

Cayosoft®

Solution Brief

Cayosoft Guardian: A Comprehensive IT Resilience Orchestration Solution

BACKGROUND

In today's digital-first world, IT resilience has become a cornerstone of business continuity and operational integrity. IT resilience refers to an organization's ability to maintain service continuity, safeguard data, and support operational capabilities in the face of disruptions. This concept extends beyond traditional disaster recovery, encompassing the ability to adapt to and recover from IT infrastructure failures, cyberattacks, and other unforeseen challenges efficiently.

In today's world, Microsoft Active Directory (AD) plays a cornerstone role in the on-premises and hybrid enterprise IT environments, acting as the backbone for user and resource management, authentication, and authorization processes. Because of its dual role, Active Directory has become the prime target of ransomware attacks:

- As the primary source of user identities and their privileges, it holds the metaphorical keys of the kingdom, used by attackers to discover resources and move laterally gaining control of ever more powerful accounts and critical resources.
- As the heart of many IT infrastructures, its availability and integrity are critical for ensuring seamless access to resources and maintaining business operations. For absolute majority of enterprises today, if Active Directory is down everything is down and the company's business comes to a complete stop.

Needless to say, these factors necessitate robust protection and recovery strategies.

WHY CAYOSOFT GUARDIAN

Enter Cayosoft Guardian, a solution uniquely positioned to address these challenges. Cayosoft Guardian distinguishes itself by offering comprehensive monitoring, protection, and recovery for Active Directory and hybrid environments. Unlike traditional solutions that may focus solely on backup or monitoring, Cayosoft Guardian integrates these capabilities with advanced features like continuous change tracking, threat detection and response, instant rollback, and automated disaster recovery processes. This integration facilitates a more resilient IT infrastructure capable of quickly responding to and recovering from incidents.

Cayosoft Guardian's emphasis on automation, enhanced public cloud support, and its no-code interface streamline the management of IT resilience tasks. By simplifying complex processes and enabling quick recovery from disruptions, Cayosoft Guardian ensures that organizations can maintain operational continuity with minimal downtime. Its advanced features, such as automated failover, failback, replication, and orchestration, along with discovery, dependency mapping, and workload analysis, make it the leading IT Resilience Orchestration solution.

In the following sections, we will delve into how Cayosoft Guardian leverages these capabilities to provide a comprehensive IT resilience orchestration solution, ensuring that enterprises can navigate the challenges of maintaining a secure, available, and reliable IT environment.



AUTOMATED FAILOVER, FAILBACK, & AVAILABILITY

Cayosoft Guardian elevates IT resilience by offering robust automated failover and failback capabilities, which are essential for ensuring continuous service availability during and after disruptions. These processes are critical for businesses that need to maintain uninterrupted operations, even in the face of unforeseen IT infrastructure failures or cyberattacks.

Failover

Cayosoft Guardian creates a standby version of on-premises Active Directory forests in the cloud. These standby forests are automatically tested, and any issues found get promptly reported. Cayosoft Guardian's enhanced public cloud support, including AWS and Azure, facilitates security isolation, provides flexibility, and removes the need for hardware provisioning. In the event of service disruption, administrators simply unpause the cloud version of the affected forests and re-route the traffic. Operations are shifted to the standby system, minimizing downtime and maintaining business continuity.

Failback

Built-in advanced threat detection, change history, and rollback help forensic analysis and restore on-premises Active Directory to a fully functional system, clean of vulnerabilities and malware. This ensures a smooth recovery process and helps maintain data integrity and consistency.

High Availability

Cayosoft Guardian in real-time captures changes made to Active Directory, Entra ID, Office 365, and Intune. Should disruption be caused by any erroneous or malicious changes, these can be rolled back immediately with no downtime. In addition to this, Cayosoft Guardian can set up isolated secure cloud recovery sites in Microsoft Azure or AWS, allowing to switch over network traffic to standby Active Directory forests should the original AD forest be taken completely down. These two mechanisms create effective multi-tiered high availability protection for incidents of all scale.

REPLICATION & ORCHESTRATION

Cayosoft Guardian's replication and orchestration features provide scheduled replication of directory data, ensuring that data is always up-to-date and recoverable. This capability is valuable for any organizations that cannot afford significant downtime or data loss.

Continuous Replication

By continuously replicating directory data, Cayosoft Guardian enables organizations to instantly roll back changes made to Active Directory, Entra IS, Office 365, or Intune, ensuring that business operations can proceed without significant interruptions. Changes can be rolled back in the original environment, or should it be damaged beyond recovery, companies can switch their traffic to the fully tested standby forest that Guardian creates in a secure cloud environment.

Orchestration

The platform's orchestration capabilities give complete end-to-end automation and peace of mind to administrators. Cayosoft Guardian creates backup and recovery plans, performs the backups, provisions target environment, automatically performs each step of Microsoft's official Active Directory Forest Recovery manual, and tests the results. This automated orchestration ensures that recovery processes are consistent, reliable, and scalable, regardless of the complexity of the IT infrastructure.

DISCOVERY, DEPENDENCY MAPPING, & WORKLOAD ANALYSIS

Cayosoft Guardian's built-in discovery and dependency mapping features provide a comprehensive view of the IT environment, identifying interdependencies between different systems and services. This is crucial for ensuring that recovery efforts are coordinated and effective, particularly in complex hybrid environments.

Object Discovery and Dependency Mapping

By automatically discovering and mapping dependencies, Cayosoft Guardian helps organizations understand the relationships between different elements of their IT infrastructure such as: AD user accounts, their corresponding Entra ID cloud accounts, their mailboxes, and devices. This is essential for restoring objects to their consistent state.

Workload Analysis and Service Dependencies

Cayosoft Guardian automatically discovers and maps dependencies between Active Directory-integrated services. It automatically creates a recovery plan (blueprint) and executes consistent recovery.

DISASTER RECOVERY MANAGEMENT & RUN BOOK CREATION

Cayosoft Guardian enables organizations to define, execute, and analyze disaster recovery plans with precision. This includes the creation of detailed run books that guide the recovery process, ensuring that every step is executed correctly.

Disaster Recovery Management

With Cayosoft Guardian, organizations can manage their disaster recovery processes more effectively, from planning and simulating, to execution, testing, and analysis. This ensures that recovery efforts are well-coordinated, transparent, and reliable.

Run Book Creation

The platform creates run books (jobs or plans) that detail every step of the recovery process. This not only simplifies the execution of complex recovery tasks but also ensures that all team members have clear understanding of the recovery process and the roles of the technology in a disaster recovery operation.



REPORTING & VALIDATION OF RECOVERY CAPABILITY

Cayosoft Guardian's reporting and validation features ensure that organizations have a clear understanding of their recovery capabilities and can demonstrate compliance with relevant regulations and standards.

Reporting

The platform provides detailed reports on the success of recovery exercises, highlighting areas of improvement and ensuring that stakeholders have visibility into the IT resilience posture of the organization.

Validation

Cayosoft Guardian automatically performs data consistency checks and integrity validations for each set of backups. This ensures that the organization's recovery capabilities are not only theoretically sound but have been practically tested and validated.

By integrating these advanced functionalities, Cayosoft Guardian offers a comprehensive solution for IT resilience orchestration, ensuring that organizations can maintain operational continuity, safeguard data, and respond effectively to disruptions.

KEY HIGHLIGHTS

- **Automated Failover and Failback**
 - Ensures continuous service availability, minimizing downtime during disruptions
- **Replication & Orchestration**
 - Provides prompt recovery & seamless management across hybrid environments
- **Discovery & Dependency Mapping**
 - Offers effective & consistent recovery of complex IT infrastructures
- **Disaster Recovery Management & Run Book Creation**
 - Facilitates detailed disaster recovery planning, execution, & analysis
- **Reporting & Validation**
 - Delivers thorough reporting & automatic validation of recovery capabilities, ensuring preparedness & compliance

CAYOSOFT GUARDIAN | IT RESILIENCE ORCHESTRATION POWERHOUSE

Cayosoft Guardian, with its advanced Forest Recovery feature, is a critical solution for organizations aiming to bolster their IT resilience. This brief has explored the multifaceted capabilities of Cayosoft Guardian, emphasizing how its innovative features facilitate robust IT resilience orchestration. Through automated failover, failback, replication, orchestration, discovery, dependency mapping, disaster recovery management, and comprehensive reporting and validation, Cayosoft Guardian ensures that businesses can maintain operational continuity, safeguard data, and efficiently manage recovery processes in the face of disruptions.

Cayosoft Guardian's emphasis on no-code interfaces, enhanced cloud support, and integrated approach makes it as a user-friendly yet powerful tool for modern IT environments. Its inclusion of features like threat detection, enhanced monitoring and reporting, aligns with the shift-left practices, enhancing collaboration across DevOps and SRE teams.

As organizations navigate the complexities of maintaining resilience in dynamic IT landscapes, Cayosoft Guardian stands out as a comprehensive solution that not only protects Active Directory and hybrid environments but also empowers IT teams to respond with agility and precision to any challenge. With Cayosoft Guardian, businesses can ensure their IT infrastructure is not just protected but also primed for rapid recovery and sustained operational excellence.

This brief underscores the importance of choosing an IT resilience orchestration solution that aligns with the evolving needs of hybrid IT environments. Cayosoft Guardian's unique blend of features and capabilities makes it an indispensable tool for organizations seeking to enhance their resilience strategies and ensure their IT infrastructure remains robust, secure, and agile in the face of ever-changing challenges.

ABOUT CAYOSOFT

Cayosoft delivers the only unified solution enabling organizations to securely manage, continuously monitor for threats or suspect changes, and instantly recover their Microsoft platforms, including on-premises Active Directory, hybrid AD, Azure AD, Office 365, and more. To learn more, visit cayosoft.com.