THE PROTECTED BUSINESS – EVAULT ENDPOINT PROTECTION

JULY 2011

Since the dawn of digital data, storing and protecting long-term data has been an ongoing IT task. But in the midst of data protection practices that nearly always focus on protecting massive scale data, IT has seldom come to grips with protecting one critical asset that may be just as important as any server - the end user's computer.

Truth be told, there has been significant progress. One vendor in particular has recently stood out by turning to the cloud to deliver secured protection of end user systems, often called the endpoint. Scalability and self-service ease of use finally makes desktop protection possible for nearly any size of business. Just as important, the ubiquitous cloud and a Microsoft Windows Azure-based infrastructure can be reached from anywhere around the globe, promising to deliver protection for any endpoint that can access the Internet. This vendor hasn't missed the opportunity to reach beyond the task of simply backing up data, but also delivers true protection that can guard data against the loss or theft of a laptop or computer. The vendor is none other than an already trusted name in data storage and protection: i365, a Seagate Company, and makers of EVault data protection solutions.

With this in mind, Taneja Group decided it was time to examine EVault Endpoint Protection solution in greater depth. To do so, we put this i365 offering through the paces in our own lab facility in Phoenix, Arizona. What did we find? While we'll discuss the testing and findings in greater depth in this report, our clear takeaway is that i365 is setting the bar for simplicity in deployment, reduction in operational costs, and comprehensiveness in protecting this critical source of data in an age rife with risk for digital loss and compromise. What we saw suggests customers can deploy an entire endpoint data protection solution in less than an hour, while empowering users with data protection (including loss protection) with only a few mouse clicks. 5 minutes to data protection? Totally possible. 15 seconds to data recovery? That's what we saw. In this Technology Validation Report we'll review these observations and more.

THE LAPTOP CONUNDRUM

Throughout the evolution of computing, the endpoint has remained one of the most critical systems in the business. The original endpoint was the common desktop computer that was the computing infrastructure for conducting business in the distant past. With the onset of desktop and mobile computing, the desktop has often been the center of content and data creation, and data often stays stored where it is created. Our discussions with end-users today suggest that no matter the type of business, at least half of the data that is used in day-to-day business processes is stored on endpoints; data ranging from Microsoft Office files to rich content like video and audio. Even in business heavily biased toward centralized data, such as scientific analysis, around-the-clock work processes and low-cost local storage encourage workers to work with and store data locally. In other businesses with remote workers and sales forces where pipelines, contracts, and key IP may be on laptops, the critical data on endpoints often ranges toward 80% of the total data corpus.

87 Elm Street, Suite 900 · Hopkinton, MA 01748 · T: 508.435.2556 · F: 508.435.2557

Protecting the endpoint across a distributed infrastructure has long been a hassle. In businesses where nearly every desktop is actually a portable laptop, the lack of protection for distributed data carries enormous risk and consequences, and there are few solutions to this problem. Not only might key business data be lost by way of hard drive or computer failure, but by the risk of theft – often for the valuable data – is rapidly rising. The rule of thumb today is that 1 in 10 laptops will be stolen during a three-year period of use. In the age of ever more complex airport security and shrinking devices that are more easily tucked away, the rate of theft and loss is only increasing. Each theft or loss incident can come at enormous cost, with the typical costs revolving around trying to deal with the recovery and rebuild of important data. But today it is just as common to incur even greater costs – the costs of making a formal disclosure, losing customer confidence, incurring reputational damage, or even blackmail. Those costs can make endpoint loss an exercise that exceeds several hundred thousand dollars.

In the past, trying to achieve protection for this precious data was an exercise in bad choices. One option was a mission impossible goal of totally centralized data control with totally controlled access, which inevitably led to a business that didn't work. The other option was complex sets of storage and application software that could only intermittently protect data, or required a painful funneling of data to a centralized site with limited bandwidth. In this scenario a growing number of users would eventually exasperate the most patient of businesses. Both choices, and anything in between, were compromises and both have fundamentally broken down in a world where data and systems are more mobile and distributed than ever before.

COMPREHENSIVE ENDPOINT PROTECTION WITH EVAULT

The criticality of endpoint data demands protection that goes well beyond purely capturing and backing up data. The endpoint requires protection against both data loss and compromise. And as past experience has demonstrated, endpoint protection must be simple and easy to use like never before. In fact, endpoint protection really needs to be user self service oriented, and it needs to deliver enhanced user value to be voluntarily adopted. But simultaneously, this needs to happen with few demands upon IT staff and IT infrastructure that are already operating at their limits.

Such a set of requirements might seem like a pipe dream at first glance, but i365 is one vendor who has set out to deliver just that list of capabilities with their EVault Endpoint Protection suite.

i365 has approached the task of endpoint protection with a hosted offering designed for simplified web management and user self-service. Setup does not require an IT administrator, although organizations desiring specific configurations can mandate protection setup through a policy profile to control end user flexibility and capability. When fully unleashed, EVault Endpoint Protection can empower the end user with the ability to protect and recover their own data, and guards that endpoint from theft or loss by making it possible to remotely wipe a protected system.

EVault Endpoint Protection suite is delivered as a hosted service, and has been architected to take advantage of the scalable cloud services on the market today. The cloud-connected offering from i365 operates on top of the Microsoft Windows Azure platform. As a Windows Azure partner, i365 has harnessed this highly scalable, globally accessible cloud service to ensure EVault Endpoint Protection can scale to the largest of customer requirements, and does so with a level of responsiveness that will satisfy the most demanding of businesses. Cloud computing on Windows Azure provides a new economic model for businesses. With a cloud-based offering, there is no need for the business customer to buy servers to run the application. As a result, businesses are able to shift the capital expenditure associated with a traditional on-premise solution to an operating expenditure. With Windows Azure, businesses pay only for the capacity they use – elastic scalability ensures that there is always capacity to meet the needs of a growing business. Windows Azure also offers the opportunity to optimize uptime and efficiency – automated service management shields the business customer from hardware failure and routine maintenance. Robust multi-layered security

87 Elm Street, Suite 900 · Hopkinton, MA 01748 · T: 508.435.2556 · F: 508.435.2557

coupled with a system designed for reliability and fault tolerance assures that the service is available when needed.

On top of that infrastructure, EVault has built an offering that completely isolates and protects separate organizations, enables sophisticated levels of delegation and policy definition, and secures the data protection repository for each user with comprehensive encryption that makes sure data in the repository can only be accessed by the authorized user. i365 looks poised to deliver a unique set of features:

- Versatile endpoint protection of data to any depth desired.
- Hands-off implementation and operation.
- Data protection that stretches into the realm of data loss prevention.

With this focus in mind, Taneja Group set out to examine these capabilities in a hands-on exercise, and see if EVault Endpoint Protection was as powerful, easy to use, and end-user enabled as i365 claims it is.

VALIDATING EVAULT ENDPOINT PROTECTION

To assess EVault Endpoint Protection, we turned to a hands-on evaluation in a Taneja Group virtualized lab environment. This environment consisted of multiple virtualized desktops running on VMware's Fusion desktop hypervisor and on a 4 core, 16GB, Intel 320 SSD-based ESXi system, connected together in a 1gb network environment but at various times operating from remote locations outside the test lab environment. At various points, individual guest VM's were ported back and forth in this environment using the VMConverter tool from VMware.

Within this environment, we simulated the acquisition, initial setup, deployment and use of EVault Endpoint Protection across approximately 5GB of general productivity and rich media data (with the heavier percentage of the mix consisting of general productivity data such as Microsoft Word, Excel, PowerPoint, and Adobe Portable Document Format files). During the course of testing, we simulated approximately 10 users setting up and utilizing EVault Endpoint Protection, across the full range of EVault Endpoint Protection capabilities. We'll turn next to take a detailed look at our hands-on experience and our observations.

SIMPLIFIED DATA PROTECTION

To put EVault Endpoint Protection through the paces, we started with a few simple user setups. The EVault Endpoint Protection solution is fully managed through a web console where administrators setup users and devices. The supported device list currently includes Microsoft Windows XP, Windows Vista, or Windows 7 laptops, tablets, or desktops, and Apple Mac OS X with Linux support coming later in 2011.

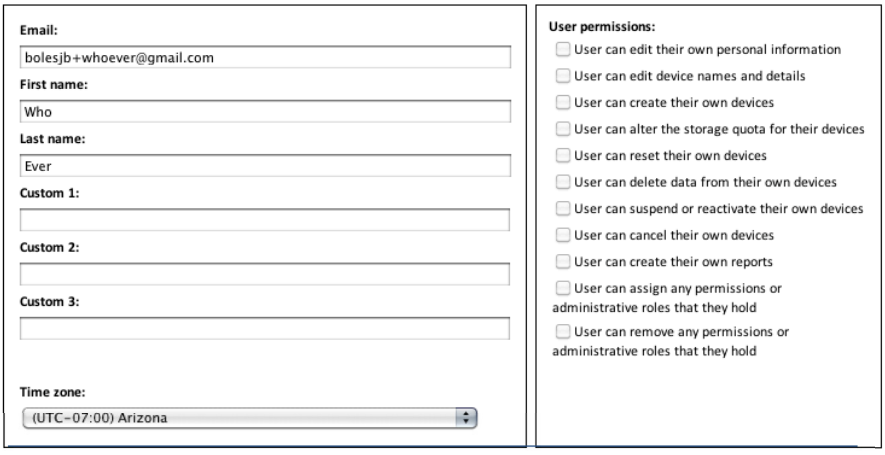

Figure 1: User setup screen in EVault Endpoint Protection web admin interface.

We first provisioned a single user and laptop in the EVault Endpoint Protection web console. When a business first signs up with i365, an administrator can access the web console and add users to the system. For larger environments, EVault Endpoint Protection supports

87 Elm Street, Suite 900 · Hopkinton, MA 01748 · T: 508.435.2556 · F: 508.435.2557

a "bulk import" capability that automatically prepopulates users and devices into the web console. As we began our testing, none of this was done and we entered the initial users and devices by filling out a few web page fields on three separate screens. Following this, an email invitation was sent to our test user, containing a link to the EVault software along with an activation code.

Acting as our test user, we downloaded and ran the executable software file. After installation, the software automatically launches a setup wizard, where the end user is prompted for the key (provided in email) and is then walked through an initial selection of what data to protect.

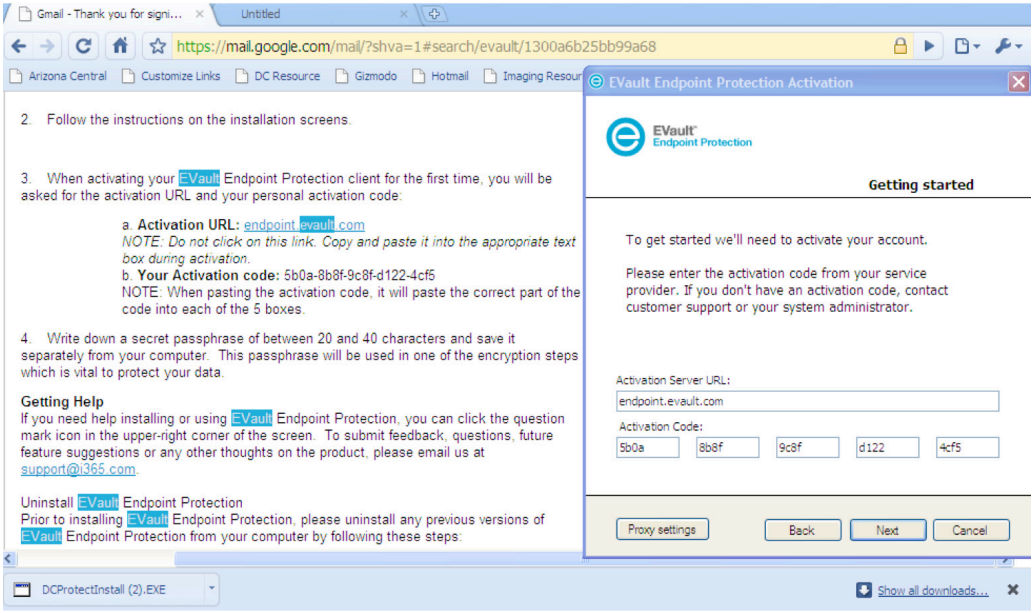

Figure 2: User self-service setup of the EVault Endpoint Protection client software.

We'll note that we did test the limits of EVault Endpoint Protection by installing it on an extremely dated and now unsupported version of Windows XP. We found that with Service Pack 3 (prior service packs are unsupported), installation went very smoothly. At the end of the installation, we were presented with an elegant interface that simplifies the user's view of EVault protection into two tabs labeled "Protect" and "Restore".

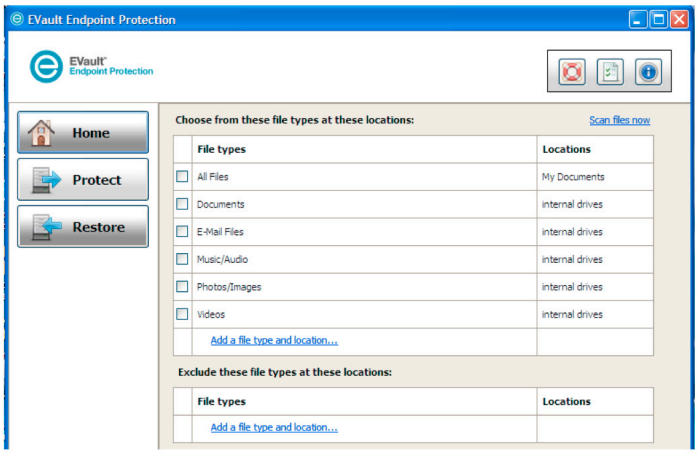

Figure 3: EVault Endpoint Protection client software.

Clearly, EVault Endpoint Protection built on an auto-scaling Microsoft Windows Azure platform is redefining the landscape for backup simplicity. There are no complex device parameters to configure. There are no communication problems to worry about - if the client can access the web, they will be able to protect data. There are no complex installation processes or hoops to jump through. Just enter basic information, and the end user is off and running on their way to protection.

Technology Validated:

5 minutes to install.

DATA PROTECTED

One of the goals with EVault Endpoint Protection was undoubtedly unobtrusive, always-available data protection and recovery. Data transmission is highly optimized to conserve bandwidth and bandwidth utilization is throttled to make sure data protection doesn't interfere with the user experience. The end user's computer is protected in the cloud and with a localized cache that retains the latest changes. This offsets bandwidth irregularities or disconnections from the network while minimizing the impact on backup and recovery operations. We put the full range of these capabilities to the test, using a variety of data sets and clients from different locations and types of networks, and under various working conditions.

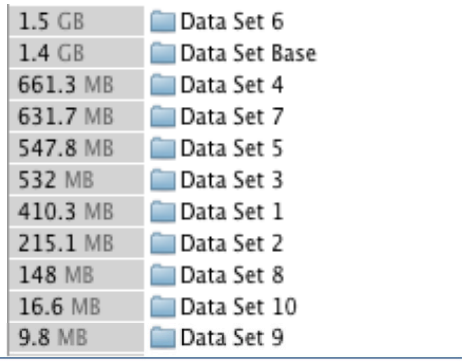

Figure 4: We used a variety of data during our test, generally revolving around MS Office files, PDFs, limited rich media, and a limited set of applications. Our initial data set included a download folder, but further test runs used just over 6GB of fairly unique data.

As the first step in our testing we started with a basic 260MB test data set in a single folder on our Windows XP laptop (a download folder that held over a year of downloaded office productivity files, PDFs, application files, and rich media). Following the installation of our client, we selected a specific folder on our laptop for protection, and started the protection process by clicking the "Scan Now" link in the top right corner of the dialog. If there was any deficiency in the EVault client interface, this would be it but it is a minor quibble - the "Scan Now" link was not entirely intuitive, and could more accurately read "Protect Now" since once it is clicked data protection immediately goes into play.

In our case, the EVault Endpoint Protection began protecting our 260MB of data. It proved fast and efficient. EVault immediately began creating a local vault of protected data and synchronizing the local vault with the Windows Azure based EVault cloud infrastructure. As data protection started, the default configuration of the EVault client kicked in and throttled our bandwidth usage to only 80KB/s.

With this level of network utilization on a residential cable connection, we saw no impact on internet performance even though we were simultaneously accessing live video streams, using Skype, and heavily multi-tasking with browser based applications across multiple systems. In turn, we removed the default bandwidth throttle under settings, and let EVault perform as fast as it wanted - generating average bandwidth utilization between 400KBps and 500KBps.

Typical bandwidth efficiency is challenging to observe short of a network sniffer, which we did not employ. But based on the timing of data synchronization and the 80KBps bandwidth limit that we left in place for additional tests, we've concluded that EVault compression reduced our data transmission by approximately 3 to 1. With this compression and the default bandwidth throttling, EVault should be capable of protecting slightly more than 400MB of data in just under 30 minutes. For the typical business only attempting to protect productivity files, it is entirely realistic to setup EVault, deploy the software, and achieve data protection within 30 minutes.

Technology Validated:

30 minutes to data protection.

87 Elm Street, Suite 900 · Hopkinton, MA 01748 · T: 508.435.2556 · F: 508.435.2557

DATA PROTECTED - THE BUSINESS EXPERIENCE

Following our initial EVault client setup, we moved on to protecting larger sets of systems and data. We created a list of 10 user accounts, including some with multiple laptop and desktop devices, and submitted them to i365 to evaluate their automated setup process. We also setup a couple of users manually ourselves to review the configuration options. We then used these accounts to backup data on several Windows 7 Enterprise virtual machines, with a variety of different data sets.

As we walked through our setup and configuration of additional users, we observed that EVault Endpoint Protection comes equipped with a number of management and policy tools that can shape the behavior of EVault for any sized business from the smallest to the largest. On one level, the EVault system has an organizational hierarchy that could conceivably support business unit delegation in large enterprises or service providers. Moreover, the system comes with pre-configured data protection policies that can both ease and control setup by dictating what data is protected and how frequently, or even opening the door to total user control of data protection. We experimented with both flavors. Simultaneously, if desired the web administrative interface can also be granularly extended to end users, power users, or other administrators with a series of check boxes that control what they can see and do.

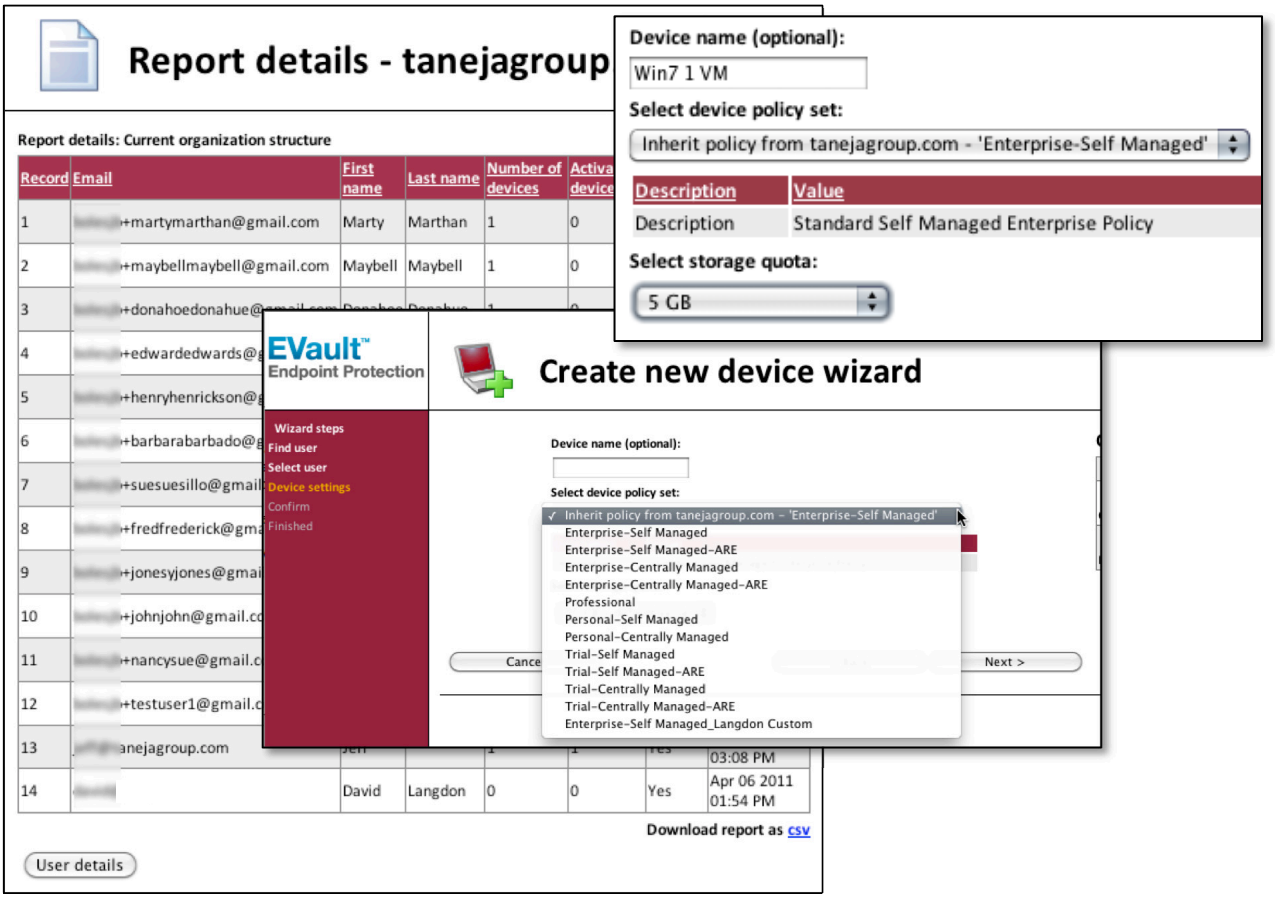

Figure 5: Device and device policy configuration screens in the web administration console, and a listing of our final end users.

Overall we were impressed by the ease of use and simplicity with which EVault could be setup to protect data, and even as we shifted from setting up one to multiple users there was little additional management involved. We can say with confidence that EVault Endpoint Protection is one of the simplest and quickest solutions for desktop and laptop protection in the market. From our

87 Elm Street, Suite 900 · Hopkinton, MA 01748 · T: 508.435.2556 · F: 508.435.2557

experience, we have a tough time believing any business would require much more than 30 minutes of time to start protection of their business.

Technology Validated:

30 minutes to *business* protection.

DATA PROTECTED - THE USER EXPERIENCE

But user experience is at least as important as the general ease of use and speed of the solution. Many endpoint solutions have fallen by the wayside because they were too complex or intrusive for the end user. After setting up our additional users in EVault Endpoint Protection, our designated user emails received invitations, and we again installed the EVault software to begin backing up our multiple clients. Moreover, we ran these backups simultaneously over the same shared residential cable network. During the initial data set backup, we also altered bandwidth configurations, and could see throughput stream to high speeds ranging between 600KBps to 1MBps over multiple machines.

In some cases we used a power user type backup policy where the end user could select the location and types of data to be protected. This includes default categories of productivity documents (PDF, DOC, XLS, etc.), audio, video, and email and contacts, as well as configuring custom filters for unique file types and specific file locations. In other cases, we used more limited policies that would automatically scan for productivity documents without involving the user, but still allow the user to restore data upon demand. We reviewed the policies for standard productivity files and found EVault to be quite thorough in scanning data across the system in all locations.

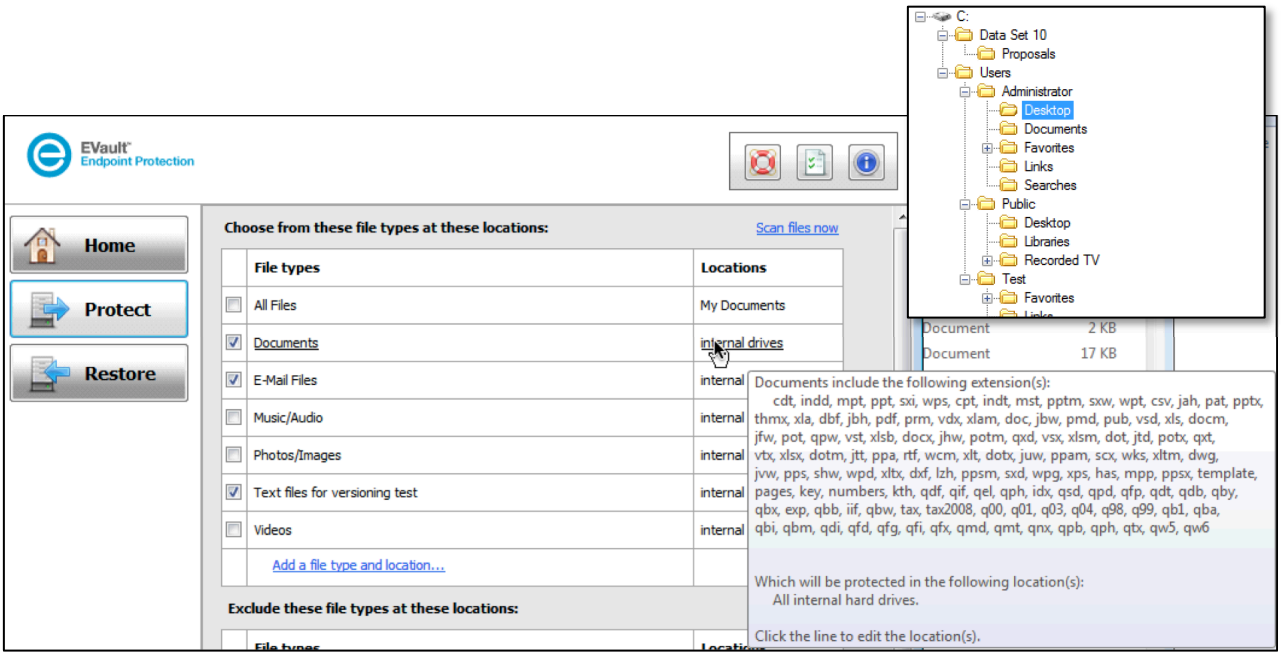

Figure 6: EVault Endpoint Protection client comes with a number of preconfigured file filters, and does a good job of finding, protecting, and restoring all files scattered across a system. Using policies, administrators can elect to let users configure their own protection, or define fixed file types and locations for protection.

87 Elm Street, Suite 900 · Hopkinton, MA 01748 · T: 508.435.2556 · F: 508.435.2557

During the backups, we also roamed to coffee shops, paused and restarted machines, came and went from wireless connections, and never had a problem. We observed continuing protection during disconnections and irregularities, with the ability to both protect and recover data still operating even when an Internet connection was not available.

Technology Validated:

Invisible in operation, with excellent ease of use for the end-user.

TOTAL PROTECTION

Simple and quick data protection isn't much good if it doesn't also pave a path to simple and quick data recovery. EVault was no slouch in this area either. As we've mentioned already, EVault can use a local cache to speed data recovery if an Internet connection is available. We performed one such recovery of 260MB of data in approximately 15 seconds, which was much faster than our in-use connection was capable of doing. The interface for selecting and restoring data is extremely straightforward, even across multiple generations of data protection. EVault gives end-users access to the latest version of protected data in every case, using the file name as the master reference to a piece of data.

Technology Validated:

15 seconds to data recovery.

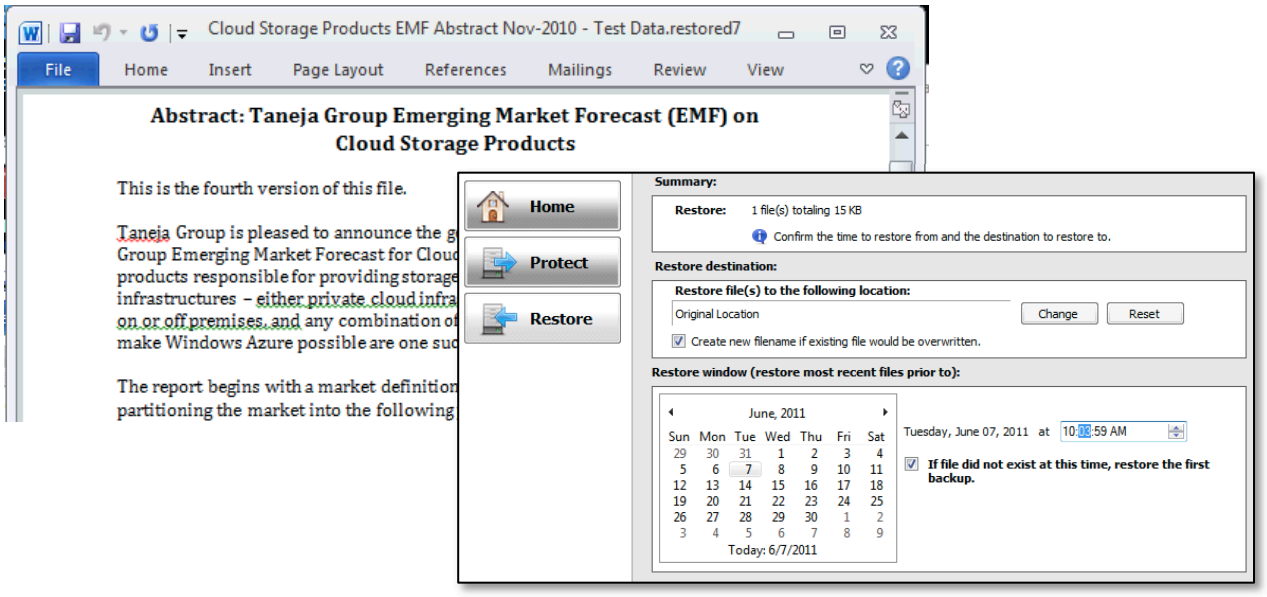

Figure 7: We versioned and restored various files throughout the course of our testing, demonstrating that EVault effectively identifies changed file versions across backup jobs. We also demonstrated that EVault allows the end user to restore files in the version they were in on disk at various points in time.

87 Elm Street, Suite 900 · Hopkinton, MA 01748 · T: 508.435.2556 · F: 508.435.2557

While EVault races along with full restore jobs, it also protects each different file version every time it does a backup. Our one single critique of the end user experience rests in this area: while every file version is protected and available, finding the individual versions must be done by cycling back the time clock without clear visibility into how many different versions of the file exist. Cycling the restore point and watching the file size information can find different versions of the individual file. But it isn't easy or very straightforward, and may be the one and only time that EVault Endpoint Protection generates a help desk call. This pales in comparison to the critique we would generate for most newly released products, and we expect to see the future bring new capabilities here.

SECURED: PROTECTION TURNED INTO SECURITY AND MANAGEMENT

But EVault hasn't just stopped at data protection. As we've mentioned, one of their most differentiating features is how they've wrapped the endpoint in additional governance by protecting the endpoint against loss. i365 does this by allowing the administrator to apply at rest encryption as well as trigger deletion of data from a lost system and recover data to a replacement system. Both of these tools work with tremendous ease of use and transparency. Loss of a system merely requires an administrator to select a device erase in the web interface, and reset the device. This will then generate a new activation key that can be passed to the user just like the original invite. The EVault software on the original machine will erase the data and reboot the machine on the next network access. Meanwhile, once the EVault software is installed on a new device, the end user can access all of their protected data and restore it to the same or different locations.

Migrating data

During our testing, we used EVault Endpoint Protection as an effective data set migration tool as well as a loss protection tool. Loss protection is a critical element in endpoint protection strategy. But in our view, the power of EVault as a total data management "and" security tool shouldn't be overlooked, as EVault may just simplify endpoint data migration tasks alongside securing data. Performing comprehensive data migration by user self-service may have tremendous desktop support impact inside any size of business.

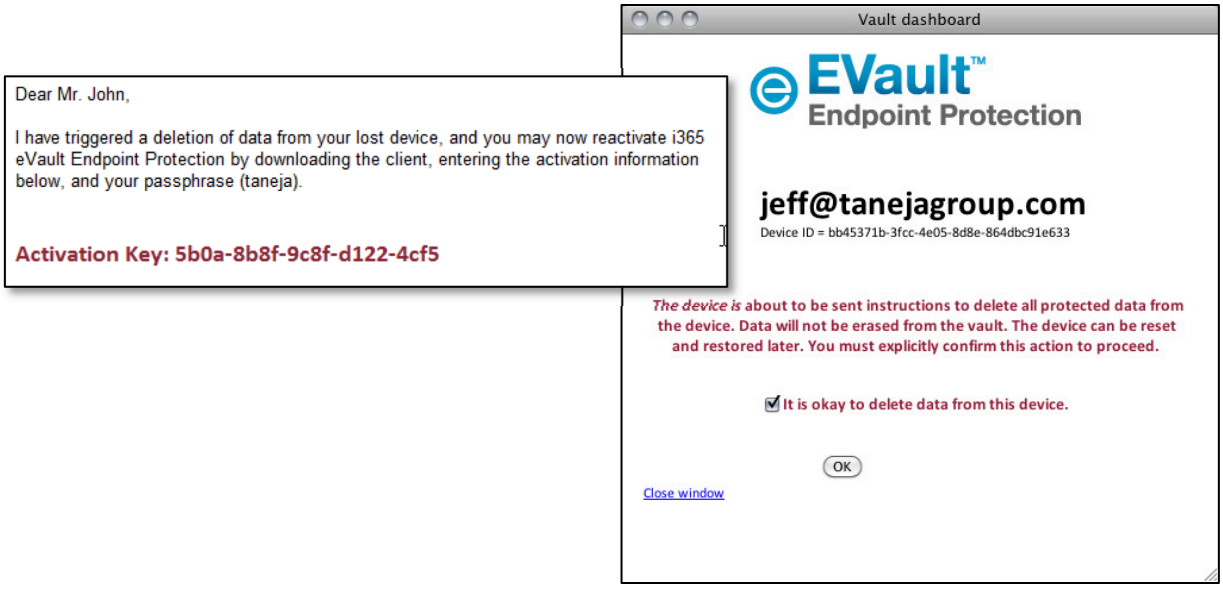

Figure 8: Protecting the endpoint against data loss by way of a remote wipe was easy and straightforward, as was reclaiming the data onto a different device.

87 Elm Street, Suite 900 · Hopkinton, MA 01748 · T: 508.435.2556 · F: 508.435.2557

We executed this task multiple times, and observed simplicity and trouble free execution irrespective of how or where the systems were connected. The implications here are much bigger than any single observation. Organizations equipped with a tool for remote wipe of lost systems can effectively guard their businesses against the potentially devastating risks of data theft or loss. Those costs aren't inconsequential – even the smallest business can imagine the consequences of having to notify tens or hundreds of thousands of customers about confidentiality breaches from a stolen laptop with emails, identifiers, or worse yet, credit card or financial information. Moreover, the data management functionality in EVault Endpoint Protection can harness the combination of at rest encryption, remote wipe and data set protection for employee exits, reprovisioning of systems, capturing a data set at the time of an eDiscovery request, or anywhere data needs to be reclaimed and moved.

Technology Validated:

i365 effectively turns data protection into a security tool by making it simple and straightforward to remotely erase data on protected machines that are lost, and enabling the user to seamlessly recover to a new system.

TANEJA GROUP OPINION

Clearly i365 is setting the bar for easy to deploy endpoint protection. As we've observed, the combination of a hosted service in the age of the ubiquitous Internet and easy, user self-service driven deployment has done away with many of the obstacles that have made protecting the critical endpoint difficult. And i365 has effectively turned their data protection expertise to the protection of data during loss or theft as well. The combination is a one-two punch that should garner the interest of every organization – it looks like the time has arrived to finally get that valuable scattered data protected.

In our view, i365's secret sauce is in the rapid deployment and ease of use they've harnessed by turning to a hosted cloud architecture for EVault Endpoint Protection. This tackles the biggest hurdle to endpoint complexity: system scaling, administrative overhead, and accessibility. This also demonstrates to many other purported cloud vendors just how a cloud service should be delivered to solve real world day-to-day challenges. i365 has certainly been comprehensive in doing so, by solving both data protection and data loss prevention with an enterprise-class scalable solution that requires no infrastructure, and almost no implementation effort. The bar has been set high for the competition, and we expect we won't see vendors come close to making endpoint protection as comprehensive and as easy to use as EVault has done.