ELISITY

CASE STUDY

How Cromwell Hospital Uses Elisity to Protect Mission-Critical Patient Data and Prevent Ransomware on its Network

Overview

With a variety of connected devices, highly sensitive patient data, and mission-critical services, hospitals have long been on the frontlines of cybersecurity and a high-profile target for bad actors. Medical devices like MRI and CT scanners often operate on legacy operating systems, making them difficult to protect with traditional IT-based security controls.

International healthcare company, British United Provident Association (Bupa)'s Cromwell Hospital is a state-of-the-art facility in London, specializing in complex procedures and advanced care. Like all healthcare organizations, Bupa is very protective of patient data and looked to improve its security posture against a new wave of threats, without disrupting hospital operations.

"Bupa is on a cloud journey," said Bupa Group CISO Paul Haywood. "We are driven to move out of our data centers into a cloud-dominant environment and customers rely on us to look after that data by effectively managing policy and access."

Bupa Cromwell Hospital

Cromwell Hospital is a private hospital located in London, England, it offers a wide range of medical and surgical services, including both inpatient and day patient care, with a total of 152 beds, well-equipped with state-of-the-art medical technology, complex network of medical devices, and facilities.

The Challenge

Bupa Cromwell hospital needs a solution to identify and secure unmanaged devices on its network.

The Solution

Elisity implemented their solution to identify and secure unmanaged devices on Bupa Cromwell hospital network in under two days.

The Outcome

Elisity platform helped to protect clinical devices and patient information at Cromwell Hospital with fast results and real-time security policy enforcement.

sales@elisity.com

www.elisity.com

Elisity Overview

The Identity Graph creates context for effective security policy management by mapping and understanding users, devices, apps and their relationships on the network.

Identity-based microsegmentation is done by using context from the identity graph to establish granular, least privilege access policies.

Elisity is a cloud-based solution that can be deployed in less than an hour, with no hardware or network upgrades required.

The Challenge

From X-ray machines and heart monitors to badge readers and security cameras, unmanaged devices present a unique threat to healthcare security. Unmanaged devices, those without a software agent or additional IT control capabilities, typically use old operating systems and can't be patched or managed with traditional network security systems. As a result, these devices are quickly becoming the preferred attack vector for ransomware and directed attacks.

Bupa, like many organizations, invested in a variety of solutions to solve individual issues with varying degrees of success. At Cromwell Hospital, the team previously employed traditional firewalls and network access control (NAC) technologies but wanted deeper visibility into the devices on its network – and the potential risks. Bupa needed an all-encompassing view to quickly identify unmanaged devices and deploy policy without undergoing a large hardware refresh.

The Solution

Elisity sat down with Haywood and the team at Cromwell Hospital to review the systems they implemented in the past and understand the challenges in managing their infrastructure. After pinpointing the policy gaps in the hospital's existing solutions, the team quickly moved into proof of concept with Elisity's Cognitive Trust Platform™ to identify the devices running on the network. From there, Elisity began developing microsegmentation and least privilege access policy, mapped to the identities of the device classes and user groups in the environment.

"We've put policies around our medical devices, which allowed us to manage the traffic going into them and now have layers of mitigation in defense and depth around the key risks we identified."

Alma Kucera, Cromwell Hospital CISO

The Outcome

Elisity's Cognitive Trust Platform™ delivers frictionless, centrally managed, and software-defined zero trust access security to effectively and efficiently protect clinical devices and patient information at Cromwell Hospital from lateral movement of ransomware payloads, advanced persistent threats, and insider threats.

"In my 30 years of working in technology and security, I've never delivered a product into an environment and got instant benefit like we did with Elisity."

Paul Haywood, Bupa CISO