THREATLOCKER®

X

ORLANDO MAGIC

Case study

A Zero Trust approach to controlling applications in a high-speed sports environment

The Orlando Magic uses ThreatLocker® to lock down application behavior, shrink the attack surface, and streamline how users request the tools they need.

EXECUTIVE SUMMARY:

Industry:
Professional sports and entertainment

Location:
Orlando, Florida

ThreatLocker solutions used:
Application Allowlisting, Ringfencing™, Storage Control, Elevation Control, Network Control, Configuration Manager

Outcomes:

- Faster, more consistent approval and deployment of applications.
- Fewer support tickets related to non-business software.
- Automated analysis and control of application behavior, saving IT significant time.
- Stronger cyber insurance position through clearer controls and better auditability.

Orlando Magic challenges and ThreatLocker® solutions

Challenge	Solution
Growing application sprawl and expanding attack surface.	Application Control lets the team specify exactly which applications can run and for whom.
Manual testing of new applications to understand risk.	Allowlisting and Ringfencing™ automate evaluation and control, replacing guesswork with defined policy.
No structured workflow for user software requests.	ThreatLocker gives end users a clean request process that reduces noise in the help desk.
Need to support insurance requirements with better visibility.	Detailed audit data provides insight into what ran, how it behaved, and where controls blocked risk.
Desire for a security partner that keeps innovating.	ThreatLocker focus on identifying and blocking existing exposures aligns with the Magic's culture of innovation.

REAL-LIFE APPLICATIONS

Centralized approvals for fast, secure deployment

With ThreatLocker, the Magic's technology team can approve an application once and safely roll it out across the organization or to a targeted set of users. Deployment and protection happen in the same workflow.

Automated controls that cut support tickets

Before ThreatLocker, the team had to install each application, observe its behavior, and manually assess its risk. Allowlisting and Ringfencing now automate that process, eliminating guesswork and sharply reducing tickets generated by users requesting personal or non-essential tools.

Visibility and assurance for leadership and insurers

ThreatLocker gives the Magic the ability to see if something happened on a laptop and also to deeply understand what happened, and how. That visibility strengthens internal confidence and supports the Magic's cyber insurance posture.

> The ThreatLocker culture of innovation matches our culture of innovation, and that is critical for us.
>
> — Jeff Lutes
> Executive Vice President
> of Technology

About ThreatLocker

ThreatLocker is a global cybersecurity leader helping organizations proactively stop cyberattacks. The ThreatLocker Zero Trust Platform features Allowlisting, Ringfencing, and Network Control to prevent breaches before they happen, including zero-day attacks, through an allow-by-exception approach that's straightforward to deploy, scale, and manage to keep business operations running uninterrupted. Built for simplicity, scalability, and speed, ThreatLocker security stack reduces complexity, accelerates compliance, and empowers businesses to take control of their cybersecurity—before threats strike. Headquartered in Orlando, Florida with a growing global footprint, ThreatLocker protects millions of networks and endpoints worldwide. Major partners include JetBlue, Heathrow Airport, the Orlando Magic, and the Indianapolis Colts. The company was recently ranked among the top performers on the Inc. 5000 list of fastest-growing private companies.