COLORTOKENS

Critical Infrastructure Powered up, securely.

A leading electricity provider thwarts cyberattacks in real-time with ColorTokens' proactive cybersecurity services.

Industry: Electric Utility **Region**: Mexico

Overview

The organization is a leading provider of electricity for Mexico City's public lighting, covering approximately 18 million inhabitants. It operates 5 hydroelectric plants and also monitors water levels across major dams in Mexico using a critical infrastructure application.

The Challenge

Having their IT network infrastructure newly separated from its parent company, security stakeholders were looking for a solution to improve the organization's security posture and provide proactive protection against advanced attacks. Having possession of data records of major dams and hydroelectric plants in Mexico made the utility provider vulnerable to ransomware and cyberattacks. Stakeholders were concerned that a breach would go undetected, giving bad actors opportunities to access critical data and disrupt the functioning of dams and hydroelectric plants.

The critical infrastructure threat landscape in Mexico is getting increasingly hostile. A breach instance can have widespread consequences beyond financial and reputational loss, by potentially impacting the smooth functioning of civil society.

With its employees working remotely, the organization wanted a solution that offered comprehensive visibility into its network traffic, applications and potential blind spots, and defended against an unpredictable threat environment without disrupting its end users.

> “*In February 2021, ColorTokens alerted us about some network anomaly that they had detected. With the Xshield visualizer console, what we saw was unbelievable. We discovered in real time some 600+ malicious IPs trying to establish connections with our cloud applications. But thanks to the timely alert, we were able to block those connections and terminate the attack within 24 hours.*”
>
> IT specialist, Electric Utility Provider

The Solution

ColorTokens brought under its scope around 245+ critical assets and deployed its platform based on a foundation of Zero Trust architecture.

Xshield

Complete Visibility and Simplified Zero Trust Micro-Segmentation

ColorTokens Xshield is deployed on Azure, on-premise servers and endpoints to provide granular visibility into network traffic, application workloads, and endpoints – all managed through a single visualization console. Micro-segmentation policies based on a dynamic policy engine help to prevent lateral movement and reduce the attack surface.

Xprotect

Hardened Endpoint Protection

ColorTokens Xprotect delivers highly granular security controls to restrict unauthorized access to endpoints and enable dynamic whitelisting for endpoints in remote locations. Coupled with Xshield micro-segmentation, this proactive security approach helps to create a Zero Trust posture, where least privilege access is granted on role-based credentials, and not locations or specific hardware.

Xassure

24x7 Threat Hunting and Monitoring

ColorTokens Xassure leverages integrated dashboards, a knowledgebase of incidents, integrated threat intel feeds, the repository of IOC's (indicators of compromise) and threat detection rules to quickly alert on anomalies and/or suspicious traffic and processes.

Key Benefits

- **Potential savings of $1M** after successfully preventing execution of Emotet malware.
- **50% more visibility** into blind spots on company's network.
- **50% blast radius reduction** by protecting critical infrastructure monitoring application that monitors water levels across major dams in Mexico.
- **Intrusion attempts prevented** from suspicious geo locations such as China and Russia.
- **Suspicious network traffic** to internet domains **blocked** with the help of ZeroTrust policies.

Results and Customer Benefits

With ColorTokens' Xtended ZeroTrust™ Platform, Mexico's leading electricity provider implemented a proactive cybersecurity approach across their organization. But even with an elevated security posture, it did fall under the radar of threat actors.

In February 2021, intrusion attempts were made to penetrate inside its webserver environment hosted on Azure cloud through 600+ malicious IP addresses from suspicious geo locations such as China and Russia.

ColorTokens' threat monitoring team detected these network anomalies and sent security alerts related to brute force attempts and botnet connections. Using Xshield's Skyview visualizer console, security stakeholders gained a deeper understanding of the attack scenario in real time and successfully blocked those connections in less than 24 hours.

This led to **a potential savings of $1M** that the organization would have spent to eradicate the infection had it materialized.

In such challenging times when the threat landscape is evolving every day, the **organization realized rapid time-to-value with ColorTokens' solution set within 6 months** and is prepared to fight against advanced threat attempts proactively.

On 18th Feb'21

ColorTokens' threat monitoring team observed the network anomalies and sent alerts to the security team.

On 18th Feb'21

The secuirty team acknowledged the alerts and confirmed that they were under an ongoing attack.

On 19th Feb'21

The security team blocked all malicious IP addresses on the firewall.

Top Use Cases

- Comprehensive visibility into network traffic and blind spots.
- Proactive Endpoint protection for all end-user systems and remote workstations.
- Zero Trust implementation for critical dam applications.
- Protection against lateral movement, data exfiltration & ransomware.
- 24 x 7 threat hunting and monitoring.

Learn More

Solution at a Glance

- Xshield for visualization and micro-segmentation
- Xprotect for endpoint protection
- Xassure Essentials for continuous monitoring service

Learn More

Why ColorTokens

- Zero disruption to business operations, as there are no hardware or infrastructure dependencies.
- Platform-generated policy recommendations that reduce the security team's efforts and time.
- Real-time alerts and managed threat detection and response services with qualified insights.

Learn More

> *What ColorTokens offered us was the most comprehensive solution we have come across. Initially, we were worried that the Zero Trust implementation would need significant time and resources. But, ColorTokens alleviated those concerns and installed agents without any disruption to our end users.*

IT Planning and Control Manager, Electric Utility 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 Santa Clara, California; New York; London; Copenhagen, Denmark; and Bengaluru, India. For more information, please visit **www.colortokens.com.**