COLORTOKENS

SOLUTION BRIEF

Xassure

Breaches happen... are you prepared?

The Goal: A Resilient, Breach-Ready Enterprise

ColorTokens addresses a fundamental challenge in cybersecurity today: despite organizations' extensive investment in firewalls and other perimeter defenses, breaches continue to occur, causing significant financial and operational damage. This is because of the inescapable reality that in the realm of cybersecurity, the defender must be right every time, and the attacker only needs to be right once. After the initial compromise, they use lateral movement to spread throughout the enterprise until they degrade operational systems or compromise sensitive data. Because of this, organizations must adopt the fundamental premise of zero trust security: assume a breach is inevitable and be prepared in advance to survive it.

Be Breach Ready: Before, During and After a Cyberattack

ColorTokens is a leader in zero-trust security solutions, with our Xshield Enterprise Microsegmentation PlatformTM. Xshield stops the lateral spread of any ransomware or malware attack, so a breach does not become a business crisis. It is a key technology to have in place before any breach so that you can minimize business disruption and quickly return to full operational capabilities after an attack. Microsegmentation is fundamental to executing a zero-trust architecture as described in the NIST Special Publication 800-207 and the CISA Zero Trust Architecture Maturity Model.

Xassure can Fill the Gaps in your Cybersecurity Capabilities

In addition to microsegmentation, there are other critical components of a holistic cyber defense described in the NIST and CISA documents: among them are threat detection & response and vulnerability management. ColorTokens can help with those as well. We can help you fill the gaps in your current cybersecurity strategy using our security operations engineers, experts from our world-class systems integrator partners, and best-of-breed software solutions from leading vendors. The result is that between your in-house team and the ColorTokens team, you will achieve a resilient and breach-ready security posture for your enterprise in a cost-effective and mutually exhaustive way.

Introducing ColorTokens XassureTM Managed Services

Xassure delivers three important cybersecurity functionalities as a service: Threat Detection & Response, Managed Microsegmentation Services, and Continuous Vulnerability Management. It uses our industry-leading microsegmentation solution as well as several other best-of-breed tools, including:

- **Next-gen SIEM and SOAR**
- **User entity behavior analytics (UEBA)**
- **Network detection and response (NDR)**
- **Endpoint Security (EDR)**
- **File integrity monitoring (FIM)**

Xassure is delivered as a managed service, including all software and services in one subscription price.

Xassure protects your whole enterprise landscape, including IT, IoT, and Operational Technology/Cyber-Physical Systems. Our security operations engineers will deliver, monitor,

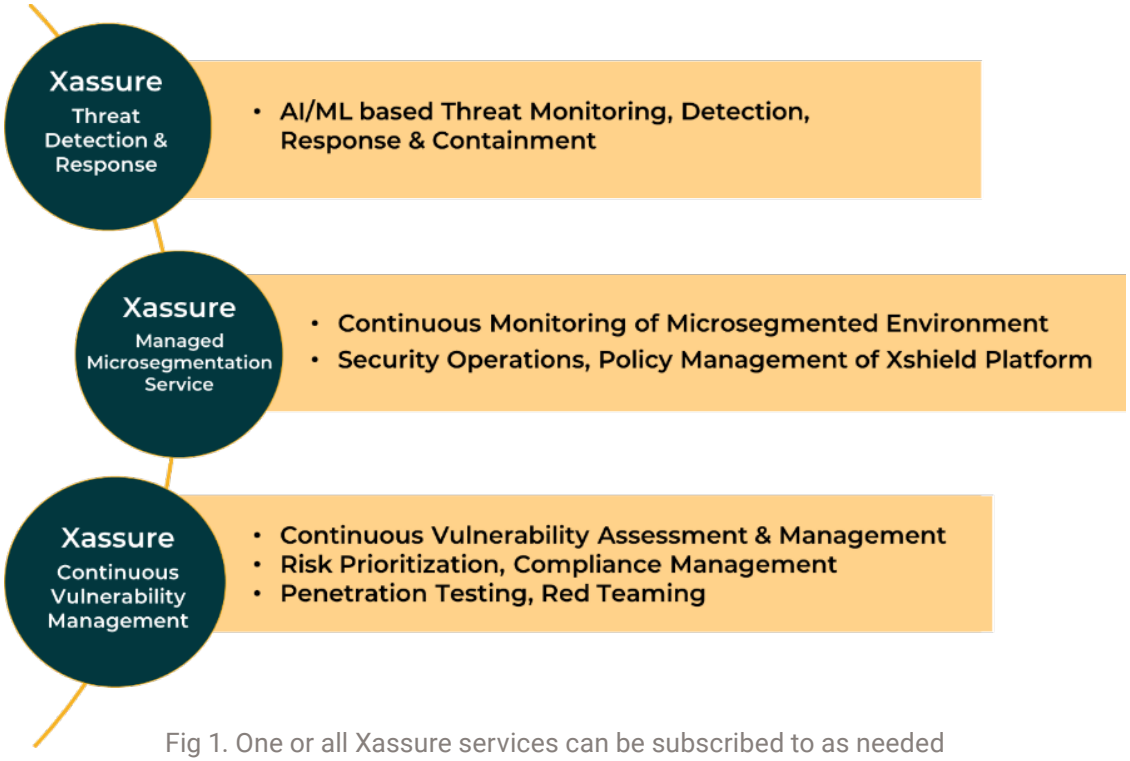

Fig 1. One or all Xassure services can be subscribed to as needed

Xassure Features and Benefits

Xassure Threat Detection Response

Key Features

Unified Security Operations Platform: Combines NG-SIEM, Network Detection and Response (NDR), Threat Intelligence Platform (TIP), Intrusion Detection System (IDS), Security Orchestration, Automation, and Response (SOAR), and User and Entity Behaviour Analytics (UEBA) for both IT and OT environments into a single interface, reducing the need for multiple disparate tools.

Open Architecture with Extensive Integrations: Supports integration with a wide range of existing security tools, including top Endpoint Detection and Response (EDR) solutions, cloud providers, and identity management systems, allowing organizations to leverage their current investments without vendor lock-in.

AI-Driven Threat Detection and Response: Employs artificial intelligence and machine learning to automatically detect, correlate, and prioritize threats across the entire attack surface, enabling faster and more accurate incident response.

24/7 Threat Monitoring and Incident Response: Deep security expertise paired with threat intelligence correlation are an integral part of the monitoring and incident response. Around-the-clock monitoring ensures that potential threats are detected and acted upon in real time, even outside of normal business hours, significantly reducing the mean time to detect (MTTD) and respond (MTTR) to incidents. This is especially critical as many cyberattacks occur during nights or weekends.

Benefits

Enhanced Visibility Across the Attack Surface: By consolidating data from various sources, the TDR platform offers comprehensive visibility into IT, OT, and security environments, aiding in the early detection of threats.

Reduced Operational Complexity and Costs: The unified platform approach simplifies security operations, reducing the need for multiple licenses and lowering the total cost of ownership.

Future-Proof Security Operations: The open and modular design ensures that organizations can adapt to evolving security landscapes and integrate new tools as needed without overhauling their existing infrastructure.

Xassure Managed Microsegmentation Services

Key Features

Managed Microsegmentation for IT environments:

1. Ongoing operations of ColorTokens Xshield platform (after the initial installation and configuration) for IT workloads, legacy systems and specialized workloads (segmented through agentless appliance) –
2. Policy finetuning, onboarding and offboarding of assets.

Managed Microsegmentation for Operational Technology/Cyber-Physical Systems

1. Ongoing operations of ColorTokens Xshield platform and agentless gatekeeper appliance for OT/IoT devices –
2. Policy finetuning, onboarding and offboarding of devices.

Managed Microsegmentation for user endpoints:

1. Ongoing operations of ColorTokens Xshield platform for users/user end points - policy finetuning, on-boarding and off-boarding new assets.

Benefits

Turn-key delivery of microsegmentation: Continuous monitoring and management of the Xshield Enterprise Microsegmentation Platform

Accommodate change in your environment seamlessly: onboarding and offboarding of assets, and application of appropriate microsegmentation policies

Xassure Continuous Vulnerability Management

Key Features

Rapid and Continuous Scanning: The CVM platform employs a smart scanning algorithm capable of detecting vulnerabilities, misconfigurations, exposures, and other risks in less than five minutes, ensuring real-time protection across the network.

Extensive Vulnerability Database: The platform boasts the world's largest built-in vulnerability database, supporting over 175,000 security checks, which aids in precise detection and assessment of network flaws.

Integrated Remediation Controls: Beyond traditional patching, the CVM platform provides integrated remediation capabilities, allowing for immediate fixes of vulnerabilities and reducing the time between detection and remediation.

Risk-Based Prioritization: Utilizing CVSS scores, risk assessments, and predictive analysis, the platform prioritizes vulnerabilities based on severity, enabling security teams to address the most critical issues first.

Compliance Alignment:: The CVM aids organizations in meeting regulatory requirements by addressing multiple risks, including IT asset exposures, patches, and configuration errors, aligning with standards like HIPAA, PCI, ISO, and NIST.

Benefits

Enhanced Security Posture: By continuously identifying and mitigating a wide range of security risks, the CVM platform strengthens the overall security framework of an organization.

Operational Efficiency: Automating vulnerability management processes reduces manual efforts, streamlines operations, and eliminates the complexities associated with traditional systems.

Reduced Attack Surface: Integrated remediation and continuous monitoring significantly diminish potential entry points for attackers, thereby lowering the risk of cyber threats.

Benefits

Regulatory Compliance: The platform's ability to address various security risks ensures that organizations can quickly implement and maintain compliance with industry benchmarks.

Proactive Threat Prevention: The CVM platform establishes a solid foundation for defending against cyberattacks by focusing on prevention through continuous assessment and remediation.

Value of the Complete Xassure Solution

1. Cost-effective and scalable solution delivered as a service
2. Comprehensive & integrated security
3. Faster threat response and operational efficiency with automation and AI-driven insights
4. 24/7 proactive threat detection and response
5. Industry-specific compliance support (e.g., HIPAA, PCI DSS, GDPR)

ColorTokens Expert Consultancy Offerings

In addition to our ongoing Xassure managed services, we offer individual consultancy engagements to enhance your cyber defense strategy:

ColorTokens Breach Readiness Assessment Consultancy

- Gain visibility into the state of your security posture, with metrics to understand your cyber resiliency and ability to withstand a breach

ColorTokens Zero Trust Readiness Assessment Consultancy

- Understand your current state and the gaps you must fill to have a complete zero-trust architecture.

ColorTokens Xshield Implementation Services

- Expert installation and configuration of your Xshield Enterprise Microsegmentation Platform deployment for you to take over and manage.

Let’s get started today!

In today’s modern threat environment, the attackers don’t delay, so neither should you. We can help you quickly get your cyber defense strategy up and running with our Xassure managed services.

If you are not sure about the status of your security posture in terms of breach readiness, you can begin with our Breach Readiness Assessment. We will deliver an executive summary and an in-depth report on the as-is state and recommendations for the to-be environment needed for you to reach true breach readiness.

You can learn more about Xassure at www.ColorTokens.com/Xassure. To schedule a discussion with our expert solutions team you can reach us at www.ColorTokens.com/contact-us

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.