COLORTOKENS

# ColorTokens Xprotect for Endpoint Protection

## Xprotect Highlights

- Easy-to-deploy cloud-delivered solution
- Tamper resistance lockdown
- Protect multiple platforms
- No AV tools required
- No signature updates required
- Protect unpatched or unpatchable systems
- Ultra-lightweight agent

Today's threat actors are becoming increasingly innovative, while endpoints remain one of the weakest links affecting an organization's security posture. Users pose a significant challenge to security, as modern businesses require them to work from anywhere, with access to critical data and applications – hosted both on-premises and in the cloud. Traditional signature-based AV and EDR tools cannot provide holistic awareness into user, application, and process behavior.

Xprotect for Endpoint Protection – part of the ColorTokens Spectrum Platform – provides enterprises with a robust signature-less approach that works at the kernel level to block unauthorized processes on endpoints, servers, and legacy/fixed-function systems. Xprotect scrutinizes all endpoints with intelligent algorithms for in-depth analyses into every running process – as well as files present in the machine. With whitelisted and/or blacklisted processes, combined with contextual behavior analysis, all suspicious activities are proactively stopped.

### Get stress-free security with one click

Visualize, define, and protect all of your endpoints, down to the individual processes

- Get consistent and uninterrupted endpoint protection, even when users are offline
- Define whitelists or blacklists for process chains and application behavior
- Deploy a cloud-delivered, ultra-lightweight agent with a single click – all while remaining invisible to users

### Implement extended endpoint protection

Hunt down and respond to zero-day threats by isolating and killing bad processes

- Go beyond signature-based security that blocks only 'known-bad' threats with powerful whitelisting
- Prevent unauthorized software execution on endpoints – even with administrator rights
- Block malicious processes from spawning and infecting legitimate applications

### Lock down legacy and fixed-function systems

Maximize uptime of critical legacy systems without degrading performance

- Protect legacy Windows and Linux systems from malware, ransomware, and fileless attacks
- Allow only known, well-behaved files, processes, memory and network connections
- Secure special-purpose terminals such as ATMs and POS systems running unpatched applications

COLORTOKENS

## Xprotect Benefits

- Multi-platform support
- Reduce patch management headache
- Cost-effective proactive protection for critical assets
- Minimal resource utilization

“

ColorTokens is the ONLY vendor that understands the customer limitations and is proactively managing the situation. Others just blame us”

– CIO of a multi-billion-dollar fashion retailer

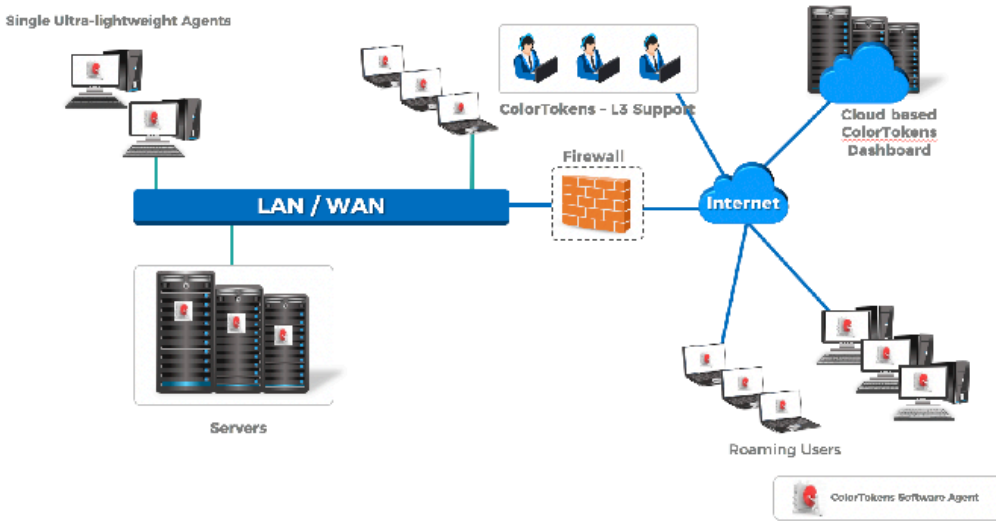
**Xprotect**

Windows XP, Windows 7, Windows 7 Embedded (32-bit & 64-bit), Windows 8, Windows 8.1, Windows 10, Windows Server 2003 (32-bit & 64-bit), Windows Server 2008 (32-bit & 64-bit), Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, CentOS (6.7, 6.8, 7.2, 7.3), RHEL (6.7, 6.8, 7.2, 7 .3), Ubuntu (12.04, 14.04, 16.04), Mac OSX, for remote access. Agents consume less than 1% CPU utilization and 30 MB RAM.

**Agent**

Xprotect console is, cloud-delivered from AWS (m5.4xlarge instance, 100 GB storage), the console requires a Google Chrome browser, version 58 or higher

# Protect any endpoint. Kill all malware.




## Key Features

**Intuitive web-based console for centralized visibility and control:** Detect and prevent threats happening on any endpoint or critical server with granular visibility and kernel-level control over all running processes.

**Whitelist/blacklist for process protection:** Whitelist/blacklist known-good/known-bad processes based on behavior, path, or MD5 to prevent zero-day, fileless malware, and other unknown threats.

**Freeze mode:** Tamper proof endpoints, including legacy/fixed-function systems, with a combination of whitelist, blacklist, and block modes to create a zero-trust environment.

**Process-level firewall:** Granular control over IP, port, and protocol for individual processes, preventing unauthorized inbound and outbound connections.

**File protect:** Control process-level access to specific files or file types based on extension, directory, or path to protect data in sensitive files.

**USB control:** Control USB access at the kernel level to make sure even system level admin rights cannot bypass the enforced set of controls.

ColorTokens Spectrum Platform delivers proactive security from the data center to edge, including public clouds. Engineered to the NIST-ZTA (Zero Trust Architecture) standards, ColorTokens defends organizations from internal and external threats. The award-winning cloud-delivered platform enables security and compliance professionals with real-time visibility, workload and endpoint protection, and zero-trust network access – while seamlessly integrating with existing security tools. For more information, please visit www.colortokens.com.