



The **5** Essential Advantages: Agentless Technology for Data Protection Management

BOCADA[®]

Technology Brief

March 2005

Abstract

Today the common approach to collecting information about computing activity across the enterprise is to use software agents installed on individual clients and servers. However, when this approach is applied to data protection management in the enterprise environment, it has proven both ineffective and inefficient. This is because agent-based technology cannot meet the following five requirements that define the viability of a data protection management solution for the enterprise: ease of installation; compatibility with existing products; change management; network impact; and system performance. Considered collectively, these five factors are daunting and require a well thought-out approach. But, agentless technology, although challenging to design, is the only approach that meets large enterprise requirements and enables data protection management success.

Trusting in Agents: The Prevailing Approach

Software agents are applications that run in the background on individual clients and servers. An agent's function is to collect information in the environment. This may include configuration data, activity logs or real time snapshots of computing activity. Examples range from Simple Network Management Protocol (SNMP) agents, frequently used in networked environments, to everyday processes running in the background of a home PC. The defining characteristic of agents is that they run where the activity takes place. The use of agents has become commonplace. In fact, agents, by default, are now considered "the" way to collect data and understand status.

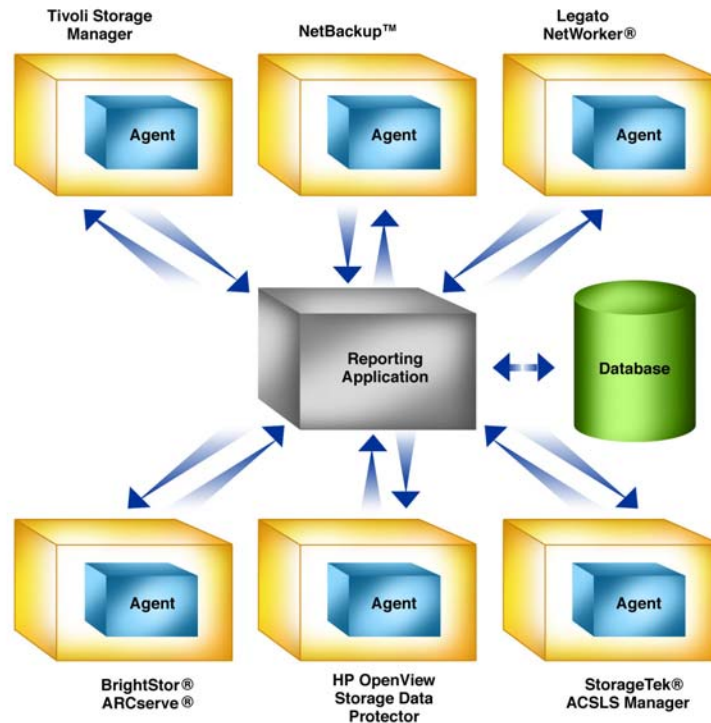


Figure 1. Agent Model. In the relatively simple scenario, the agent based model requires numerous different programs to be installed and running.

In data protection, virtually every reporting application uses an agent-based architecture to mine performance data and deliver it to a central collection place. Generally, these agent-based solutions have been well tested in controlled settings, and when they are installed properly on a dedicated backup server, they work according to specifications. However, when agent-based solutions are implemented in open systems across large enterprises, the complex nature of the environment often creates performance challenges beyond vendor control. Competition for network resources, an amalgam of software and hardware, and collisions with core application processes undermine agent-based solutions. Reliable data protection management for the enterprise demands a different approach.

Agentless Technology: Longer-term Investment, Greater Rewards

Agentless technology is quickly gaining traction in IT, specifically in patch management and application monitoring. However, it is still rarely used to support data protection management. Both practical and economic factors are behind this, as agentless solutions are time-consuming to develop. Most software companies would rather avoid the upfront investment and long development window required to deliver a feature-rich, robust agentless application.

With an agentless approach, the application resides on a central server and collects data by accessing monitored computers through standard

file-sharing methods. The application requires file-system access, and it must automate a complex two-way dialog when authenticating each machine. However, once these hurdles have been cleared, the challenging of extracting, processing and distributing the relevant information still remains. This challenge requires a deep understanding of the fundamental operation, application program interfaces (APIs) and the log file formats of each supported application.

In spite of the challenges inherent in an agentless approach, in data protection management it is the only way to handle the millions of transactions generated by hundreds of backup servers in a large enterprise.

The Data Protection Dilemma: A Matter of Scale

Working with multinational corporations, in some of the largest data protection environments in the world, Bocada has gained firsthand knowledge about the limitations of software agents. For example, some enterprises have attempted to address data protection management challenging by implementing self-built solutions. While these self-built solutions may have successfully achieved basic capabilities, most of systems continue to be limited to a basic set of operations and partial-scale deployments. Further, many enterprises find that continual maintenance and support are necessary to keep these self-built solutions in operation as software, applications and data structures evolve.

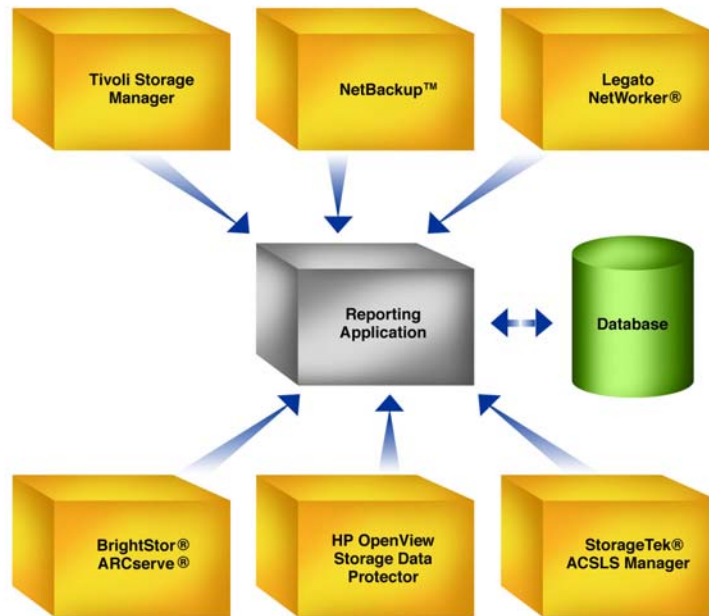


Figure 2. Agentless Model. In the same scenario as Figure 1, the agentless approach requires only one reporting application to be centrally installed on a single server. This simplifies installation and maintenance, while having little to no impact on system performance and reliability.

At the root of these problems lies the agent-based approach. In the enterprise data center, agent-based data mining and consolidation quickly becomes unmanageable beyond a certain number of assets. This threshold, in a structured environment with a single backup software application, is typically reached at 50 backup servers. In mixed or heterogeneous environments, the threshold may be reached at fewer than 25 backup servers.

Agentless technology, on the other hand, is an infinitely scalable approach to enterprise-wide data collection and is essential to successful data protection management in a large enterprise.

Key Issues, Essential Advantages

The agentless approach to data protection management offers five fundamental advantages.

Fast, Single-Node Installation. With installation confined to a single server, an agentless application can begin to gather information and provide useful reports within hours of installation. There is little to no impact on the operation of the data protection system—this is critical given the nature of continuous operations in large data centers. With the exception of network access to the backup servers and data, no configuration is necessary. Usually a backup server account with the proper permissions already exists; therefore, additional configuration is not required.

In contrast, the installation process of agent-based technologies is much more complex: each agent must be individually installed and configured. Often the IT staff must take each server out of production during available windows of downtime, which are ever-shrinking due to 24x7 operations of high-availability applications. If the installation does not go smoothly, production windows can be affected as well.

Compatibility Across Applications and Platforms. Most enterprises consist of a broad mix of backup applications, operating systems and versions. An agentless application is designed with this kind of environment in mind. The agentless application runs only on the central server, communicating with backup servers through standard file-access methods and protocols. A plug-in at the server handles the specific requirements of each backup application.

On the other hand, agent-based applications often conflict with underlying operating systems and existing processes. Moreover, a separate agent must be coded and compiled for each operating system, application and platform and take into account for endless combinations of release versions.

Change Management of Patches and Upgrades. An agentless application costs less to upgrade and maintain over time because it eliminates the need to maintain various versions of agents across individual servers. When a backup application is upgraded, the core functionality of the management platform can be retained by installing a new interface on the platform itself. The platform automatically detects the software version running on each backup server and then selects the appropriate interface.

However, in an agent-based environment both major and minor backup application upgrades generally require a new agent version to be installed. Every upgrade to an operating system (OS) or an infrastructure

component is a potential patch event. This causes a substantial change management burden—including hours of system downtime, staff time and expense and, most importantly, unnecessary risk.

Improved System Performance and Reliability. Agentless technology requires less resources from each backup server. Information transfers are managed through file-sharing, rather than by an application running continuously in the background. This method allows the backup server to control the frequency and depth of the dialog, which minimizes the impact on applications running concurrently.

Conversely, agent-based technology in a production environment demands considerable resources because it impacts the core function of the device or server being monitored. In fact, agents can over-consume resources and compromise server performance. A single server may even have multiple agents running simultaneously. When this scenario is multiplied by the hundreds of backup server that exist in most scaled environments, the likelihood of failure is overwhelming.

Predictable Network Traffic through Centralized Management. Agentless technology uses an orderly “pull” method for collecting data. The data protection application centrally manages and schedules queries. Subsequently, data retrieval is continuously conducted at regular and predictable intervals. Instead, agent-based technology “pushes” the data without centralized control, increasing the risk of system performance degradation as updates occur randomly. Scheduling for agent activities takes place at the individual server level and as the number of servers increases update management becomes an increasingly difficult and time-consuming issue for IT staff.

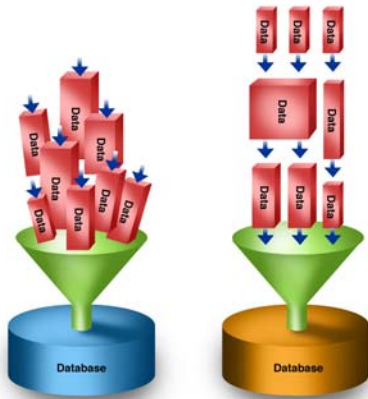


Figure 3. “Push” Method vs. “Pull” Method. With the agent based approach, software agents “push” data packages of different sizes at unpredictable times, which results in traffic bursts that bog down the network. In contrast, the agentless approach is centrally managed, “pulling” the data packages so that the network traffic is orderly and predictable.

Summary

Agent-based solutions have a secure place in IT systems and operations. However, data protection management challenges in large enterprises require a solution that meets the demands of scalability, performance and deployment without demanding ongoing support. The agentless approach is the answer because it meets the five essential requirements for an enterprise class data protection solution: ease of installation; compatibility with existing products; easy change management; low network impact; and minimal impact on system performance.

About Bocada

Bocada is dedicated to ensuring that data protection services, systems and processes meet organizational objectives for quality, cost and compliance. Our flagship product, BackupReport, provides objective insight into SLA performance, helping companies to improve data recoverability, reduce the cost of managing data protection operations, ensure compliance and communicate results. Bocada data protection management solutions have been deployed in more than 165 market-leading customer and partner environments worldwide, including Amgen, BankOne, Cap Gemini Ernst & Young, SBC, Sprint, Unilever and Xerox. Bocada is a private company headquartered in Bellevue, Washington.

For more information about Bocada and BackupReport, please contact us or visit www.bocada.com.

Bocada
 10500 NE 8th Street
 Bellevue, WA 98004
 Tel: +1.425.818.4400
 Fax: +1.425.818.4455
sales@bocada.com
www.bocada.com