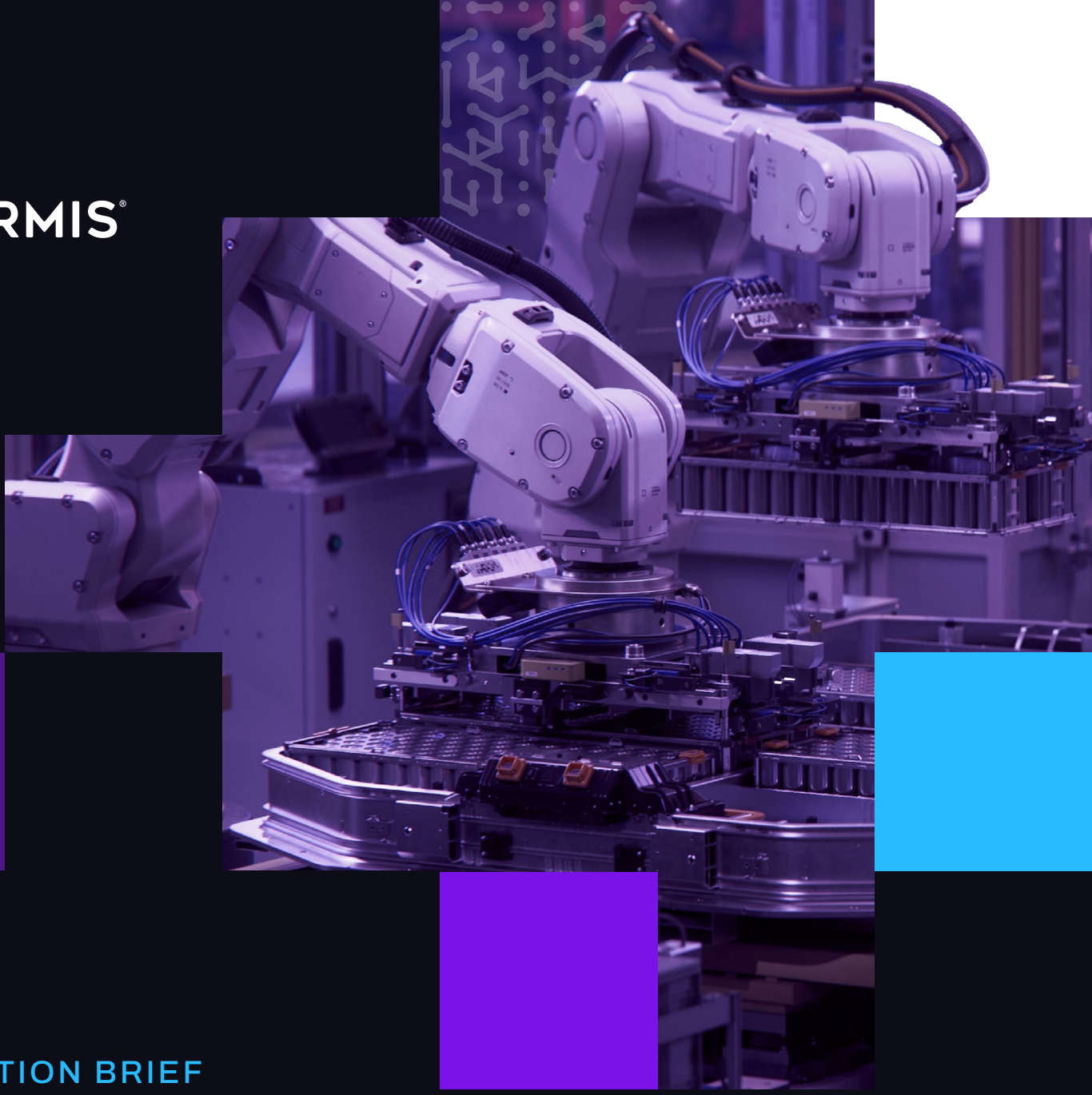
ARMIS®



SOLUTION BRIEF

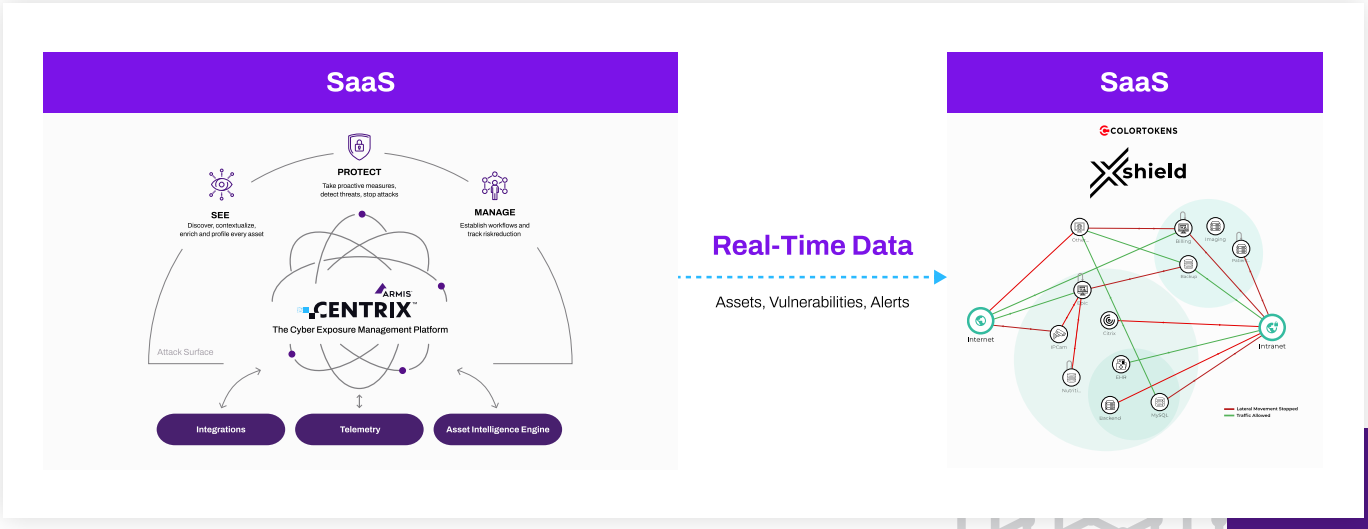
Secure Your OT/IoT Environments with Precision: with ColorTokens and Armis

Prevent Lateral Movement of Cyberattacks with Rich Asset Inventory, Prioritized Vulnerability Management, Compensating Controls & Microsegmentation

Cybersecurity in OT environments is inherently difficult due to unpatched legacy systems and OT/IoT devices that don't support traditional security agents. The convergence of IT and OT adds complexity by expanding the attack surface, increasing interconnectivity, and blurring security boundaries, thus making it harder to detect and contain threats.

As is shown in the many news stories about high profile breaches, enterprise security leaders today must assume that breaches are inevitable and be prepared to survive them. While many enterprises today deploy perimeter defenses such as firewalls, identity management, and endpoint detection, these tools are primarily focused on breach prevention. However, initial network access by the attacker is just the beginning. Once inside, they must move laterally across networks to reach their target systems, escalating privileges and access. In converged IT/OT environments, this movement may go undetected until it's too late. If they can reach their target systems, they can disrupt, steal, or encrypt sensitive data for ransom, and compromise operations. Enterprises must prevent lateral movement to disrupt the kill chain by not just focusing on prevention, but also on **containment and resilience**, to be breach ready.

ColorTokens and Armis deliver a complementary, integrated solution that brings together best-in-class microsegmentation, asset identification, comprehensive asset intelligence, and vulnerability management and microsegmentation and microsegmentation that empowers enterprises with a Zero Trust Architecture purpose-built for converged IT/OT environments.



Key Challenges in Securing OT/IoT Environments

1. **Legacy and Agentless Systems -** Many OT/IoT devices can't support traditional security agents, leaving them exposed.
2. **Expanded Attack Surface -** Converged IT/OT networks introduce complexity and more pathways for adversaries to exploit.
3. **Lateral Movement -** Once inside the network, attackers often move laterally undetected, seeking high-value systems or causing operational disruption.
4. **Limited Visibility -** Many organizations struggle to gain full visibility and situational awareness into all assets, especially unmanaged or unauthorized devices.
5. **Compliance Requirements -** Meeting frameworks like NERC CIP, IEC 62443, and HIPAA requires not only monitoring but demonstrable control over network segmentation and threat response.

Joint Solution Overview

Through the joint integration, Armis Centrix™ & ColorTokens Xshield Enterprise Microsegmentation Platform™ now leverages rich asset intelligence, threat detection, and vulnerability data to deliver more precise and rigorous microsegmentation policies across traditionally hard-to-secure OT and IoT environments. This powerful combination enhances the resilience of operational systems while streamlining security operations.

ColorTokens Xshield Enterprise Microsegmentation Platform™

- Enterprise-class microsegmentation and breach containment
- Agentless Gatekeeper device enforces Zero Trust traffic policies on unpatched legacy systems or OT/IoT devices
- Xshield Visualizer maps East-West traffic and enables granular traffic policy enforcement
- Real-time segmentation response to breach attempts

Armis Centrix™

- Unified asset intelligence across OT, IoT, IT, and health environments
- Deep situational awareness including device type, OS, firmware, vendor, vulnerabilities
- Continuous real-time threat detection and risk-based prioritization
- Contextual insights to support enforcement of segmentation decisions

Combined Power:

This integration enables policy-based microsegmentation tailored to device risk, enforces isolation of compromised asset(s), and supports real-time breach response, all with zero disruption to sensitive operations.

Top Use Cases for the Integrated Solution

1. Vulnerability-Aware Microsegmentation
ColorTokens leverages Armis's detailed device vulnerability intelligence to apply risk-based microsegmentation policies. Vulnerable or high-risk assets are proactively segmented to limit blast radius until remediation is complete.

2. Real-Time Breach Containment
When Armis detects lateral movement, a command injection, or exploitation attempt, Xshield can automatically apply alternate segmentation templates to isolate the threat and stop propagation.

3. Environment Separation
Create and enforce a dynamic and logical separation between IT, OT, and IoT environments to ensure the breach doesn't compromise interconnected domains.

4. Unified Visibility with Actionable Context
Visualizes asset communications and enriches it with context like OS version, manufacturer, and risk posture. Security teams gain a single pane of glass for understanding device behavior and policy gaps.

5. Accelerated Compliance
Support Zero Trust mandates and industry-specific compliance requirements with fine-grained segmentation and continuous monitoring. Audit trails and real-time alerts simplify regulatory reporting.

Key Benefits of the Joint Solution

Reduced Attack Surface & Lateral Movement
Microsegmentation limits attackers' ability to traverse networks, thus containing threats before they impact critical systems.

Agentless & Non-Disruptive
Designed for environments where agent deployment is not feasible. The combined solution is built to fully address and support the technical requirements of OT systems while ensuring operational continuity.

Stronger Cyber Resilience
Combining Armis's real-time detection with Xshield's traffic policy enforcement enables rapid responses and compensating controls that minimize impact.

Improved Visibility & Control
Together, the joint solution delivers comprehensive visibility of assets, traffic flows, and risk profiles, enabling prioritized issues handling and intelligent policy enforcement.

Faster Incident Response & Recovery
Emergency microsegmentation templates, when triggered, allow near-instant containment of threats, reducing mean time to response (MTTR).

Streamlined Compliance Readiness
Supports critical regulations and security frameworks by demonstrating control over devices, their traffic, segmentation, and incident response.

ColorTokens + Armis: Breach Ready by Design

As digital environments become increasingly targeted, security strategies must span from prevention to rapid detection and containment. The integration between ColorTokens Xshield Enterprise Microsegmentation Platform™ and Armis Centrix™ provides organizations with a coordinated, intelligence-driven approach to Zero Trust security.

Together, they empower enterprises to:

- **See every device**
- **Understand every risk**
- **Control every connection**

All while minimizing disruption and maximizing operational safety.

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.

ARMIS

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization’s cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo