ENDPOINT ZERO TRUST

What to Expect for Users

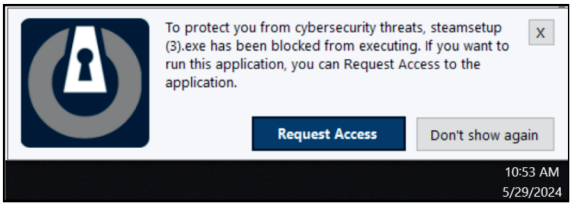
WHY IS ENDPOINT ZERO TRUST IMPORTANT?

As ransomware, malware, and data encryption have become more prevalent over the past few years, organizations of all sizes and industries must add additional layers of security to ensure safety of their organization's data.

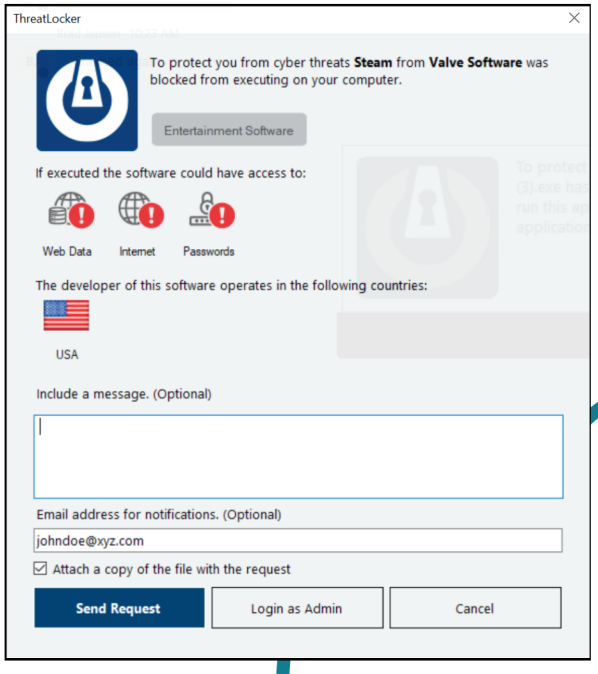
Although we may call this service "Zero Trust", it doesn't mean YOU are not trusted! "Zero Trust" is instead referencing applications and other types of software. In today's cybersecurity climate, all sorts of bad players can be hiding in an enticing application promising to make your job easier. This service allows your IT Team to ensure you only have the applications or software you need, and puts a streamlined process in place for you to request access when you are needing to install additional items on your machine. It's a win-win solution - removing headaches from you and your IT Team, and removing risk from your organization.

HOW TO REQUEST A NEW APPLICATION

When you try to install a new application/software, you will receive the pop-up images below. Simply click on the "Request Access" button and include a message to your IT Team. (Elevation Control Requests follows a similar request process.)



Once approved, most applications will automatically restart the installation process. Please note, some applications may require you to start the install process again.



NETWORKS PLUS

ENDPOINT ZERO TRUST

Onboarding Expectations

01

INSTALLATION

The Networks Plus team rolls out inital deployment to endpoints. Users will not notice any changes other than a new icon in the system tray.

02

THE LEARNING PERIOD

The tool will be observing all applications installed and running in the environment for approximately 14-21 days. All systems must be powered on for a few hours each day during this period.

03

CREATING POLICIES & ALLOW LISTS

The Networks Plus team will create new policies and allow lists based on the applications identified and the system audits. We will reach out to the client on applications we feel are questionable.

04

SWITCHING TO SECURE MODE

Any applications not approved will now be blocked unless allowed by the Cyber Hero (NOC) or Networks Plus team.

05

FOLLOW ESCALATION PROCESS AS NEEDED

Requests for new applications or policy changes will follow the escalation process below:

1. User submits escalation request for a new application or policy change.
2. If the application policy already exists, or the new application is a known business application, the Cyber Hero Team will automatically update the policy.
3. If the request is for an unknown application or the legitimacy is questionable, the escalation will be assigned to the Networks Plus team for review and resolution.
4. Any application that does not appear to fill an obvious business need will need to be approved first by the partner.

NETWORKS PLUS