DATA SHEET

Guardian Ready

DESIGNED FOR ACTIVE RESILIENCE – RECOVERY IS THE GOAL

THE PROBLEM

Most organizations still build their security strategy around preventing the attack. But attacks are still getting through—and the pace is accelerating. Cybersecurity Ventures predicts that by 2031, ransomware will attack a business, consumer, or device every two seconds.[1]

That's why modern ransomware operators don't just target production systems - they target recovery. They go after backup infrastructure and recovery dependencies: deleting shadow copies, encrypting catalogs, corrupting recovery points, and undermining your confidence in what's safe to restore.

Traditional backup was built for a world of hardware failures and accidental deletions. In a ransomware incident, "we have backups" doesn't guarantee "we can recover" - because your last good backup may be compromised, incomplete, or untrusted when you need it most.

When the attack finally triggers, your "last good backup" might not be available or compromised.

SERVICE OVERVIEW

The Commvault Guardian Ready service is a comprehensive advisory engagement designed to help organizations assess and strengthen their cyber resilience posture against modern threats such as ransomware, identity compromise, and operational disruption.

The service is available in Gold and Platinum tiers, allowing customers to select the offering that best meets their needs.

CUSTOMER OUTCOMES

- Improved cyber recovery readiness
- Enhanced executive preparedness and decision-making
- Greater visibility into identity and threat risks
- Assessment of resilience and recovery strategies
- Actionable recommendations and prioritized improvement roadmap
- Increased confidence in responding to and recovering from cyber incidents

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

KEY COMPONENTS AND BENEFITS

- **Cyber Resilience Workshop & Simulated Lab**
  - Immersive experience covering real-world attack & recovery scenarios
  - Cleanroom Recovery with ThreatScan Analysis Simulation
- **Customized Executive Tabletop Exercise**
  - Industry-specific cyber crisis scenarios
  - Executive decision-making and response validation
- **CloudSEK & Identity Resilience Correlation**
  - Threat intelligence analysis covering deep and dark web threats and leaked data
  - External exposure and identity risk assessment
- **Cyber Resilience Assessment (Platinum)**
  - Risk posture evaluation across Commvault Platform
  - Recovery readiness maturity scoring
- **Cyber Resilience Plan Gap Analysis**
  - Review of recovery, incident response, and continuity plans
  - Lessons learned and preparedness validation
- **Action Planning & Executive Recommendations**
  - Prioritized roadmap for improving resilience and recovery capabilities

Strengthen Readiness. Validate Recovery. Improve Active Resilience.

WHAT IS ACTIVE RESILIENCE?

Active Resilience is the ability to confidently answer two critical questions:

- *Are you protected?*
- *Can you recover?*

Commvault Services helps you answer **YES** to both - not just at go-live, but consistently over time. This confidence is built by helping you achieve capability, not dependency.

Through structured knowledge transfer, clear and reusable document deliverables, and witness testing that supports recovery outcomes, your teams can gain the skills, evidence, and operational readiness required to recover. Protection enables resilience, but **recovery is the goal** - and Active Resilience enables you to be able to achieve it when it matters most.

To learn more, visit **commvault.com/services**