2025 STATE OF RANSOMWARE

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

ThreatDown™
Powered by Malwarebytes

Contents

Introduction

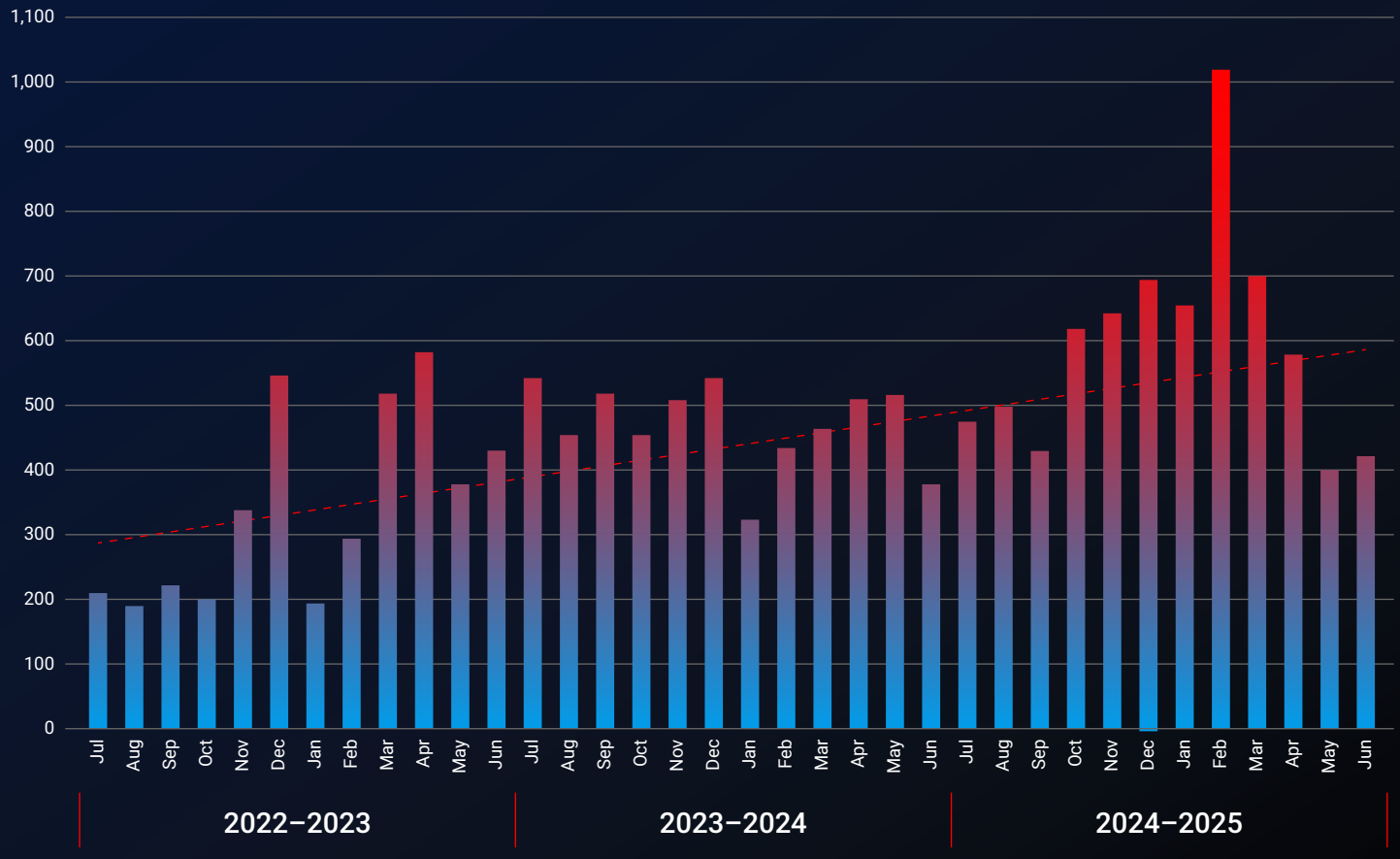
In the 12 months from July 2024 to June 2025, ransomware attacks increased 25% year-over-year. In that time, 41 new groups emerged, active groups topped 60 for the first time, 42 countries recorded their first ransomware incident, and February 2025 became the worst month on record, with over 1,000 attacks.

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

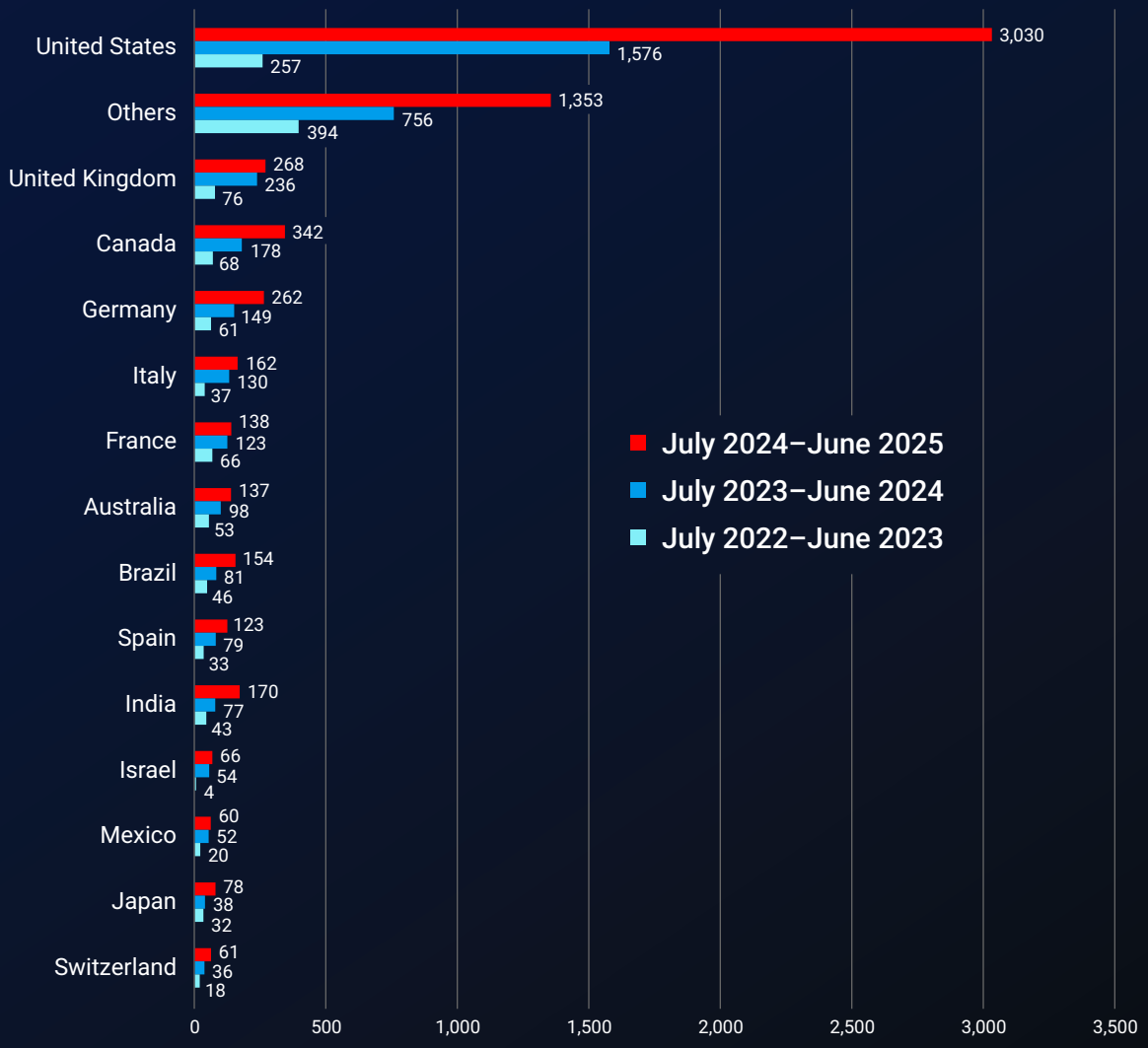


The ransomware ecosystem

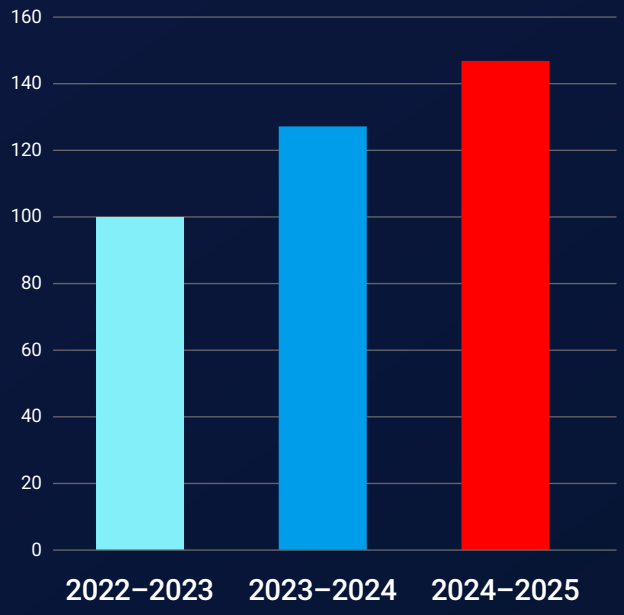
Over the past 12 months, the United States maintained its position as the biggest ransomware target, accounting for 47% of known attacks. Ransomware groups continued their preference for English-speaking countries and Western Europe, with notable campaigns like Scattered Spider's early 2025 attacks on 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. 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



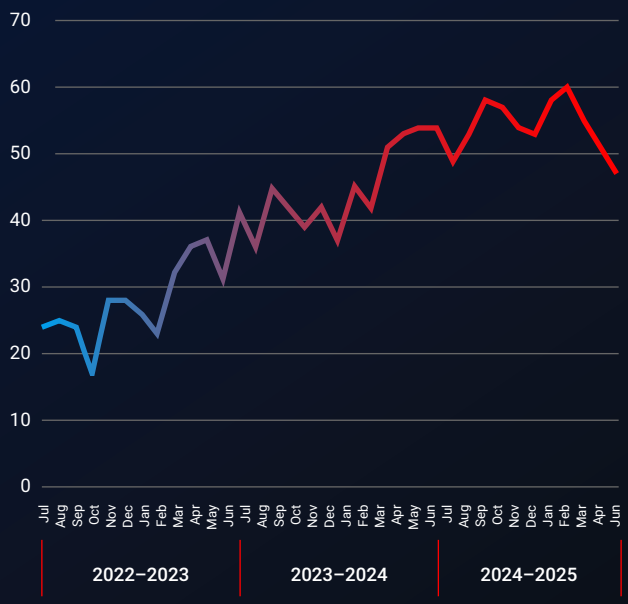
The balance of industries targeted remained largely unchanged, with the services sector hit hardest. Healthcare continued to be a prime target for ransomware groups, and in a world desensitized to the effects of cyberattacks, attacks on hospitals continued to shock.

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 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.

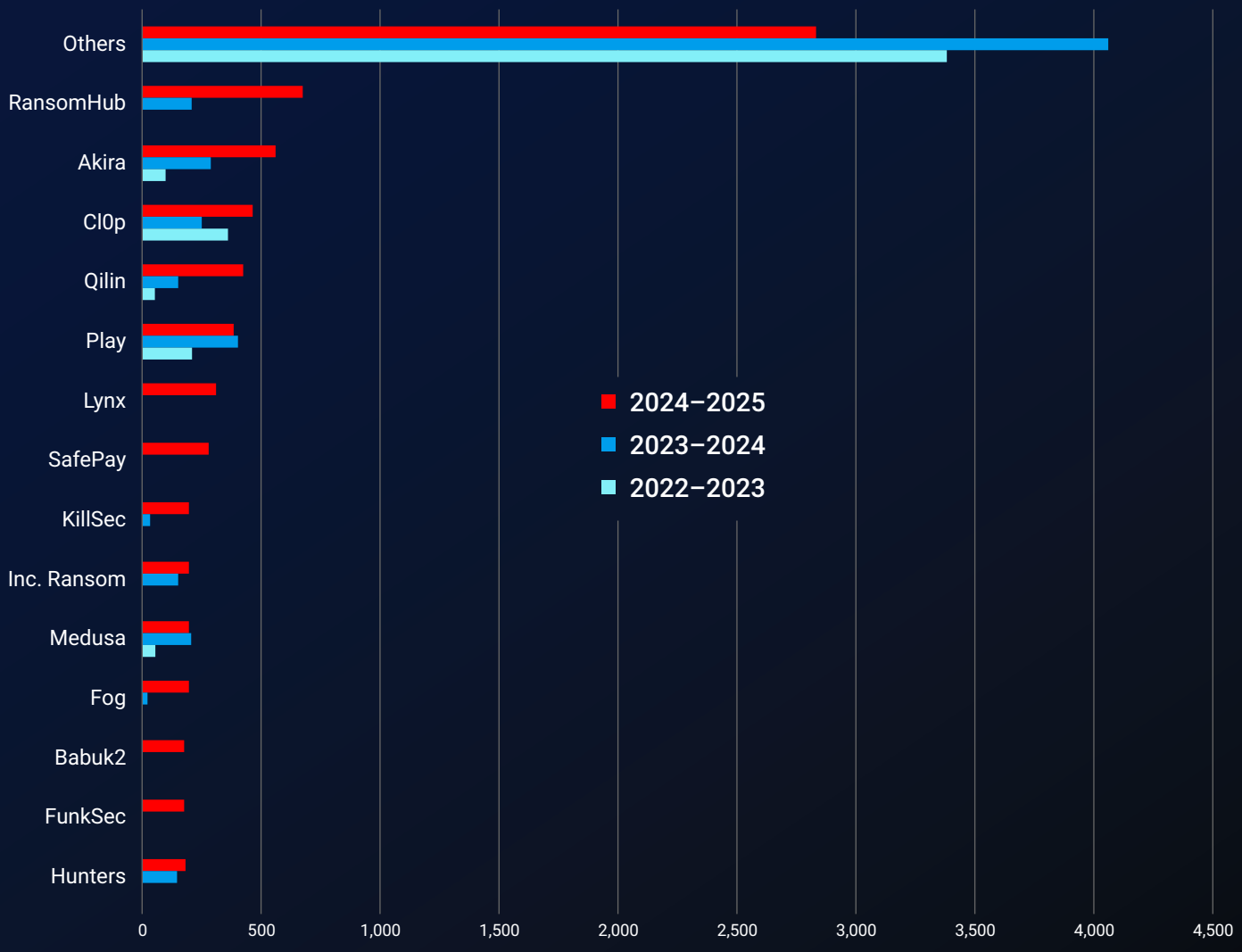


Active ransomware groups per month, July 2022–June 2025

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.

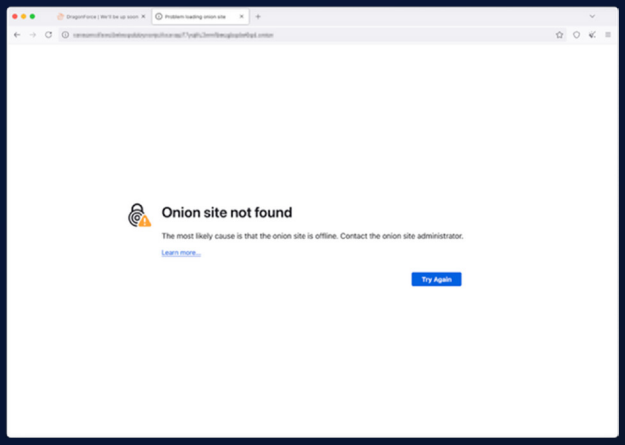
Ransomware is also highly volatile, particularly at the top. Dominant groups leave suddenly and new ones rise quickly to replace them. Among the top 15 most active groups in the last year, most had little or no footprint at all in the previous year.

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.

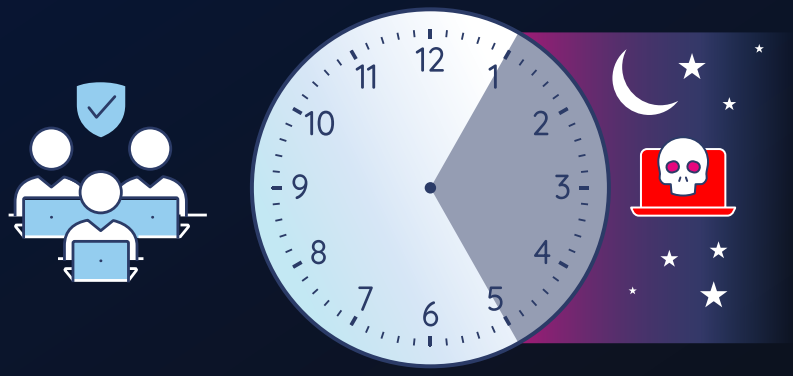
1 | Firewall vulnerabilities

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.

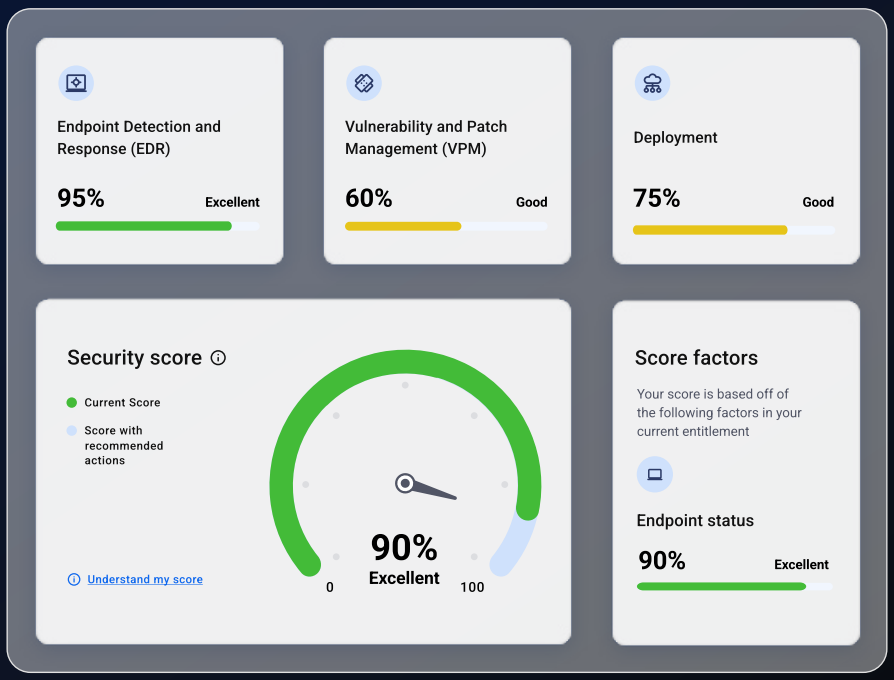
Recommendations

To avoid blind spots, server vulnerabilities, and absent backups, organizations should:

- Maintain an up-to-date inventory of hardware and actively seek out unauthorized “shadow IT” devices.
- Install licensed EDR software on every device that will run it.
- Audit exclusions periodically to ensure that they adequately balance business priorities and protection.
- Monitor CVEs for critical software like ESXi and firewalls, and patch aggressively.
- Keep comprehensive, air-gapped backups, and a gold disk image that can be used to quickly create a new computer with a basic set of applications.

To identify and contain a ransomware attack by an unknown group using LOTL tactics at night, organizations need security software like ThreatDown, that:

- Focuses on AI signatures capable of identifying unknown malware.
- Provides early warnings of suspicious activity with low false-positive rates.
- Auto-isolates infected machines from the network, containing the threat.
- Rolls back ransomware encryption without relying on the easy-to-bypass Windows vssadmin.
- Can be monitored remotely by a managed detection and response team.



Conclusion

Despite notable successes by law enforcement in 2024 and the effectiveness of security tooling like EDR, ransomware continues to thrive in 2025.

While major groups like RansomHub and Cl0p made headlines, the ransomware landscape of the last 12 months was defined by fragmentation and volatility at the top. Ransomware was deployed by a growing pool of groups with an expanding global reach, driven by lower barriers to entry and astronomical rewards.

Tactics have evolved to emphasize stealth, speed, and the exploitation of under-protected systems—particularly "shadow IT," outdated or misconfigured endpoints, and unpatched servers. Attackers work at night and increasingly rely on "living off the land," using legitimate tools to evade detection.

In an ecosystem where attackers adapt quickly and unpredictably, success for defenders rests on proactive security hygiene, disciplined operational practices, and timely responses. Organizations must embrace the proven effectiveness of EDR by eliminating blind spots in their environments and ensuring that alerts are monitored 24/7, via a managed service provider (MSP) or a managed detection and response (MDR) service.

Ransomware cannot thrive
in the daylight created by EDR.

How to protect your company

In today's ransomware landscape, threat actors don't work 9 to 5—and your defenses shouldn't either.

ThreatDown Managed Detection & Response (MDR)

ThreatDown MDR, powered by Malwarebytes, delivers around-the-clock threat detection, investigation, and remediation by elite security analysts who specialize in stopping ransomware and other advanced threats before damage is done.

Why ThreatDown MDR

Organizations face mounting pressure to stay secure with limited staff, expertise, and time. ThreatDown MDR is built to close that gap. You'll experience always-on coverage designed to deliver peace of mind and support your business continuity at every turn.

- **24x7x365 monitoring**
  Our expert MDR team never sleeps. We watch your endpoints day and night, including weekends and holidays, so you can rest easy.
- **Powered by award-winning EDR**
  Our ThreatDown Endpoint Detection & Response (EDR) platform detects and blocks threats with advanced layers of protection, persistent ransomware rollback, and deep malware cleanup.
- **Backed by SIEM and SOAR**
  Detection data is enriched and prioritized in real time using integrated threat intelligence, automation, and correlation to reduce noise and accelerate response.
- **Flexible response options**
  Choose hands-on analyst-led remediation or actionable guidance for your team, whichever fits your operating model best.
- **Fast deployment, full visibility**
  Get up and running in minutes with lightweight agents and intuitive onboarding. Our dashboards give you a clear view of what's happening, what we've stopped, and what actions were taken.
- **Affordable and scalable**
  Our pricing is transparent and cost-effective. Whether you're supporting 50 endpoints or 5,000, ThreatDown MDR scales with your needs.

Proven, recognized protection

ThreatDown MDR is backed by industry validation:

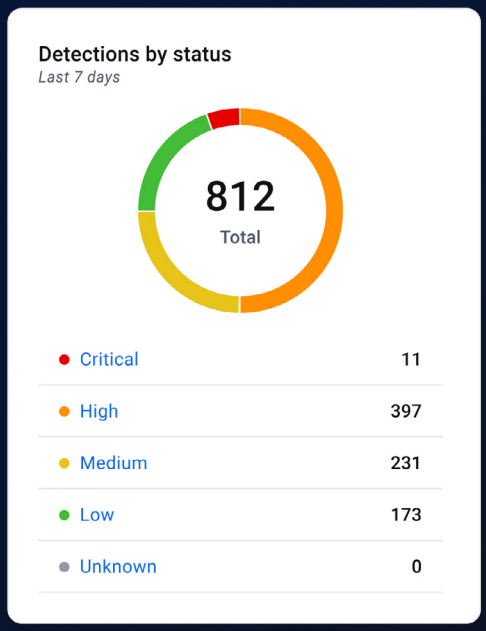
- **MRG Effitas Certified**
  Top ranking in Level 1 360° Assessments
- **#1 Endpoint Security Suite by G2**
  Based on real customer reviews
- **Award-Winning Ransomware Rollback**
  7-day persistent recovery

Born from Malwarebytes. Built for Business.

Formerly known as Malwarebytes for Business, ThreatDown delivers cybersecurity for businesses.

Built on Malwarebytes' expertise in malware detection and remediation, ThreatDown's comprehensive suite of solutions is designed for IT-constrained teams that need advanced protection, without the complexity.

Improve your security posture with one easy-to-manage platform that combines EDR, MDR, Patch Management, 7-day Ransomware Rollback, and AI-driven insights—deployed with a single, lightweight agent. No extra headcount or complex setup required.



MRG Effitas CERTIFIED
ThreatDown Powered by Malwarebytes
PRODUCT OF THE YEAR 2025

SPRING 2025
Grid Leader

IT teams trust us to deliver enterprise-grade protection that's easy to deploy and manage. From award-winning tools to top ratings on Gartner Peer Insights™ and G2, security professionals choose ThreatDown for ease-of-use, fast deployment, and responsive support.

Ready to Strengthen Your Ransomware Defenses?

Talk to an expert

ThreatDown™
Powered by Malwarebytes

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/