COLORTOKENS

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

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, 20,000 endpoints, and 120+ 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 60% of the hospital revenues 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 alternate Zero Trust micro-segmentation solutions that could both simplify the process from installation to enforcement and get their systems up and running with no disruption to existing infrastructure

Desired Project Outcomes

Security automation

Time and cost efficiencies

Reduced risk

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:** 66% 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.

ColorTokens Solution

The ColorTokens team worked with the IT infrastructure team on a holistic plan for achieving the desired outcomes, implementing Zero Trust micro-segmentation throughout the network on all systems, and tracking their Zero Trust journey with strategic business-driven reporting.

The ColorTokens solution:

Zero Trust-based approach for securing crown jewels that account for 60%+ of revenues

Automatic policy recommendations with dynamic policy graph for high scalability

ML/AI-based auto-tags for automatically tagging 10K+ servers

End-to-end Zero Trust that can be deployed on servers and endpoints on-prem and/or cloud

Why ColorTokens

- Easy to deploy and use micro-segmentation based on Zero Trust principles.
- No hardware required, and zero disruption to existing infrastructure.
- Easy to manage – didn't require a large team or intensive training to learn how to use Xshield.
- To isolate these legacy systems, it would have taken the customer several months and significant effort to re-architect the existing network to achieve the same results that **ColorTokens achieved in 2 days.**

ColorTokens Zero Trust Process

- Pilot kick off
- Proving Phase 1 use cases, then validation
- Expanding Phase 1 use cases to include more complex use cases
- In principle technical sign-off
- Dashboard review of Zero Trust posture with Chief Digital Officer
- Pricing proposal submission and negotiations
- Go/no-go decision point – approval provided by CIO and CISO

By comparison, the competition (VMware NSX and Illumio) lacked several capabilities that were needed for a successful outcome:

Ease of management

Legacy system support

No disruption deployment

No changes to existing infrastructure

The customer appreciated the ease-of-use of the ColorTokens solution and one of the critical factors which helped us progress to a win was the creation of segments with zero disruption/changes to the existing infrastructure. With our solution, the customer had access to high availability, real time reporting, and increased business velocity and agility.

Use Cases Demonstrated

- Isolate and secure Epic Back-up Servers which can cause catastrophic losses and operational downtime in the event of an attack.
- Secure legacy systems by isolating them from the network to reduce risks.
- Provide visibility into all network connections on the systems to monitor risk levels.
- Segment CITRIX servers and enforce policies such that servers can only make authorized network connections.
- Ring-fence crown jewel application and Radiation Oncology application.

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

ColorTokens Inc. is a leading innovator in SaaS-based Zero Trust cybersecurity solutions providing global enterprises with a unique set of products and services for securing applications, data, and users across cloud and hybrid environments. Through its award-winning Xtended ZeroTrust™ Platform and context-aware machine learning-powered technologies, ColorTokens helps businesses accurately assess and improve their security posture dynamically.

As cloud adoption grows, traditional perimeters get redefined, and new attack vectors and threat actors materialize, corporations recognize their security posture needs to reflect their Zero Trust philosophy. ColorTokens' technology allows customers to achieve Zero Trust by utilizing rich, meaningful contextual information about the application, microservice, or protected resource, so customers can apply Zero Trust with as secure of a perimeter as they can. ColorTokens' cloud-based SaaS platform can automatically deploy next-generation security controls and increase security posture dynamically without any new hardware, downtime, reboots, or changes to a client's existing systems.

With a team of over 400 people, ColorTokens has global office locations in San Jose, California; New York; London; Copenhagen, Denmark; and Bengaluru, India. For more information, please visit **www.colortokens.com.**