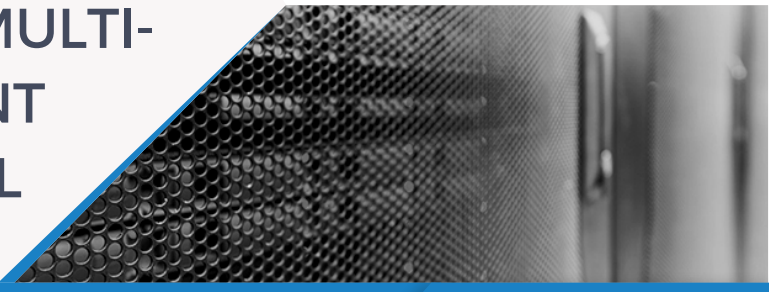
# COLORTOKENS PROTECTS HETEROGENEOUS AND MULTI-CAMPUS IT ENVIRONMENT AT FERNANDEZ HOSPITAL



Case Study

**ColorTokens protects patient data from cyber attacks launched using sophisticated techniques like fileless malware and ransomware.**

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

> ColorTokens Xprotect has made us resilient to fileless malware, ransomware, and other unknown healthcare malware. Our InfoSec team 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 P,**
> Head of Technology,
> Fernandez Hospital

Fernandez Hospitals is known to provide reliable, efficient and personalized care of highest possible medical standards. The hospital has helped mothers to deliver over 1.7lac healthy babies to date.

Fernandez hospitals have heterogeneous and a multi-campus IT environment. There are over 50 servers running Ubuntu 14.x to 16.x, Red Hat and other opensource and Windows operating systems (including legacy Windows XP). Antivirus, firewall and email security have been deployed across the hospital campus. In addition, the hospital has Win XP and Win 10 desktops for hospital staff, Wi-Fi enabled campus with separate Wi-Fi networks: one for patients, one for doctors and staff. The network across these hospitals is segmented using internal firewalls. The hospital has a modern HIS application, vendor management & finance applications.

## The challenge

Despite heavy investments in security, the surge in the number of attacks has always kept the InfoSec team on toes. An unsuccessful cyber-attack in the past made the InfoSec team realize that the traditional security controls cannot protect them from APT, file-less malware and ransomware attacks. The hospital had to restore data from the last available backup. Since then Fernandez hospital carries out VAPT assessment every six months. It takes over one month for the hospital to fix the discovered vulnerabilities this is a huge operational and cost overhead. In addition, there are several challenges that the security team are firefighting:

- 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 & management

## The solution

ColorTokens Xprotect protects end-points and servers, including legacy and unpatched systems, against APT, fileless malware and ransomware attacks. The two-pronged deployment includes 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 compliance requirement. ColorTokens RADAR360 intuitive dashboard provides an asset inventory of all managed resources that process sensitive patient information (ePHI). The InfoSec team at Fernandez hospital can now investigate individual asset, their access level and define allocation of user privileges (Apps., USB etc.).

In addition, ColorTokens Xprotect protection mode avoids the need for any future patch management and signature updates, keeping security posture intact. With ColorTokens Xprotect Fernandez hospital is protected from zero-day attacks, insider attacks, unknown attacks, APT, ransomware, and fileless malware.

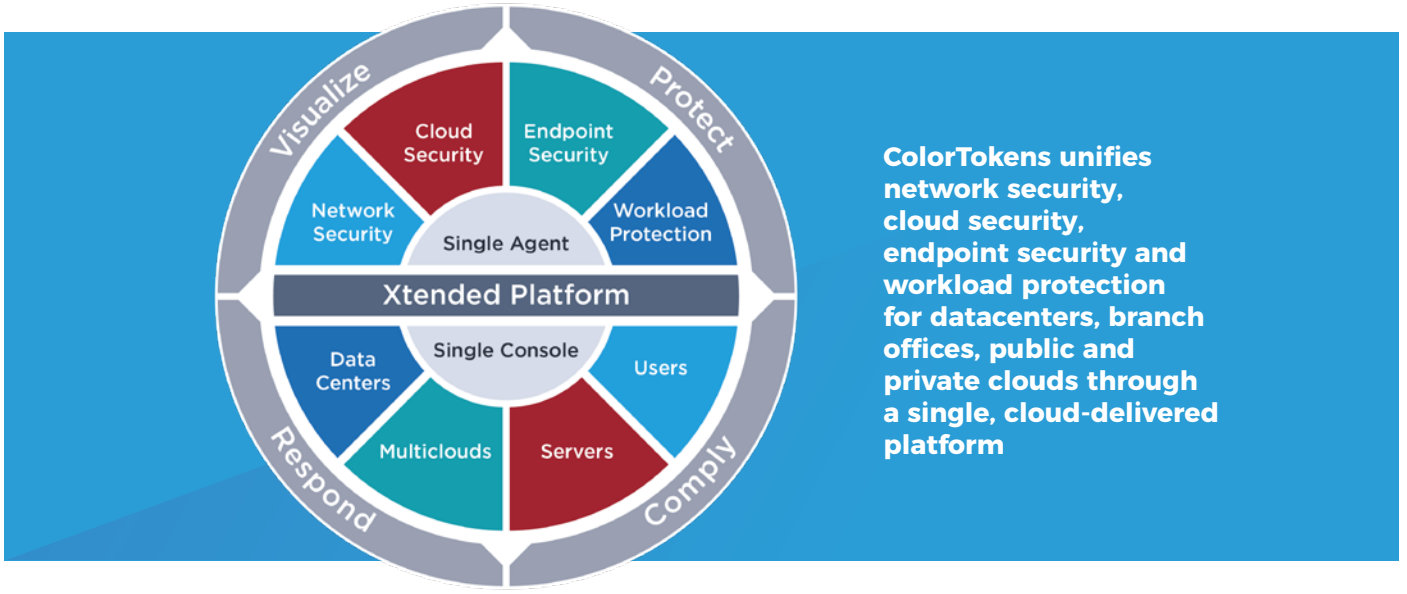
## Client benefits

ColorTokens unified security solution provides faster ROI, the client is benefited with:

- Protection from installation and execution of malicious processes at the endpoints
- Centralized asset visibility & control for compliance and faster incident response
- Real-time visibility to the processes running at endpoints
- Reduced computing resources, improved asset efficiency & energy conservation
- Elimination of periodical patching & VAPT, translating into costs and time savings
- Sanitization of existing technology infrastructure from preexisting malware
- Complete data privacy & log management for audit compliance
- 100% proactive defense protects the organizational credibility and boosts investor confidence

# ColorTokens Xtended ZeroTrust Platform

Built from the ground up to make zero trust a reality for any enterprise, the ColorTokens Xtended ZeroTrust Platform delivers a refreshing, new-generation of security to provide the following unique benefits:




## Xview for Visualization

**Xview** – part of the Xtended ZeroTrust Platform – provides unified visibility across on-premises and mulitcloud infrastructure, giving a telescopic view into networks, clouds, applications and endpoints. The Xtended Visualization analytics engine integrates with market-leading threat intelligence to investigate suspicious behavior anywhere in the enterprise—while protecting against zero-day threats. Integrated widgets and canned reports enable security teams to achieve faster time-to-compliance for critical mandates like PCI, HIPAA and GDPR. And, the platform's built-in scanner hunts for vulnerabilities in real-time – providing an immediate return on your security investments.

## Xshield for Workload Protection

**Xshield** – part of the Xtended ZeroTrust Platform – enables enterprises to achieve consistent visibility and control of all cloud workloads – regardless of the location or granularity of the instances. Built from the ground up for unrivaled software-defined micro-segmentation, ColorTokens enables the modern enterprise with instant workload visibility, automated and dynamic policy enforcement, and the ability to control any communications to/from the workload instances.

## Xprotect for Endpoint Detect and response

**Xprotect** – part of the Xtended ZeroTrust Platform – provides enterprises with a robust signature-less approach that works at the kernel level to block unauthorized processes on endpoints, servers and legacy/fixed-function systems. Go beyond signature-based security, that blocks only 'known-bad' threats, with powerful whitelisting, prevent unauthorized software execution on endpoints – even with administrator rights and block malicious processes from spawning and infecting legitimate applications.

---

CIOs and security teams are frustrated with too many complex, reactive point products—and are still vulnerable to sophisticated threats and attacks. ColorTokens proactively secures enterprises through a single, cloud-based Xtended ZeroTrust Platform. This enables enterprises to instantly visualize and segment their entire IT infrastructure, block advanced malware, contain and respond to APTs and zero-day attacks – all while seamlessly integrating with existing security tools. ColorTokens makes end-to-end zero trust security a reality for any enterprise—covering protection, detection, investigation and response through a single-agent, single-platform architecture. Enterprises can now protect networks, multiclouds, containers, workloads and endpoints with the world's first single agent and platform that unifies network, cloud and endpoint security.

COLORTOKENS

ColorTokens Inc., a leader in cloud-delivered ZeroTrust security, provides a modern and new-generation of security that empowers global enterprises with a proactive approach to single-handedly secure cloud workloads, dynamic applications, endpoints and users. Through its award-winning Xtended ZeroTrust Platform, ColorTokens delivers the only cloud-based solution that combines AV, EDR, workload protection and application control into one ultra-lightweight agent. This enables enterprises to instantly visualize and segment their entire IT infrastructure, block advanced malware, contain and respond to APTs and zero-day attacks—all while seamlessly integrating with existing security tools.



colortokens.com
sales@colortokens.com