proofpoint®

REPORT

2026

AI-Era Ransomware Report

Why AI-enhanced attacks are making ransomware more convincing, effective, and difficult to stop

Table of **contents**

Introduction

Most ransomware plans start too late in the attack chain. They focus on post-compromise recovery—restoring encrypted systems, managing downtime, negotiating payment—but often underinvest in stopping the initial access that makes the attack possible.

That access starts with people. Every day, employees open seemingly routine attachments, enter their credentials on login pages that look right, and respond to conversations that have been hijacked so cleanly there's no reason to question them. But by the time the attack is revealed, adversaries may have already moved through the network and stolen data before any encryption payload is deployed.

AI is now a big reason why these attacks are so hard to catch. The subtle clues that people have been trained to spot (clumsy phrasing, mismatched logos, login pages that don't look quite right) are exactly what AI is best at erasing.

Across the incidents examined in this report, evidence of AI involvement was the norm, not the exception. What's more, most organizations said that it made those attacks more effective. AI isn't just introducing new tactics. It's making the ones that already work, such as phishing, impersonation, and credential theft, harder to detect and easier to scale.

We surveyed 953 security professionals across 12 markets about ransomware incidents in the past year—and about the role that AI played in those attacks. Our findings are organized around three structural changes that should reshape how we think about defending against ransomware: who gets targeted, how attackers monetize access, and why existing controls keep falling short.

AI isn't just introducing new tactics. It's making the ones that already work, such as phishing, impersonation, and credential theft, harder to detect and easier to scale.

Key findings

65%

of ransomware victims confirmed AI use made the attack more effective.

54%

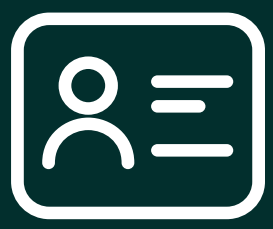
of affected organizations paid a ransom.

37%

of organizations that paid a ransom faced a second demand.

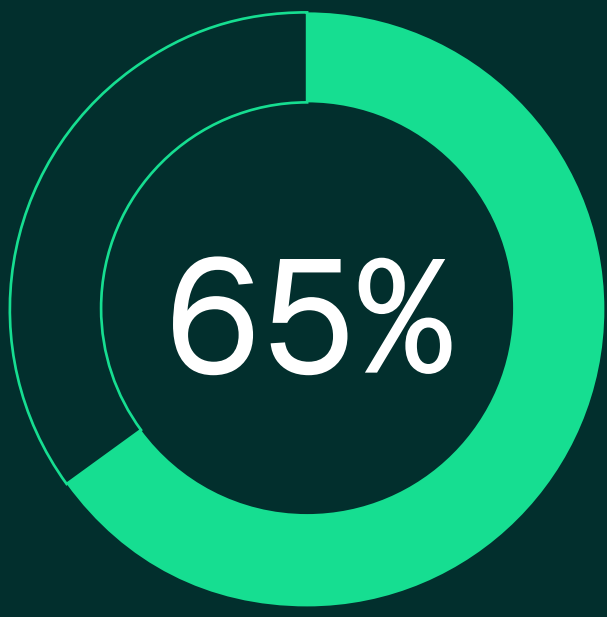
47%

of incidents began with a malicious link, which was the leading entry vector.



40%

of attacks appeared legitimate enough that employees did not suspect them.



of affected organizations experienced some form of data theft during the incident.

01. People are the primary ransomware attack surface—and AI is making it worse

When organizations assess their ransomware risk, they often focus on technical exposure, such as unpatched systems, open ports, and misconfigured services. However, our survey found that the entry vector was often somewhere else entirely.

The most common initial threats are human dependent. And AI is making each of them harder to detect.

AI is amplifying ransomware

The AI data in this survey should end the debate on whether AI-enhanced ransomware is a concern. Among organizations that experienced a ransomware attack, 28% said that AI significantly increased the attack's effectiveness. Another 37% said that it somewhat increased effectiveness. Combined, 65% said AI made the attack more effective. Only 9% reported no evidence of AI use at all.

This is not a story about AI creating new attack types. It's about AI making existing human-centric methods harder to detect and more effective at scale. With AI, attackers can create more convincing phishing lures, write more targeted impersonation messages, and do faster reconnaissance of organizational structures and message patterns.

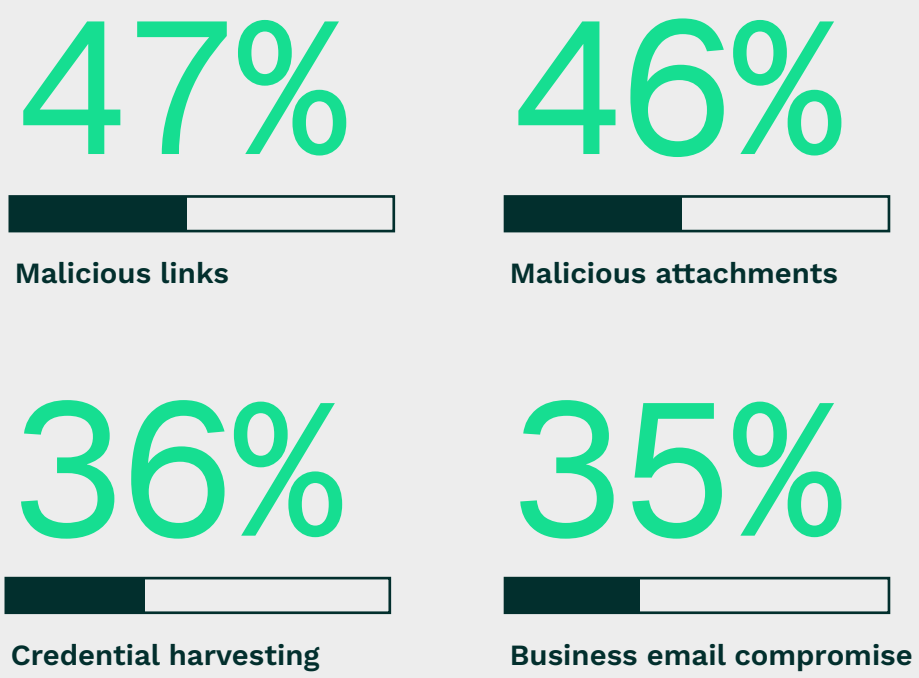
How AI affected ransomware attack effectiveness

The leading entry methods are all human-dependent

When organizations identified the primary initial point of entry for their ransomware incident, the results pointed overwhelmingly to human interaction.

Malicious links led at 47%, followed closely by malicious attachments at 46%. This was followed by credential harvesting at 36% and business email compromise at 35%. Every one of these methods depends on a person opening, clicking, or responding to something that looks like it belongs in their inbox.

Top initial access vectors for ransomware



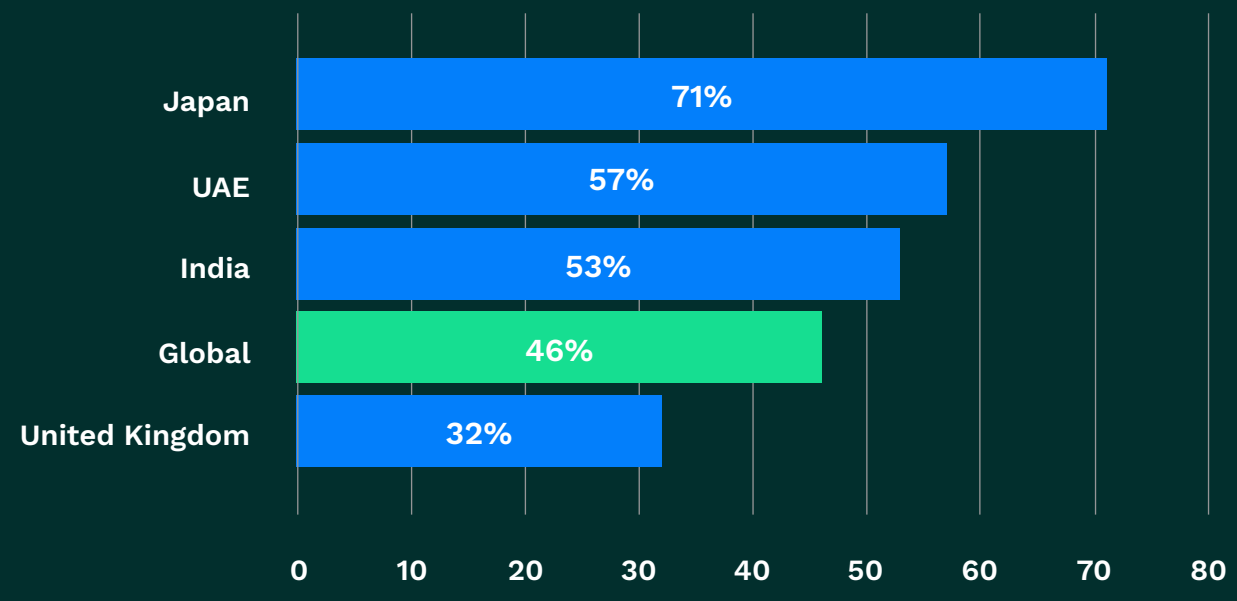
The primary point-of-entry data reinforces this. Phishing or email-based social engineering accounted for the largest share of initial access at 34%. Vulnerability exploitation followed at 20%, compromised credentials at 18%, and remote access compromise at 15%.

That 20% figure is also likely to grow. Frontier AI models have demonstrated the ability to autonomously discover and exploit zero-day vulnerabilities, compressing the window between disclosure and weaponization from days to hours. But even as technical exploitation accelerates, the delivery mechanism remains the same. Threats that rely on malicious attachments, weaponized links, and trusted communications all still need humans.

Same pattern, different tactics

Country-level data shows that the human-centric attack pattern is universal, even though specific threat types vary by market. Malicious links and attachments were among the most common initial threats, but their prevalence shifted by country. In India, 71% cited malicious links, while Japan reported 71% for malicious attachments. While the tactic changes depending on what works in each market, the attack surface is always human.

Malicious attachments as an initial threat type, by country



Proofpoint threat insight

Device code phishing turns identity into a ransomware pathway

Attackers are exploiting legitimate device authorization flows to bypass multifactor authentication (MFA) and take over accounts. In device code phishing, the victim is tricked into entering an attacker-generated code on a real authentication page. As a result, they unknowingly grant the attacker a valid session token. No password is stolen, and no MFA prompt is intercepted. The user authorizes the access themselves.

The scale of these attacks is significant. In 2025, 99% of organizations experienced account takeover attempts. What's more, 67% experienced at least one successful takeover. Of the accounts that were compromised, 59% had MFA enabled.

Why this matters

This is the identity-first pathway that the survey data points to. The user isn't tricked into downloading ransomware but tricked into authorizing access. From there, the attacker can move through trusted systems with valid credentials, steal data, and create the conditions for ransomware to be deployed.

02.

Ransomware is now an extortion and identity problem, not just an encryption event

Once attackers are inside, the damage doesn't stop at encryption. Ransomware has outgrown its own name because the next move is extortion. Attackers issue a demand, collect payment, and follow it with a second demand when the first one is paid.

These threats now look less like a malware event and more like a sustained campaign built on identity compromise and trust exploitation. And the broader breach landscape reinforces the point. In 2025, ransomware was involved in 44% of breaches, up 37% year over year.[1]

After payment, the incident doesn't end. Next comes the negotiation.

1. Verizon. *Data Breach Investigations Report*. 2025.

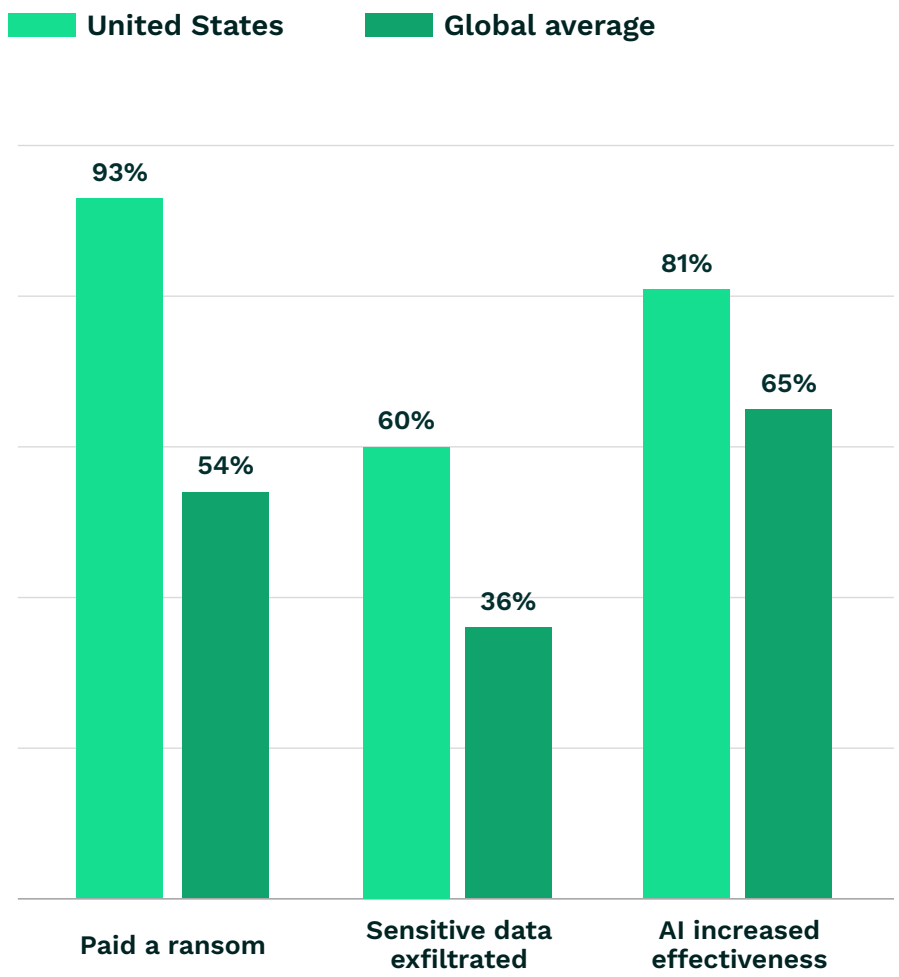
More than half of affected organizations paid

Despite years of guidance from law enforcement and security agencies recommending against payment, 54% of affected organizations paid a ransom. That reflects the real-world pressure that organizations face when operations are disrupted, data is at risk, and recovery timelines stretch further than the business can tolerate.

The global payment rate of 54% masks dramatic variation by market. In the United States, 93% of affected organizations paid a ransom, nearly double the global average. The U.S. also reported the highest rates of confirmed sensitive data exfiltration (60%) and AI-confirmed effectiveness (81%). At the other end of the spectrum, only 19% of Italian organizations paid, followed by 33% in France and 37% in Japan.

These differences matter because they suggest that payment pressure is shaped by a combination of regulatory environment, recovery capability, insurance incentive structures, and cultural norms around negotiation. But the core finding holds everywhere: ransomware creates enough pressure that a significant share of organizations in each of the surveyed markets choose to pay.

United States vs. global average

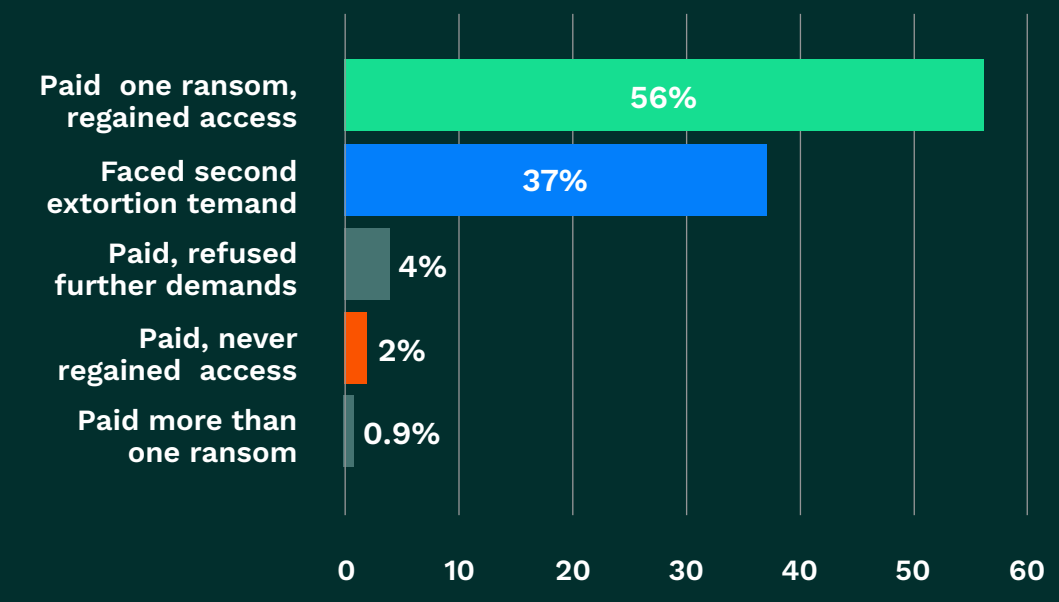


Payment leads to escalation, not resolution

Among organizations that paid, the outcomes were mixed at best and alarming at worst. While 56% paid one ransom and regained access, 37% faced a second extortion demand after paying. That means more than 1 in 3 organizations that chose to pay found themselves facing a follow-on demand. Nearly 2% paid and never regained access at all.

What the data tells us is that ransomware has evolved beyond a single transactional event where paying attackers restores normal operations. It now functions as an ongoing negotiation in which attackers hold multiple forms of leverage at the same time: continued encryption, stolen data, and the threat of public disclosure.

What happened after the ransom was paid



Data theft is par for the course

36% of affected respondents confirmed that sensitive data was stolen during the incident. Another 29% had data exfiltrated but could not determine its sensitivity. Only 32% reported no exfiltration at all.

Combined, roughly two-thirds of organizations experienced some form of data theft. What that says about modern ransomware campaigns is that they're less about locking systems and more about acquiring data, identities, and persistent access. These can be monetized through repeated demands, sold on criminal marketplaces, or used as launching pads for secondary attacks.

Cyber insurance is the default response

Approximately 93% of organizations filed a cyber insurance claim following the incident. Only 3% chose not to file, and just under 3% had no cyber insurance coverage at all. This near-universal reliance on insurance raises a strategic question: if almost every ransomware victim files a claim, is the insurance model accurately pricing the risk? When payment rates remain above 50%, the relationship between insurance coverage and payment behavior is worth examining more closely.

Proofpoint threat insight

A compromised account gives attackers more than access

Ransomware increasingly starts with identity, but the damage doesn't stop there. Proofpoint research on account compromise shows just how quickly attackers turn access into expansion. Among organizations that experienced account takeover, 88% showed post-access activity. That included suspicious mailbox activity in 83% and suspicious file activity in 53%.

Why this matters

A stolen account gives attackers context. Once inside a mailbox, they can read internal messages, map trusted relationships, and identify the people and partners who are most likely to respond. That context fuels everything that follows, including data theft, impersonation of trusted senders, pressure on victims, and secondary attacks that continue long after the first compromise is discovered.

03. Attacks succeed through manipulation, and most defenses aren’t built for it

Having controls and being protected aren’t the same thing. Most organizations that experienced ransomware had security tools in place across email and endpoints. But the attacks got through anyway. The reasons reveal more about how defenses are designed than about how well they perform.

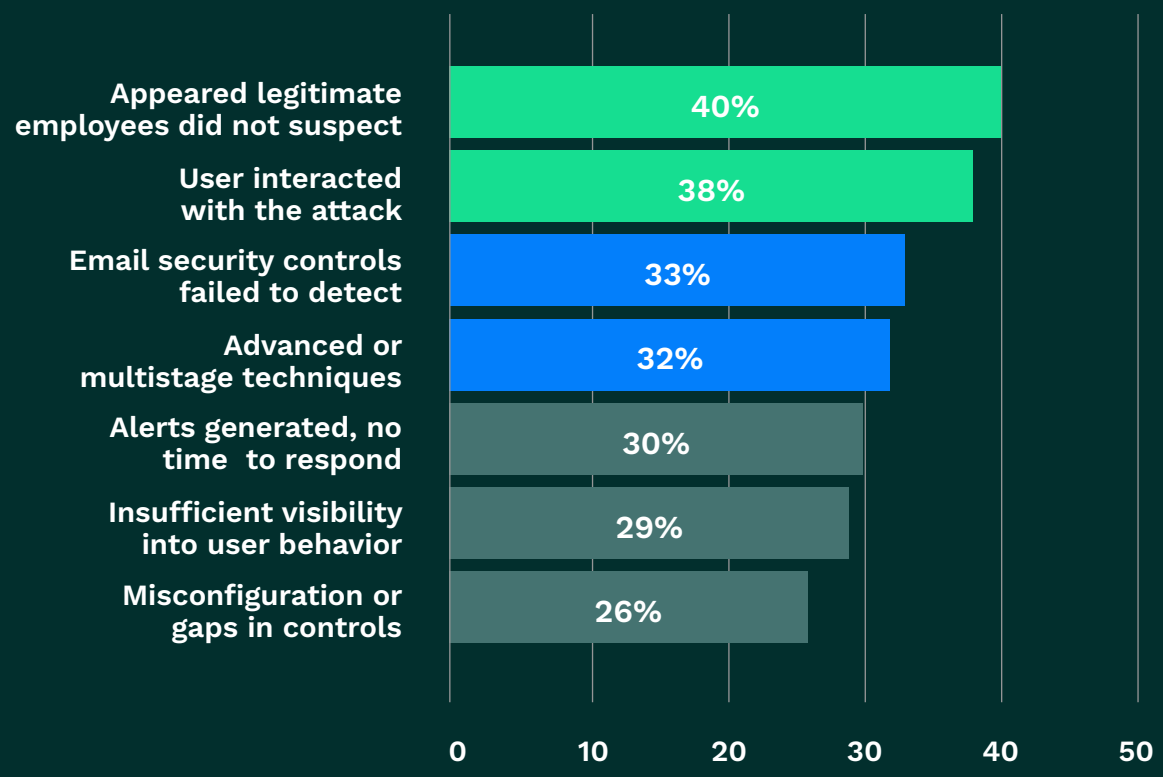
Attacks succeed because they don’t look like threats. And the controls that many organizations rely on were designed for a different problem.

Attacks succeed because they look legitimate

When respondents were asked why the ransomware attack was able to bypass their existing controls, the top two answers had nothing to do with technical failures. 40% said that the attack appeared legitimate enough that employees did not suspect it. And 38% said that the attack succeeded because a user interacted with malicious content, whether by clicking, opening, or engaging with a threat.

This suggests that the primary cause of defenses against ransomware failing isn't because controls are absent or poorly configured. Instead, it's because attacks are now designed to look like normal business communication, so people respond to them as they would respond to the real thing.

Why the attack bypassed existing controls



Trust exploitation is highest in the U.S.

The country data adds another dimension to this finding. In the United States, 56% of respondents said that the attack appeared legitimate, compared to a global average of 40% and just 24% in the United Kingdom. The pattern suggests that U.S.-based organizations, which also reported the highest payment rates and data exfiltration rates, face attacks that are more sophisticated in their impersonation.

Meanwhile, user interaction as a bypass factor was highest in Japan (49%), India (49%), and Singapore (48%). In these markets, the most common failure mode was users engaging directly with malicious content rather than being deceived by impersonation.

Proofpoint threat insight

ClickFix shows why user interaction is now part of the payload

Proofpoint researchers have tracked a sharp rise in ClickFix, a social engineering technique that tricks users into copying and running malicious commands. Instead of relying on a traditional attachment, the attacker presents a fake error message, CAPTCHA, browser update, document prompt, or verification step. The user is instructed to "fix" the issue by running a command in PowerShell or the Windows Run dialog box.

Why this matters

ClickFix bypasses traditional attachment scanning entirely because there's no malicious file to detect. The user becomes part of the execution chain, manually running the command that delivers the payload. It's a direct example of why defenses that are built around known-bad indicators struggle against attacks that are designed to get humans to interact with them.

Controls are part of the problem, but not the whole problem

The survey data does show technical failures alongside the human ones. 33% said existing email security controls failed to detect the attack entirely, and 26% cited misconfiguration or gaps in security controls. But those numbers, while significant, are lower than the trust exploitation and user interaction figures.

The implication is that technical controls alone, even if they're well-configured, would have struggled to catch a substantial share of these attacks. That's because the attacks were designed to pass through controls that look for known-bad signals rather than sophisticated deception.

Speed is outpacing response

Even when controls detect something, the response often comes too late. 30% of respondents said that their security tools generated alerts, but there wasn't enough time to respond before damage was done. Another 29% cited insufficient visibility into user behavior as a contributing factor.

Not surprisingly, the speed problem gets worse as attacks grow more complex. 32% said that the attack involved advanced or multistage techniques. When phishing, credential theft, and lateral movement are combined into a single campaign, defenses that examine each step on its own can't keep up.

AI amplification closes the loop

This is where we revisit the AI data from Chapter 1. When 65% of respondents say that AI made the attack more effective, and 40% of attacks succeeded because they appear legitimate, it's easy to see the connection.

AI is making phishing and impersonation more convincing, more targeted, and harder to tell apart from real communication. The defenses that are failing today were built for a world where malicious content looked obviously malicious. However, for a growing share of today's attacks, that assumption is outdated.

Proofpoint threat insight

AI-built phishing infrastructure is already showing up at scale

Cybercriminals are using AI website creation tools to build phishing, malware, and fraud infrastructure without technical expertise. Since February 2025, Proofpoint has observed tens of thousands of Lovable-generated URLs detected as threats each month in email data. In one campaign that month, attackers used Lovable URLs in a file-sharing-themed credential phishing operation that included hundreds of thousands of messages and affected more than 5,000 organizations.

Why this matters

AI website builders have lowered the barrier to creating convincing phishing infrastructure, hosting it on legitimate platforms, and scaling it through familiar social engineering workflows. Attackers no longer need technical skills to build experiences that look legitimate and drive engagement.

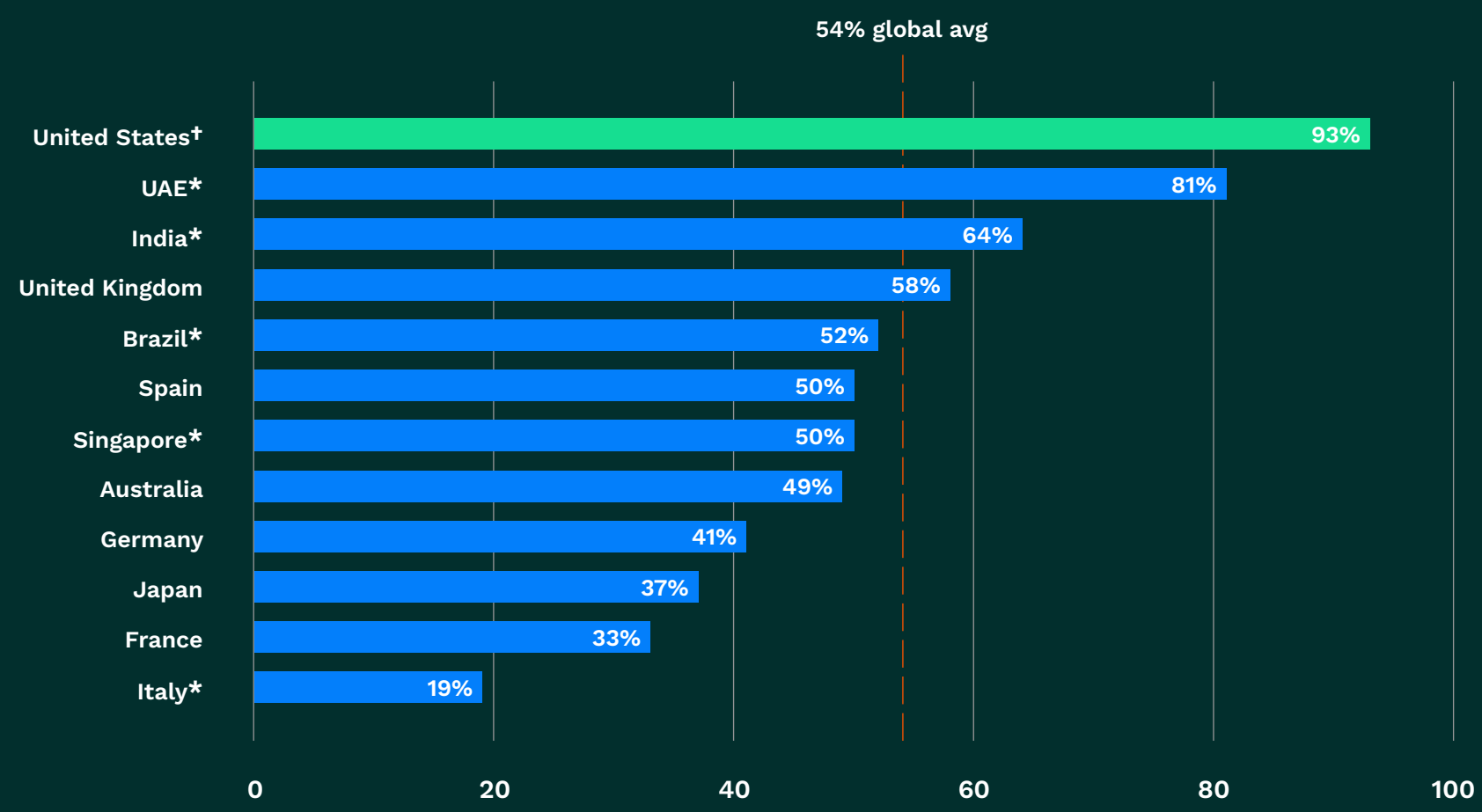
04. Ransomware impact by country

The country-level data tells a consistent story: the ransomware pattern described in this report varies more in intensity than in underlying mechanics. Payment rates range from 19% in Italy to 93% in the United States. Data exfiltration ranges from 17% in Spain to 60% in the United States. Notably, the share reporting that AI increased attack effectiveness remains above 50% in nearly every market.

The entry and bypass data described in the preceding chapters point in the same direction everywhere. Ransomware succeeds when attackers exploit trusted channels, identities, and human behavior.

Country	Paid ransom	Data exfiltrated	AI increased effectiveness	Attack appeared legitimate	Base (affected)
Global	54%	36%	65%	40%	803
United States†	93%	60%	81%	56%	96
UAE*	81%	47%	83%	36%	47
India*	64%	33%	62%	42%	45
United Kingdom	58%	44%	65%	24%	93
Brazil*	52%	18%	39%	34%	44
Spain	50%	17%	52%	42%	92
Singapore*	50%	40%	68%	45%	40
Australia	49%	49%	67%	41%	76
Germany	41%	41%	65%	36%	86
Japan	37%	21%	66%	42%	73
France	33%	28%	65%	35%	75
Italy*	19%	22%	58%	44%	36

Ransom payment rate by country



† The United States had the highest incident rate at 96%, compared to a global average of 84%, which should be considered when interpreting U.S.-specific figures.

* Country base under 50 organizations. Findings for these markets should be treated as directional.

What this means

This report's findings show that ransomware has evolved beyond the defenses that many organizations currently have in place. The attacks that succeeded over the past year didn't depend only on a technical vulnerability or a missing patch, they also exploited something that's much harder to fix: the trust that employees place in the communication channels that they use every day.

The same trust is also what helps modern work get done. Organizations can't tell employees to treat every interaction as suspicious without grinding collaboration to a halt. The challenge is to protect that trust without undermining it—by stopping threats at the point of entry, securing the identities that attackers compromise, and responding fast enough that a single stolen credential doesn't become a full extortion cycle.

The organizations that solve this challenge won't be those with the most tools. Instead, they'll be the ones that learn how to unify protection around people, identities, and every channel where trusted communication happens.

Protect Against Ransomware with Proofpoint

Organizations that want to reduce ransomware risk must focus on stopping attacks at the point of entry, protecting identities from compromise, and responding before attackers can turn access into extortion.

Stop threats before they reach people

Modern ransomware attacks begin with messages, links, attachments, and conversations that appear legitimate. Proofpoint helps organizations stop these threats before they reach users, while also providing post-delivery and click-time protection when attacks evolve after they are delivered.

Protect identities and stop account compromise

Compromised identities often escalate into data theft, extortion, and broader business disruption. Proofpoint helps organizations detect account compromise, prevent impersonation attacks, and protect trusted business communications across email and collaboration channels.

See the full attack, respond faster

Attackers often move across users, identities, communication channels, and systems faster than security teams can manually investigate. Proofpoint helps organizations correlate signals across attack stages, automate response actions, and gain visibility into the full attack chain through a unified security experience.

Proofpoint Collaboration Security Prime brings together threat protection, identity protection, and investigation capabilities in a unified platform.
To learn more, visit proofpoint.com.

Methodology

This report is based on a survey of 953 full-time security professionals conducted in March–April 2026 across 12 markets: the United States, the United Kingdom, France, Germany, Spain, Italy, the United Arab Emirates, Australia, Brazil, India, Singapore, and Japan. Of those, 84% (803) experienced a ransomware incident within the prior 12 months. This report's findings are based on the responses of that affected group. Respondents were predominantly IT professionals (86%), with 79% serving as primary decision makers.

Country-level sample sizes varied. Markets with 100 respondents provide more robust country-level findings; markets with 50 respondents (Brazil, Italy, UAE, India, and Singapore) should be treated as directional. The United States had the highest incident rate at 96%, compared with the global average of 84%, which should be considered when interpreting U.S.-specific findings.

proofpoint®

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com.

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM →