COLORTOKENS

CASE STUDY

Apparel Brand Strengthens Breach Defense with ColorTokens Zero Trust Microsegmentation

Manufacturing
U.S.A.

Overview

One of the most prominent apparel manufacturing brands making everyday apparel that is known and loved by consumers around the world for comfort, quality, and value approached ColorTokens to fortify their cyber defense. It employs tens of thousands personnel in 29 countries and has built a strong reputation for workplace quality and ethical business practices. Unlike most apparel companies, more than 2/3 of the apparel they sell is manufactured in their own facilities or those of dedicated contractors. Owning the majority of their supply chain not only impacts cost, scale, and flexibility, but also the ability to adhere to best-in-class workplace and sustainability practices.

The leading apparel brand had suffered a ransomware attack in the recent past which triggered them to look for a solution against such attacks in the future. To address this concern, they needed a holistic cybersecurity solution to safeguard their data across a wide range of assets, which is why they reached out to **ColorTokens**.

The Challenge

With the dynamic landscape, the apparel brand sought a cyber defense strategy that could significantly improve its security posture and reduce risk in a short period. The solution must:

- **Eliminate Lateral Movement:** The firm had diverse IT environments and applications hosted across multiple locations and the cloud presented a potential risk of lateral movement attacks like ransomware.
- Reduce Significant “network pollution”, a term they used to define misconfigurations and non-compliance with corporate guidelines.
- Work for a wide range of systems – legacy to modern to cloud: Secure OT/IoT assets along with data center assets.
- Implement security controls for legacy systems such as HP-UX, Windows 2000, AIX systems which are not supported by their current EDR vendor.
- Easy to use at scale, with no business disruption.

Approach

ColorTokens swiftly addressed the apparel brand's challenges through a comprehensive approach, leveraging **Xshield** Enterprise Microsegmentation Platform. Listed below are the key security use cases delivered through our end-to-end approach:

- **Panoptic Visibility:** ColorTokens Xshield protected the vast IT real estate, by providing granular visibility and control in a centralized manner. We created path-based policies that helped the customer identify familiar domains and allow restricted access to only those instead of high exposure to other unwanted domains.

- **Deep contextual visibility and control:** Xshield was demonstrated for a wide range of systems using agent and agentless technology, providing visibility and control across data center and assets.

- **Restrict infra-based communications:** Xshield restricted communications across all systems except managed servers, thereby reducing the blast radius across E-W traffic.

- **Ease of Implementation:** Xshield was rolled out in a phased, progressive, and non-disruptive manner within a few months across their critical infrastructure.

- **Ease of Use:** The employees at the organization were able to easily master the concepts over the PoV period without formal training and were able to deploy and manage at scale.

- **Lateral Movement Prevention:** Xshield demonstrated blocking of various attack scenarios to prevent unauthorized lateral movement including blocked ports, open access from the Internet, and selective intranet locations.

- **Securing Legacy Data Center Systems:** Xshield is also instrumental in securing legacy data center systems using agentless technology.

Results and Benefits

In just a few weeks, the apparel brand had achieved significant improvement in the security posture due to the implementation of our Xshield Enterprise Microsegmentation Platform:

1. **Reduce Risk by 70%:** The blast radius of potential attacks was significantly minimized, preventing widespread damage to their critical systems. We blocked all outbound traffic and reduced the N-S traffic.

2. **Block all known malicious ports:** We effectively restricted the unused ports that were in listening mode for a certain time period.

3. Faster resolution to their requests.

In addition, the apparel brand is now considering to secure OT and IoT systems leveraging Xshield Enterprise Microsegmentation Platform for comprehensive coverage.

Conclusion

With ColorTokens, the apparel brand gained a comprehensive approach towards proactive cyber defense and implemented a holistic solution against cybersecurity breaches. Adopting a tailored cybersecurity strategy empowered the brand to thrive in the manufacturing sector, fostering continuous growth and innovation, while empowering the apparel brand for sustained growth and innovation in the manufacturing landscape.

The upcoming course of action involves application-level segmentation to ensure we securely isolate critical applications and fortify them from any potential breaches.

Furthermore, ColorTokens managed cyber operations seamlessly on a single integrated platform, ensuring a non-disruptive transition towards elevated cybersecurity at scale. With the full adoption of the zero-trust architecture, they have successfully bolstered their digital defenses, providing robust protection against cyber threats.

See how ColorTokens' Xshield platform can protect your organization's critical assets.

Sign up for a personalized demo today.

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.