SOLUTIONS NOTE

Open XDR Security Platform High Availability (HA)

THE IMPORTANCE OF DATA AVAILABILITY

It only takes minutes for a hacker to enter your network, and if at any moment collected data is lost due to a power, network or system outage, an organization may have lost total visibility into breach attempts. **At Stellar Cyber, we realize the importance of high availability and have built multiple approaches to ensuring data loss is mitigated.** This solutions note will give you a basic understanding of how high availability is achieved on our Open XDR Security Platform.

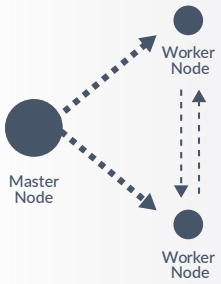
CLOUD NATIVE ARCHITECTURE

It is important to understand the Open XDR security platform's architecture in the context of HA. Our Open XDR platform consists of a family of sensors, agents, and a centralized data processor. Depending on the customer requirements and size of deployment, the sensors and the data processor can be deployed on the same physical server, or separately with sensors and agents to be distributed across the network while the data processor is centralized in a private data center or a public cloud.

The data processor is built upon a cloud native micro-service architecture with clustering. It leverages Containers and Kubernetes as the building blocks for such an architecture. This architecture enables auto-healing functionality if any of the micro-services has issues inside the data processor, with real-time health checks and container management.

NODE CLUSTERING AND DATA REPLICATION

The data processor can be deployed as a cluster of nodes to increase performance and provide node redundancy. **The cluster architecture consists of a single master node and multiple worker nodes.** The master node acts as a data load balancer and distributes data to available worker nodes. The data processor can be configured to keep at least two copies of the same data to provide extra redundancy through data replication and prevent data loss against the loss of a node when there is more than one worker node in the cluster. Also, the data processor can handle up to the performance limits if one or more of the data analyzer worker nodes becomes unavailable. Once a worker node goes offline, the master node will become aware



of this failure and distribute the data to other online worker nodes. Clusters are built to survive loss of worker nodes. If the master node were to go offline, the system would rely on data buffering provided by the network sensors until the master node is brought online again or the standby node becomes active (please see the warm standby section).

Although data replication is great for data availability, it does have a performance impact on the entire cluster, which accounts for roughly 33% reduction when replication is enabled.

Although the data processor has a clustering technology natively built in as described above, it can still be deployed in a single system or in multiple systems as a cluster based on the requirements and needs of the customer.

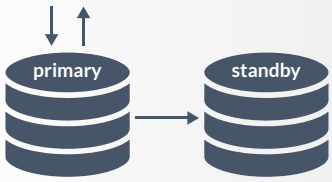
DISASTER RECOVERY

Open XDR supports a data/configuration backup and restore. It is extremely important to set this up if you have a single system for the data processor or need an offsite copy of the data. You can have a data backup and a configuration backup, or a single combined data/configuration backup. If you have separate data and configuration backups, you can configure a different frequency for each. Note that the data backup is very heavy operation and will have performance impact of the system and better schedule at off-peak time.

Although the backup process can be automated at the preconfigured frequency, the restore is a completely manual process which might take a long time, depending on the volume of data to be restored.

WARM STANDBY

In the 3.9 release, the warm standby HA solution becomes available. In a warm standby configuration, nodes can be added to an active cluster, i.e. the primary system, to become a standby system for master node redundancy. After setup, both data and configuration are automatically backed up from the primary system to the standby system. Upon detection of the failure of any master node, the warm standby system can be become the primary in minutes after activated manually. This avoids a lengthy data restoring process in an unfortunate event.



COLD STORAGE

Not all data are equal. For performance and cost reasons, not all the data should be stored as “hot” data which is accessible by the data processor at any time. You can choose to store older data from your data processor on another server which provides cold storage for a long time period, so that you can re-analyze it later or

keep it within reach for compliance reasons. You can import the stored cold data to your working data processor or to a dedicated forensic data processor. This would allow you to visualize and interact with the older data any time with full functionality of the platform at hand.

IN-SERVICE UPGRADES

Interruptions in service sometimes can be intentional, such as taking a system down to perform a software upgrade to the latest version. If a software upgrade were to take 30 minutes, for example, it could create a scenario where a hacker could gain entry undetected during this upgrade period. **Stellar Cyber's built-in "In-Service Upgrade" features allow a software upgrade to be performed at the same time that data ingestion is occurring.** This is achieved by the data processor's micro-services architecture that allows isolated containers that provide various services to be upgraded separately from data ingestion and data lake containers. The data ingestion and data lake containers are components in the system that are rarely upgraded, and even when they are upgraded, these containers are upgraded last in the process and restart within minutes. This method is much more efficient than upgrading a single component or multiple components all at the same time.

DATA BUFFERING

In a distributed deployment, if the sensors that are collecting data lose communication with the data processor due to a network connectivity loss, the sensors can start buffering data to on-board disks and data will be stored locally, based on how much storage has been configured for data buffering. The sensor will continue to send heartbeat checks to the data processor, and once it sees that connectivity has been restored, the sensor will slowly start to transmit its buffer to the data processor so not to overload the data processor with a surge of data after coming back online. **This smart approach ensures data is always available to monitor breaches even if there is a network connection issue.**