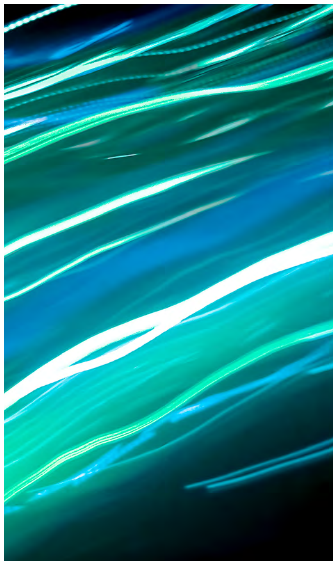
8 steps to consider before ransomware strikes

Ransomware recovery options are far more limited if you haven't taken the steps to prepare before an attack. This checklist will help you to create a viable recovery plan and reduce the massive impact of ransomware.



Step 1: Isolate backup data

Cloud data protection performs regular backups across endpoints, data centers, and workloads, protecting distributed data in case of a ransomware strike. Selecting a cloud-based backup solution offers an additional layer of protection by providing off-site data storage. Off-site data is isolated from the enterprise network, preventing malware attacks from spreading to critical data backups.

Step 2: Backup distributed data

Does your current backup plan cover 100 percent of your business-critical data, including data from geographically distributed teams and servers? Evaluate your distributed data and determine backup needs for bandwidth challenged remote locations. Centralized management and visibility of physical and virtual workloads is critical for backup efficiency.

Step 3: Review the backup scope of your SaaS apps

You're probably protecting servers, virtual machines, desktops, and email, but what about other sources where business-critical data is generated and stored, like Office 365 or G Suite? It's important to have complete visibility and control over your SaaS apps and ensure that you have a modern, integrated backup plan in place to prevent further SaaS data loss.

Step 4: Check backup frequency across distributed teams

Make sure that automated backup of all mission-critical data is periodically completed. As a general rule, your backup frequency objectives should align with your recovery point objectives (RPOs). You may also want to select a different backup frequency depending on the requirements of specific servers, users, and teams.

Step 5: Validate your data retention policy

How long are you keeping your backups? 14 days? Six months? Obtain a longer retention policy if needed to meet internal objectives — especially for key people, servers, and departments. Your data retention policy will vary depending on your industry, regulations, and internal IT policies — IT, legal, and compliance teams may need to weigh in on data retention needs.

Step 6: Test your backups and reassess policies periodically

Regular restore tests from backup data will ensure you have an effective tool when ransomware strikes. You should revisit your backup policies approximately every six months to ensure they continue to meet your organization's needs. IT often has the primary responsibility for these routines and, in some cases, acts in coordination with the legal team.

Step 7: Monitor for ransomware attacks

Keeping track of unusual file deletions, modifications, encryptions, and header changes can minimize damage by enabling fast responses such as isolating infected hardware before malware has the chance to spread. The earlier you isolate a problem, the sooner you'll be able to restore lost data, minimizing downtime and lost productivity.

Step 8: Streamline disaster recovery

In the event of a ransomware attack, your organization should have a "fail-safe" security model that allows impacted systems to recover faster. Being able to quickly restore all of your enterprise data from the safety of the cloud — including recovering virtual machines in minutes in a virtual private cloud such as an AWS VPC — is the essence of disaster recovery (DR) and the primary benefit of full-featured data protection and management. The right cloud-native solution can clone VPCs across regions and accounts for added resiliency. Eliminating on-premises DR hardware can also significantly lower your data protection/DR solution TCO.

Check out druva.com/solutions/ransomware/ and start incorporating ransomware protection into your strategy.