RECOVER GUARD

Cyber Resilience Configuration Validation

Ensure Successful Data Recovery Following a Ransomware or Other Cyberattack

Cyberattack – will you be able to recover?

Experts rank cyberattacks and ransomware as the “biggest threat facing the business world today”[1] and warn that malware targets backup storage and files, and seeks to delete any means by which an organization could recover following a cyberattack.[2]

So, when it comes to your critical data – the *crown jewels* at the heart of your business – a successful attack will lead to business catastrophe if your organization has not made certain its most valuable data assets can be recovered in the event of a ransomware or other cyberattack.

Recovery from a cyberattack is not only a pressing matter for the organization, it’s a matter of regulation. Governments and industry standards groups require enterprise IT environments to be resilient to cyberattack and to be able to recover quickly following a cyberattack.

Traditional disaster recovery solutions will not do

Although a cyberattack may be regarded as a “disaster,” having a traditional disaster recovery (DR) solution in place is not what is required. A DR solution is obligatory for incidents such as power outages, natural disasters or human error, but is the wrong solution for system and data recovery following a cyberattack.

A cyberattack, by its nature, involves malicious intent. Often, cyberattacks and ransomware involve attempted encryption or deletion, not only of production, but also of backup data. When both production and backup data are lost, recovery is no longer a viable option; irrevocable consequences, such as bankruptcy, can follow.

All this makes it imperative for enterprise IT to be constantly aware of the status of their core data and IT configurations, ensuring these systems are misconfiguration-free, able to recover critical data assets and resume critical operations in the event of a ransomware or other cyberattack. To do so, enterprises must deploy and configure advanced backup and recovery solutions and features to ensure recovery copies cannot be compromised even when production is hacked.

Introducing RecoverGuard™ - Automatic cyber resilience validation

The RecoverGuard™ cyber resilience validation solution proactively detects risks to cyber recovery in any type of IT environment, from on-prem to cloud to hybrid, and ensures swift recovery of data following a cyberattack.

RecoverGuard focuses on cyber resilience configuration assessments. **It verifies that recovery and backup copies of data are kept in a secure, immutable and isolated manner.** And, it verifies that cyber-recoverability architecture and configuration best-practices are followed and are in compliance with regulations, standards and RPO requirements. RecoverGuard achieves these aims using automatic and continuous processes of *knowledge-driven IT configuration analysis* to detect and enable repair of deviations from best practices. The solution facilitates automated compliance reporting and automatic healing.

> “Cybersecurity efforts must include, in addition to assessment, prevention and mitigation, resilience and recovery”
>
> Chairman Jay Clayton
> US Securities and Exchange Commission (SEC)

> “Financial Market Infrastructures arrangements should be designed to enable it to resume critical operations rapidly, safely and with accurate data”
>
> The European Central Bank (ECB)

Key Solution Benefits

- Hardens data system configuration to prevent unauthorized access to masses of high-value data assets
- Ensures compliance with information security standards
- Facilitates successful information security audits
- Validates compliance with organizational baseline security policy

[1] HBR - How a cyber attack could cause the next financial crisis. Sept 2018

[2] TechTarget - Protect backups from ransomware and other security risks. Aug 2019

ContinuitySoftware.com

RECOVER GUARD

RecoverGuard™ is built on the foundation of proven technology used by major enterprises worldwide

Ensure data recoverability from a cyberattack

RecoverGuard operates proactively to ensure data is recoverable in the event of a cyberattack. The solution analyzes database, storage and file system configurations to check whether they have valid and secured recovery copies available. It verifies that these copies are immutable, stored in an isolated manner and conform to stated recovery objectives and ransomware protection guidelines. This ensures that in the event of a ransomware attack, the copies will not be affected and will expedite successful recovery.

Unparalleled, deep knowledgebase of configuration and regulatory information

In whatever type of environment data storage is located, RecoverGuard scans all relevant IT systems and components including databases, file systems, compute, virtualization, and storage to proactively detect cross-domain and in-layer resiliency risks and check for misconfigurations that could affect recoverability of high-value assets.

The solution analyzes the collected configuration information against our proprietary knowledgebase, a continuously updated repository of hundreds of vendor, industry and organizational best practices, and regulatory guidelines for recovery. It checks issues such as copy hygiene, air gapping, existence of remote recovery copies of data assets, immutable data recovery copies and that RPO and retention goals are being met and recovery systems are hardened and isolated. Organizations can implement their own customized checks and routinely scan for them to ensure their selected baseline mandates are being followed.

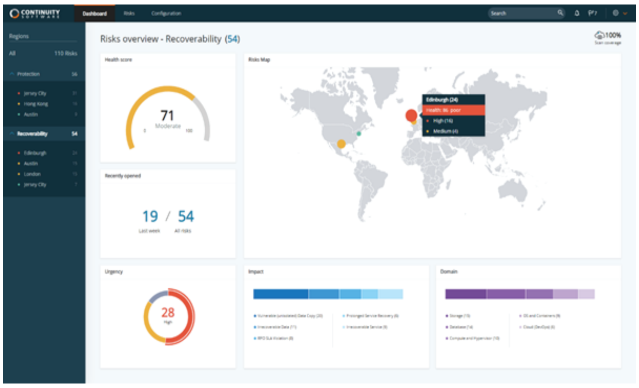
Meet best practices, comply with regulations for recoverability and gain visibility

RecoverGuard facilitates a repeatable, trackable, and ongoing configuration assessment process, proving compliance with all relevant cyber recoverability regulations. It automatically and proactively detects violations of vendor best practices for data recovery, community-driven best practices for cyber resilience, data protection baseline requirements (built-in and custom), ransomware protection guidelines, and standards and regulations (NIST, SEC, FINRA, FFIEC, etc.).

RecoverGuard provides visibility into recoverability metrics, such as RPO, immutability and isolation, all easily accessible and understandable via reports and a dashboard filled with relevant data and drill-down capability.

An enterprise-grade solution

Developed on the foundation of proven technology used by leading enterprises worldwide, RecoverGuard is fully scalable, lightweight and secure. It meets the cyber recoverability challenges of large, ever-more-complex IT environments that often include legacy (on-prem), private cloud, public cloud, or a mix of these. Built-in plugins and APIs enable enterprises to seamlessly integrate with vulnerability management systems, providing a complete view of all security gaps and vulnerabilities and prioritization of repairs according to their business impact. It integrates with the enterprise's ITSM tools such as ServiceNOW and others to facilitate automatic incident generation and assignment for remediation.



RecoverGuard dashboard: Get an up-to-date picture of cyber-recoverability for all relevant systems throughout the enterprise.

About Continuity Software

Founded in 2005, Continuity Software helps the world's leading organizations, including 6 of the top 10 US banks, to achieve resilience in every type of IT environment. Our solutions proactively prevent outages and data loss incidents on critical IT infrastructure. As a result, unplanned infrastructure outages are reduced by an average of 80% and configuration errors are resolved before they turn into costly service incidents. Our proven technology and methodology now encompasses cyber resilience. Our solutions protect mission-critical data residing in vulnerable storage systems against cyberattacks, prevent data loss, and ensure data recoverability.