COLORTOKENS

DATASHEET

Xshield

SIMPLIFIED ZERO TRUST MICRO-SEGMENTATION FOR HYBRID ENVIRONMENTS

Today enterprises develop and deploy applications in increasingly hybrid or multi-cloud environments, and access has expanded beyond corporate offices and networks to remote locations across the internet. The corporate data centers, servers, and networks give customers inherent ownership and control-based trusts. However, the cloud and internet need a Zero Trust security model to meet this requirement.

ColorTokens Xshield is a cloud-delivered micro-segmentation solution based on a Zero Trust platform that secure critical corporate assets, including applications and workloads. Our solution provides remote access user control for micro-segments within a single platform. The infrastructure-agnostic platform simplifies and accelerates the enterprise journey for distributed hybrid environments, driving full cloud adoption with a Zero Trust security model. It deploys seamlessly and enables enterprises to visualize and define secure micro-segment boundaries (micro-perimeters) through automation for their application workloads.

Xshield in Action

The ultra-lightweight agents collect telemetry data and enable the security administrator with rich visualization, automated policy management, progress reports, and actionable contextual alerts via a cloud console shown to the right. The cloud platform ingests telemetry data coupled with the vulnerability feed, threat feed, and identity feed to guide the learning engine to automate segmentation by auto-creating system tags reducing the administrative burden, and creating access policies.

ColorTokens Xshield Dashboard / Architecture

ColorTokens Xshield Dashboard / Architecture

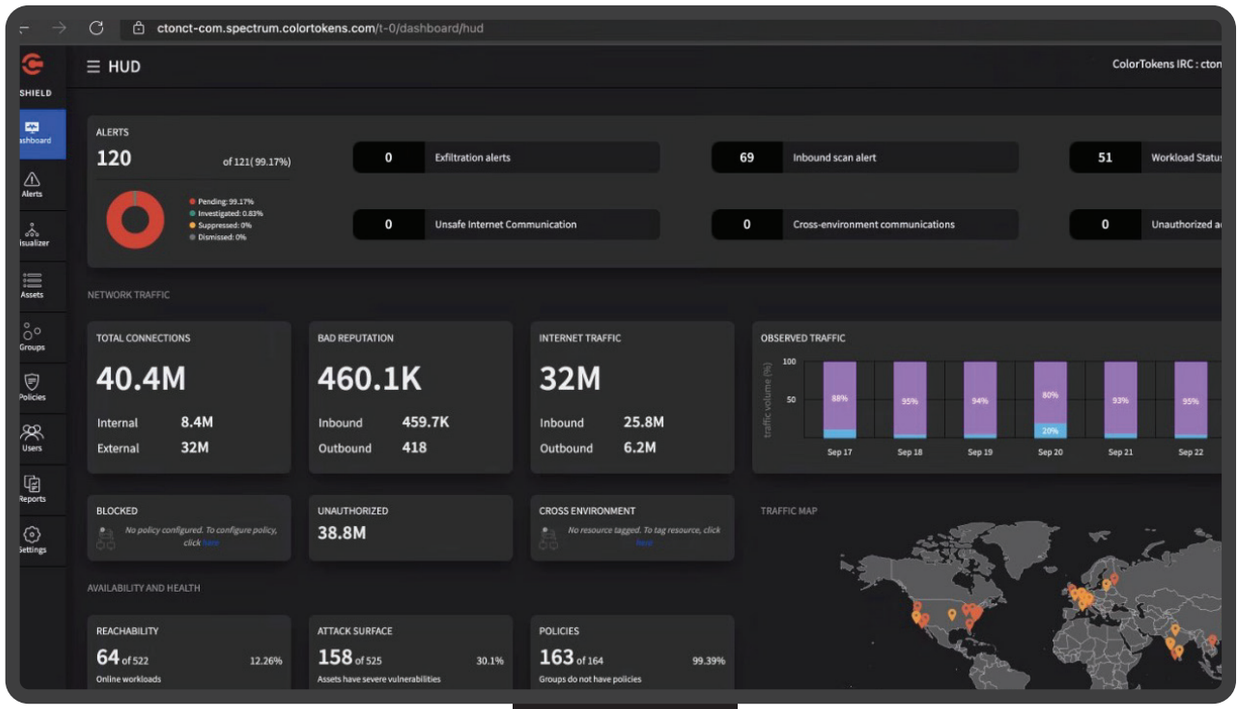


Figure: Cloud Console

NIST NVD (National Vulnerability Database)

Vulnerability

BrightCloud / AlienVault

Threat Intelligence

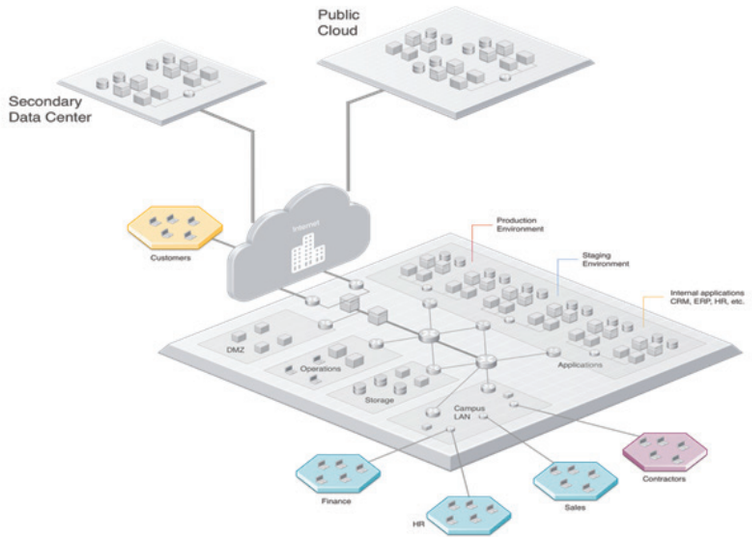
Connectivity to Cloud Providers (AWS, Azure, GCP and others)

Visualization Policy Management Reports

Agents collect Telemetry

Policy

Identity Feed (SIEM Integration)



Xshield Features & Benefits

Features / Capabilities	Benefits
Skyview Visualizer	• Simplified console eases log collection drives better debugging and reduces the need to collect firewall logs manually • Rich, contextual visibility into network flows from the most significant trend to individual workload service • Simulate each security change to minimize business disruption • Instantly correlating threats from risk, malicious flows, processes, and vulnerabilities, and users • Perform powerful searches using tags, addresses, names, and asset types based on natural language processing capabilities • Manage cloud workloads with pre-assigned tags, reducing the time to identify cloud workloads, including resource name, type, configuration
AI Segmentation Engine	• Effortlessly segment and save time using the Xshield deep learning engine to, recommend tags and Zero Trust segments across your hybrid cloud environments • Reduce, the attack surface, minimize business risk and prevent lateral movement of threats • Seamlessly clone policies within workload groups and automatically recognize asset metadata to apply and create a flexible grouping with custom tags based on business needs • Policy templates for enterprise applications and build custom policy templates for known applications
ML Policy Engine	• Automate and optimize policy recommendations based on software identity, user identity, application awareness, historical network, threat, and vulnerability data • Progressively create policies to secure applications externally and internally that extend to protect against intra-application threats and user access • Understand the policy impact before enforcement to minimize any • View entire policy state from policy creation to firewall rule on the workload from the console
Dynamic Policy Graph	• Translate and apply natural language policies automatically to workload-specific policies across environments (physical servers, virtual machines, cloud, and containers) and operating systems (Windows, Linux, Solaris) • Recognize any changes in IP address, auto-scaling and removal of workloads, implement policy updates to cover any blind spots, and quarantine the workloads in case of any compromise • Freedom to selectively enforce policies at your own pace for inbound and outbound traffic, with domain-based policies instead of just IP address
Native Integrations	• Fasten security operations by responding to operational issues and security incidents by integrating Xshield API to SIEM console using our Splunk and Azure apps • Zero-touch agent rollout via integration with existing IT automation tools like Ansible, GPO across distributed infrastructure without manual intervention • Extend identity-based segmentation to users by integrating with your identity provider • Consume audit logs with log type and time range

Segmentation Readiness and Compliance

- Accelerate compliance by simplifying audits and reporting on compliance needs such as PCI
- Receive notifications instantly for any unauthorized changes to the environment
- Streamline Xshield administrative workflows using RBAC
- Assess segmentation progress through a readiness score and find gaps in security posture.

Public APIs

- Availability of public API for assets, tags, groups, policy creation, flow, audit logs, alerts, and quarantine.
- Gather data for assets, including policy tampering, vulnerability exposure, and network exposure
- Search FQL-based keywords for filtering assets with asset API filter

Key Use Cases

Zero Trust Security for Crown Jewels

Challenges	ColorTokens Solution
Enterprises host critical applications across bare-metal, traditional servers, cloud-hosted virtual machines, containerized workloads, and other host systems. Organizations lack visibility into what assets are in their network, where data exists in their distributed environment, who has access to data, and how to secure the data from malicious or unauthorized access. Regulatory requirements enforce heavy penalties to secure data. However, the critical assets (crown jewels) have security risks from east-west communications within the data center or cloud. Enterprises need a platform-agnostic, easy-to-deploy solution that protects their crown jewels from unauthorized east-west communications and lateral movement.	Xshield ensures that customers have complete visibility into their assets through a visual dashboard, gain insight into data-related business risk, and are continuously aware of the security posture of their crown jewels. The security policy is close to the data, and it moves with the assets as they shift from on-premises to the cloud. ColorTokens provides a simplified, Zero Trust (“never trust, always verify”) approach to securing an enterprise’s most valuable crown jewels against cyberattack. ColorTokens Xshield is based on the NIST Zero Trust framework to address evolving threats and compliance requirements. 100% cloud-delivered, SaaS-based for fast time-to-value, Xshield enables granular visibility, security, and control over applications and network assets to reduce the attack surface and the impact of breaches significantly. Customers benefit from increased resilience to attacks, rapid containment, and minimal business disruption or downtime.

Environment Separation

Challenges	ColorTokens Solution
Properly configured environment separation reduces the risk of data breaches arising due to unwanted or unmonitored movement of production data into a development environment. Data breaches also happen when development teams have access to sensitive production data in the development environment. Secure environment separation, ensuring compliance and data privacy, is the best strategy to prevent data breaches. However, this can become time-consuming and challenging in distributed and hybrid data center environments. The biggest challenge to any enterprise IT-consisting of multiple applications spread across development, testing, and production servers – is enabling secure environment separation. For every movement of a resource or an application in the data center, all stakeholders, from the CIOs to the network and system engineers, must be aligned to ensure data security, privacy, and compliance.	ColorTokens Xshield helps create Zero Trust Secure Zones™ (micro-perimeters) around applications with just a few clicks to prevent lateral movement and the spread of breaches. With environment separation, the security boundary moves with the application, reducing the attack surface and preventing the spread of violations in a hybrid and multi-cloud environment. It enables customers to isolate and protect their critical applications in development, staging, and production environments from one another. Xshield fits into any stage of an enterprise’s cloud journey by enabling security policies to follow the application environment as they move to and from the moment a new workload is born.

Cloud Workload Protection

Challenges	ColorTokens Solution
Enterprises on an accelerated journey to cloud adoption need to gain complete visibility into distributed assets, ensure compliance, and protect application workloads in dynamic public cloud networks. Compliance with industry regulations demands consistent security policies for cloud workloads. A breach could also affect one of the host clouds, increasing security risks to other applications and workloads. Enterprises need cloud workload protection solutions that help reduce risk from data breaches caused by unauthorized workload access within a multi-vendor public cloud environment.	ColorTokens Xshield delivers complete network visibility and cloud workload security based on a Zero Trust platform. It is infrastructure and network-independent, cloud-delivered, and enables workload protection in minutes. Xshield reduces the attack surface, improves overall security posture, and secures dynamic workloads as they move across a multi-vendor cloud environment and data centers. Xshield enforces least-privilege Zero Trust policies that dynamically adapt to cloud environment architecture changes and updates while staying compliant.

Proving Compliance

Challenges	ColorTokens Solution
Whether your organization is a brick-and-mortar business or has an online presence with e-commerce, achieving PCI compliance can be challenging. Merchants process cardholder data and store it across data centers and cloud platforms to the point of sale (POS) systems, PCs, and in-store kiosks. To avoid PCI violations, IT teams need to understand precisely where cardholder data flows, minimize access by users and applications, and scan their environments for vulnerabilities and unprotected paths to confidential data. To protect PII (Personal Identifiable Information) processing and storage servers against vulnerabilities and streamline PCI compliance, micro-segmentation is the right solution.	Achieving and supporting compliance with PCI standards can be challenging for any organization, regardless of size or industry. And even businesses that do manage to meet PCI requirements may find audits expensive, time-consuming, and stressful. ColorTokens helps enterprises address these challenges by simplifying ongoing PCI compliance, identifying changes in compliance scope, reducing the audit scope and time to audit, and accelerating any needed remediation. Our solution supports PCI cloud compliance, can enable merchants and retailers to prepare for their cloud transformation without added security or hardware requirements. ColorTokens Xshield micro-segmentation solution can see, stop, and predict security and PCI compliance violations across any workload, deployment, and user. It delivers a unified approach for organizations to simplify security and compliance across their hybrid infrastructures.

Preventing Lateral Movement

Challenges	ColorTokens Solution
Organizations have started to realize that perimeter security solutions are ineffective against preventing ransomware. The blurring of the perimeter has resulted in opening new entry points for cybercriminals to exploit. Once inside, ransomware spreads laterally to other endpoints and assets in the network if left undetected. Attackers focus on spreading the malware through lateral movement, making the perimeter security ineffective. Cybercriminals often exploit organizations using remote access tools for their employees and outsourced staff by gaining a more accessible path through a remote connection and crippling the system through lateral movement.	ColorTokens Xshield delivers real-time protection against ransomware in core data center and cloud workloads by segmenting and preventing lateral movement. Xshield helps prevent large-scale, costly corporate attacks with a software-defined micro-segmentation solution based on a Zero Trust architecture. The Zero Trust architecture works on the principles of least-privilege access to segment the network. The Zero Trust security model helps secure networks and workloads by restricting internet access, reducing the attack surface, preventing lateral infection, and stopping a ransomware attack efficiently.

Defending Legacy Systems Against Attacks

Challenges

Many organizations depend on legacy systems because they are hard to replace and many core enterprise applications still run on these legacy systems. Legacy solutions no longer receive technical support or O.S. patches/software upgrades and are vulnerable to cyberattacks that could compromise the entire network. With the cyber threat landscape evolving faster than security teams' ability to update and replace legacy systems, securing legacy systems against cyberattacks has become a key priority for organizations. Unsupported legacy systems allow attackers to infiltrate the network and move laterally to gain access to sensitive data and critical applications. With no support or patches to address these security vulnerabilities, legacy systems can put businesses at risk for costly data breaches. Hackers make use of the end-of-support dates available online to find zero-day exploits that are unpatched. Organizations must take the correct cybersecurity steps to keep operations running and prevent downtime, potential revenue loss, and regulatory penalties.

ColorTokens Solution

ColorTokens extends support to data center legacy systems, including vulnerable and unpatched applications running Windows 2003, XP, and above by performing identity-based segmentation and offering comprehensive network visibility. Many cybersecurity vendors do not support legacy systems beyond Windows 7, increasing vulnerability for customer assets that share applications or have traffic flowing in a hybrid environment. Our solution ensures that the customer can manage their unpatched systems without compromising the security of their assets or network. Our solution also investigates security issues while providing complete visibility and reducing lateral movement.

Supported workload OSes

Xshield agents for workloads are available for AIX, Linux, and Windows OS families.

OS Family	Supported Versions
Windows 32-bit	OS XP SP3 and above
Windows 64-bit	OS 2003 SP2 and above
macOS	OS 10.10 and above
Ubuntu	OS 12.4 and above
Redhat	OS 6.7 and above
CentOS	OS 6.7 and above
SUSE	OS 12 and above
AIX	OS 7.1
Sun Solaris	OS 10
Oracle Linux	OS 7.8 and above

Supported user OSes

Xshield agents for clients (end users) are available for macOS and Windows OS families.

OS Family	Supported Versions
MacOS	OS 10.10 and above
Windows 32-bit	OS 7 and above
Windows 64-bit	OS 7 and above

Start Free Trial

or send your query to info@colortokens.com

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.**

COLORTOKENS

Xprotect

DATASHEET

Hardened Endpoint Protection Based on Zero Trust

Highlights

- Protect fixed-function devices such as POS systems, ATMs, and kiosks from malware
- Reduce organizations' attack surface by only allowing company sanctioned applications
- Complement AV tools by mitigating zero-day attacks and advanced malware such as ransomware
- Complement EDR protections by reducing false positives and alert storms
- Enforce USB control to fortify endpoints
- Protect unpatched legacy systems, avoiding patch management costs and time
- Ultra-lightweight agent is non-intrusive, deploys in minutes with no business disruption

Traditional endpoint security is losing the battle with advanced ransomware and malware. In 2020 the average total cost of a data breach was $3.86 million USD. In 2021 ransomware attacks caused an average of $1.85 million USD damage to affected companies, with only 8% receiving all their data back even when paying the ransom. Corporate endpoints such as servers, laptops, desktops, and critical point of sales (POS) systems are often targeted to gain access to valuable network assets. These attacks persist even though most organizations have installed some form of traditional endpoint security controls. Endpoints are the most common and easiest way for ransomware and malware to enter your network.

Traditional security controls rely on signature-based techniques to detect known threats, utilizing signature database files accompanied by continuous scans to remove infected files. These traditional solutions are CPU-intensive, require constant connectivity, frequent updates, and are ineffective against file-less attacks. The newer generation of endpoint detection and response (EDR) security tools that combat file-less attacks are also network and data intensive. EDR tools function by recording every single activity at each endpoint, resulting in alert fatigue for analysts in security operations centers (SOC) and compromising an organization's security.

As part of the ColorTokens Xtended ZeroTrust™ cloud-delivered, software-defined platform, ColorTokens Xprotect utilizes a proactive Zero Trust architecture to provide complete process-level control for endpoints. In a Zero Trust architecture only good behavior is allowed and any deviations from normal behavior are automatically blocked. Xprotect is designed with intelligent algorithms for in-depth analysis of every running process and file present in the endpoint system. The running processes are analyzed with the known good processes and combined with contextual behavioral analysis to detect and stop suspicious activity. Xprotect enables businesses to easily deploy and manage endpoint security from the cloud-hosted console, providing real business value in minutes.

Centralized Web-Based Console

“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.”

– Uday Inamdar, CEO, ITCube Solutions Pvt. Ltd.

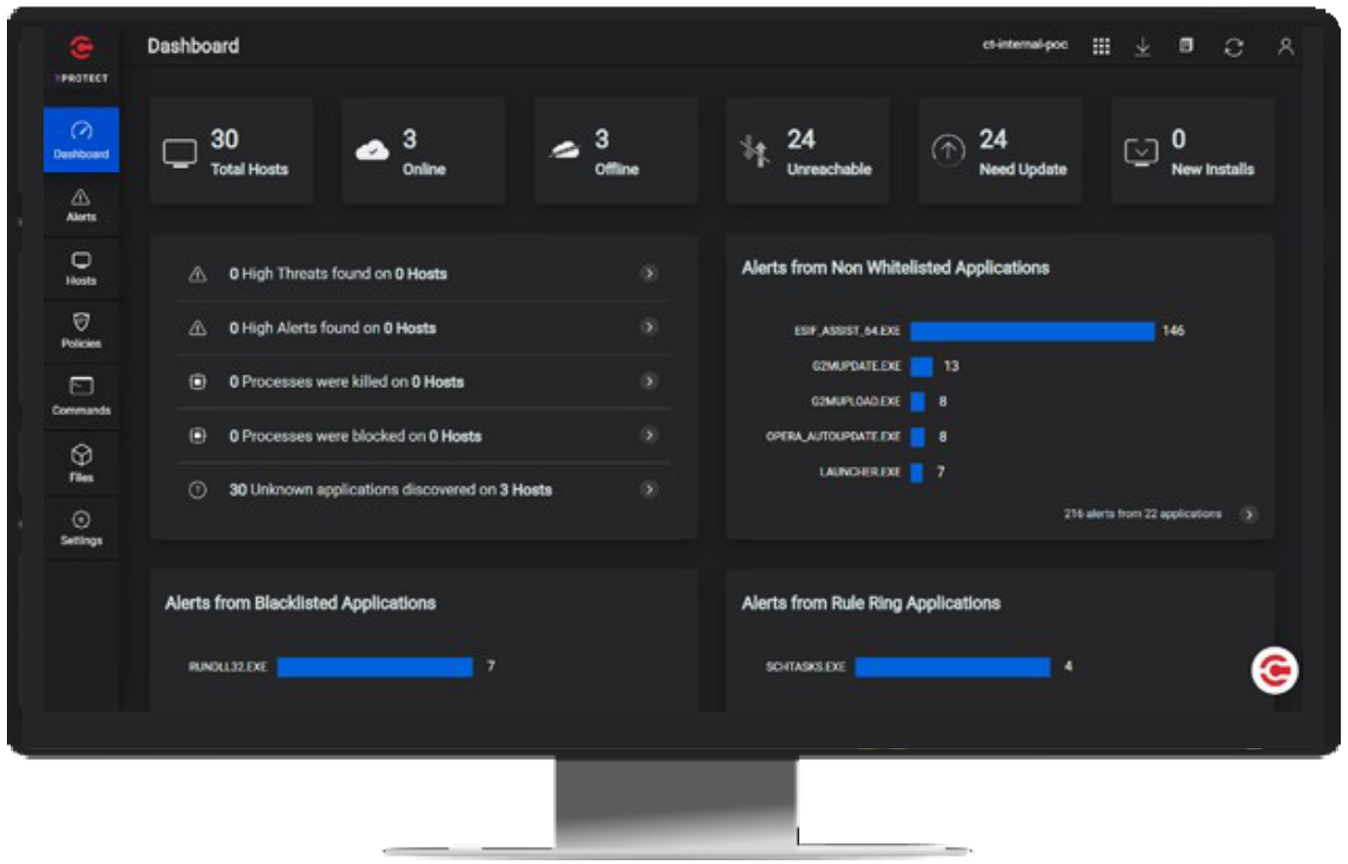


Figure 1: ColorTokens’ Xprotect’s graphical, intuitive dashboard simplifies monitoring and visualization of host statistics.

ColorTokens Xprotect Deployment

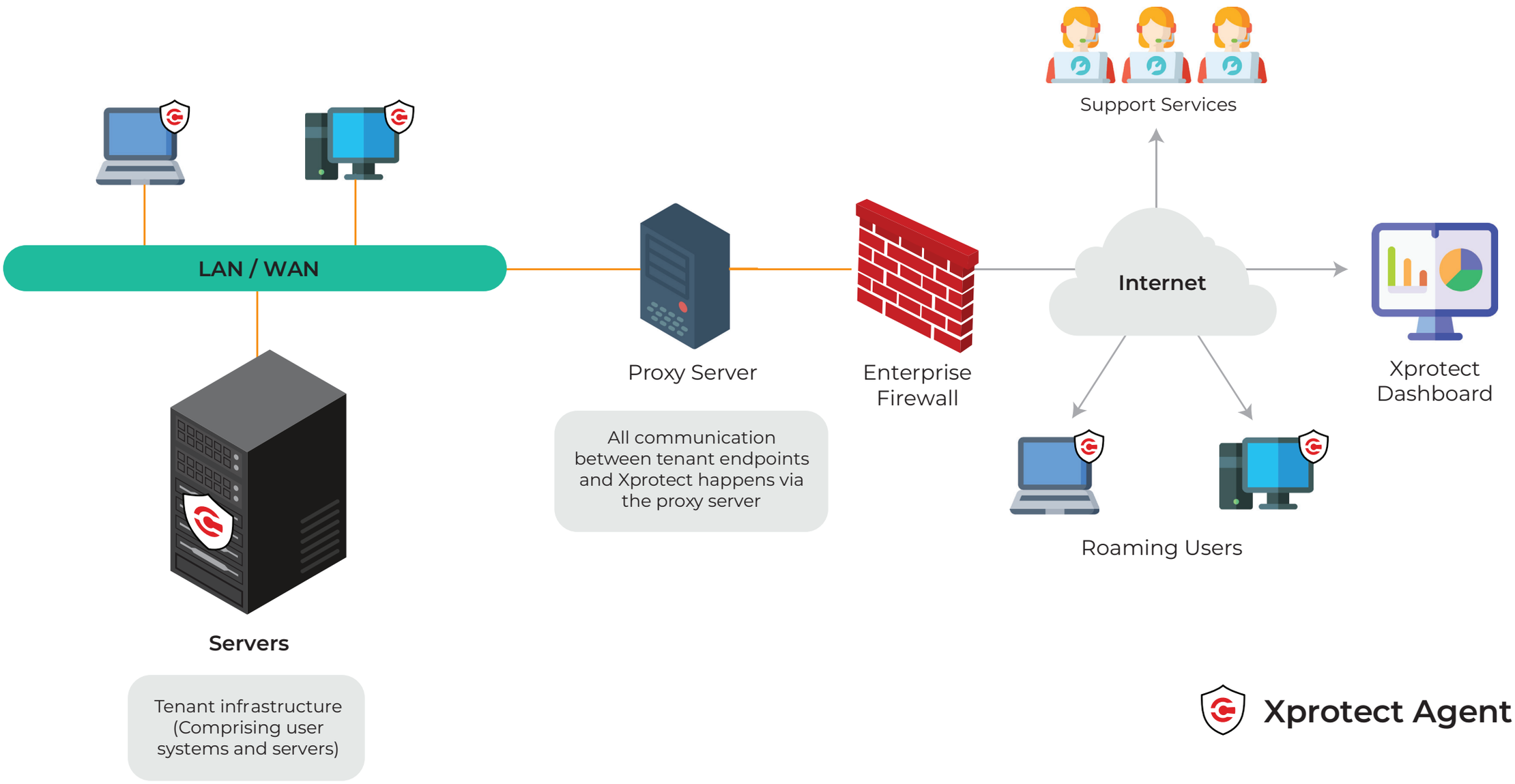


Figure 2: Xprotect is cloud-delivered and its ultra-lightweight agent can be deployed remotely and monitored centrally.

- **Xprotect Dashboard:** A centralized, web-based console provides full visibility and control of all assets in the network and processes running on every machine. The intuitive dashboard helps security professionals quickly view connectivity status with the tenant, agent status, and alerts. The multi-tenant dashboard provides key indicators and list widgets that display each tenant's critical metrics and the level of threat observed on the tenant's hosts.

- **Xprotect Agent:** Ultra-lightweight software agents are installed on endpoints. The agent contains built-in rules and configuration information, and incident logs are correlated within the agent. This architecture allows for offline protection of the endpoints, as the Xprotect agent has predefined security rules. Once the endpoint is back online, it sends all the telemetry data to the dashboard.

Xprotect Features & Benefits

Features	Benefits
Granular Process-Level Control	Allows administrators to dictate behavior at the process level for parent and child processes. Also provides visibility and the ability to lock down an endpoint at the process level.
Whitelisting & Blacklisting	Whitelist and/or blacklist known-good and known-bad processes based on behavior, path, or MD5 to prevent zero-day attacks, file-less malware, and unknown threats.
Freeze Mode	Tamper-proof endpoints, fixed-function devices, and legacy systems with a combination of whitelist, blacklist, and block modes to create a Zero Trust environment.
Rule Rings	Contextual behavioral rules allow the administrator to dictate behaviors for processes, including parent and child process behavior, network behavior visibility, and the ability to lock down an endpoint at the process level.
File Protect	Safeguard data by controlling process-level access to specific files or file types based on extension, directory, or path. As an example, only MS Word can be used to open word documents.
USB Control	Control USB access at the kernel level to make sure even system-level admin rights cannot bypass the enforced set of controls.
Security Incident Management	Fast query language (FQL) drastically simplifies the search and analysis of security incidents for IRC and SOC teams.
Agent Proxy	Agent proxy can be set up on a virtual machine, so that communication between air-gapped systems and ColorTokens security cloud can be routed via internal networks instead of the internet.
Auto-Scale	Eliminate manual handling of suspended instances in an auto-scale environment; users can enable auto-delete and configure the time for deleting instances, leading to more optimized use of resources.
User-Based Policies	Host-based policies give the ability to assign policies based on the current user logged in to the endpoint. This allows identity-based security settings for multiple users accessing the same endpoint machine.
RBAC	Role-based Access Control - Instance Admin, Policy Manager, Asset Manager, and Read-Only Admin is available for separation of duties when accessing Xprotect features.
Audit Logs	Keeps track of all operations performed via the Xprotect cloud dashboard, with detailed insights on who did what, and when, along with operation-related metadata. This is a must-have for compliance purposes.

Key Use Cases

Protect Fixed-Function Devices

Challenge

Point of sale (POS) and fixed-function retail systems have low memory, CPU, and storage, with typically low bandwidth connections. Traditional signature-based AV tools have a massive footprint, and EDR tools are bandwidth-hungry. These tools can often disrupt business and compromise the security of fixed-function devices.

ColorTokens Solution

Xaccess enables role- and identity-based secure access to distributed applications, cloud services, and workload segments across any public cloud, hybrid cloud, or data center with zero-complexity deployment and operations. The solution is software-defined, seamless across environments, and makes it easy to define and manage policies at scale across clouds. It is the only remote access solution that is integrated with workload-to-workload segmentation for maximum security of applications and services being accessed by internal and external users.

Endpoint Lockdown

Challenge

Businesses today want to control what runs on their fragmented endpoints for security and compliance reasons. However, legacy endpoint protection solutions can be cumbersome to implement, are very limiting in scope, and lead to business disruption.

ColorTokens Solution

ColorTokens Xprotect takes a Zero Trust approach to endpoint protection where only good application behavior is allowed, and any deviations from normal behavior are not allowed. The running processes are analyzed with the whitelisted processes and combined with contextual behavioral analysis to protect from advanced malware, ransomware, file-less attacks, and zero-day or unknown threats.

Ransomware Prevention

Challenge

Ransomware has been wreaking havoc on enterprises in recent years. Since 2017, the number of ransomware variants has quadrupled. Businesses and government agencies are all struggling to thwart ransomware attacks. These attacks are increasingly becoming more successful, rewarding, and challenging to track, causing substantial financial and brand damage to corporations.

ColorTokens Solution

ColorTokens Xprotect delivers real-time protection against ransomware, preventing attacks from becoming large-scale and costly corporate incidents. Xprotect effectively reduces the attack surface on an endpoint, contains and prevents the lateral spread by locking down the endpoint, and efficiently stops ransomware attacks by visualizing, intervening, and blocking unauthorized and malicious behavior during the ransomware attack phases.

ColorTokens Xprotect – Enhanced Protection for Endpoints

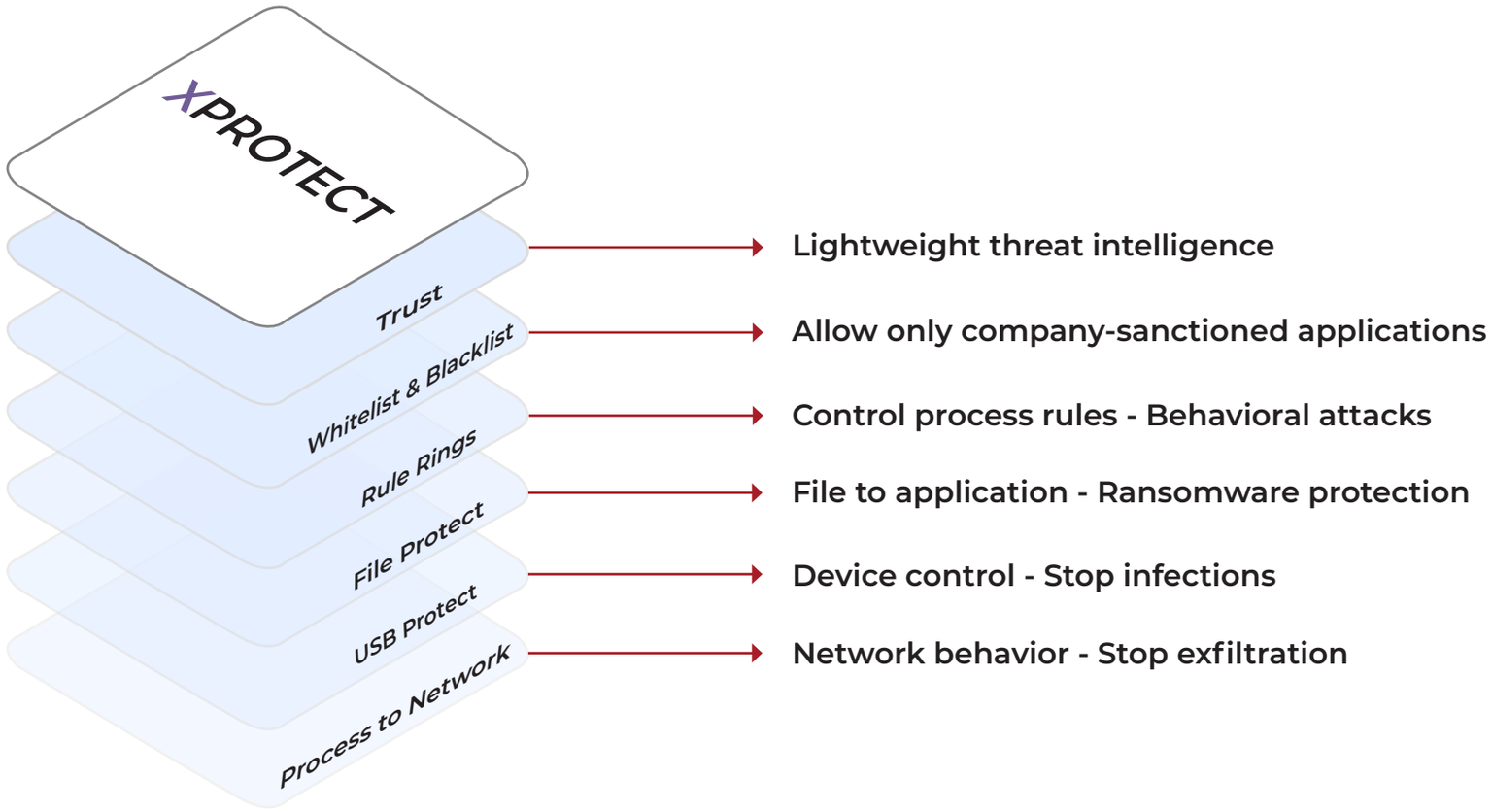


Figure 3: Multi-layer protection for endpoints.

Complement AV tools by ensuring zero-day attacks, malware and ransomware are thwarted

Proactive protection improves EDR performance by reducing false positives and alert storms

Protect fixed-function systems, legacy applications and unpatched endpoints unobtrusively and easily

Supported OS Versions

OS Family	Supported Versions
CentOS	6, 7
MacOS	10.14, 10.15
Red Hat Enterprise Linux	7
SUSE Linux	15.01
Ubuntu	14.04, 16.04, 18.04, 19.01
Windows 64-bit	Win XP SP3, Win 7 Professional with Security update KB4025341, Win 10 Pro, Win 2003 R2 Standard Win 2008R2 Enterprise - SP1 with patch KB4025341, Win 2008R2, Win 2012 R2 Standard

Minimum System Requirements

20Mb Ram

30Mb Disk Space

Minimum network bandwith (As there are no signature updates)

Start Free Trial

or send your query 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.

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.

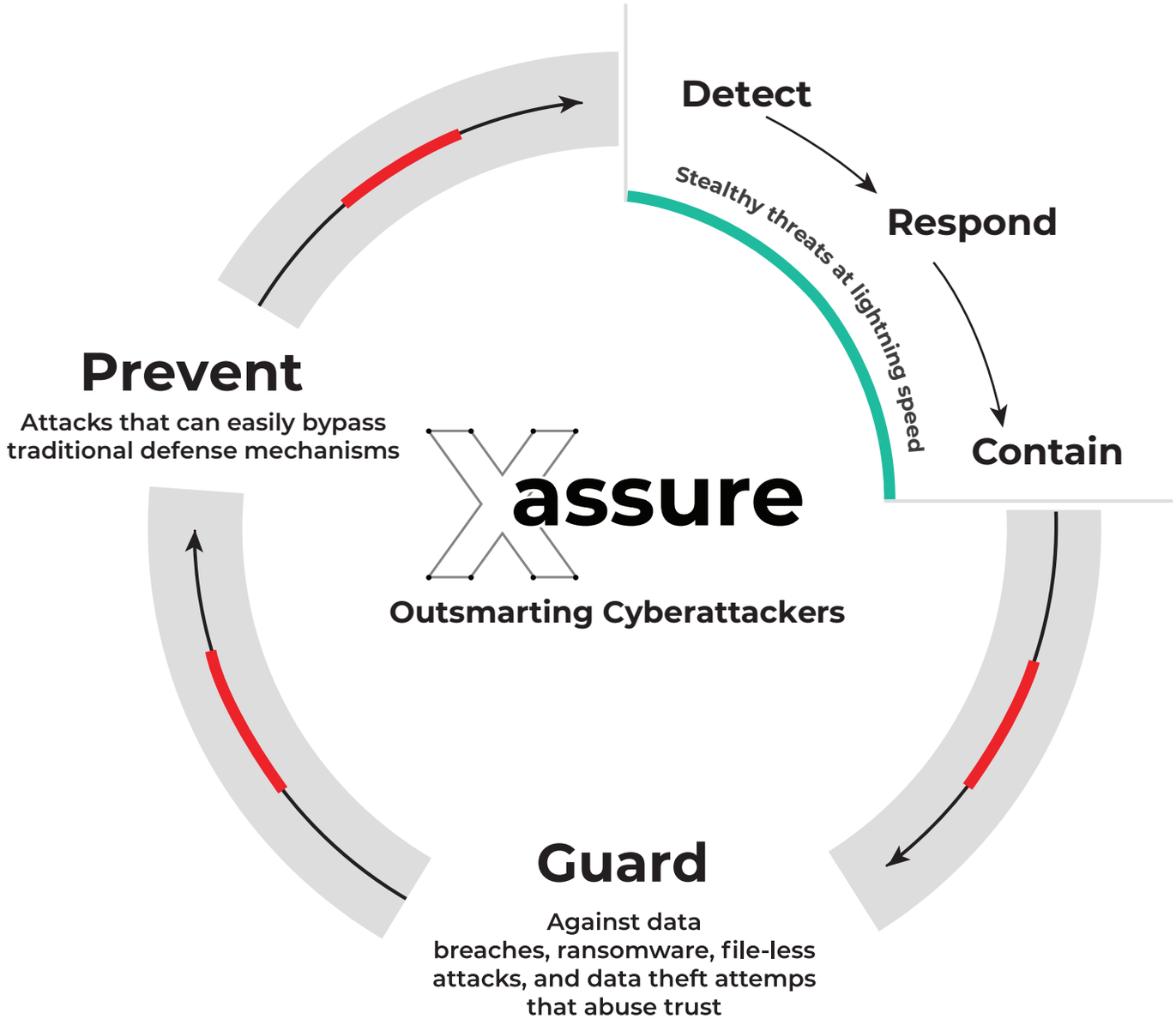
Today's threat landscape is constantly evolving, but many organizations still rely on traditional perimeter-based security and have resource-strapped IT teams, leading to poor visibility, slow investigations, and scores of false positives. Faced with such challenges, organizations, especially those on 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.”

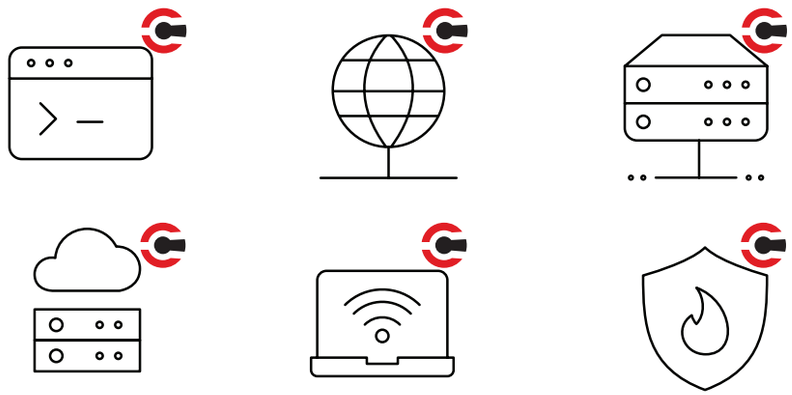
– CEO ITCube Solutions Pvt.

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.**