

# ColorTokens Cybersecurity Solutions for Government Organizations

Government organizations continue to be a prime target for cyberthreats, hackers, 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

- a 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.
- a 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

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

### ColorTokens Solution for Government Organizations:

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

