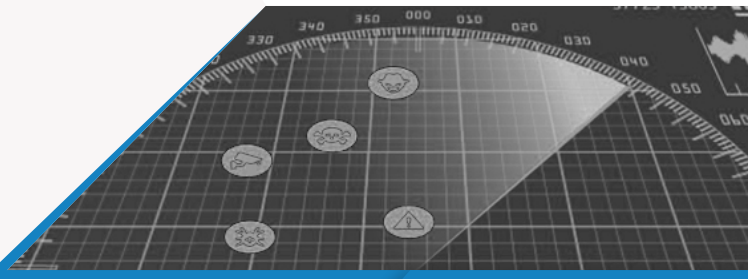
COLORTOKENS PROTECTS COMPEX BY PROVIDING COMPLETE VISIBLITY INTO UNDETECTED THREATS

COLORTOKENS



Case Study

Compex Legal Services, Inc., based in Torrance, CA, offers a variety of services to the legal, insurance and medical industries.

Compex provides record retrieval, deposition reporting, medical record summarization and multi-plaintiff litigation services. They have a wide geographical footprint in the US, with offices in Florida, Illinois, Washington and New Jersey, to name a few.

> "Fantastic visibility to my entire network. Helped save time and money as we found and plugged a perimeter firewall vulnerability, just in time before the external audit."
>
> **Tony Bazurto, SVP**

The Challenge

Compex's enterprise setup has about 200 servers and 350 clients, and is a flat network spanning 15 VLANs. The VLANs have no access control lists (ACLs) defined for the ingress and egress traffic through them. The workstation clients and servers have been segregated using VLANs. Since there are several public facing services provided by Compex, VLANs are used to separate these from the local area network. Compex uses a centralized data center architecture, with a mix of bare metal and virtual machines.

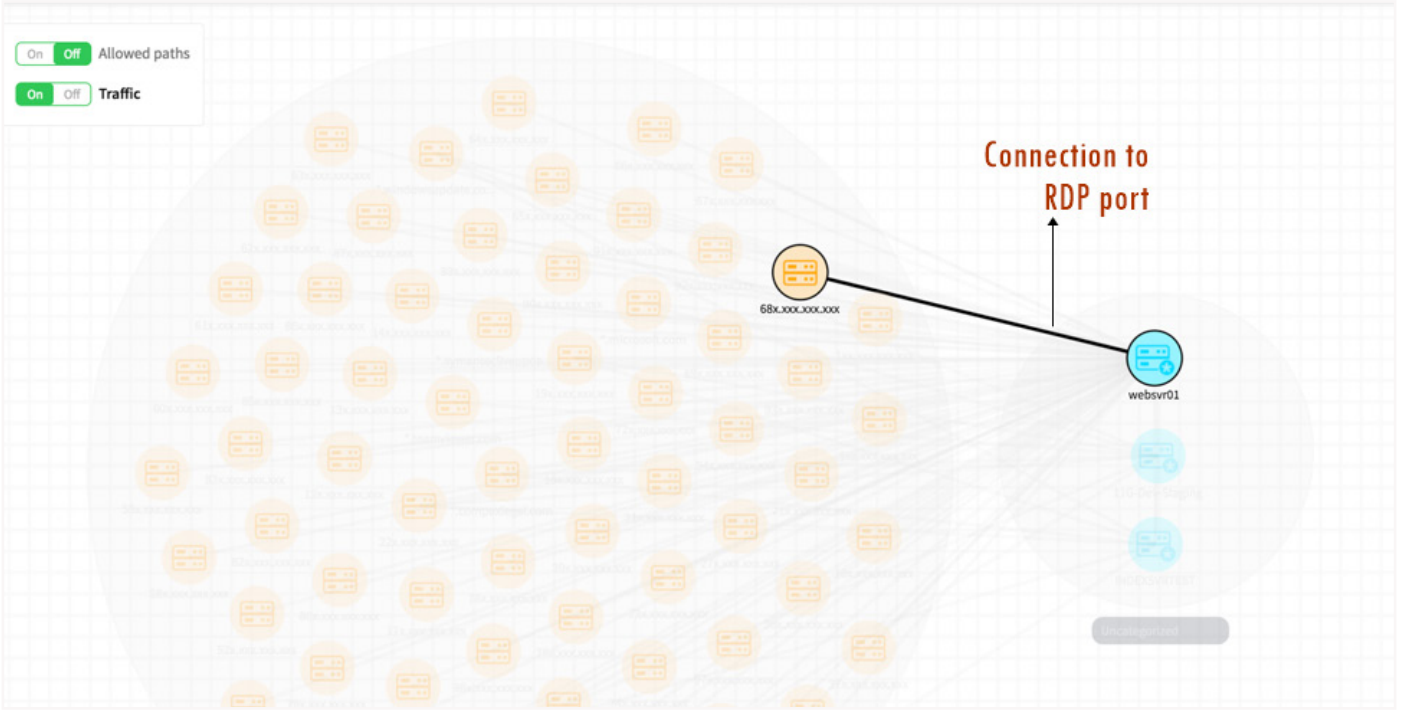
Since Compex deals with thousands of sensitive legal and medical documents, data security and compliance are of utmost importance, and that's a continuous challenge. Compex has deployed firewalls that provide intrusion prevention/detection systems (IPS/IDS) and Web filtering. Aware of the ever-increasing number of data breaches happening in enterprises around the world, Compex wanted to take a proactive approach in protecting their data center. They wanted to have complete security and compliance visibility for all workloads and users in their network, so that they can quickly identify and mitigate threats.

"With our expanding national footprint, we want to be absolutely sure that our customers can trust us with their documents." — says Bazurto

The Solution

Compex deployed Xshield for Workload Protection solution on its Web, app and database servers and started getting granular visibility on the network traffic. This extensive visibility provided Compex an overview of its security posture. ColorTokens' intuitive Web-based interface helped Compex drill into specific segments of its network, for a more thorough understanding of any suspicious network activity.

With ColorTokens Xshield, Compex was able to quickly identify an inbound connection to the RDP port, instead of the regular HTTP/HTTPS port – providing evidence of a reconnaissance attack on the Web server. Upon further investigation, this was traced back to a firewall misconfiguration and fixed immediately.



Compex's IT team immediately resolved the threat, just prior to an external audit -- saving time and money.

Further, Compex used ColorTokens to:

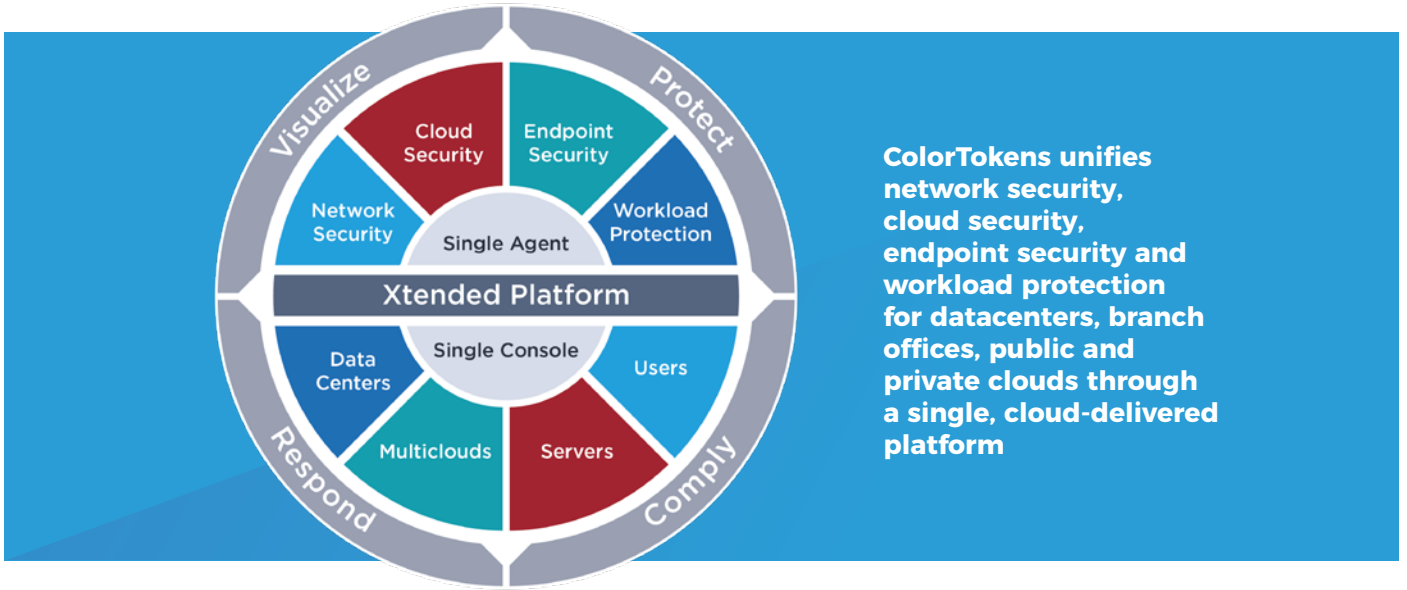
- Ensure there were no unauthorized connections to/from the public Internet to their servers/databases
- Identify where the traffic originates from for further security analysis
- Get instant visibility of connectivity between production and test environments

Key Benefits

- Instant visibility to cross-segment traffic
- Application-centric network views
- In-depth analysis of individual traffic segments to identify suspicious behavior
- Platform-independent software-defined security

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:



ColorTokens unifies network security, cloud security, endpoint security and workload protection for datacenters, branch offices, public and private clouds through a single, cloud-delivered platform

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