MULTI-BILLION DOLLAR RETAIL CUSTOMER MEETS PCI-DSS COMPLIANCE WITH COLORTOKENS XTENDED ZEROTRUST SECURITY SOLUTIONS

Case Study

The customer is a multi-billion dollar American fast fashion retailer with over 800 stores across the world.

> ColorTokens is the ONLY vendor that understands the customer's limitations and is proactively managing the situation. Others just blame us.
>
> **CIO - Leading Fashion Retailer.**

The fashion retailer has significant investments in brick and mortar and online stores. Enabling this business to run smoothly is a massive IT infrastructure of 10,000 plus endpoints that is heterogeneous and spread across geographies. The customer's data center includes over 600 VMs and the servers are a mix of modern and legacy systems, with Linux and Windows OS. The endpoints include Windows XP, Windows 10, embedded XP and tablets. The company is in the process of migrating some of its applications on the public cloud.

The Challenge

With over 800 stores and a complex IT infrastructure, the retailer's IT team had to deal with an array of problems:

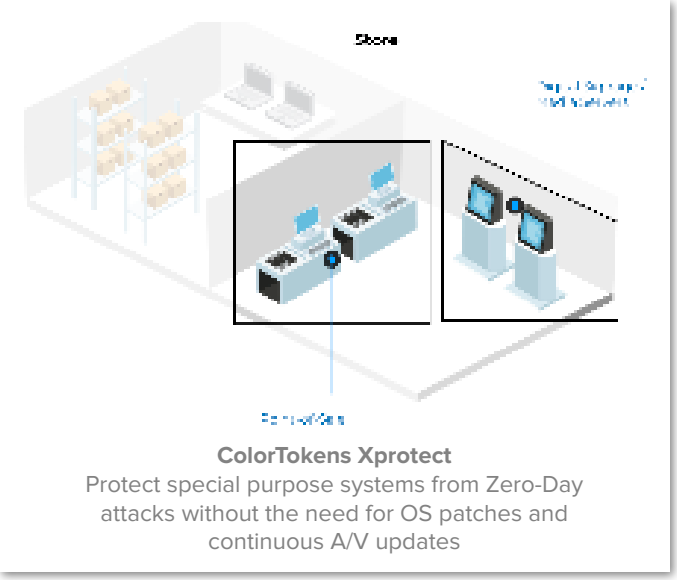
- Lack of application traffic visibility
- Identification of network misconfigurations (Policies, ACLs/VLANs)
- Micro-segmenting, implementing and modifying security policies across a physical and virtual environment
- Protecting low powered and legacy POS machines and servers (XP, embedded OS) from modern-day malware and APT lateral threats
- Achieving PCI compliance, auditing, and reporting

The ColorTokens Solution

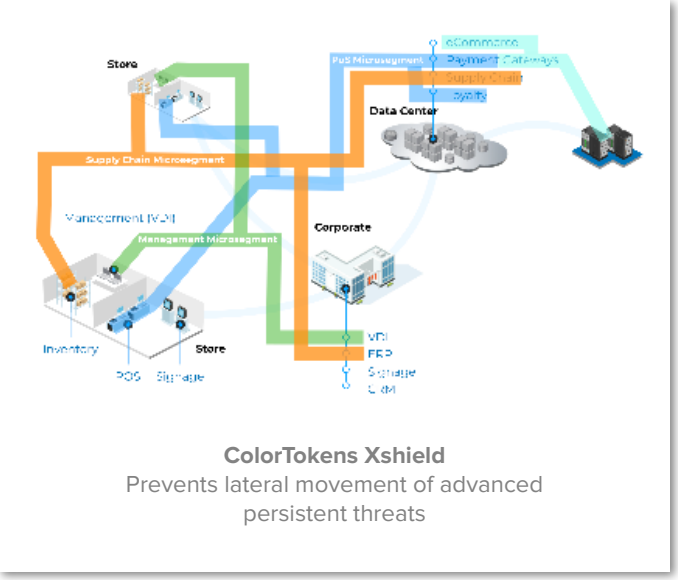
The fashion retailer had lost customer data in a breach that happened a few years ago. Despite significant investments of nearly a million dollars in leading advanced threat protection solutions, endpoint protection, and 25+ consultants, the security measures couldn't thwart modern malware that continued to show up at different locations periodically. The management immediately swung into action and started evaluating cybersecurity experts who can provide proactive defense in the real sense – without affecting business continuity.

ColorTokens, in consultation with the customer, employed a two-pronged approach to protect POS systems and critical data center assets.

- ColorTokens Xprotect was deployed on all endpoints to detect and prevent unwanted programs, including malware, from manifesting even if it existed on the machines. Xprotect's proactive security approach allowed the customer to lockdown endpoints and render them tamper-resistant against known and unknown threats, thereby ensuring complete protection and business continuity.
- ColorTokens Xtended ZeroTrust Security Platform was installed in the data center to visualize East-West traffic and implement zero-trust security to isolate retail applications. Visualization further helped in auditing flow data and adhering to compliance guidelines. Micro-segmenting the applications stopped malware propagation and prevented data exfiltration – achieving greater PCI compliance in the process.



ColorTokens Xprotect
Protect special purpose systems from Zero-Day attacks without the need for OS patches and continuous A/V updates



ColorTokens Xshield
Prevents lateral movement of advanced persistent threats

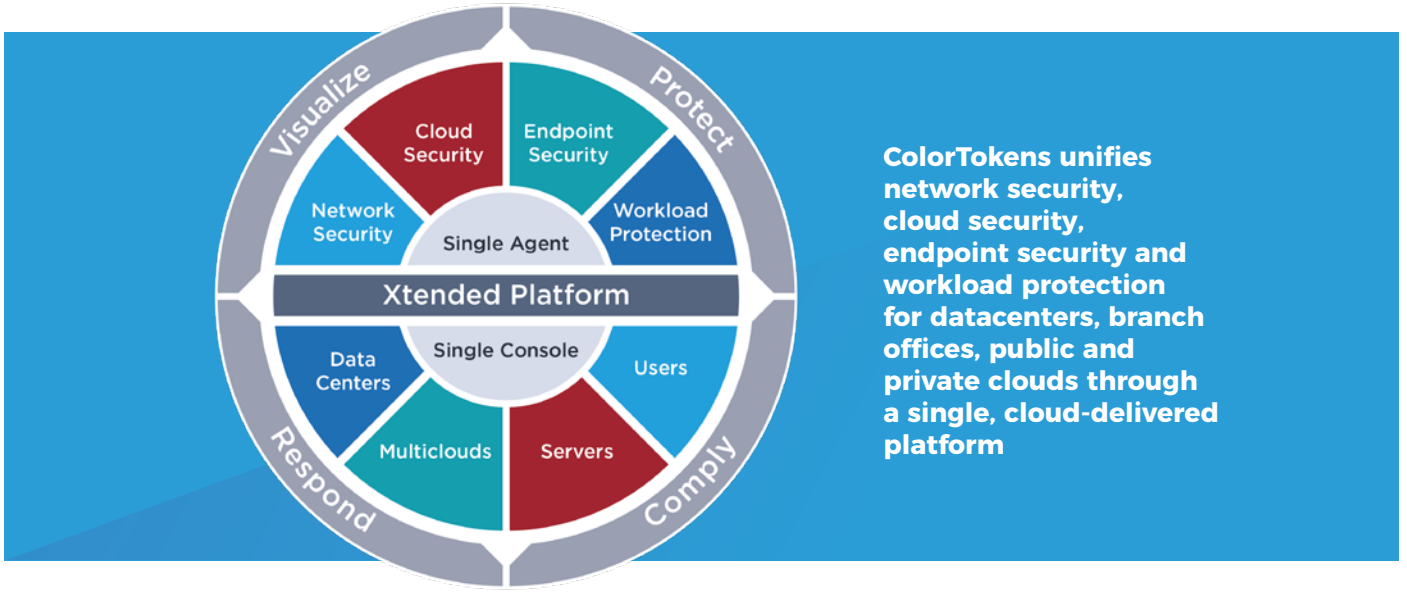
ColorTokens also provided 24x7 monitoring services for its products, a dedicated security consultant, incident – response and investigation, a management dashboard, and reporting.

Customer Benefits

- Single pane of glass for real-time visibility of cross-segment traffic and flow reports
- Visualization of misconfigured ports for faster debugging of applications
- Centralized control to define and enforce consistent security policies
- Reduced operational overhead with attribute-based policies and reusable policy templates
- Costs benefits; scope of the audit reduced through micro-segmentation
- Complete lockdown of POS and end-user machines – protection from malware, APTs, and POS attacks
- Simplified auditing & reporting to demonstrate PCI compliance

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