DATASHEET

Checklist for Cybersecurity Threat Protection

Protect your environment from cyberthreats

Cyberthreats, specifically ransomware, continue to be a top risk and top of mind for our customers. It is a challenge for all of us. We must protect against threats, monitor our environment, and stay recovery ready. To help ensure you are covered, please review these best practices to protect your data against a cybersecurity event.

Six tips for greater cybersecurity threat protection and recovery

As of March 21, 2022, The White House is reporting increased intelligence on potential cyberthreat activity from Russia. The White House Fact Sheet, Act Now to Protect Against Potential Cyberattacks, details cybersecurity best practices, including "ensuring you have offline backups beyond the reach of malicious actors."

The risks and rewards of defending against a cyberattack are significant to your organization and career. Done poorly, it results in lost data, revenue, and credibility. Done correctly, it can lead to operations being successfully restored quickly and greater recognition for a job well done. To help you better protect your data against a cybersecurity event, here are six tips you can easily implement.

1 Verify your cybersecurity recovery and disaster recovery runbooks are up-to-date.

Protecting against external threats requires diligence and constant attention to detail. Reviewing your Cybersecurity and Disaster Recovery Runbooks validates your recovery and verifies implementation of previous recommendations and that no adverse changes have occurred since the last review.

Commvault Complete™ Data Protection

Protect your CommServe® server in the Commvault cloud or your cloud, so it is offsite and easily recoverable.

Learn more >

Metallic®

Review your existing backup policies to ensure existing configurations align with expected SLAs.

Learn more >

2 Segment your networks to prevent lateral movements.

Don't give malware unlimited access within your network. Preserve your backups in isolated locations to prevent lateral movement and contain potential threats

Commvault Complete Data Protection

To create a cloud copy, Commvault offers a cloud storage solution called Metallic® Recovery Reserve™. This is the quick, easy button for safe, isolated copies of data to the cloud.

Learn more >

Metallic

Metallic® Office 365, Dynamics 365, Salesforce, and endpoint data protection offerings include built-in cloud storage. For on-premises and hybrid cloud workloads, consider leveraging Metallic® Recovery Reserve™ for a cost-effective, isolated storage target in the cloud.

Learn more >

3 Implement multifactor authentication.

The authentication process requires each user to have a unique set of criteria for gaining access. Enabling multifactor authentication methods makes it highly unlikely that a valid user account can be impersonated.

Commvault Complete™ Data Protection

Enable two-factor authentication for all users in an organization or only some user groups.

Learn more >

Metallic®

Enable multifactor authentication for users and groups.

Learn more >

4 Monitor your data protection environment.

Utilize the security dashboard to identify, assess, mitigate, and monitor security controls within the Commvault or Metallic environment. The dashboard will identify controls available in the environment, provide scoring and remarks to assess risks properly, continuously monitor your security posture, and offer insights to take appropriate actions.

Commvault Complete Data Protection

Check the Security Dashboard for assessing and applying other security controls.

Learn more >

Metallic

Check out Security IQ to stay up to date and improve your security posture and identify potential risks in real time.

Learn more >

5 Perform regular backups with immutability.

Consider increasing the frequency of backups and expanding your data protection to a 3-2-1 backup strategy; 3 copies of your data, on 2 different media types, with a copy offsite and preferably air-gapped. Other essential data protection tools include encryption, write once, read many (WORM), and strict access controls.

Commvault Complete Data Protection

Make sure you have immutable storage. Enable ransomware protection on your MediaAgents and Commvault HyperScale™ nodes.

Learn more >

Metallic

Check your Security Posture Score to ensure encryption and multi-authorization workflows are enabled.

Learn more >

6 Test and update your recovery plans.

Verify your recovery procedures and technologies will work as needed by testing. Perform frequent tests to confirm you can meet the SLAs you have defined for critical and high-priority data and applications. Update your Runbook based on any updates or changes from the test results.

Commvault Complete Data Protection

Add high availability to your CommServe using CommServe LiveSync – this will allow you to failover and test much faster.

Learn more >

Metallic

Perform routine backup and restore tests to ensure operations are set up correctly.

Select a Workload in the left nav > Click 'Getting Started'> Select 'Perform a Test Backup and Restore.'

Learn more >

Additional cybersecurity threat protection tips

- **Know your data to protect your data**
  Identify business-critical and sensitive data across your environment and data silos. Then determine if the data are exposed to vulnerabilities. You can efficiently remediate these risks using data insights by removing, moving, or securing this exposed data.

- **Install antivirus and antimalware protection**
  Use antivirus software with active monitoring designed to thwart advanced malware attacks. Verify you are using the latest release for maximum protection.

- **Ensure patches are up-to-date and stay current**
  When leveraging installed solutions, keep software, firmware, and applications up to date to reduce the risk of cyberthreats exploiting common vulnerabilities.

- **Conduct employee security training**
  Educate employees on avoiding cyberthreats and detecting phishing campaigns, suspicious websites, and other scams. Employees are critical to a good defense. Despite their best intentions, employees are still a leading cause of malware propagation.

Commvault understands that a cybersecurity attack or other disaster means all eyes are focused on the IT organization. We are here to help if you have questions or need assistance. **A few areas are:**

- Identifying your business's critical and sensitive data
- Quickly protect applications and workloads with our SaaS data protection offerings
- Easily implement an extra layer of protection in the cloud with Metallic
- Streamlining your recovery operations or testing your SLAs

If you need guidance on enabling any of the security features mentioned above, please contact Commvault Customer Support or Metallic Customer Support for additional assistance.

commvault.com | 888.746.3849