DCIG Product Review Article

A Product Review of StorageCraft OneXafe

StorageCraft OneXafe Delivers on Its Promise of Easy Setup and Configuration

Scheduled Publication Date
January 2020

By
DCIG President & Founder
Jerome Wendt

DCIG, LLC
7511 Madison Street
Omaha NE 68127

O 844.324.4552
StorageCraft OneXafe Product Review

StorageCraft OneXafe Delivers on Its Promise of Easy Setup and Configuration
Final Draft

Backup and disaster recovery represent universal IT needs for almost every small or midsize enterprise. To address them, many acquire and implement backup and recovery solutions themselves. Others engage managed service providers (MSPs) for this service.

Whether organizations perform these tasks themselves or use an MSP, they require a solution to deliver these functions. StorageCraft’s OneXafe represents an integrated, converged solution that provides scale-out storage as well as backup and recovery for midsize enterprises.

OneXafe’s Feature Offerings Pass Muster

On a feature-by-feature basis, the OneXafe appliance provides the ones midsize enterprises typically expect. It ships as a single integrated solution. It protects applications and data hosted on Windows operating systems. It protects virtual machines (VMs) hosted on VMware vSphere and Microsoft HyperV. It offers fast, non-disruptive recoveries. It provides these features at an attractive price point.

The deeper question becomes, “How well does StorageCraft translate its features into real-world deliverables?” I recently completed a product review on the StorageCraft OneXafe to assess how well it delivers on the following:

- Setting up its hardware and software
- Adding more capacity
- Auto discovering virtual machines (VMs)
- Protecting VMs using its immutable continuous data protection (CDP)
- Virtualboot recovery of VMs
- Protection against ransomware

OneXafe Hardware Configuration and Setup

I remotely reviewed two OneXafe appliances running in the StorageCraft labs, its HDD-based 4417 and all-flash 5410 models. This review was done with the help of StorageCraft staff.
I began by reviewing the setup of each OneXafe appliance. Each appliance follows the same setup process. StorageCraft provides a Quick Start guide that walks users through the initial setup. Exactly following the steps in this document is critical to quickly and easily set up OneXafe for the first time.

Each OneXafe appliance, optionally, ships with its disk drives installed. StorageCraft does give organizations the option to purchase their own HDDs or SSDs from a qualification list. One may add more drives during the initial install or at any time in the future. This frees organizations to obtain higher capacity drives as they become available and better manage their costs.

Each OneXafe model has redundant power supplies and 4 x 10GbE network ports (optionally configured with six (6) network ports). One may plug in and use from one to six networks ports on the OneXafe. We left all six ports in the single, default port group instead of subdividing them into multiple port groups.

**OneXafe Initial Software Configuration and Setup**

After installing and powering on OneXafe, we connected to and managed its network interface via a web browser. By default, OneXafe preconfigures all network interfaces into a single port group. It assigns them all the same dynamic IP address with a standard maximum frame size of 1500. One may assign static IP addresses at any time.

OneXafe can use the Dynamic Host Control Protocol (DHCP) if available on a network. DHCP was available and we used it to assign an IP address to OneXafe. This freed us to immediately move to setup and use StorageCraft’s OneSystem single pane of management to manage OneXafe.

Setting up OneSystem requires the following 4-step process:

**Step 1 – OneSystem Setup**

One can set up and manage OneSystem in two ways:

- A hosted application
• An on-premises VM

We used StorageCraft’s hosted OneSystem application for management that we accessed at onesystem.storagecraft.com.

**Step 2 – Create StorageCraft OneSystem User Account**

Whether installing OneSystem on-premises or using StorageCraft's hosted OneSystem application, one must create a StorageCraft Cloud Services account to replicate and failover to StorageCraft's Cloud Services. I registered at the following [link](#).

![StorageCraft Cloud Services](image)

The registration and initial login were straightforward. It required filling out a few fields and supplying a code that was emailed to me.

**Step 3 – Register OneXafe with OneSystem**

Once we logged into the hosted OneSystem, we clicked on the **View Clusters** button from the Welcome Screen.
After accepting the OneXafe warranty, EULA, and software and hardware agreements, we came to the Discover OneXafe tab. Since we had the IP address for each OneXafe, we entered them.

OneSystem prompted us for a challenge code generated by each OneXafe appliance. We entered the challenge codes to complete the registration of the two OneXafe appliances.
Step 4 – Complete OneXafe Configuration through OneXafe Web Console Console

Available Network Profiles

<table>
<thead>
<tr>
<th>Network</th>
<th>Port Group</th>
<th>Method</th>
<th>IP Address</th>
<th>Netmask</th>
<th>Gateway</th>
<th>VLAN Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage</td>
<td>1</td>
<td>DHCP</td>
<td>10.30.15.11</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>0</td>
<td>DHCP</td>
<td>10.30.14.13</td>
<td>255.255.255.0</td>
<td>10.30.14.1</td>
<td></td>
</tr>
</tbody>
</table>

Port Groups

- Port Group 0
- Port Group 1

We completed the configuration of all the OneXafe appliances by accepting their default settings. We could have changed the following:

- IP address
- Network profile. A OneXafe supports up to 25 network profiles across 25 different subnets
- Ports groups. A OneXafe supports up to three port groups
- Network bond modes and maximum packet transmission sizes

We accepted the defaults. In about 10 minutes, each OneXafe came online.

Ease of Software Installation and Setup Depends Upon Your Environment
If your first OneXafe appliance can quickly communicate with StorageCraft’s hosted OneSystem application, you could complete setup in under 30 minutes.

Regardless of the time the initial setup takes, subsequent OneXafe deployments in your environment should be easy and straightforward. After physically installing a OneXafe, one may immediately jump to steps 3 and 4 above to complete its registration and configuration.

**Adding Capacity is Simple, But Plan Ahead**

OneXafe scales storage very granularly but to very high capacities (over 1PB). We found OneXafe makes adding more capacity to a node or nodes to a cluster almost a non-event.

**Drive Capacity Discovered Automatically**

If one only needs to add a new drive (HDD or SSD), simply install it into an available OneXafe drive slot and you are done. OneXafe automatically discovers the new drive and makes that capacity available in its storage pool.

**Join a Cluster with a Click**

To grow an existing OneXafe cluster, one adds another node to it. While in the Web Console Configuration tab, we selected a OneXafe appliance and clicked the **Join** button. This joined one OneXafe appliance to the other to create a logical OneXafe cluster. This task completed seamlessly in the background.

**Planning a Prerequisite to Adding More Capacity**

One needs to consider disk and cluster fault domains when increasing capacity. OneXafe automatically spreads data across multiple drives in an appliance and across multiple appliances in a cluster to maintain data resiliency.

In small deployments with one or two OneXafe appliances, only add drives of the same size and type to each OneXafe appliance. Further, make sure each appliance in a small cluster has the same number of drives in it.

**When Thinking OneXafe Data Protection, Think Snap**

We now prepared to back up a VM. Having registered OneSystem with vCenter during setup, OneSystem had discovered all the VMs in the environment.

**Creating a New Policy**

To back up a VM, we navigated to the **Policies** tab on the OneSystem console. This displayed a list of pre-existing policies. To add a new policy, we clicked on the **Add New** button on the Policies tab. This brought up a pop-up window in which we configured the following:

- **Policy name.** This is a name you create
- **Snapshot frequency.** The frequency options ranged from once every 15 minutes to monthly
- **Storage target.** Displayed available folders on the OneXafe appliance to store snapshots
- **Retention periods.** The length of time for OneXafe to retain the snapshots it takes. It could create 15 minute, daily, weekly and monthly snapshots
- **Replication.** Optionally choose another OneXafe appliance or StorageCraft’s Cloud Services as a replication target

We saved this newly created policy.

**Policies Displayed in a Pop-up**

After saving the policy, we clicked on the Protection tab, which displayed the available VMs and physical machines to protect. We hovered our mouse over an already protected machine to examine its policy. A pop-up window appeared that displayed the machine’s RPO, storage target, retention period, and recovery points.
To change the policy, we selected a machine and clicked on the Assign Policy button which brought up a pop-up window. We selected the policy we created and clicked Save. This assigned the data protection policy to the VM, which took effect immediately.

**Built-in Protection Against Ransomware**

OneXafe exclusively uses snapshot technology for data protection and natively gives organizations four means to protect against ransomware.

First, it automatically protects any data that organizations store on OneXafe folders or shares. Its continuous data protection (CDP) takes a snapshot once every 90 seconds for the first hour on each folder or share.

Second, OneXafe imposes no limit on the number of snapshots taken.

Third, OneXafe automatically retains snapshots taken on the hour for a day and snapshots taken daily for a month. It retains weekly snapshots indefinitely.

Fourth, OneXafe’s file system uses an immutable object store. This immutable object store protects the data from infection by ransomware by freezing the data so it cannot be changed.

**No Wait Recovery**

Having protected a VM, we tested OneXafe’s Virtualboot recovery capabilities.

**Pick a Snapshot, Any Snapshot**

By again going to its OneSystem Console, we clicked on the Recover option. We selected the System Recovery tab to do a system level VM recovery. We got a wizard-like experience that walked us through a VM recovery.
We selected a VM to recover, which took us to the **Recovery Point** tab. This tab displayed all the VMs available snapshots. We selected the snapshot we wanted to use as the recovery point. This selection took us to the **Target Machine** tab. Here, we selected the location to where which we wanted to recover the VM, verified the information on the **Summary** page, and clicked the **Recover** button.

**Instant Recovery**

The selected VM immediately began to recover. The VM boot process began shortly thereafter. The VM initially recovers using OneXafe as its source of the VMs data. In the background, StorageCraft migrates all the VMs data from OneXafe to the target machine’s storage.

It first moves all data accessed by the application on the VM as quickly as possible. Over time, it migrates the application’s remaining data during periods of low activity in the environment.

**Full Data Protection, Minimal Human Effort**

Anyone with basic IT knowledge can manage and maintain OneXafe with minimal challenges and effort. OneXafe with its OneSystem provides the core set of data protection, data recovery, and storage features that midsize organizations require.

One can easily create and apply data protection policies and simply perform recoveries. OneXafe eliminates the complexities of setup, machine discovery, data protection, and application recovery. One completes these tasks assured that the applications and data are protected. Using OneXafe, one can perform partial or full recoveries of business-critical data if required.

Depending on one’s technical experience, one may want to contact StorageCraft support to help setup the first OneXafe appliance and OneSystem management console. Ongoing success with
OneXafe depends heavily upon successfully setting up and correctly configuring the OneSystem management console.

While OneSystem is not difficult to setup and configure, some steps were not intuitive to me. Since setup represents a one-time task, StorageCraft support can help ensure one completes it quickly and correctly. Once finished, one can move on to using OneXafe and leveraging all its features.