COLORTOKENS

DATA SHEET

Xprotect

Hardened Endpoint Protection Based on Zero Trust

Highlights

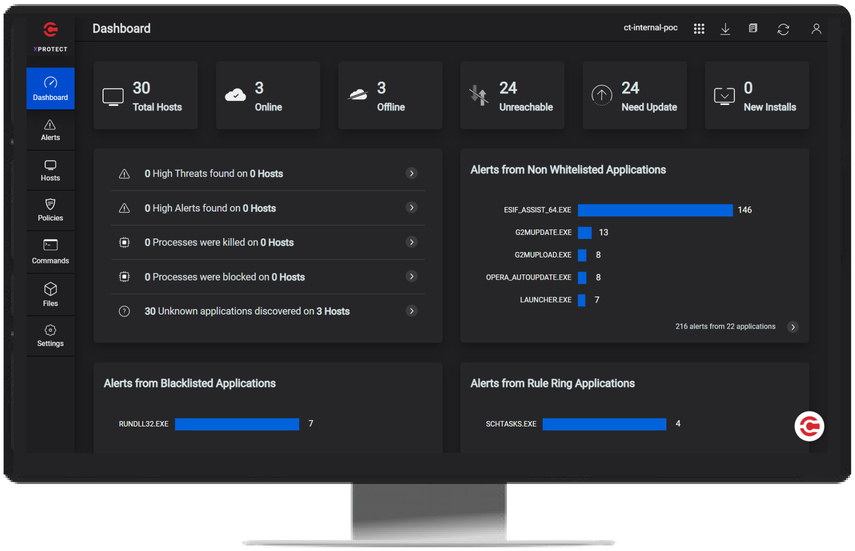
- Protect fixed-function devices such as POS systems, ATMs, and kiosks from malware
- Reduce organizations' attack surface by only allowing company-sanctioned applications
- Complement AV tools by mitigating zero-day attacks and advanced malware such as ransomware
- Complement EDR protections by reducing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

> "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.

Endpoints are the easiest way for ransomware and malware to gain entry into the network. There were 157,525 security incidents and over 108,069 data breaches in 2019. Over 70 percent of these attacks targeted corporate endpoints such as servers, laptops, desktops, and critical point of sales (POS) systems to gain access to valuable network assets — even though most organizations have installed some form of traditional endpoint security control.

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 and, moreover, ineffective against fileless attacks. The newer generation of endpoint detection and response (EDR) security tools combat fileless attacks but can be network- and data-intensive. EDR tools also have to record every single activity at the endpoint, resulting in alert fatigue for analysts in security operations centers (SOC) and compromising an organization's security. A proactive, Zero Trust approach to endpoint security can avoid alert fatigue and enhance user experience without compromising security.

ColorTokens Xprotect utilizes a proactive Zero Trust approach for endpoint protection where only good behavior is allowed, and any deviations from normal behavior are not allowed. The solution 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 or the whitelisted processes and combined with contextual behavioral analysis to detect suspicious activity. Xprotect enables businesses to block behavioral attacks using contextual security, and additionally fortify hardware entry points with USB lockdown.



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

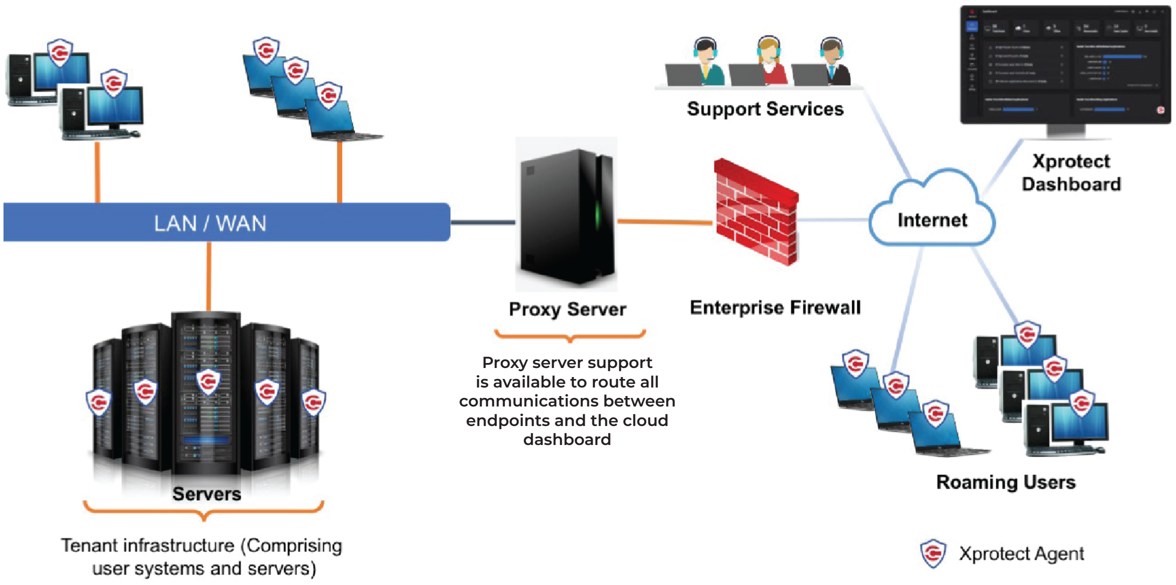
RUNDLL32.EXE	7

Alerts from Rule Ring Applications

SCHTASKS.EXE	4

Figure 1: Xprotect's graphic, intuitive dashboard simplifies monitoring and visualization of host statistics.

ColorTokens Xprotect Deployment



Proxy server support is available to route all communications between endpoints and the cloud dashboard

Tenant infrastructure (Comprising user systems and servers)

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, as well as 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 threats 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

Feature	Benefit
Whitelisting & Blacklisting	Whitelist and/or blacklist known-good and known-bad processes based on behavior, path, or MD5 to prevent zero-day attacks, fileless 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 and network behavior.
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.

Key Use Cases

Protect Fixed-Function Devices

Challenges	ColorTokens Solution
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 Xprotect is exceptionally lightweight and designed to operate on low CPU and memory devices while consuming significantly less bandwidth. Application whitelisting, blacklisting, and rule rings avoid the need for costly AV scans and excessive data transmissions typical of EDR solutions.

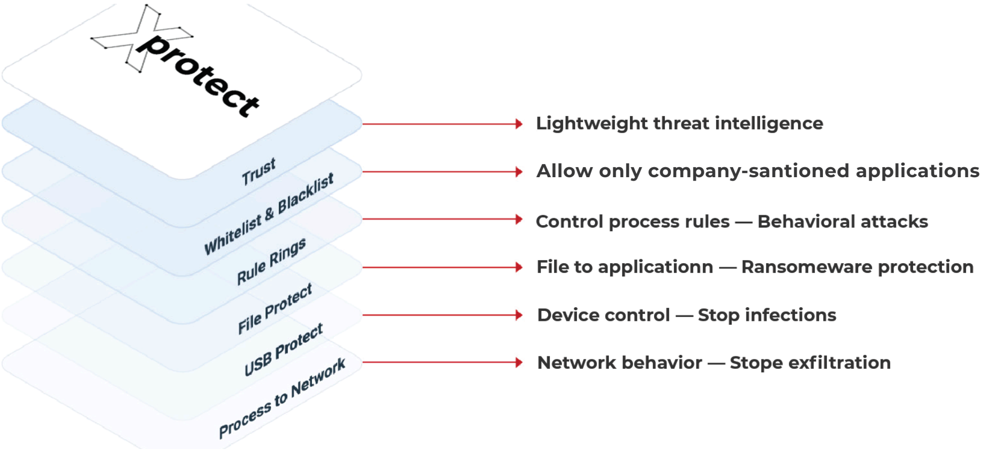
Endpoint Lockdown

Challenges	ColorTokens Solution
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 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 against advanced malware, ransomware, fileless attacks, and zero-day or unknown threats.

Ransomware Prevention

Challenges	ColorTokens Solution
Ransomware has been wreaking havoc on enterprises in recent years. Since 2017, the number of ransomware variants has quadrupled. Business 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 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-santioned applications

Control process rules — Behavioral attacks

File to applicationn — Ransomeware protection

Device control — Stop infections

Network behavior — Stope exfiltration

Figure 3: Multi-layer protection for endpoints.

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

Proactive protection makes EDR better by reducing false positives and alert storms

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

Minimum System Requirements

20Mb RAM
30Mb Disk space
Minimum network bandwidth (no signature updates)

Supported OS Versions

OS Family	Supported Versions
CentOS	6.7, 6.8, 6.9, 6.10, 7.2, 7.3, 7.6
MacOS	10.10, 10.11, 10.12, 10.13
Red Hat Enterprise Linux	6.7, 6.8, 7.2, 7.3, 7.4
SUSE Linux	12.4 SP4
Ubuntu	12.04, 14.04, 16.04, 18.04
Windows 32-bit	Windows XP, 7 Windows Server 2003 SP2, Server 2003 R2, Server 2008 SP1, Server 2008 SP2, Server2008 R2, Server 2019
Windows 64-bit	Windows XP, 7, 8, 8.1, 10, Windows Server 2003 SP2, Server 2003 R2, Server 2008 SP1, Server 2008SP2, Server 2008 R2, Server 2012, Server 2012 R2 and later, Server 2016, Server2019

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.