Be Breach Ready

COLORTOKENS™

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 Strategy1 and the Execution Roadmap targeting 2027. 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] DoD Zero Trust Capability Execution Road#map (COA 1)

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

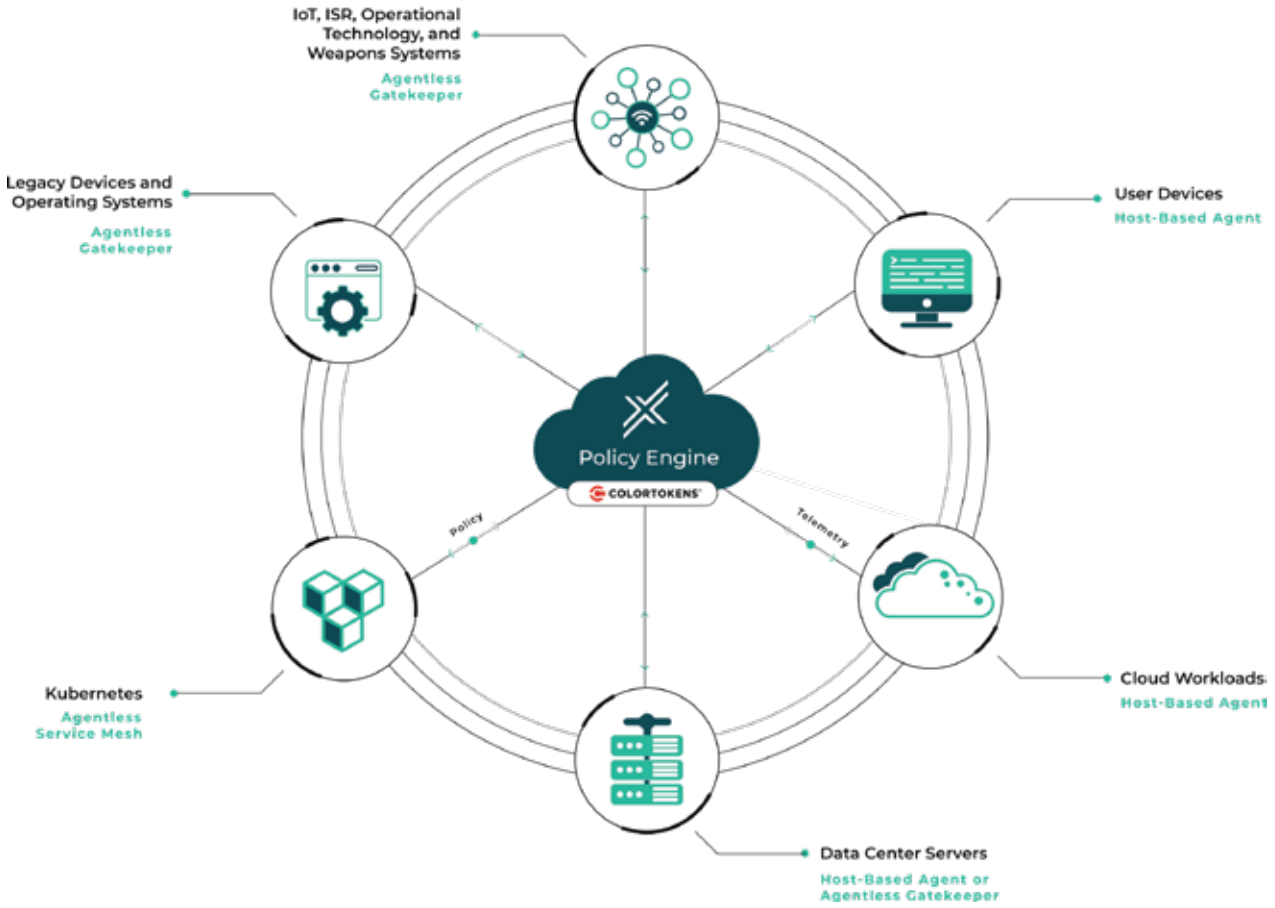
Protect
Critical systems & data

43
MEDIUM

Measure
Attack surface & blast radius

Xshield stops the lateral movement of an attack that has breached the network's perimeter defenses before it can significantly degrade operations or compromise sensitive data. First, it establishes granular micro-perimeters around hosts and devices. Then, it enforces zero trust communications policies that stop the spread of malware while allowing valid processes to proceed. Xshield increases your cyber resilience so digital operations can continue to support the mission, despite a cyberattack. Using Xshield's comprehensive, centralized management interface, administrators can visualize all assets and the traffic between them and define zero trust traffic policies to stop the lateral movement of an attack. Xshield uses both agent-based and agentless policy enforcement points as appropriate for different types of network assets and devices: data center servers, containers, cloud workloads, user endpoints, as well as ISR platforms, weapons systems, IoT and operational technology devices.

To empower a comprehensive strategy for zero-trust architecture, Xshield has out-of-the-box integrations with best-of-breed cybersecurity solutions in the categories of Identity Management, Configuration Management Databases, Zero Trust Network Access, Endpoint Detection and Response, SIEM, and others. In addition, Xshield leverages standards-based APIs and SDKs to ease integration with any enterprise architecture



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**

2025 GLOBEE AWARDS GOLD WINNER CYBERSECURITY
2025 GLOBEE AWARDS SILVER WINNER CYBERSECURITY
ShortList 2025
FORRESTER WAVE LEADER 2024 Microsegmentation Solutions
GIGAOM RADAR REPORT 2024