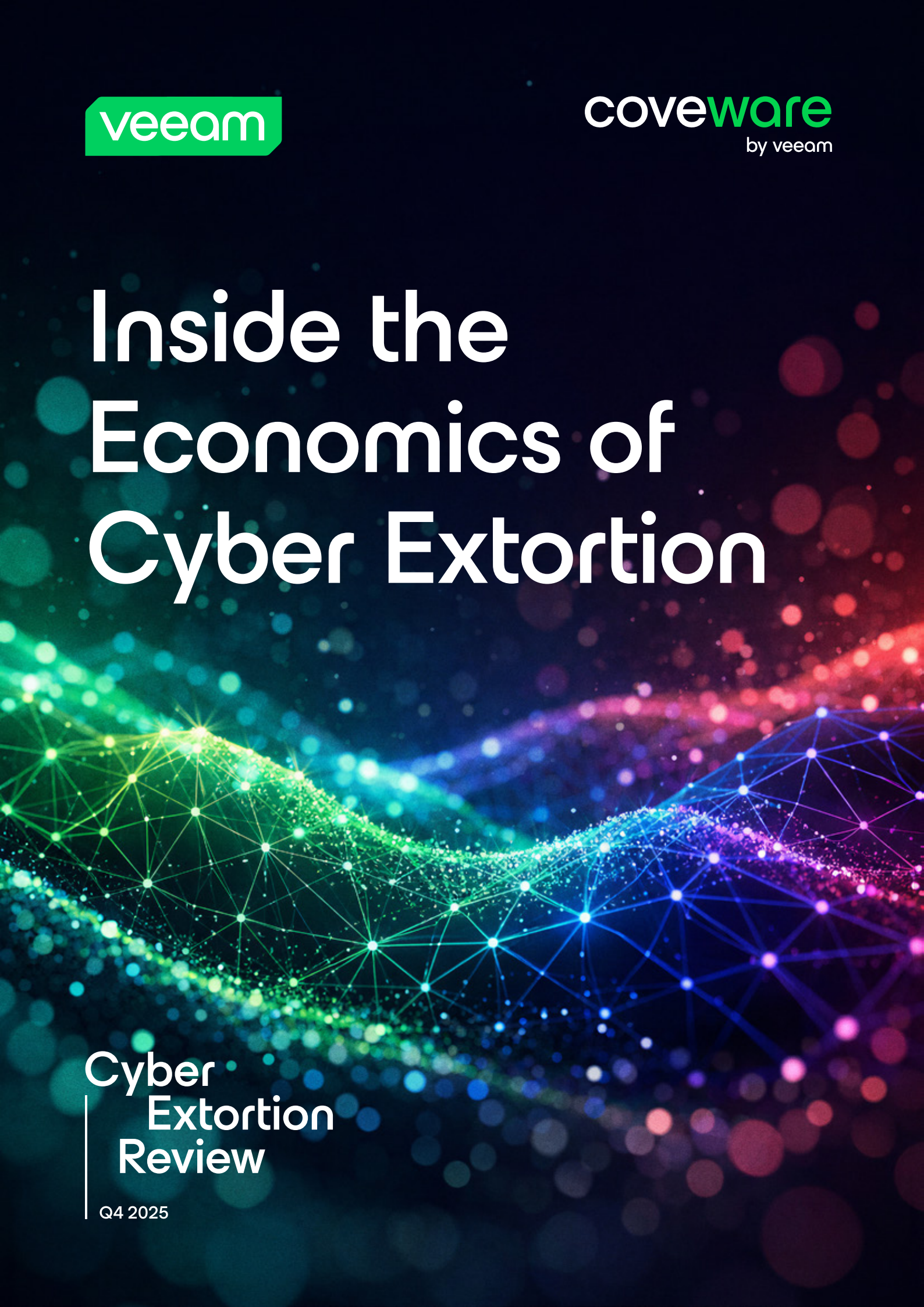
veeam

coveware by veeam

Inside the Economics of Cyber Extortion



Cyber Extortion Review

Q4 2025

Ransomware incidents force high-stakes decisions, where payment can appear to offer the quickest path forward, but the data shows outcomes are rarely as straightforward as they seem.

Foreword

When a company is hit by ransomware, paying for a decryption key can seem like the least expensive path forward. But according to Veeam's 2025 Risk to Resilience report, only 10% of organizations that paid recovered more than 90% of their data, while most recovered less than half. Worse still, 69% of those who paid a ransom reported being attacked more than once.[1]

These incidents can force impossible decisions. For example, research has shown a 35%–41% increase in mortality rates when hospitals were hit by ransomware.[2] In cases like these, it is easy to see why payment can feel like the least bad option.

But there are signs of a change. In 2025, 94% of all incidents included data exfiltration as part of the attacker's plan, but just one in four of ransomware victims ultimately paid, far below the level of previous years.[3]

What changed? And for the minority who still pay, why does this still feel like the only option left?

A Quarter in Review: Q4 Data at a Glance

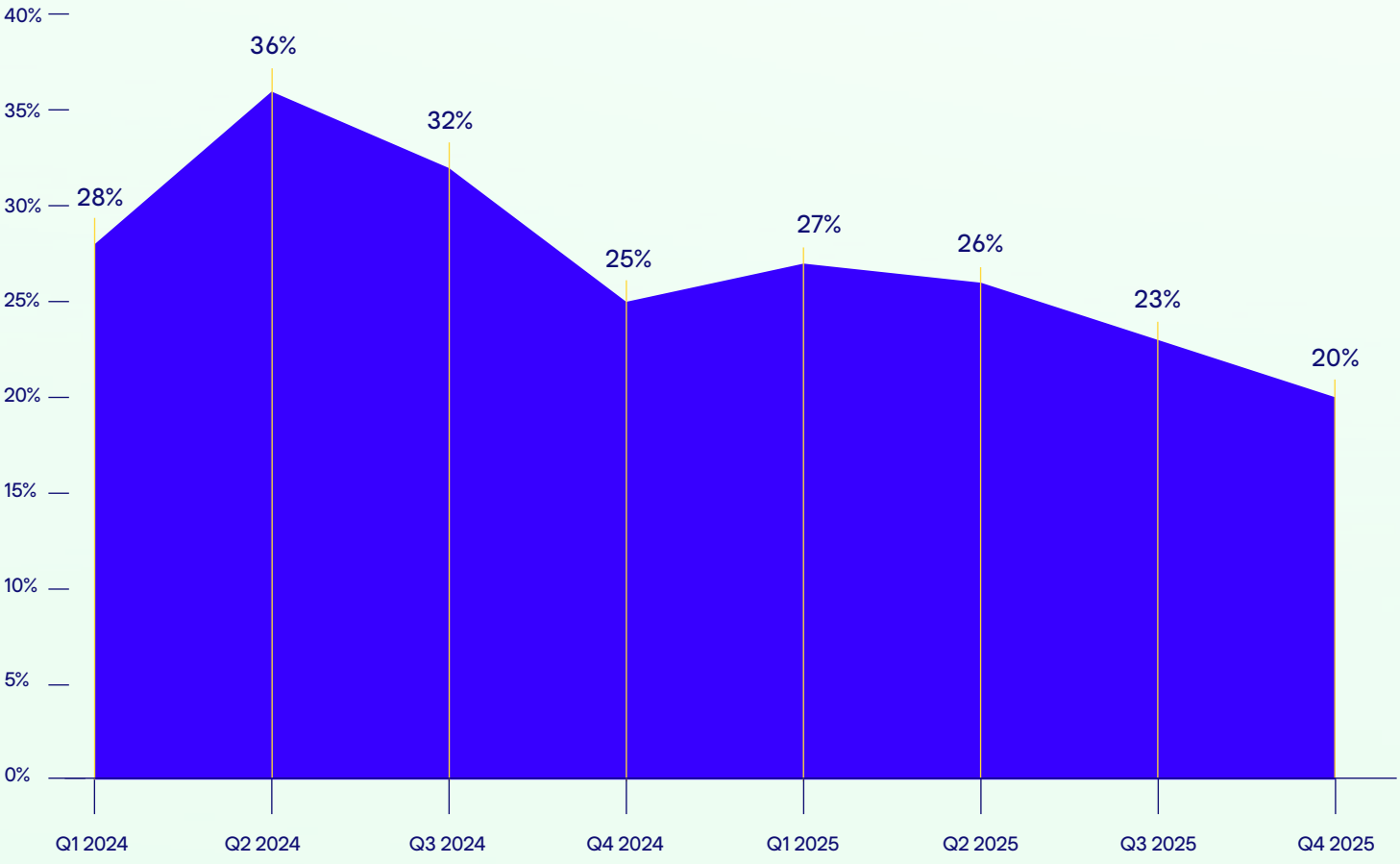
Average payments reached $591,988 in Q4 2025, up 57% from Q3, while the median was just $325,000. That gap reflects a small number of large, operationally motivated settlements, not a broad return to routine payment.[4]

Payment resolution rates fell **3 percentage points** quarter-on-quarter, reaching a record low of

20%

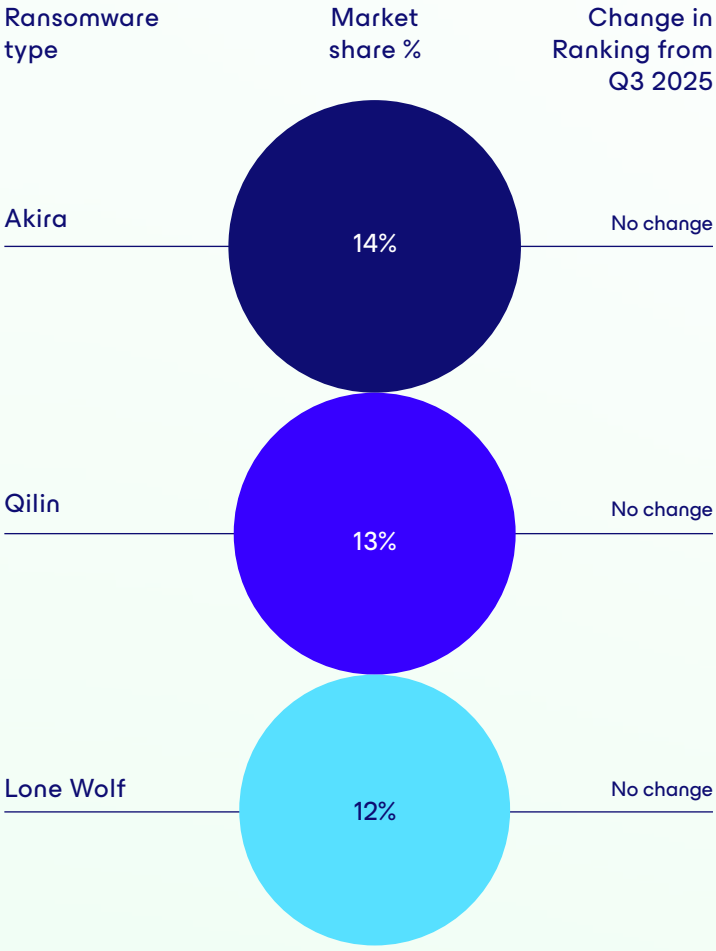
Extortion pressure is no longer converting at scale

All ransomware payment resolution rates



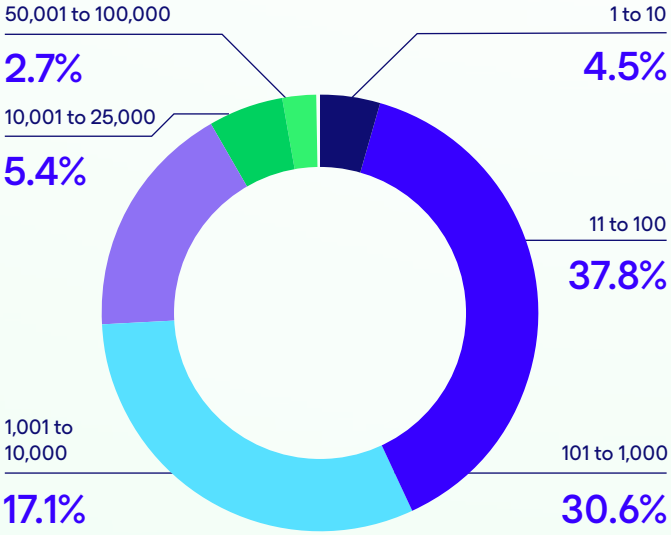
Top Three Most Common Ransom Variants in Q4 2025

The same actors continue to drive the market



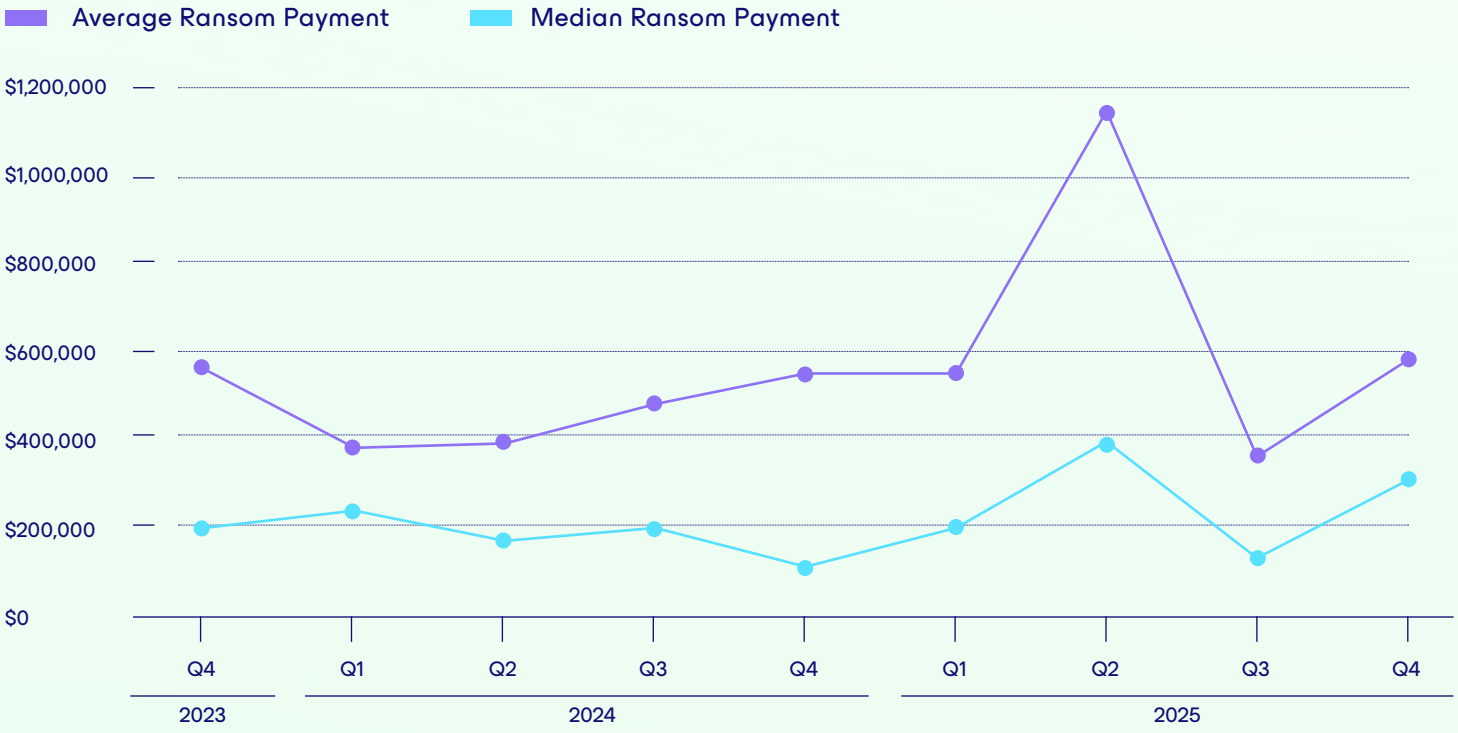
Ransomware Impacted Companies by Size

Extortion still lands hardest in the mid-market



Ransom Payments by Quarter Since 2023

As payment falls, outlier payouts rise



Most organizations now refuse to meet ransomware demands.

Security has tightened and victims realize there is little benefit to payment.

ARTICLE ONE

Why Non-Payment is Becoming the Default Response to Extortion

At the start of 2019, ransomware victims paid 85% of the time, but the average ransom payment was only $12,762. Defenses were weaker and attackers had not yet learned to maximize disruption, so paying was painful but survivable. It was often the path of least resistance.[5]

Today, backups are standard practice, and organizations rehearse recovery often enough to trust the process. Years of high-profile breaches — many originating from third-party suppliers — have made organizations more practiced at managing the fallout when data is stolen. The leverage of exfiltration not only because the data is protected better, but because the response has become excellent. Regulators, customers, and insurers now expect a baseline level of cybersecurity and penalize those that fall short. As a result, attackers that once enjoyed near-guaranteed returns have watched their model erode. By late 2025, the two groups gaining market share, Akira at 14% and Qilin at 13%, were the ones still prioritizing encryption.[6]

Threat actors like CL0P illustrate this shift clearly. Their first data-exfiltration-only campaign, the Accelion breach in 2021, reportedly generated tens of millions of dollars. In 2023, their exploitation of GoAnywhere MFT affected more than 100 organizations: close to 20% paid.[7] Months later, MOVEit impacted more than 2,000 organizations, but the payment rate had already fallen to around 2.5%. By 2024, when CL0P exploited a vulnerability in Cleo's managed file transfer product, the payment rate fell to zero, even though several hundred downstream organizations were affected.

The Oracle EBS campaign should have been lucrative. The stolen data was operationally and commercially sensitive, and victims generally couldn't reconstruct exactly what had been taken. But by then, the calculus had shifted. The central promise behind paying to suppress stolen data had been exposed as hollow.

“Payment does not eliminate notification obligations, reduce litigation risk, or prevent the data from being selectively leaked, resold, or recycled months later.”

At best, payment buys temporary suppression. When law enforcement disrupted LockBit in 2024, after the group had hit approximately 7,000 victims over two years, investigators confirmed that none of the data had been intentionally deleted since 2022 despite repeated payments.[8]

Payment does not eliminate notification obligations, reduce litigation risk, or prevent the data from being selectively leaked, resold, or recycled months later. Add the risk of sanctions violations, reputational damage if payment becomes public, and the chance that attackers could return through the same exploit, and the case for paying becomes much harder to defend.

By 2025, leadership teams increasingly treated backup recovery as a given. The real question was whether their organization could absorb the legal, reputational, and operational fallout without paying. Eighty percent decided they could.

20% Payment resolution rate in Q4 2025

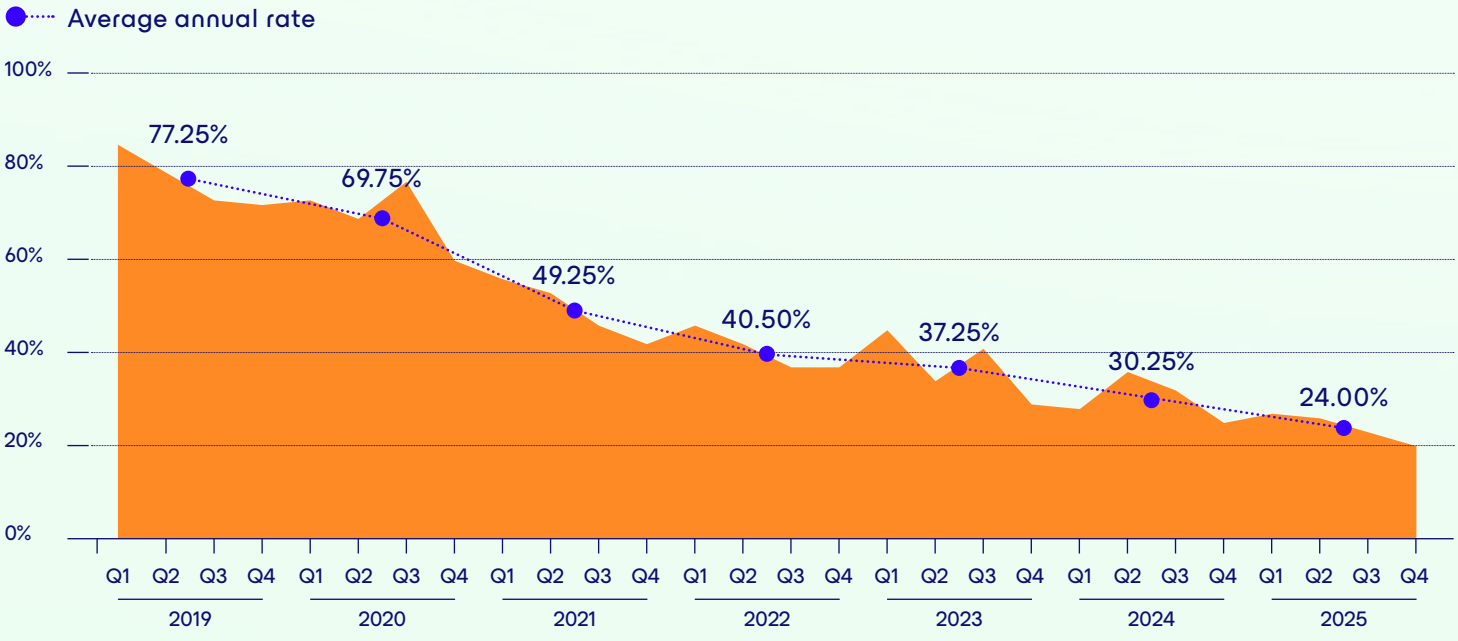
vs. **25%–35% range** from 2024–2025

What this means for defenders

- **Validate every attacker claim forensically before it reaches leadership.** Threat actors exaggerate exfiltration volumes, recycle old data, and impersonate other groups.
- **Assume stolen data is permanent.** No payment has ever produced verifiable deletion. Plan your legal and notification response accordingly.
- **Remediate the entry point before you restore.** Repeat targeting is the norm.

Ransomware payment resolution rates over time

From 77% to 20%: six years of declining returns



ARTICLE TWO

The Numbers Leaders Rely On Can Escalate Extortion Pressure

Security is built on an honest and forensic analysis of your situation.

In 2023, two major casino companies were hit by ransomware within days of each other. One reportedly paid a $15 million ransom. The other refused and absorbed an estimated $100 million in losses over 10 days of downtime.[9]

For some executives, the comparison suggested a simple lesson: paying is cheaper. Ray Umerley, CISO of Coveware by Veeam, says the example still surfaces in meetings with ransomware victims years later. The problem is that the two incidents had almost nothing in common: different data was stolen, different systems were encrypted, and operations were disrupted in different ways.

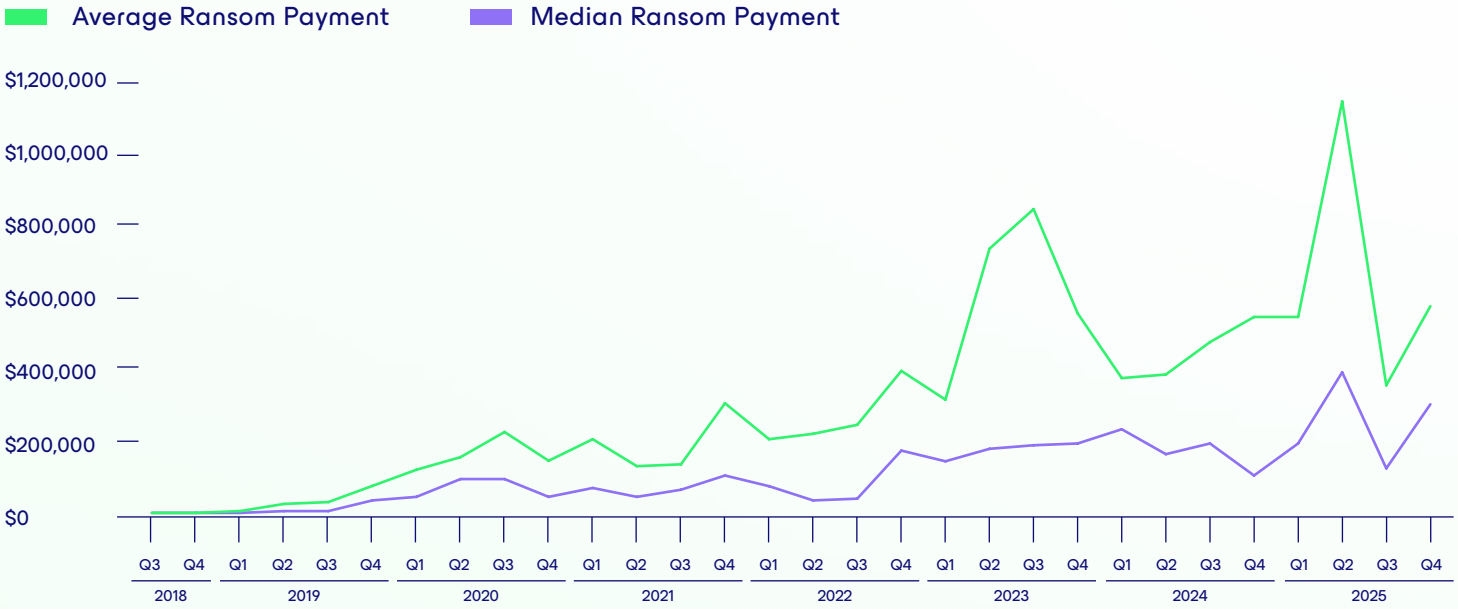
"They're kind of apples to avocados," Umerley says. "I have to educate the stakeholders and say, 'That was interesting, but here's what really happened. Now, let's talk about you.'"

That instinct, mapping a familiar reference point onto your own situation, is exactly how numbers can intensify extortion pressure rather than reduce it.

The first numbers most victims encounter come from the attackers themselves: how many files were encrypted, how many sensitive records are allegedly about to be released. Such figures are often exaggerated. Attackers recycle previously leaked data as proof of a new breach and impersonate groups they have no connection to. Last year, for example, the FBI warned that scammers posing as BianLian were sending extortion letters directly to executives.[10]

Ransom payments by quarter since 2018

The gap between average and median tells the real story



Average Ransom Payment

$591,988

+57% from Q3 2025

Median Ransom Payment

$325,000

+132% from Q3 2025

Even an authentic-looking file list may only prove an attacker cataloged file names, not that they exfiltrated the contents. "When a threat actor is telling you anything about stolen data, they're going to tell you whatever benefits them the most," Umerley says.

There is a persistent assumption that ransom size tracks with company size. Coveware incident data shows it correlates more closely with incident severity: the loss of critical systems, the absence of viable backups, or a prolonged recovery timeline.

The most dangerous miscalculation is believing that paying buys a fast return to normal. Acquiring the key takes time. Once it arrives, decryption is slow and fragile, often complicated by data corruption, virtualization issues, and compatibility failures. Files that were actively in use when the ransomware hit may be corrupted beyond recovery whether you have the key or not.

Across Coveware cases, the average recovery time with a decryption key is eight days, even with what Umerley describes as "the best tooling and reverse engineering in the industry." When distorted reference points combine with manufactured urgency, the numbers that should support rational decision-making become part of the mechanism that undermines it.

"The most dangerous miscalculation is believing that paying buys a fast return to normal."

What this means for defenders

- Every number in an extortion event serves someone's interest. The question is whose.
- **Forensically verify attacker claims.** File lists, volumes, and group affiliations are routinely fabricated. If your incident response team cannot confirm it, treat it as marketing.
- **Benchmark against your own incident.** Consider your recovery time, your data exposure, your operational impact. The casino comparison is memorable because it is simple, which is exactly why it is misleading.
- **Price decryption honestly.** Plan for eight days average recovery with the key, plus corruption, plus files that may be lost regardless.[11] Remember, payment often simply buys a second recovery project.

Attackers use wide-ranging tactics to exploit their victims, such as targeting the supply chain. Harden your infrastructure and prepare for defense in-depth.

ARTICLE THREE

When Payment Becomes a Last-Resort Response to Operational Pressure

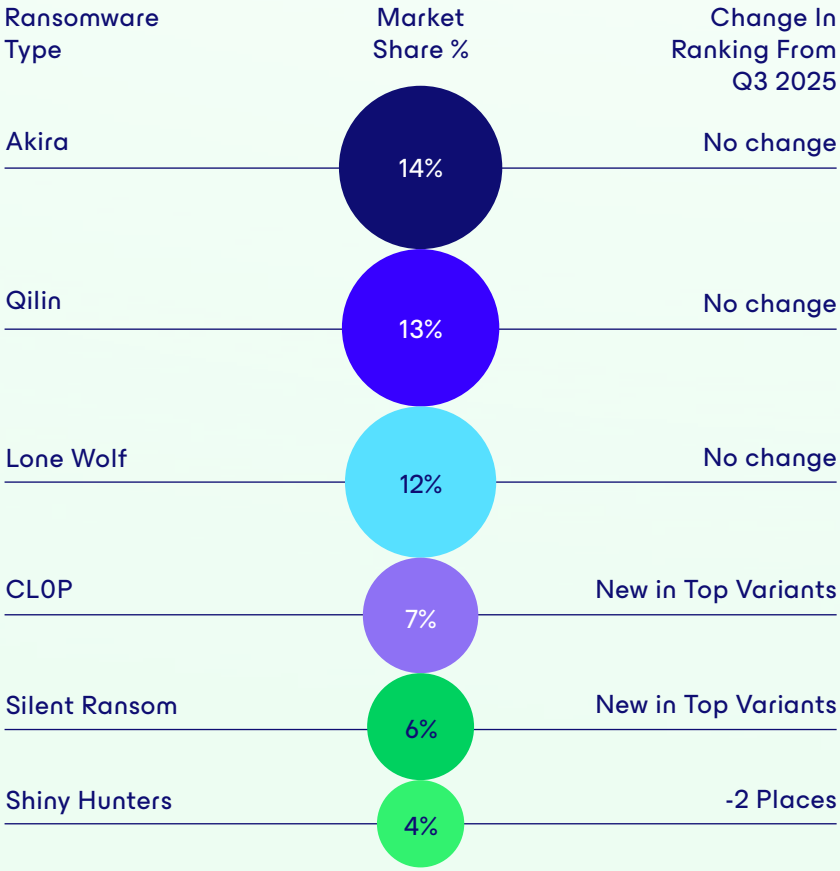
Two-thirds of all decisions to pay a ransomware demand trace back to one problem: backups that were not there when they were needed. In most cases, this was not because the organization skipped backups entirely. Coveware's data is full of examples of outcomes driven by backup jobs whose configurations drifted over time without anyone updating the recovery plan, protections that looked sound until tested.[12]

"We see threat actors attempting to tamper with the backups themselves," says Ray Umerley, CISO of Coveware by Veeam.

As more organizations adopt immutable or offline storage, outright deletion has become harder, so attackers adapt. They infiltrate the environment and quietly alter backup configurations or reduce backup frequency, then wait for older copies to age out before launching the attack. By the time the ransomware detonates, the most recent clean backup may already be weeks old.

Most Common Ransom Variants in Q4 2025

Encryption-first groups hold position while data-only campaigns stall



"You have to restore identity and trust within the organization itself just to get to the point that you can even start your first restore."

Before restoring a single system, incident responders must confirm that the attacker is no longer in the environment and that the backups themselves are clean. "You have to restore identity and trust within the organization itself just to get to the point that you can even start your first restore," Umerley says. "That can be four or five days or longer depending on the threat actor and impact."

That pressure intensifies when attackers target the victim's customers directly, most often at small or midsized service firms with Fortune 500 clients. The attacker contacts those clients, and suddenly the MSP is fielding calls not only about its own recovery timeline, but about theirs. Umerley calls this drag-along extortion, and says it has been increasing, especially in data theft campaigns. The victim might have the resilience to outlast the attacker, but its clients may not have the patience. "We've also seen some instances where the larger organization will help fund the ransom payment," says Umerley.

But the longer negotiations drag on, the more the leverage shifts. "As the downtime continues, you're going to find both clarity and resolve, and a lot of individual heroics and alternative recovery methods emerge," says Umerley.

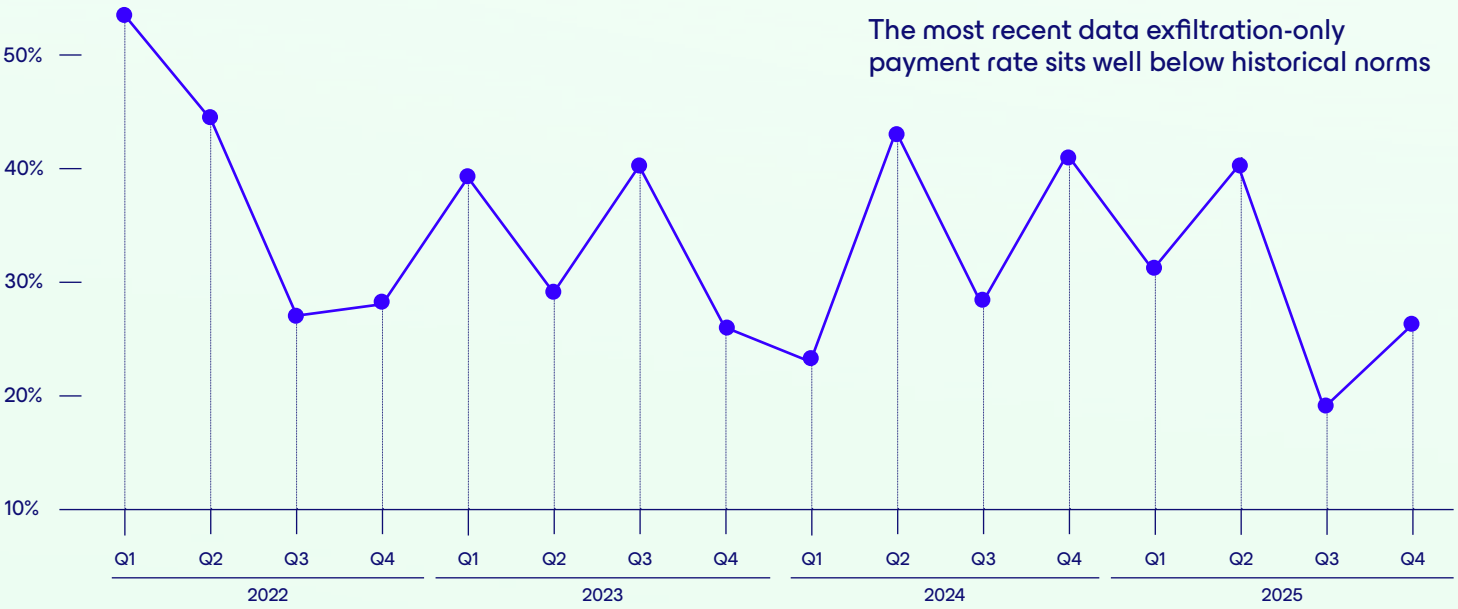
In the first 48 hours, no one knows what was lost, what is recoverable, or what is gone for good. As forensic work progresses, leadership gets a clearer picture of which systems were affected and what recovery looks like without payment.

What this means for defenders

- **Test that your backups actually restore.** Two-thirds of ransomware payments trace back to backups that existed on paper but failed under pressure. A backup you have never restored from is just a hypothesis.
- **Harden the backup infrastructure itself.** Attackers now target configurations and retention policies. By detonation day, your most recent clean copy may be weeks old.
- **Budget four to five days before your first restore.** Even with clean backups, incident responders must confirm the attacker is out and the copies are uninfected before recovery can begin.
- **Expect the blast radius to widen.** When leverage shifts toward the defender, anticipate escalation through client outreach, selective leaks, or swatting attacks against executives.

DXF-Only payment resolution rates since 2022

Data theft alone is losing leverage



25%

The most recent data exfiltration-only payment rate sits well below historical norms

Conclusion

As technical defenses improve, the gap between prepared and unprepared organizations continues to widen. Executives who have tested their response plans, verified recovery timelines, and run tabletop exercises are not immune to ransomware. They simply negotiate from a position where payment is one option among several, rather than the only one left.

Meanwhile, attackers are adapting. With payment rates at record lows, Coveware expects another pivot. Akira and Qilin, the two groups that continued to prioritize encryption over pure data theft alone, held the top two market-share positions through the second half of 2025. As data-exfiltration-only campaigns continue to lose traction, more groups are expected to revert to that model. Threat actors may also move beyond direct extortion altogether, finding other ways to monetize access to compromised networks.

The worst time to learn how a new attack works is while you are negotiating with the attackers. By that point, the technical details are no longer abstract: they are dictating the terms of your recovery, your legal exposure, and your ability to keep the business running. It's not untrue that a healthy organization is one that avoids disruption. But the strongest organizations, those that survive and thrive, are the ones that test their assumptions before an attacker gets the chance to exploit them.

"The strongest organizations are the ones that test their assumptions before an attacker gets the chance to exploit them."

Veeam is the Data and AI Trust Company, specializing in helping organizations ensure their data and AI are fully understood, secured, and resilient to enable the acceleration of safe AI at scale. As the market leader in both data resilience and data security posture management, Veeam is built for the convergence of identity, data, security, and AI risk.

Veeam delivers deep contextual intelligence across every data asset, identity, and AI model. The company governs access for both humans and AI agents, automates privacy, compliance, and remediation processes, and protects and recovers organizations from modern threats – including ransomware, disasters, AI errors, and ensuring the restoration of clean, trusted data. Veeam empowers organizations to move beyond simply protecting data, enabling them to activate and unlock its full potential.

Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 82% of the Fortune 500, who trust Veeam to keep their businesses running. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

[1] Veeam, "Ransomware Trends and Proactive Strategies," 2025.
[2] STAT News, "Hospital ransomware attacks linked to increased patient mortality," 2023.
[3 4] Coveware by Veeam, Q4 2025 incident data.
[5] Coveware by Veeam incident response data.
[6] Coveware by Veeam, Q4 2025 incident data.
[7] CISA.gov, "CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability," June 2023.
[8] Justice.gov, "U.S. and U.K. Disrupt LockBit Ransomware Variant," February 2024.
[9] Bloomberg, "Caesars Entertainment Paid Millions to Hackers in Attack," September 2023.
[10] FBI.gov, "Mail Scam Targeting Corporate Executives Claims Ties to Ransomware," March 2025.
[11] Coveware by Veeam, Q4 2025 incident data.
[12] Coveware by Veeam, Q4 2025 incident data.