COLORTOKENS

FERNANDEZ HOSPITAL
A unit of FERNANDEZ FOUNDATION

Fernandez Hospital Implements Xprotect to Secure Patient Data, Medical Devices, and Critical Applications from Cyberattacks

Industry
Healthcare

Location
India

Key Challenges

- Lack of protection from insider attacks, unknown attacks, and file-less malware
- Poor visibility of existing vulnerabilities in the multi-campus heterogeneous network
- Bandwidth and resource intensive patch management and signature updates for all onsite and remote systems
- No centralized asset management
- Need for application control and management

Solution
ColorTokens Xprotect solution defends patient data from cyberattacks launched using sophisticated techniques like file-less malware and ransomware.

Fernandez hospital was established in 1948 with a mission to increase the natural birth rate and provide state-of-the-art healthcare to women and newborn babies. The hospital boasts multiple healthcare facilities in Hyderabad, India.

Fernandez hospital is known to provide reliable, efficient, and personalized care of the highest possible medical standards. The hospital has helped women to deliver over 190,000 healthy babies to date.

Fernandez hospital has a heterogeneous and multi-campus IT environment. There are more than 25 servers running Ubuntu precise, Oracle Linux Server 7 to 7.3, Red Hat Enterprise Linux Server 7.0 to 7.4 and other opensource and Windows operating systems (including legacy Windows XP). Antivirus, firewall, and email security products have been deployed across the hospital campus. In addition, the hospital has Win XP and Windows 10 desktops for hospital staff, and a Wi-Fi enabled campus with separate Wi-Fi networks: one for patients, and one for doctors and staff. The network across these hospitals is segmented using internal firewalls. The hospital has implemented a modern Hospital Information System (HIS) application, vendor management, and finance applications.

The Challenge

Despite heavy investments in security, the surge in the number of attacks has always kept the infosec team on their toes. An unsuccessful cyberattack in the past made the infosec team realize that the traditional security controls in their network could not protect them from APTs (advanced persistent threats), file-less malware, and ransomware attacks. The hospital had to restore data from the last available backup. Since then Fernandez hospital carries out a Voluntary Product Accessibility Template (VPAT) assessment every six months. It takes over one month for the hospital to fix discovered vulnerabilities, resulting in a huge operational and cost overhead.

The Solution

ColorTokens Xprotect was deployed to protect endpoints and servers, including legacy and unpatched systems, against APTs, file-less malware, and ransomware attacks. The two-phased deployment included sanitization of processes at endpoints followed by installation of Xprotect across all endpoints. The flexible deployment option provided an on-premise dashboard deployment, helping the hospital meet its compliance requirements. ColorTokens' intuitive dashboard provided an asset inventory of all managed resources that process sensitive patient information (ePHI) in a single pane of glass. The infosec team at Fernandez hospital can now investigate an individual asset, its access levels, and define allocation of user privileges (e.g., hospital applications, USB sticks, and CDs).

COLORTOKENS

Business Benefits

- ColorTokens solution successfully blocked 140+ malware while protecting 2100+ critical assets across 75+ datacenters
- Secured all critical systems including MRI scanning machines, HIS, and front desk systems to ensure protection and business continuity
- Protected mission critical medical machines that were not allowed to upgrade or apply patches
- Sanitized existing technology infrastructure from pre-existing malware

ColorTokens Solution Stack

ColorTokens Xprotect solution for endpoint protection

“ColorTokens Xprotect has made us resilient to file-less malware, ransomware, and other unknown healthcare malware. Our infosec team now have a unified view of the security posture across the multi-campus environment. Xprotect has given the team more confidence to face compliance.”

– Nanda Kishore, Head of Technology, Fernandez Hospital

In addition, Xprotect’s protection mode has avoided the need for any future patch management and signature updates, keeping the hospital’s security posture intact. With ColorTokens Xprotect, Fernandez hospital is protected from zero-day attacks, insider attacks, unknown attacks, APTs, ransomware, and file-less malware.

Results and Benefits

With ColorTokens Xprotect, Fernandez hospital has benefited from enhanced protection against execution of malicious processes at the endpoints. A 100% proactive defense has increased the hospital’s organizational credibility in the eyes of auditors and investors. The solution’s centralized visibility capability provides real-time granular views into processes running at endpoints and has enabled faster incident response and improved compliance. ColorTokens’ solution and services provided a faster ROI by reducing computing resources, eliminating periodical patching and VPAT, and improving asset efficiency — all of which translated into energy, cost, and time savings.