SecurityFirst™
Data-Centric Cyber Solutions

Data Protection Technology for Managed Service Providers

Deliver Data Security to Get Your Share

Nearly every business is interested in cloud-based resources as a means to outsource many traditional IT applications and expand their mobile-friendly customer services. The compelling reasons are that it's just quicker, easier and often cheaper than doing it themselves, but many still have security concerns. They wonder if they can truly trust a managed services provider (MSP) to both deliver on its service level agreements and protect the company's critical data because no CIO or CISO wants their company to be the next posterchild for a data breach disclosure.

So what can you do to help these organizations make the leap to your cloud environment? Part of the answer lies in your ability to provide data protection services. Imagine how much more effective your value proposition would be if you could guarantee that any data stored within your environment would always be encrypted and protected against unauthorized viewing. Need more? Tell your clients that they--and only they--will hold the encryption keys, so in the off chance a cybercriminal gets into your environment, any theft of your customers' data yields nothing more than gibberish.

Data is Your Customer's Most Valuable Asset

There are many forms of data that organizations rely upon to perpetuate the business. Some of it represents the 'secret sauce' or intellectual property behind the core of what they do. The chances that a CEO would approve storing this kind of data in a cloud environment are not good. But then there's a whole class of other data associated with day-to-day operational applications that while sensitive, might be something the C-suite would be willing to entrust to the cloud if the motivations were compelling. Few and far between are companies that don't have a backlog of requested IT enhancements and showing them a path to a new level of competitiveness is just a win-win situation.

Internal data aside, a growing reason for offering data protection services is the increasing regulation for collecting, storing and safeguarding customer private data. One need look no further than the impending General Data Protection Regulation (GDPR) in the European Union regarding what comprises 'private' data and how access to it must be controlled. Beyond social security and credit card numbers, even a picture of an EU citizen (say for a loyalty program) it needs to be carefully protected. Lose it, and your customer might lose their business.

Here's where data protection services can help. As an MSP, you can assure potential customers that any and all of their data will be protected. Intellectual property, general ledger entries, prior customer activities and payment data can all be encrypted and secured against any prying eyes including your own. Using DataKeep™ technology, anything uploaded to your cloud environment is stored in an encrypted form that meets the most stringent standards of the U.S. government for its top-secret information. Can you see it? No.

Help Your Company and Help Your Clients Avoid Reporting

One of the best reasons why you and your customers should employ data protection is to avoid the issue of data breach reporting.

Imagine that your cloud environment is penetrated and terabytes of customer data is exfiltrated. Upon discovering the breach, any number of disclosure activities must be initiated. Some regulations specify a tight timeframe for disclosure; others are more relaxed, but also require that your customers offer identity protection services for a period of one year. In either case, this amounts to a significant business disruption and added cost.

Yet all of this can typically be avoided if you offer the ability to encrypt your customer's data. Most regulations have a clause that relieves the organization of consumer or individual notification duties if the lost data was previously encrypted and therefore useless. It's tantamount to a get-out-of-jail-free card that you never want your customers to use. Beyond the embarrassment and potential loss of customers, these activities are always a huge cost to your customers. Be the MSP that saves its customers from this form of agony.

This push towards stricter data governance is only going to get stronger. GDPR, China's new Cybersecurity Law, and the recent cyber security regulation in New York City, have all clearly indicated a trend towards increased oversight in the realm of consumer data. As more businesses are held responsible for the privacy of data, MSPs in turn, will see an increased demand to help customers meet those requirements.

Primary Data Privacy Considerations for MSSPs

The first and most important piece of the data security puzzle is

encryption. It is crucial that an MSP can provide strong data protection to its customers, and easily manage this service from a remote location; yet allow the customer to remain in ultimate control. An important part of this equation is key management. As an MSP, you don't want to become the key holder for all of your clients. Rather, sell them on the benefits of generating and holding their own decryption keys.

The second is the access control mechanism. This must go beyond traditional Microsoft Active Directory style control, and identity management solutions to create secure silos of information. Customers must be given insight and control into the security rules that govern the data they wish to protect, and they must enjoy this without unnecessary burden. DataKeep excels in its ability to simplify who has access to what data by individual or group policy.

Thirdly, any data security service offered by an MSP must take into consideration regulatory requirements and offer or forward real-time reports of operations. Often that means integrating with other security solutions designed to detect anomalous conditions. Logs from DataKeep can be an integral feed into complex correlation rules that detect attempted data access as some sort of lateral movement between compromised network assets.

DataKeep – The Solution

DataKeep is an advanced data-centric software solution that protects sensitive and personal data from being exposed in the event of a breach, while ensuring compliance with regulatory requirements and data privacy mandates.

Security teams can define and log access policies by job role, while blocking privileged user access, securely encrypting at the source and transparently managing encryption keys. DataKeep technology protects data on Windows and Linux, physical and virtual servers and encrypts at volume-level or file-level for additional granularity. Powered by secure SPxCore technology, DataKeep combines AES-256 encryption with cryptographic splitting and internal key management certified by the NIST to be FIPS 140-2 compliant.

The need for data protection is clear. The public is demanding data privacy, and network perimeter controls alone aren't enough. Data must be protected at its core to provide protection and as a last line of defense.

Help Your Customers Embrace the Future

Ask anyone--MSP or not--about the security of any organization's data; it's a jungle out there and it's only going to get worse in the next decade. What are you doing to offer your customers some kind of assurances? If you currently have no data protection measures, pick up the phone and call us immediately. A byte is a terrible thing to lose—terabytes more so.

DataKeep can be the insurance policy your prospects need to overcome their inhibitions to embracing cloud services technology. Lead with the idea of (tough as nails) encryption and close with the concept that they're in control. And what the heck, throw in All your cost savings metrics to close the deal.

SecurityFirst™ delivers data-centric solutions that address the high-profile cyber threats facing organizations today, such as data breaches, ransomware and cloud security. We emphasize protection of the data itself to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure.

DataKeep™, by SecurityFirst, secures critical data at its core to deliver unrivaled protection, control and resiliency. Customer-defined access policies, strong encryption and event logging combine with native secure backup/restore capabilities to address your data privacy, compliance and recovery needs. Organizations can utilize the backup and restore capabilities with object storage for secure cloud backup and archiving to improve resiliency and enable prompt recovery of archived data in the event of a ransomware attack. Leading OEMs and integrators have selected DataKeep to safeguard enterprise and multi-cloud environments.

SecurityFirst™
Data-Centric Cyber Solutions

For a product demonstration or more information call
1.888.884.7152
securityfirstcorp.com