MSP

2025 STATE OF RANSOMWARE

Inside a **record-breaking year** of ransomware attacks

THREATDOWN™

Contents

Introduction

In the 12 months from July 2024 to June 2025, ransomware attacks increased 25% year-over-year. In that time, 41 new ransomware groups emerged, active groups topped 60 for the first time, 42 countries recorded their first ransomware incident, and February 2025 became the worst month on record, with over 1,000 attacks.

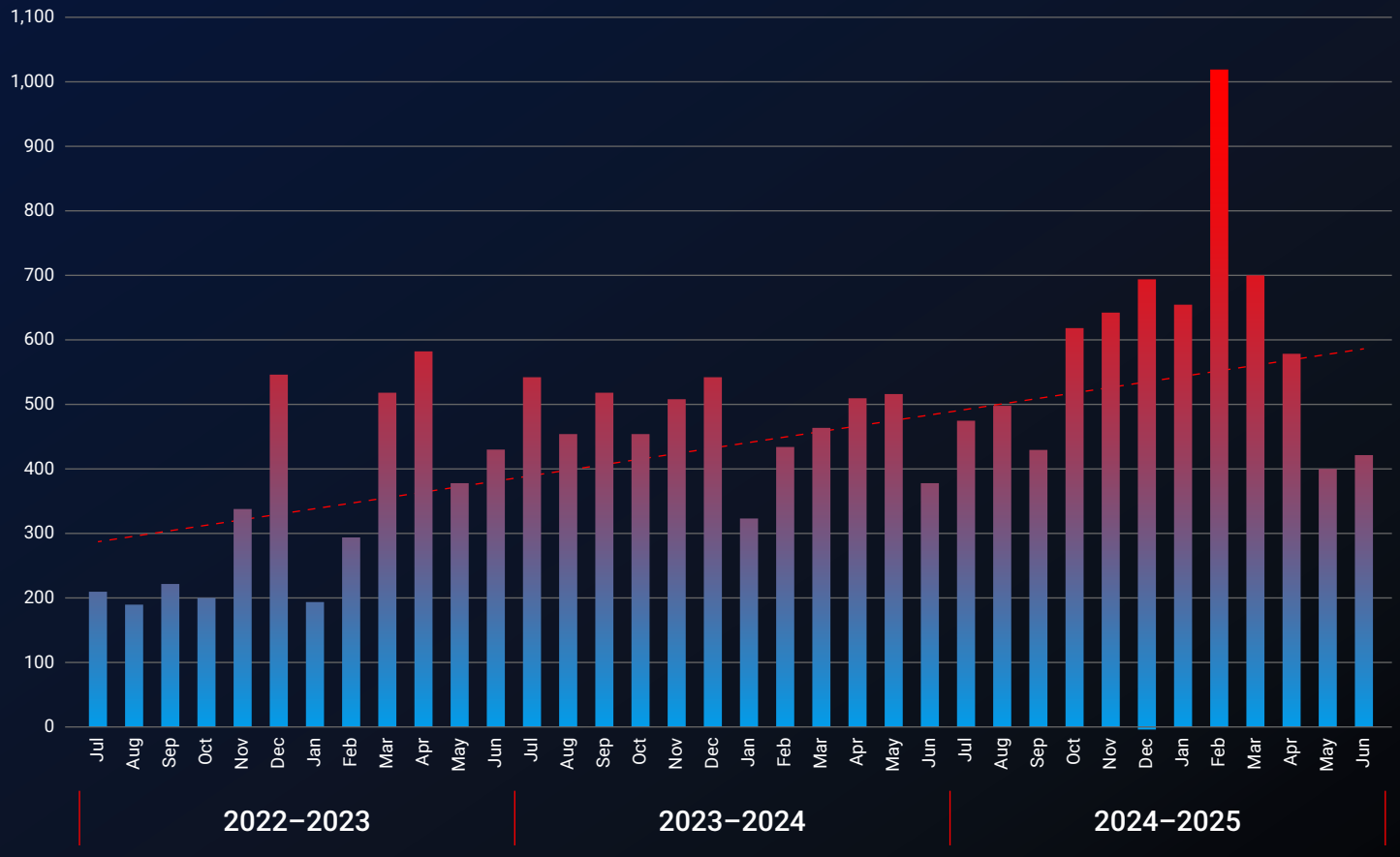
Behind the numbers, real people suffered. In June 2024, an attack on a blood-test provider, Synnovis, harmed 170 patients and caused one of the first deaths officially linked to ransomware.[1] The Frederick Health cyberattack in January 2025 exposed 934,000 highly sensitive patient records.[2] In April 2025, a ransomware attack wiped more than $930 million from Marks & Spencer's market value.[3]

And in June 2025, attacks on Kettering Health and Nucor disrupted 14 hospitals across Ohio and forced temporary shutdowns at steel production facilities.[4,5]

Yet there are reasons for optimism. Criminal groups increasingly use legitimate software, strike at night, and target blind spots to avoid detection. These tactics show that ransomware cannot thrive in the daylight created by endpoint detection and response (EDR). Criminals either try to avoid detection entirely or gamble that alerts won't be addressed quickly enough.

As ransomware tactics evolve, so too must defenses. This report explores the current landscape, the forces shaping it, and how organizations can build resilience.

Known ransomware attacks per month

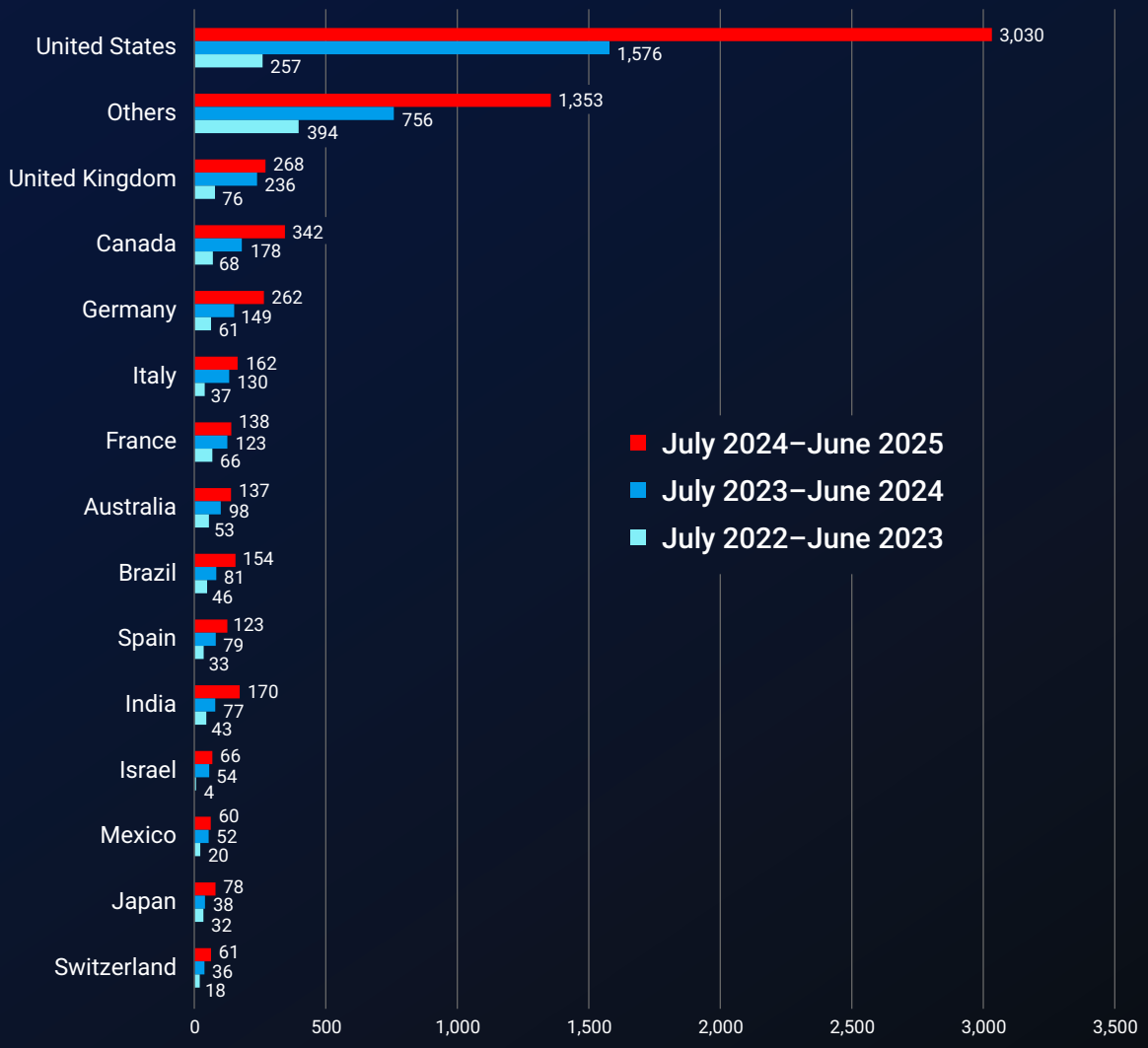


The ransomware ecosystem

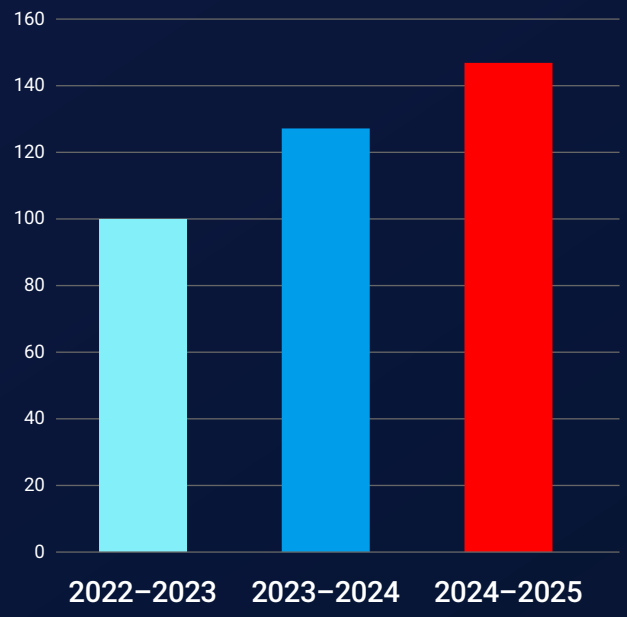
Over the past 12 months, the United States maintained its position as the biggest ransomware target, accounting for 47% of known attacks. Ransomware groups continued their preference for English-speaking countries and Western Europe, with notable campaigns like Scattered Spider's early 2025 attacks on UK retail. Among the victims, Marks & Spencer reported £300 million in lost profits[6], while the Cooperative Group disclosed that data from 6.5 million members had been compromised.[7]

However, ransomware is spreading beyond its traditional strongholds. In the past year 42 previously unaffected countries experienced their first ransomware attack in the last 12 months, and the number of countries fighting off ransomware attacks has increased 46% over three years. Rather than reflecting defensive improvements in established targets, this expansion likely reflects ransomware's inevitable spread through an increasingly digitized global economy.

Known ransomware attacks by country



Distinct countries experiencing ransomware attacks per year, July 2022 - June 2025



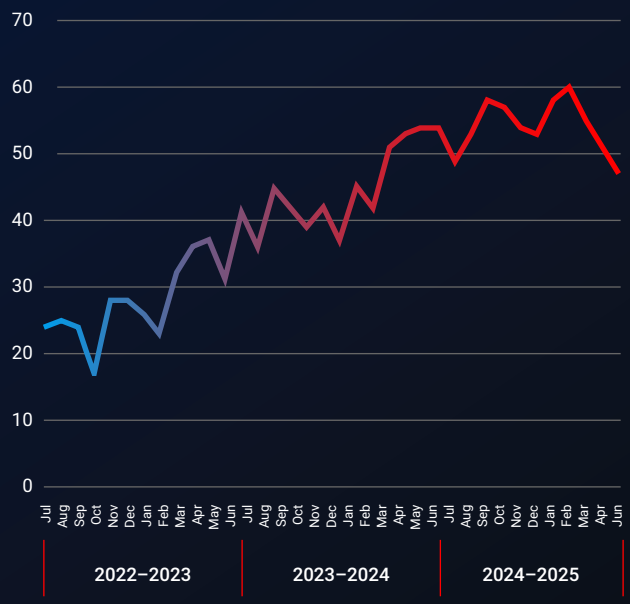
The balance of industries targeted remained largely unchanged, with the services sector hit hardest. Healthcare continued to be a prime target for ransomware groups, and in a world desensitized to the effects of cyberattacks, attacks on hospitals continued to shock.

In June 2024, the Synnovis attack in London caused severe diagnostic delays and one of the first deaths officially linked to ransomware. A month later, McLaren Health Care in Michigan saw nearly 750,000 exposed patient records.[8]

Groups

The increase in ransomware attacks over the last three years has been driven by a steady month-on-month increase in the number of active ransomeware groups, which has doubled in that time. Whether this reflects more participants or smaller group sizes, it suggests that something—perhaps a mix of domain experience, commoditized malware, and abundant AI—is lowering the barrier to entry.

This steady growth in active ransomware groups has been fueled by consistent patterns of formation, closure, and activity. Over the last three years, approximately 50 new groups have appeared each year, around 30 have exited, and a typical group has attacked around five targets per month.

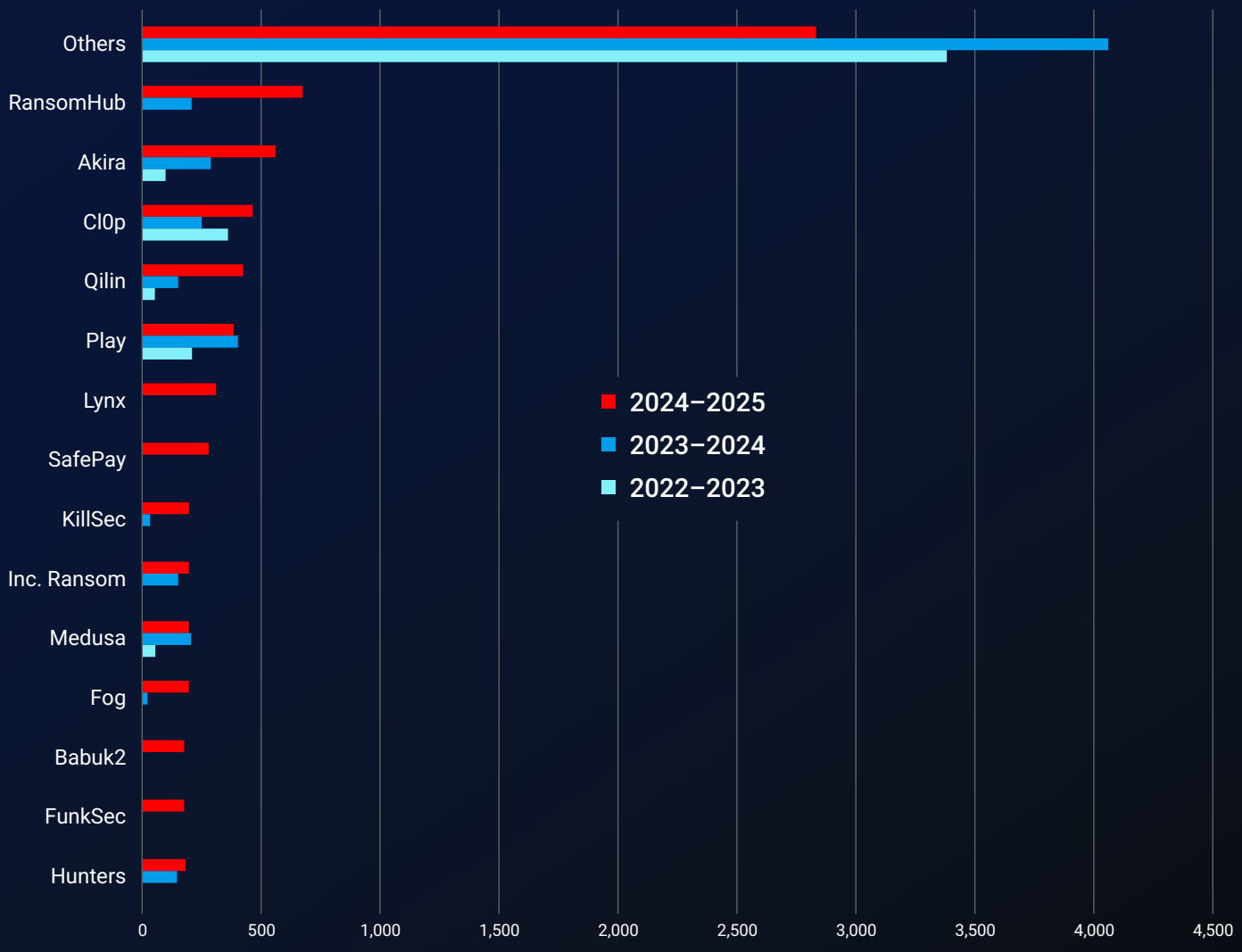


Active ransomware groups per month, July 2022–June 2025

However, while the ransomware landscape is structurally stable, it is fragmenting. The top ten most active groups now account for only 50% of attacks, down from 69% between July 2022 and June 2023. This shift reflects how lower barriers to entry are breaking up the ecosystem's previous reliance on major ransomware-as-a-service vendors for malware and infrastructure.

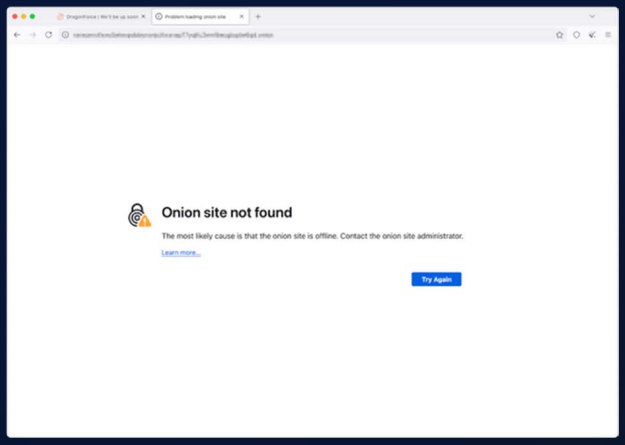
Ransomware is also highly volatile, particularly at the top. Dominant groups leave suddenly and new ones rise quickly to replace them. Among the top 15 most active groups in the last year, most had little or no footprint at all in the previous year.

Known ransomware attacks by group



This churn at the top is exemplified by groups like RansomHub, which emerged out of nowhere to become the leading ransomware group following the demise of LockBit and ALPHV. While less dominant than its predecessors, RansomHub accounted for about 10% of all known attacks over the last 12 months, but its reign lasted less than a year and the group's leak site and negotiation portals went silent after March 31, 2025, for unknown reasons.

The RansomHub onion site went dark in March for unknown reasons



Monthly volatility in ransomware attacks has also increased 50% year-over-year, driven by stop-start behavior among the biggest ransomware groups.

No group is more responsible for this than Cl0p—an extremely dangerous ransomware gang with a unique operational model. Cl0p operates in cycles, going dark for months, then erupting in brief bursts of intense activity. Unlike its peers, the group prioritizes quantity over quality, conducting smash-and-grab campaigns against large numbers of targets using zero-day exploits.

After 16 months of dormancy, Cl0p returned in December 2024. In just three months, it became the third most active group of the past year, claiming almost 7% of known victims. Remarkably, 335 of those victims were recorded in February 2025 alone—the worst month ever for ransomware, and the first to exceed 1,000 known attacks.

Unpredictable patterns of attack, fragmentation, churn at the top, and the increasing role of smaller groups make combating ransomware an ever-more complex and demanding task. On the ground, IT teams are more likely to face acute periods of overwork in the face of "feast or famine" ransomware activity, while group-specific playbooks, indicators of compromise, and law enforcement takedowns are likely to have less impact.

Taken together, these factors amplify the need for security tools with smart automation and low false positive rates, so that IT staff can focus on high-impact activity, and group-agnostic detection.

2X

The number of active ransomware groups has doubled in three years.

Tactics and observations

Ransomware groups continue to use the key tactics highlighted in last year's State of Ransomware report: Attacking at night, when IT staff are least likely to be on hand, and using legitimate system administration tools rather than malware to avoid detection—a tactic known as living off the land (LOTL).

Ransomware tactics continue to evolve though, and ThreatDown's Malware Removal Specialists (MRS) and Managed Detection and Response (MDR) analysts have identified three new patterns in attacks carried out over the last 12 months.

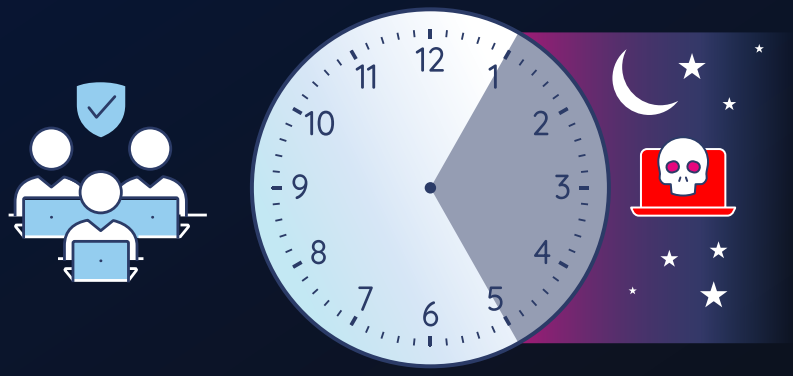
1 | Firewall vulnerabilities

In the last year, ransomware gangs actively targeted Fortinet and SonicWall vulnerabilities. It is easy to understand why: Firewalls are abundant—every organization has one; they occupy highly privileged positions in a network; and they are often hard to patch.

2 | Absent backups

In the last 12 months, ThreatDown analysts encountered an increased number of organizations that did not have adequate backups. Backups are the last line of defense against ransomware, allowing organizations to restore data that has been encrypted, without paying a ransom.

Most ransomware attacks happen at night, between the hours of 1 am and 5 am, while IT staff are asleep



3 | Blind spots

One of the most persistent themes of the last 12 months has been attackers' reliance on fully or partially unprotected endpoints and servers to stage attacks. These blind spots allow criminals to act unobserved, away from the sensors and countermeasures of EDR and MDR.

Unknown computers

"Shadow IT" devices that are unknown to IT staff are the perfect bridgehead for ransomware attacks because they are vulnerable, unmonitored, and unprotected. Threat actors can use them to work unhindered and at their own pace.

Unprotected computers

Some organizations choose not to install EDR on every device, either as a cost saving measure or because they run versions of Windows that are too old to support EDR (such as Windows Server 2012, which Microsoft has not supported since 2023).

ESXi Hypervisors

Over the last year, ThreatDown analysts have also observed several attacks that started by leveraging known vulnerabilities in VMware's ESXi hypervisor, a bare-metal hypervisor that acts like a minimal operating system, but does not run EDR software.

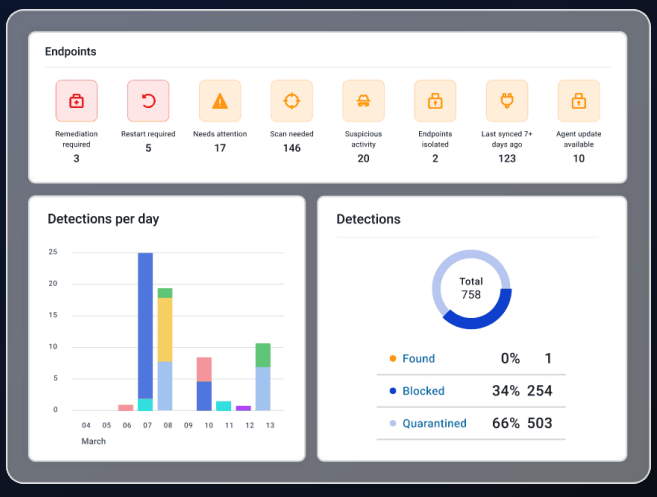
Under-protected computers

EDR software allows organizations to exclude files and folders from monitoring. Overzealous exclusions—such as excluding entire hard drives or powerful apps like CMD—can create blind spots large enough for attackers to operate undetected.

Checklist for MSPs: Building Resilience Against Ransomware

To protect client environments and close visibility gaps, MSPs should:

- ☑ **Map every endpoint** — Maintain a live, multi-tenant inventory of client devices to identify "shadow IT" and unmanaged assets across all tenants.
- ☑ **Standardize full coverage** — Ensure every supported endpoint has licensed EDR protection with correct policies applied and exclusions reviewed quarterly.
- ☑ **Monitor 24×7** — Use a managed detection and response (MDR) service or equivalent to provide continuous monitoring and containment after business hours.
- ☑ **Prioritize patching** — Regularly patch critical systems like ESXi hosts, firewalls, and VPNs; automate patch deployment where possible.
- ☑ **Maintain regular backups** — Ensure backups are air-gapped or immutable and maintain "gold images" ready for fast recovery.
- ☑ **Automate alert triage** — Leverage ThreatDown OneView automation and MDR insights to eliminate alert fatigue and accelerate incident response.
- ☑ **Integrate security layers** — Correlate EDR, DNS filtering, and email security data in a unified dashboard to reduce blind spots.
- ☑ **Educate clients** — Conduct quarterly ransomware readiness reviews with customers to reinforce backup testing and security awareness training.
- ☑ **Document and report** — Use built-in MDR and patch management reporting for compliance, audit evidence, and client transparency.
- ☑ **Plan for scale** — Align security delivery models (self-delivered, vendor-delivered, or hybrid MDR) with business growth and margin goals.



Conclusion for MSPs

Ransomware remains the most disruptive and profitable form of cybercrime in 2025 with attacks growing 25% year-over-year and expanding into 42 new countries. For managed service providers, the implications are direct: every client is a potential target, and every gap in security monitoring is an opportunity for attackers.

The diversification of ransomware groups and their reliance on stealth tactics—night attacks, living-off-the-land tools, and exploitation of unmonitored endpoints—demonstrate that detection alone is not enough. MSPs that depend solely on EDR without continuous monitoring risk falling behind adversaries who operate 24×7.

To deliver on the "managed" promise, MSPs must evolve beyond reactive alert handling toward proactive, always-on security operations. Integrating ThreatDown Managed Detection and Response (MDR) closes the coverage gap, extending expert monitoring and incident response to every hour of the day—without adding staff or building a SOC.

By adopting MDR-as-a-Service, MSPs strengthen client trust, prevent costly breaches, and unlock new recurring revenue streams. In short, resilience—and growth—belong to the providers who never sleep.

Ransomware cannot thrive
in the daylight created by EDR.

How to protect your clients

Cybercriminals don't keep office hours—and neither should your defenses. MSPs must deliver continuous protection that scales effortlessly across all customers.

ThreatDown Managed Detection & Response (MDR) for MSPs

ThreatDown MDR, powered by Malwarebytes, is designed to help MSPs extend 24×7 protection to every client without the cost of building a SOC. It combines always-on monitoring, rapid triage, and guided remediation led by expert analysts.

Why MSPs Choose ThreatDown MDR

- **24x7x365 Coverage**
  Real-time monitoring and containment even when your team is offline.
- **Multi-Tenant Simplicity**
  Manage all clients through ThreatDown OneView with unified visibility, bulk actions, and automated workflows.
- **Expert-Led Remediation**
  Our analysts act as your team, delivering prioritized guidance or directly executing response actions.
- **Integration-Ready**
  Consolidate protection across ThreatDown solutions: EDR, DNS Filtering, Patch Management, and Email Security—all in one lightweight agent.
- **Fast Deployment, Instant Value**
  Onboard new clients in minutes and scale coverage without adding staff.
- **Predictable, Profitable Pricing**
  Offer enterprise-grade security at a cost aligned to your service model.

The Result:

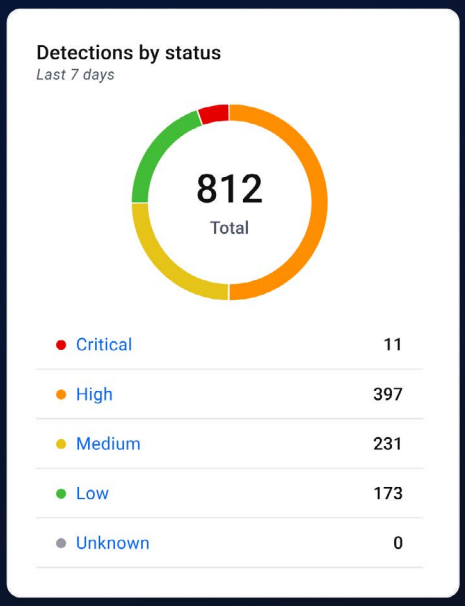
Your clients stay protected. You gain differentiated, high-margin services. Together, we make ransomware defense continuous and effortless.

- **ThreatDown MDR**
  Always-On Protection. Delivered for MSPs.

The Ransomware Reality for MSPs: Opportunity and Obligation

Ransomware's evolution is reshaping the MSP landscape. In 2025, more than half of all recorded attacks targeted small and mid-sized organizations—core MSP customers—because they depend on external IT providers and often lack dedicated cybersecurity staff. This shift places MSPs squarely in the crosshairs of both attackers and client expectations.

Attackers are exploiting the same tools MSPs use to deliver service, turning the managed network itself into a weaponized entry point. But it also means MSPs are uniquely positioned to prevent those breaches—if they evolve from reactive IT management to proactive threat defense.



What Leading MSPs Are Doing:

- Embedding security-by-design into every managed service offering.
- Replacing standalone AV tools with integrated EDR + MDR protection.
- Leveraging ThreatDown's multi-tenant OneView console to correlate alerts across clients and close visibility gaps.
- Turning MDR into a recurring-revenue differentiator—offering "always-on" protection that clients can trust.

Talk to an expert

In today's ransomware economy, protection is no longer optional; it's the product. MSPs that deliver continuous detection, rapid containment, and visible proof of protection not only safeguard their clients—they strengthen loyalty, margins, and reputation.

ThreatDown empowers MSPs to transform ransomware risk into a competitive advantage—protecting clients while growing profitably, from a single pane of glass.

THREATDOWN™

threatdown.com

[1] BBC (2025), Ransomware attack contributed to patient's death, https://www.bbc.co.uk/news/articles/cp3ly4v2kp2o
[2] The HIPAA Journal (2025), Ransomware Attack on Frederick Health Medical Group Affects 934,000 Patients, https://www.hipaajournal.com/frederick-health-medical-group-ransomware-attack/
[3] Reuters (2025), Cyberattacks blight Britain's retailers as M&S, Co-op's systems' breached, https://www.reuters.com/business/retail-consumer/britains-ms-enters-second-week-sales-disruption-after-cyberattack-2025-05-02/
[4] The HIPAA Journal (2025), Kettering Health Resumes Normal Operations for Key Services Following Ransomware Attack, https://www.hipaajournal.com/kettering-health-ransomware-attack/
[5] Reuters (2025), Steelmaker Nucor halts some production after cyber security incident, https://www.reuters.com/business/steelmaker-nucor-halts-some-production-after-cyber-security-incident-2025-05-14/
[6] Reuters (2025), UK companies should have to disclose major cyberattacks, M&S says, https://www.reuters.com/business/retail-consumer/ms-cyberattack-was-carried-out-by-dragonforce-chairman-says-2025-07-08/
[7] The Times (2025), All 6.5m Co-op members had data stolen in cyberattack, https://www.thetimes.com/uk/crime/article/co-op-data-hack-cyber-attack-698bvwr0p
[8] The HIPAA Journal (2025), McLaren Health Care Notifies Almost 750,000 Individuals About August 2024 Ransomware Attack, https://www.hipaajournal.com/mclaren-health-care-investigating-potential-cyberattack/