COLORTOKENS

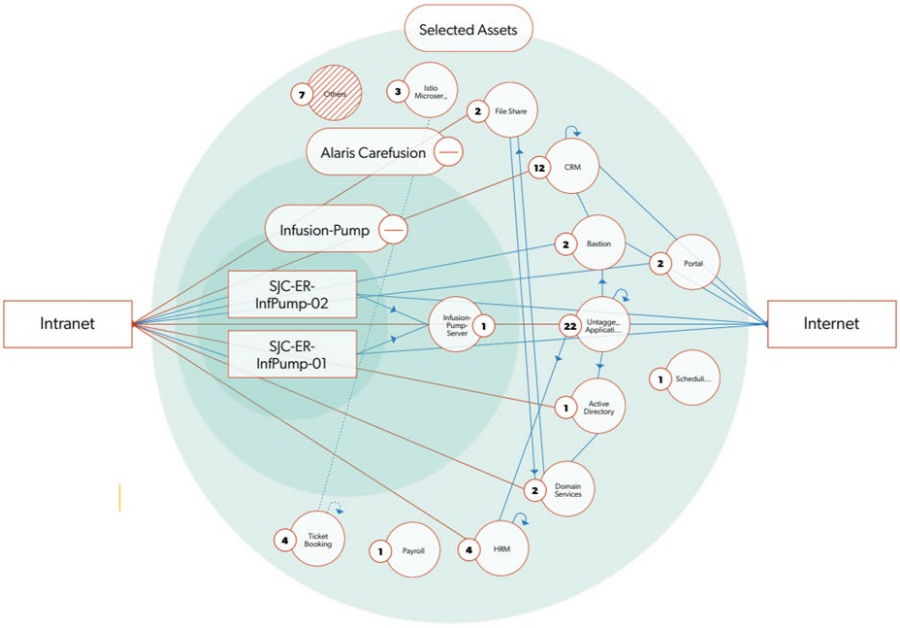
Data Sheet

The Xshield Enterprise Microsegmentation Platform™

Xshield addresses a fundamental challenge in cybersecurity today: despite extensive investments in perimeter defenses (such as firewalls, network access controls, IAM, VPNs, ZTNA, and SASE), breaches continue to occur, resulting in significant financial and operational damage. This is because, in the realm of cybersecurity, the defender must be right every time; the attacker only needs to be right once to gain an initial breach.

After the initial compromise, hackers use lateral movement to spread through the enterprise until they locate important assets and resources. Then they steal sensitive data, degrade digital operations, or encrypt critical systems for ransom. That's where Xshield comes in: it stops lateral movement attacks by enforcing zero-trust policies, preventing a breach from becoming a business crisis. Xshield makes your enterprise Breach Ready.

Xshield visualizes network assets, applications, traffic flows, and dependencies in an intuitive, interactive map. Traffic lines are color-coded to distinguish in-policy (allowed) from out-of-policy (unauthorized) communications, with clickable details for deeper inspection. Views are customizable across up to 20 dimensions (e.g., location, application, business criticality, role-based), enabling tailored perspectives for security, infrastructure, application, and executive teams.



Key Benefits

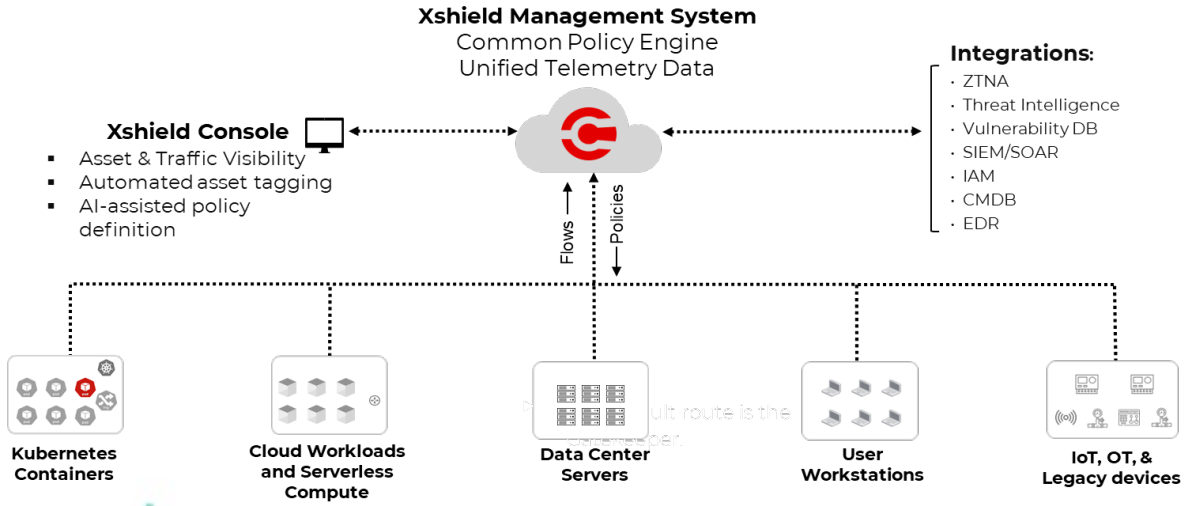
- Stops lateral movement attacks while permitting legitimate business processes.
- Breaks the kill chain of ransomware and malware attacks
- Provides actionable visibility and risk measurement for proactive security posture improvement.
- Enables organizations to go beyond breach prevention to become "breach-ready."
- Reduces administrative complexity, training needs, costs, and policy errors via unified management and AI-assisted policy definition.

Supported Environments and Enforcement

Xshield delivers pervasive Zero Trust protection across diverse, hybrid infrastructures using a single-pane-of-glass SaaS-based administration console for centralized policy configuration, management, and enforcement.

Supported asset types include:

- Data center servers and VMs (Linux, Windows)
- Cloud workloads (multi-cloud and hybrid)
- Kubernetes containers
- User endpoints (Windows, macOS, legacy OS)
- Internet-of-Things (IoT) devices
- Operational Technology (OT) / Cyber-Physical Systems / Industrial Controls / IoMT
- Legacy OS devices and systems



Enforcement approaches:

- **Agent-based**: Lightweight agents configure host-based OS firewalls (e.g., for servers, endpoints). Uses the Xshield agent, **or existing EDR agents** already deployed (e.g., CrowdStrike, SentinelOne, MDE)
- **Agentless**: Suitable for environments where agents are impractical (e.g., OT/IoT, legacy Windows, HP-UX, AIX, mainframes) via the Xshield Gatekeeper appliance.
- **Native Controls**: visualizes and enforces agentlessly using native controls for cloud workloads and serverless compute (e.g., Azure NSGs, AWS SGs) and integrates with Kubernetes service meshes' Open Policy Agent (e.g., Istio Envoy, Ambient Mesh, and OpenShift) to protect containerized microservices applications.

This hybrid model ensures comprehensive coverage without gaps—if the "fence" isn't continuous, threats can bypass defenses.

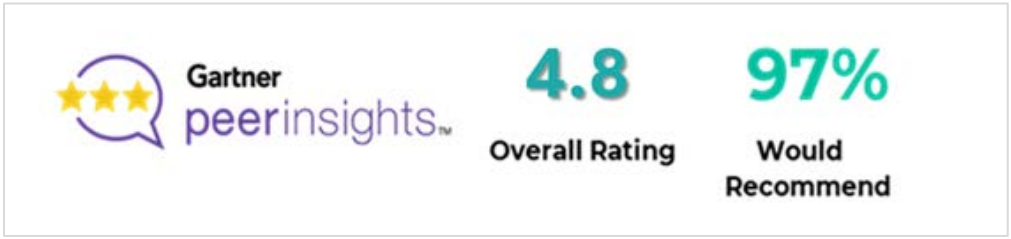
Core Capabilities

- **Visualization and Mapping**: Real-time, multi-dimensional views of assets, interdependencies, and traffic; risk dashboards and reports.
- **Policy Enforcement**: Granular micro-perimeters (Zero Trust policies) to isolate critical assets, contain breaches, and enable swift response.
- **Policy Management Features**: AI-enabled environment interrogation and policy recommendation, simulation on historical data before enforcement, progressive enforcement for faster time-to-value.
- **Integrations**: Out-of-the-box connectors with threat intelligence, vulnerability databases, IAM, SIEM, EDR (e.g., CrowdStrike Falcon, SentinelOne), ZTNA (e.g., Netskope, Appgate), CMDB, and more for unified Zero Trust architecture.
- **Deployment and Scalability**: Cloud-powered, platform-agnostic, rapid deployment (weeks vs. months), no hardware dependencies for many scenarios, scalable across environments.

Recognition and Leadership

Named a **Leader** in the Forrester Wave™: Microsegmentation Solutions, Q3 2024, with top scores in multiple criteria, including OT/IoT security, visibility, and product vision.

High ratings in industry reports (e.g., perfect 5.0 in key features comparisons) and strong user feedback (e.g., 4.8/5 on Gartner Peer Insights).



About ColorTokens

ColorTokens is a premier provider of enterprise microsegmentation solutions, dedicated to making organizations "breach-ready" by preventing the lateral spread of ransomware and advanced malware. The innovative Xshield™ platform protects complex IT, OT, IoT, and cloud infrastructures through granular micro-perimeters, asset isolation, and effective incident response.

For more information, visit www.colortokens.com.