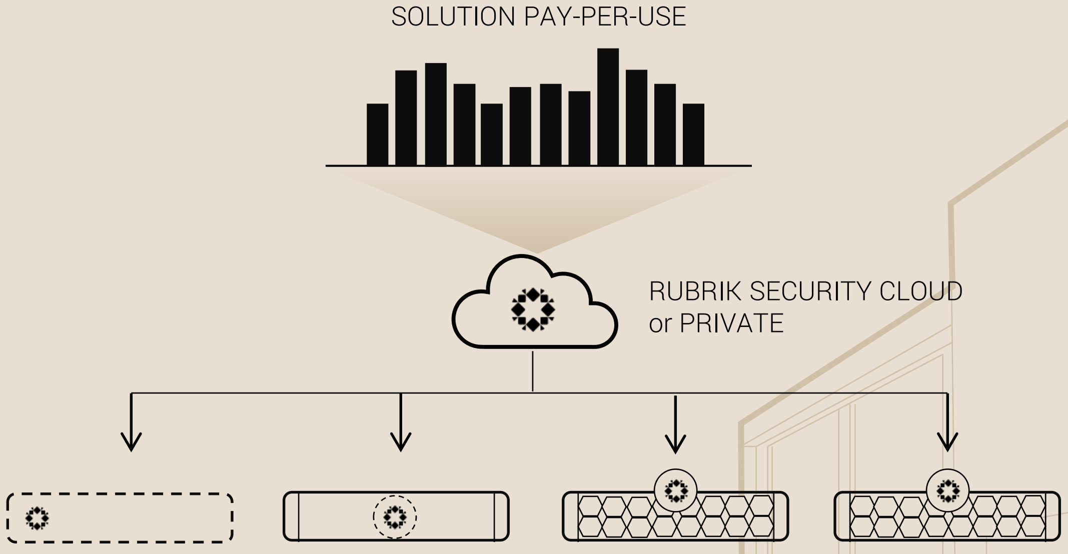


RUBRIK® SECURITY CLOUD MODULES

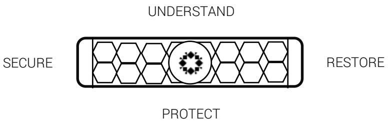
Cristie Solurtion – powered by Rubrik®. Choose your Cristie module based on Foundation Edition Primary, Foundation Edition Replication, MSP Edition Primary, Ransomware Recoverability Edition Primary or Enterprise Edition Primary. Cristie also provide optional value-adds listed in the table.

All versions can be obtained through pre-payment, subscription, or pay-per-use models. Additionally, Cristie provides licenses for both the Primary cluster and Replication cluster.

EDITION	FOUNDATION v8/9	FOUNDATION v8/9	MSP	RANSOMWARE RECOVERABILITY EDITION	ENTERPRISE
LICENSE	PRIMARY	REPLICATION	PRIMARY	PRIMARY	PRIMARY
Payment options					
Monthly Pay-per-use	Yes	Yes	Yes	Yes	Yes
Monthly Subscription	Yes	Yes	Yes	Yes	Yes
Annuall Payments	Yes	Yes	Yes	Yes	Yes
Pre-Payement	Yes	Yes	Yes	Yes	Yes
Contract					
Contract time	12 – 60 months	12 – 60 months	12 – 60 months	12 – 60 months	12 – 60 months
Hardware Options					
Standard appliance	Yes	Yes	Yes	Yes	Yes
High Density appliance	Yes	Yes	Yes	Yes	Yes
Monthly Subscription	Yes	Yes	Yes	Yes	Yes
Pre-Payement	Yes	Yes	Yes	Yes	Yes

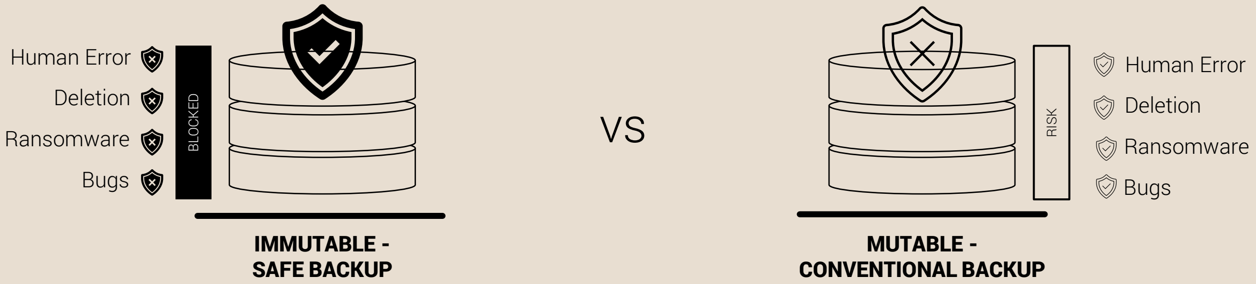
RUBRIK® EDITIONS OVERVIEW

Choose your preferred module for your cluster.



		FOUNDATION EDITION v8	FOUNDATION EDITION v9	MSP EDITION	RANSOMWARE RECOVERABILITY EDITION	ENTERPRISE EDITION
		Keep your data resilient and recoverable to protect against cyber attacks and operational failure.	Keep your data resilient and recoverable to protect against cyber attacks and operational failure. Included Cloud Services.	Keep your data resilient and recoverable to protect against cyber attacks and operational failure with multitenant self-service and included Cloud Services	Secure your data, continuously monitor risks to your data, and deliver orchestrated recovery of your applications on-prem.	Secure your data, continuously monitor risks to your data, and deliver orchestrated recovery of your applications in the event of operational disruptions.
Data Protection	Enterprise, Cloud, and SaaS Data Protection	Yes	Yes	Yes	Yes	Yes
	Cloud Data Protection – Universal Cloud License	-	Yes	Yes	Yes	Yes
	Immutable Data Backup	Yes	Yes	Yes	Yes	Yes
	End-to-End Data Encryption	Yes	Yes	Yes	Yes	Yes
	Air-Gap & Isolated Recovery	Yes	Yes	Yes	Yes	Yes
	Multi-factor Authentication (MFA)	Yes	Yes	Yes	Yes	Yes
	Retention lock	Yes	Yes	Yes	Yes	Yes
	Two-Person Rule	Yes	Yes	Yes	Yes	Yes
	More NTP Protect / Hardened Linux etc.	Yes	Yes	Yes	Yes	Yes
	Mass Recovery – Restore at scale	Yes	Yes	Yes	Yes	Yes
Data Threat Analytics	Anomaly Detection	-	-	-	Yes*	Yes
	Threat Monitoring	-	-	-	Yes*	Yes
	Threat Hunting	-	-	-	Yes*	Yes
	On-Prem	-	-	-	Yes	Option
Data Security Posture	Sensitive Data Monitoring	-	-	-	Yes*	Yes
	Data Security Command Center	-	-	-	Yes*	Yes
	On-Prem	-	-	-	Yes	Option
Cyber Recovery	Threat Containment	-	-	-	Yes	Yes
	Cyber Recovery Simulation	-	-	-	Yes	Yes
	On-Prem	-	-	-	Yes	Option
More	Cristie Advisory Service (Support + Speaking Partner)	Yes	Yes	Yes	Yes	Yes
	Cristie Self-Service Portal (Cloutility)	Option	Option	Yes	Option	Option
	Cristie Rubrik® BMR (RBMR)	Option	Option	Option	Option	Option
	Cristie Rubrik® Automated Restore Test (RBMR)	Option	Option	Option	Option	Option
	Tape Option	Option	Option	Option	Option	Option
	Domestic Replication – secondary DC	Option	Option	Option	Option	Option
	Cloud Archive option (public, domestic, green)	Option	Option	Option	Option	Option

*include a thin digital twin (TDT) that will leverage your existing security systems for vulnerability assessment and threat hunting, ransomware recoverability validation, remediation implementation and validation, penetration testing, patching. Optional: Pentera



What is Immutable Data Backup?

Protect your data assets from ransomware and other malicious attacks with immutable backups. Quickly recover from attacks and prevent data loss.

Reference Rubrik Insights:

An immutable backup is a backup file that can't be altered in any way. An immutable backup should be unchangeable and able to deploy to production servers immediately in case of ransomware attacks or other data loss.

Why are Immutable Backups Critical?
One of the most pressing risks facing every organization is the threat of a ransomware attack. Ransomware can strike any Internet-accessible device without warning and then quickly spread throughout your entire infrastructure. An attack can disable business operations and cost significant time and real money to resolve. In addition, the pervasive use of network share techniques throughout enterprise computing elevates the risk of spreading malware once any system connected to your network is breached.

Conventional data backups may not be effective for restoring data that has been encrypted by an attack, because your backup may also be encrypted or deleted by an attack. In fact, ransomware attacks that specifically target backups are on the rise. How do you ensure that your backup data is not vulnerable?

While primary storage systems must be open and available to client systems, your backup data should be isolated and immutable. It's the only way to ensure recovery when production systems are compromised. An immutable backup is immune to subsequent ransomware infections.

Data protection goes well beyond simple file permissions, folder ACLs, or storage protocols. Because these protocols are not completely secure and can be circumvented, immutability must be integral to your backup architecture and not be bolted on after the fact.

A built-in immutable backup helps ensure recovery from ransomware attacks by ensuring you always have a clean backup. Maintaining immutable backups means you will be able to recover data after a ransomware infection and avoid paying a ransom.

Rubrik's Immutability Approach

Rubrik uses an architecture that combines an immutable filesystem with a zero-trust cluster design in which operations can only be performed through authenticated APIs.

Rubrik's approach contrasts with other data management systems that use general purpose storage. Those systems rely on standard protocols such as NFS or SMB to advertise availability to clients.

Because data management solutions that use general purpose storage can employ limited or ineffective techniques for securely transacting data, they can leave files in their native format while allowing clients to read the backup data directly. This represents a breach of confidentiality that forces you to secure data storage independently from your data management solution. Not so with Rubrik.