

Be Breach Ready



Increase network resilience to maintain information superiority despite cyberattacks.

Network-centric warfare is a force multiplier, which provides an asymmetric information advantage by making data more readily available and usable, enabling the sensor-to-shooter kill chain.

However, these powerful capabilities open a new attack surface for adversaries to exploit. To ensure that critical mission systems and network assets are protected, ColorTokens assists our DoD clients in implementing cutting-edge cybersecurity measures that use zero trust security principles, as mandated in the DoD Zero Trust Strategy^[1] and the Execution Roadmap targeting 2027^[2]. Our solution allows you to segment, isolate and logically control granular traffic accessing network resources. This ensures that critical systems have the resilience needed to continue the mission, even in the face of a successful breach of the perimeter defenses.

[1] <https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>

[2] <https://dodcio.defense.gov/Portals/0/Documents/Library/ZTCapabilityExecutionRoadmap.pdf>

The Xshield Enterprise Microsegmentation Platform

Xshield, ColorTokens' flagship product, protects the digital battlespace by stopping the spread of malware from a network breach while allowing mission information systems to continue to operate. Xshield provides traffic visibility within the diverse network landscape and establishes micro-perimeters around critical network resources. It enforces zero trust policies on every server and endpoint to stop illicit traffic from an initial compromise. Even if the perimeter network defenses are penetrated, Xshield's microsegmentation prevents the spread of an attack laterally across the network.



Visualize

Assets & network flows



Protect

Critical systems & data

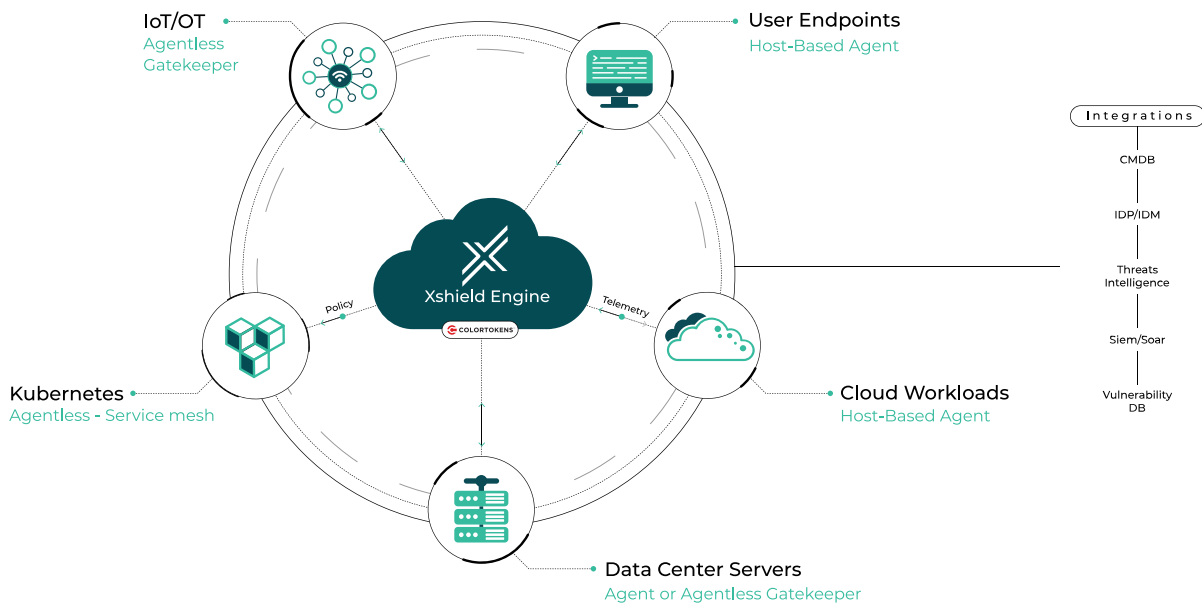


Measure

Attack surface & blast radius



ColorTokens offers a containerized microsegmentation engine that can be deployed in a secure cloud environment or data center using Kubernetes. It provides a unified policy decision point that enforces zero trust policy for all asset types, using both agent-based and agentless policy enforcement. With Xshield, you have a single-pane-of-glass approach to protect your hybrid network topology, covering data center servers, cloud workloads, user endpoints, containerized Kubernetes applications, Internet-of-Things devices, and Operational Technology (OT) networks. It also enforces zero trust policies for legacy applications and operating systems such as Windows 2003 and HP-UX. This unified approach is superior to separate point solutions for different types of assets because it is simpler, easier to administer, and more complete.



Procurement Vehicles

SBIR Phase 2 Contract: Zero Trust Security for IT Systems and OT: FA864924P0427
Topic No. AFX244-DPCSO1

UEI: CFMHTXGXLSE1 | DUNS: 079893358 | CAGE: 7JG33

A Leader in Cyber Innovation

Founded in 2015, ColorTokens is an innovator in cybersecurity. Headquartered in San Jose, CA, the company has over 20 patents and a diverse customer base in both the private sector and government. **E-mail us at fedbusiness@ColorTokens.com.** For more information, please go to: www.ColorTokens.com

