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.

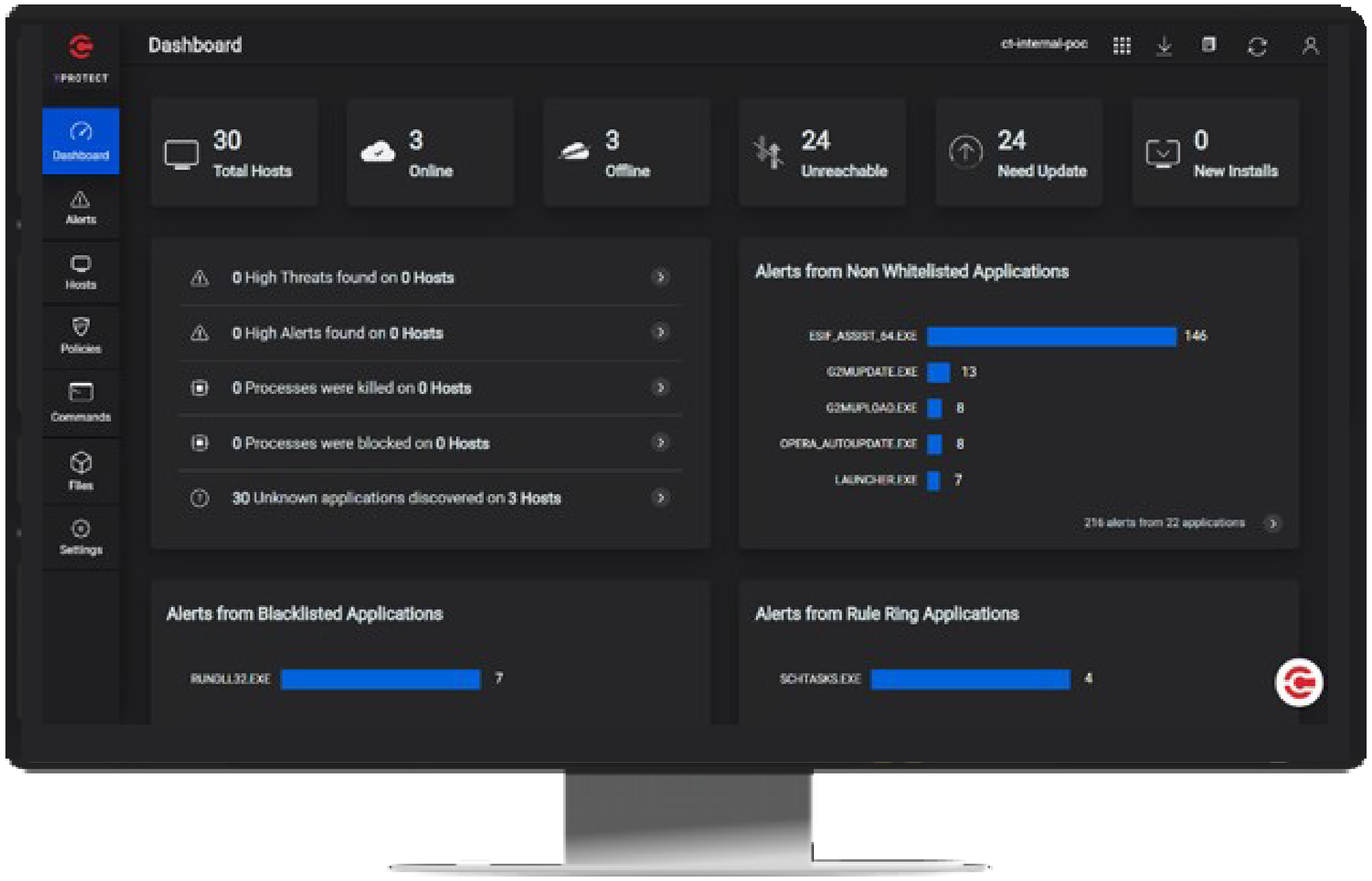
Traditional security controls rely on signature-based techniques to detect known threats, utilizing signature database files accompanied by continuous scans to remove infected files. These traditional solutions are CPU-intensive, require constant connectivity, frequent updates, and are ineffective against 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.



Dashboard

30 Total Hosts

3 Online

3 Offline

24 Unreachable

24 Need Update

0 New Installs

0 High Threats found on 0 Hosts

0 High Alerts found on 0 Hosts

0 Processes were killed on 0 Hosts

0 Processes were blocked on 0 Hosts

30 Unknown applications discovered on 3 Hosts

Alerts from Non Whitelisted Applications

ESIF_ASSIST_64.EXE	146
G2MUPDATE.EXE	13
G2MUPLOAD.EXE	8
OPERA_AUTOUPDATE.EXE	8
LAUNCHER.EXE	7

216 alerts from 22 applications

Alerts from Blacklisted Applications

RUNDLL32.EXE	7

Alerts from Rule Ring Applications

SCHTASKS.EXE	4

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

ColorTokens Xprotect Deployment

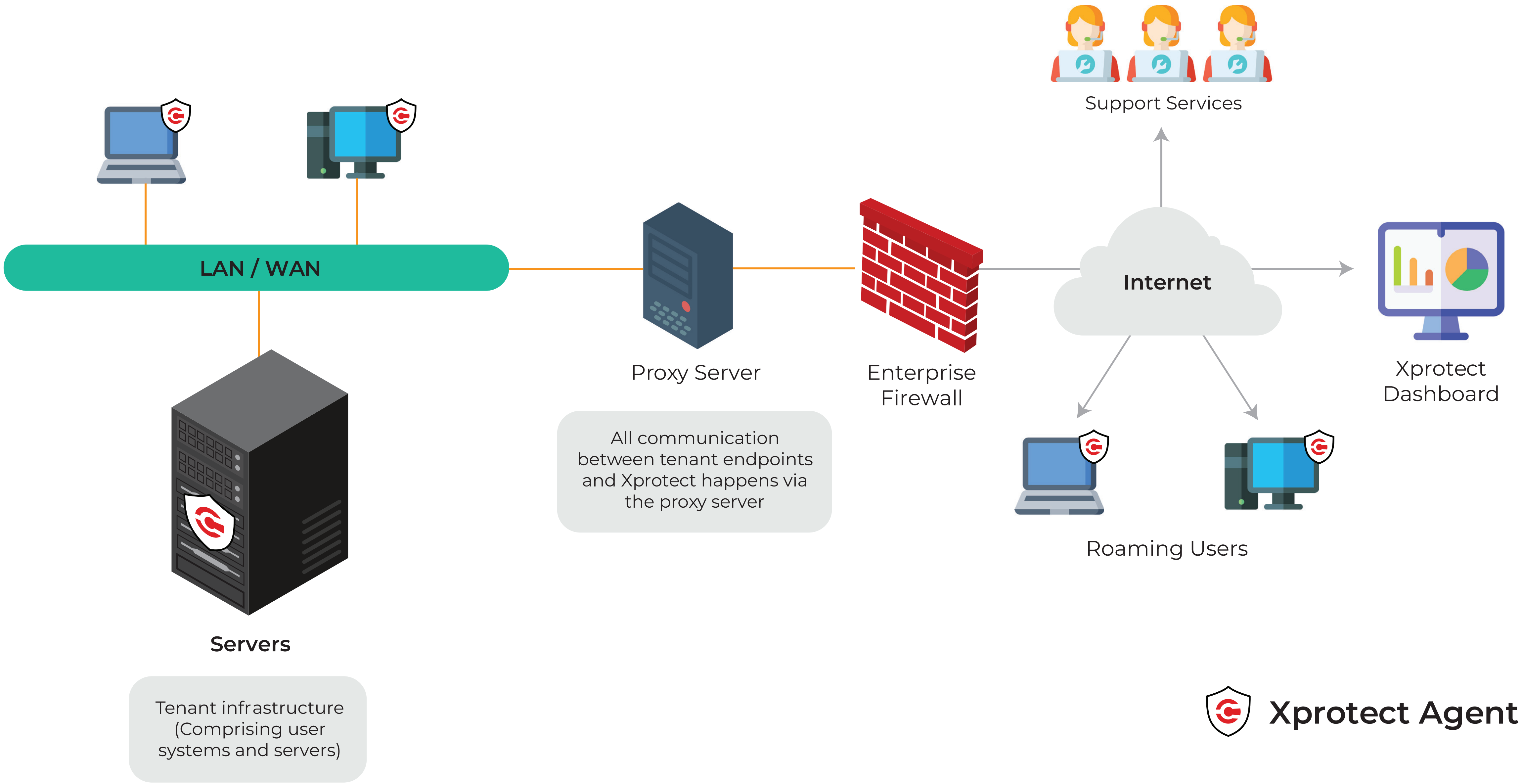

Support Services
LAN / WAN
Proxy Server
Enterprise Firewall
Internet
Xprotect Dashboard
All communication between tenant endpoints and Xprotect happens via the proxy server
Roaming Users
Servers
Tenant infrastructure (Comprising user systems and servers)
Xprotect Agent

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

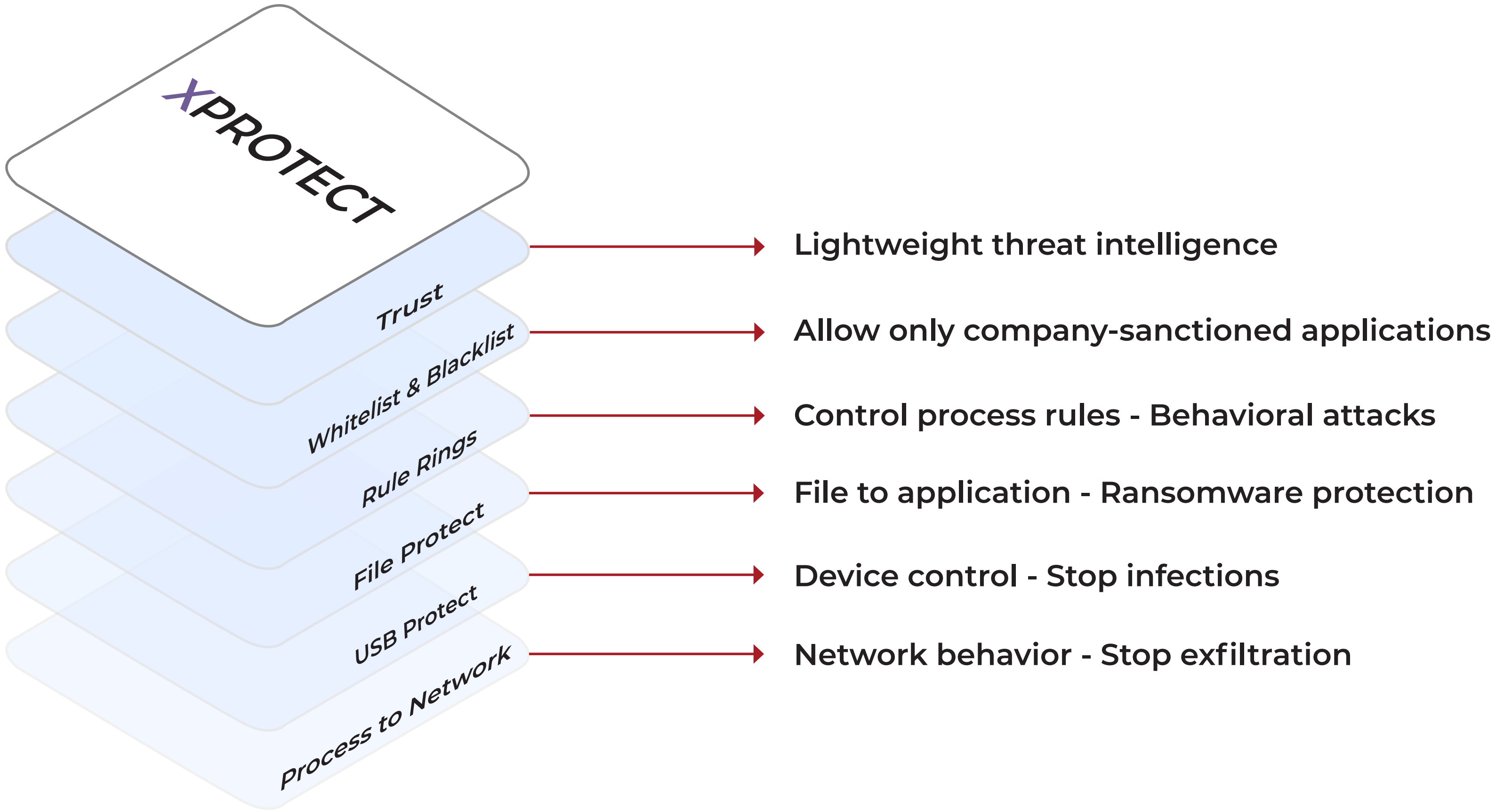
Challenge

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



Lightweight threat intelligence

Allow only company-sanctioned applications

Control process rules - Behavioral attacks

File to application - Ransomware protection

Device control - Stop infections

Network behavior - Stop exfiltration

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.