PARABLU

HOW A LARGE IT SERVICES ORGANIZATION CRACKED THE CODE ON LEVERAGING THE PUBLIC CLOUD

SUCCESS STORY

CLIENT: World leader in IT services

INDUSTRY: IT Services

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

THE CHALLENGE

Studies and surveys consistently show that the greatest single deterrent for public cloud adoption is the fear around security and privacy. While many organizations, large and small, have started to use the public cloud more than ever, the reality is that a majority of their business still runs on premise and the bulk of their storage assets are still within their network perimeter. In order to fully leverage the promise of the public cloud, it is necessary that this fear around security and privacy be overcome.

Recently, a world leader in IT services, with over a 100,000 employees was posed with a troubling problem - backups of 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 – and many employees were using external USB drives for backups. The Security team recognized that this was not a secure approach given the possibilities of data leakage and disallowed such an approach thereby seeding the need for a centralized backup solution.

The company was at that point working with Microsoft on an Office 365 purchase to allow migration of several of their digital assets into the Microsoft cloud. As part of this arrangement they had already purchased 1TB of cloud storage per employee. The logical assumption was that this storage could be used to substitute for the USB drive based backups employees were performing manually.

The public cloud however, poses a bevy of challenges for a business' security team. The company was concerned (and rightfully so) about the safety of their employee data sitting in a public cloud. A recent survey of Enterprise and SMB customers across the world shows that Security remains the single biggest inhibitor towards increased cloud adoption. Fully 61% of respondents cite that as the #1 concern about moving their data and workloads to the cloud.

Most public cloud vendors do encrypt the data sitting in their data centers, but the catch is that they encrypt using encryption keys which they own and keep with them. This of course means that they can decrypt data at any time and gain full access to it. Public cloud vendors don't usually have any designs on their customers' confidential data, but the risk of a rogue employee in their organization having access to a business' sensitive information is a showstopper for many security teams. Also, if asked by government bodies to turn over sensitive data, many public cloud vendors have no choice to comply because they're bound by the laws of the land.

One way public cloud vendors have tried to mitigate this problem is by creating Hardware Security Modules (HSMs) in their clouds and allowing users to manage keys using such a mechanism. The logic here is that the customer is able to manage their keys via the HSM without necessarily the knowledge of the public cloud vendor. Even with such an approach, the reality is that the encryption keys travel outside the customer network perimeter and into the cloud – which makes security teams highly uncomfortable.

THE SOLUTION

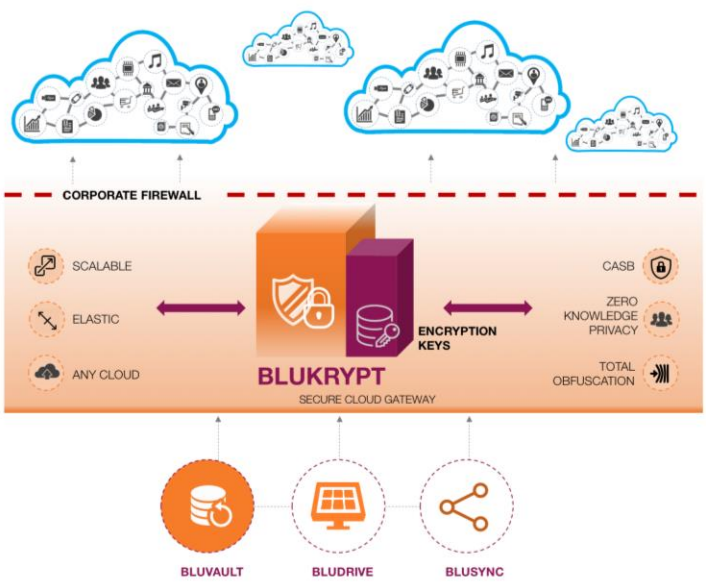
What was needed here was a backup solution which was sensitive to the security needs in the public cloud. A solution which would allow the business' digital assets to be stored securely in the cloud without allowing unauthorized access to anybody outside the organization. It also needed to be high performing, 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 Privacy Gateway software called BluKrypt was designed for exactly this need. By installing BluKrypt inside their network perimeter and routing all backup traffic through it, they ensured that the backup data stream was encrypted on-premise before it traveled to its Microsoft OneDrive destination. This encryption is persistent in that it isn't just encryption "in-flight" – the data remains encrypted with client's keys even once the data reaches the cloud destination and is at rest. Most importantly, the company is in complete control of the encryption keys.

Parablu also offered a BluVault – a full featured Backup and Recovery solution that could easily be deployed on the organization's endpoints. The simple-to-use software allows for flexible scheduling, incremental backups, deduplication of files, file versioning, retention policies and easy self-service restores by end users. Intuitive policies allow flexibility on types of files and folders that are included or excluded for backup.

Although 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.

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.



THE SOLUTION

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 Azure Blob, 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.