CASE STUDY

BUSINESS CONTNUITY & DISASTER RECOVERY

FOR A LEADING HEALTHCARE PROVIDER

CCS
technologies

ABOUT CLIENT

The client is a South Asian healthcare provider delivering advanced patient care through integrated practice units, superior infrastructure, medical facilities, and clinical services.

BUSINESS CHALLENGE

The on-premises data center of the healthcare provider was attacked by ransomware, which called for efficient threat resolution. During the failback operation, they were attacked again, and PACS (picture archiving and communication system) showed signs of being infected by the virus.

CCS SOLUTION

CCS Cloud team was judicious when assessing the situation at hand and carried out the recovery with extreme caution.

Phases of the recovery process:

01 Ransomware attack happens at the client's on-premises data center on Dec 3rd, 2020

02 CCS quickly isolates the infection, enables DR through Azure site recovery console on the same day

03 On day 2, CCS works with Microsoft team to resolve failback of particular VM on-premises

04 On day 3, 2nd targeted ransomware attack takes place

05 CCS identifies 2nd ransomware infection on the same day

06 Restores data from cloud to the NAS server on-premises

07 Moves about 7 TB of Azure VM data (PACS VM) to Azure storage account

08 All PACS app data successfully moved to the Azure storage account

09 Creates the Azure Import/export jobs & requests the Microsoft team to send data on hard disk by day 8

10 CCS receives the hard disk from the Microsoft data center by day 20 and completes the DR process successfully

- Isolating the affected servers took precedence over DR enablement.
- Post isolation, CCS enabled DR through the Azure Site Recovery console.
- CCS worked with Microsoft to restore the data from Azure to get the PACS up and running and used shippable devices to transfer data to the on-premises NAS (Network Attached Storage) server - in an offline manner.
- CCS moved about 7 TB of Azure VM data (PACS VM) to the Azure storage account.
- Given latency issues, CCS sent a hard disk to the Microsoft data center and subsequently copied the received data to the client's on-premises server.
- To avoid future issues, we recommended and helped the client to implement security best practices.

BUSINESS BENEFITS

- Despite facing newer challenges throughout the recovery phase, CCS Cloud Experts carried out the recovery efficiently and had all systems up and running in a short time.
- The client experienced minimal business disruption.
- CCS implemented new firewall policies and threat analysis monitoring to help the client detect future threats, if any.
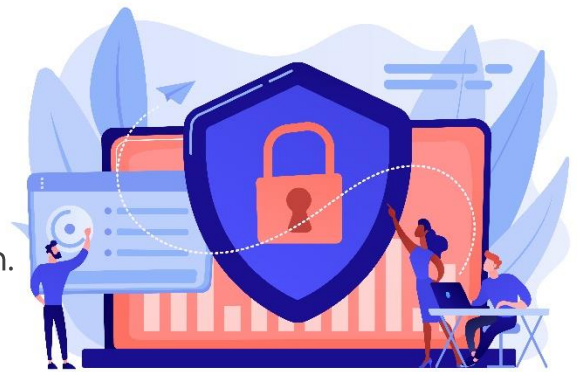
CORPORATE OFFICE

39/5173 - D, K C Abraham Master Road,
Panampilly Nagar, Ernakulam, India

US OFFICE

919 North Market Street, Suite 950
Wilmington, DE 19801, USA

DEVELOPMENT CENTER 1 & 2

1st & 4th floor, Lulu Cyber Tower 1,
Infopark, Kakkanad, Cochin 682030, India

DEVELOPMENT CENTER 3

Erayilkadavu, Kottayam, Kerala
686 001, India

collaborate@ccs-technologies.com

Business Enquiries: +91 96564 89733, +91 95676 71727, +1 909 979 9884