

MetaVault

Enterprise Backup & Disaster Recovery

Powered by **VaultUSA**©

The Agentless Backup/Recovery Architecture:

How It Works to Reduce Costs, Bolster Security, and Simplify Scaling in All Business Environments

Vault USA and the Vault USA logo are trademarks of Vault USA LLC. All other brand and product names are, or may be trademarks of their respective owners. Vault USA LLC reserves the right to change or modify any of the product specifications or features described herein without notice. This document is for information only. Vault USA

TABLE of CONTENTS

<u>Section</u>	<u>Page No.</u>
<i>1: Preface</i>	3
<i>2: Background</i>	3
<i>3: The Problem With Agents</i>	4
<i>4: The MetaVault/VaultUSA Architecture</i>	5
<i>5: Why It Works</i>	6
<i>6: The Benefits of Agentless: Reduced Costs, Robust Security, and Simpler Scaling</i>	7
<i>7: MetaVault Provided by Optiva Systems</i>	8

Preface

This white paper describes how the Vault USA™ agentless solution improves the backup and recovery processes to reduce costs, bolster security and simplify scaling. The paper contrasts these benefits with the security risks, high licensing costs, administrative complexity, and CPU/LAN overhead problems associated with agent-based backup/recovery alternatives.

The Vault USA™ disk-to-disk (D2D) agentless software solution offers a highly reliable, high-speed replacement for legacy tape-based, remote site backup/recovery systems. Designed with a focus on fast data recovery, the Vault USA™ solution offers a unique agentless design, plus hard-coded security and WAN optimization techniques that differentiate it from competitive D-2-D backup-consolidation software products. Simple to set up and manage, the Vault USA™ solution offers bottom-line benefits that range from lower administrative costs to pay-as-you-grow scalability. Emphasizing data recoverability, the Vault USA™ solution helps organizations a single location or with geographically distributed sites reduce business risk by meeting Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) and ensuring dependable, ready access to critical office data.

Background

Businesses, especially with geographically distributed sites, are feeling the pain of protecting their valuable data. Ask IT managers to elaborate, and most will describe a trio of troubles:

- **Unabated growth.** Expanding from gigabytes to terabytes, petabytes, and beyond, and seemingly overnight—such is the storage challenge confronting IT administrators. Small office/home office (SOHO) businesses, small- and medium-sized businesses (SMBs), and corporate enterprises alike face the relentless pressures of data growth. The impact on backup and recovery processes is particularly painful: tape backup systems that sufficed in protecting a few offices' worth of data are too cumbersome, complex, and costly in larger environments. The problem only worsens as organizations add sites, systems, applications, and users. Recovery of large data stores is an even bigger concern. Day after day, companies need ready access to more and more data in order to keep critical operations running. Existing backup/recovery solutions often fall short in meeting RTOs and RPOs.
- **Increased security pressures.** Moving data to and from remote sites can be fraught with danger, particularly if the primary backup media is tape. Recent reports of tape-parcels vanishing from delivery trucks, unencrypted tapes packed with employee data gone missing from off-site data-protection services, and mounting threats of litigation and penalties have many businesses running scared. Companies also acknowledge that the hackers they face off against today are no longer just bored or mischievous teenagers, but more likely criminal organizations with paid technical thieves searching for high-payoff security holes.
- **Scarce local expertise.** Most tape backup products, even in their simplest forms, require an attendant at remote sites. But few organizations have technically proficient staffing resources available to administer backup operations at every single branch office or remote site. It forces an unpleasant choice—incur on-site IT staffing costs, or hand off the protection of business-critical data to inexperienced users who have other primary obligations. And again, the problem only worsens with data growth and increasing infrastructure complexity.

The Problem With Agents

Organizations typically address these issues by consolidating backup processes, choosing either to assign responsibility to a central data center or to outsource data protection to a service provider. Whichever path an organization follows, the presence of agents in the backup/recovery software utilized (be it either a tape or a disk-to-disk (D2D) product), will directly impact data security, recoverability, and costs. IT managers already know the downsides that accompany agent-based solutions:

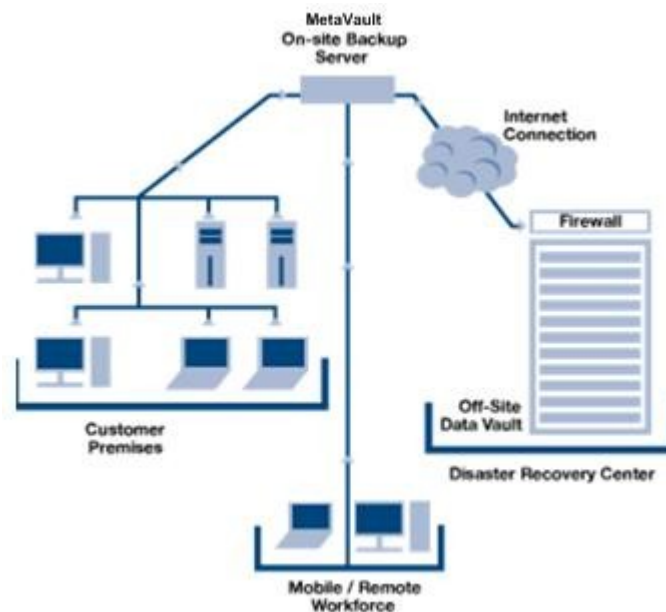
- **Compromised security.** A port in the firewall must be opened for every agent. And, because almost every agent has administrative privileges, it effectively creates a backdoor hole in the server architecture—tap into the agent and have your way with the server. With no “in-flight” encryption mechanisms, agents also put data at risk during transmission from the remote office to the data center.
- **More pieces of software to manage and to fail.** More sites, more data, more applications, more users, more systems, more agents—growth makes everything harder to manage, and agents only compound the problem. As the infrastructure expands in size and complexity, problem diagnosis takes longer. Operating system upgrades (now implemented monthly by many organizations) have broader impact and potential to break software, including proliferating backup agents. Agent management drains IT resources, causes disruptive downtime, and negatively impacts data recoverability.
- **Exorbitant licensing fees.** ‘Veritas users plead for simpler licensing’—that recent StorageSearch.com headline says it all (Source: StorageSearch.com, 26 Apr 2005). Most software vendors charge for software based on the old per-system model, a pricey plan that requires customers to keep close tabs on complex system and user landscapes. For many growing organizations, buying a site license is actually a simpler—albeit even more costly and often unnecessary—solution than trying to keep track of large numbers of backup products installed across hundreds or thousands of sites. There are even companies that now consult on doing audits to help enterprises try and lower license fees.
- **Mounting administrative costs.** Heterogeneous application environments can be administrative nightmares when backup processes require the installation and management of agents for every single flavor of database, application and operating system platform. It takes time and a lot of ‘touching’ of remote-site systems to push agents and agent upgrades out to every server in the backup roster. And each time a data center administrator or service provider has to deploy an agent or intervene to support it at a remote site, that cost rolls back into their business model, making it increasingly difficult to be competitive or stay within budget constraints.

To put licensing and administrative costs in perspective, an enterprise with just five offices can easily spend \$50,000 to purchase and maintain the file/print server, email server, database, and workstation agents required for backup processes. For large enterprises with thousands of agents, licensing and support costs can quickly add up to millions of dollars.

The Vault USA™ Architecture

Vault USA™ technology completely eliminates the negative impact of agents. How does it work? The Vault USA™ architecture consists of two software components: the DS-Client and the DS-System. DS-Client software, installed at the locations requiring backup on an existing or dedicated Windows, Macintosh, or Linux server, captures data from target backup machines. The DS-Client then conducts several data reduction processes, compresses, encrypts, and transmits the data via an IP WAN to the DS-System at the central location.

The DS-Client does not require installation of any backup agents on target servers, desktops, or laptops. The agentless DS-Client fully integrates with NT domains, Trusts and Novell NDS trees, and otherwise adopts the remote site's existing LAN security settings. Using standard APIs, the DS-Client can remotely log in to target backup systems, capture requested data, and securely manage transmissions to the central site. Utilizing delta blocking and common file elimination technologies, the DS-Client reduces the amount of raw data transmitted and stored at the off-site vault.



Our Backend Infrastructure, referred to as the DS-System, runs on IBM, NetApps, and Cisco hardware to manage the online storage repository for backup data transmitted from all our customers DS-Clients.

Vault USA™ software integrates a comprehensive feature set designed to maximize and accelerate data recoverability. An autonomic healing mechanism, for example, runs seamlessly in the background to identify and isolate corrupted or otherwise problematic files. As an added value, if a file is found to be unfixable, it is marked to be re-transmitted on the next scheduled backup. Another feature, the Local Restore tool, allows remote-office storage of the latest generation of a backup data file. This ensures that local users can restore critical data immediately and at LAN speed.

Additional Vault USA™ tools include an Online File Summary, Long Term Storage policy-making, a Discovery Tool to automatically ascertain characteristics of primary data, Service Level Agreement Management, Budget Allocation to set backup/restore capacity limits, Email Message Level Restore, Bare Metal Restore capability, Client and System Monitoring, and SNMP Integration.

Why It Works

The Vault USA™ software eliminates the requirement for locally installed agents because it leverages the protocols, APIs, methods and functionality that platform, operating system, database, and other application vendors utilize for remotely accessing and managing their own systems. While other backup/restore solutions require a unique backup agent (installed on every target server and workstation) for each type of system and application, the Vault USA™ architecture integrates support for all major platforms and applications into a single, optimized software system comprised of just two major components: the DS-Client (just one installed at each remote site) and the DS-System (installed at the vaulting location).

Another advantage of the Vault USA™ software is that it enables multi-level access controls. At installation, the DS-Client is assigned privileges to establish access rights that match the requirements of the site or organization. The DS-Client, for example, might be assigned multiple credentials for the same network to allow the domain administrator to back up all systems, including servers and workstations, while enabling users to control the backups of individual workstations. The Vault USA™ software has also been highly optimized to conserve both LAN and target-system CPU resources.

Another characteristic that differentiates the Vault USA™ software from other backup/restore solutions is that the software was designed from the ground up to be non-invasive and invisible in the customer environment. Because service providers must support multiple distributed customers with limited visibility and control of their clients' environments, a cost-effective solution must enable non-intrusive management—the backup/recovery solution must be centrally deployed, administered and supported across multiple client sites.

Admittedly a technology-development challenge with a unique-in-the-industry approach, the agentless design of the Vault USA™ architecture was nonetheless the right thing to do to ensure efficiency and profitability for Vault USA™ customers—both service providers and the customer. The result of that design and its real-world testing in demanding service provider and customer installations has helped make Vault USA™ today's technology leader with an innovative, sophisticated, and proven architecture.

The Benefits of Agentless: **Reduced Costs, Robust Security, Simpler Scaling**

Implementing an Vault USA™ backup/recovery solution produces immediate and dramatic benefits. Compared to agent-based alternatives, Vault USA™ software offers:

- **Significant savings.** Even if agents from other vendors were free, an Vault USA™ solution would still enable huge reductions in operating expenses. Example first-year operating expenses alone approach \$150,000 for an enterprise environment with 1,000 server agents. Annual server maintenance and operating expenses for this same configuration add up to nearly \$60,000. Eliminating agents eliminates those costs that are in addition to the purchase price of agents.
- **Simple licensing.** DS-Client licenses actually ARE FREE. The Vault USA™ offers businesses a unique pay-as-you-grow pricing model based on the aggregate amount of compressed data stored across the network. Simply purchase software the same as disk capacity—no license fees, no tracking, no overspending on site licenses—customers pay only for compressed capacity consumed.
- **One piece of software to install, manage, and diagnose.** The Vault USA™ solution even self-upgrades, so there is no time-consuming and administrative-resource-draining pushing of agents or updates out to hundreds or thousands of remote-site systems.
- **WAN/LAN/CPU resource conservation.** Vault USA™ software runs with negligible impact on servers and workstations, eliminating the CPU-cycle hits associated with agent-based solutions. Delta blocking, common file elimination and compression technologies also minimize impact on bandwidth and storage resources. While many agent-based backup/recovery solutions require implementation of high-speed pipes between the central data center and remote offices, the Vault USA™ solution enables the effective use of existing links such as DSL.
- **Robust, hardcoded security.** The Vault USA™ solution provides both 'in-flight' and 'at-rest' data protection, utilizing up to 256 bits for AES encryption keys to guarantee extremely safe data transfer and storage. And, it works within the organization's security framework—there are no agents to open hacker-tempting ports in the firewall. With secure data transmission across an IP WAN, the Vault USA™ solution helps businesses achieve compliance, minimize information-loss liabilities, and protect customer confidence.
- **Elegant scaling.** The DS-Client is capable of elegantly scaling both in the dimensions of capacity and performance. This type of scalability is critical for environments with large numbers of remote sites, high-capacity data sets, and rapid high data growth. While agent-based solutions compound complexity in rapid-growth environments, the Vault USA™ agentless backup/recovery solution easily accommodates new capacity, new applications, and new sites.
- **Backup consistency, improved recoverability.** The simplicity, efficiency, and security of the Vault USA™ system promotes implementation of consistent data backup programs across remote sites. With the ability to implement more frequent, successful backup processes, companies can significantly boost data recoverability in environments where success rates below 50% were once the norm.

About Optiva Systems

Optiva Systems is a provider of several business data solutions, including MetaVault. MetaVault uses VaultUSA technology; which is the nation's premier business continuity tool. Through our network of local service providers, disaster recovery centers, and immediate secure access to detain the event of a disaster, Optiva Systems promises secure online backup, fast data recovery, and steady business in today's uncertain world.

Contact Optiva Systems

For more information on Optiva Systems' MetaVault,

EMAIL: MetaVault@optivasystems.com

VISIT: www.optivasystems.com/MetaVault

CALL: (877) OPTIVA-1 x226

