COLORTOKENS

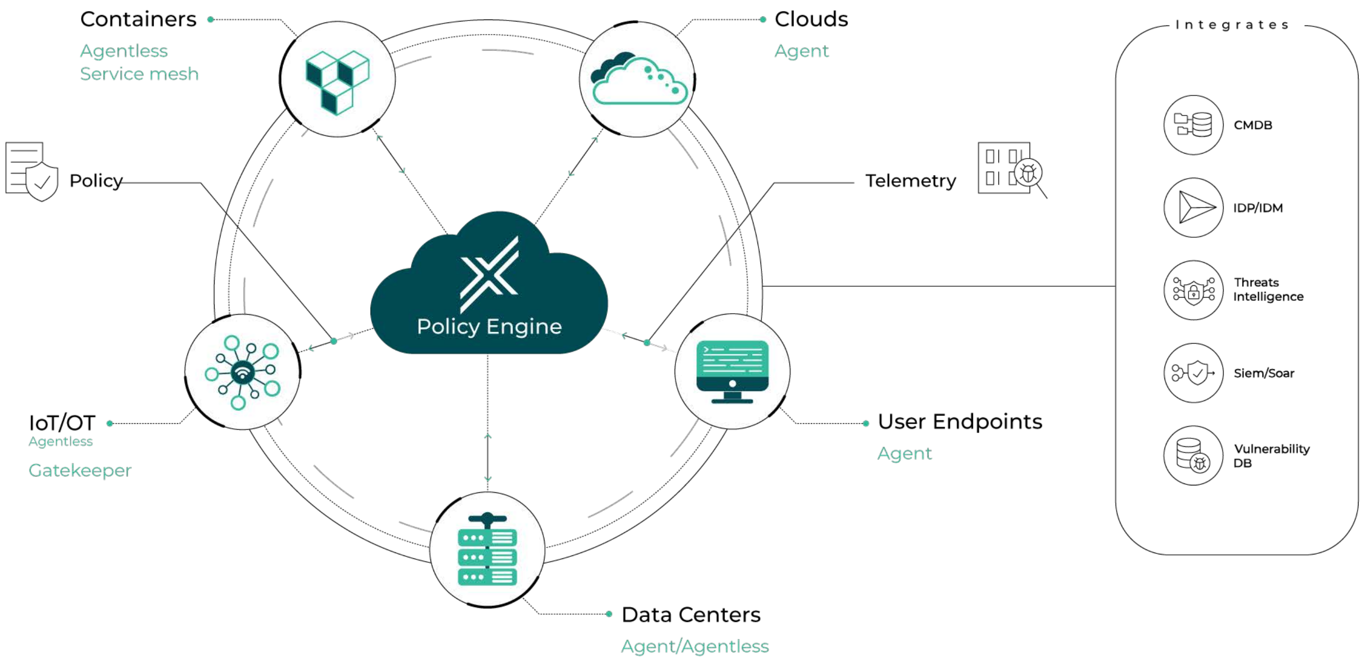
SOLUTION BRIEF

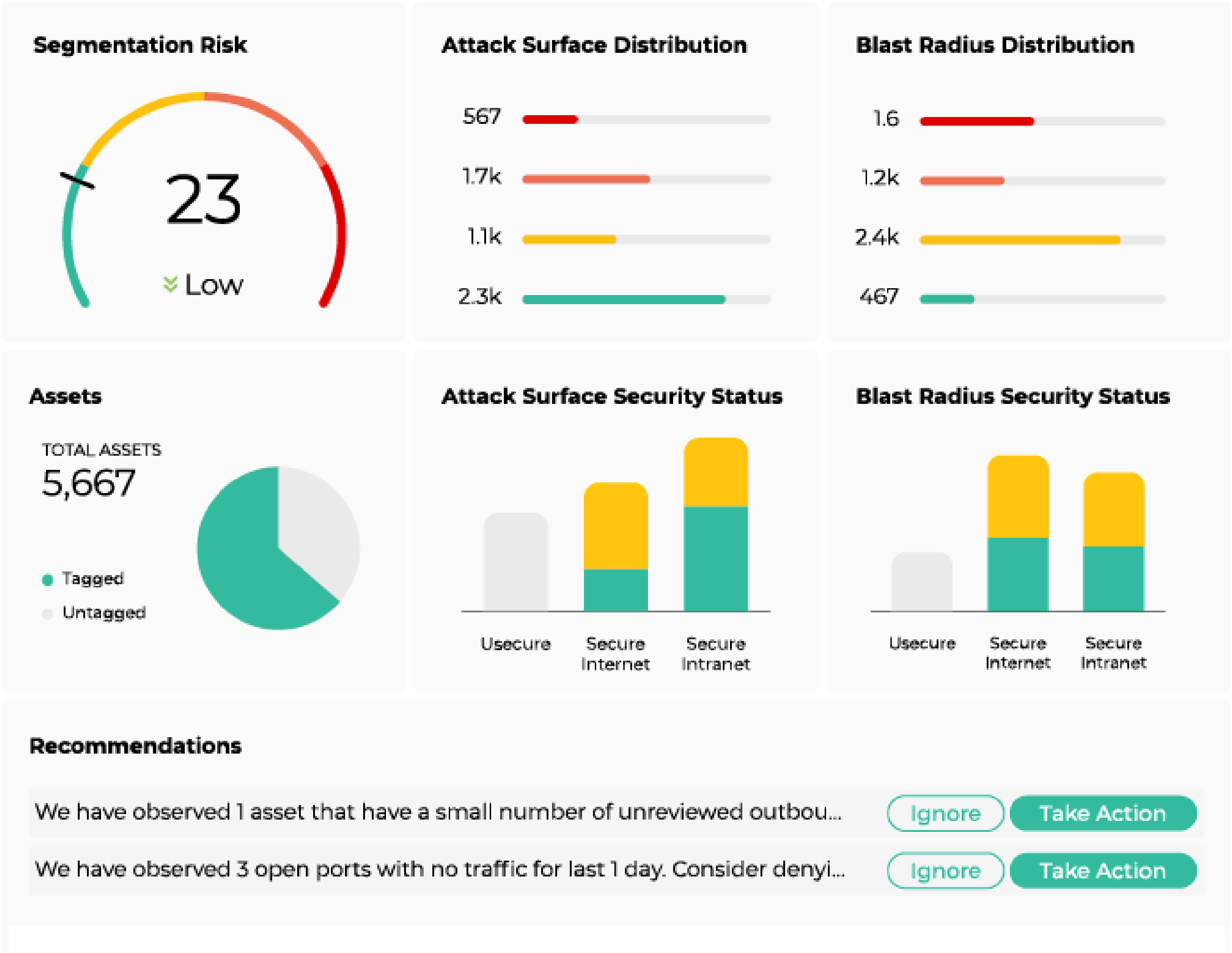
Xshield Enterprise Microsegmentation Platform

For most enterprises, a breach of their network defenses is a matter of when, not if. Cybersecurity strategies such as anti-virus and perimeter firewalls are prudent and necessary. But no matter the type of attack, all the recently reported breaches have one thing in common: they penetrated the defenses. CISOs, CIOs, Risk Officers, and IT managers want to make their company's information systems resilient so they can continue their critical business processes and protect their precious data—even in the face of a successful attack. They need to be breach-ready.

Microsegmentation prevents malware and ransomware from spreading by stopping unauthorized lateral traffic between network resources—preventing catastrophic damage. As a defense-in-depth strategy, it goes beyond perimeter firewalls, VLAN segmentation, and anti-virus solutions by enforcing micro-perimeters around all resources, applications, and endpoints. It's a foundational part of **zero-trust security.**

With Xshield, you can visualize a map of all your network assets, applications, and their dependencies, and then set up traffic policies to protect them. It lets you manage multiple policy enforcement points, **both agent-based and agentless,** from one central console, decreasing complexity and saving on training and staffing. Xshield protects all possible points of breach, so there are no soft spots in your proactive cyber defense: data center servers, cloud workloads, Kubernetes containers, user endpoints, OT & IoT devices, and even legacy OS devices.





We have observed 1 asset that have a small number of unreviewed outbou...

We have observed 3 open ports with no traffic for last 1 day. Consider denyi...

Xshield uses an innovative approach to microsegmentation implementation: it immediately improves your security posture by giving you enterprise-wide control of risky ports and sensitive or privileged flows. This lets you show a quick return on investment for your security initiative, in mere hours after installation. Then it progresses to continuous improvement with fine-grained application-specific zero-trust controls. It lets you measure your risk and security posture through dashboard reports so you can communicate the improvements to your stakeholders

The Xshield Difference

Comprehensive microsegmentation

Xshield is the only microsegmentation platform with complete coverage so there are no soft spots in your defense. It protects data center servers, cloud workloads, user endpoints, Kubernetes containers, OT/IoT, and even legacy OS devices with both agent-based and agentless traffic policy enforcement. The unified administrator experience reduces complexity and saves on training and staffing.

Immediate security benefits and continuous improvement

Quick-start your security initiative and build consensus with an innovative approach that immediately improves your security by giving you enterprise-wide controls privileged and sensitive flows, then progresses to continuous improvement with application-specific zero-trust controls.

Visualize and communicate risk measurements

Xshield's dashboards and reports let you see your security gains over time and communicate them to your stakeholders, measured by business risk, attack surface, and blast radius.

Actionable visibility of your enterprise landscape

The Xshield visualizer gives you a global, panoptic view across your network landscape, empowering administrators to analyze their assets and applications using multiple attributes and dimensions so they can create more precise and secure controls.

Capabilities

- Visualize your network assets, applications, and dependencies with multi-dimensional flexibility, uncovering misconfigurations that expose you to risk.
- Use a single-pane-of-glass approach to administer microsegmentation for all possible points of breach: data center servers, cloud workloads, user endpoints, Kubernetes containers, OT/IoT devices, and even legacy OS devices.
- Centrally control multiple policy enforcement points for all types of resources: the hundreds (or thousands) of host-based OS firewalls in your environment, Kubernetes service mesh sidecar proxies for containerized applications, and the Xshield Gateway for IoT, OT, legacy OS devices, or wherever agentless enforcement is preferred.
- Immediately increase your security posture with enterprise-wide controls on high-risk ports and sensitive flows—and progress to continuous security improvement with fine-grained application-specific controls.
- Use risk-scoring dashboards so you can report progress to your C-suite, line-of-business leaders, the Board of Directors, and regulatory oversight.
- Use Xshield’s non-disruptive workflow for implementing microsegmentation. It separates policy authoring from policy push and lets you simulate policies on historical data before enforcement.
- Leverage automated templates so you can define traffic policies to instantly shut down the spread of malware in the event of a breach.

About ColorTokens

ColorTokens is a leader in delivering innovative and award-winning cyber security solutions. It is a US corporation headquartered in Silicon Valley with offices in the US, the UK, Europe, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please go to colortokens.com