Datasheet

Our Cloud Backup Solution Provides Secure Data Protection for Endpoints Beyond the Firewall

Today's mobile workforces rely on laptops, smartphones, and tablets, connected to vast information sources in corporate data centers or off in the cloud. But granting such access to critical corporate information beyond the corporate firewall comes with risks. Every day, thousands of laptops, tablets, and smartphones are lost or stolen, potentially exposing confidential information such as social security numbers, credit card PINs, customer lists, medical records, cached emails, or future business plans. Data thieves readily sell this information on the black market if they can acess it.

Your organization can minimize the risk of data breaches caused by lost or stolen mobile devices by putting into place a comprehensive endpoint device data protection plan that includes data loss prevention and security provided by our solution.

6 Ways Our Secure Data Backup Helps Manage Risk Exposure

1. **Easily recover employee data —** By backing up critical data located on mobile endpoints to a secure data center with our solution, you can easily recover an employee's data if a device is lost, stolen, or damaged. A point in time backup copy previously taken from their old mobile device is used to restore data to a replacement device.
2. **Know what data is missing —** Data backups can also give you a clear sense of what data was on a lost or stolen device, helping you to decide on the best course of action to mitigate the potential damage. For example, if analysis of the backup data reveals that customer credit card payment information was on a stolen laptop, the affected customers can be proactively notified and counseled to change the PINs, hopefully before any data thief is able to breach the information.
3. **Encrypt backup data in transit and at rest —** Ensure the backup data itself doesn't become a source of security concerns. Our solution

POWERED BY Asigra.

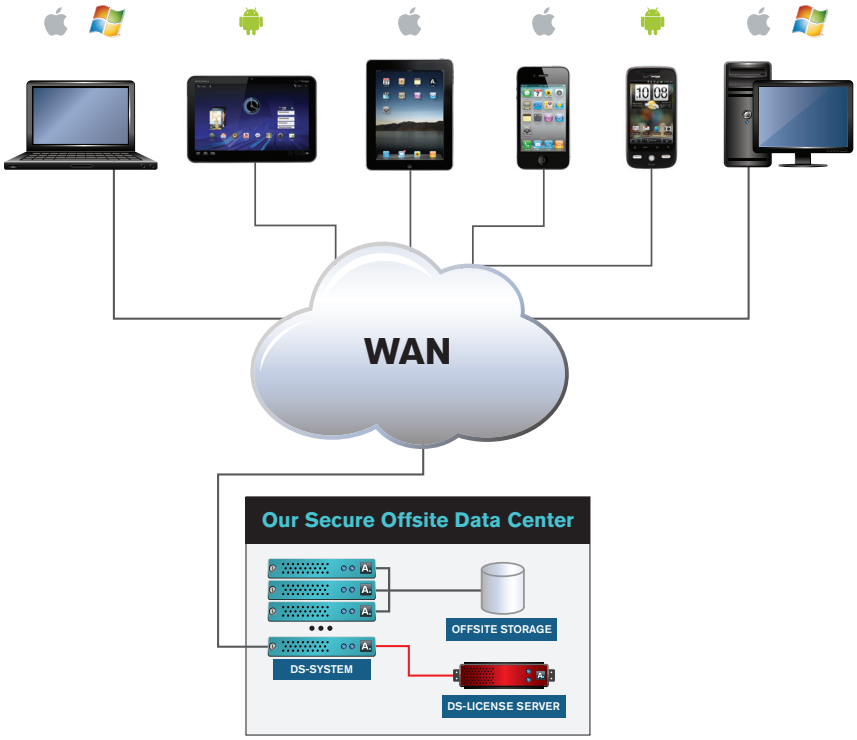


Figure 1

uses NIST FIPS 140-2 certified encryption for all backup data, so your backup data is useless to unauthorized individuals. As the only encryption standard permitted under US Government mandated HIPAA HIHTEC rules for use by US healthcare and other government agencies, NIST FIPS 140-2 encryption makes our solution ideal for mobile workers operating under strict data security compliance requirements, such as outpatient nurses and financial advisors.

4. **Remotely wipe data with selective data destruction —** With our solution, you can remotely delete any lost or stolen mobile device before data thieves can access it. Wipe any data included in the backup policy that you have defined—without touching any data excluded from that backup policy. While other mobile device wipe options reset devices back to factory settings, this selective data destruction allows you to retain control over corporate data without impacting employee's personal data if you have a BYOD policy.
5. **Schedule periodic cleansing of enterprise data —** The remote wipe feature in our solution also lets you limit how long your data can live on remote devices. If employees no longer require critical information, why leave forgotten files on their device file systems where it only increases your risk exposure if the device is lost or stolen? Instead, use the remote wipe feature to periodically cleanse corporate data from all remote devices, in 90-day or less increments. Employees won't notice the data they no longer use is gone from their devices, and any data they need can be easily recovered in just a few clicks from the backup copy of their data.

Business Benefits

- Increase productivity
- Eliminate data breaches
- Reduce costs with one comprehensive data protection solution for endpoint devices, virtual and physical servers, and SaaS-based solutions like Google Apps, Office 365, Salesforce.com
- Meet corporate governance and regulatory compliance mandates
- 100% Recovery Assurance

Key Features and Capabilities

- Secure Backup and Recovery for Workstations, Laptops, Smartphones and Tablets
- Autonomic Healing and Validation Restore
- Continuous Data Protection
- Remote Wipe
- Geo-Location
- Selective Data Destruction
- Microsoft System Center Configuration Manager Integration
- Web-based NOC
- NIST FIPS 140-2 Certified

6. **Geo-locate devices with your data —** our solution includes geo-location, which when enabled allows you to locate any endpoint device to within a few meters of its current physical locations, via an intuitive Google maps interface built into our Network Operations Center (NOC) (Figure 2). Geo-location helps you decide at a glance whether or not your data on a missing device is at risk of a breach. If the device is someplace your employee hasn't been to recently, then you can wipe your corporate data from the device just to be safe.

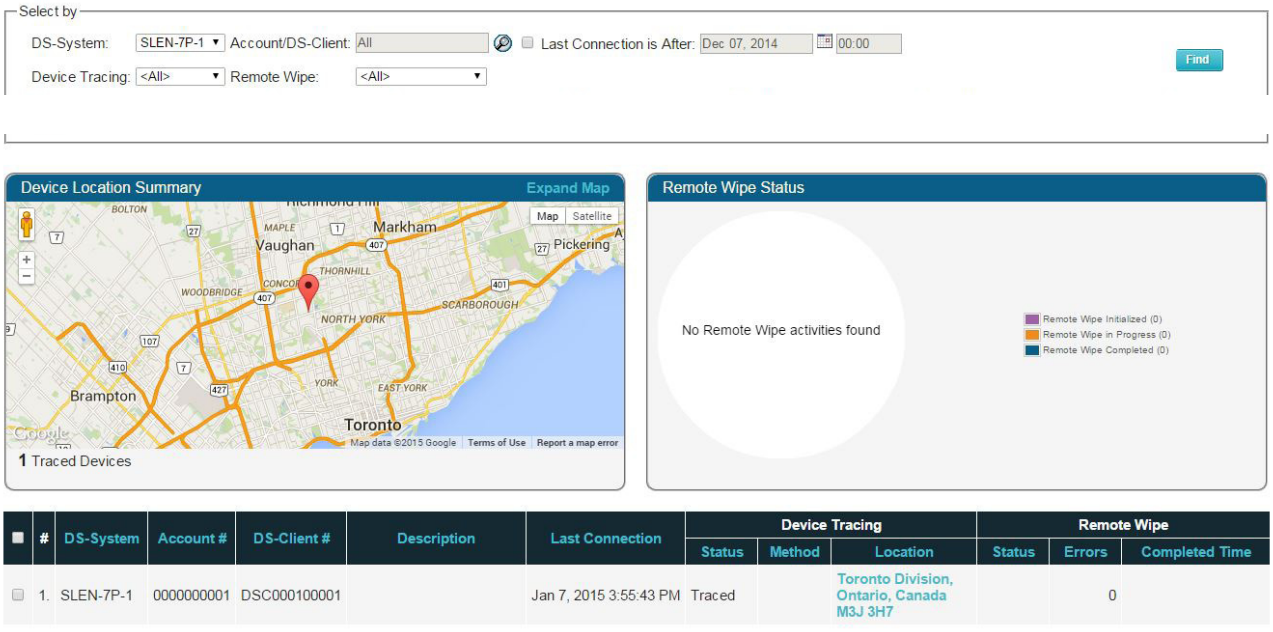
Flexible yet consistent data protection across all endpoint devices

Any effective mobile data security plan must address how to ensure consistent, gap-free protection across all devices: if some mobile devices with critical corporate data are under-protected—or not protected at all—then your data is still at risk. But you may also need the flexibility to tailor your data protection to different classes of users. For example, your field sales reps may access the CRM system and email while your technicians may only access order and customer information.

How do you enable data protection differentiation across different types of mobile workers without undermining your overall data security objectives? And how do you achieve this without introducing needless complexity to your IT processes? Here's how:

- **Platform independence —** our solution protects critical data on virtually all endpoint devices in the market today.
- **Mass deployment —** Integrations with device management tools like Microsoft System Center Configuration Manager (SCCM) make it easy to push out protection components and policies to any endpoint devices that connect to your network
- **Self-management options —** The backup policies that you push out to endpoint devices can be the same for all endpoints, or you can assign differentiated policies to different classes of users. Either way, default data protection applies to all endpoint devices according to rules you define. However, end users also have the ability to manually backup and recover data on demand anytime, anywhere (ex. under default corporate policy, mobile devices may back up data only when connected to WiFi, but if a user has important data they want to back up immediately, they can over a cellular network).

Leverage our solution to protect and secure your corporate data on endpoint devices, both within your firewall and beyond.



#	DS-System	Account #	DS-Client #	Description	Last Connection	Device Tracing			Remote Wipe		
						Status	Method	Location	Status	Errors	Completed Time
1.	SLEN-7P-1	0000000001	DSC000100001		Jan 7, 2015 3:55:43 PM	Traced		Toronto Division, Ontario, Canada M3J 3H7		0	

Figure 2

To learn more about our endpoint device data protection, contact us or visit our website.

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-class 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. In 2014, Asigra Cloud Backup was also named the Top Enterprise Backup Solution by Storage Magazine. More information on Asigra can be found at www.asigra.com.