The Asigra TrueNAS Appliance: Addressing Enterprise Concerns about Explosive Backup Data Growth and the Insidious Threat of Malware

by Jerome M Wendt

Enterprises want all aspects of their backup environment to be simple, scalable, and secure. But with growing amounts of backup data and the threat of malware becoming ever more pervasive, that ideal can seem more like a pipe dream than a viable objective. The Asigra TrueNAS appliance addresses these challenges. It delivers enterprise caliber backup software, robust cybersecurity software, and scalable storage in a single, turnkey solution to help enterprises put these emerging concerns to rest.

COMPANY

iXsystems, Inc.
2490 Kruse Dr
San Jose, CA 95131
(408) 943-4100

www.iXsystems.com

INDUSTRY

Information Technology

KEY ENTERPRISE CHALLENGES

- Backup data stores continuing to grow
- Backup appliances too small for enterprise requirements
- New threat of malware finding its way into production and backup data stores
- Testing backups for malware is costly and resource intensive

SOLUTION

Asigra TrueNAS Appliance

KEY BENEFITS

- Bundles backup, cybersecurity and scalable storage in a single solution
- Enterprise caliber backup software
- Eliminates need to set up separate processes to test backups for malware
- Scales to multiple petabytes of capacity
- Scans for malware both during backup and recovery

Re-thinking the Makeup of Backup Appliances

Simple, secure, recoverable, and scalable. Those four words summarize how enterprises want their backup appliance to operate. Until recently, they could have a high degree of confidence that existing backup appliances satisfied these requirements. However, explosive data growth and the increased threat of malware have forced them to re-think the makeup of these appliances to ensure they best address their backup challenges.

Data growth continues unabated. The growth in the use of edge, endpoint, and mobile devices; the need to protect data in the cloud; and the organic data growth inside corporate data centers result in more data than ever to protect. To respond, backup appliances must, as part of their solution, incorporate more cost-effective, easy to manage, and scalable storage strategies.

Exacerbating this problem, enterprises must also deal with the threat of malware. This includes identifying ways to protect their backup repositories from this threat.

Malware already finds its way undetected into production data stores. However, as some enterprises have learned the hard way, malware can also find its way undetected into backup repositories. This demands that enterprises establish internal processes, implement cybersecurity software, or do both to mitigate the ability of malware to infect their backup repositories or hinder their recovery efforts. (See *Malware's Insidious Nature.*)

To address both these challenges, enterprises must look for a next generation of backup appliances that include both cybersecurity software and scalable storage as part of their make-up.

Backup and Scalable Storage Convergence Well Under Way

Backup and storage providers have made significant strides in recent years to deliver the best of these two technologies as a single enterprise solution. While backup appliances have always used disk drives for data storage, the continuing growth in the amount of data that enterprises must protect and retain dictates that backup appliances must adapt to become more scalable, while remaining cost-effective and simple to manage.

Backup appliances have done so in two general ways by introducing:

1. ***Scale-out backup appliances.*** A few backup providers employ a hyperconverged, scale-out architecture as part of their respective backup appliances. Enterprises buy a few nodes and add on more as their capacity needs increase.
2. ***Scale-up backup appliances.*** Some like Asigra and iXsystems have combined to deliver backup services on a storage array. The Asigra Cloud Backup™ software comes pre-installed and available as a service on the iXsystems TrueNAS storage system that one may turn on at any time. Should the Asigra TrueNAS appliance need more capacity, one simply needs to add more disk drives to the TrueNAS array.

While both architectures have their respective merits, they illustrate how backup providers have stepped up to deliver higher performing, simpler to manage, and more scalable backup appliances. Yet where almost all these appliances still fall short is in making cybersecurity software an integral part of their solution to help combat the pervasive threat of malware.

Malware's Insidious Nature

Malware can all too easily slip undetected past corporate firewalls and other antivirus software into corporate production data stores for various reasons. Due to the multiple variations of malware, the multiple entry points (mobile devices, sensors, thumb drives, etc.) it has into enterprises, and constant updates applied to "approved" corporate software, among others, malware will likely find its way into corporate data repositories.

Once there, it can manifest itself as ransomware or, in its latest iteration, cryptojacking software that hijacks corporate servers and turns them into bitcoin mining operations for cybercriminals. Adguard estimates that cybercriminals may have already compromised more than half a billion devices and are using them for this purpose.[1]

While any occurrence of malware on production data stores causes concern, enterprises may fail to consider malware's even more insidious side. It may NOT immediately execute and may spread silently and undetected for days, weeks, months or even years before detonating.

Once it does "detonate," it may delete or encrypt corporate backups residing on disk. Also, depending on the time lapse from the malware's first entry into the enterprise to when it does detonate, the malware may have infested the backup repository.

Should an enterprise then try to recover from a malware attack by performing restores from their backup data, it may inadvertently re-introduce malware back into its production environment. This may continue with each subsequent restore until the threat can be identified and eliminated. This can result in the enterprise losing days, weeks, or months of data along the way.

This insidious nature of malware sends a chilling message to enterprises. They must assume that malware, in some form, already resides in their corporate data stores and backup repositories. Further, they cannot assume their backups are immune from malware attacks or infestation nor can they automatically assume that the data they recover is free of malware.

1. https://www.webopedia.com/TERM/C/cryptomining-malware.html

Creating a Secondary Perimeter Around Backup Stores

Due to the multiple ways that malware can find its way past standard perimeter defenses such as firewalls and antivirus software, it becomes almost inevitable that malware will eventually find its way into backup data stores since they house copies of production data. To mitigate the possibility of malware getting into their backup data stores, enterprises should look to put in place a secondary perimeter around them.

Enterprises have one major advantage working in their favor as they look to do so. Backup software will, at some point, touch and make a copy of the production data prior to it entering the backup data stores. By leveraging backup software that uses cybersecurity software to scan backup data for malware as the data enters or exits the backup data stores, enterprises can have a high degree of confidence their backup repositories remain malware-free.

To deliver on this ideal, enterprises prefer to obtain this combination of technologies—backup, cybersecurity, and scalable storage—from a single source, packaged together in one solution in the form of an appliance. In so doing, they reduce and simplify their costs and efforts associated with the acquisition, management, and support of these various yet now interrelated technologies. The Asigra TrueNAS appliance represents the first enterprise backup appliance to bring these three respective technologies together and deliver them in a single solution.

The Asigra TrueNAS Appliance: A Single Source for Simple, Scalable, Secure Backups

The foundation of the Asigra TrueNAS appliance is the iXsystems TrueNAS storage system, a full featured array suitable for use within enterprises as a primary storage array. DCIG has evaluated and included the TrueNAS systems in its Enterprise Midrange Array Buyer's Guides, consistently ranks them highly, and considers them a viable alternative to established brands in the market.

The Asigra TrueNAS backup appliance offers the same performance capabilities as primary tier 1 storage that more than meets corporate requirements for a tier 2 or tier 3 backup target. With 10, 40, or 100 GbE interconnect and scalable to several petabytes, this storage system can handle backups of hundreds to thousands of clients and VMs.

"The Asigra TrueNAS appliance represents one of the first products to bring backup, cybersecurity software and scalable storage together as one and deliver them as a single solution for enterprises."

The iXsystems TrueNAS Appliance

A single TrueNAS appliance can start as small as 10 TB and scale to as large as 10 PB, more than enough to meet the most aggressive enterprise backup storage requirements. iXsystems offers single controller configurations for cost-conscious enterprises as well as dual controller options for enterprises concerned about high availability. It offers NAS (AFP, SMB, and NFS) and SAN (FC and iSCSI) interfaces. Further, performance tests conducted on TrueNAS systems

demonstrate that it consistently outperforms comparable brand-name storage systems.

On the software side, TrueNAS has all the features that enterprises need when using it in this role as a secondary storage system. It offers virtually unlimited snapshots and replication, adaptive compression, and a unified block, file, and object (S3-compliant) interface. To deliver these services, it uses the proven, tested, and hardened open source ZFS platform.

"Enterprises do not have the time, patience, or desire to separately manage backup software, cybersecurity software, and scalable storage systems. The Asigra TrueNAS appliance addresses all these challenges."

ZFS was specifically designed, among other things, to protect against data corruption even as it supports massive storage capacities.[2] These two characteristics make ZFS-based storage systems such as the iXsystems TrueNAS well-suited to function in this role as a secondary storage device. By using a familiar and proven scale-up storage architecture with ZFS, enterprises can implement a scalable yet cost-effective solution in their environment.

Asigra Cloud Backup

Asigra Cloud Backup is an enterprise-class backup solution that uniquely helps prevent malware from compromising backups of infected systems. It comes pre-installed on the TrueNAS appliance and may be optionally turned on and run as a service at any time.

Like other leading enterprise backup software offerings, Asigra Cloud Backup offers core backup features that enterprises expect for their environment such as support for:

- The protection of cloud, physical, and virtual environments
- The protection of data residing on NFS and SMB file shares
- The protection of enterprise applications such as Microsoft Exchange and Oracle and SQL Server databases
- Global data deduplication to minimize backup data stores which, when combined with TrueNAS' physical PB capacities, can achieve effective storage capacities scaling into the tens of PBs
- Multi-tenancy to facilitate consolidating the backups of discrete companies or divisions.

Agentless Backups, Embedded Cybersecurity

Asigra Cloud Backup does differentiate itself in two key ways from other enterprise backup software offerings.

First, it remains one of the only enterprise backup solutions that offers agentless backup support across all types of environments: cloud, physical, and virtual. This flexibility makes it easy for enterprises to non-disruptively adopt and deploy Asigra Cloud Backup in their environment since they do not need to deploy any agents to protect their servers or clients.

Second, Asigra embeds cybersecurity software in its Cloud Backup software. By taking this step, Asigra enables enterprises to go the extra mile to protect their backup repositories from malware and ensure enterprises can recover from a malware attack in their production environment.

By using the Asigra Cloud Backup software present on the Asigra TrueNAS appliance, enterprises may not need to buy additional cybersecurity software. They also may not need to create separate sandbox environments that require them to set up and manage separate processes to screen and test their backups for the presence of malware. Enterprises only need to enable the cybersecurity software feature within Asigra Cloud Backup to automatically protect their backup environments from malware.

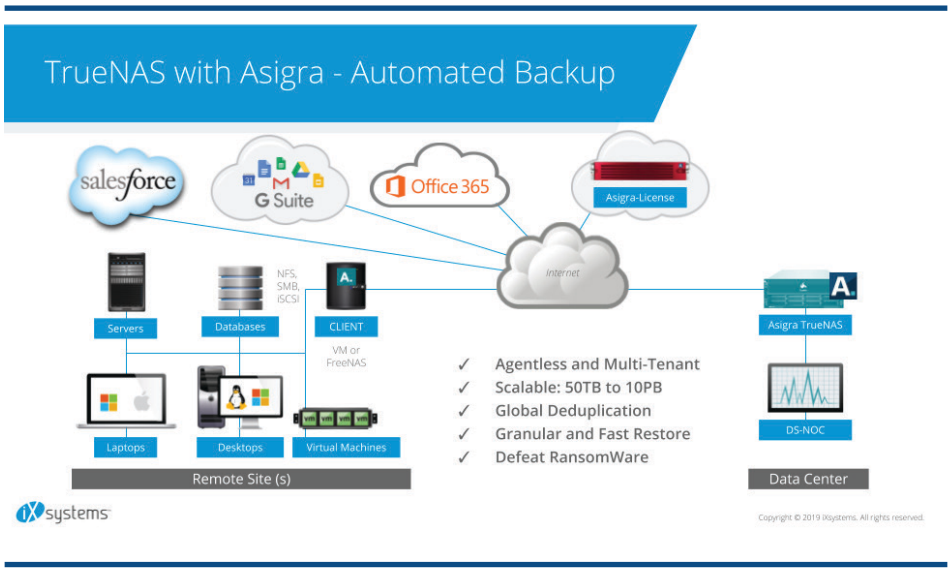
The implementation of the cybersecurity software works hand-in-glove with the Asigra Cloud Backup solution. Once enabled, it scans incoming backup data for known malware signatures. If it identifies any malware, it immediately sends out a notification to alert the enterprise that malware exists in their production data so they can take steps to address the problem.

"Enterprises can get in front of the challenges of storing increasing amounts of backup data while simultaneously keeping malware at bay using a turnkey solution like the Asigra TrueNAS appliance."

Equally important, Asigra also leverages its embedded cybersecurity software to scan backup data when and if it is recovered. Scanning data during the recovery process can identify malware that was present, but not yet identifiable by the cybersecurity software at the time the backup occurred.

This two-step process helps ensure enterprises can avoid re-introducing malware into their production environment that was dormant and unrecognizable at the time the backup originally occurred. Failure to take this step can result in what is known as a zero-day attack loop where a recovery from backups does not resolve a malware attack but perpetuates it.

2. https://en.wikipedia.org/wiki/ZFS



Source: iXsystems

The Asigra TrueNAS Appliance Addresses Enterprise Challenges to Explosive Data Growth and the Threat of Malware

Enterprises widely recognize that the time has come for backup appliances to include cost-effective, robust, scalable secondary storage systems as part of their solution. In this respect, the Asigra TrueNAS appliance more than meets enterprise capacity, performance, and reliability requirements.

At the same time, enterprises remain concerned about the pervasive and increasing threat that malware presents to the safety and security of their data. Here the Asigra TrueNAS appliance currently stands apart. It offers enterprise backup and cybersecurity software on a scalable backup appliance. By deploying it, enterprises can get in front of the challenges of storing increasing amounts of backup data, while simultaneously keeping malware at bay.

Enterprises do not have the time, patience, or desire to manage separate backup, cybersecurity and storage solutions. The Asigra TrueNAS appliance consolidates these disparate technologies onto a single device. Compared to many other solutions that require a VM or physical server to run on, and then need agents and a separate storage system for data integrity, enterprises can start running this solution within minutes of powering it on. Administrators simply need to decide which backup plan from Asigra they want to employ, add the license, and begin setting policies.

The Asigra TrueNAS appliance addresses the concerns that enterprises have about the escalating challenges of data growth and malware by mitigating the need for them to acquire, implement, and manage separate technologies and processes to manage them. Additionally, it delivers a comprehensive backup that is cost-effective and simple for enterprises to deploy with cybersecurity software that detects current malware threats and those yet to be discovered. ■