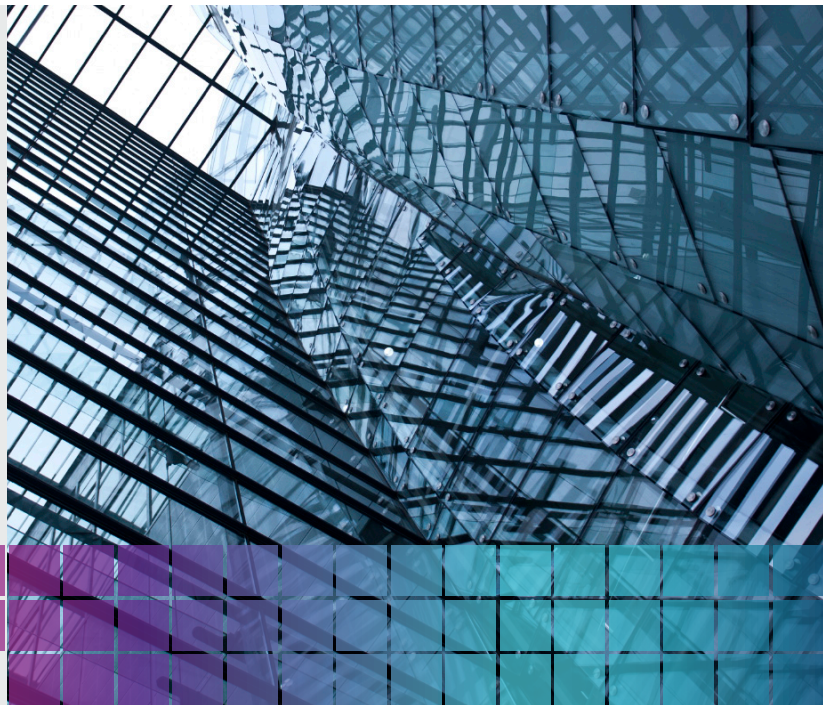
Asigra.

Recovery is Everything®

Datasheet

End-to-End Data Protection Solutions for the Enterprise

From the Data Center to Endpoint Devices



Your Corporate Data Might be at Risk

- Do your employees use their smart phones, tablets, or personal computing devices for work in addition to their PC at the workplace?
- Do you have a traveling workforce which needs to access and edit corporate data while on the move?
- Does your corporate IT environment have laptops, smart phones, or tablet PCs?
- Do you have a “bring your own device” policy?
- Is more than 10% of your workforce less than 30 years of age?

If you answered yes to even one of these questions, and do not yet have a policy for backing up data on mobile endpoint devices such as desktops, laptops, smart phones or tablet PCs, your corporate intellectual property assets may be at risk. This risk can expose you to a potential loss of competitive advantage, reputational loss, regulatory non-compliance, or worse, litigation. To understand how you can protect yourself from these challenges, using an endpoint cloud backup and recovery cloud backup solution powered by Asigra, read on.

Introduction

The world we live in today is very different from the world that we lived in a decade ago. Today’s world is a lot more global, interconnected by digital technology. Technology is a much bigger part of our lives than ever before. We are always connected. Our digital work lives and our digital personal lives have collided and often the same devices are used for accessing both work applications and personal social networks. This means your corporate data is now residing on personal devices. This is a world in which we demand access to our data and applications wherever we are and at all times during the day. And this is just the beginning.

The convergence of creation, consumption, and distribution of personal and professional information has been redefining the modern workplace. This process has been hastened

Asigra.

by advances in endpoint device technology related to the development of devices that are intuitive, powerful, interactive, and mobile. From smart phones to tablets to netbooks, all the way to laptops – these powerful devices have provided the changing workplace with the momentum and the ammunition to break through organizational inertia, hierarchies, and rigid policies to make workplaces flat, democratic, and collaborative.

The adoption of these trends has pervaded across organizational levels, departments, and business functions. From executives to new entrants into the workforce, the use of a mobile device for work has become the norm rather than the exception. End users now want to have a single device for their work and personal use and want to have the power to choose those devices themselves. "Bring your own device" (BYOD), a concept that would have sounded absurd even five years ago is the new mantra – and workplaces are being forced to acquiesce to these demands. IT departments and service providers are being challenged as the new work force demands immense flexibility in work hours, data access, device profiles, hardware and software platforms, and applications.

An important outcome of these changes is the fact that their intellectual property is no longer protected within its physical offices and corporate data centers – company IP now resides on end user devices that are in and out of the workplace. This exposes companies to enormous risks resulting from the loss of a device, to security being compromised due to viruses and malicious hardware. A data breach or loss can result in disastrous circumstances – from a loss of competitive advantage to reputational loss, and the costs of litigation, compliance, and remediation. As workplaces cede more and more control to employees in the form of flexible work options that provides access to corporate information, these risks will only increase.

Yet, companies have been paying very little importance to the backup of sensitive organizational data and intellectual property that resides on their environments that include such endpoint devices. Only about four out of every ten companies have a policy to backup the data on laptops. This number falls to even lower when you consider tablets and smart phones. In fact, many companies place the onus of backing up their mobile devices on the end user. Corporate data therefore finds itself backed up on USB drives and detachable hard disks. This further broadens the risk of data breaches.

Asigra Provides End-to-End Data Protection with a Single Enterprise Platform

With the aim of helping companies protect their intellectual property that is spread over these disparate devices, as well as successfully achieve their compliance obligations, Asigra offers a single enterprise platform that provides endpoint device data protection. By deploying a cloud backup service powered by Asigra for desktops, laptops, smart phones and tablets you can ensure that all your corporate information from across your data center, LAN, and endpoint devices can be safely backed up and restored in the unfortunate event of a data loss. Using Asigra Cloud Backup™, you can ensure that all your organization's intellectual property is stored in an encrypted and compressed form on a single redundant platform and that all of the information assets can be restored in their native format when required.

We understand that whether you are a SMB or an Enterprise you are facing the challenges of BYOD and the increasing consumerization of IT. We recognize the fact that

- Companies face enormous risks due to the fact that corporate information now is edited and maintained on end user devices outside the data center
- A data breach or loss can lead to disastrous circumstances from lost competitive advantage to reputational loss and the costs of litigation, compliance, and remediation
- Fortunately, a cloud backup service powered by Asigra has a solution for just this situation

Endpoint Device Data Protection Challenges:

- No single solution that backs up both LAN and endpoints
- Endpoint device backups don't happen as devices are powered down or out of network coverage area
- Users complain of performance degradation due to backup jobs
- Backups hog bandwidth
- Needs too much end user input, but too complex for them to use

Asigra.

your employees now want to bring their own devices to work and this means that the IT environment not just has more devices but more types of devices to backup. In recognition of the diversity of such an environment and with the desire to offer a solution to the complete data protection needs of organizations, Asigra Cloud Backup comes in different flavors:

- **FullFeatured** – offers data protection to the entire IT environment from the LAN to the endpoint device, unifying the data protection infrastructure into a single offline shared storage
- **Mobile** – a data protection solution offering end-to-end data protection to small businesses looking to backup all user devices in their environment – from desktops and laptops to tablets and smart phones
- **Consumer** – tailored to the needs of a small office/home office, this solution offers a bundled data protection solution protecting desktops, smart phones and tablet devices

Asigra Cloud Backup can also capture information from devices running different software platforms – from Windows Mac, and Linux to Android, and iOS. Asigra Cloud Backup also includes other key advantages that provide you with additional business benefits such as – agentless and therefore easy to run and maintain, incremental only data backups, data compression techniques such as common file elimination and data deduplication, in flight and at rest security assurance through AES 256-bit encryption and NIST FIPS 140-2 certified cryptography, and restore and recovery assurance through autonomic healing and validation restore.

Once installed and configured, the Asigra Cloud Backup software runs in the background requiring little or no user intervention as the software backs up the information on the endpoint device. Even during restore scenarios, the service platform requires little user intervention as files and folders can be restored easily by IT staff.

We Understand Your Operational Challenges

We are cognizant of the challenges that you face in implementing a centralized backup policy for your organization. We recognize the fact that deploying a backup strategy for endpoint devices, in particular, can be a challenging task. A number of such devices may not have access to the network at all times. Therefore, unlike desktop PCs which can be backed up at specific times in a day or on specific times in a week / month, scheduled backup jobs on mobile devices may not work as planned as some of these devices may not have access to the network at those times. Further, end users may power down laptops and tablet PCs when they are not in use resulting in scheduled backup jobs not being able to complete or even get kicked off.

We understand the frustrations of end users due to performance degradation when long pending backup jobs start up, making it a challenge to even work on the device while backups run in the background. We believe that users coming into the branch office after a prolonged time should not dread connecting back to the corporate network from the fear of backups numbing the capabilities of their machines. Traveling employees connecting from hotels or airports should not worry about the high network bills that they may incur due to backups. We realize that many of your technology savvy workers will kill backup jobs when they start to avoid CPU, battery, or network hogging by backup applications. And, if backup administrators are unable to track the progress of such terminated jobs, the very purpose of deploying a backup solution will be worthless.

Finally, we understand the challenges that you will face in convincing your staff to download updates on a regular basis. We also recognize the importance of providing self service options to end users and the fact that in order to do so, the user interface and the configuration must not be complex or difficult to use. We know that if the tool is not intuitive to use, your empowered workforce will shop around for simpler, unsecure, and unauthorized alternatives such as consumer oriented unsecure software or worse, sync and share software. Such solutions may send corporate data outside organizational boundaries and into non-secure clouds further increasing organizational data risk. Moreover, you will be left with needing to manage a new piece of standalone infrastructure that is different from your existing technology environment.

Asigra Cloud Backup is Designed to Overcome These Challenges

Asigra Cloud Backup has been designed to overcome a number of these challenges. The simple and intuitive user interface ensures that backup and recovery jobs can be initiated by end users themselves. This can help take the load off backup administrators and provide end users with control of their backup and recovery tasks. As mentioned earlier, Asigra Cloud Backup can also be configured to run in the background with little or no user intervention. Further, the agentless Asigra technology with auto-upgrade capabilities enables IT departments and service

End-to-End Data Protection

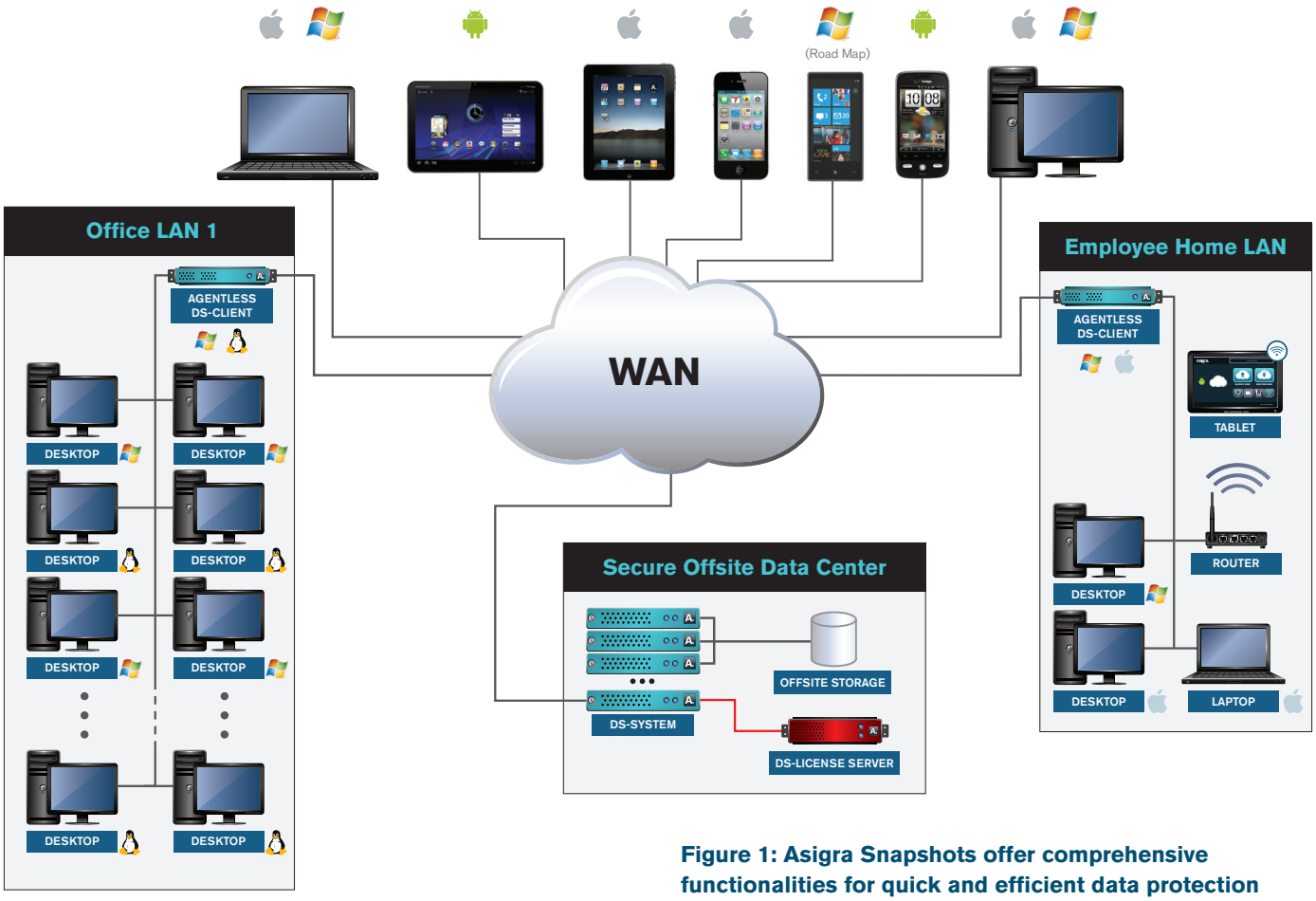


Figure 1: Asigra Snapshots offer comprehensive functionalities for quick and efficient data protection

providers to seamlessly push software updates from the backend without needing the end user to intervene in the process.

Asigra Cloud Backup is designed to limit the drain on CPU, battery, and bandwidth ensuring that end users do not face much degradation in system performance. By utilizing the powerful bandwidth and CPU throttling capabilities of Asigra Cloud Backup, IT departments and service providers can ensure that your employees can continue to use their devices and the corporate network while the backup jobs proceed in the background. Given that Asigra Cloud Backup only performs incremental backups of information that has changed, the volume of data to be backed up is severely reduced. This ensures that backup windows are kept to a minimum. The intelligent data compression and deduplication capability of Asigra Cloud Backup also reduces the bandwidth required for transferring the data over the network.

Using Asigra Cloud Backup, your IT department or service provider can automate the backup process by scheduling the backup for specific times of the day or particular times in the month. If the device is turned off at the time that the backup is scheduled, Asigra Cloud Backup ensures that the backup job begins once the device is turned on. In the event of not finding a connection to a network to back up the data, Asigra Cloud Backup waits for the next scheduled backup job before

attempting to back up the information. The Asigra Cloud Backup software provides the IT administrator with a status of all the backup jobs that have not completed and provides him with notifications on users who have not backed up in time. This capability helps him work with you and your employees in ensuring that your backups are always up to date and that your data is secured.

Finally, and most importantly, Asigra Cloud Backup integrates with your existing standardized IT infrastructure and offers a simple and secure method to backup corporate data to your authorized cloud data center. The Asigra software, though robust and secure, is designed to be inherently flexible in supporting multiple cloud deployment models – public, private or hybrid. So, as you evolve in your cloud journey through those models, Asigra Cloud Backup continues to protect your data through the process, making the transformation seamless from a data protection standpoint.

Conclusion

We are cognizant that the workplace of the future will be significantly different from the workplace of today across all segments – from small office to mid market to the enterprise. Workers will use more than one computing device for data creation, sharing, and consumption. Further, in a globally integrated world, dispersed virtual teams will work together to create the technologies and products of tomorrow.

In responding to and embracing these changes, Asigra has developed a platform that enables IT departments and service providers to provide you with a proven cloud backup and recovery solution that can support such an environment for companies of all sizes where employees use varied devices and run their devices on a multitude of software and hardware platforms. Our technology offers the assurance of being able to backup not just the information assets of today but in the future as well. Relax; we've got your back!

About Asigra

Trusted since 1986, Asigra provides organizations around the world the ability to recover their data now from anywhere through a global network of partners who deliver cloud backup and recovery services as public, private and/or hybrid deployments. As the industry's first enterprise agentless cloud-based recovery software to provide data backup and recovery of servers, virtual machines, endpoint devices, databases and applications, SaaS and IaaS based applications, Asigra lowers the total cost of ownership, reduces recovery time objectives, eliminates silos of backup data by providing a single consolidated repository, and provides 100% recovery assurance. Asigra's revolutionary patent-pending Recovery License Model provides organizations with a cost effective data recovery business model unlike any other offered in the storage market. Asigra has been recognized as a Gartner Cool Vendor and has been included in the Gartner Magic Quadrant for Enterprise Backup and Recovery Software since 2010.

More information on Asigra can be found at www.recoveryiseverything.com

Asigra.