Xprotect

ZERO-TRUST ENDPOINT & SERVER HARDENING

Why Zero Trust?

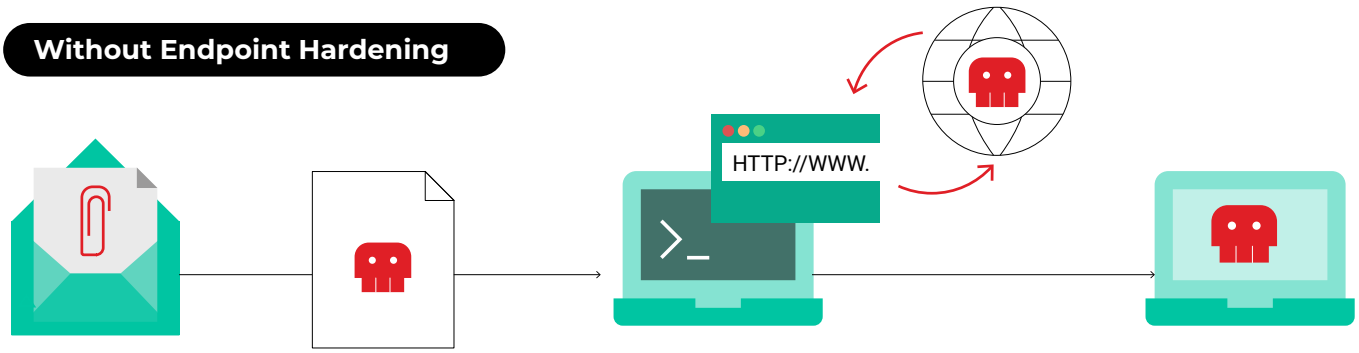
Traditional approaches to cyber-security employ a "perimeter defense" methodology, using hardware firewalls and anti-virus signature scanning to protect against attacks from the external internet. The problem with this approach is that the adversary only has to be lucky once; the defenders must be right every single time. In contrast, the Zero Trust security approach assumes the adversary is already inside your perimeter; internal users, programs and processes are not to be trusted by default. Xprotect is part of Colortoken's suite of components that can simplify your journey to a complete Zero Trust architecture.

Adding Device Hardening to your Endpoint Protection

Xprotect gives you server & endpoint device hardening through whitelisting of applications and their child processes. It executes the Zero-Trust methodology by first observing the normal application usage in your business processes, and then only allowing those necessary processes to run. Therefore, it stops malicious processes and programs from running, by default, even if a novel malware has evaded the scanning of traditional anti-virus, Endpoint Protection (EPP) and Endpoint Detection & Response (EDR). This makes device hardening an important addition to your total cyber defense strategy.

ⓘ By its nature, EDR is responsive; in contrast, device hardening is proactive.

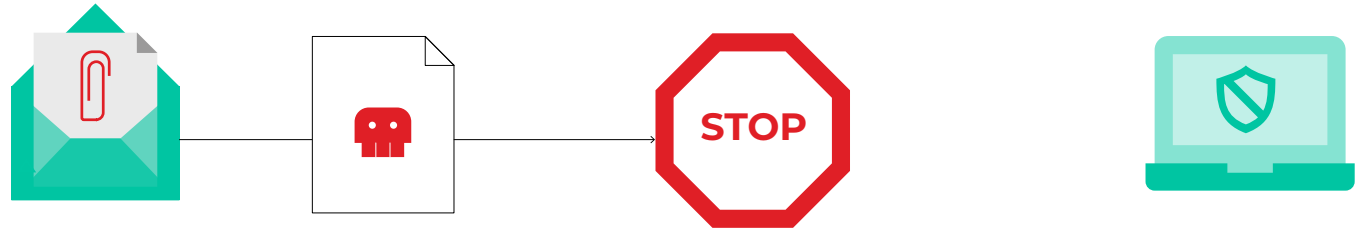
Without Endpoint Hardening



Victim opens document with novel attack unknown to anti-virus

Malicious script connects with remote web server and runs PowerShell

Xprotect Endpoint Hardening



Malicious process is blocked since it is not whitelisted

Support for Legacy Systems and Special Purpose Devices

Many environments include special purpose devices such as point-of-sale or medical devices or even general-purpose computers running older versions of operating systems (such as Windows XP and Windows Server 2003) that are no longer supported and/or patched by the manufacturer, and which have not or cannot be upgraded. Many EDR and anti-virus solutions will not run on those older operating systems environments. Xprotect allows you to harden those legacy devices through whitelisting.

Central Governance of Whitelisting Policy

Xprotect comes with out-of-the-box templates for policies, so your security team is not starting from a blank slate. First run Xprotect in assimilation mode, so it can baseline what processes are needed during your normal business workflows; after that, lock it down. If a non-whitelisted process attempts to run, Xprotect blocks it and generates an alert. If the users want a policy change to allow that process to run, only a few clicks are needed for the security team to convert that into a policy for that particular group. This makes it easy to respond to your users' requests for permission to download and run new software on their endpoint devices, as well as for your security team to harden your servers.

Very Lightweight Agent

Xprotect's agent typically consumes less than one percent of CPU cycles and it is only about 30 megabytes in size. It will not adversely affect end-users' device performance; nor will it interfere with your existing EDR agents on endpoints and servers.

USB Security

Xprotect locks down the USB ports with fine-grained controls for read/write, execute, and delete.

File Protection

Xprotect lets you define which processes and what users are allowed to access sensitive files--even if that user is an admin role. You can protect your "crown jewel" data from local admin user access.

Contextual Whitelisting Rules

Xprotect lets you specify allowed parent-child relationships between processes. Malware often takes advantages of system processes like PowerShell and DASH etc. With contextual whitelisting, you can stop bad actors from using these utilities by creating "rule rings" which define who or what can launch a process, and what that that process can invoke downstream.

Simplifying Your Journey to Zero-Trust

Device hardening supports one pillar in the Zero Trust Maturity Model defined by the Cybersecurity & Infrastructure Security Agency. (https://www.cisa.gov/zero-trust-maturity-model) In addition, ColorTokens can help as you progress along the Maturity Model with components for network Micro-Segmentation, Zero-Trust Network Access, Cloud Configuration Security and Container Security. With ColorTokens, you can implement zero-Trust incrementally, without disruption to your business.