



# Group Tyre Strengthens Security, Reduces Risk, and Reclaims Time With ThreatDown

**UK tire wholesaler reduces patching time by 95%, achieves government certification, and builds security team with ThreatDown's unified platform.**

Group Tyre Wholesale Ltd. has been supplying tires to independent garages and national chains across Southeast England since 2010. From their head office in Aylesbury and satellite depot in Potters Bar, the company supports thousands of customers with multiple deliveries each day. With roughly 150 endpoints the business operates in a fast-moving environment where uptime and continuity are essential.

## Where security gaps created operational risk

When John Kingman, Chief Technology Officer, joined the company, he was a one-person department responsible for everything from infrastructure to cybersecurity. Legacy antivirus software only detected threats after scheduled scans, patching required days of hands-on work each month, and the environment grew more complex each year. By 2020, Group Tyre entered a period of significant digital transformation, modernizing its warehouse systems and mobility workflows.

**With ThreatDown, we operate with real-time visibility and far greater confidence that nothing critical is slipping through.**

**John Kingman**  
Chief Technology Officer

Kingman knew the company needed stronger, faster, and more unified protection. He also knew he needed a way to scale security without adding complexity or taxing his lean resources. That search led Group Tyre to ThreatDown.

## Regaining time by automating vulnerability and patch management

For years, Kingman struggled with limited threat visibility from his previous security tools. ThreatDown EDR and its integrated patch and vulnerability management changed the equation. "Our previous solution wasn't identifying threats on our network as quickly as it needed to," Kingman said. "With ThreatDown, we operate with real-time visibility and far greater confidence that nothing critical is slipping through."

**Group Tyre**  
Wholesale Ltd



## Customer-at-a-glance

**Customer** - Group Tyre

**Industry** - Tire Wholesale/Distribution

**Country** - United Kingdom



## ThreatDown Solutions

ThreatDown Ultimate, including:

Endpoint Protection

Endpoint Detection & Response

Managed Threat Hunting

Managed Detection & Response

Application Block

Firewall Management

Vulnerability Assessment

Patch Management

DNS Filtering

Premium Support

**Plus, Email Security and**

**Mobile Security**

Plus, ThreatDown's automated vulnerability scans uncover outdated software and missing patches across the environment. Built-in policies then keep devices current without constant intervention.

The operational impact was immediate and measurable. Tasks that once consumed 40 hours a month now required only a few hours of exception handling. "Before ThreatDown, I lost an entire week every month to patching. Now I spend a few hours on exceptions, and the rest simply runs," said Kingman.

The impact extended beyond time savings. Automated remediation empowered Kingman to focus on higher-value digital transformation projects, including the company's modern warehouse management system and expanded mobility footprint. It also made it possible to bring on an apprentice and ramp him up on the ThreatDown platform. The Nebula console was intuitive enough that a junior team member could support day-to-day security tasks without extensive instruction.

## Results

- **Automated patching** reduced monthly workload from 40 hours to a few hours
- **Response times improved** from one hour to minutes with MDR
- **Unified platform** reduced investigation time and simplified operations
- **Email threats blocked** before reaching users, reducing phishing risk
- **Supported Cyber Essentials Plus** certification by strengthening baseline controls
- **Enabled a lean IT team structure** by making it practical to hire and train an apprentice

**ThreatDown MDR gave me my nights and weekends back. Alerts move from detection to triage in seconds—I wouldn't even have my laptop open by that point.**

**John Kingman**  
Chief Technology Officer

This shift—from firefighting to proactive maintenance—gave Group Tyre a stronger, more predictable security baseline and freed IT resources to support the company's broader growth strategy.

## Building 24/7 Security Coverage With MDR and Reducing After-Hours Incidents

As the business grew, there was one unavoidable reality: Nights, weekends, and holidays left the company without anyone monitoring activity. Kingman couldn't be everywhere at once, and cyber threats don't respect business hours.

ThreatDown MDR provided the coverage he needed. With round-the-clock monitoring, AI-driven triage, and ThreatDown's expert security analysts validating and containing threats in minutes, the company gained the continuous protection it previously lacked.

"ThreatDown MDR gave me my nights and weekends back. Alerts move from detection to triage in seconds—I wouldn't even have my laptop open by that point," said Kingman. "Now, when an alert is raised, I know it's already being worked by the ThreatDown team. And quite often, when I review MDR cases, they've been dealt with in the first minute."

Previously, even false alarms forced Kingman to interrupt his evening, boot up his laptop, VPN into the network, and investigate. Now, the MDR team handles the initial assessment and response, escalating only when human intervention is truly required. The result is continuous coverage with far less operational drag—and the confidence that threats are addressed even when the internal team is offline.

## One Console, One Partner: Reducing Complexity and Improving Visibility

With multiple device types, remote staff, and an expanding attack surface, Group Tyre needed a more unified security model. Before ThreatDown, endpoint data, email filtering, and threat indicators lived in separate tools. Investigations meant jumping between consoles, reconciling logs, and manually stitching together fragments of the story.


ThreatDown consolidated endpoint telemetry, detection data, software inventory, email indicators, and DNS filtering into a single platform. That shift simplified daily operations and materially improved how the team visualized threats across the environment.

“Security breaks down when visibility is fragmented,” said Kingman. “With ThreatDown, we have one consolidated view across endpoint, email, and network activity—and that’s transformed how we investigate and respond. ThreatDown enables us to move faster, investigate with confidence, and explain risk clearly at the executive level.”

This consolidation strengthened Group Tyre’s security posture and provided the reporting clarity needed for board-level updates. Reports generated from MDR cases enable Kingman to explain incidents and outcomes without manually assembling logs or timelines.

## ThreatDown Email Security That Catches What Microsoft Misses

As attackers adopted AI-generated phishing lures and more convincing credential-harvesting pages, Group Tyre saw a rise in suspicious emails slipping past Microsoft 365’s default filters. These threats were polished, subtle, and increasingly difficult for employees to identify.



With ThreatDown, we have **one consolidated view** across endpoint, email, and network activity—and that’s transformed how we investigate and respond. ThreatDown enables us to **move faster, investigate with confidence, and explain risk clearly at the executive level.**

**John Kingman**  
Chief Technology Officer

ThreatDown Email Security immediately revealed the scale of the problem. Within its first scan, it identified phishing attempts, spoofed Microsoft login pages, and suspicious sender patterns that had previously reached user mailboxes.

“ThreatDown Email Security gives us confidence that high-risk messages are stopped before employees ever see them. It adds real depth to how we defend the business,” said Kingman.

The team uses ThreatDown Email Security findings as a training opportunity, walking employees through real examples and reinforcing how modern phishing attempts disguise themselves. ThreatDown’s quarantine and review model also give IT greater control, preventing risky messages from reaching end users and reducing the chance of accidental compromise.

The improvement directly addressed a critical business risk. Group Tyre had previously encountered a highly convincing “executive impersonation” attempt targeting their accounts team. Although the attempt was caught before it could do damage, it underscored how easily a single email could lead to financial loss. ThreatDown’s email threat analysis and detection prevent similar scenarios from gaining traction.

## Achieving Cyber Essentials Plus Certification

As Group Tyre strengthened its security program, the company decided to pursue Cyber Essentials Plus, a UK government-backed certification that involves hands-on technical validation from a third-party assessor to verify controls and confirm that the environment meets defined security standards.

ThreatDown's visibility, automated patching, and continuous monitoring gave Kingman confidence ahead of the assessment. Routine scans surfaced issues early, MDR reduced exposure, and the unified console made it easy to show that the environment stayed in a healthy state.

"When we went through Cyber Essentials Plus, it was clear how much ThreatDown had already done for us. The platform kept our endpoints clean and our exposure low, and it played a major part in passing the certification," said Kingman.

Earning Cyber Essentials Plus gave Group Tyre a reliable benchmark for its security posture and a defensible standard to maintain year after year.



[threatdown.com](https://threatdown.com)



[sales@threatdown.com](mailto:sales@threatdown.com)