Case Study

ThreatDown
Powered by Malwarebytes

IT LeasingTeam Strengthens Security and Streamlines Management with ThreatDown

IT LeasingTeam is a staffing agency based in Poland, delivering temporary and long-term employment solutions for both local and international clients. Their business spans a wide range of roles, from executives to IT professionals, with additional HR and payroll services, as well as the provision of IT services. Technology is central to their operations: advanced recruitment platforms and custom-built applications enable the company to streamline placements and manage contracts digitally.

The company supports 200 users working in hybrid mode. Their environment consists of 180 workstations and 15 servers, nearly all running Windows. The IT team carries the responsibility for security across the business.

> "ThreatDown was the first solution we tested that actually found and neutralized the crypto virus we'd been hit by—before it could start encrypting. This real-world validation proved the platform could stop attacks that their previous solution had missed entirely."
>
> **Łukasz Dąbrowski, System Administrator**
> **IT LeasingTeam**

The Breaking Point: When Prevention Fails

Before turning to ThreatDown, IT LeasingTeam relied on a legacy antivirus solution. The solution's limitations became catastrophically clear during a ransomware attack that crippled operations and forced the IT team into crisis mode.

"We were hit by a cryptographic attack and noticed that our previous antivirus, waited until after our files were encrypted before classifying it as a virus," said Łukasz Dąbrowski, System Administrator at IT LeasingTeam. This reactive approach meant malware could complete its destructive work before detection triggered—exactly the opposite of what endpoint protection should accomplish.

ITLT

Customer-at-a-glance

Customer - IT LeasingTeam
Industry - Staffing & HR Services
Country - Poland

ThreatDown Solutions

ThreatDown Ultimate, including:

- Endpoint Protection (EP)
- Endpoint Detection & Response (EDR)
- Managed Detection & Response (MDR)
- Vulnerability Assessment
- Patch Management
- DNS Filtering

The incident forced a massive recovery effort. As a precautionary measure, the team reinstalled nearly 150 workstations since they couldn't determine which systems were infected. For the IT team, this represented weeks of lost productivity and demonstrated how inadequate security controls compound operational costs.

Additionally, the previous solution created persistent management challenges. The antivirus platform featured only a local console, which meant the team couldn't effectively manage remote endpoints. Client updates failed regularly, particularly on machines outside the corporate network. Cross-domain license management proved clunky and time-consuming. These limitations cost the team several hours each week in routine maintenance.

> "We saw right away that ThreatDown's ransomware protection was different. It detected the crypto virus in real time and neutralized it before it could do any harm. That's the reason we chose it."
>
> **Łukasz Dąbrowski, System Administrator**
> **IT LeasingTeam**

Results

- **Zero major infections** since deployment
- **5 hours per week reclaimed** for IT staff
- **Support tickets reduced** from 150/year to just a few
- **No endpoint issues** flagged in recent security audit
- **WSUS server retirement** through integrated patch management
- **Improved work-life balance** with 24/7 MDR coverage

Solution: One platform for protection and management

The cryptographic attack forced IT LeasingTeam to establish clear evaluation criteria for a replacement solution: reliable threat detection, centralized management capabilities, and robust ransomware prevention that actually works before damage occurs. After researching options, they began testing multiple vendors, including ThreatDown, against their specific requirements.

ThreatDown distinguished itself immediately during the proof-of-concept phase. The team tested the platform against the same crypto virus that had previously infiltrated their environment—and ThreatDown detected and neutralized the threat before any encryption could begin.

"ThreatDown was the first solution we tested that actually found and neutralized the crypto virus we'd been hit by—before it could start encrypting. This real-world validation proved the platform could stop attacks that their previous solution had missed entirely," said Łukasz.

Effectiveness was the deciding factor, but ThreatDown's unified architecture sealed the decision. The ThreatDown Ultimate bundle consolidates next-generation endpoint protection, EDR, MDR, vulnerability assessment, patch management, brute force protection, and DNS filtering into a single cloud-native solution. This consolidation gives the IT team the ability to manage broad security responsibilities without added complexity.

Stopping ransomware before it starts

Since deployment, IT LeasingTeam has not experienced another serious security incident. What previously constituted high-stakes events requiring system rebuilds now amounts to routine quarantine of potentially unwanted programs—automated responses that require no IT intervention. The team estimates they've achieved a 99% reduction in actual security incidents, with remaining alerts typically involving user attempts to access blocked websites rather than malware infections.

“We saw right away that ThreatDown’s ransomware protection was different. It detected the crypto virus in real time and neutralized it before it could do any harm. That’s the reason we chose it,” Łukasz shared.

The shift from reactive to proactive defense fundamentally changes IT LeasingTeam’s security posture. ThreatDown prevents malicious execution from the start rather than relying on post-infection detection. This delivers steadfast protection that eliminates the cascading operational costs that follow successful attacks—no emergency response protocols, no forensic analysis to determine infection scope, and no mass system rebuilds.

Consolidating management into one console

ThreatDown transformed how IT LeasingTeam manages security across their hybrid environment. Previously, keeping endpoints current required multiple management interfaces, individual server logins for updates, and extensive troubleshooting when remote machines failed to synchronize properly with corporate security policies.

The most significant operational improvement came through integrated patch management. IT LeasingTeam had previously relied on Windows Server Update Services (WSUS) to distribute patches across their environment—a solution that required dedicated server resources, ongoing maintenance, and manual intervention when updates failed on remote endpoints.

> “With ThreatDown, we simply stopped worrying about cyberattacks—ThreatDown just works, and the time and stress saved is immeasurable. We receive email notifications about all events that interest us, such as malware detection or the quarantine of an unwanted application, which means we only need to log in to the console when we want to make changes.”
>
> **Łukasz Dąbrowski, System Administrator**
> **IT LeasingTeam**

“ThreatDown Patch Management is a real difference-maker for us,” said Łukasz. “We were able to remove the WSUS server entirely. Now, instead of logging into each system, we apply updates with a simple checkmark.” This consolidation eliminated the need for dedicated patch management infrastructure while providing superior visibility into update status across the company’s distributed endpoints.

The cloud-based console also solved cross-domain management challenges that had plagued the previous solution. With ThreatDown, the IT team can now manage servers and workstations across multiple domains—and devices without domain membership—through a single interface. This unified approach eliminated repetitive configuration tasks and reduced the potential for errors when managing security policies across different network segments.

Reclaiming Time for Strategic Work

Before ThreatDown, the IT team spent considerable time maintaining their security infrastructure. Client updates failed regularly, requiring manual intervention. The local-only management console meant time-consuming individual system logins for routine tasks. Cross-domain functionality gaps forced the team to repeat identical configurations multiple times across different network segments.

Users also submitted a steady stream of security-related support tickets—approximately 10-15 per month covering maintenance issues, failed updates, and user-reported problems with the antivirus platform. These interruptions fragmented the team's attention and prevented focus on higher-value projects.

ThreatDown eliminated this operational overhead. Support tickets related to security dropped from 150 per year to just a few annually, usually tied to blocked websites. The team estimates they've reclaimed at least five hours each week—time now invested in strategic IT initiatives rather than security maintenance.

"With ThreatDown, we simply stopped worrying about cyberattacks—ThreatDown just works, and the time and stress saved is immeasurable. We receive email notifications about all events that interest us, such as malware detection or the quarantine of an unwanted application, which means we only need to log in to the console when we want to make changes," explained Łukasz.

The efficiency gains extended beyond IT operations. Employees no longer lose productivity due to reimaging or infection-related downtime. In the company's most recent security audit, not a single endpoint security issue was flagged, which is a clear indication that the ThreatDown investment is delivering measurable risk reduction.

24/7 Coverage: Adding Managed Detection & Response

One year after adopting ThreatDown, IT LeasingTeam expanded their security posture with ThreatDown Managed Detection & Response services. For the IT team, the appeal of expert monitoring around the clock was immediate and compelling.

Previously, security alerts after hours or on weekends meant interrupted personal time with the company's internal IT team serving as first responders for all security events, regardless of timing or severity.

"Before, we were always first on the line. The ThreatDown MDR service not only saves us time, it gives us peace of mind during our time off. We know that someone is watching and will act if there's a problem," Łukasz shared. ThreatDown's MDR team now triages events, escalates only when necessary, and takes containment actions when threats require immediate response. This professional support enables the internal team to focus on other IT projects while maintaining confidence that security incidents won't go undetected or unaddressed.

Łukasz points to the MDR team's responsiveness as another proof point. "We rarely need to contact them, which shows how well the service runs. When we have, the support has been excellent."

The combination of ThreatDown's powerful software and 24/7 oversight from the MDR security experts has given IT LeasingTeam a level of resilience they couldn't achieve on their own. It has also restored confidence that their business, employees, and clients are protected if a threat arises.