ESG SHOWCASE

Changing the Hybrid Cloud Data Protection Game for Managed Services with FalconStor

Date: December 2021 **Authors:** Christophe Bertrand, Senior Analyst; and Monya Keane, Senior Research Analyst

ABSTRACT: IT partners are shifting to deliver more managed services to end-users, with cyber resilience and data protection at the top of the priority list. This is happening at a time of heightened business risk and increasingly stringent service level agreements (SLAs) for backup and recovery. Through predictable MSP-designed pricing—one flat rate per month, per client—FalconStor software-defined technology offerings can help MSPs create and deliver more valuable services to its clients.

The Market Landscape

Managed IT services are evolving. Data protection is now among the top-three areas of strategic importance for IT channel partners, with 67% of ESG research survey respondents reporting that data protection is among the managed security services they sell. Additionally, 41% of these value-add channel partners—including managed services providers, VARs, and systems integrators—said their strategy is to choose best-of-breed IT vendors/service providers.[1] They are intent on cultivating the right relationships and using the best tools available.

Ransomware

Seeking best-of-breed technology to protect data is a smart decision in our present era of ransomware. Ransomware attacks are business-interruption events that have significant negative consequences on data availability and application uptime, an area in which MSPs are expected to support their customers. These days, attack frequency is frighteningly high: 18% of ESG survey respondents are experiencing daily attacks, and 24% report being attacked on a weekly basis. The research also showed that 43% of IT decision makers are very concerned that their organization's "golden copies" (protected copies) could also become infected/corrupted by such attacks.[2]

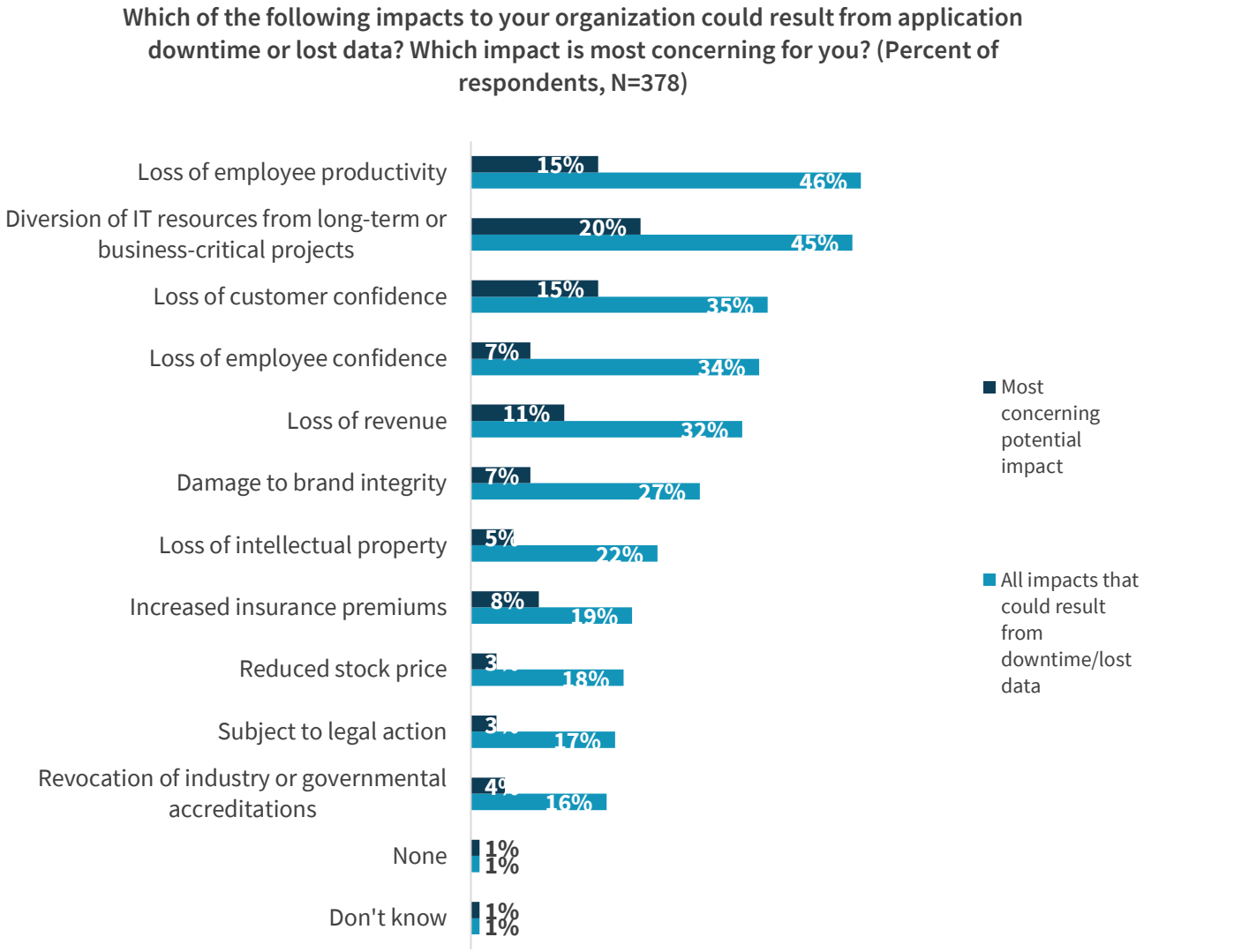
Stringent Service Levels

IT organizations face extremely low tolerance for data unavailability from their end-users. Fifteen percent of organizations surveyed by ESG tolerate no downtime at all for their mission-critical applications. Another 42% say that their mission-critical applications must be back online in less than one hour. In addition, RPOs are very stringent, with 15% aiming for no mission-critical data loss at all.[3]

These low tolerances stem from the fact that downtime has such significant economic, operational, and legal impacts (see Figure 1). For example, one in five survey respondents cite the diversion of IT resources from other business-critical projects as the potential impact that concerns them most.[4]

[1] Source: ESG Master Survey Results, *MSP Partner Landscape 2020*; January 2021.
[2] Source: ESG Research Report, *Tape's Place in an Increasingly Cloud-based IT Landscape*, January 2021.
[3] Source: ESG Master Survey Results, *Real-world SLAs and Availability Requirements*, August 2020.
[4] ibid.

Figure 1. The Impact of Downtime and Lost Data



Source: Enterprise Strategy Group

Being able to minimize IT staff resource diversion gives MSPs a great opportunity. They can deliver impactful services to help their clients meet SLAs, keep the lights on, and fend off attacks. Data protection is a hot topic that is transforming the channel ecosystem, and picking the best protection tool is crucial.

Capabilities and Requirements—What to Look For

What are the key characteristics of a best-of-breed data protection platform? ESG's MSP research shows that channel ecosystem players like to prioritize vendors and products that fit well with the rest of their MSP product/service portfolio (64% of respondents), and they want to work with technology vendors whose pricing models allow them to both maximize their margins and differentiate their business from the competition.[5]

To meet clients' requirements, MSPs should focus on finding solutions that possess the capabilities shown in Table 1.

[5] Source: ESG Master Survey Results, *MSP Partner Landscape 2020*, January 2021.

Table 1. The Ten Key Capabilities MSPs Must Consider in a Data Protection Platform

Capability	Description
Wide cloud destination support	Cloud as the DR destination for BaaS or DRaaS/cloud migrations, with multi-cloud in mind
Designed with security in mind	From access controls, to encryption and immutability
Easy to manage at scale	Multi-tenancy, single point of control, and reporting
Performance oriented	Performance to deal with the growing amount of data that organizations face
Storage optimized	Leveraging tiered storage across disk, tape, and cloud and efficient deduplication (to optimize storage)
Wide platform support	The ability to manage a wide array of platforms and applications
Continuous data protection/high availability	HA at the storage and application level to meet stringent RPO and RTO requirements
Replication options	Local, in-region, and out of region (sync/async)
Tape and virtual tape support	Tape is still used by many organizations today and can provide a very favorable economic advantage as part of a tiered storage strategy
Easy to do business with the vendor	Simplified licensing and pricing for operational and economic/margin efficiency

Source: Enterprise Strategy Group

FalconStor Technology to the Rescue

Three FalconStor software products—StorSafe, StorGuard, and StorSight—collectively embody many of the key traits identified above:

- StorSafe creates a backup-to-disk target on industry-standard servers that appears as a virtual tape library and NAS share for 100% compatibility with an organization's existing enterprise backup and recovery software, providing encryption throughout the process.
- StorGuard provides several data protection services, relying on core replication and continuous data protection to provide disaster recovery, granular data restores, and cloud migration services. One use case for MSPs involves using StorGuard to keep track of each disk-write operation, enabling metro-region-wide HA, DR, and application recovery to milliseconds prior to the ransomware attack.
- StorSight provides a centralized user experience across both StorSafe and StorGuard that is designed for multitenancy (essential for MSPs). Running on a virtual machine or any industry-standard server, StorSight enables real-time analytics, reporting, dashboarding, and alerting for all StorSafe or StorGuard servers running on-premises,

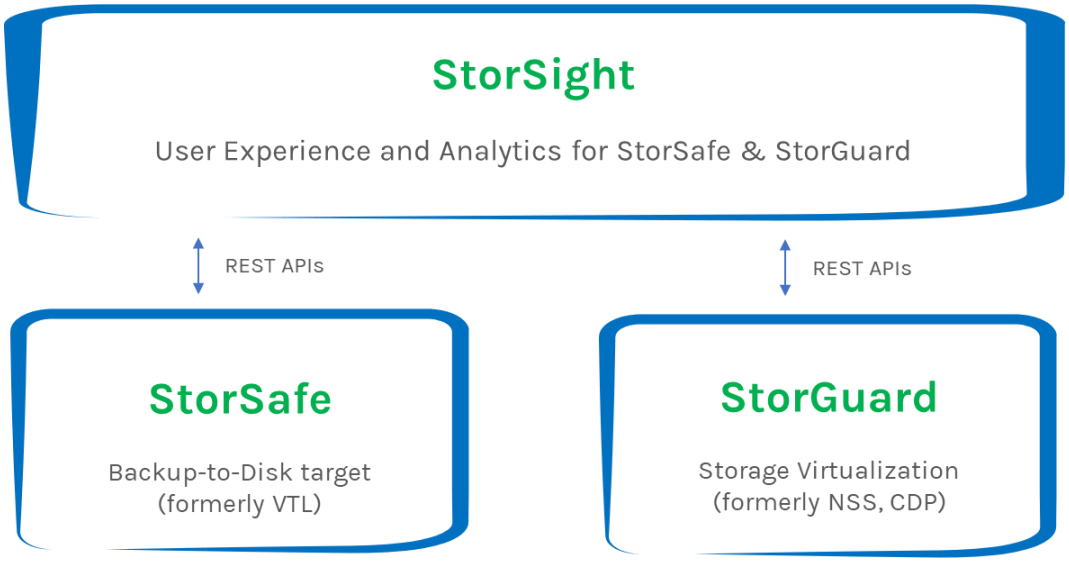
remotely, or in any private or public cloud. It keeps tabs on backups, replication, and data readiness in any location, even behind a firewall. It also manages all encryption keys (see Table 2 and Figure 2).

Table 2. Capabilities at a Glance

StorSafe	StorGuard	StorSight
Accelerate backups and restores	Data migration across arrays, sites, and clouds	Central multitenant console across all sites and clouds
Optimize cost and size of backup storage	Continuous data protection	Manages all FalconStor servers
Scale as you grow	High availability	Chargeback capabilities
Protect backups using offsite tapes or cloud destinations	Disaster recovery	Real-time status, health, and integrity visibility
Wide backup software support	Application-consistent snapshots	Analytics, reports, and forecasts
Designed to be rolled out as BaaS	Non-disruptive LUNs mirroring	Designed for BaaS provided by MSPs
In-flight and at-rest AES-256 encryption and encryption key management		

Source: FalconStor

Figure 2. FalconStor's Portfolio



Source: FalconStor

The depth and breadth of these solutions provide MSPs with a powerful, software-defined offering that blends advanced data protection with storage efficiency. It supports cloud destinations, and it is wrapped in a modern management tool that promotes operational effectiveness. These solutions open up many possibilities for MSPs to create value-added managed services that can be expanded as end-users' SLAs evolve. They even include end-to-end encryption for data in flight and at rest.

MSPs Are at the Heart of FalconStor's Go-to-market Strategy

FalconStor offers a program for MSPs centered on how to make money with its BaaS offering powered by FalconStor, including help with integrated sales/marketing. Fees are a flat rate per month, per client. For an MSP, that means no complicated sales motion is required to onboard a tenant—no measuring of dedupe rates, cataloging of data sources, or

estimation of data volumes. The MSP knows exactly what its cost profile is going to be. There's no upfront cost, either. This is a true SaaS model. All that is needed is a minimum of ten clients to start. Thereafter, it's per tenant, per month.

It is therefore easy for an MSP to pilot the offering before diving in. For example, the MSP might start with StorSafe and backup-as-a-service, then find out a client needs to move four petabytes of data to a new array in the same data center. That's a migration job, so the MSP would start using StorGuard, with no extra add-on charges incurred. It's a great way for an MSP to boost its customer service (and optimize its margins).

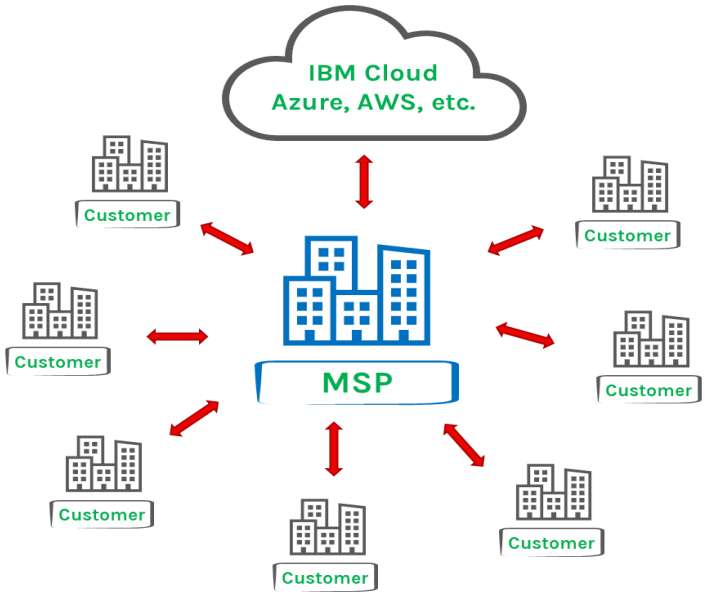
Software-defined scale-out can intimidate many enterprises, but it is embraced by MSPs because they have the in-house architectural skills. These projects can improve MSPs' margins and allow them to accommodate the footprint each client desires. After all, MSPs don't get to choose the applications and hardware their clients have already standardized on. Flexibility is key.

FalconStor's ability to import tapes from older LTO formats is also an advantage. It gives MSPs a way to help their clients move that data "from the pile to the cloud."

The FalconStor support team also provides a free optimization service. Experts examine the metrics, lining them up to show where an MSP is achieving best-in-class and where it is not. The support team then provides recommendations to the MSP on areas to improve.

For the most part, MSPs using FalconStor are serving as the cloud provider. But if the MSP's business model is instead to use Azure, IBM, or another cloud, they can do that, too. The MSP is the hub—it could be the cloud or use a preferred public cloud—and the client is the spoke (see Figure 3). And again, no matter how many instances of FalconStor software the MSP uses to serve a client, it's all covered under one monthly fee.

Figure 3. FalconStor's Hub and Spoke Model



Source: FalconStor

The Bigger Truth

FalconStor is essentially selling a "recipe" for MSPs to create their own BaaS and DRaaS offerings. That recipe centers on hybrid cloud data protection. A hybrid cloud solution is really now the only way to succeed as an MSP because today, for safety, everyone needs to support tape and cloud to store backup data remotely.

The single biggest differentiator of this offering is its software-defined approach. Unlike other solutions that are all-in-one appliances requiring repeated forklift upgrades as needs grow, with FalconStor, it is possible to run a BaaS protection environment on as little as one VM, or as many as nine industry-standard servers (for demanding environments). Software definition makes it possible to right-size an environment, and then expand compute and storage as needed over time.

The extensive support matrix FalconStor has built between the software, hardware, and now the cloud is also impressive. MSPs can't dictate which hardware and applications their clients use on-premises. They inherit a mix of legacy and new systems, and they have to make sense of it all.

FalconStor has the enterprise-class capabilities MSPs are looking for. It also now has a distinctive strategy for providing a very MSP-friendly platform for enterprise backup, recovery, and archiving at scale. FalconStor appears determined to achieve shared success—convinced that it will only be successful if its MSP partners are successful, too.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188