SIOS

SIOS WHITEPAPER

# How to Patch Without the Pause: Near-Zero Downtime with HA

Protecting Critical Systems from Downtime & Disasters

us.sios.com

In today's fast-paced digital landscape, effective patch management is critical to maintaining cyber security, stability, and compliance. Patch management is the process of applying updates to OS and applications to protect against cybersecurity attacks and fix software bugs. Operating systems, databases, and application-level vulnerabilities are prime targets for cybercriminals seeking to exploit weaknesses. However, applying OS and application patches and updates—especially in mission-critical environments, where even short periods of downtime are costly—can introduce downtime risks, that can disrupt important business operations and lead to serious financial losses, regulatory fines, customer dissatisfaction, and brand loyalty.

SIOS LifeKeeper and DataKeeper high availability (HA) clustering software provides a strategic solution, enabling organizations to apply updates while maintaining application availability. By integrating advanced HA into patch management strategies, IT teams can test and deploy patches with minimal disruption, enhancing both security posture and business resilience.

## High Availability in Cybersecurity and Patch Management

Historically, IT organizations have taken a cautious approach to any changes related to their OS or critical applications. Following best practices, they test updates and patches extensively in quality assurance (QA) environments before deploying them to production systems. They have traditionally prioritized testing and risk reduction over speed of deployment.

However, the growing sophistication and frequency of cyber attacks, combined with regulatory demands and rising expectations for 24/7 uptime, has put pressure on IT organizations to apply updates and patches as quickly as possible. IT teams face a dilemma: either delay patching to test thoroughly but risk cyberattacks, or deploy untested patches and risk costly downtime and troubleshooting.

### Key Terms: Patch Management with HA Clustering Solutions

**Failover:** Active workloads are moved to a standby node in the cluster.

**Patch & Test:** Patches are applied to the inactive server and tested without impacting production.

**Failback:** If testing is successful, workloads shift back, and the patch process repeats on the second node.

**Rollback Ready:** If issues are detected, workloads remain on the unaffected server while further investigation occurs.

## The Impact of Zero-Day Exploits

The rise of zero-day attacks and ransomware campaigns has shifted patching priorities toward speed and agility. Attackers now actively scan for known vulnerabilities within hours of patch announcements. Delayed patching dramatically increases the risk of a breach. According to the Ponemon Institute, 57% of data breaches were linked to vulnerabilities for which patches were available but not applied.

Depending on the industry, IT may also need to comply with regulations requiring timely application of software updates, such as National Institute of Standards and Technology (NIST 800-53), Health Insurance Portability and Accountability Act (HIPAA Security Rule), and Payment Card Industry Data Security

Standard (PCI DSS 4.0). However, incidents like the recent CrowdStrike update failure underscore the potential consequences of rushed patches or insufficient testing.

## Challenges of Planned Application Downtime in Patch Management

Planned downtime is another challenge posed by patch and update management. In many cases, IT teams have to bring the entire environment offline while they implement the updates and perform a full restart of the system. For critical environments—such as hospitals, manufacturing plants, emergency services, and airports—downtime is not just expensive; it can be life-threatening. Gartner estimates the average cost of downtime at $5,600 per minute.

## High Availability Clustering: Enabling Seamless Patch Management with Near Zero Downtime

SIOS LifeKeeper and DataKeeper HA clustering solutions enable near-zero downtime maintenance while providing high availability and disaster protection at the application layer. With HA clustering, IT teams can apply patches rapidly using a "rolling update" methodology.

## How It Works: Advanced HA Clustering

In a SIOS HA clustering environment, critical applications are run on a primary server node that is connected in a "clustered" configuration with a secondary server node. Local storage on each of the server nodes is kept synchronized with efficient replication, such as SIOS DataKeeper. SIOS LifeKeeper clustering software monitors the health of the application and its supporting environment—network, storage, OS. If it detects a failure, it automatically moves application operation over to the secondary node through a process called a failover, where it continues to operate. When the issue is resolved, operation can be moved back to the original configuration. It also allows IT teams to manually switch operation to the secondary node and back again, quickly and without risk of data loss.

### Challenges of Traditional Patch Management

**Stability Concerns:** Patches sometimes introduce bugs, performance issues, or application conflicts. Testing patches before applying them in production is essential.

**Operational Downtime:** Applying patches to critical systems often required planned outages, leading to lost productivity and potential revenue loss.

**Complex Interdependencies:** Modern enterprise IT environments involve layered dependencies that complicate testing and deployment.

## Seamless Patching and Testing

This clustered configuration allows IT teams to apply patches to the secondary node first while the primary node remains operational. A patch can fail in one of two ways: either immediately during the initial patching process—causing obvious issues like crashes—or after the secondary node is brought into service, when application-level problems may emerge. In either case, the ability to quickly revert

operations back to the primary, unpatched node dramatically minimizes disruption and reduces risk. If testing is successful, operations can safely shift to the secondary node, allowing the primary to be patched without impacting availability. This methodology has several key advantages:

- **Accelerated Security Updates:** With failover support, organizations can apply patches promptly—minimizing the window of vulnerability and reducing exposure to ransomware or zero-day attacks.
- **Near-Zero Downtime:** Rolling updates eliminate the need for system-wide downtime, ensuring continuous availability of critical applications during maintenance.
- **Reduced Risk of Patch Failures:** SIOS HA clustering provides a built-in rollback plan. If a patch causes issues, production workloads can remain on the stable node until resolved—avoiding costly outages.
- **Compliance with Industry Regulations:** Healthcare, finance, and other regulated industries require timely patching for compliance (HIPAA, PCI-DSS, GDPR, SOX). HA clustering ensures these updates can happen without interrupting services or breaching service-level agreements (SLAs).
- **Improved Operational Efficiency:** Automation of failover processes reduces manual intervention, freeing IT staff to focus on strategic initiatives while ensuring reliable patch management.

### Case Study

A leading electronic health record (EHR) software provider struggled with downtime during monthly Windows patch cycles. With customers operating 24/7, including emergency departments, even planned outages were unacceptable.

By deploying SIOS HA clustering:

- Patches were tested on secondary servers without disrupting production.
- Updates were applied with near-zero downtime for users.
- Compliance with healthcare security mandates was maintained.

## Conclusion

In an era where both security threats and uptime expectations are at an all-time high, integrating high availability clustering into patch management strategies is no longer optional—it's essential.

With SIOS LifeKeeper and DataKeeper, organizations gain the tools to execute timely patches with confidence, minimize downtime, maintain compliance, and ensure operational continuity. By adopting this proactive approach, businesses strengthen their overall IT resilience and mitigate risks associated with both cyberattacks and patch failures.

## About SIOS Technology

SIOS Technology Corp. high availability and disaster recovery solutions ensure availability and disaster protection for critical Windows and Linux applications operating across physical, virtual, cloud, and hybrid cloud environments. SIOS clustering software is essential for any IT infrastructure with applications requiring a high degree of resilience, ensuring uptime without sacrificing performance or data – protecting businesses from local failures and regional outages, planned and unplanned. Founded in 1999, SIOS Technology Corp. (https://us.sios.com) is headquartered in San Mateo, California, with offices worldwide.


SIOS Technology Corp.
4 West 4th Avenue
San Mateo, CA 94402
Tel: 650-645-7000

info@us.sios.com
https://us.sios.com