

Threat Risk Analysis



WHY MNP DID THIS ANALYSIS

MNP was contracted to perform a Threat and Risk Analysis (TRA) of CognisantMD's Ocean environment in the summer of 2018. There were two main threat actors considered in the analysis.

MNP's TRA helps an organization measure their risk exposure using the best sources of security incident and breach data (the Verizon Data Breach Investigation Report (DBIR)), allowing MNP to measure industry specific risk posed by threat actors. CognisantMD chose two specific threat actors that they are primarily concerned with and feel their platform is designed to protect against.

The scope of this analysis was the CognisantMD IT Ocean platform, in particular the encrypted Personal Health Information (PHI) data that is handled by Ocean. The two threat actors considered are:

- 1) Individual External Hacker
- 2) Internal Rogue Employee

Our approach included gathering information through interviews. Based on the results of the interviews it was determined if the controls were in place and their maturity level.

SUMMARY OF FINDINGS

Based on MNP's understanding of the CognisantMD's Ocean platform and information gathered from interviews and documentation both threat actors represent a low risk.

MNP identified the following risk issues:

Threat Actor	Threat Vector	Risk
Individual Hacker	Web Application Attacks	Low
Rogue CognisantMD Employee	Access to PHI	Low

This is due to a few key controls:

- The Ocean platform is using strong encryption mechanisms throughout.
- The Cloud connect component used for establishing the encryption mechanism runs autonomously and allows a transparent client experience of the Ocean application.

These are not the only controls that CognisantMD has in place but are the strongest and most efficacious. The key used for encryption is based on a passphrase chosen by CognisantMD's customers. A key recommendation is that customers be required to pick a very strong passphrase.

Beyond this recommendation, CognisantMD should consider a number of the other recommendations that MNP suggests. They will reduce the likelihood of successful Web Application attacks and data, including PHI, exfiltration.

COGNISANTMD'S SECURITY STANCE IS GOOD.

