PARABLU

MAXIMIZING THE RETURN FROM MICROSOFT ONEDRIVE FOR BUSINESS

SUCCESS STORY

CLIENT: World leader in IT services

INDUSTRY: IT Services

SOLUTION: BluVault. Secure enterprise backup management suite for end-points and servers

MS OFFICE 365 & ONEDRIVE FOR BUSINESS

As Microsoft aggressively pushes Office 365, a number of organizations, large and small, who were hitherto strictly on-premise shops, are now finding themselves using the public cloud. A number of MS Office 365 users also find themselves now having a ton of OneDrive for Storage in the cloud as part of the Office 365 deal they just signed – 1TB of storage per end-user to be precise.

Recently, a world-leader in IT Services with 150,000+ employees converted to using Office 365. They were excited about the 1TB/user of OneDrive for Business allocation they would get – and planned to use it to protect data on user endpoints. They had for years, dealt with a troubling problem – protection for data contained on their employee desktops and laptops. Like many organizations, they had allowed employees to be responsible for backups on systems issued to them. Employees could either copy important data to file shares (which were backed up rightly by the IT team) or make their own backup arrangements. Many employees were using external USB drives for backups, and worse – several others were doing nothing at all.

As soon as the IT team was able to roll out OneDrive for Business, they aggressively messaged employees to start using it. The thinking was that employees would place their important files on OneDrive and get the benefit of having a backup copy of their data in the cloud.

THE CHALLENGE

But, a strange thing happened. Usage of OneDrive increased in the beginning but plateaued off around 22% and never rose above that. When one investigates the reasons, there are some interesting findings:

- It turns out, users don't change their behavior easily. If they've been used to storing files in My Documents or another favorite folder on their hard disk drive, they're not about to change and use OneDrive simply because they're asked to.
- While OneDrive does have a client which automatically syncs user data, it synchronizes only what users place in the OneDrive folder on the client. If they have important files in other locations on their endpoint systems, those don't get synced.
- Unfortunately, OneDrive also comes with several limitations around file sizes, folder sizes, path length limits and special character limits. So, some users who tried OneDrive and found that it doesn't always work for them, simply give up using it.

The other question that the IT team started asking themselves is whether the protection OneDrive natively provides is really effective. OneDrive is basically an Enterprise File Sync and Share or an EFSS offering, not a Backup. Since it is a sync client, it faithfully replicates all changes on the endpoint over to the cloud. Sometimes these changes can be bad – like loss of data or a Ransomware attack.

On top of all this, there were also questions and concerns around using OneDrive due to fears around security and privacy in the public cloud.

THE SOLUTION

The IT team realized that while it made a lot of sense to utilize the OneDrive storage in the cloud, they needed an enterprise class Backup product which could be utilized to work with OneDrive. It had to be a solution which was sensitive to the security needs in the public cloud. A solution which would allow the business' digital assets to be stored securely in the cloud without allowing unauthorized access to anybody outside the organization. It also needed to be high performing, sensible in terms of network bandwidth usage, scalable across multiple geographies and not add additional processing burden to the existing employee endpoint devices.

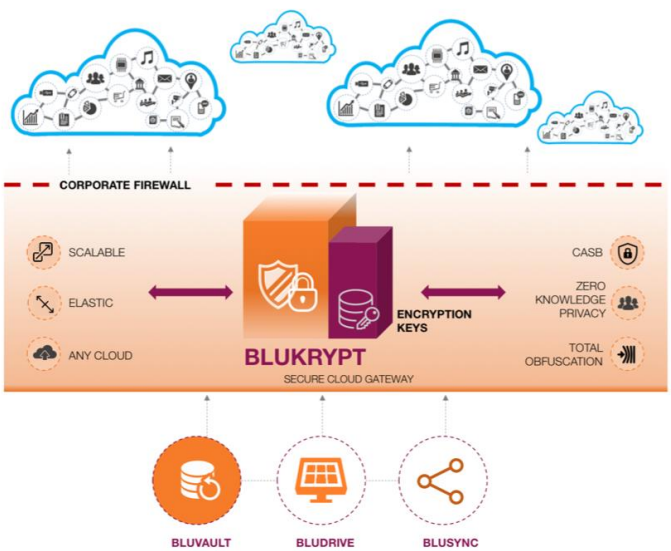
Parablu was able to offer a solution that addressed these needs perfectly. Parablu's BluVault solution provided a backup agent which identifies all important data on user endpoints, based on policies that an administrator sets. This agent scans all the hard disks on user endpoints to identify the files that needs to be backed up to OneDrive in the cloud – not just the OneDrive folder. Users could continue using their endpoint systems the way they always have been used to doing.

Also, BluVault didn't depend on the OneDrive sync client on endpoint at all. Parablu integrates separately with MS Office 365 APIs and was thus able to overcome all the native limitations OneDrive posed around file sizes, folder sizes, path length limits and special character limitations. Perhaps most importantly, BluVault is actually a Backup product - not a sync client. It creates retrievable, versioned copies of users' files on their own OneDrive storage in the cloud. These copies are insulated from any actions on the endpoint – such as data loss or a ransomware attack. Lastly, BluVault integrates with Parablu's BluKrypt, which was designed to act as a "Privacy Gateway" and keep data safe in the cloud.

By installing BluKrypt and routing all backup traffic through it, the IT team ensured that the backup data stream was encrypted before it traveled to its OneDrive destination.

This encryption is persistent in that it isn't just encryption "in-flight" – the data remains encrypted with the organization's keys even once the data reaches the cloud destination and is at rest. Most importantly, the IT organization is in complete control of the encryption keys.

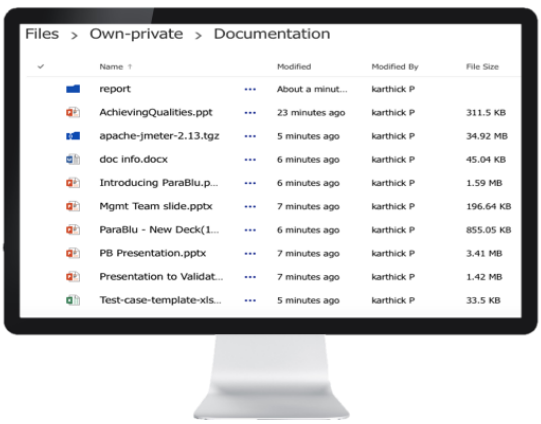
While easy to use, BluVault offers several enterprise class features like network bandwidth optimization, flow control, resume-able backups, compression, partial file transfers, integration with LDAP based directory services, SCCM based deployment, audit trails, as well as dashboards and reports for compliance. Further, given that security is always at the heart of Parablu's solution design, all devices that connect to the BluKrypt gateway are securely authenticated and not allowed to transact unless they pass appropriate certificate checks.



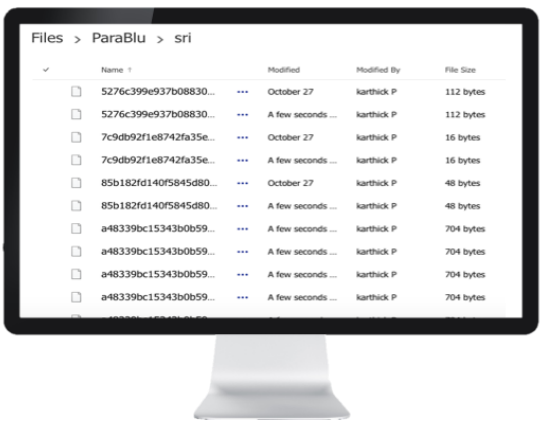
THE SOLUTION

BluKrypt doesn't merely encrypt data – it obfuscates it thoroughly. File names, folder names etc. become undecipherable on the target storage when BluKrypt is in use. Files may also be chunked up into smaller components and encrypted separately. Parablu's solution ensures that piecing together data off the target cloud storage is completely impossible unless the user authenticated themselves appropriately, at which BluKrypt de-obfuscates and decrypts the data back to its original form.

Before encryption



After BluKrypt encryption



The IT Services company in question, being as large an organization as they are, employees work in several locations across the world. What if an employee who's backups have been encrypted and transferred to the cloud for several weeks from one office location, travels on business to another? Will he or she have seamless access to the data in the new office? Parablu's ingenious solution handles this elegantly. The BluKrypt gateways in each location are constantly in sync with a central Backup Management Server called the ParaCloud and thus have access to the Master Catalog of all backed up data. Thus an employee or their endpoint system, no matter where they're currently located always enjoy seamless access to their data. Their files are decrypted by the BluKrypt gateway most proximal to their location and served up to them with no fuss. Because of the elegant, distributed nature of the solution, Parablu can scale to hundreds of offices or company locations with ease.

While there are other solutions that offer to encrypt inside the network perimeter, Parablu is unique in adoption the approach of a privacy gateway.

This effectively allows the endpoints to offload the burden of encryption and decryption instead of having to bear that load on themselves. This means no performance degradation on employee desktops and laptops due to the solution. This approach is also what makes possible other features Parablu offers – like file de-duplication, content indexing, file caching and partial file transfer. Further the gateway approach eases scalability and allows a finite number of gateways to easily stay in sync with each other versus a potentially unlimited number of endpoints.

Lastly, while this illustrates Parablu's integration with Microsoft's OneDrive as part of the solution implementation, Parablu has similar integration with several cloud storage targets – such as Microsoft Azure Blog storage, Google Drive, Amazon S3, IBM Softlayer storage, to name just a few.

Parablu's mission is to help customers feel secure taking their business to the cloud. We are focused on ensuring privacy, confidentiality and security of our customers' digital assets no matter where they reside - public, private or a hybrid cloud.

> "The Parablu team was an absolute pleasure to work with. There are very few companies we've seen that are so responsive to feedback and so rapid in their response to requirements. Parablu was able to tailor their solution to our needs in a matter of weeks."

ABOUT US

Parablu, an award winning provider of secure data management solutions, engineers new-age cloud data protection solutions for the digital enterprise. Our Privacy Gateway powered solutions protect enterprise data completely and provide total visibility into all data movement. Our suite of products include: BluKrypt - a Privacy Gateway that completely secures critical data on the cloud, BluVault - a powerful and secure data backup solution designed for the cloud, BluSync - a secure file sharing and collaboration solution for the agile enterprise, and BluDrive - a secure file transfer solution. These solutions easily integrate with your existing infrastructure making it a seamless solution for your enterprise data protection and management needs. Get a demo today.