COLORTOKENS

DATA SHEET

Xassure

Progressive Zero Trust as a Service

Highlights

- Attain a proactive security posture with Zero Trust security model adoption
- Prevention, detection, response, and remediation of advanced threats
- MITRE ATT&CK based detection all through the cyber kill chain
- Advanced AI/ML-driven behavioral detection to uncover hidden threats
- Breach response and remediation
- Single click containment
- Leverage global insights through curated threat intelligence

Businesses need to modernize from traditional to digital ways of doing business, leading to cloud and perimeter less environments. These environments are under sophisticated cyber-attacks and cannot be protected by conventional perimeter-based security. To add, the COVID-19 crisis forces businesses to adopt remote working and, at times, through personal devices. This shift has increased the threat profile due to vulnerable access mechanisms, inadequate controls, and unmanaged infrastructure. These challenges put pressure on resource crunched security teams. Businesses need to identify, design, and implement the optimal security controls that include technology, architecture, solutions, and highly skilled resources. Companies must adopt a managed risk approach to security and collaborate with trusted security partners who provide next-gen security solutions and niche expertise to enable running the business hassle-free.

Xassure is an outcome-driven security-as-a-service that helps customers rapidly adopt the proactive Zero Trust security framework and augments it by providing advanced threat detection, response, and containment solution. This provides businesses with a robust security setup that protects from advanced and hidden attacks, ransomware, and data theft attempts, which traditional defense mechanisms do not catch. With Xassure, our expert professionals continuously measure baseline and enhance your security preparedness by uncovering vulnerabilities, check defense effectiveness, and mitigate the gaps to provide you a consistent and elevated security posture.

Xassure is delivered through the ColorTokens breach protection & monitoring platform that harnesses the power of AI/ML to provide advanced detection capabilities that can detect a threat very early in the cyber kill chain and protect you from significant impact. You also leverage the benefits of integrated threat intel built using a global threat knowledgebase to keep your defenses updated from any new outbreak.

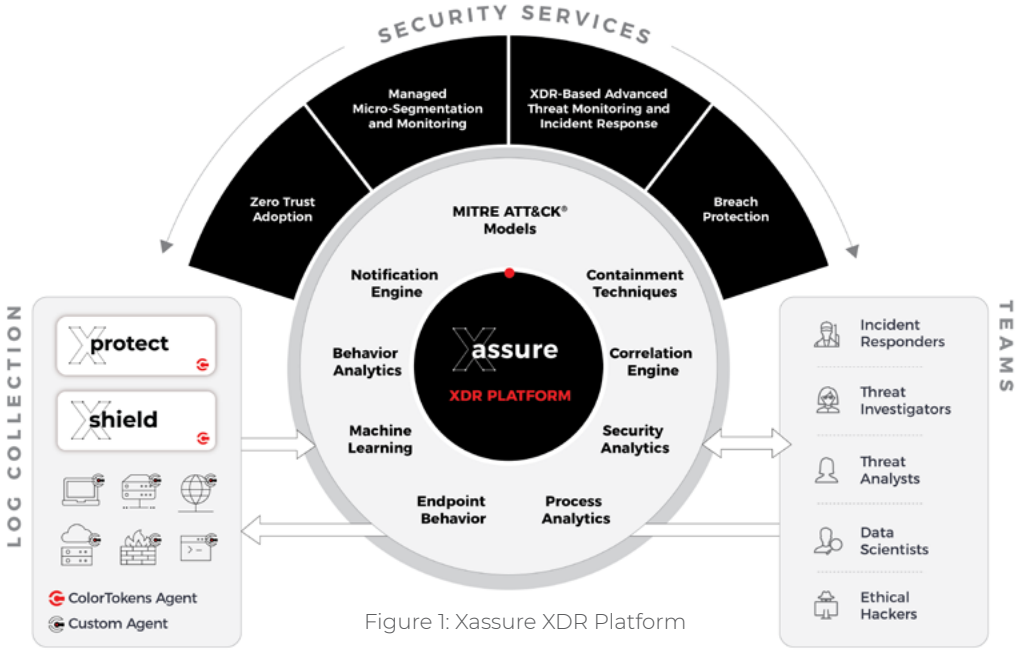

Figure 1: Xassure XDR Platform

Key Capabilities

AI/ML Based Threat Detection: Xassure leverages artificial intelligence and machine learning to detect threats related to any changes in asset environment or user behavior.

XDR Capabilities: A proactive approach to threat detection and response while providing comprehensive visibility into networks, clouds, and endpoints.

Aligned to NIST SP 800-207: Zero Trust implementation augmented with managed risk service and Continuous Diagnostics and Mitigation (CDM) capabilities.

MITRE Based APT Detection: Implements a comprehensive list of MITRE ATT&CK TTP's to provide detection of advanced attacks and their variants across the cyber kill chain.

Specialised Models to Detect Focused Attacks: We have designed specialised threat models that can detect ransomware attacks and data thefts

Unified Solution: A single solution that delivers prevention, detection, response & containment of threats across your multi-vendor and multi-environment IT.

Xassure Services

Zero Trust Adoption

ColorTokens experts will collaborate with customers to design, implement, and operationalize the Zero Trust security framework leveraging ColorTokens offerings. The service will leverage a proprietary 3 stage SET (Secure | Expand | Transform) framework to deliver faster and tangible benefits. The scope will span across servers, workloads, endpoints, or critical IT assets by implementing micro-segmentation and endpoint security products from ColorTokens.

Managed Micro-segmentation and Monitoring

Security controls need to keep pace and scale with the rapidly growing business and digital transformation initiatives to thwart modern-day threats. ColorTokens experts will ensure security posture is intact even as your business scales and evolves. Daily operational updates to microsegments, defined policies, endpoint security profiles are provided in this service. Besides, we will continuously monitor managed resources for any common and frequently occurring threats and notify the concerned teams.

XDR-Based Advanced Threat Monitoring and Incident Response

Cyber attacks are continuously evolving and changing attack methods. Detecting these advanced threats requires advanced anomaly identification techniques and pattern-based detection instead of just relying on signatures and IOC's. ColorTokens leverages machine learning, knowledge-base, threat patterns, and security experts to detect anomalies. Xassure leverage the intelligence of more than 108 MITRE ATT&CK techniques and curated threat intelligence to quickly notify/ contain any anomaly detected across endpoint and network. All the security incidents are thoroughly analyzed and investigated before notifying the customer. This results in a lower number of alerts and hence reduces alert fatigue.

Breach Protection

Cyber attacks are getting sophisticated and are successfully bypassing 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 fileless attacks. The service delivers deep monitoring and analysis across network and endpoints to provide contextual and early detection. It provides deep and continuous analysis to hunt for traditional and targeted attacks designed to evade standard security technologies.

Additionally, Xassure guarantees your defense readiness and elevating your security posture by adopting a managed risk approach. This involves continuous mitigation of observed gaps, periodic vulnerability scans and validation of defense mechanisms using red/blue teaming, and penetration testing.

Xassure Service Packs

		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			

> “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. Ltd.

Challenges and Solution

Challenges	ColorTokens Solution
Siloed Monitoring Tools (AV, NTA, SIEM)	Unified visibility into network and endpoint traffic with integrated breach detection and response capabilities. With a comprehensive attack scenario analysis to ascertain the blast radius and root cause of the attack.
Detecting Insider and Advanced Threats	ColorTokens team of analysts and investigators leverage network & endpoint data coupled with different threat models and AI/ML-based threat detection capabilities for early detection of insider and advanced threats.
Cloud & Remote Workforce Monitoring	Monitoring services aligned with Zero Trust architecture to protect critical resources in hybrid clouds and on-premises. The offering also includes monitoring accesses of remote users to corporate assets, thereby minimizing threats.
Reduce Operational Overhead	Significantly reduce the false positives and achieve operational efficiency with early detection and quick response to any breach with Zero Trust Adoption security-as-a-service.

Xassure Features & Benefits

Feature	Benefit
Aligning with MITRE ATT&CK® Supporting 108 techniques	Early detection and containment of malicious assets, reducing the infection radius.
Detecting Attack Variants from 125 APT Groups	Achieve a low probability of advanced persistent threats, that are otherwise sophisticated, well-funded and difficult to detect.
AI/ML Based Threat Detection	It provides the means to accelerate threat detection events for complex cyber threats by adding the context needed to prioritize investigation efforts.
Tracking 1500+ Active Ransomwares	Early detection of ransomware attacks to protect from financial and brand reputation damage.
Curated Threat Intelligence from 80M Indicators of Compromise	Obtain timely, reliable, and contextual notification of global threat outbreaks across industry verticals and geographies.
Concurrent Analysis of Networks, Endpoints and User Behaviour	Minimize false positives, utilize security analyst and resources efficiently.
Response & Containment leveraging ColorTokens Xshield & Xprotect Products	Faster containment and remediation of threats and minimize the blast radius of the attack.
24x7 Coverage	Real-time monitoring of networks, endpoints, and user behavior across multi-vendor and hybrid environments.

Send your queries or questions to info@colortokens.com

ColorTokens Inc., a leader in proactive security, provides a modern and new generation of security that empowers global enterprises to singlehandedly secure cloud workloads, dynamic applications, endpoints, and users. Through its award-winning cloud-delivered solution, ColorTokens enables security and compliance professionals to leverage real-time visibility, workload protection, endpoint protection, application security, and Zero Trust network access—all while seamlessly integrating with existing security tools. For more information, please visit www.colortokens.com