CRISTIE
RECOVERY
SOLUTION

COVERY. BACKUP & RECOVE
CKUP & RECOVERY. BACKUP
COVERY. **CRISTIE** BACKUP &
CKUP & **RECOVERY** BACKUP
COVERY **SOLUTION** BACKU
CKUP & RECOVERY. BACKUP
COVERY. BACKUP & RECOVE
CKUP & RECOVERY. BACKUP
COVERY. BACKUP & RECOVE
CKUP & RECOVERY. BACKUP
SOVERY. BACKUP & RECOVE
KUP & RECOVERY. BACKUP

FOR CLOUD! AND MORE..
SECURITY LEVELS

“To be truly cyber-resilient, organizations need both proactive defense and reactive recovery”

CRISTIE
RECOVERY
SOLUTION

ZERO TRUST
Security Levels

	SILVER	GOLD	PLATINUM
Air-gapped architecture	Y	Y	Y
Immutable Backups	Y	Y	Y
Access Controls (MFA, RBAC)	Y	Y	Y
Dual Envelope Encryption	Y	Y	Y
Data Lock	Y	Y	Y
Safe Mod	Y	Y	Y
Security Command Center		Y	Y
Cyber Resilience Scorecard		Y	Y
Rollback Actions		Y	Y
Security Events		Y	Y
Data Anomaly Detection		Y	Y
SIEM / XDR Integrations		Y	Y
Data Audit Logs		Y	Y
Quarantine			Y
Recovery Scans			Y
Curated Recovery			Y
Sandbox Recovery			Y
Recovery Intelligence			Y
Recovery Playbooks			Y
Threat Hunting & Threat Watch			Y

SILVER – ZERO TRUST FOR EVERYONE

CHALLENGE

01. Clean backups are essential—but even replicated or cross-region copies can still be vulnerable.

02. Attackers can alter policies or delete recovery points, leaving backups exposed.

SOLUTION

01. Air-gapped backups isolate your data from the production environment, blocking ransomware from reaching and compromising protected copies.

02. Data Lock prevents deletion of restore points—even by insiders—and allows secure, controlled unlock via included support for compliance needs.

ZERO TRUST SILVER

Ensure immutability of your backup data with Air-Gap, Data Lock - all included by default.

GOLD – ZERO TRUST MONITORING

CHALLENGE

01. Encryption and immutability protect data but don't detect threats or ensure fast recovery.

02. Data loss from accidental or malicious deletions, including insider threats.

03. Frequent CVEs and complex patching make security management difficult.

SOLUTION

01. Security Command Center provides continuous monitoring, anomaly detection within 1 hour, activity tracking, rollback capabilities, SIEM integrations, and easy access to audit logs for faster response.

02. Self-service rollback enables recovery of deleted data with time-based controls, selectable undo actions, and reporting on affected entities.

03. Data Security Cloud removes platform management, with bi-monthly updates, flexible rollout timing, and transparent status and release visibility.

ZERO TRUST GOLD

Adds Security Command Center for continuous monitoring, anomaly detection, and enhanced security and recovery readiness.

CRISTIE
RECOVERY
SOLUTION

PLATINUM – ZERO TRUST THREAT HUNTING

CHALLENGE

01. Slow ransomware recovery and difficulty isolating infected systems.

02. Infected backups slow recovery, increase manual effort, and risk reinfection and data loss.

03. Recovering from contaminated data risks reinfection.

04. Compliance requires proof of successful recoveries.

SOLUTION

01. Automates response with SIEM/SOAR integrations, quarantines infected data, scans for threats, and uses Curated Recovery to restore the latest clean data with confidence.

02. Automatically restore the latest clean version of each file by selecting the optimal point and creating a single “golden snapshot” for recovery.

03. Scan snapshots for malware and IoCs during recovery to ensure clean restores, using built-in antivirus and custom threat indicators.

04. Automated restore testing with threat hunting and scheduled compliance reporting.

ZERO TRUST PLATINUM

Includes all core features, plus threat hunting, restore testing, and recovery playbooks to accelerate and optimize ransomware recovery.

EU REGULATIONS & COMPLIANCE

NIS2 DIRECTIVE

The Network and Information Security Directive (NIS2), adopted by the European Union Parliament on December 27, 2022, is a pivotal regulation aiming to enhance cybersecurity resilience across the EU. More recently, the European Commission reached political agreement on a new regulation on June 26, 2023, to fortify cybersecurity measures within EU institutions, bodies, offices, and agencies.

These regulations aim to strengthen cybersecurity measures across the EU. While the NIS2 directive targets escalating cyberattacks globally, the new regulation sets a framework for governance, risk management, and cybersecurity control across EU entities. The Computer Emergency Response Team (CERT-EU) will serve as a coordination hub for threat intelligence, information exchange, and incident response.

SOLUTION

CRS-d offers a robust backup and data management solution that supports organizations in protecting both their SaaS and Hybrid workloads, thereby aiding business continuity. Powered by Druva means alignment with the NIS2 Directive and new Cybersecurity Regulation requirements, ensuring organizations meet these critical cybersecurity standards.

Recommended Security Level
ZERO TRUST PLATINUM

CRISTIE **RECOVERY** SOLUTION
FOR CLOUD! AND MORE..

Powered by
druva

cristie

Headquarter
CRISTIE NORDIC AB

Kungsgatan 38
111 35 Stockholm, Sweden

+46 8-718 43 30
info@cristie.se

www.cristienordic.com