COLORTOKENS™

SOLUTION BRIEF

Xshield

Enterprise Microsegmentation Platform

Be Breach Ready

Breaches Happen. Are You Prepared?

Security breaches are no longer a question of if, but when. Even organizations with mature security programs and extensive perimeter defense solutions experience compromises. Key to maintaining resilience during a breach is speed—the ability to contain and prevent the spread of a breach fast before it disrupts the business.

Being Breach Ready means proactively strengthening your security posture to withstand an inevitable breach—putting the right controls in place to limit blast radius, contain incidents quickly, and sustain critical operations even after initial compromise. By stopping unauthorized lateral movement—the primary path from minor intrusion to major crisis—organizations can minimize operational disruption, reduce ransom risk, and mitigate reputational damage and loss of customer confidence caused by data loss.

ColorTokens' Xshield Enterprise Microsegmentation Platform™ is purpose-built to deliver breach readiness. Xshield provides the fastest path to effective microsegmentation, helping organizations achieve measurable risk reduction by reducing attack surface and blast radius by up to 90% in under 90 days. The result is stronger cyber resilience: faster containment, reduced impact, and confidence that when a breach happens, it stays contained.

Xshield for Speed at Every Stage of Breach Readiness

Speed is critical to breach readiness across every attack phase—before, during, and after a breach.

- **Before a breach:** Deploy defenses quickly and strengthen posture in advance.
- **During a breach:** Contain the spread immediately and maintain business continuity.
- **After a breach:** Minimize impact and restore normal operations rapidly.

Xshield is engineered to deliver all three—without long design cycles, architectural changes, or operational disruption.

Speed Before a Breach: Deploy Enterprise-Scale Microsegmentation Fast

Xshield accelerates microsegmentation by adapting to your existing architecture—without requiring re-platforming or disruptive redesign.

From a single, pervasive platform, Xshield delivers Zero Trust microsegmentation across IT, OT, IoT, cloud, data centers, containers, endpoints, and legacy systems. It gives organizations the flexibility to apply the most effective enforcement method for each environment, whether through lightweight host agents, existing EDR agents, Kubernetes service-mesh controls, cloud-native constructs, or the Xshield Gatekeeper for agentless OT and IoT.

To eliminate slow, application-by-application policy design, Xshield enables Progressive Policy Enforcement—rapidly restricting the most exploited attack paths and privileged management ports first, while refining granular controls over time.

The result is pervasive, flexible, and progressive enforcement that removes deployment bottlenecks, closes security gaps, and strengthens breach readiness—reducing attack surface and blast radius by up to 90% in under 90 days.

Speed During a Breach: Immediate Containment to Prevent Escalation

When a breach is detected, minutes determine whether it remains an incident or becomes a crisis.

Xshield enables immediate containment through emergency policy templates triggered automatically by signals from your SIEM or detection platforms. These controls instantly restrict unauthorized lateral movement and isolate affected systems, stopping the spread before it reaches critical assets.

Unlike broad shutdown approaches, Xshield applies targeted isolation to ensure minimum viable business operations continue running while the threat is contained.

AI-assisted guidance strengthens this response by correlating observed activity with the latest MITRE lateral movement attack techniques and CISA threat advisories, identifying likely propagation paths, and recommending the fastest containment actions, enabling teams to act with speed and confidence under pressure.

The outcome: rapid containment, protected operations, and an incident that never escalates into business disruption.

Speed After a Breach: Restore Operations Without Re-Exposing Risk

True resilience is measured not just by containment, but by how quickly the business can recover.

Xshield supports faster recovery by enabling precise, targeted isolation instead of broad shutdowns. Critical systems can remain operational where possible, and connectivity can be restored in a controlled, policy-driven manner, while strengthening controls to prevent similar attack paths from being exploited again.

With consistent enforcement and a proactively hardened security posture, organizations return to normal operations with confidence—minimizing downtime, reducing operational impact, and sustaining breach-ready controls.

Measurable Risk Reduction With Breach Readiness

Speed in microsegmentation translates directly into business impact. By containing lateral movement attacks early, Xshield helps organizations limit the impact of a breach and reduce its operational, financial, and regulatory consequences.

Organizations using Xshield can:

- **Reduce mean time to contain (MTTC)** a breach from days to seconds by isolating compromised systems before attackers can move laterally.
- **Protect business continuity** by preventing breaches from spreading to mission-critical applications, OT environments, and production systems.
- **Reduce post-breach legal, recovery, and notification costs** by minimizing the number of affected systems and data exposures.
- **Improve audit posture and accelerate compliance cycles** by enforcing and demonstrating consistent Zero Trust controls across the enterprise.

Be Breach Ready With Xshield

Breach readiness demands three things - speed, containment, and coverage everywhere attackers move.

Organizations must be able to restrict unauthorized lateral movement fast and do so without long design cycles or operational disruption. Anything slower turns a breach into a crisis.

Xshield delivers enterprise-wide microsegmentation fast, contains breaches in real time, and continuously adapts to evolving attack techniques—so security teams can reduce risk quickly and consistently.

The result is simple and lasting: breaches don't spread, operations keep running, and risk is measurably lower.

That is what it truly means to be Breach Ready.

Contact us to discover how we can help you achieve breach readiness.

About ColorTokens:

ColorTokens is a leading provider of enterprise microsegmentation and breach containment solutions, dedicated to making organizations "breach ready." By preventing the lateral spread of ransomware and advanced malware, ColorTokens protects complex network infrastructures through its innovative Xshield™ platform. The platform visualizes traffic between workloads, OT/IoT/IoMT devices, and users, enabling the enforcement of granular micro-perimeters, swift isolation of critical assets, and effective breach response. Recognized as a Leader in the Forrester Wave™: Microsegmentation Solutions (Q3 2024), ColorTokens delivers proactive security that prevents disruptions and safeguards global enterprises. For more information, visit www.colortokens.com.