COLORTOKENS

CASE STUDY

# Leading Cancer Center Partners with ColorTokens to Strengthen its Cyber Resiliency and Reduce Risk

INDUSTRY: Healthcare and Lifesciences

HEADQUARTERS: U.S.A.

## Overview

One of the leading, nationally ranked cancer and research centers in the U.S. with multiple data centers and campuses, has extensive collaborations with many universities across the globe. Their network is comprised of 10,000+ servers running a mix of modern and legacy applications, over 20,000 endpoints, and over 100+ petabytes of data.

The cancer center witnessed an increased frequency of sophisticated ransomware attacks, specifically targeting backup administration control. They had a clear need to control the processes during backup along with minimizing exposure to the environment. Due to the large amounts of data generated daily requiring granular visibility and control, they needed to protect the backup servers storing the EMR (EPIC) system data against ransomware attacks. In addition, the radiation oncology application that accounts for over 50% of hospital revenue also needed protection from malware and ransomware.

The healthcare provider was experiencing lengthy timelines and high costs to achieve the desired outcome with their existing solution and were exploring alternative Zero Trust microsegmentation solutions that could both simplify the process from installation to enforcement and get their systems up and running with no disruption to existing infrastructure.

## The Challenge

**SECURE EPIC:** The customer using traditional tools (FW, ACL's) to secure their patient information and related systems. However, considering recent ransomware attacks, they wanted to adopt a Zero Trust architecture to secure its patient data and systems.

**SECURE LEGACY SYSTEMS:** The customer has several systems in the network that are no longer supported by the manufacturer, no patches are available and hence these were left exposed to attacks.

**BLOCK UNAUTHORIZED TRAFFIC:** over 60% of the healthcare provider's revenues are tied to their ability to perform diagnostic work in one department. They wanted to gain complete visibility into this application and quickly block un-authorized traffic without making significant changes to the network architecture.

**SEGMENT A FLAT DATA CENTER NETWORK:** With a flat network, even if one application is compromised it can be used as a launch pad to spread ransomware throughout the throughout the entire network.

> "With ColorTokens Zero Trust solution, we were able to achieve the desired outcome we needed with surprising ease and zero disruption given the complexity of the task. This resulted in breaking down silos within our organization, creating agility and driving decision-making using accurate data – we've seen amazing results with ColorTokens."
>
> - Head of Infrastructure, Healthcare Provider

## The Approach

In order to safeguard the cancer center from future potential ransomware attacks in both new and legacy systems, the ColorTokens team had to work diligently with the IT infrastructure team on a holistic plan for achieving the desired outcomes. ColorTokens implemented Zero Trust microsegmentation throughout the network on all systems, tracking their Zero Trust journey with strategic business-driven reporting. This method enabled a Zero Trust-based approach for securing crown jewels that account for over 50% of revenue.

In addition, ColorTokens made automatic policy recommendations with dynamic policy graphs for high scalability, ML/AI-based auto-tags for automatically tagging over 10K servers, and end-to-end Zero Trust that can be deployed on servers and endpoints on-premises and/or cloud, providing the cancer center with all the flexibility and security that they needed.

## Results and Benefits

With the implementation of Xshield, it was easy to deploy and use microsegmentation based on Zero Trust principles. Having no hardware required meant there was zero disruption to the cancer center's existing infrastructure. Although the cancer center has several campuses ranging in sizes, keeping them cyber secure with ColorTokens' approach was easy to manage, did not require a large team or intensive training to learn how to use Xshield. The cancer center was able to isolate their legacy systems within just two days, not only reducing their risk, but doing so in an extremely speedy fashion.

## Conclusion

Overall, ColorTokens supported the cancer center and their campuses regain their security in their legacy systems, implemented Xshield in order to provide full visibility into all network connections to monitor risk levels, and isolate and secure EPIC back-up servers, which can cause catastrophic losses and operational downtime in the event of an attack. The cancer center is now fully capable and confident of running Xshield on their own.

**Simplifying Your Journey to Zero-Trust Architecture**

ColorTokens is a leader in delivering innovative and award-winning zero-trust cyber security technology solutions such as network micro-segmentation, endpoint hardening and whitelisting, cloud and container security, and zero-trust network access. ColorTokens is a US corporation headquartered in Silicon Valley, and has approximately 400 employees world-wide, with offices in the United States, the United Kingdom, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please visit **colortokens.com**