CONTINUITY SOFTWARE

Cyber Resilience Assurance

Uncover Hidden Security Risks to Critical Data Storage Systems and Protect High-Value Data Assets

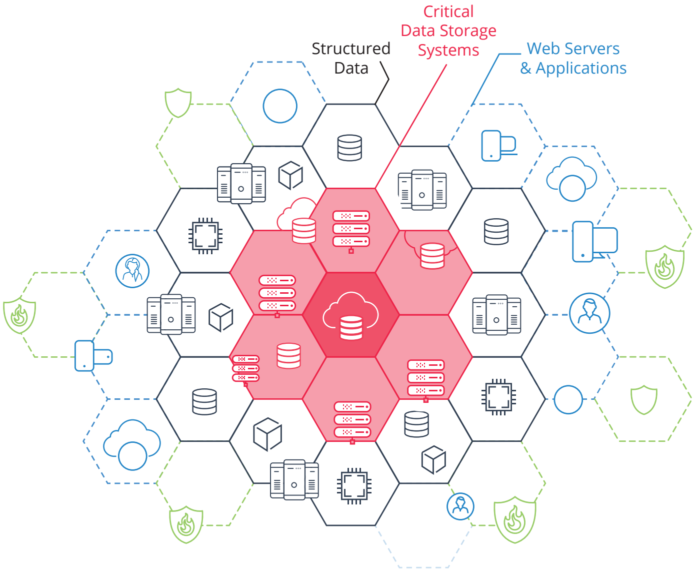
Every enterprise's IT environment stores a data goldmine: Is that data verifiably secured?

Cyberattacks. The consensus is that they are inevitable. To protect against malicious attacks, enterprises are securing their IT environments with solutions for hardening end-points, networks and operating systems. **Data storage system configurations, however, have been neglected**, with the rationale that protecting the outer perimeter of the environment will prevent infiltration to core data storage systems. Yet, data critical to the trusted and continuous operation of enterprises flows through data storage systems. The storage environment is home to critical data used by many applications and databases and is saved there in various systems: storage arrays (block, IP, object), storage network switches, cloud storage, virtual SAN, file servers, file systems, raw devices, appliances, and more. And, these may be vulnerable to attack.

The increasing sophistication and success of nefarious actors necessitates additional steps to protect enterprises' *crown jewels* – their high-value data assets – which, if held for ransom, compromised, or deleted, would cripple the entire enterprise.

In parallel, government regulators throughout Europe, the U.S. and much of the world, demanding resiliency for high-value data assets, have established regulations requiring adherence to cyber resilience guidelines. Enterprises, and specifically financial organizations, must demonstrate compliance and the "ability to resume critical operations rapidly, safely and with accurate data."*

* ECB: Cyber resilience oversight expectations for financial market infrastructures. Dec. 2018



Hackers have proven they can gain entry into "protected and secured" networks. The enterprise's crown jewels reside in vulnerable inner-core data storage systems.

Introducing Data Security Advisor™- Securing the resilience of data storage Systems

Continuity Software's Data Security Advisor™ cyber resilience solution addresses the above challenges to security in any type of IT environment, from on-prem to cloud to hybrid. It unobtrusively and automatically accesses up-to-date information about the configurations in the enterprise's data storage systems and checks for vulnerabilities, violation of industry best practices, organizational security baseline requirements, ransomware guidelines and non-compliance with regulations. It informs the relevant IT teams of violations and how to repair them in order to close the security gaps that put critical data systems at risk. And, it makes certain that configurations in place will ensure ability to recover data in the event of a cyberattack. Data Security Advisor runs on our Resilience Assurance Platform.

Key Solution Benefits

Hardens data system configuration to prevent unauthorized access to masses of high-value data assets

Ensures compliance with cyber resilience regulations and standards

Facilitates successful internal and external InfoSec audits
Automates vulnerability assessment and compliance for data storage systems

Ensures recovery from a data-focused cyber attack
Verifies data copies and backups are isolated and up to date

ContinuitySoftware.com

Data Security Advisor is built on the foundation of a proven methodology used by major enterprises worldwide

Data Security Advisor provides the first and one-of-a-kind comprehensive cyber resilience solution while also enabling enterprises to prepare for and meet information security audit requirements. **The solution** focuses on four fundamentals to achieve and maintain cyber resilience in IT environments:

Meet security best practices and comply with regulations

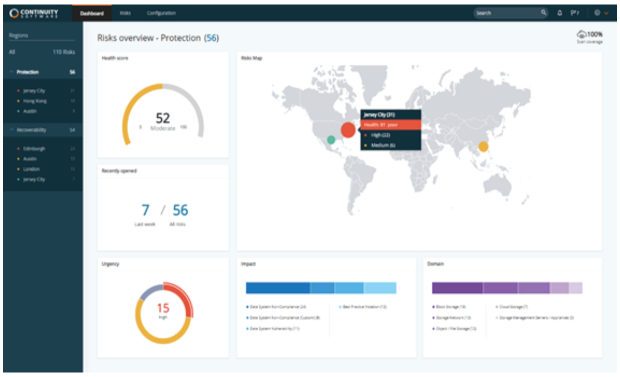
Enterprises must follow security best practices and comply with regulations in the face of constantly changing component configuration which puts critical data systems holding high-value data assets at risk.

Data Security Advisor analyzes the configuration of on-prem and cloud data storage systems and detects vulnerabilities that pose a security risk to critical business data. It enables automatic detection of violations of vendor security best practices, community-driven best practices, security baseline requirements (built-in and custom), ransomware protection guidelines, non-compliance with standards and regulations (PCI DSS, HIPAA, NIST, etc.), and vulnerabilities.

The solution enables demonstration of a repeatable, trackable, and ongoing vulnerability assessment process, proving compliance with all relevant regulations.

Support all enterprise data storage – on premises and in the cloud

In whatever type of environment data storage is located (on-prem, public cloud, private cloud or hybrid), Data Security Advisor scans for cross-domain and in-layer resiliency risks and checks for misconfigurations that could affect security, compliance and recoverability of high-value assets on all relevant systems and components such as EMC, Netapp, Brocade, AWS S3, etc. Configuration deviations from best practices and regulation are proactively detected.



Data Security Dashboard provides a health score of critical high value data assets

An enterprise-grade solution

Data Security Advisor enables enterprises to scan thousands of target systems in multiple locations and rank detected risks in terms of urgency and business impact, supplying detailed information such as the affected service, application, datacenter, etc. Comprehensive guidance for repairing the risks are automatically delivered to the relevant teams and business/service owners.

Data Security Advisor's built-in plugins and APIs enable enterprises to seamlessly integrate with Vulnerability Management systems enabling a complete view of all security gaps and vulnerabilities and prioritization of repairs. It also integrates with the enterprise's ITSM tools such as ServiceNOW and others to facilitate automatic incident generation and assignment for remediation.

Ensure recoverability from a cyberattack

Data Security Advisor verifies cyber-recoverability best practices (isolation, retention, immutability) to ensure that data is recoverable in the event of a cyberattack. The solution analyzes storage and file system configurations to check whether they have valid and secured recovery copies available and comply with stated recovery objectives; compliance with ransomware protection guidelines is also examined.

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 encompass cyber resilience. Our solutions protect mission-critical data residing in vulnerable storage systems against cyberattacks, prevent data loss, and ensure data recoverability.