COLORTOKENS

Xassure

DATASHEET

Protect against Breaches with 24/7 Zero Trust as a Service

Business Benefits

- Receive Actionable Alerts with Minimal False Positives
- Prevent Malware Infection
- Prevent Unauthorized Process Execution
- Detect and Contain Threats in Minutes with One-Click
- Reduce Attack Surface, Blast Radius & Blind Spots
- Obtain Best-In Class Intelligence
- Adopt Zero Trust Without Business Disruption

Secure your business from advanced threats and gain peace of mind 24/7 with Xassure that tracks down the most elusive threats with just-in-time detection and response.

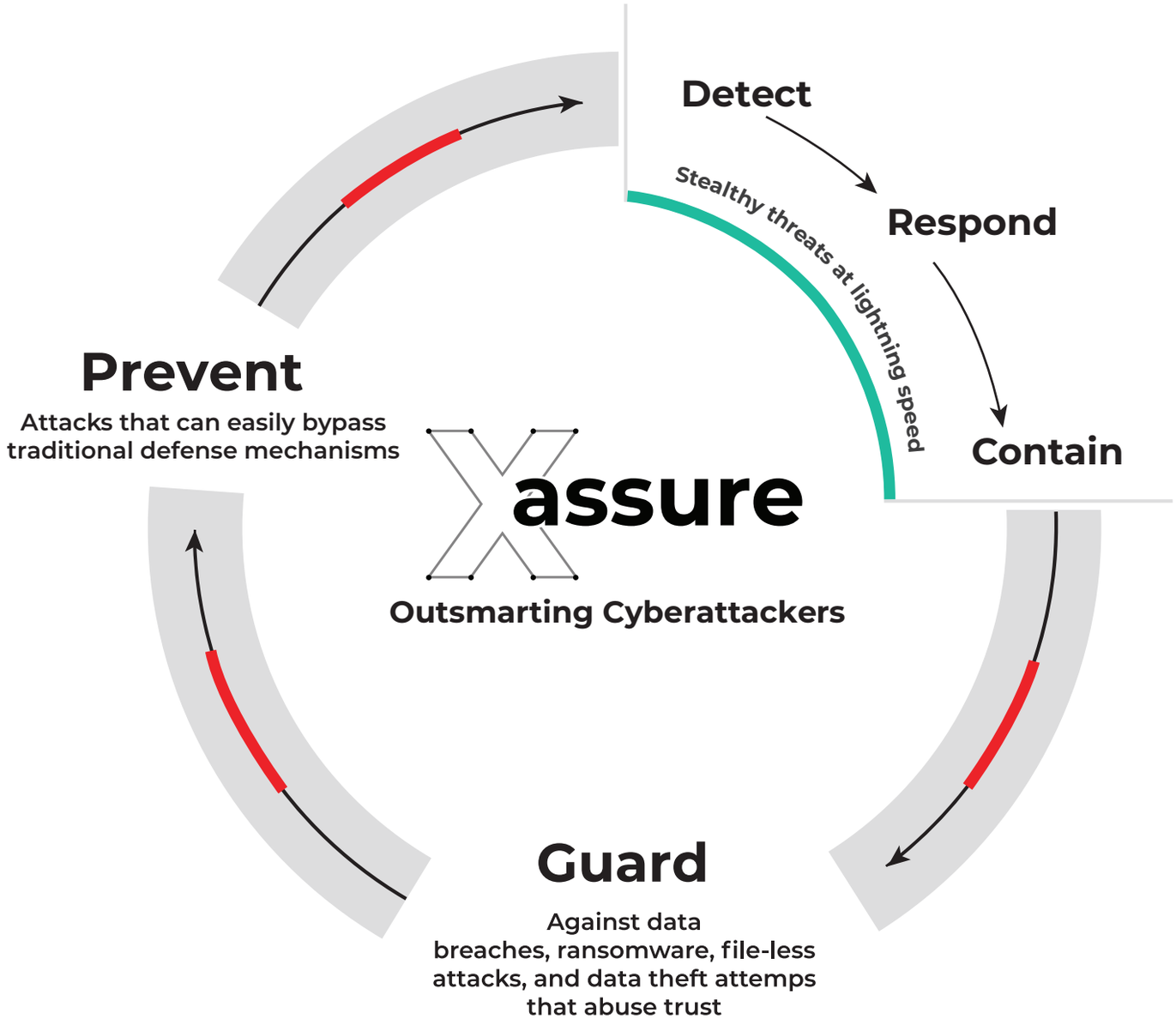
Today's threat landscape is constantly evolving, but many organizations still rely on traditional perimeter-based security and have resource-strapped IT teams, leading to poor visibility, slow investigations, and scores of false positives. Faced with such challenges, organizations, especially those on a digital transformation journey, need a comprehensive security solution that sweeps their network assets and security infrastructure in search of evasive hidden threats without increasing operational overhead and cost or causing business disruption.

ColorTokens Xassure is that solution.

Available as a monthly subscription and customized to suit your business needs, Xassure is an outcome-driven, managed Zero Trust security solution that both augments your security preparedness and enhances your security posture with seamless Zero Trust adoption. Xassure complements your security IT team with advanced threat detection, response, and breach containment capabilities. You get the peace of mind that comes with knowing your network is protected 24/7 with robust Zero Trust security.

With Xassure, our certified security experts watch your back 24x7 and ensure that the security alerts you receive are truly actionable, not false positives. Harnessing the power of AI/ML, ColorTokens' monitoring platform and a global threat knowledge base, our experts halt advanced attacks very early in the cyber kill chain, thus stopping the enterprise-wide intrusion attempts.

Key Capabilities



- AI/ML Based Threat Detection
- XDR Capabilities Across Network, Cloud, and Endpoints
- Ransomware and Data Theft Prevention Using Specialized Threat Models
- APT Detection Based on MITRE ATT&CK Framework
- Extended Integration Across Existing Solutions
- Zero Trust Implementation with Managed Services - Aligned to NIST SP 800-207

Challenges and Solutions

Challenge	ColorTokens Solution
Shortage of Skilled In-House Security Staff	ColorTokens Xassure works as an extension of your security team by leveraging AI/ML, highly skilled team of experts and knowledge base to deliver advanced threat detection and incident response for endpoints and workloads.
High Reliance on Traditional Security Measures (AV, NTA, SIEM)	Unified visibility into network and endpoint traffic with integrated breach detection and response capabilities. A comprehensive attack scenario analysis helps ascertain the blast radius and root cause of the attack.
High Operational Security Overhead	Significant reduction of false positives improves operational efficiency with early detection and quick response to any breach through 24x7 monitoring and managed service.
Timely Detection and Response to Insider and Advanced Threats	ColorTokens' team of analysts and investigators leverage network and endpoint data coupled with different threat models and AI/ML-based threat detection capabilities for early detection of insider and advanced threats.
Remote Workforce Monitoring	Monitoring services aligned with Zero Trust architecture protect critical resources in hybrid clouds and on-premises. The service also monitors remote users' access to corporate assets, thereby minimizing threats.

Xassure Services

Proactive Breach Protection

Modern cyberattacks easily bypass signature-based security controls. Xassure leverages AI/ML, data scientists, threat hunters, and incident responders to detect sophisticated and hidden threats, advanced malware like ransomware, and file-less attacks. The service delivers deep monitoring and analysis across network and endpoints to provide contextual and early detection. Additionally, Xassure guarantees your defence readiness by continuously elevating your security posture. This involves continuous mitigation of observed gaps, periodic vulnerability scans and validation of defense mechanisms using red/blue teaming, and penetration testing.

Seamless Zero Trust Adoption

ColorTokens' experts collaborate with customers to design, implement, and operationalize the Zero Trust security framework leveraging ColorTokens' offerings. The scope spans servers, workloads, endpoints, and critical IT assets and includes customized white-glove onboarding and deployment of ColorTokens Xshield for workload visibility and security and Xprotect for endpoint protection in the customer's environment.

XDR-Based Advanced Threat Monitoring and Incident Response

Relying on signatures and IOCs is no longer sufficient to detect advanced threats lurking in your environment. Defending against advanced attack calls for advanced anomaly identification techniques and pattern-based detection. ColorTokens' team of certified security experts leverages AI/ML, a global threat knowledge base, and the curated intelligence of more than 108 MITRE ATT&CK techniques to quickly detect and contain any anomaly observed across endpoints and network. All the security incidents are thoroughly analyzed and investigated before notifying the customer, reducing alert fatigue with fewer false positives.

Managed Micro-segmentation and Monitoring

Security controls need to scale with the rapidly growing business and digital transformation initiatives to thwart modern-day threats. ColorTokens' experts ensure security posture is intact even as your business scales and evolves. This service includes daily operational updates to micro-segments, defined policies, and endpoint security profiles. In addition, experts continuously monitor managed resources for any common and frequently occurring threats and notify the concerned teams.

Key Features and Benefits

Features / Capabilities	Business Benefits
Aligns with MITRE ATT&CK® Supporting 108 Techniques	Detect and contain malicious assets early and reduce the infection radius.
Detects Attack Variants from 125 APT Groups	Achieve a low probability of advanced persistent threats which are sophisticated, well-funded, and difficult to detect.
Detects Threats Using AI/ML	Accelerate threat detection of complex cyberevents by adding necessary context to prioritize investigation efforts.
Tracks 1,500+ Active Ransomwares	Detect ransomware attacks early to reduce the chances of financial and brand reputation damage.
Curates Threat Intelligence from 80M Indicators of Compromise (IOCs)	Obtain timely, reliable, and contextual notification of global threat outbreaks across industry verticals and geographies.
Analyzes Networks, Endpoints and User Behavior Concurrently	Minimize false positives by utilizing security analysts and resources efficiently.
Responds to and Contains Threats Using ColorTokens Xshield and Xprotect Products	Contain and remediate threats early in the cyber kill chain and minimize the blast radius of the attack.
Monitors Threats 24x7	Monitor networks, endpoints, and user behavior in real time across multi-vendor and hybrid environments.

“We chose to work with ColorTokens because of its commitment to simplifying our security operations and its minimally invasive, cloud-delivered approach to our infrastructure and team. Implementation was seamless from start to finish: we deployed ColorTokens’ lightweight agents on our 700 systems, and got up and running with minimal configuration and no disruption or redesign. This was of critical importance to us, as it allowed us to continue our customer service business without skipping a beat.”

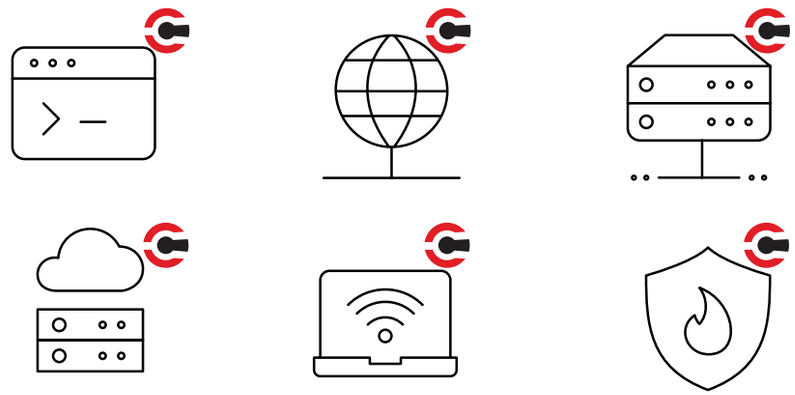
– CEO ITCube Solutions Pvt.

How Xassure Elevates Your Security Posture

LOG COLLECTION

Xshield Workload Visibility and Segmentation

Xprotect Endpoint and host protection



Colortokens Agent

Custom Agent

XDR SECURITY OPERATIONS

ML Powered Advanced Threat Detection

MITRE ATT&CK Models

Specialized Ransomware Detection Models

Advanced Data Theft Detection

Behavioral Analytics

One Click Containment

COLORTOKENS TEAM OF SECURITY EXPERTS

Incident Responders

Data Scientists

Ethicle Hackers

Threats Investigators

Threats Analysts

Threat Hunters

DELIVERED SECURITY SERVICES

Breach Protection

XDR-Based Advanced Threat Monitoring and Incident Response

Zero Trust Adoption

Managed Micro-Segmentation and Monitoring

Security Posture Elevation

Xassure Packages Tailored to Your Specific Needs

		Xassure Essentials	Xassure Prime	Xassure Prime +
Zero Trust Adoption	Installation and Configurations on Workloads and Endpoints	✓	✓	✓
	Micro-segmentation and Endpoint Security Profile Design and Implementation	✓	✓	✓
	Product Subscription for Xshield and Xprotect	✓	✓	✓
Managed Micro-segmentation & Monitoring	Management of ColorTokens Products	✓	✓	✓
	Manage day-to-day Security Operations of ColorTokens Products	✓	✓	✓
	Threat Alerting for Common and frequently occurring threats	✓	✓	✓
	Product Support	**8X5**	**24X7**	**24X7**
XDR Based Advanced Threat Monitoring and Incident Response	Deep Monitoring using Patterns, Signature, and Reputation Check		✓	✓
	Validation of Threats using Analysis and Investigation		✓	✓
	Detection of APTs using MITRE ATT&CK Framework		✓	✓
	Customization of Threat Alerts for customer specific scenarios		✓	✓
	Global Threat Intelligence covering Bad Hash, Bad IP, Bad Domain		✓	✓
	Managed Incident Response		✓	✓
	Managed Breach Response		✓	✓
	Threat Containment		✓	✓
	Regular Review of Operations Effectiveness		✓	✓
Breach Protection	AI/ML Based Detection for Advanced Ransomware and Data Theft attempts			✓
	AI/ML based detection of advanced Stealthy and Hidden Attacks			✓
	Behavioral Based Detection of Attacks that abuse trusted processes and applications authorized by the business			✓
	Periodic measurement of posture improvement and elevation recommendations			✓
	Periodic RED/BLUE Teaming and Penetration Testing Exercises			✓
	Periodic Vulnerability Scans			✓

WANT TO CUSTOMIZE XASSURE?

CONTACT US

ColorTokens Inc. is a leading innovator in SaaS-based Zero Trust cybersecurity solutions providing global enterprises with a unique set of products and services for securing applications, data, and users across cloud and hybrid environments. Through its award-winning Xtended ZeroTrust™ Platform and context-aware machine learning-powered technologies, ColorTokens helps businesses accurately assess and improve their security posture dynamically.

As cloud adoption grows, traditional perimeters get redefined, and new attack vectors and threat actors materialize, corporations recognize their security posture needs to reflect their Zero Trust philosophy. ColorTokens' technology allows customers to achieve Zero Trust by utilizing rich, meaningful contextual information about the application, microservice, or protected resource, so customers can apply Zero Trust with as secure of a perimeter as they can. ColorTokens' cloud-based SaaS platform can automatically deploy next-generation security controls and increase security posture dynamically without any new hardware, downtime, reboots, or changes to a client's existing systems.

With a team of over 400 people, ColorTokens has global office locations in Santa Clara, California; New York; London; Copenhagen, Denmark; and Bengaluru, India. For more information, please visit **www.colortokens.com.**