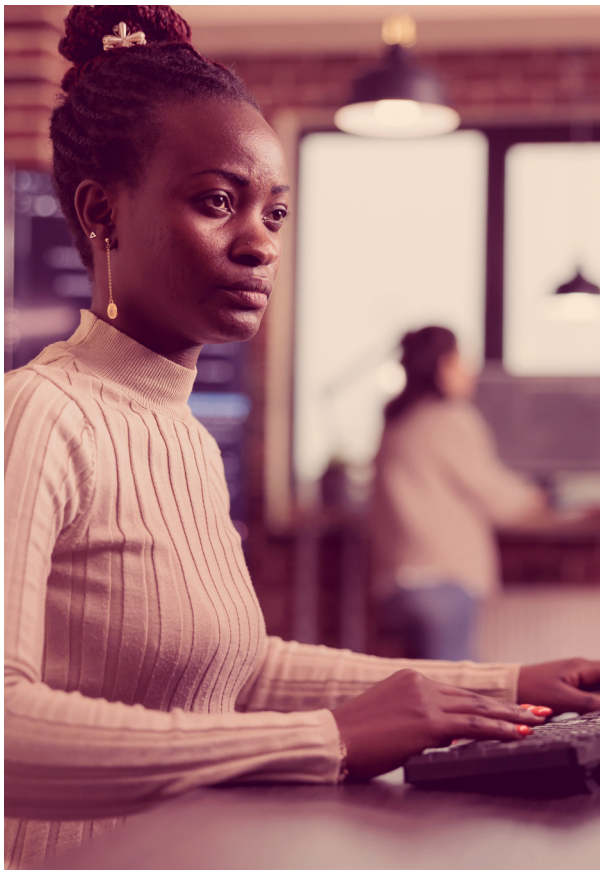
10 The attacker

11 Readiness solutions

12 Your call to action

13 Success is critical

BEING PREPARED



Cyberthreats are continuously evolving. What used to be isolated, solo hackers have now become organized digital criminals who want to exploit and harm businesses of all sizes. From hyper-focused zero-day attacks to broad-sweeping supply chain breaches, bad actors share one common goal: stealing, damaging, and monetizing your data to their advantage.

The cold truth is this: it's not a matter of if you'll have a breach, but when you detect it, what you did to prepare, and how you respond. Being ready for recovery means your teams have the confidence and the ability to quickly recover any data across your environment, including physical servers, virtual machines, and your various cloud platforms. To help you better secure, defend, and recover your data, maintain healthy business operations, and manage risk, you need a cyber-resilient approach that brings together IT, Security, and critical stakeholders.

DID YOU KNOW?

83%

of successful ransomware attacks feature double or triple extortion.[1]

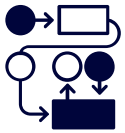
1 83% of organizations facing double, triple ransomware extortion | TechHQ | 2022

IT'S GOING TO TAKE A VILLAGE

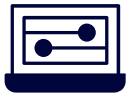
Cyberthreats take many shapes and forms, from stealthy zero-day attacks to phishing attempts targeting unsuspecting employees. Safeguarding your business and data and defending against these threats requires a well-rounded and multi-faceted approach, and no single team can combat them on their own.

It takes a well-equipped, prepared, and practiced village to deal with complex threats successfully. **This village includes:**

01
PEOPLE

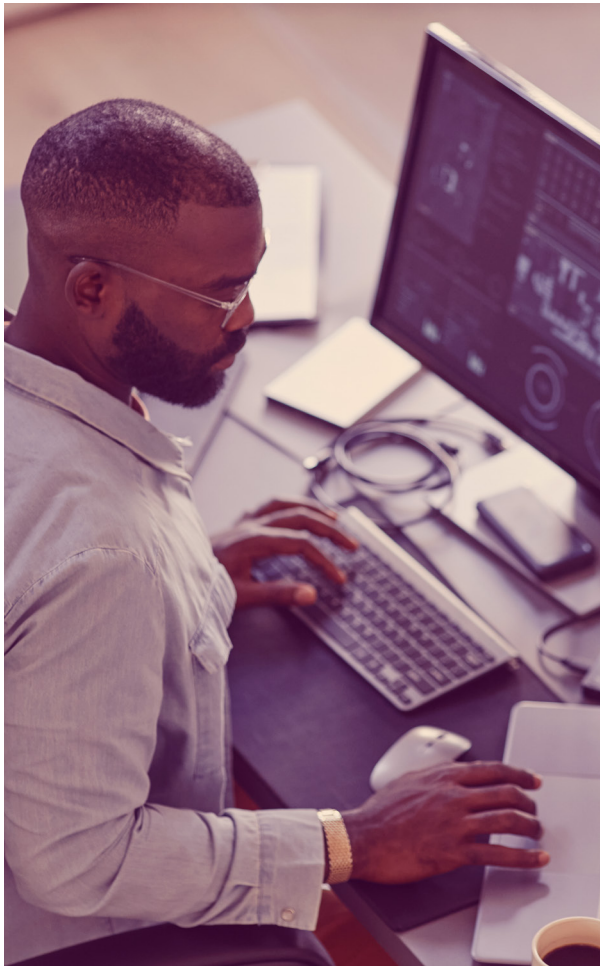


02
PROCESS



03
TECHNOLOGY

It's vital that you align internal and external teams before, during, and after a ransomware attack to ensure a speedy recovery. Teams must know and understand their roles and how they communicate with each other for a successful cyber recovery.



INTERNAL TEAMS

Begin by devising a communication plan to ensure everyone understands their roles. When facing a cyber incident, IT and security stakeholders need tools and solutions that work hand-in-hand to remove silos, increase visibility, and accelerate response–alongside proven processes to actively protect and recover data.

LEGAL AND PUBLIC RELATIONS

Clear communications are key, so make sure these teams are equipped with the right information to create factual, client-facing statements and have conversations with the press.

INSURANCE CARRIERS

If you don't carry cyber insurance, consider doing so. Discussions with ransomware underwriters can help you determine your preparedness and resiliency.

LAW ENFORCEMENT

If something does happen to your organization, do you need to contact law enforcement? Have you met them? Do you have their numbers?

EXTERNAL TEAMS

There may be a need for incident response and recovery assistance to help with replacement laptops, servers, and other equipment when facing various cyber recovery scenarios.

Internal and external teams must be aware of and in sync regarding their responsibilities. It's equally important that these processes are tested, vetted, and validated before putting them into action.

PRACTICE AND REFINE: HOW WILL YOU COMMUNICATE DURING A RANSOMWARE ATTACK?

- Does your organization's process support one another and your cyber defense and recovery objectives?
- How does your infrastructure fit together?
- Does your team understand their role during an attack? Do they understand their counterparts' roles?
- Does your team understand recovery plan interdependencies?
- How will you communicate about restoring your infrastructure and recovery steps with your business and clients?

SPEED: MAKE SURE YOU'RE THINKING IN TERMS OF SPEED

- How quickly can you close those watertight doors in the infrastructure to limit an attack's exposure or blast radius?
- Make recovery as easy as possible because you have the attack contained to the smallest amount of infrastructure.

PREPARED AUTOMATION

Well-intended automation can often go awry and cause more business disruption. It's important to understand that you've got the malware contained, and only the appropriate people can launch the remediation.

03 TECHNOLOGY

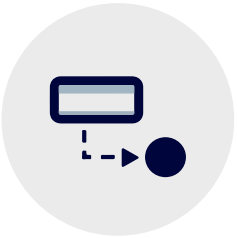
FOLLOW THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBERSECURITY FRAMEWORK TO AID YOUR PREPARATION.

Ransomware is relentless and demands accountability if you neglect cybersecurity. Our multilayered framework follows NIST in securing, defending, and recovering data by addressing the five areas below. To learn more about our multilayered framework, read our buyer's guide: Aligning Ransomware Protection and Recovery Plans with Critical Capabilities.

Identify

Protect

Monitor



Respond

Recover

LAYERED DEFENSE STRATEGIES

01 **ASSET MANAGEMENT:** Consider what is most critical. What will you bring up first, and what is the underlying infrastructure required to make that happen?

02 **SECURITY TRAINING AND AWARENESS PROGRAM:** You can educate your associates and employees, but how will they contact the people who will help them respond?

03 **CONFIGURATION AND VULNERABILITY MANAGEMENT:** Harden the environment from a vulnerability management perspective to ensure your team applies security patches promptly.

04 **EMAIL CONTENT, SCANNING, AND ENCODING URLS:** If an employee clicks on a URL in a hurried moment, make sure you've rewritten those URLs to go to a safe place for detonation examination. Emails should remain there from when they are received until users have read and interacted with them.

05 **NETWORK SEGMENTATION:** If malware gets through the perimeter, make sure the network is segmented. Ensure credentials that may be compromised are only usable in the smallest section of the infrastructure.

Layered defense strategies help safeguard your data and drive compliance in the face of evolving cyberthreats. Following the NIST Framework and zero trust principles will provide the best capabilities to secure, defend, and recover your data.

LAYERED DEFENSE STRATEGIES

06 **LEAST PRIVILEGE AND PRIVILEGED ACCESS MANAGEMENT:** Allow only a small set of IT individuals to have elevated rights to interact with the infrastructure and applications.

- Make sure IT (and others) use a different set of credentials than those they may be using as "users" with their laptops and email.
- Enable multifactor authentication (MFA), multi-person authentication (MPA), and common access cards if available.

07 **MULTIFACTOR AUTHENTICATION AND REMOTE ACCESS:** Multifactor authentication is a critical area for remote access (VPN, cloud-enabled SAS solution, or virtual desktop remote access, etc.).

08 **ENDPOINT DETECTION AND RESPONSE:** Ensure you have the right set of controls in place, so malware is cut short in its tracks and can't detonate. And if you cannot stop malware from executing, it should be firing alerts to the incident response team.

09 **INCIDENT RESPONSE:** Make sure your incident response teams are well-trained and equipped with the permissions and authority necessary to make swift decisions. In the event of an attack, waiting for an hour for the "right" people to give an OK in order to shut off an area of the network or a server could end up to be very costly.

10 **BACKUP AND RESILIENCY:** Knowing what you need to restore first is critical. This ties back to asset management. What is the most important data you are going to have the deepest resiliency for? Backups are perhaps the most important as you must determine what you are going to bring back first.

THE ATTACKER

Today's bad actors are experts at dealing with layered defenses. They continue to improve their methods and are particularly aware of what it takes to make assets unrecoverable until a ransom is paid.

Attackers figure out your backup retention period. They wait for a longer period, so the backups have rolled off, and you don't have clean backups to restore from.

Attackers know that backups are often on the network, and because they're accessible, they attempt to encrypt them as part of their attack.

PROACTIVE DEFENSE

- Ensure backup copies are air-gapped and immutable, removed from the network, and stored off-site.
- Change your backup credentials to differ from those used for the rest of the infrastructure. Ideally, protect passwords using multifactor authentication and multi-person authentication.
- Consider early warning threat detection to surface advanced cyberattacks before impact.
- Leverage solutions that coordinate IT and security tools to increase visibility and automate countermeasures.
- Safeguard production and backup environments with real-time visibility and a unified platform.
- Coordinate a unified response with bidirectional integrations with leading security tools to increase visibility, automate countermeasures, and accelerate response.
- Routinely validate and test your cyber defense and ransomware recovery processes.

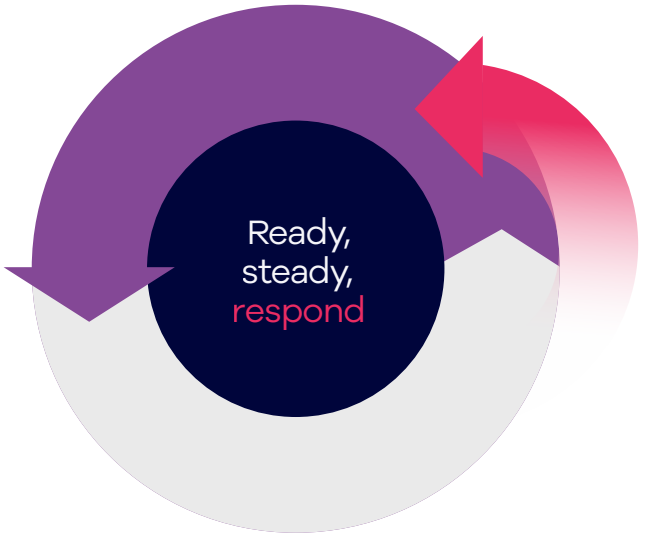
READINESS SOLUTIONS

Like we said before, it is not a matter of if you have a breach but when and how you respond. Should you ever need to recover from ransomware or a cyberattack, Commvault® Ransomware Readiness Solutions provide unparalleled support and can step you through a consistent, rapid cyber recovery process across platforms and clouds.

Preparing a disaster recovery plan takes time and expertise. With the increasing likelihood of an outage, disaster, or ransomware attack, you can't put it off until tomorrow. Commvault Readiness Solutions help you accelerate the return to normal business operations through three phases:

- **Ready:** Helps you align Commvault's technical capabilities with your business and recovery objectives. Learn more about our Recovery Readiness Assessment.
- **Steady:** Assists you in monitoring and maintaining a state of recovery readiness. Learn more about our Remote Managed Services.
- **Respond:** Helps accelerate your return to normal business operations in the event of an outage or disaster. Learn more about our Ransomware Response Service.

When disaster strikes your data, you need a plan. Accelerate your return to normal business operations through the proper planning, implementation, administration, and support of your data protection and management environment. Read more here.



YOUR CALL TO ACTION

01

IDENTIFY KEY STAKEHOLDERS

Determine who needs to be involved.

- Make sure you actively have conversations and express your concern that this is a huge problem.
- Make sure they understand that you must work together to solve this problem.

02

IDENTIFY KEY ASSETS

Understand what assets are important, get agreement between stakeholders. It's vital to know the recovery priorities.

03

CONDUCT A TABLETOP EXERCISE

All of this is theory. It's essential to proactively review and communicate your plans.

- Include a paper exercise to demonstrate what the teams are really going to be working through.
- Test, test, test.
- Gain an in-depth understanding of what has happened to other organizations during a malware attack and apply this knowledge to your plan.
- Find areas that you can improve upon.

04

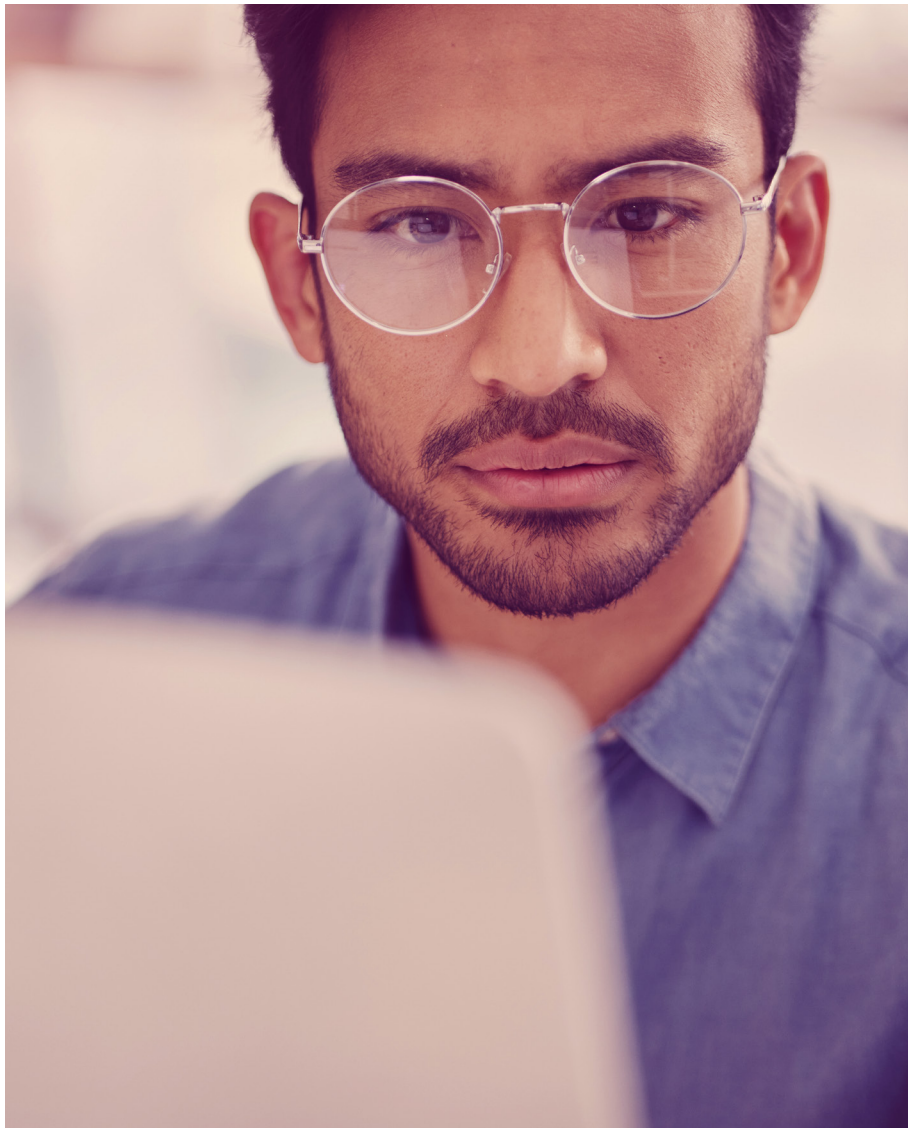
POSTMORTEM AND CHANGE IMPLEMENTATION

Make sure somebody is responsible for capturing areas of improvement and enacting those changes. Your goal is to come through your testing cycle and say, "Yes, we've made things much better now."

SUCCESS IS CRITICAL. PREPARATION IS EVERYTHING.

Make sure you have backups and the recoveries work as planned. Test, test, and continually test.

Ensure the backups are segmented from the network and use different credentials to increase their effectiveness.



eBOOK

STEP ONE: GET COMMVAULT CLOUD FOR THE BEST SECURITY, THE MOST INTELLIGENCE, AND THE FASTEST RECOVERY.

LEARN MORE

The content for this eBook is derived from Dave Martin's Connections presentation.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®