COLORTOKENS

SOLUTION BRIEF

ColorTokens Cybersecurity Solutions for Government Organizations

Government organizations continue to be a prime target for cyberthreats, hacktivists, state-sponsored cybercriminals, and others as they attempt to steal or manipulate valuable sensitive data. According to US Govt. Accountability Office (GOA), federal, state, and local governments were subjected to over 35,000 security incidents in 2017 alone.

One of the main challenges organizations face in managing cyber risk is lack of visibility into their north-south and east-west network traffic, and the inability to detect data exfiltration. According to Ponemon (2019 - Cost of a Data Breach Report), on average the public sector takes 324 days to identify and contain a breach. In the face of visibility gaps, Government and public sector agencies struggle to effectively secure their environment from cyberthreats. Adding to these challenges is the inability of traditional enterprise security tools to keep pace with advanced and highly targeted dynamic attacks such as ransomware that succeed by moving stealthily and laterally within the network. According to Ponemon's 2019 Data Breach Report, 56% of the public sector organizations use manual processes that are cumbersome, error prone and provide an easy path for attackers to gain entry.

In this dynamic threat landscape, federal, state, and local agencies have a pressing need to proactively protect their systems, the nation's critical infrastructure, and individuals' private data from cybercriminals.

ColorTokens Security Solution for Public Sector Organizations

ColorTokens delivers proactive security solutions for government and public sector organizations. Built to the NIST-ZTA (Zero Trust Architecture) standards, ColorTokens defends organizations from internal and external cyberthreats with real time visibility, application workload protection and endpoint security. ColorTokens partners with Winvale to provide proactive security for companies' business-critical assets and endpoints against cyberattacks. ColorTokens solutions are sold through Winvale's GSA Schedule GS-35F-0074S.

Deep visibility and Micro-segmentation of Critical Assets and Infrastructure

- ColorTokens Xshield delivers comprehensive visibility into network traffic across multi-cloud environments, identifying application dependencies, policy violations and gaps, and providing security teams with flow data statistics for incident response, reporting, and dashboarding.
- Xshield's deep visibility enables the fast and flexible creation of application segmentation (secure zones) with least privilege policies that reduce the attack surface and prevent lateral movement.

Highlights

- Gain deep visibility into application workloads, VMs, servers, and endpoints across your data center and cloud
- Reduce the attack surface with Zero Trust micro-segmentation of critical assets
- Prevent unauthorized software execution, even by privileged users
- Achieve faster compliance with Federal standards such as FISMA and NIST
- Protect fixed function, legacy and unpatched endpoint systems with Zero Trust default deny policies and lockdown
- Infrastructure agnostic, quickly deployed, with no business disruption

ColorTokens Solution for Government Organizations:

- Xshield for complete visibility and micro-segmentation
- Xprotect for endpoint security
- 24/7 managed breach prevention services for round-the-clock protection

- Helps to enforce compliance with cybersecurity regulations such as NIST by isolating and controlling all communication within, across, and to segmented resources.

Proactive Endpoint Security

- ColorTokens Xprotect proactively locks down and protects endpoints including laptops, servers, and lab computers from file-less attacks, ransomware, and other advanced malware
- This Zero Trust approach helps federal, state, and local agencies worry less about end-of-life legacy, unpatched and unsupported endpoints
- Avoids the need for frequent patch management, and expensive operating system refresh cycles
- Visualizes the chain of events and investigates threat behavior to lock down compromised systems and contain lateral threats
- Ultra light-weight, seamlessly co-exists with existing endpoint security tools to deliver comprehensive protection.

ColorTokens Zero Trust Security Platform

The ColorTokens Xtended ZeroTrust™ Platform is 100% cloud-delivered for fast time to value, enables granular visibility, security and control over endpoints, applications and network assets to vastly reduce the attack surface and prevent breaches. Customers benefit from increased cyber resilience to attacks, rapid containment, and minimized business disruption or downtime.

Xshield

Xshield provides comprehensive visibility and protection for critical network assets, workloads and applications distributed across data center and hybrid/multi-cloud environments. A software-defined micro-segmentation solution for internal networks, Xshield prevents lateral movement and the spread of breaches by creating Zero Trust Secure Zones™ (micro-perimeters) around network assets such as workloads/applications. It blocks unauthorized communications between assets, enforces least privilege access policies, and effectively prevents malware propagation and insider threats.

Xprotect

Xprotect provides an enhanced layer of security for endpoints with application whitelisting and USB device control. Transparent to end users, the ultra light weight agent allows only legitimate applications to execute while blocking all unauthorized processes. This delivers a Zero Trust based approach that goes beyond traditional endpoint security to protect business-critical endpoints including POS, fixed and unpatched systems, from malicious access and advanced threats such as ransomware.

ColorTokens Breach Prevention Services

Breach services are fully managed, threat prevention and remediation services for businesses of all sizes. We deploy and manage Zero Trust security in the network.

START FREE TRIAL NOW

or send your query to
info@colortokens.com

> The Winvale and ColorTokens partnership brings the power of Micro-Segmentation Security to the federal and defense markets where cyber security is an ever-evolving issue from the end-user to the Pentagon, and even the highest levels of the government branches. With average cost of data breaches exceeding more than $3.9 million, government Chief Information Officers and cyber leaders can leverage the capabilities of ColorTokens and the expertise of Winvale to significantly reduce surface attacks as well as prevent threats from cyber attackers within their network environments."
>
> **– Jeff Vittone, President, Winvale**