Assure
Managed IT Solutions

COLORTOKENS

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

BLACK UNICORN AWARDS 2019 NOTABLE MENTION

INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2019

DATA SHEET

# Xassure

# Zero Trust Security Delivered as-a-service

## Highlights

- a Minimize the attack spread and impact
- a Achieve a low probability of malicious attacks
- a Gain a faster adoption of Zero Trust architecture
- a Obtain early notification of global threat outbreaks
- a Assurance of no half measures to attacks
- a Minimize false positives on notified threats
- a Early detection of attacks
- a Faster containment and remediation of threats

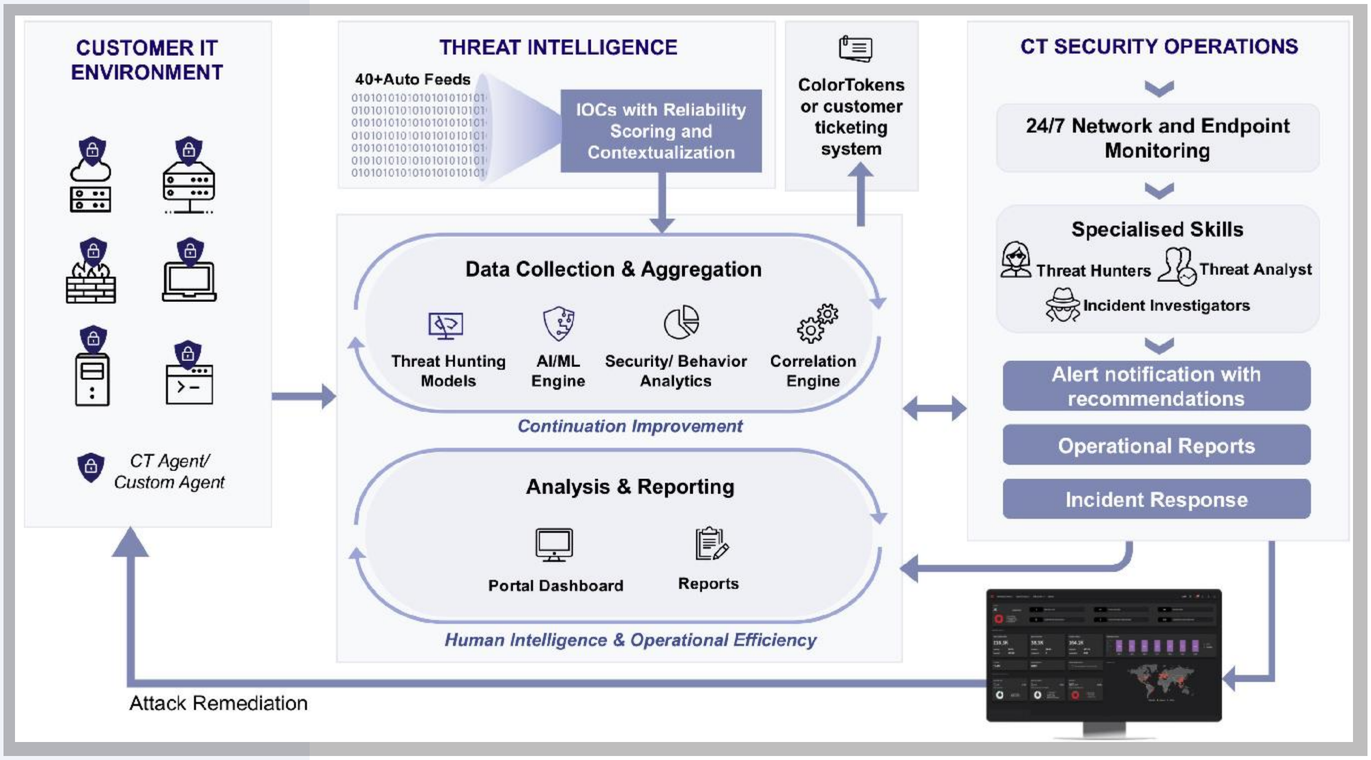
Small and medium businesses worldwide are rapidly embracing technology to innovate faster. But they struggle to protect applications and data across the hybrid enterprise and meet stringent regulatory and data protection laws. These factors add to security operations challenges such as a siloed view of security, detecting advanced and insider threats, alert fatigue, and a staggering 279 days to identify and contain a breach[1].

Ideally, businesses should focus on innovation and wealth creation, but the severity of security threats has made it a board room topic. To shift the focus back to core business objectives, they need to collaborate with a trusted security partner for turnkey security-as-a -services solutions built on proactive security technology, highly skilled security talent, and a continuous learning process to achieve Zero Trust security posture.

ColorTokens Xassure is a security-as-a-service that leverages machine learning, artificial intelligence, highly skilled resources & knowledge-base to deliver advanced threat detection and incident response for endpoints and workloads. Xassure provides deep and continuous analysis around the clock to hunt for traditional and targeted attacks designed to evade standard security technologies. Xassure comprises of multiple independent services, including breach protection, ransomware protection, data theft protection, and security monitoring. Xassure leverages the built-in contextual data collected from ColorTokens products Xshield and Xprotect, in the form of patterns that are then leveraged by a team of threat hunters and security analysts to detect any anomalies and identify a threat attack before it matures.

Xassure provides early detection, faster response, and one-click containment against advanced threats. The services protect workloads, applications, user endpoints, and enterprise networks by leveraging ColorTokens network and endpoint security products.

Figure 1: Xassure Breach Protection & Monitoring Platform



[1] Cost of Data Breach report 2019 by IBM security

## Key Service Capabilities

**Intelligence Driven:** Xassure service leverages ColorTokens curated threat intelligence that updates IOCs frequently based on the threat actors identified across the globe.

**AI/MLBased Threat Detection:** Thanks to technology that Xassure brings in by leveraging Artificial intelligence and Machine learning to detect threat related to any change in environment or behaviour of assets or users.

**24/7Expertise:** Xassure service continuously learns evolving threats driven by roles like security analysts and Threat Hunters, Investigators, Incident responders and Data scientists.

**MITRE Based APT Detection:** This service leverages MITRE attack techniques mapping to detect advanced attacks.

**Specialised Models to Detect Focused Attacks:** Xassure provides models to detect focused attacks like ransomware and data theft attack scenarios.

**Cross PlatformCorrelation:** Real time correlation of endpoint and network telemetry data enabling complete visibility to threat landscape.

## Service Components

| | Breach Protection | Ransomware Protection | Data Theft Protection | Security Monitoring (Basic) | Security Monitoring (Advanced) |
|---|---|---|---|---|---|
| Malware Detection w/o Scanning | √ | √ | √ | √ | √ |
| Threat Hunting using MITRE Attacks Techniques | √ | | | | |
| Threat Validation and Investigation | √ | √ | √ | | √ |
| Incident Response and Containment | √ | √ | √ | | √ |
| Threat Intelligence Driven | √ | √ | √ | √ | √ |
| Access to Specialised Skillsets | √ | √ | √ | | √ |
| Predefined Threat Alerts | | | | √ | √ |
| Custom Threat Alerts | | | | | √ |
| UEBA based Threat Detection | √ | | | | |
| AI/ ML driven Threat Detection | √ | √ | √ | | |
| On-demand Breach Response | √ | | | | √ |
| Hunting Models for Ransomware Attacks | √ | √ | | | |
| Hunting Models of Data Theft Attacks | √ | | √ | | |
| Hunting Models for APTs and Targeted Attacks | √ | | | | |

Table 1: Xassure Service Components

## Challenges and Solution

| Challenges | ColorTokens Solution |
|---|---|
| Siloed Monitoring Tools (AV, NTA, SIEM) | Unified visibility into network and endpoint traffic with integrated threat hunting capabilities. With a comprehensive attack scenario analysis to ascertain the blast radius and root cause of the attack. |
| Detecting Insider and Advanced Threats | The threat hunting teams 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. |

# Xassure Security Packs

| | Xassure Essentials | Xassure Prime | Xassure Prime Plus |
|---|---|---|---|
| Zero Trust Implementation on Workloads and Endpoints | √ | √ | √ |
| Product Subscription (applicable to new customers) | √ | √ | √ |
| Continuous Management of ColorTokens Products | √ | √ | √ |
| Detection and Alerting of Common and High Occurring Threats | √ | √ | √ |
| Customise Threat Alerts and Notification | | √ | √ |
| Detection and Alerting Based on Deep Monitoring across Networks and Endpoints | | √ | √ |
| Threat Intelligence covering Bad Hash, Bad IP, Bad Domain | | √ | √ |
| Threat Investigation | | √ | √ |
| Managed Incident and Breach Response for Threat Containment | | √ | √ |
| Quarterly Review of Operations | | √ | √ |
| Detection of APTs using MITRE ATT&CK Framework | | √ | √ |
| AI/ML Based Detection for Ransomware, Data Theft and Hidden Attacks | | | √ |
| RED and BLUE Teaming Exercises | | | √ |
| Periodic Vulnerability Assessment | | | √ |
| Product Support | 8X5 | 24X7 | 24X7 |