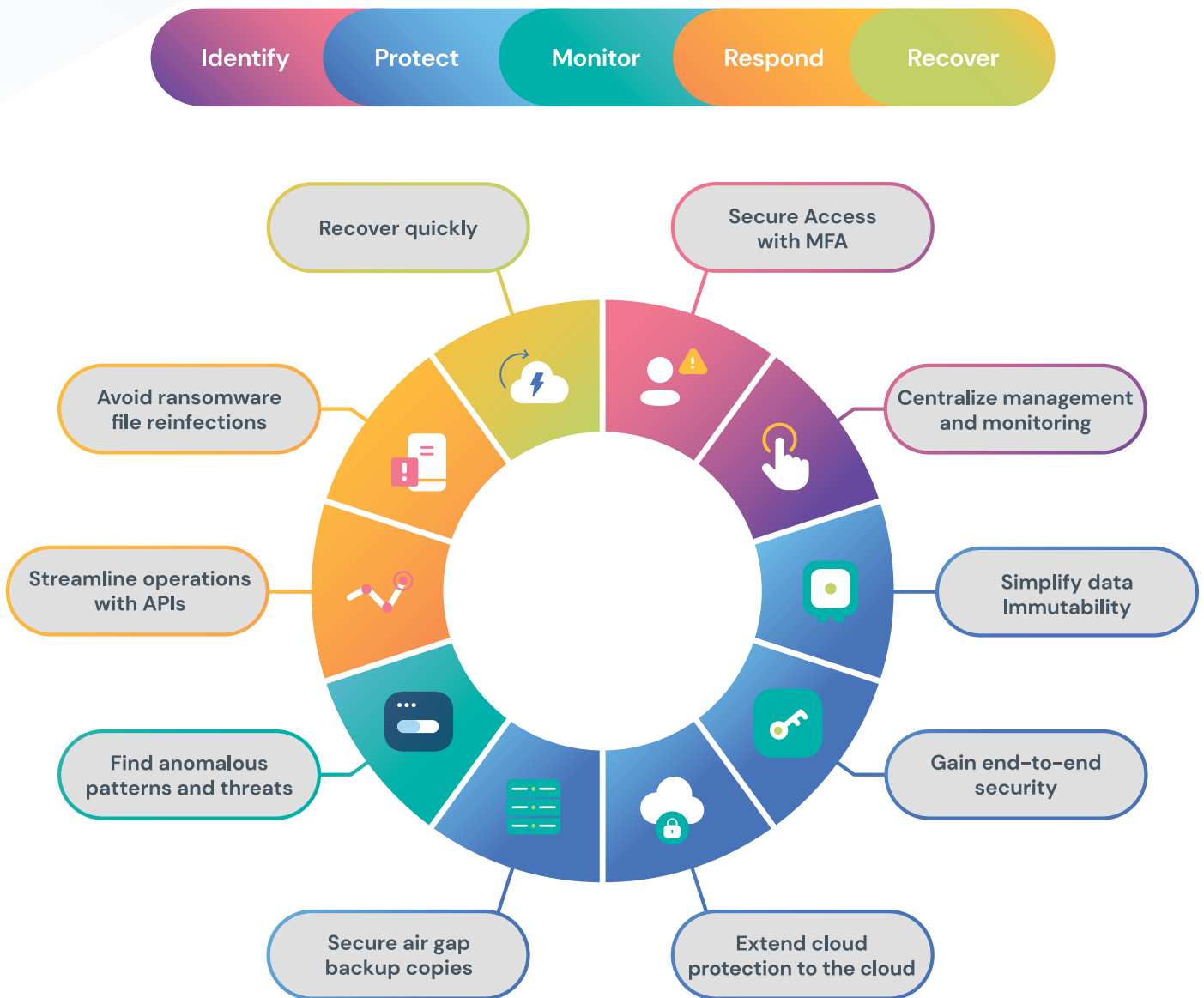**COMMVAULT®**
Be ready™

The Multi-layered Approach to Ransomware Protection and Recovery

Safeguard your data and reduce cybersecurity risk through our secure backup framework. This end-to-end framework follows NIST and Zero Trust principles, providing you with the best protection and recovery capabilities.

The security framework

| Identify | Protect | Monitor | Respond | Recover |

- Recover quickly
- Secure Access with MFA
- Avoid ransomware file reinfections
- Centralize management and monitoring
- Streamline operations with APIs
- Simplify data Immutability
- Find anomalous patterns and threats
- Gain end-to-end security
- Secure air gap backup copies
- Extend cloud protection to the cloud

The Plan in Details

Security-conscious organizations like yours can trust Commvault on ransomware protection and recovery to get your businesses back up and running in hours, not weeks. Through our multi-layered security approach and with zero trust principles, your organization is prepared and ready.

Zero Trust Principles

Zero trust principles follow a comprehensive IT security model to restrict access controls to networks, applications, and environments without sacrificing performance or user experience, and, in short, the approach trusts no one. Commvault embraces zero trust principles and security architecture as defined by NIST. Our ransomware protection and recovery solution helps organization prepare for and respond to cyberattacks.

Identify	**Secure Access with MFA**	The AAA security framework for Authentication, Authorization, and Accounting protects who has access and what they have access to while monitoring events and activities for proper security. **Learn more ›**
	Centralize management and monitoring	Single pane of glass to centrally monitor, manage, and adjust the security levels and parameters. **Learn more ›**
Protect	**Simplify data immutability**	Protect against changes from inside and outside the backup solution. Restore unchanged and unmodified backup data anytime. **Learn more ›**
	Gain end-to-end security	Data is encrypted at the source, in flight, and at rest using industry-standard protocols with multiple options for key management and interoperability. **Learn more ›**
	Extend cloud protection to the cloud	Metallic™ Cloud Storage Service makes it simple to securely adopt cloud storage and ease digital transformation. **Learn more ›**
	Secure air gap backup copies	Isolate and segment storage targets from public networks to mitigate lateral moving threats. **Learn more ›**
Monitor	**Find anomalous patterns and threats**	Use machine learning, artificial intelligence, and honeypots to monitor and detect suspicious or unusual activity for greater insights and faster time to recovery. **Learn more ›**
Respond	**Streamline operations with APIs**	Coordinate interactive responses and actions using APIs, workflows, and integrations with external orchestration platforms. **Learn more ›**
	Avoid ransomware file reinfections	Ensure a clean and secure recovery by surgically deleting suspicious or unnecessary files, or by creating an isolated recovery. **Learn more ›**
Recover	**Recover quickly**	Minimize lost revenue with fast, flexible cloud, virtual, and on-premises recovery options. **Learn more ›**

Learn more about Commvault ransomware protection and recovery. **Visit commvault.com/ransomware ›**