CHECKLIST

Commvault® CLUMIO A Commvault® Company

Defense Against Ransomware Attacks

Protecting your data against ransomware attacks involves developing and establishing a multi-layer defensive plan that covers everything from thwarting such attacks to recovering quickly in the event of a breach. This checklist provides a guideline to help you follow best practices to protect your cloud data against ransomware.

VENDOR AND SUPPLIER MANAGEMENT

- ☐ Confirm that your organization’s systems and applications are up to date and patched continuously
- ☐ Evaluate—on at least an annual basis—all your existing and future vendors to determine the risk their services add to your organization
- ☐ Meet with your vendors’ security teams and go over their practices for information security
- ☐ Confirm these vendors have the appropriate certifications and reports in place, including ISO 27001 and SOC 2 Type 2
- ☐ Determine if your vendors perform penetration tests from qualified security vendors and do they have attestations available

TRAINING AND AWARENESS

- ☐ Set up an ongoing security and privacy training program for your employees, and track the results
- ☐ Establish a regular cadence of internal communications around security and the dangers of ransomware, keeping employees aware of the issues and what needs to be done to enable business continuity
- ☐ Conduct annual company meetings dedicated to overall security awareness and training
- ☐ Conduct quarterly employee meetings addressing specific subjects such as BECs, SIM hijacking, SMS scams, etc.
- ☐ Implement a comprehensive set of drills to test your organization’s ability to manage risk and response in the event of a ransomware attack

TECHNICAL MITIGATIONS

- ☐ Identify and prioritize the security risks—assets, systems, data, people—that are most vulnerable to ransomware attacks
- ☐ Develop and implement an overall plan for defending against ransomware attacks
- ☐ Reduce your attack surface by confirming that your vulnerable endpoints are optimized for security
- ☐ Secure your email system against ransomware attack
- ☐ Prohibit the use of USB storage devices and restrict unnecessary open ports

PRIVILEGE AND AUTHORIZATION MANAGEMENT

- ☐ Limit the “blast radius” of what an attacker can do by managing the level of permissions with groups or roles
- ☐ Confirm you have strong authentications for all services, with no shared credentials
- ☐ Develop strict access control policies, such as a zero-trust framework that protects and authenticates user access for your systems
- ☐ Adopt and implement the principle of least privilege; Review privileged access frequently
- ☐ Establish a quarterly review of users who have admin level access and confirm with HR if there is any change in their status
- ☐ Monitor all access logs, checking for anomalies in access

DISASTER RECOVERY

- □ Establish a comprehensive backup and recovery strategy in case of a ransomware attack
- □ Confirm your backed up data is stored securely off site or in the cloud and allows for at least seven days of incremental rollback
- □ Protect your backed up data in an air-gapped solution that is separated from your production environment
- □ Make certain that your backup data is immutable and as secure as possible
- □ Validate that your data is encrypted in flight and at rest with keys that cycle frequently Make sure you have the ability to use your own encryption keys
- □ Confirm that data can be quickly restored to an account/region that is different from the compromised account/region
- □ Periodically test your ability to recover data from backups

HOW CLUMIO CAN HELP

The frequency and severity of ransomware attacks is truly alarming. It's a global, industry-spanning threat and needs to be taken seriously. But there's no need to feel helpless. Specifically, when it comes to having a trustworthy backup and recovery strategy in place, Clumio can help.

With the Clumio platform, your data is encrypted with your key before it leaves your cloud and is transmitted to the platform. Built-in integrity checking and object versioning enable immutability, and the platform is a completely separated environment from your company's. You can also configure your backup policy to archive and retain data on the schedule that best fits with your organization and data type.

Additionally, testing data restoration with Clumio is among the easiest tasks to do. View your protected assets, examine their backup calendar, and click to restore. That's it. With Clumio's granular recovery you can also restore individual files or database records, speeding up time to recovery. Clumio's ability to restore to any account or region also enables the flexibility to restore your data to a new site and get your business back up and running while the compromised site remains isolated for investigative purposes.

See for yourself how Clumio can simplify data protection and help you quickly recover from ransomware attacks—try Clumio for free.

To learn more, visit **commvault.com**