THREATLOCKER®

X

INDIANAPOLIS COLTS

Case study

How the Indianapolis Colts use ThreatLocker® Allowlisting and Ringfencing™ to get control of their environment

Overview: A stronger baseline

The Indianapolis Colts needed greater control over the software operating across their environment. Their security team wanted a trusted application baseline that would support Zero Trust principles without disrupting football operations, travel workflows, or day-to-day productivity.

With ThreatLocker Allowlisting and Ringfencing they had a platform that helped to centralize control, reduce risk, and streamline the security stack while keeping users fully productive.

> What sets ThreatLocker apart is how much they lower the barrier to entry. It is designed to integrate seamlessly into an environment, allowing you to baseline known-good activity on a device. That means you minimize disruption to business operations while still continuously improving your security at a highly granular level.
>
> — Jack Thompson,
> Director of Information Security

WHY ALLOWLISTING AND RINGFENCING™?

The Colts' IT and security teams faced a common enterprise issue:

They did not have a complete or reliable inventory of the software running on endpoints. Staff worked in many locations, often on the move, making it difficult to ensure that devices were not running unauthorized or potentially harmful applications. This created a reactive security posture and increased operational risk.

SECURITY SOLUTIONS DESIGNED TO BE PROACTIVE

ThreatLocker® Application Allowlisting and Ringfencing helped the Colts establish a known-good baseline of approved applications. The platform made it possible to identify unexpected software, approve new tools efficiently, and control how applications interact with each other. The Cyber Hero® Team supported the deployment and provided ongoing expertise as the Colts refined their security architecture.

With a trusted application baseline and stronger control over endpoint behavior, the organization shifted from reactive security to a proactive Zero Trust posture. ThreatLocker minimized user disruption, streamlined approval workflows, and reduced tool sprawl by centralizing key functions in one platform. The Colts' security team gained the visibility and control needed to operate confidently across stadiums, training facilities, and travel environments. "With ThreatLocker, we have the ability to centralize disparate elements in the security stack, and support from the ThreatLocker Cyber Hero Team is bar none." **— Jack Thompson, Director of Information Security.**

> Three of the best things about ThreatLocker are the **support from the Cyber Hero Team**, the ability to **increase your security posture** while minimizing negative business impact, and the way it **streamlines your security stack** by consolidating disparate tools.
>
> — Jack Thompson,
> Director of Information Security

ALLOWLISTING AND RINGFENCING — A ZERO TRUST APPROACH.

Discover the features that gave the Indianapolis Colts control of their environment.

Allowlisting

Deploy in Learning Mode

Automatically catalog all apps and dependencies. With 10,000+ of pre-built apps recognized, you'll gain immediate visibility, streamline your application list (a potential major efficiency across your organization), and get policy suggestions on the fly. No more manual list building or creating policies from scratch, a significant reduction in your operational burden.

Approve what you need

Select the apps you want to run and approve them with one click. From now on, no unapproved apps, scripts, or libraries can execute.

Easily add new apps

When needed, users request new app access via a popup. IT can approve internally, or ThreatLocker can handle it for you through Cyber Hero Approvals or Cyber Hero MDR team, that responds in minutes. With the ThreatLocker User Store, users swiftly access trusted apps or alternatives for minimum operational disruptions without compromising your Zero Trust environment.

Ringfencing

Deploy with strong, default protections

Need PowerShell to run, but not reach the internet? Done. Want Word to open documents, but never launch another app? Easy. These powerful out-of-the-box rules let you control hundreds of applications, so they behave exactly the way you want.

Bonus: ThreatLocker 24/7 Cyber Hero Team is always on hand to help you fine-tune policies fast, responding in just minutes.

Customize with high granularity

Decide which files your applications can access, which programs they can interact with, and whether they can connect to the internet. Restrict scripts, block unauthorized process launches, and prevent apps from sending data outside approved channels.