How Nuabee improves its customers’ cyber-resilience

Cyber-Resilience by Nuabee · https://nuabee.com/documents/how-nuabee-improves-customers-cyber-resilience/

Cybersecurity vs. cyber-resilience

In the face of increasingly complex threats, particularly cyber-attacks that can be "enhanced" via AI, detection and protection security measures, known as cybersecurity, are not infallible.

Cyber resilience plays a key role in implementing **prevention and recovery measures** to minimize the impact of cyber attacks and other more traditional disasters.

How Nuabee improves cyber resilience

Regular DRP testing essential

Nuabee believes that confidence in cyber resilience can only be achieved through regular DRP testing.

It helps answer the following questions :

- are the applications within the scope of the DRP sufficient to ensure business continuity?
- are server dependencies managed correctly?
- do user reconnection mechanisms work?

Performing regular DRP tests is the only remedy for the false sense of security that comes from having an untested backup solution.

Automatic DRP activation procedures

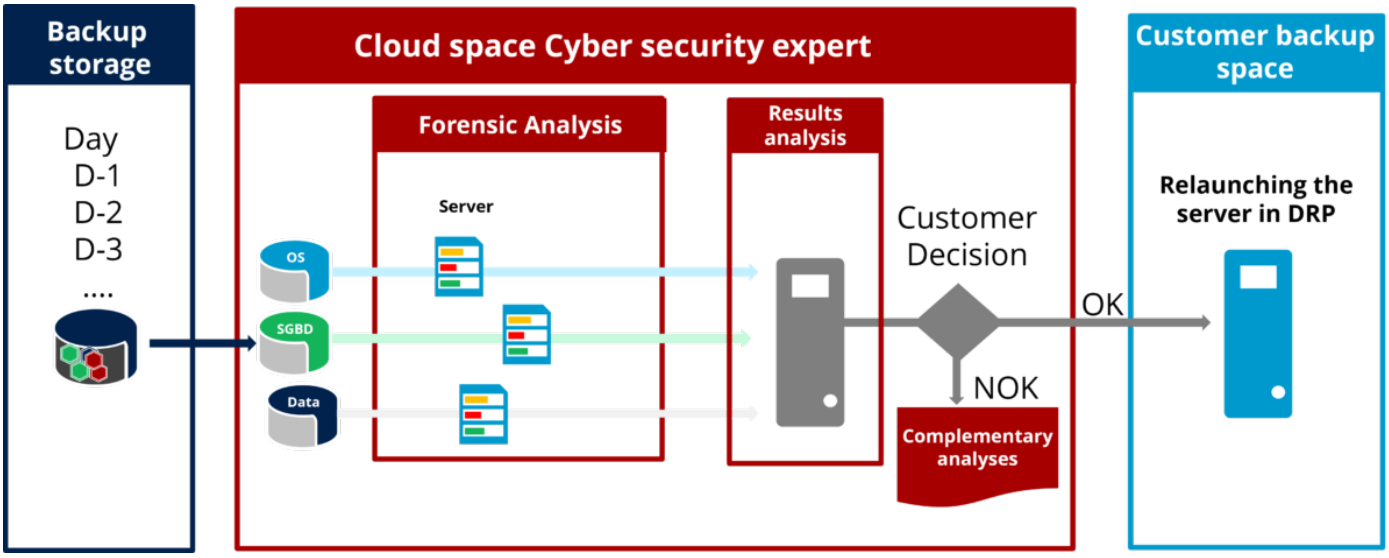
Nuabee has developed clear and detailed procedures for **DRP activation**.

These procedures include specific steps for assessing the situation, verifying the identity of the caller, deciding whether to activate the plan and coordinating recovery efforts. Nuabee teams are trained to follow these procedures, ensuring a smooth transition to rescue operations.

Cyber crisis management

In the event of a cyber attack, Nuabee supports the customer (and your cybersecurity firm) in **cyber crisis management**.

Nuabee provides complementary isolated and air gap environments to run expert digital investigation tools.



It is also possible to provide the service provider with different versions of the machines in the customer environment to carry out investigations. The service provider has autonomy to carry out his actions via administrator access to an isolated Cloud environment.