

## Case Study

### Rampant Rise in Ransomware Attacks Plagues Businesses for Millions – Sandz Hits Back with Powerful OpEx Backup Appliance

- Ransomware Protection “As-a-Service”
- 100%-OpEx, multi-tier data backup and protection
- Fully-managed service with increased data resiliency



## SUMMARY

Founded in 2000, Sandz Solutions Philippines Inc. is a managed services provider specializing in IT infrastructure optimization and data protection. The company provides customized solutions that address demanding SLAs, risk mitigation, cost reduction and regulatory compliance for various industries. Delivering technology solutions through a network of channel partners, and guided by the company's Datacenter Optimization Framework, Sandz offers managed services that enable IT groups to support the changing and increasing demands of businesses throughout Southeast Asia. The company provides enterprise solutions which transform datacenters in order to provide the necessary flexibility and agility to support business requirements.

## CUSTOMER OVERVIEW

One of the services offered by Sandz is enterprise-class data protection. The company's end-to-end approach to data protection allows each customer or partner to protect their data against loss and corruption through highly secure and efficient solutions – regardless of the SLA requirement. Services include backup-as-a-service (BaaS), disaster-recovery-as-a-service (DRaaS) and archiving-as-a-service (AaaS). As part of the BaaS solution suite, the company has partnered with Asigra and Zadara to deliver the highly secure and cost-efficient OpEx Backup Appliance, optimized to counter ransomware attacks on backup data.

## BUSINESS SITUATION

According to the FBI, Ransomware attacks are becoming more targeted, sophisticated, and costly, even as the overall frequency of attacks remains consistent. Cybercriminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware. For example, recently exploited vulnerabilities were discovered in two remote management tools used by managed service providers (MSPs) to deploy ransomware on the networks of customers of at least three MSPs.<sup>1</sup>

Security experts say that even currently available numbers underestimate the true cost of ransomware attacks, which have disrupted factories and basic infrastructure and forced businesses to shut down. What has been found to be most concerning is that these attacks not only result in direct costs, but also indirect costs from lost operations. For organizations today, ransomware is certainly viewed as one of the most serious cybercriminal problems facing IT and cybersecurity teams right now.

## CHALLENGES

- How to minimize the vectors of ransomware attacks
- Mitigating cybersecurity risks and being able to restore business critical information after a disaster
- Reduced resource strain of host-based backup balancing recovery speed and storage affordability to keep data safe.

## ASIGRA CLOUD-BASED DATA RECOVERY DELIVERS

- Data protection & recovery by people who study cyber criminals
- Signature-less malware detection solution that identifies and quarantines unauthorized or malicious embedded code
- Reduced points of failure through agentless architecture
- Data encryption that secures data in-flight and at-rest with full support of compliance requirements
- Integrated multi-factor authentication (MFA)

## BUSINESS SOLUTION

Businesses today are resolved to avoid the disruption and expense of a ransomware attack. To accomplish this, organizations must ensure they have the necessary data protection platform and strategy in place. Successful recovery in the event of a ransomware attack can be measured by how quickly access to systems and data is restored following one of these unfortunate incidents.

An effective strategy recommended by Sandz for organizations concerned about ransomware is to use a cybersecurity-enabled platform using a 3-2-2 deployment methodology, where three copies of data are stored locally on secondary storage; two additional copies of backup data are kept on different locally available mediums (devices); and two backup copies are stored offsite at two remote locations, such as a remote facility or cloud-based platform. The company strongly recommends the Asigra OpEx Backup Appliance powered by Zadara; it is a backup solution that addresses criminally crafted ransomware Attack Loops™ by scanning for malware instream as data is backed up and scanned again before the data is returned to production, among other techniques.

The Asigra-Zadara solution is optimally designed for managed service provider delivery to end-customers, but can also be sold as a complete solution for standalone implementation within the enterprise. Regardless of deployment option, the consumption-based service is a new addition to the company's product line. The appliance allows IT and MSP professionals to move from a CapEx to an OpEx

model in order to cost-effectively safeguard business data for assured business continuity.

“Backup has received much more attention and is a higher priority aspect of our technology solutions suite with the surge of ransomware attacks now impacting organizations globally. The Asigra OpEx Backup Appliance with Zadara storage serves as a resiliency orchestration platform that supports critical data recovery requirements for business continuity, while also reducing the capital and management costs of traditional backup systems.”

**Henry Velasco,**  
Managing Director, Sandz Solutions Philippines

## RESULTS

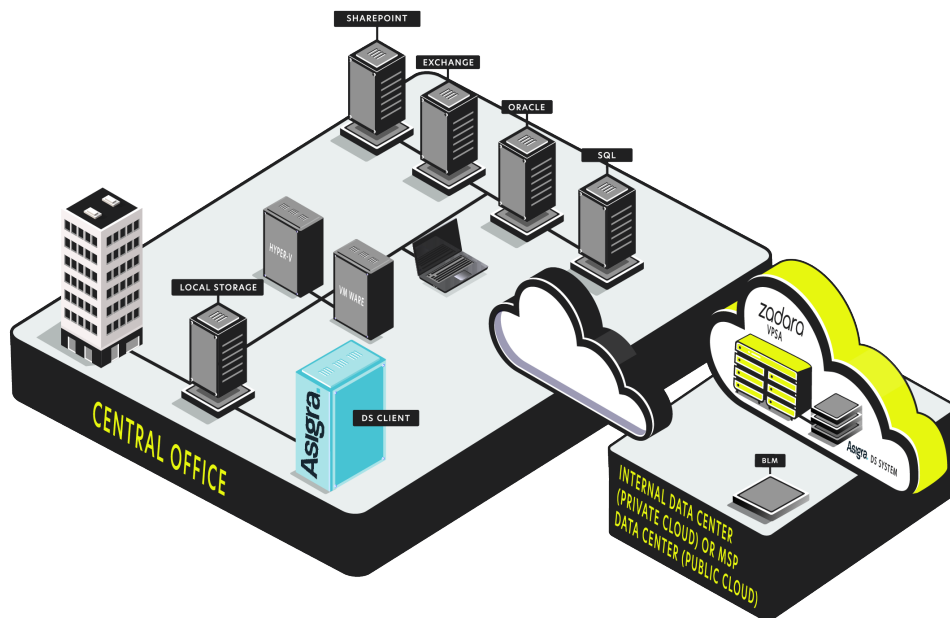
Since adopting the Asigra OpEx Backup Appliance with Zadara Storage-as-a-service, Sandz' MSP partner ecosystem and enterprise customers have been extremely interested in the system. For those that have implemented the system, the reviews have been impressive. The number of Sandz MSPs implementing the solution either in their own datacenters or colocation centers. With a lower barrier of entry than competitive options and with a much higher caliber

The OpEx Backup Appliance performs on two levels – price and functionality. The subscription-based pricing model has allowed us to scale operations quickly, slashing the capital expense traditionally required to spin up backup service infrastructure. In terms of functionality, the solution is feature-packed and built for deployment flexibility, feature set and most importantly, capabilities – especially cybersecurity.

Sandz enterprise customers utilizing services based on the OpEx Backup Appliance note that the technology has been a game changer, adding an entirely new layer of protection with Attack-Loop™ preventative technology using bi-directional malware detection, zero-day exploit protection, variable repository naming, and multi-factor authentication (MFA) – a full defensive suite against advanced ransomware variants.



## Simple Backup Using Zadara & Asigra Appliance



### About Zadara

Founded in 2011, Zadara is changing how enterprise data is stored and managed, by offering enterprise data storage as a fully managed service. With solutions available on premises and through cloud and colocation providers, Zadara's proprietary software, combined with commodity hardware in a 100%-OpEx, pay-only-for-what-you-use service, helps companies be more agile without sacrificing the features and functionality that advanced enterprise users demand. To deliver on this promise Zadara operates worldwide, including hundreds of data centers at public- and private-cloud partners, and an expert team that provides services and support 24/7. More information can be found at [www.zadara.com](http://www.zadara.com), or follow the company on [LinkedIn](#), and [Twitter](#), like on [Facebook](#) or subscribe on [YouTube](#).

### About Asigra

Trusted since 1986, Asigra's multi-award-winning backup and recovery technology is proudly developed in and supported from North America, providing organizations around the world the ability to quickly recover their data from anywhere through a global network of IT service providers. As the industry's most comprehensive data protection platform for servers, virtual machines, endpoint devices, databases and applications, SaaS and IaaS based applications, Asigra lowers the total cost of ownership, reduces recovery time objectives, and eliminates silos of backup data by providing a single consolidated repository with 100% recovery assurance and anti-ransomware defense.

More information on Asigra can be found at [www.asigra.com](http://www.asigra.com)

