Customer Overview:
Large global financial technology company employing over 9.000 people, with multiple locations across Europe, the Americas and Asia Pacific.

Large Global Fintech Organisation turns to ProLion to recover from Ransomware Attack

Solution: Deploy and utilise ProLion RestoreManager and CryptoSpike

Challenge:

This global financial services company was hit by a ransomware attack that infected their NetApp file system. As a result, 14 filers were taken offline to avoid further spread, with all user access blocked, significantly impacting business operations.

Impact:

Loss of business, unplanned downtime, damaged reputation due to negative coverage in the financial and technology press.

Stage 1 Install and run RestoreManager

- Utilise RestoreManager to index the entire NetApp storage environment
- Ingest 'blocklist' threats from CryptoSpike to identify all known threats present in the environment
- Delete identified threats and recover cleansed data

Stage 2 Install and activate CryptoSpike

- CryptoSpike was deployed for ongoing proactive protection of the storage environment
- CryptoSpike is now set to block known threats as well as alerting to anomalous user behavior

Result:

Using both products in tandem the organisation was able to quickly identify threats that had infected their environment and take the necessary steps to nullify threats and recover the data, allowing the filer environment to be brought back online. CryptoSpike now provides ongoing proactive threat prevention from future ransomware attacks.

Key Benefits:

- The organisation was able to rapidly get back into production, meaning less downtime and loss of business
- The organisation avoided paying a ransom
- Mitigated negative reputationaldamage

Key Learnings:

Endpoint / edge protection was enabled on the customer's network; however, this was not enough to stop the attack getting into the file system.

It is therefore essential to protect the NetApp file system with a multi-layered security approachProLion's integration with native NetApp technologies such as FPolicy and SnapDiff means that customers can enable ransomware protection and centralized catalog with minimal system impact.

Ongoing benefits:

- Risk mitigation – **Blocks Ransomwarebefore** it enters the system
- Risk mitigation – Stops the spread of any suspicious outbreak
- Risk mitigation – instant recovery of data without major data loss – just the affected files, not the whole volume
- Operational – Data & Access Transparency enables easy daily operations to identify all user behavior on the file system (finding lost files etc.)
- Auditing – Data & Access Transparency provides forensic data on user behavior and helps minimize **Insider Threats**

Installation Details:

The installation was completed remotely:

- 3 Sites
- 3 CryptoSpike servers
- 6 FPolicy Servers
- 3 RestoreManager servers
- All remotely deployed and configured within a week