COLORTOKENS

CASE STUDY

Compex Legal Implements Proactive Security, Fights Cyberattacks with ColorTokens

Industry
Legal Services

Location
California, with offices throughout the United States

Key Challenges

- A lack of full visibility across the firm's office networks
- Constant pressure to meet compliance requirements and keep sensitive customer data safe
- The time-consuming task of updating a large number of firewall rules which increased potential to introduce errors
- IT assets that were vulnerable to unknown cyberattacks

Solution

Compex Legal selected ColorTokens to gain holistic visibility, secure critical IT assets through micro-segmentation, and protect endpoints from malware, ransomware, and zero-day attacks with easily configurable rules that enable proactive security.

Compex Legal Services, Inc., (Compex) 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.

Compex Legal uses a centralized data center architecture, with a mix of bare metal and virtual machines. 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) configured to filter ingress and egress traffic through them. The workstations and servers have been segregated using VLANs. Since there are several Internet facing services provided by Compex, VLANs are used to separate these from the local area network.

The Challenge

Since Compex Legal manages thousands of sensitive legal and medical documents, data security and compliance are of the utmost importance. The firm has deployed firewalls that provide intrusion prevention/detection systems (IPS/IDS) and web filtering.

In response to the increasingly sophisticated cyber threat landscape, Compex Legal sought a proactive approach to securing its datacenter assets from cybercriminals. The firm determined that identifying and mitigating threats in real-time would require holistic security and compliance visibility for all workloads and users in its network.

The Solution

Compex Legal selected ColorTokens' security platform for its award-winning visibility, Zero Trust micro-segmentation, and endpoint security. ColorTokens' security solution includes Xshield for workload protection and visibility and Xprotect for endpoint protection.

Compex Legal implemented Xshield on its web, application, and database servers. The firm leveraged Xshield's visualization capabilities to gain a comprehensive view of its security posture. Plus, ColorTokens' intuitive, web-

> "With ColorTokens, we have achieved rock-solid security of our internal network and endpoints, and we have been able to really streamline our audit process. The real-time visibility of current and historical traffic allowed the auditors to quickly certify us. Passing external security audits by our customers is very important to us, as we handle sensitive customer data."
>
> — Tony Bazurto, SVP

ColorTokens Solution Stack

- ColorTokens Xshield for Workload Visibility and Security
- ColorTokens Xprotect for Endpoint Protection

Business Benefits

- Gained holistic visibility into its entire network.
- Prevented credential theft by blocking hacking tools from executing on systems
- Blocked an unauthorized data exfiltration attempt to blacklisted geolocations
- Stopped 15+ malwares from executing
- Thwarted 30+ ransomware attack attempts on critical assets

> "With ColorTokens' solutions and security experts, we were able to see a cyberattack as it was happening and successfully prevented a breach. The fantastic visibility into our entire network helped save time and money. Just before an external compliance audit, we saw and plugged a firewall vulnerability which we never knew existed."
>
> — Tony Bazurto, SVP

based interface helped Compex Legal drill down into specific segments of its network and gain a more thorough understanding of any suspicious activity.

Immediately after deploying Xshield, the firm quickly discovered an inbound connection on the RDP port instead of the regular HTTP/HTTPS port – providing evidence of a reconnaissance attempt on the web server. Upon further investigation, Compex Legal determined that the inbound connection on the RDP port was allowed due to a misconfiguration on the perimeter firewall, which was fixed immediately without any data loss.

The firm deployed ColorTokens Xprotect on servers and endpoints to detect and prevent unwanted programs, including malware, ransomware, zero-day attacks, and other malicious code. Xprotect's proactive security approach enabled Compex Legal to lock down endpoints and render them tamper-resistant against known and unknown threats, thereby ensuring complete protection.

The firm also used ColorTokens Threat Hunting Services, which continuously monitored its networks for any anomalies. ColorTokens security experts helped the customer follow cybersecurity best practices by deploying Xprotect agents in enforcement mode and Xshield agents to define and enforce micro-segmentation policies on all critical assets.

In one particular instance, ColorTokens' security team discovered suspicious activities on a server that was running Xprotect in observe mode. Further investigation revealed traces of Mimikatz malware and attempts to move laterally within the environment. ColorTokens security experts proactively moved all pending servers to block mode. Xprotect successfully blocked an attempt to execute Mimikatz to recover Windows Service Accounts.

Results & Benefits

Just-in-time discovery of the attack by ColorTokens' security team, along with Xshield and Xprotect, saved the customer from losing sensitive data to a cyberattack. Plus, since Compex Legal was able to stop and remove the bad actor so quickly – right before an external compliance audit – the firm saved significant time and money.

Additionally, ColorTokens' solutions strengthened Compex Legal's existing perimeter controls by detecting and blocking unauthorized connections to/from the internet to servers/databases. As a result, Compex Legal has significantly reduced its attack surface, and the firm's security team has complete visibility into its security and compliance posture.

ColorTokens Inc., a leader in proactive security, provides a modern and new generation of security that empowers global enterprises to singlehandedly secure cloud workloads, dynamic applications, endpoints, and users. Through its award-winning cloud-delivered solution, ColorTokens enables security and compliance professionals to leverage real-time visibility, workload protection, endpoint protection, application security, and Zero Trust network access—all while seamlessly integrating with existing security tools. For more information, please visit www.colortokens.com

© 2020 ColorTokens. All rights reserved