

## *Avoid Private Cloud Downtime and Data Loss Risks*



### **Ready or not, the cloud is here**

Industry studies show that increasingly large portions of enterprise mission-critical applications are already running in a virtualized environment. With significant operational benefits offered by the cloud, this trend is expected to continue.

***But are you confident that your cloud infrastructure is resilient enough to provide the level of service availability required for your business?***

### **Built-in High Availability is great, but not risk-free**

While the cloud offers built-in redundancy and high availability options, no environment is fail-proof. The dynamic nature and abstraction which make the cloud so powerful are the very same features that make the management of cloud configuration extremely challenging and risk-prone.

As the cloud environment grows in size and complexity, it is practically impossible for IT teams to ensure 100% adherence to vendor best-practices. Many organizations have learned the hard way how even a minor mistake in ESX cluster configuration or storage allocation can result in a major outage or data loss incident.

### **Proactively detect private cloud risks**

The AvailabilityGuard Risk Discovery Engine™ automatically scans your private cloud environment in a non-intrusive, read-only mode, collecting up-to-date configuration information from vCenter, storage devices, virtual machines, and virtualized database servers.

It then analyzes the information gathered against the continuously updated Risk Signature Knowledgebase™ and pinpoints any misconfigurations that can lead to potential downtime and data loss.

### **Correct vulnerabilities before they impact the business**

Automated notifications and alerts are sent to the appropriate resources when availability or data loss risks are uncovered, allowing your IT teams to proactively address issues before they impact business operations.

### **Product Highlights**

- Automatic detection of private cloud availability and data protection vulnerabilities using a knowledgebase of thousands of risk signatures
- Analysis and presentation of potential impact on business services
- Identification of private cloud infrastructure optimization opportunities and best-practice recommendations
- Agentless, non-intrusive data collection using standard communication protocols (SSH, WMI, WinRM, Storage APIs, JDBC, Sudo) with zero impact on the scanned environment
- Integration with leading configuration management databases (CMDBs), ticket management systems, and enterprise consoles.

### **Key Benefits**

- Eliminate 90%+ of critical business downtime and data loss incidents by automatically detecting risks in your private cloud environment
- Continuously audit and improve private cloud resiliency and data protection practices
- Proactively address issues and eliminate time wasted fighting fires
- Improve coordination between virtualization, storage, and other IT teams
- Maximize the return on your private cloud assets

AvailabilityGuard delivers a robust feature set and cross-vendor/cross-domain/cross-platform support that allow IT teams to proactively identify and eliminate downtime and data loss risks across the entire IT infrastructure.

**Best-Practice Violation Detection**

Risk Detection Engine automatically uncovers deviations from vendor best-practices that could cause downtime or data loss risks.

**Configuration Gap Monitoring**

Continuous monitoring and verification of IT changes ensures proactive detection of configuration gaps between the production and DR/HA environments that create data protection, availability, or disaster recovery risks.

**The Power of the Community**

Community-driven Risk Knowledgebase contains thousands of configuration risk signatures and is constantly updated.

**Comprehensive SLA Management**

Policy-driven SLA Management monitors established SLA policies and alerts the appropriate teams when violations are detected.

**Automated Alerts & Notifications**

Instant notification of a potential problem to the proper team in your organization ensures timely response to any issue before it impacts the business.

**Risk Assessment Dashboard**

Provide non-IT executives with insight into the company's readiness and risk levels.

**Live Data Center Documentation**

Gain insight with an interactive, graphical topology of all data center entities, dependencies, and relationships.

**Data Center Change Audit Trail**

Ensure the entire data center team stays informed of all changes.

**Identification of Optimization Opportunities**

Discover unutilized storage space or other opportunities to reduce costs and improve overall system performance.

**Comprehensive Reporting**

Get the information you need, on-demand, to monitor and analyze your service availability risks.

**Integration with CMDBs and Tickets Management Systems\***

AvailabilityGuard can be integrated with CMDBs and ticket management systems from leading vendors (IBM Tivoli, HP OpenView, BMC Remedy, and others), allowing you to consolidate system management across the enterprise.

*\* Integration with Ticket Management Systems requires AvailabilityGuard/Enterprise+ Edition*

**Supported Platforms**

**Operating Systems**

- Solaris 8+
- Linux RedHat AS 3+, SuSE 8+
- Windows 2000+
- ESX / ESXi 3.5+

**Virtualization**

- VMware vSphere

**Databases**

- Oracle 8.1.7+
- MS SQL Server 2000 SP3+
- Sybase 12.5+
- DB2 UDB 8.1+

**Storage**

- EMC Symmetrix / VNX/ CLARiON / RecoverPoint
- NetApp Filers – All
- HDS AMS, USP, VSP
- IBM DS 6K, 8K, XIV, SVC
- HP XP

**Clusters**

All major cluster environments

**Replication**

All native local replication engines

**Volume Management**

All major LVMs and file systems

**The AvailabilityGuard Dashboard**

The AvailabilityGuard dashboard provides an immediate snapshot of service availability risks throughout your IT infrastructure and the ability to drill down to the details of any issue.



**The AvailabilityGuard Trouble Ticket**

AvailabilityGuard trouble tickets include detailed problem description, the potential business impact, and a suggested remediation action. Each ticket serves as consolidated view to facilitate collaboration among the IT resources tasked with solving the issue.

