COLORTOKENS

CASE STUDY

Adopting Zero Trust Architecture

Large Children's Hospital in United States Partners with ColorTokens to Adopt Zero Trust Architecture and Strengthen Cyber Resiliency

Healthcare

U.S.A.

Overview

One of the nation's largest children's hospitals is partnering with ColorTokens to support its mission to strengthen its digital resiliency by adopting the zero-trust architecture. With the adoption of ColorTokens' Xshield Enterprise Microsegmentation Platform, the hospital will be able to strengthen its defenses against advanced persistent threats, ensure compliance, help reduce cost and de-skill adoption of zero trust architecture.

To keep up with the increasing sophistication and frequency of cyberattacks on healthcare organizations and ensure that clinical operations can continue as usual even despite a cyberattack, the hospital decided to establish dynamic micro-perimeters for critical applications to strengthen resiliency. After careful evaluation and testing, the hospital decided to partner with ColorTokens to help with its mission.

The Challenge

Over the years, the hospital had spent significant amounts of money, time and resources to strengthen its perimeter security. They invested in several technologies like firewalls, deception, anti-virus and had created multiple layers of defenses to keep the adversaries from entering its network. They also had a strong endpoint detection and response technology to respond if they were able to breach the multiple layers of defenses.

Recognizing that it's a question of 'when' and not 'if' that the adversary will gain access to its network, the hospital wanted to ensure that ransomware does not create a catastrophic event and affect patient life in anyway once it breaches their traditional defenses.

Keeping this in mind, the hospital set the following as their desired outcome:

1. Establish a dynamic micro-perimeter for mission-critical applications like EHR (EPIC, Cerner, PeopleSoft and other clinical applications), without impacting application performance.

2. Reduce the attack surface for hackers, by restricting lateral movement of ransomware.

3. Reduce the blast radius, by containing the ransomware to a small segment of the networ

4. Reduce blind spots by gaining complete visibility of internal network traffic (typically, firewalls are blind to 70%+ network traffic).

5. De-skill adoption of zero trust architecture by adopting an easy to use and manage solution.

The Impact

Within four weeks, ColorTokens was able to demonstrate how the hospital could achieve all its desired outcomes by leveraging its Xshield Enterprise Microsegmentation Platform. Listed below are the key security and non-security values delivered through the evaluation phase.

Discovery of unauthorized traffic and misconfigurations within hours of deployme.

Auto tagging of assets to save operational time (also enriched CMDB).

Ability to block unauthorized traffic with a few clicks.

Accurate flow map to and from un-managed devices on the hospital network.

Automated policy recommendation to allow or block traffic.

Low memory and CPU consumption, no impact on application performance.

Conclusion

Before trying ColorTokens, the hospital had tried to achieve the same outcomes using legacy technologies from major networking hardware companies. Often, these companies offer their microsegmentation product at no or low cost, however this hospital quickly realized that legacy technologies require a lot of manual effort to use and maintain and this would become an unsustainable burden for hospital employees.

With ColorTokens, the hospital has already been able to break down organizational silos, standardize processes, and manage its cyber operations on a single integrated platform. Once fully implemented, the solution is expected to have a profound impact as the hospital will be closer to fully adopting the zero-trust architecture and significantly strengthen its digital resiliency

About ColorTokens:

ColorTokens, the leading enterprise microsegmentation company, stops the lateral spread of ransomware and malware within an organization's diverse network topology. The ColorTokens Xshield platform visualizes traffic flows between workloads, devices, and the internet, enforces granular micro-perimeters to stop unauthorized traffic, and isolates crown-jewel assets and compromised systems in response to a breach. ColorTokens protects organizations by stopping ransomware and malware in their tracks, saving millions of dollars in business operations interruption.