Delinea

2025 State of Ransomware Report

# Adapting with Agility to a Fast-Changing Threat Landscape

# Executive Summary

The ransomware landscape is shifting again as attackers use AI to launch more sophisticated attacks, pushing organizations to adapt quickly and strengthen their defenses.

Adversaries are tapping a vast cyber crime underground to trade the latest hacking tools and tips, upskilling their campaigns with deepfake-driven social engineering, intelligent detection evasion, and automated target selection. Increasingly, their primary vector for initial access is compromised credentials.

To understand what's really happening behind the headlines, Delinea turned to those on the frontlines: IT and security leaders who work tirelessly to safeguard their organizations. This year's study captures insights from over 1,000 security professionals across multiple regions, offering a broader perspective on the state of cybersecurity. The message is clear: ransomware attacks are increasing, even as ransom payments fall, and business disruption can last for weeks. What's more, extortion now accounts for over half of ransomware attacks. These network defenders are adopting AI, but that alone is no guarantee of success.

In this report you will learn how threat actors are growing more aggressive and sophisticated, as well as how organizations are adopting proactive measures to detect, mitigate and prevent ransomware attacks, enabling you to make informed choices for your own security program.

## Key takeaways

- **Ransomware breaches continue to rise even as fewer victims pay**
  - Ransomware is pervasive, with 69% of firms breached and over a quarter hit more than once
  - 60% of ransomware now features data theft-related extortion
  - Fewer (57%) companies are paying
  - Actors remain incentivized to strike
- **Executives are increasingly concerned, but security is falling short**
  - Ransomware is causing chaos, with 3/4 of victims taking two weeks to recover
  - 90% of executives are concerned about ransomware
  - Traditional anti-ransomware tactics are not bearing fruit
  - Only a third of organizations have adopted a least privilege posture, leaving critical access paths open to attackers
- **AI use is surging as ransomware threats evolve**
  - AI is empowering threat actors
  - Ransomware groups are resilient shape-shifters
  - 90% of companies are using AI to tackle ransomware

Key Finding 1:

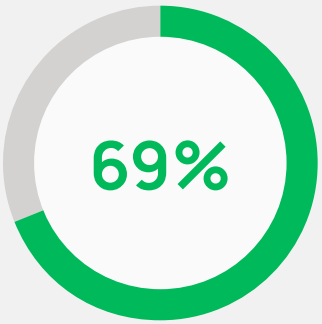
# Ransomware breaches continue to spiral even as fewer victims pay

### Ransomware is pervasive

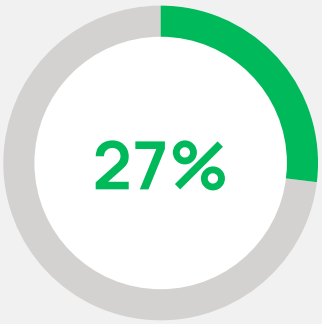
Successful ransomware attacks have continued to increase. More than two-thirds of respondents experienced ransomware breaches in the last year, with U.S. breaches increasing by about a third. What's more, over a quarter of respondents were victimized more than once. Whatever organizations are doing, it is not enough to push back against the rising tide of digital extortion.

## Most firms experienced a breach in the last year

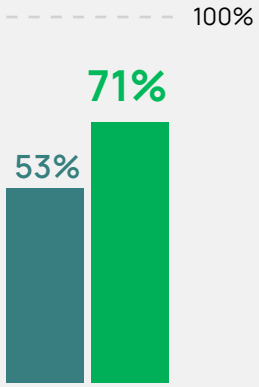
*Q: Has your company been the victim of a ransomware attack in the last 12 months?*




of organizations were breached by ransomware actors




of firms were breached more than once

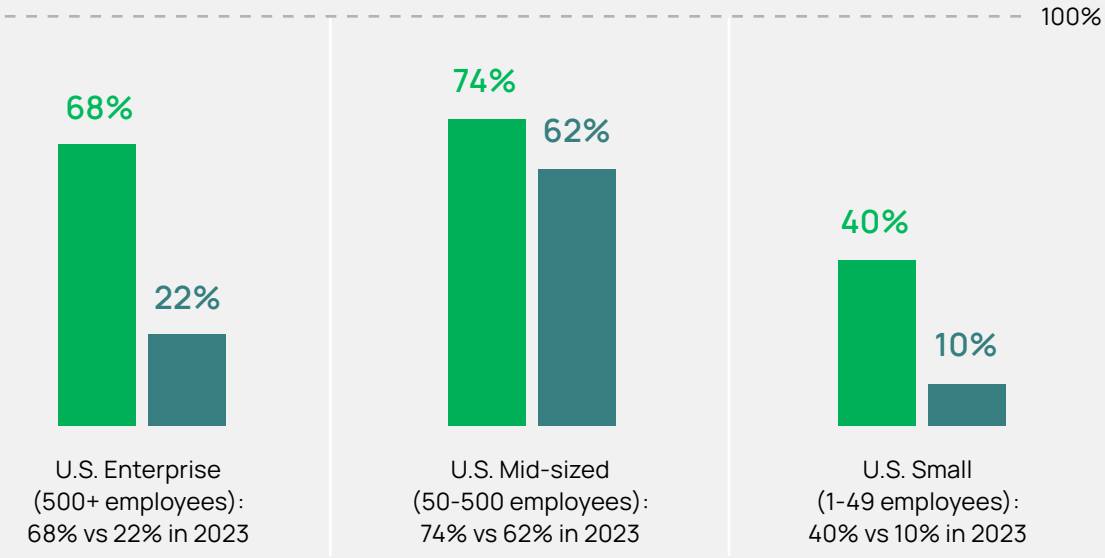



U.S. breaches increased from 53% in 2023 to 71%

In the U.S., the largest organizations experienced the biggest increase in breaches. Large enterprises are singled out as "big game" and targeted with sophisticated "hands-on-keyboard" attacks for big payouts. But smaller firms are not immune. Smaller firms are often seen as easy prey for simpler, commodity campaigns.

## U.S. ransomware attacks surged last year

*Q: Has your company been the victim of a ransomware attack in the last 12 months?*




U.S. Enterprise (500+ employees): 68% vs 22% in 2023

U.S. Mid-sized (50-500 employees): 74% vs 62% in 2023

U.S. Small (1-49 employees): 40% vs 10% in 2023

Which industries are seeing the biggest threat increase? According to Delinea's survey, the U.S. IT and Telecom industry experienced 65% more attacks last year than in the prior year. While retail, catering and leisure had 57% more attacks. Healthcare organizations also remain a popular target, with one in two reporting attacks last year. While no two organizations are the same, these sectors share various high-level characteristics—notably, their low tolerance for outages and/or the large volumes of sensitive data they hold on customers and employees.

## Which industries are hit the hardest?

According to the Delinea Labs research team in their "Cybersecurity and the AI Threat Landscape" report, technology, manufacturing and healthcare were amongst the most targeted industries last year. These industries were probably selected for their low tolerance for outages and therefore higher likelihood to pay. Healthcare, in particular, was vulnerable due to the sensitive nature of patient data, with breaches exposing critical information and endangering lives.

Source: Delinea Labs, "Cybersecurity and the AI Threat Landscape", January 2025

The big question is why does the number of successful ransomware attacks continue to increase? Here are a few key factors:

- **Credential theft is rampant.** According to the 2025 Verizon Data Breach Investigations Report, the use of stolen credentials appeared in almost a third (32%) of breaches last year. These stolen username/password combos provide an easy way for adversaries to waltz past traditional defenses and into corporate networks.
- **Ransomware-as-a-service (RaaS) has proliferated.** The 2025 Delinea Labs Report Cybersecurity and the AI Threat Landscape, reports that RaaS has become more widespread, opening up the field of sophisticated attacks to less skilled actors. RaaS often targets sectors like technology, manufacturing, and construction.
- **Initial access brokers (IABs) are on the rise.** Delinea Labs believes that IABs—specialized threat actors focused on compromising victims—are further contributing to the growth in ransomware attacks. Some IAB sites even allow potential buyers to test whether compromised credentials work before purchasing. Privileged account credentials are particularly prized—especially those that can provide access to corporate identity systems like Active Directory, which store the "keys to the kingdom."

## Ransomware groups are resilient shape-shifters

Delinea research reveals the top five ransomware groups accounted for 36% of the 5,700 incidents assessed in the last year. It notes how fluid and resilient the cyber crime underground is, with groups typically rebranding to escape scrutiny and persisting even despite law enforcement action. According to the Delinea Labs Report, the top five groups by activity are:

- **RansomHub:** A rebranded version of Knight focused on extortion primarily via data theft is a major RaaS group.
- **LockBit:** A notorious and prolific RaaS group since 2019, which uses sophisticated encryption techniques. It persists in a reduced capacity, despite arrests and takedowns
- **Play:** Active since 2022, it uses intermittent encryption as part of its double extortion tactics, which speeds up the scrambling of victims' files
- **Akira:** An aggressive group which appeared in 2023 and is affiliated with the defunct Conti group
- **Hunters International:** Another RaaS group, notable for its sophisticated malware and believed to be an offshoot of the dismantled Hive ransomware group

### Most ransomware today includes data theft extortion

Delinea researchers indicate that most of the main ransomware groups now follow a double extortion model. This is corroborated by this study, with 60% of ransomware victims surveyed claiming they experienced a data breach, and 85% stating they were threatened with having their data published or sold.

If extortion is now predominantly focused on information theft, then backing up is a less useful mitigation strategy if used in isolation. Organizations must instead have a variety of defensive techniques at their disposal. The emphasis must be on proactive, preventative security that blocks data theft from happening in the first place.

### Fewer companies are paying, but there's plenty of road left to run

Over half of those surveyed said they went against the advice of law enforcement and government authorities and paid a ransom last year in order to speed up their recovery. Although less U.S. firms paid last year than the year before.

Paying the ransom doesn't always bring the desired results. About one in four respondents who paid a ransom said they didn't get all their data back, rising to one in three in the UK. Even if they do, it's likely that their adversaries will still try to monetize that data.

## Paying ransom doesn't guarantee data recovery

*Q: If your company has been the victim of a ransomware attack in the last 12 months, did your company pay the ransom? If your company paid the ransom, did you successfully recover the data?*

**57%**

of organizations paid ransomware

**60%**

of U.S. organizations paid ransomware vs. 76% in 2023

**54%**

of UK organizations paid ransomware

**26%**

of organizations that paid a ransom did not get their data back (35% in the UK; 18% in the U.S.)

As long as there are security gaps to probe, victims willing to pay, and regimes prepared to shelter criminal activity, the threat will continue. With AI giving adversaries a fresh advantage, your network defenders must urgently reevaluate their ransomware strategy.

Key Finding 2:

# Executives are increasingly concerned, but security is falling short

### Ransomware is causing chaos and disruption

Organizations continue to be hit hard by ransomware attacks. We found that nearly half of victims took up to a week (one to six days) to recover from a ransomware breach. Three-quarters of respondents say it took them up to two weeks. Few were able to recover in under 24 hours. And it's likely that, in those cases, threat actors were discovered quickly, before they had a chance to steal data or encrypt systems.

## Recovery time is slow

*Q: If your company was targeted by ransomware, how long did it take to fully recover the operations?*

**46%**

of victims took up to a week to recover from a ransomware breach

(50% of UK firms and 42% of U.S. firms)

**75%**

of victims took up to two weeks to recover

**18%**

Only 18% of victims recovered within 24 hours

Many organizations are not so fortunate. There are multiple stages of incident response and recovery to work through. These start with isolating affected systems and determining the scope of the attack. Then fully removing any malware and rebuilding systems. Next, you must notify any relevant parties. In some cases, it may also be useful to open a dialog with the threat actors. Finally, restore encrypted data from backup. This all takes time and money.

Although our study reveals that less than 1% of organizations are still recovering from an attack after a month, such cases can have an outsized impact on customers—and sometimes even whole communities. For example, in June 2024, a ransomware attack on NHS supplier Synnovis led to the postponement of thousands of outpatient appointments and elective procedures in the London area. An urgent call for new blood donors was announced. Even three months later, not all systems had been restored.

Similarly, recent ransomware attacks on UK retailers Marks & Spencer and Co-op significantly disrupted operations, impacting services and supply chains. In the case of some organizations, a serious ransomware breach can even become an existential threat. Kettering-based KNP Logistics Group was forced into administration following a ransomware attack in June 2023, with the loss of 730 jobs.

According to a UK government study, organizations breached by ransomware could face:

- Reduced profit margins
- Missed business opportunities
- Extra IT costs
- Reputational impact
- Loss of confidence in senior management
- Psychological and physical impact on staff of extra stress and anxiety

If your organization doesn't have a robust Business Continuity and Disaster Recovery (BCDR) program, including a well-designed and rehearsed incident response plan, it may struggle. Practicing worst-case scenarios is essential to ensure each stakeholder knows their role, and any unseen issues are identified. It could be something as basic as deciding in what order to restore data from backups. IT teams should not assume that, just because everything is backed up to the cloud, this will be straightforward.

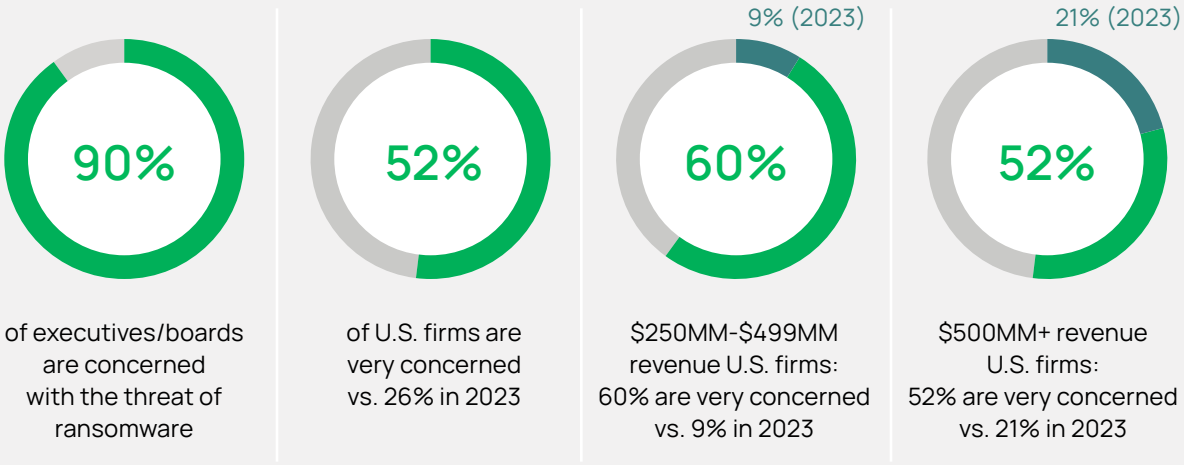
Privileged Access Management (PAM) could help to reduce recovery time and costs by limiting lateral movement of threat actors in the first place. If they have a smaller environment in which to operate and cause damage, it's likely that less data will be taken.

### Executives are rightly concerned

Given the potential impact of ransomware on their organization, it's not surprising that we found nine out of ten decision-makers expressed concern at the threat. And their concern is rising. More than half of the U.S. executives are now very concerned, compared to just over a quarter in 2023. The biggest increase came from some of the largest companies. That aligns both with the rising number of victims from these sized companies and the potential financial and reputational impact of a serious breach.

## Executive leaders are increasingly concerned

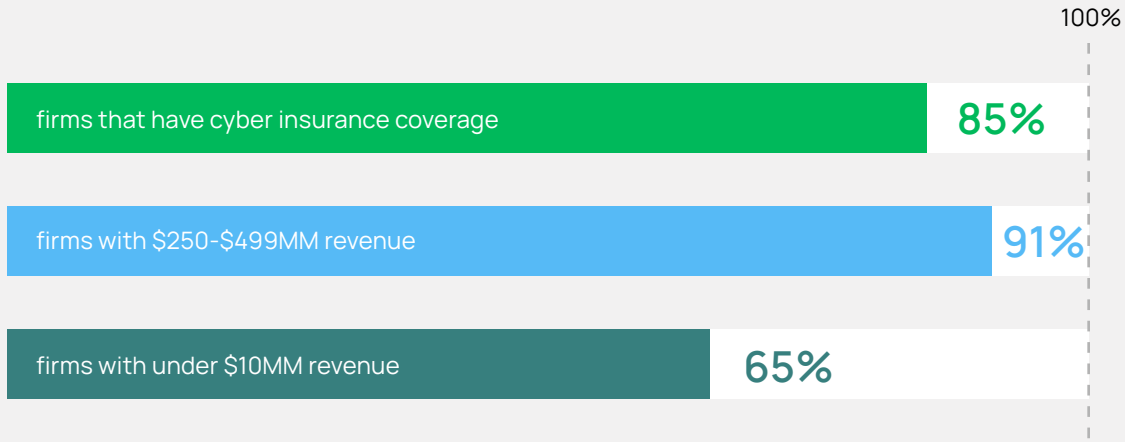
*Q: Which statement below best describes your board and executive leadership team's concerns about ransomware targeting your organization?*




These concerns may be translating into relatively high levels of cyber insurance coverage. On average, four in five firms report having cyber insurance. With larger firms more likely to be insured. Although the smallest companies have the lowest rates of coverage, they should consider it as a useful part of a holistic security posture.

## Larger firms are more likely to have cyber insurance

*Q: Does your company have cyber insurance that includes coverage for ransomware attacks?*



An insurance policy can help to mitigate financial risk stemming from an incident. But increasingly, insurers also demand best practice security measures as a prerequisite of coverage, which can help to improve corporate security posture. Some also offer support, and resources for preventative security and incident response, which may be useful for smaller policyholders.

### Anti-ransomware tactics are not bearing fruit

So exactly how are executives acting on their growing ransomware concerns?

The number of respondents with incident response plans in place is 90% on average, which is reassuringly high even if the figure hasn't moved much from the previous year. It's also notable that the smallest companies (with fewer than 50 employees) recorded the most significant increase in incident response: from 60% to 79% over the course of a year. As long as you design your response plan pragmatically, include stakeholders from across the business, and regularly practice, it should help streamline ransomware recovery efforts.

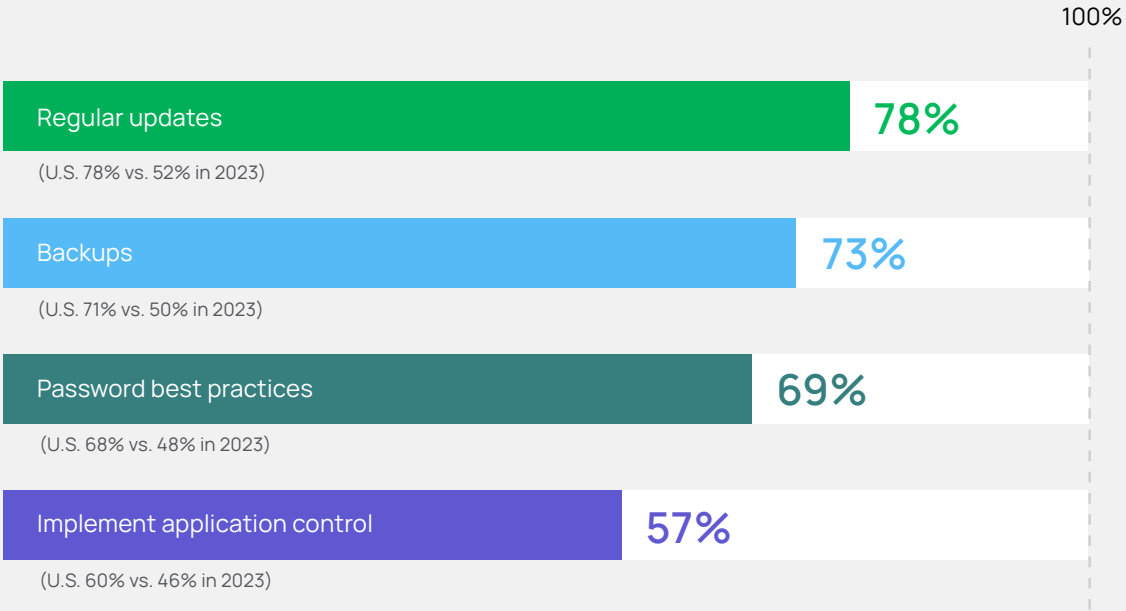
However, a more effective strategy is to focus on prevention—because once data has been stolen, it will most likely be monetized by threat actors. The top four preventative measures taken by respondents last year are:

1. Regularly update systems and software
2. Back up critical data
3. Enforce password best practices
4. Implement application control

In the U.S., there was a major leap in the adoption of these best practices compared to the prior year.

## U.S. steps up preventive measures

*Q: What, if any, steps have you taken to prevent a ransomware attack? (Select all that apply)*



Yet as useful as cyber-hygiene best practices like this are, one glance at the ransomware victim numbers at the top of this report show they are clearly not working. Part of the reason is the sheer size of the corporate attack surface. This has exploded over recent years thanks to remote working, investments in cloud assets, Internet of Things (IoT) endpoints, homegrown cloud-native applications, and the rise of agentic AI.

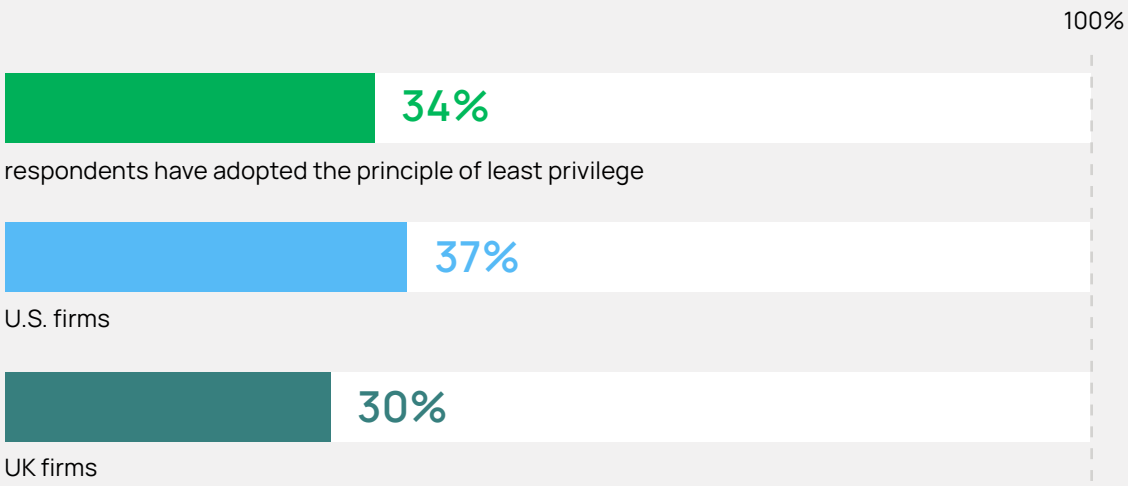
What this means in practice is that your adversaries have a large target to aim at, with many potential vectors for attack. Pre-packaged, service-based offerings help to lower the barriers to entry. IABs offer easy access to corporate networks and cloud accounts. And there's a ready-made market on which they can sell stolen data.

### Least privilege is woefully under-deployed

Another reason ransomware actors are thriving is the relative lack of attention organizations are paying to identity. About one in three respondents claim to have adopted a least privilege posture. Least privilege is the best practice security principle that stipulates users and machines only receive permissions essential for completing their tasks, and no more.

## Few firms adopt principle of least privilege

*Q: What, if any, steps have you taken to prevent a ransomware attack? (Select all that apply)*




Why is it important? In a ransomware context, least privilege helps to reduce the attack surface and the blast radius of attacks by:

- Preventing users from installing potentially unauthorized/insecure applications, which could enable initial access for threat actors.
- Blocking avenues for lateral movement, by restricting what users, accounts, applications and services can access.
- Restricting access for potentially risky third-party suppliers.

When combined with segregation of duties (SoD) and complemented by PAM, multi-factor authentication (MFA) and AI-powered analytics, least privilege can form an essential pillar of zero trust. This best practice security approach posits that no user or machine should be inherently trusted, and all should be continuously authenticated in a risk-based manner.

Yet in some ways, least privilege is more challenging to achieve than patching, backing up or enforcing strong password policies—which may account for its relatively low take up among respondents. Depending on the size of your organization, it may require the continuous management of thousands of users, applications and services.

To achieve this successfully, you need a mature identity and access management (IAM) program in which roles and responsibilities are well-defined, tied to users and regularly audited from an access perspective. Cloud Infrastructure Entitlement Management (CIEM) and Identity Theft Detection and Response (ITDR) tools are vitally important here in helping to continuously discover, manage and protect privileged accounts, monitor usage, investigate abnormal behavior, respond to incidents, and evaluate privileged access controls. Governance is also a critical overlay for your IAM strategy, combining people, process and technology in a single, coherent approach.

Key Finding 3:

# AI use is surging as ransomware threats evolve

### AI is empowering ransomware actors

Zero Trust, PAM and least privilege enforcement are increasingly important in the context of a fast-evolving threat landscape. The UK's National Cyber Security Centre (NCSC) **warned back in early 2024** that AI would "almost certainly increase the volume and heighten the impact of cyberattacks over the next two years." Its predictions are already coming true. Consider, for example, the FunkSec ransomware group, **which is believed** to have used generative AI (GenAI) to build its own malware.

Delinea Labs researchers believe that threat actors will use GenAI in the future to mimic the writing style of employees, clients and suppliers, in order to increase the success rate for phishing attacks. They could also generate unique phishing sites that impersonate an organization's brand, use deepfake audio or video to impersonate trusted colleagues and trick employees into downloading malware.

The future of AI is increasingly agentic: a model whereby the AI operates autonomously and dynamically, solving problems and completing tasks on the fly in order to achieve its goals. Delinea is already seeing examples of this nascent technology, to automate many of the stages of a typical ransomware attack, including reconnaissance, exploitation, exploration and exfiltration. The danger here is that it further lowers the barriers to entry for would-be ransomware affiliates, and empowers bad actors to launch highly targeted attacks at scale—using few resources.

The challenge for your organization is that this could not only increase the volume of attacks but also shorten the lifecycle of the typical kill chain. That makes detection and response much more challenging, and again puts the focus back on preventative, proactive security.

### AI is widely adopted in the fight against ransomware

The good news is that 90% of corporate IT security teams we spoke to are leveraging AI to keep pace with their adversaries. They are doing so in three main ways:

1. **In the Security Operations Center (SOC)**

SOC teams sit on the front line against incoming cyber threats including ransomware. They are often under pressure and under-staffed, struggling with skills gaps and alert overload. This is where AI can provide a much needed helping hand: by triaging and enriching events with additional data and then routing to the right analyst so they can make better-informed decisions. More advanced models may be able to perform Tier-3 analyst work by reviewing threat data and providing recommendations on how to proceed. Agentic AI can autonomously perform threat hunting to surface useful information on possible malicious activity inside the network.

2. **To analyze Indicators of Compromise (IoCs)**

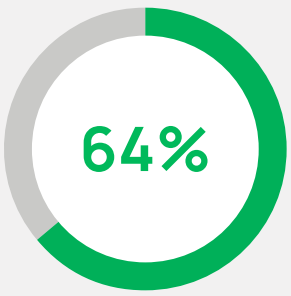
AI is great at analyzing large volumes of data and looking for patterns that human eyes might miss—and doing so on a 24/7/365 basis. To this end, it's perfect for helping sift through IoCs—often in a SOC environment. An AI could be programmed to collect a wide variety of IoCs from different internal and external sources. It's all about freeing up human experts to focus on more valuable security operations tasks, by handing them actionable information. This can accelerate threat detection and response.

3. **Phishing prevention**

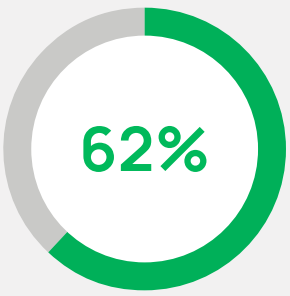
You can train AI algorithms to analyze emails for suspicious writing styles that doesn't match the author, or unusual behavior like messages sent at the wrong time of day or with unusual content. AI can analyze links, attachments and images, including QR codes. It can even help to create realistic simulation exercises for staff training, as well as monitoring employee responses.

## 3 ways IT security is using AI

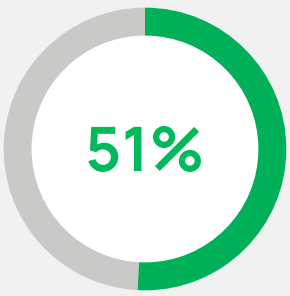
*Q: How is your organization using AI today to protect against ransomware attacks? (Select all that apply)*




In the Security Operations Center




To analyze Indicators of Compromise




Phishing prevention

### Other AI use cases

In addition to these uses, the technology is also making its way into IAM and PAM tools, with impressive results. This includes:

- **Automating routine tasks**

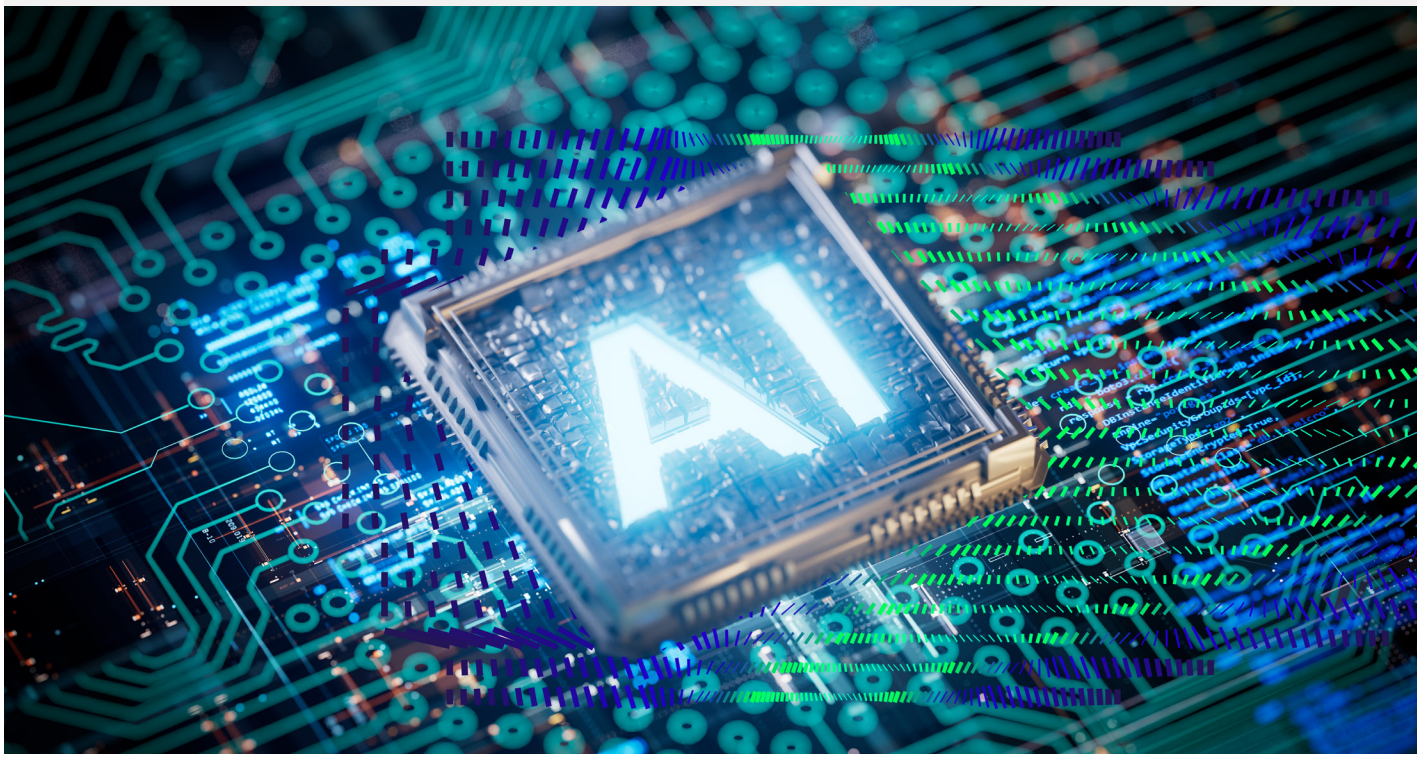
  Automating account provisioning, user access reviews, role modelling and other tasks that are time consuming and prone to human error if done manually—especially in large organizations.

- **Session auditing**

  Using AI to monitor sessions and flag security issues such as overprivileged identities or unexpected privileged behavior. It provides teams with a more efficient approach, compared to time-consuming manual log reviews.

- **Intelligent authorization for ransomware defense**

  The agentic AI defines and optimizes authorization policies and automatically applies them. This means users don't need to create or remember passwords, and IT teams don't need to set permissions or track policy changes. This kind of AI-driven authorization will become increasingly critical for ransomware prevention as threat volumes, attack surfaces, cybersecurity skills gaps and the complexity of environments increase.



# How businesses can protect themselves

Stolen credentials continue to be a primary factor in data breaches. They don't just help threat actors gain initial access to corporate networks, but also escalate privileges and move laterally to cause maximum damage.

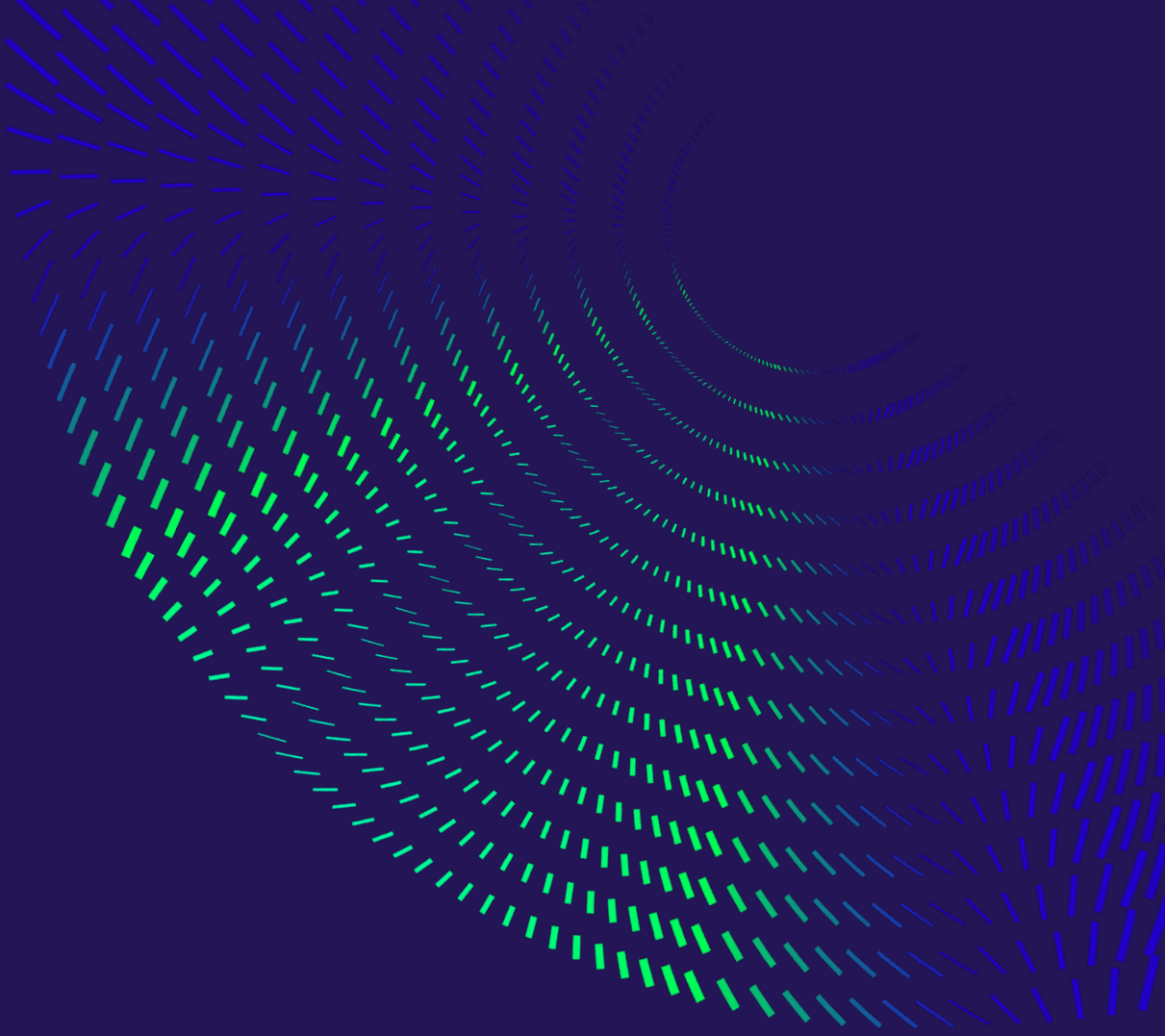
It's one of many reasons why ransomware breaches are on the rise. As AI makes attacks quicker and more successful, executives are concerned, and rightly so. Now it's time to turn that concern into action.

Layered defenses are important. They should include effective training and awareness programs, risk-based patching, regular backups, app controls, anti-malware, network monitoring, and a regularly tested incident response plan. Moreover, a robust identity security strategy is absolutely foundational. Comprehensive, centralized visibility and control over all of your employee and machine identities will help to lock the bad actors out, and limit the harm they can do if they compromise your resources.

Take time when assessing vendors. Choose a trusted name that offers AI-enhanced capabilities like session monitoring and intelligent authorization. This will help to minimize friction, enhance resilience and optimize ransomware defense—while lighting a pathway to zero trust.

It's the peace of mind you need to build your business and harness the power of your people, without compromising on security.

**Learn more about how a robust Identity Security strategy can help combat ransomware at Delinea.com.**



Delinea

Securing identities at every interaction

Delinea is a pioneer in securing human and machine identities through intelligent, centralized authorization, empowering organizations to seamlessly govern their interactions across the modern enterprise. Leveraging AI-powered intelligence, Delinea's leading cloud-native Identity Security Platform applies context throughout the entire identity lifecycle across cloud and traditional infrastructure, data, SaaS applications, and AI. It is the only platform that enables you to discover all identities — including workforce, IT administrator, developers, and machines — assign appropriate access levels, detect irregularities, and respond to threats in real-time. With deployment in weeks, not months, 90% fewer resources to manage than the nearest competitor, and a 99.995% uptime, the Delinea Platform delivers robust security and operational efficiency without complexity. Learn more about Delinea on **Delinea.com**, **LinkedIn**, **X**, and **YouTube**.