SpyCloud

PRESENTS

THE 2024 MALWARE AND RANSOMWARE DEFENSE REPORT

FROM THE COMPANY THAT BROUGHT YOU

THE WORLD'S LARGEST RECAPTURED RECORDS COLLECTION

IN COLLABORATION WITH

INSIGHTS FROM MORE THAN 500 security professionals

By the year 2024, the computer had become the central force of the workplace. Long gone were the days of the typewriter, filing cabinets, and notepads – and in their place, every office worker had become a machine of one, powered by their device, speeding through each eight-hour day on a keyboard and furiously clicking in the name of Productivity.

With the surge in global computer use came the creation of a new role within the modern organization – the security operations center (SOC). Given the difficult task of safeguarding the productive relationship between people and machines, the SOC quickly realized the daunting challenges they were up against. Rampant password reuse, burgeoning digital users, and the rise of crafty cybercriminals threatened their organizations at every turn.

And as the world and workplace continued to develop, the challenges only grew – from high-volume data leaks to stealthy infostealer malware, stolen session cookies, and profit-hungry ransomware gangs. The SOC gathered what tools they could find, and together with their fellow Defenders gave an admirable attempt at leveling the fight between themselves and the enemies that threatened Productivity – enemies that were shapeshifting and multiplying before their eyes.

Would it be enough?

This report describes the state of the malware and ransomware challenges today. The obstacles. The strength and cunning of the enemy. But also the progress that's being made to strengthen organizational defenses.

The wins.

The hope.

The ransomware battle is a tough one – but not a losing one.

To all those in the fight, this report is for you.

BEGIN YOUR JOURNEY ›

TABLE OF CONTENTS →

SUMMARY OF KEY FINDINGS →

1 RANSOMWARE IS THE LEADING CYBERSECURITY THREAT ACROSS EVERY INDUSTRY

Every year, improving ransomware prevention capabilities is one of the top priorities for organizations in the immediate future. Even with focused efforts, the risk of the ransomware threat remains high – **survey respondents rank ransomware as their biggest threat among eight categories**.

The survey data validates security teams' concerns, with **75% of organizations reporting being affected[1] by ransomware more than once** in the past 12 months – a jump from 61% last year.

2 THERE IS UNIVERSAL CONCERN ABOUT RANSOMWARE RISKS DRIVEN BY MALWARE EXPOSURES

Nearly 100% of the surveyed organizations are concerned about the potential for identity, session cookie, and other data siphoned from malware-infected devices being used to enable follow-on attacks like ransomware. But some good news – **respondents' second biggest priority for the next 12-18 months is to improve visibility and remediation for compromised credentials and malware-exfiltrated data.**

3 SECURITY TEAMS IDENTIFY THE NEWEST ATTACK VECTOR FOR RANSOMWARE AS MFA BYPASS VIA SESSION HIJACKING

For organizations who reported being affected by ransomware in the past year, stolen cookies that enabled session hijacking ranked as the **third most common entry point for ransomware attempts and successful attacks**, following phishing/social engineering and third-party access.

More than half (57.5%) of teams report that they routinely invalidate or terminate open sessions for applications in response to a managed device getting infected with malware, which shows heightened awareness of the growing session hijacking problem.

4 THIRD-PARTY EXPOSURE IS FUELING EXPONENTIAL RISK ACROSS THE BOARD, AND ORGANIZATIONS ARE FEELING THE IMPLICATIONS

Nearly all surveyed organizations are concerned about the risks from third-party accounts being compromised due to malware infections – and **82% are either extremely or significantly concerned**. Additionally, participants rank third-party access as the second most common entry point for ransomware.

[1] 'Affected' in this context means teams allocated resources to address ransomware attempts and/or full-blown attacks.

KEY FINDINGS BY ROLE AND INDUSTRY →

1

LEADERSHIP VS. SECURITY TEAMS SHOW A DISCONNECT IN CYBERSECURITY PERSPECTIVES

CIOs, CISOs, and other IT security executives are much more confident about their organization's ability to prevent a full-blown ransomware attack – **91% of leaders are generally confident, compared to 54% of security operators, analysts, and incident responders, and 71% of access and identity management professionals**. Likewise, leaders express much higher confidence in their organization's malware and ransomware response capabilities. This difference in perception reflects a disconnect when it comes to shared understanding of an organization's cybersecurity posture.

2

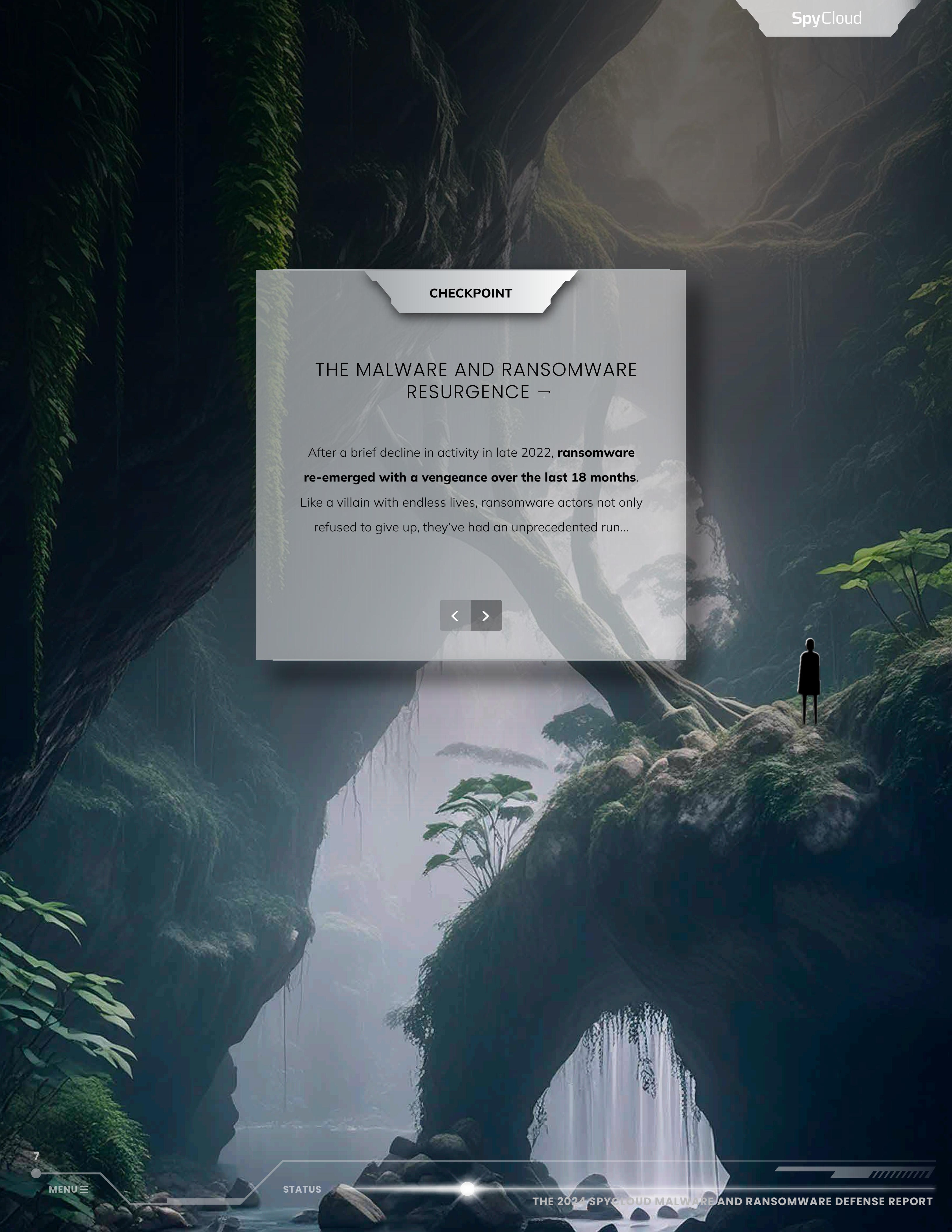
IDENTITY TEAMS ON THE FRONTLINES HAVE MAJOR CONCERNS OVER MALWARE-INFECTED USERS AND RISKS FROM THIRD-PARTY EXPOSURE

Identity and access management (IAM) directors, managers, and team leads are the cohort most concerned about exposure from malware-infected devices and compromised or infected third-party accounts. Case in point, **95% are extremely or significantly concerned about data siphoned from malware-infected devices being used for more harmful attacks**, vs. 83% of security directors, managers, and team leads, and vs. 69% of analysts and incident responders. Additionally, IAM professionals are more concerned about risks to their organization from third-party accounts compromised by malware infections, and are also more likely to name stolen cookies as one of the riskiest ransomware entry points.

3

RANSOMWARE IS THE TOP THREAT ACROSS ALL SECTORS, BUT RELATED CONCERNS, PRIORITIES, AND DEFENSE CAPABILITIES VARY

Survey respondents from each sector rank ransomware as the biggest threat to their organization. However, only three sectors – **manufacturing, retail, and technology** – rate improved ransomware prevention capabilities among their two main priorities in the next 12 to 18 months. **Technology and manufacturing** also express the highest concern for compromised third-party accounts. Interestingly, **retail** respondents rank their ability to identify business applications exposed by a malware infection as their organization's top capability.



CHECKPOINT

THE MALWARE AND RANSOMWARE RESURGENCE →

After a brief decline in activity in late 2022, **ransomware re-emerged with a vengeance over the last 18 months**. Like a villain with endless lives, ransomware actors not only refused to give up, they've had an unprecedented run...

Ransomware payments soared **past $1 billion** in 2023 while the volume, frequency, scope of attacks, and number of new players spiked as well, ranging from solo actors and small groups to powerful syndicates with robust affiliate business models.

Collectively, these actors continuously wreaked havoc across sectors. In the past 12 months, they:

- **Disrupted** the operations of thousands of automotive dealerships for days
- Caused **$100 million** in financial losses to a major hotel and casino chain
- Forced the ninth-largest US city to **close court** hearings and other services for weeks
- Stole **6TB** worth of data belonging to as many as **one-third** of American consumers – including identity and health information – and caused widespread outages across the healthcare ecosystem

These are just a few examples of the destructive power that ransomware wields over organizations. The losses from this destruction can be immense – **the average cost of a ransomware attack is now $4.91 million**.

The resurgence of ransomware comes at a time when another big shift is taking place. Cybercriminals have pivoted to next-generation tactics, using information-stealing malware (or "infostealers") to siphon credentials, session cookies, and identity data from infected users and selling this information to ransomware operators.

At SpyCloud, we have continuously tracked the ongoing rise of the infostealer trend and its impact on follow-on attacks like ransomware. Combined with a similarly explosive growth in digital identity exposure in the past few years, these two trends are fueling a perfect storm for ransomware crimes.

PLAYER TIP

IBM security researchers reported a **266% upsurge in the use of infostealers** by groups that specialize in ransomware.

They also noted signs of "continued investment in infostealer innovation."

PLAYER TIP !

Here are just a few of the components that remove the barrier to entry into cybercrime for aspiring and seasoned players alike:

MALWARE-AS-A-SERVICE (MaaS)

This off-the-shelf model for a variety of malware, and especially infostealers, enables even low-skilled cybercriminals to steal fresh and accurate identity data in bulk, including login credentials, session cookies, and device details – basically everything needed to impersonate an identity.

INSTALL BROKERS

Also known as ad brokers, install services, and pay-per-install (PPI) services, these specialists offer a network of websites and advertisements that facilitate an affordable way to distribute malware at scale.

INITIAL ACCESS BROKERS (IABs)

These individuals or entities sell guaranteed access into an organization's network. IABs typically rent access to tools like infostealers from MaaS providers and then sell the access data to ransomware operators.

RANSOMWARE-AS-A-SERVICE (RaaS)

This widely available business model provides access to an operator's proven tools and tactics – everything needed to launch ransomware attacks, complete with support service and even tutorials – for a subscription fee or percentage of ransom payments.

WHAT SPYCLOUD RESEARCH SAYS

MASSIVE SCALE OF IDENTITY EXPOSURES CREATES NEW RISKS

The scale of identity exposure due to infostealers is massive: **61% of breaches last year were malware-related and responsible for 343.78 million stolen credentials.**

Our recaptured data also shows that as many as **1 in 5 people are the victim of an infostealer infection**, with each infection **exposing anywhere from 10 to 25+ third-party business application credentials, on average.**

INFOSTEALERS LEAD TO FUTURE RANSOMWARE ATTACKS

Through a deep analysis of recaptured infostealer logs, we discovered that the presence of infostealer malware correlates to the likelihood that a company will experience a ransomware attack in the near future.

Nearly one-third of companies that experienced a ransomware event last year had at least one infostealer infection in the 16 weeks prior to being attacked.

ANTIVIRUS, MFA, AND TRADITIONAL DEFENSES AREN'T ENOUGH

According to our recent research, for the first six months of 2024, at least **54% of devices infected with infostealer malware had an antivirus or EDR solution installed at the time of successful malware infection**.[2]

With infostealers and session hijacking at play, traditional solutions like antivirus and multifactor authentication (MFA) don't mean you're fully protected.

So how well are current ransomware defenses keeping up with the pace, tactics, and scale of cybercriminal innovation? That's what we set out to uncover.

[2] 54% is likely low, as not all infostealers collect sufficient data to determine whether an antivirus/endpoint detection & response (EDR) solution was installed and running on the infected device.

CHECKPOINT

WHY WE DO THIS REPORT →

The numbers in this report that show the prevalence and impact of ransomware only tell part of the story. The developments that every organization should be concerned about happen beyond the edges of the cybersecurity world, deep in the criminal underground. This hidden, sprawling ecosystem is home to a burgeoning number of specialized products and services for **cybercrime enablement**.

The standardization and professionalizing of what were once ad-hoc activities is a contributing factor that makes digital identities a top attack vector. With identity data – exfiltrated from user devices infected by malware – at their fingertips, a growing crop of unskilled cybercriminals can hijack a user session, initiate account takeover (ATO), and gain access that enables them to launch ransomware attacks.

We do this survey because our mission is to disrupt the cycle of cybercrime, and the cybercrime problem as it stands today is big.

SURVEY METHOD: HOW WE COLLECTED DATA FOR THIS REPORT →

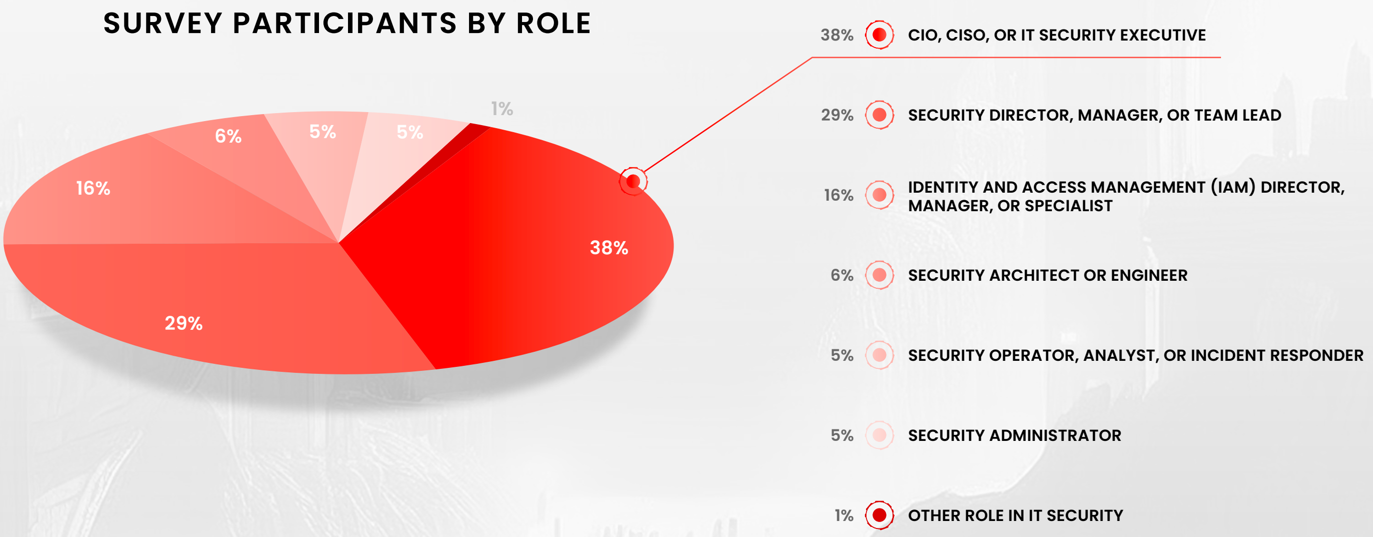
For this fourth annual report, we surveyed 510 individuals in active cybersecurity roles within organizations in the US and the UK with at least 500 employees.

As you'll see, we asked them about:

- Their top concerns about malware and ransomware, as well as current defense practices
- Common entry points for real-life ransomware incidents
- The impact of ransomware attacks on their organization in the past 12 months, including ransom payments, data recovery, and cumulative response costs
- Key ransomware prevention strategies and future security priorities

Survey respondents' roles range from cybersecurity analysts to C-suite security executives. About one-third of the participants come from practitioner roles and others outside of leadership (Figure 1).

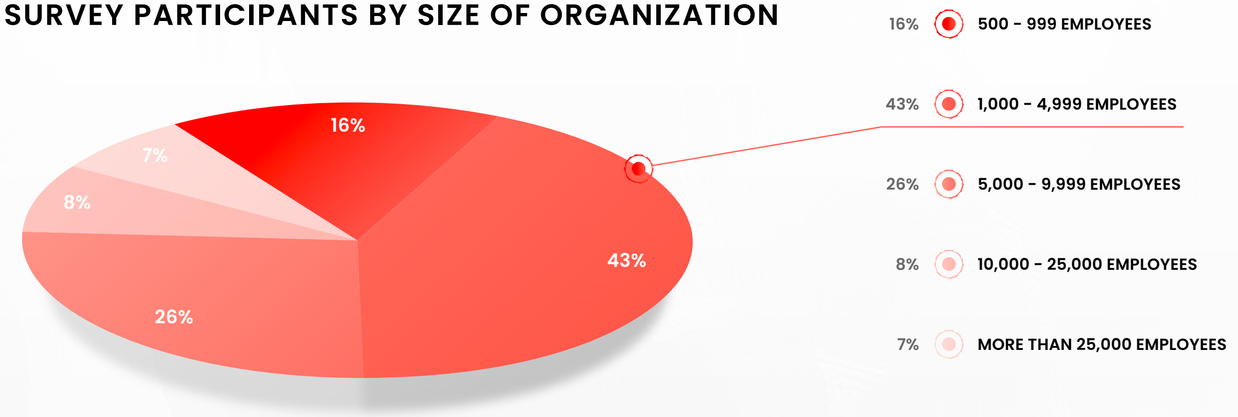
FIGURE 1.



The size of surveyed organizations ranges from small (500-999 employees) and mid-market (between 1,000 and 9,999 employees) to large enterprises (with 10,000 or more employees). The two biggest cohorts represent mid-sized employers: 43% with 1,000-4,999 workers and 26% with 5,000-9,999. Large enterprises (10,000+ employees) comprise a total of 15% of respondents (Figure 2).

FIGURE 2.

SURVEY PARTICIPANTS BY SIZE OF ORGANIZATION

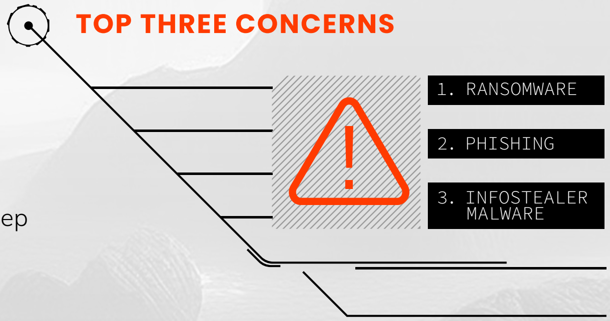


THE DARK BEGINNINGS OF THE RANSOMWARE JOURNEY →

Like the majority of cybercriminals, ransomware actors are largely driven by their desire to build a cache of profits, and businesses are the ones that ultimately pay that price.

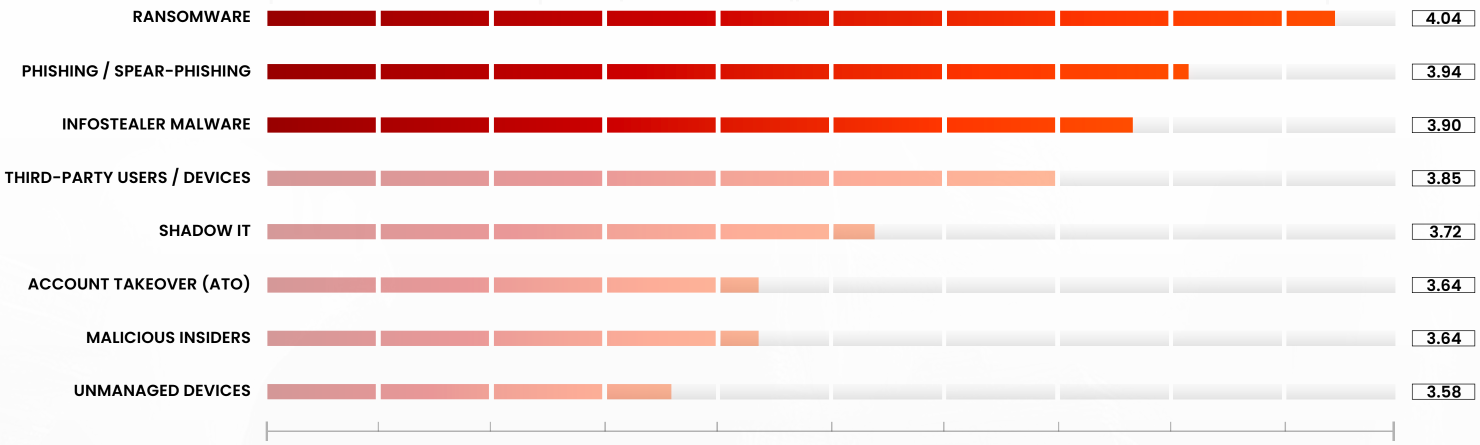
Research suggests that ransom payments surged last year, with a **2.6x increase in the average payment** and 5x in the median. Likewise, recovery costs have followed an upward trajectory every year, climbing to an average of $2.73 million in 2024 (compared to $1.82 million in 2023). As financial losses from ransomware continue to climb, so does the **frequency of incidents**: insurance claims data shows a 64% increase in 2023 compared to the prior year.

So it's no surprise that ransomware maintained a strong lead among our survey respondents as the greatest threat to their organization. Like last year, ransomware, phishing, and infostealers remain the top three concerns that keep security professionals up at night (Figure 3).



TOP THREATS / RISKS REPORTED BY SECURITY TEAMS

FIGURE 3.

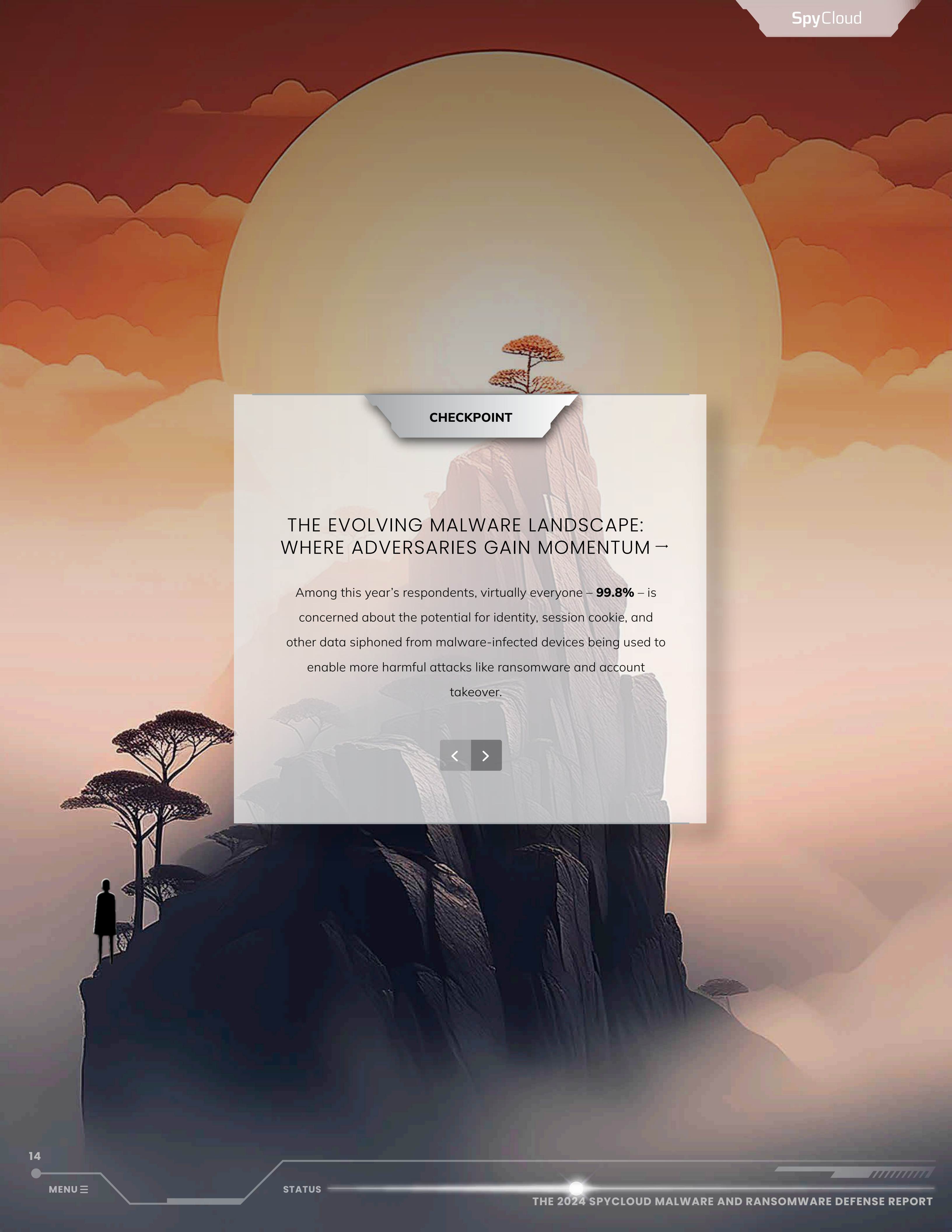


PLAYER TIP

A NEXT-GEN THREAT: HOW SESSION HIJACKING COMPOUNDS RANSOMWARE RISK

Next-generation ATO – which uses **session hijacking** instead of relying on traditional credentials – allows threat actors to sidestep all types of authentication, including MFA and passwordless authentication. By hijacking user sessions that have already been authenticated, cybercriminals (including ransomware operators) become a clone of a legitimate employee, without setting off typical anti-fraud alarm bells. This greatly increases their success rate of gaining access to an organization's network and systems to launch an attack.

Last year, SpyCloud recaptured more than **20 billion cookie records** from infostealer malware, with an average 2,000+ records per infected device. Leveraging malware-siphoned session cookies for next-generation account takeover is becoming an increasingly common cybercrime tactic.



CHECKPOINT

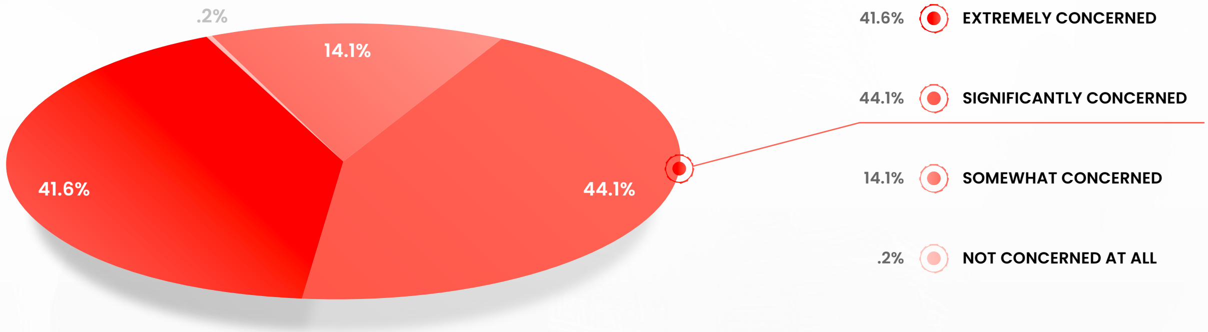
THE EVOLVING MALWARE LANDSCAPE: WHERE ADVERSARIES GAIN MOMENTUM →

Among this year's respondents, virtually everyone – **99.8%** – is concerned about the potential for identity, session cookie, and other data siphoned from malware-infected devices being used to enable more harmful attacks like ransomware and account takeover.

Large breaches like the **Medibank** hack (which leveraged stolen credentials from an infostealer infection) are raising the profile of infostealer malware for security teams. Interestingly, security architects and engineers are the least concerned among the teams surveyed (Figure 4).

FIGURE 4.

CONCERN FOR MALWARE-SIPHONED DATA LEADING TO FUTURE ATTACKS



Our survey findings reflect the growing presence of infostealers in headlines as well as their prevalence as a tactic. What worries us the most is the stealers' continued evolution. Every year, the vast malware expanse draws in **new infostealer families** – often with new capabilities that allow them to bypass IAM security features and evade detection. **Elusive**, for instance, uses advanced encryption to stay stealthy, while **Lumma** can allegedly restore expired auth cookies to hijack user accounts.

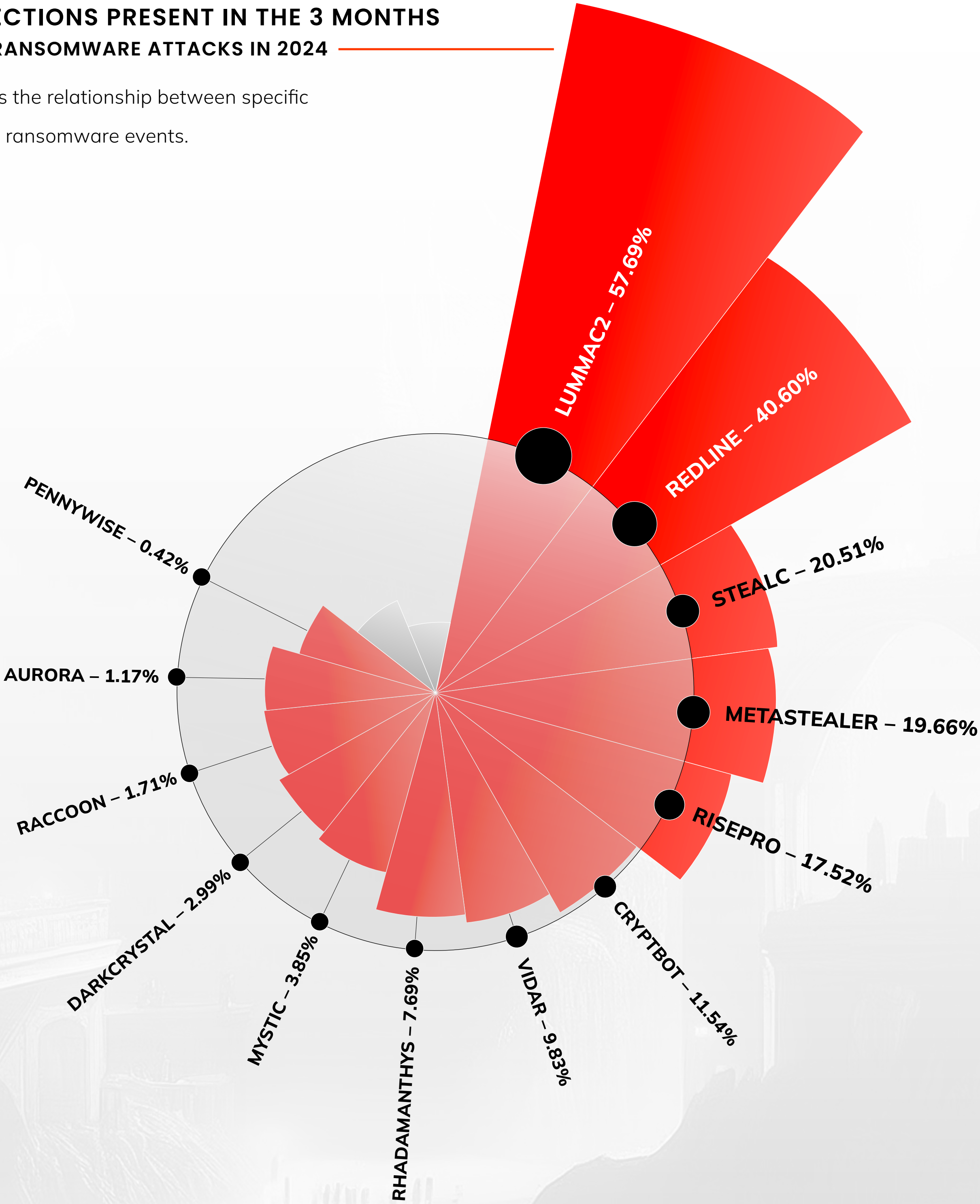
STEALTHY STEALERS AT PLAY

Because infostealers are designed to steal information from an infected host, they make great accomplices to ransomware actors attempting to gain credentials before moving laterally in an environment.

Many infostealers also double as malware loaders, allowing the stealers to load secondary payloads such as persistent malware or ransomware. This behavior is observed in RisePro, Lumma, Mystic Stealer, and others.

INFOSTEALER INFECTIONS PRESENT IN THE 3 MONTHS PRIOR TO REPORTED RANSOMWARE ATTACKS IN 2024

SpyCloud research shows the relationship between specific infostealer infections and ransomware events.



*Domains may have been infected by multiple stealers so percentage totals do not sum to 100%.

TOP INFOSTEALER VILLAINS

LummaC2

Known for its dynamic configurations, LummaC2 can customize what data it steals in real time. In late 2023, it added email theft from various clients, Google cookie regeneration, and turning infected bots into SOCKS proxies. It also targets browser extensions and claims to steal 2FA secrets, making it a multi-faceted threat.

RedLine

A highly adaptable stealer recognized for its dynamic configurations, enabling it to adjust its stealing and loading capabilities on the fly. It can also regenerate expired Google cookies, a feature first observed with LummaC2. Its flexibility and advanced functionalities make it a significant threat, and it has wide acceptance by the criminal community.

StealC

Described as a “copycat of Vidar and Raccoon,” StealC can be customized to steal data based on the cybercriminals’ needs. This infostealer is commonly distributed by so-called **malware traffers** – organized cybercrime workers who are responsible for redirecting victim traffic to malicious content operated by others.

MetaStealer

An “improved version” of RedLine that steals credentials and cryptocurrency wallets. It’s deployed through malspam email campaigns, cracked software advertisements on social media like YouTube, and malvertising.

RisePro

A sophisticated stealer that not only exfiltrates sensitive data but also serves as a malware loader, enabling the deployment of secondary payloads like other malware or ransomware. This dual functionality enhances its threat level.

CryptBot

Reemerged with a new and improved version targeting sensitive data like logins and credit card data stored in browsers. This infostealer is distributed via compromised websites that seem to offer cracked video games and other popular software.

OTHER STEALERS TO KEEP ON YOUR RADAR

WorldWind / Prynt Stealer

While not as configurable as other stealers on this list, WorldWind uses Telegram as its exfiltration route by default, shortening the time to stolen information access, especially for less-technical cybercriminals.

Atomic Stealer

Atomic is notorious for targeting macOS, and particularly cryptocurrency enthusiasts as its victims. It deploys a backdoor specifically designed to steal seed phrases from victims using the Ledger Live crypto wallet. It’s also well-known for harvesting data from browser extensions, making it a broad-spectrum threat.

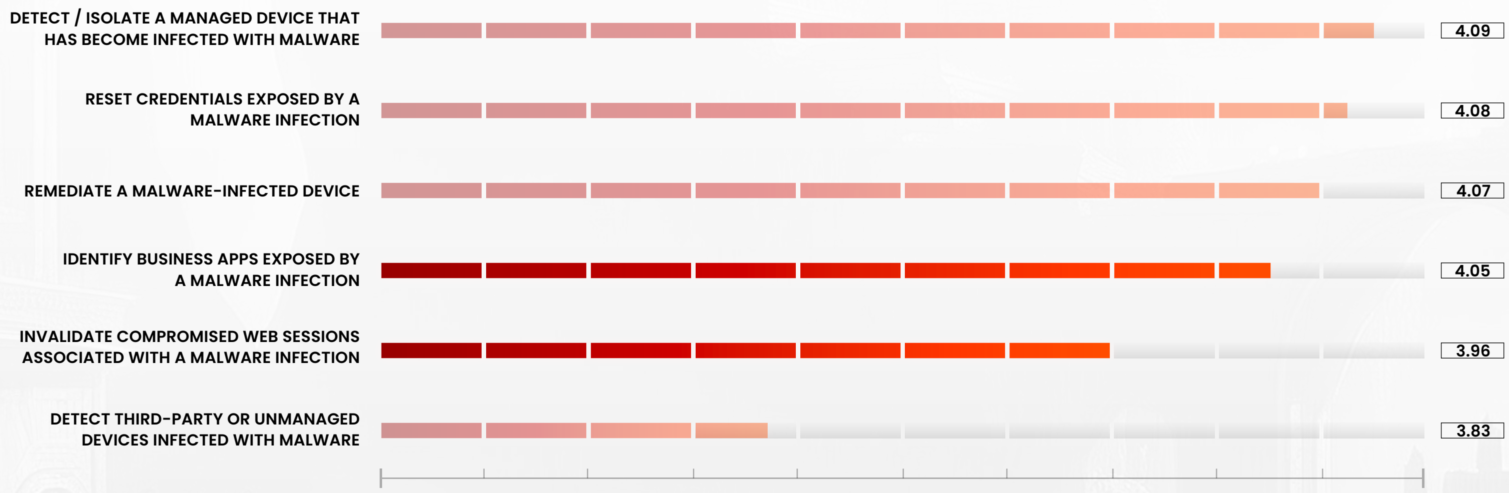
BATTLING CYBER THREATS: FIGHTING FOR THE UPPER HAND

Despite worthwhile concerns about infostealers, surveyed organizations show some big gaps in their ability to remediate malware exposures. **Identifying business applications exposed by malware and invalidating compromised web sessions are two of the most critical steps that address the long-term risks of malware – yet they rank at the bottom of malware detection and response capabilities** (Figure 5).

Perceptions do vary across roles, though. Most notably, executive leaders are the only group that rank all of their organization's capabilities higher than the average across all roles. In general, they seem more confident than other cybersecurity professionals in their security teams' capabilities.

MALWARE DETECTION AND RESPONSE CAPABILITIES

FIGURE 5.



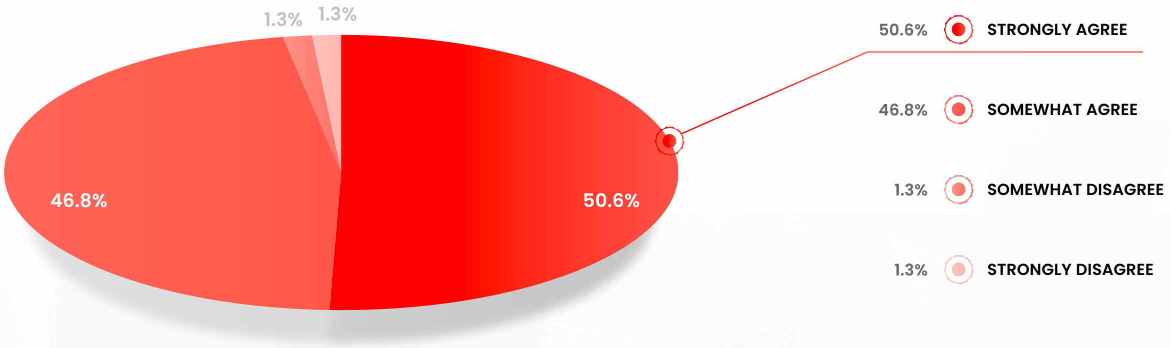
PLAYER TIP

To fully negate opportunities for ransomware and other critical threats, organizations need to leverage **post-infection remediation** steps like resetting application credentials and invalidating session cookies siphoned by infostealer malware. With this extra boost, IAM teams – who are becoming instrumental in the battle against ransomware – and other defenders can finally make strides in the journey to preventing this threat.

Remediating malware can feel a bit like playing in a fog of war. Overwhelmingly, our respondents agree that having better visibility of malware-exfiltrated data (such as exposed credentials and session cookies/tokens) and automating remediation workflows would significantly improve their organization's resistance to ransomware attacks and security posture overall (Figure 6).

FIGURE 6.

BETTER VISIBILITY & REMEDIATION OF MALWARE-EXFILTRATED DATA IS NEEDED



Year over year, **very large enterprises** (25,000+ employees) and the **financial services industry** show the biggest growth in the number of respondents who "strongly agree" with the need to better address malware exposures – a change of +17 and +32 percentage points, respectively.

MALWARE INFECTION REMEDIATION PRACTICES: FAR FROM A CRITICAL HIT

While there's universal agreement that more needs to be done to address the malware problem, we also asked organizations what their standard practices look like today to better understand the baseline.

The top routine actions that organizations take in response to a malware infection on an infected device are:

- Investigating the incident (**79%**)
- Resetting passwords for portentially exposed applications (**77%**)
- Attempting to remove the malware (**67%**)

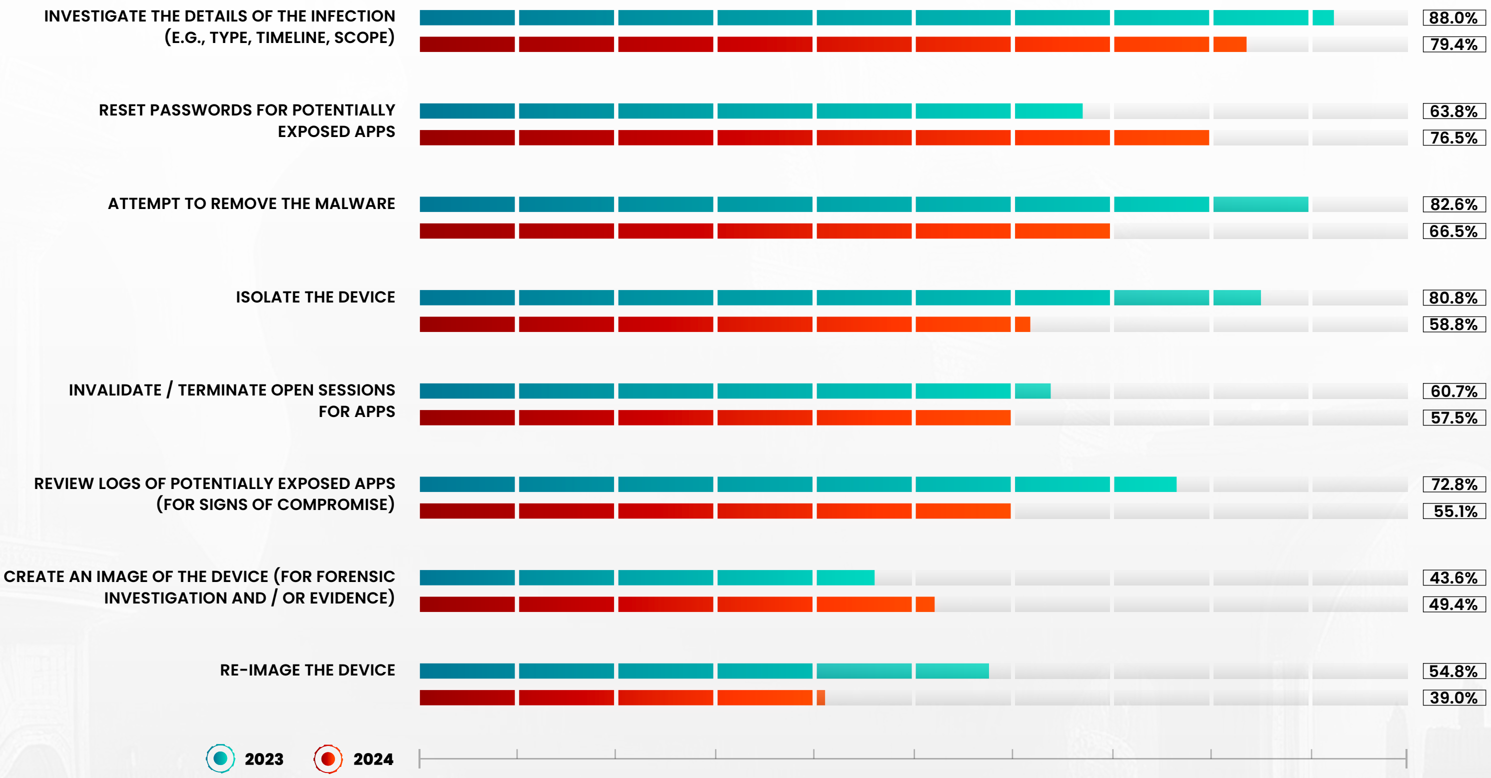
PLAYER TIP

We were pleasantly surprised to see a big year-over-year jump in password resets (**from 64% to 77%**), which may be a positive sign of maturity – though it could just as easily indicate that this is a simple, low-hanging-fruit action.

Regardless of what drove the change, keep in mind the shift to a "brute force" reset and wipe doesn't solve the larger issue of stolen data, and thus access, in the wrong hands. Reviewing logs to analyze exposure and determine the necessary remediation path should be a high priority. Yet even fewer security teams do this than before: only 55% this year vs. 73% last year (Figure 7).

ROUTINE RESPONSES TO MALWARE INFECTIONS

FIGURE 7.



RISK FROM THIRD-PARTY EXPOSURE: ADVERSARIES' EXTRA ADVANTAGE

Threat actors leverage plenty of strategies to gain an upper hand in the malware landscape, but nothing presents as big an opportunity as infected third-party and unmanaged devices. The digital-first environment has opened the floodgates to unmanaged and third-party devices, and security teams often have little-to-no visibility into vulnerabilities associated with these endpoints. This has huge implications because third-party devices and users greatly increase exposure to threats.

PLAYER TIP !

ILLUMINATE YOUR ATTACK SURFACE

Security researchers found that as many as **90% of security compromises originate from unmanaged devices.** Outside of IT control and visibility and with limited security, these devices hold an undeniable appeal for threat actors.

Whether these devices belong to your employees or third parties, they're used to access your corporate applications – and our research shows that, on average, a single malware infection exposes access to **10 to 25 business applications**. Add to that the fact that the average organization has more than **300** applications – technically, a single malware infection can expose access to all of them.

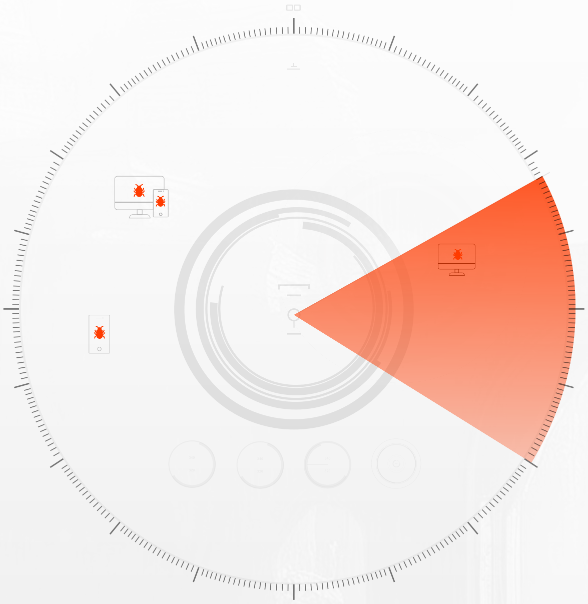
Last year, SpyCloud recaptured more than 4.7 million third-party application credentials harvested by malware on both managed and unmanaged devices. These malware-harvested third-party credentials came from numerous popular business apps in these categories:

- **Communication & collaboration (nearly 2M credentials)**
- **Human resources (1M)**
- **Software development & IT tools (714k)**
- **Customer support (208k)**
- **Identity & access management (204k)**

Each of these compromised third-party applications – as well as every single unmanaged and third-party device – opens the door to sensitive information that can be ransomed.

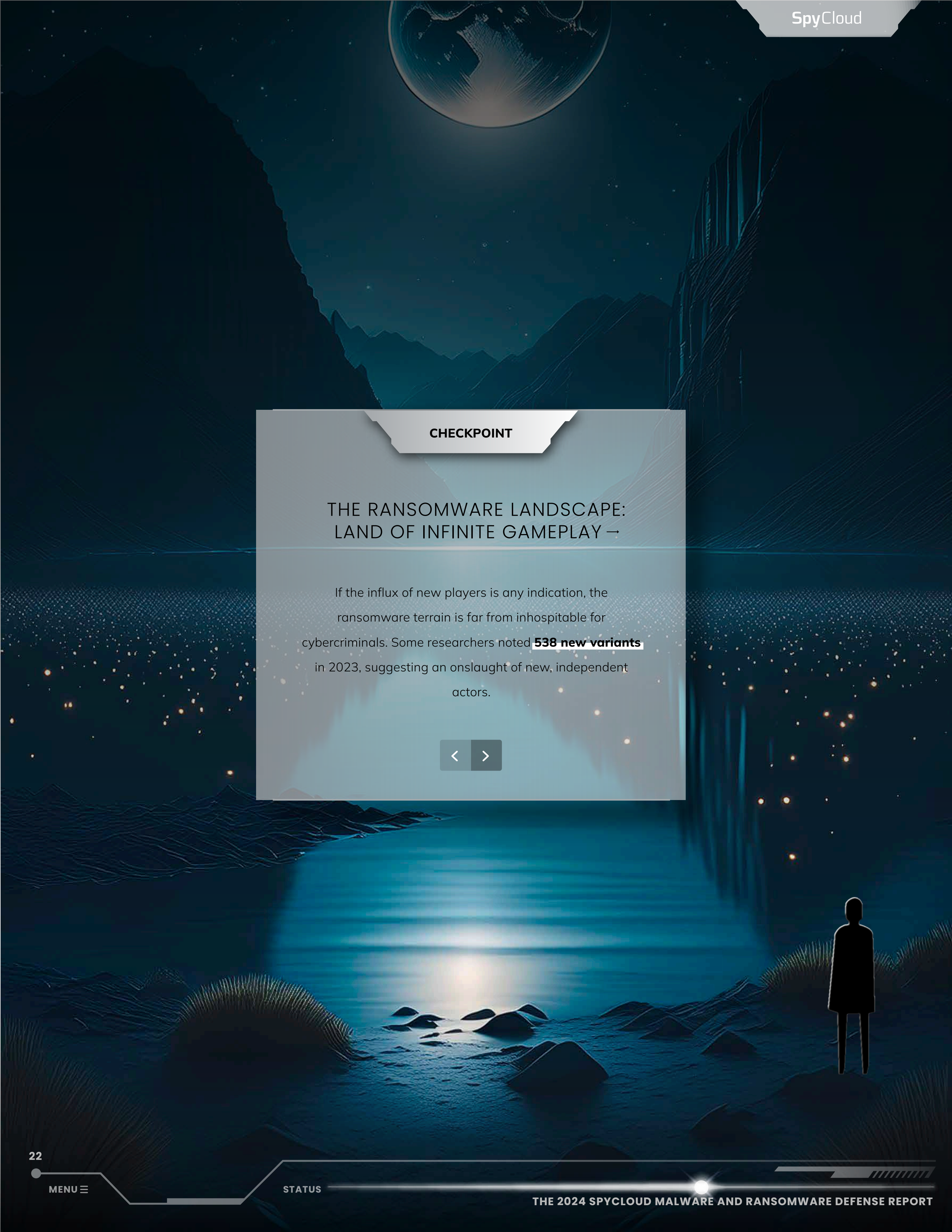
Without visibility into these exposures, it's difficult for an organization to fully understand its risk and properly defend itself.

As shown in Figure 5 earlier, detecting third-party or unmanaged devices infected by malware is the capability organizations lack the most today.



Additionally, almost all survey participants are concerned about risks stemming from infected or compromised third-party accounts (Figure 8, Page 23). Nobody understands the risks better than **IAM teams**, who are the most "extremely" concerned – likely because they understand the reality of both the scale of third-party access to corporate applications, and limitations in organizations' ability to detect or remediate resulting unauthorized access.

Whether cybercriminals leverage compromised third-party accounts, unmanaged devices, or other vulnerable entry points, chances are that with malware tactics, they can quickly escalate to the next level: ransomware.



CHECKPOINT

THE RANSOMWARE LANDSCAPE: LAND OF INFINITE GAMEPLAY →

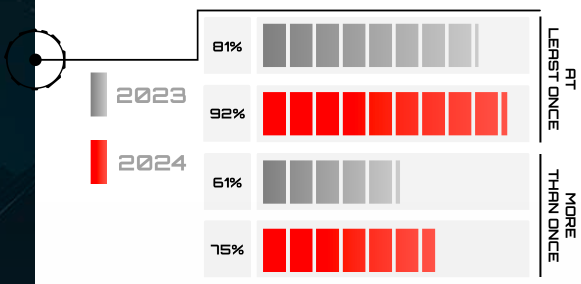
If the influx of new players is any indication, the ransomware terrain is far from inhospitable for cybercriminals. Some researchers noted **538 new variants** in 2023, suggesting an onslaught of new, independent actors.

PLAYER TIP

RANSOMWARE GROUPS – OR EXTORTIONISTS?

Technically, it can be very difficult to encrypt a target and provide keys to unencrypt it after receiving a ransomware payment. Some ransomware groups have taken to skipping the lock and encrypt component of traditional ransomware and have instead largely pivoted to simply **exfiltrating data and extorting payment** in order to prevent the ransomware actor from posting the stolen data on a leak site.

AFFECTED BY RANSOMWARE



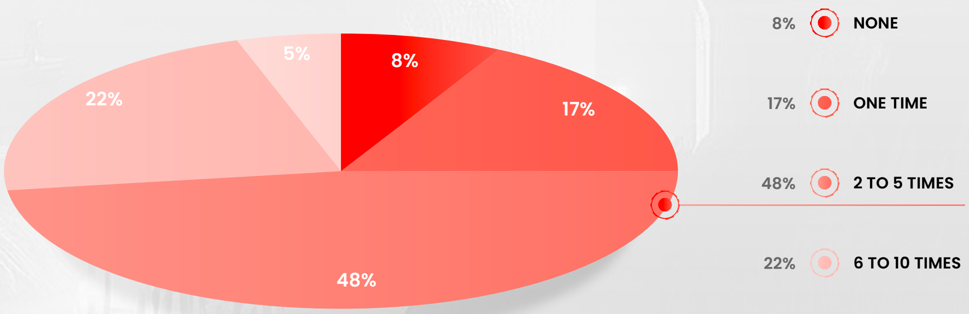
Of course, we've seen some turbulence in this landscape, too, as law enforcement cracked down on the likes of **Hive**, **LockBit**, and **Blackcat AlphV**. But the setback to cybercriminals was temporary, as new ransomware actors quickly stepped up to the plate or others changed groups to avoid detection or sanctioning. Meanwhile, in the latest example of threat actors' resilience, LockBit – **though weakened** – simply respawned a few days later with a new leak site and resumed posting data.

Given the ransomware cybercriminals' stamina, it comes as no surprise to see an increase in the number of surveyed organizations that have been affected by ransomware in the past 12 months. **The number of organizations affected by ransomware at least once rose from 81% to 92% – and those affected[3] more than once grew even more significantly, from 61% last year to 75% this year**.

This means that we saw a sharp decline in organizations that weren't hit at all, down to just 8% this year, compared to 19% in 2023.

FIGURE 8.

FREQUENCY OF RANSOMWARE INCIDENTS IN THE PAST YEAR



[3] 'Affected' in this context means teams allocated resources to address ransomware attempts and/or full-blown attacks.

While all sectors were reportedly affected by ransomware events, based on respondents' answers we found that:

FINANCIAL SERVICES

is the most likely to have been affected at least one time (only 8% answered "none")

TECH COMPANIES

were the most likely to have been affected at least 6 times (83%) as well as more than 10 times (6%)

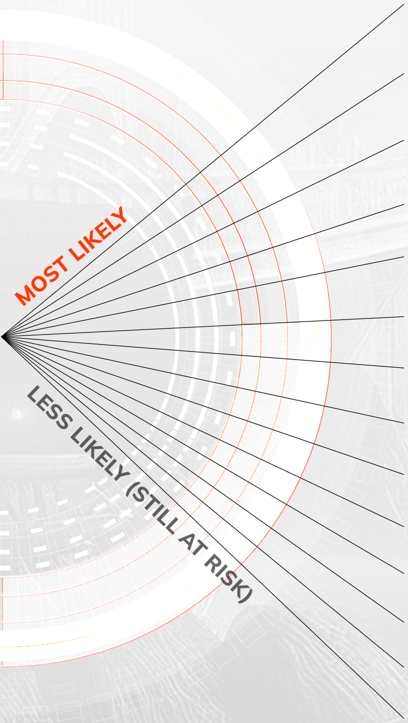
HEALTHCARE

is the least likely to have not been affected at all (17%), followed by professional services (12%)

TOP INDUSTRIES MOST LIKELY TO BE TARGETED BY A FUTURE RANSOMWARE ATTACK IN 2024

SpyCloud
PREDICTION MODEL

Based on recaptured data and malware logs tied to the industries we surveyed, as well as previous self-reported ransomware attacks, SpyCloud calculated a prediction to identify the industries with the greatest risk of future ransomware events.



Insurance (6.3x more likely to experience a ransomware attack)

Healthcare (2.1x more likely to experience a ransomware attack)

Manufacturing

Hospitality

Travel & Tourism

Government

Retail

Financial Services

Energy

Information Technology

Education

Software

Utilities

Telecommunications

DATA, FINANCIAL KNOCKOUTS

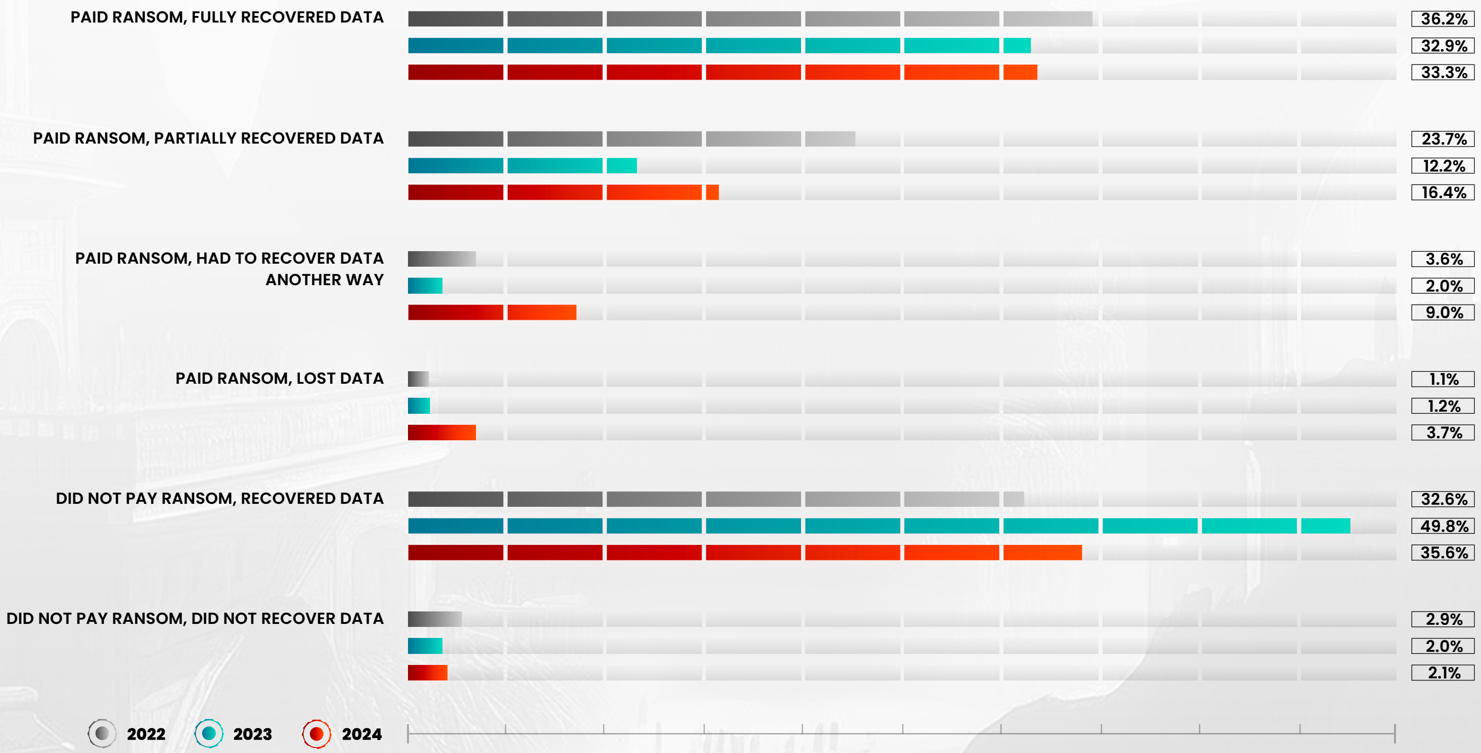
Unfortunately, our data shows that year-over-year, significantly more organizations paid a ransom in the past 12 months: **62% this year vs. 48% in last year's report** (Figure 9). But only about a third of those organizations fully recovered their data, which is a stark reminder that giving in to cybercriminals' demands is a gamble, and the odds are not always in your favor.

Additionally:

- There was a significant uptick in those who paid and lost the data or had to recover it another way: **13% vs. 3% last year**.
- The number of those who paid ransom and lost all their data tripled, from **1.2% to 3.7%**. Fortunately, this number is comparatively small; however, the implications for those who experience this data loss could be felt deeply.

RESPONSE AND OUTCOME TO RANSOMWARE ATTACK

FIGURE 9.

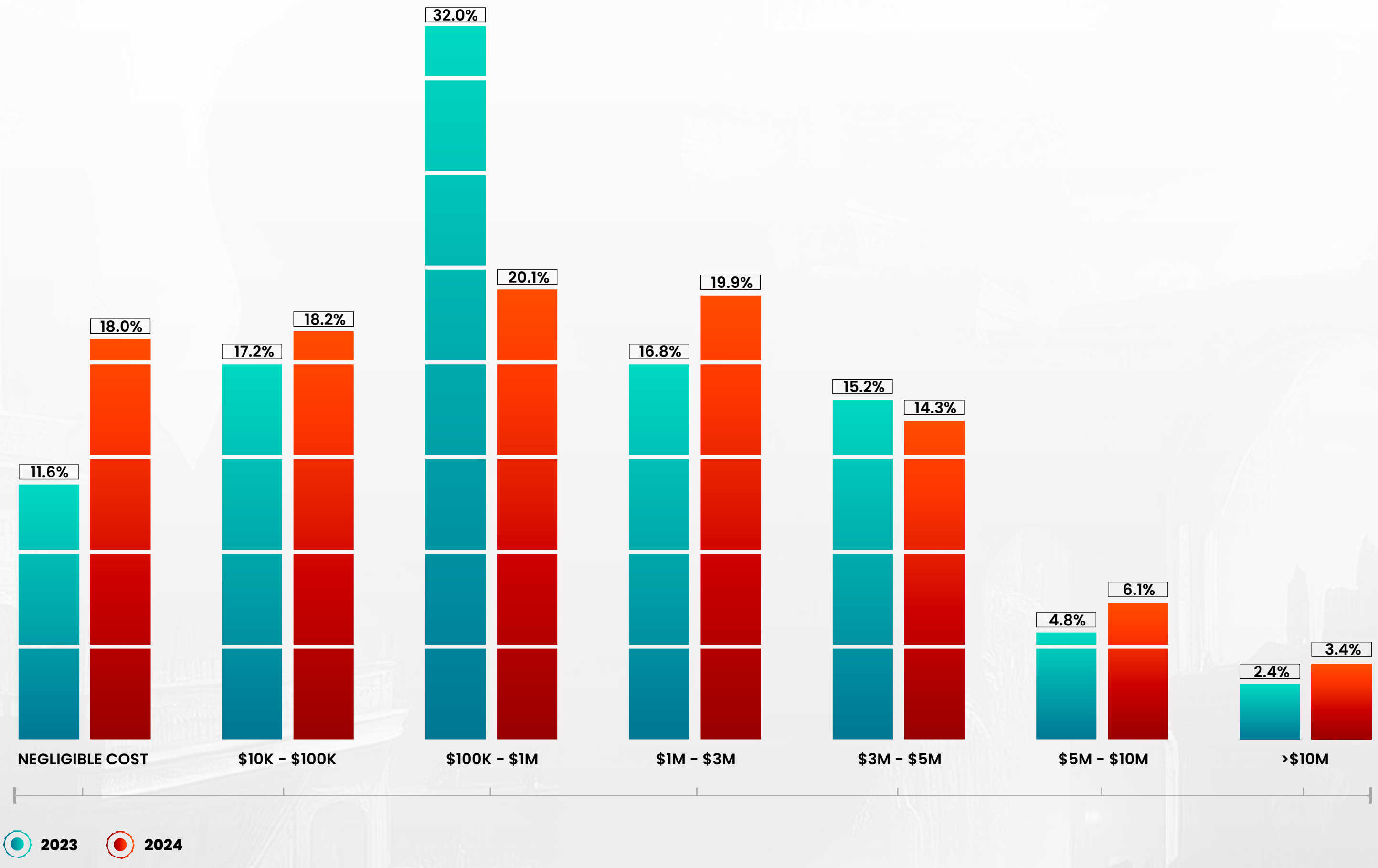


Perhaps buoyed by their growing success rates, ransomware groups have become bolder: **nearly two-thirds of ransom demands last year were for $1 million or more**, with an average of $4.3 million. One ransomware group recently received an unprecedented ransom payment of **$75 million**. And reports to the FBI last year show a 74% increase in the cost of ransomware incidents last year compared to 2022.

We see some of this reflected in our data as well. **There was an increase in the number of organizations paying more than $1 million in cumulative costs – from 39% last year to 44% this year** (Figure 10).

CUMULATIVE COST OF RANSOMWARE ATTACKS IN THE LAST 12 MONTHS

FIGURE 10.



In some cases, cumulative costs can extend to general disruption, loss of business and opportunities, productivity decreases, reputational damage, and more. For instance, **49%** of an organization's computers are impacted by a ransomware attack, which can severely cripple business functions. And, as we saw from some of the recent incidents mentioned earlier, this disruption can last for weeks and sometimes months.

CRACKS IN YOUR CYBER DEFENSES: COMMON ATTACK ENTRY POINTS

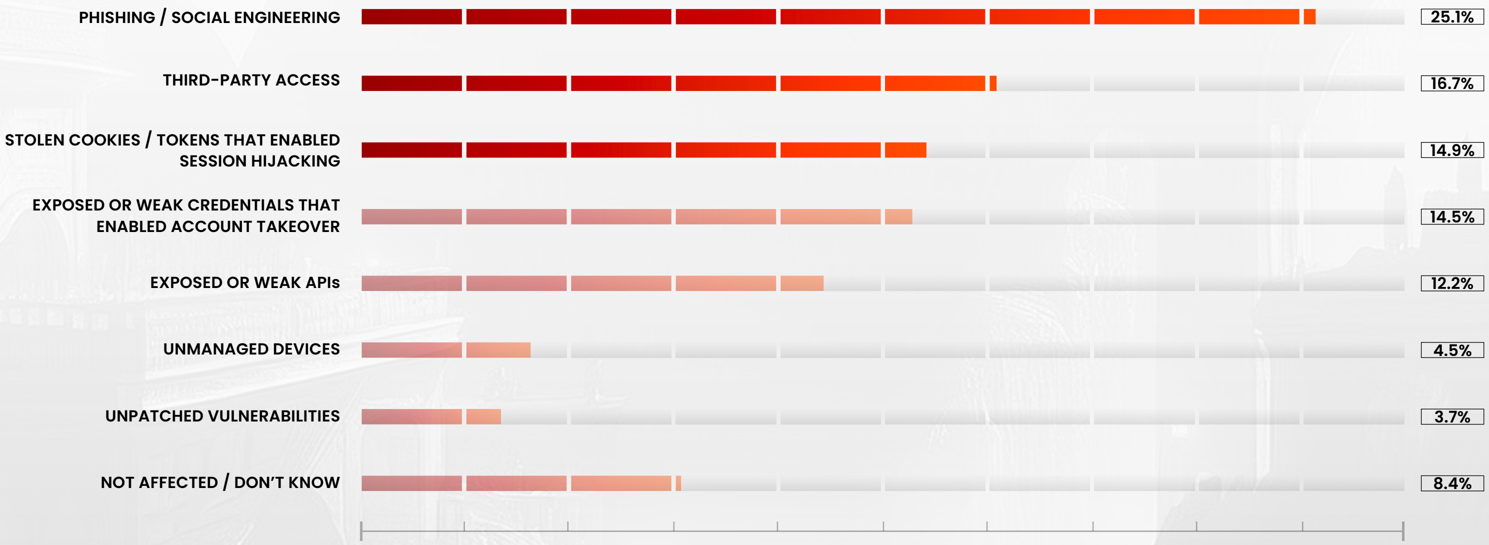
For the first time, we also asked survey participants who were affected by ransomware to share the entry points used by attackers to gain initial access. **They reported the most common entry points to be phishing/social engineering, third-party access, and stolen cookies that enabled session hijacking** (Figure 11).

While compromised session cookies are a newer entry point for ransomware, we expect to see session hijacking continue to gather momentum, and the more organizations are aware and prepared, the better off they'll be. Interestingly enough, identity teams are ahead of others in seeing this entry point more often: 20% of IAM directors, managers, or specialists called it out, compared to only 12% of their security counterparts and 15% of analysts and incident responders.

Some session cookies can remain valid for weeks, months, and even longer. Since many organizations don't yet monitor for cookies stolen by infostealer malware – let alone invalidate those sessions – a single infection could leave an organization exposed. When leveraged by ransomware perpetrators, this access can come with immense consequences.

MOST COMMON ENTRY POINTS FOR RANSOMWARE

FIGURE 11.



In terms of general perceptions about the riskiest potential entry point, it's not unexpected to see phishing/social engineering and unpatched vulnerabilities among the top factors. Most organizations are going to think about areas that historically have been big issues. But this perception also colors their remediation efforts – and traditional remediation methods have lost their effectiveness when it comes to combating the full scope of the ransomware threat.

With ransomware operators showing more interest in next-generation tactics – like using infostealer-exfiltrated session cookies – organizations must shift to next-generation defense. So, are they? As our data below shows, not as much as we'd like to see.

NEXT-GEN SHOWDOWN: THE FUTURE OF RANSOMWARE DEFENSE

Traditional malware mitigation, which is only focused on the infected device, is akin to a stun. At best, it gets rid of the infection. It doesn't prevent cybercriminals from taking advantage of the data they siphoned from the device because it stops short of remediating the prolonged risk from that exposed data. To negate the opportunities created by infostealer-exfiltrated data and to disrupt ransomware attacks, security teams and their counterparts in fraud prevention need to shift their focus to the digital identity.

PLAYER TIP

THE IDENTITY-CENTRIC APPROACH

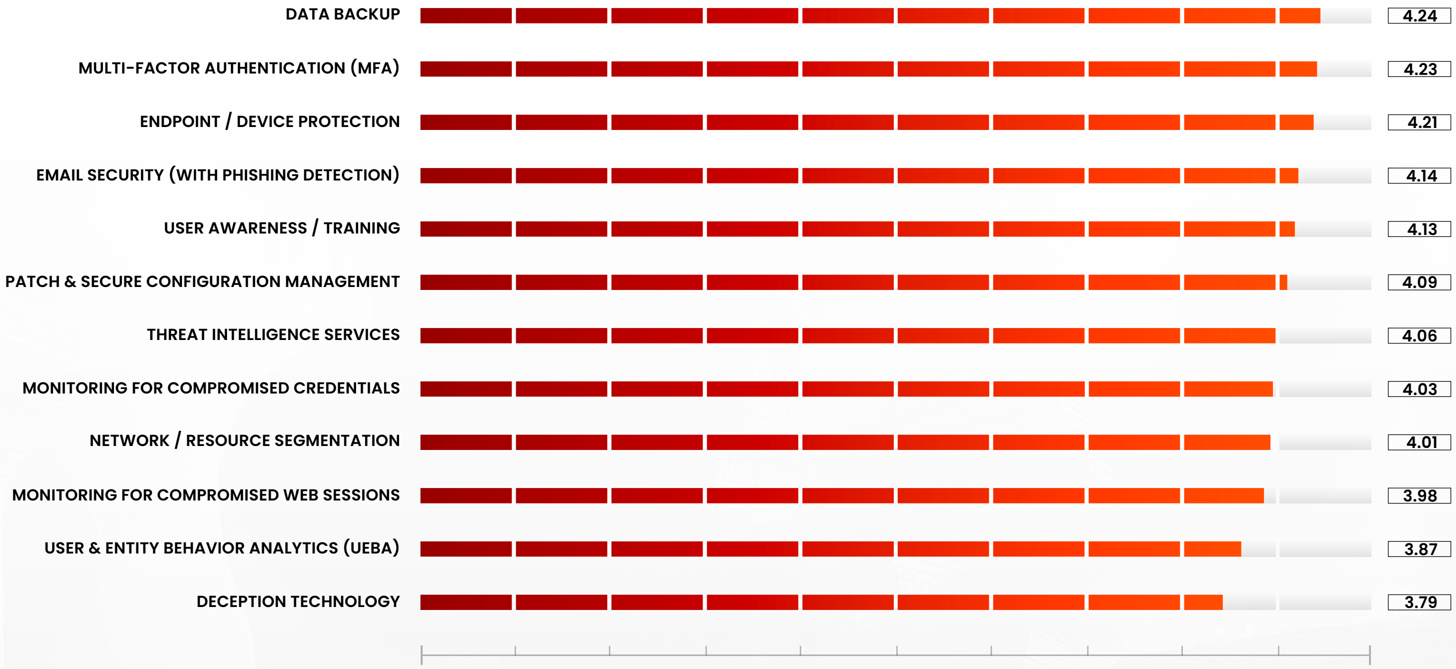
Malicious actors are moving beyond the traditional use of stolen username and password pairs to perpetrate crimes against employees and organizations. Using expanded datasets, criminals have increased the scope of their attack patterns, based upon identity records that come from different sources and that can be linked together using PII, like social security numbers or social handles. Case in point, the **National Public Data breach** is a prime example of how bad actors are targeting identity data that can be used in follow-on attacks.

In this way, users now have to worry about their combined digital identity, which can be formed by cross-referencing the information that has been stolen about them from dozens or hundreds of sources. An identity-centric approach means SOC teams expand their defensive posture beyond just the device to account for the many facets of the modern digital identity.

Identity-centric malware remediation includes extra steps like resetting application credentials and invalidating session cookies that have been exfiltrated by malware. But first, you must monitor for compromised credentials and session cookies – a countermeasure lower on many organizations' priority list this year (Figure 12).

MOST IMPORTANT RANSOMWARE COUNTERMEASURES

FIGURE 12.



Data backup and endpoint or device protection have maintained their position on the list of the most important countermeasures from last year, while MFA moved up six spots to No. 2. This suggests that MFA adoption is now more mainstream, but it's also a cautionary tale. Cybercriminals are adapting to current trends, and as we've seen in the past year, they're targeting MFA. With infostealer-siphoned session cookies, they can simply hijack the session and bypass even the most robust MFA setup.

The bottom line is that a multilayered strategy is as important as ever, but you need to adapt your strategy to make sure old and new critical layers are covered.

CHECKPOINT

INTO THE LIGHT: THE HERO'S JOURNEY →

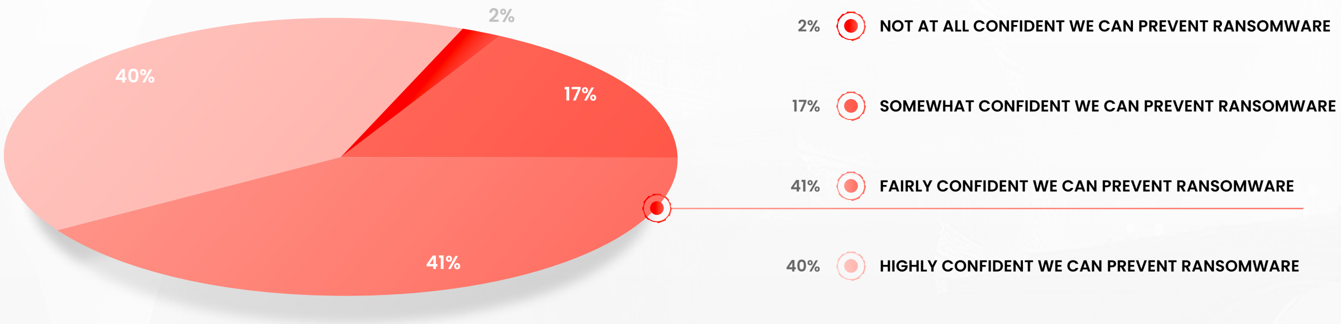
‹ ›

Studies about ransomware sometimes feel apocalyptic – no matter what defenders do, they fall behind. But we noted a ray of optimism this year: there's an uptick in the number of respondents' expressing general confidence in their organization's ability to prevent a full-blown ransomware attack – from 79% last year to 81% this year (Figure 13).

It's worth noting that not all data points support this level of confidence, particularly in areas relating to holistic malware remediation, but it does seem organizations are paving the path to higher ground.

FIGURE 13.

CONFIDENCE ABOUT PREVENTING A RANSOMWARE ATTACK



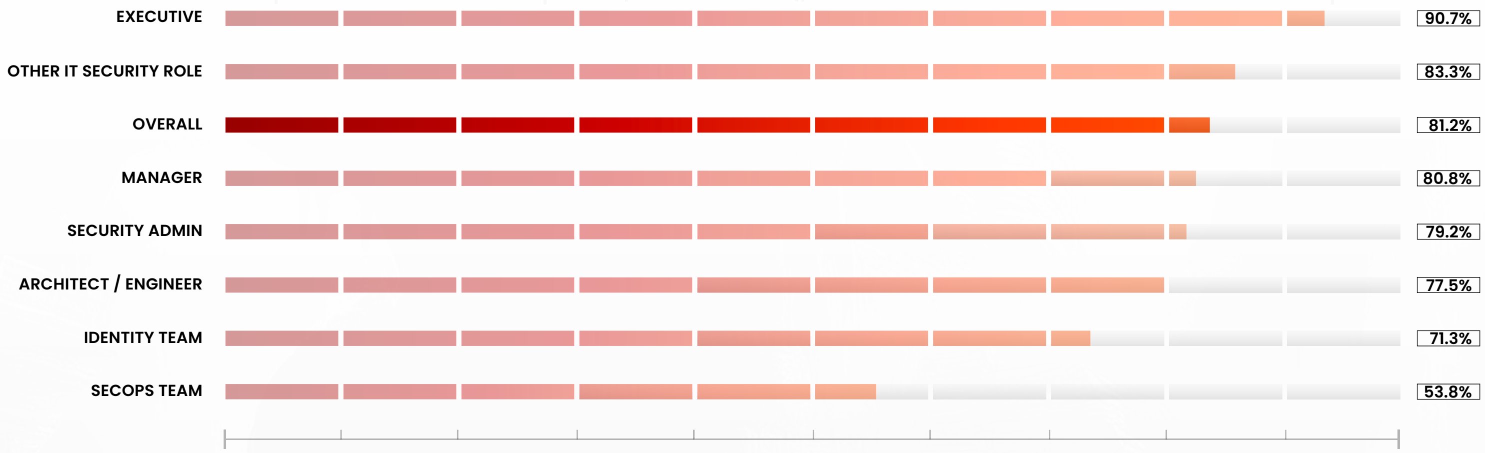
PLAYER TIP

BOOSTING TEAM PLAY

Executive leaders once again are much more optimistic than practitioners and mid-level managers: **91%** are generally confident about preventing a full-scale ransomware attack, compared to **80%** of security directors, managers, and leads. On the other end of the scale, only **54%** of security operators, analysts, and incident responders share this sentiment – likely colored by the flood of threats they see day in and out.

CONFIDENCE IN ABILITY TO PREVENT RANSOMWARE ATTACKS BY ROLE

FIGURE 14.



As noted earlier, executives are also more confident than everyone else in their organization's malware detection and response capabilities. This is perhaps a sign of a small disconnect, showing a need for the C-suite to be deeper acquainted with their organizational cybersecurity posture.

Both sides can be the heroes of their story if they work together to ensure better alignment. After all, they're on the same team. That makes them partners in upholding their organization's trust and brand reputation – choosing more preventative, layered, and calculated approaches that suit the needs of their board, their customers, and external stakeholders.

Add to that some other good news that tips the odds in favor of the SOC:

- More teams "strongly agree" that they need visibility into malware-exfiltrated data, particularly the very large enterprises (25,000+ employees) and the financial services industry.
- More organizations are taking the right steps to remediate malware, with an uptick in respondents reporting that they proactively reset passwords for exposed applications. Larger organizations show even more signs of maturity, like adopting full remediation steps to respond to malware infections on managed devices.
- Organizations are recognizing that stolen cookies that enable account takeover create high risk of ransomware attacks, and are adopting practices to routinely invalidate or terminate open sessions on managed devices compromised by malware.
- IAM teams appear to be more tuned into the identity-related threats and are playing a bigger role in the fight.

REEVALUATING PRIORITIES FOR THE BATTLE AHEAD

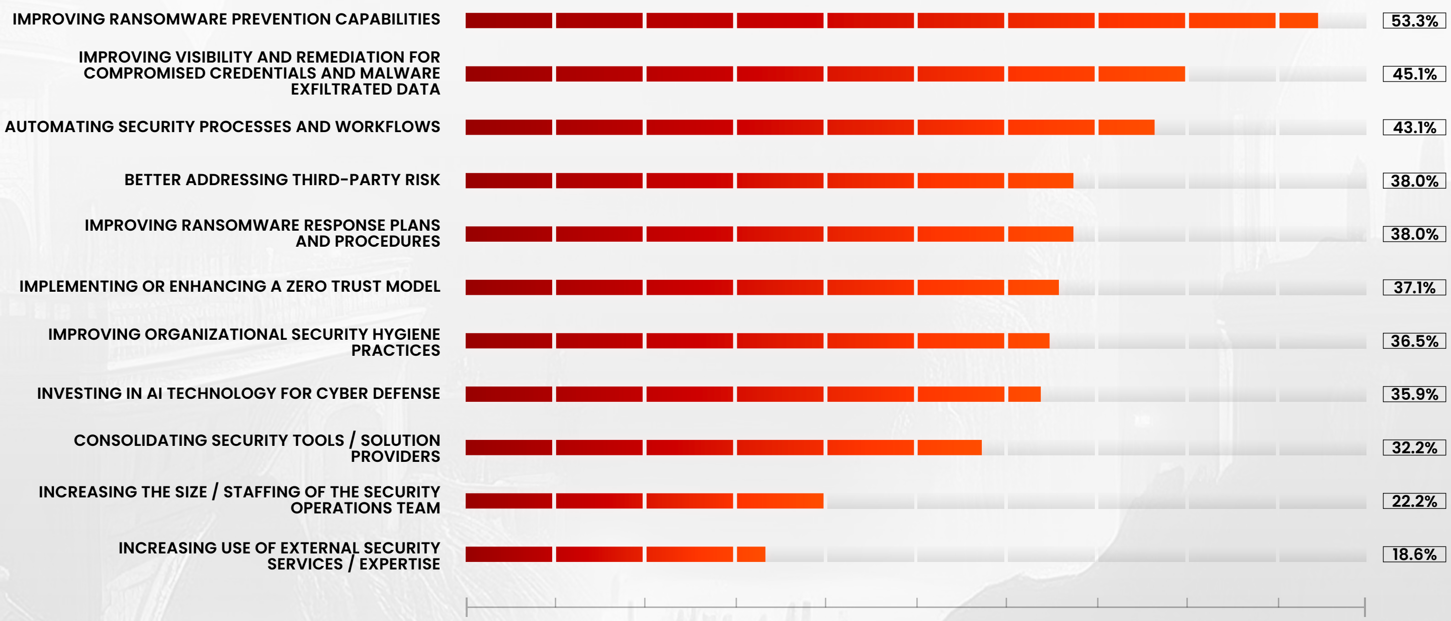
So where are we headed next? Looking ahead at the next 12 to 18 months, the top five priorities for organizations are:

- Improving ransomware prevention capabilities
- Improving visibility and remediation for compromised credentials and malware-exfiltrated data
- Automating security processes and controls
- Better addressing risk tied to third-party exposures
- Improving ransomware response plans and procedures

These are solid plans, and we're cautiously optimistic – we have seen many of the same priorities in the past year, yet exposure remains high. We're also surprised to see Zero Trust implementation in the middle of the pack, considering this model has become somewhat of a standard across all sectors (Figure 15).

TOP FUTURE SECURITY PRIORITIES

FIGURE 15.



Ultimately, making headway in this fight will require a paradigm shift to an identity-centric approach. And, as the number of exposed identities continues to expand, making this shift grows increasingly urgent.

LOOKING TO THE HORIZON: HOW TO DEFEAT CYBERCRIMINALS IN THE LONG GAME →

As opposed to more targeted attacks, infostealers are often launched at scale against a wide array of targets. To identify targets for follow-on attacks, criminals using stealers employ tools and services to sift through massive amounts of exfiltrated data, selling the most critical access to specialized brokers or using the access themselves for other attacks, including ransomware.

To stop cybercriminals before they can profit from stolen data, security teams need to work quickly and proactively. Strategies we recommend:

ADOPT AN IDENTITY-CENTRIC SECURITY APPROACH

With digital identities now firmly in cybercriminals' sights, relying on old defense tactics like device-centric remediation is bound to fail. Outpacing ransomware players is an attainable goal when you can act on the full expanse of compromised identity data for your users, whether it involves employees, contractors, or vendors.

ILLUMINATE YOUR FULL ATTACK SURFACE, INCLUDING UNMANAGED AND THIRD-PARTY USERS

Unauthorized third-party access is high on teams' radar, rated as the second most risky entry point for ransomware in this year's survey. By improving visibility into malware-exfiltrated data – including unmanaged and third-party devices outside of traditional corporate oversight – you'll have more complete coverage and faster discovery of exposed applications, and therefore drastically reduce your time to remediation.

USE AUTOMATION TO SPEED UP DETECTION AND MITIGATION

We know cybercriminals are **leveraging automation**, but as they get faster, so can we. By leveraging automated alerts and incident notifications for new breaches and malware infections, you can more quickly operationalize data and feed it into automated remediation workflows to negate its impact.

EXPAND ATO PREVENTION TO ACCOUNT FOR BOTH TRADITIONAL AND NEXT-GENERATION THREATS

In addition to hardening credentials to block traditional ATO, defenders have to expand focus to prevent session hijacking by monitoring for stolen web sessions programmatically – and then implement processes for invalidating web sessions associated with infected identities. Think of it as changing the locks before anyone can get in.

DEPLOY A CONTINUOUS ZERO TRUST APPROACH

Only 37% of organizations plan to prioritize implementing or enhancing their Zero Trust model in the near future. As it's become a standard, continuing to invest in **Continuous Zero Trust** can go a long way to help organizations account for the full scope of identity, device, and access information that criminals have in hand about employees. By continuously verifying every user's identity for compromise when accessing your applications, you can get ahead of costly attacks and prevent unauthorized access.

YES, THE ENEMY LURKS, BUT ONWARD WE TREAD →

MOVING FORWARD DESPITE PERSISTENT RISKS

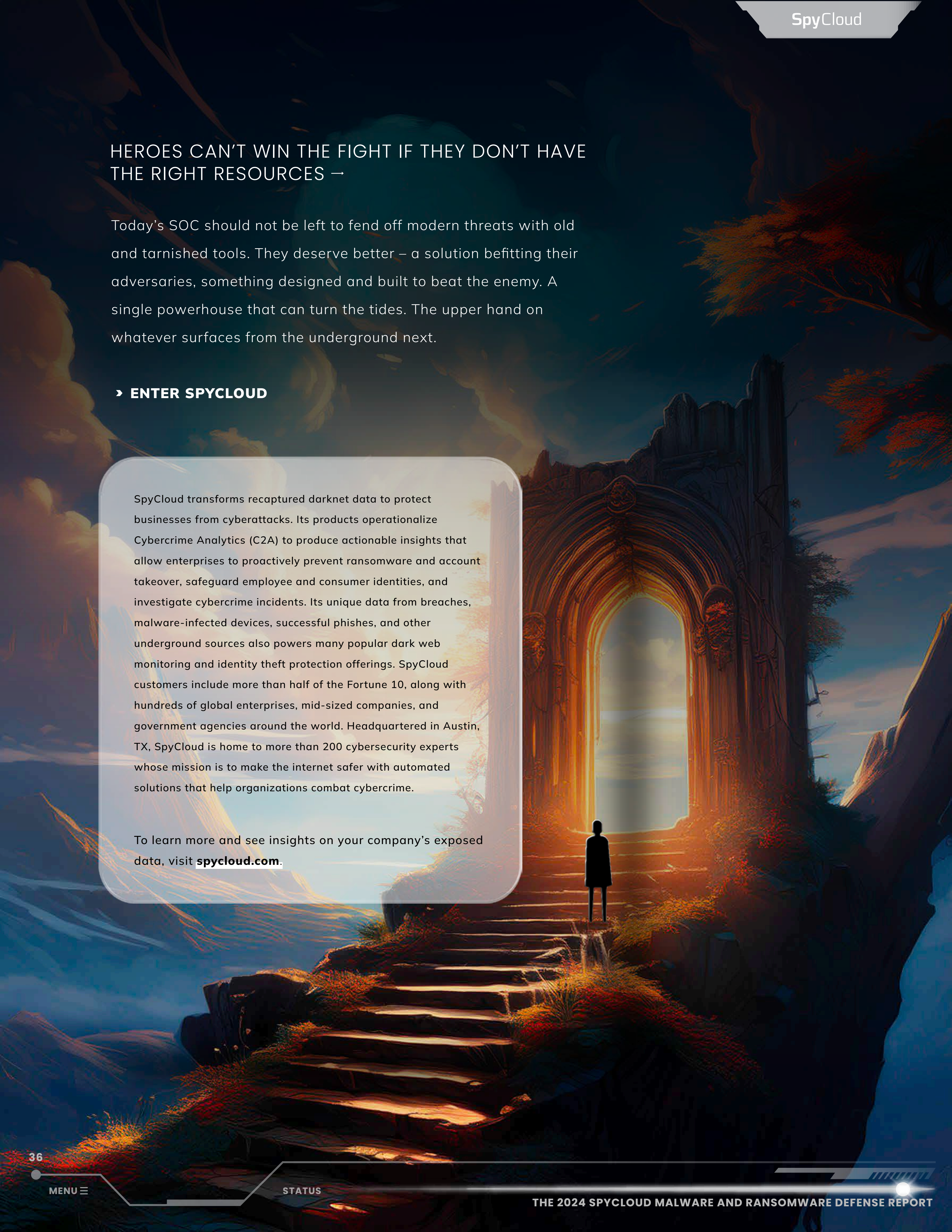
Infostealers are too successful for ransomware operators to stop using any time soon. This quiet precursor to ransomware is notoriously difficult to detect. Virtually all our survey respondents are worried about the potential of malware-siphoned data to be leveraged for follow-on attacks – and rightfully so.

Although this year’s results give us a sliver of hope, organizations can strategically focus resources to achieve a more complete malware response to prevent ransomware attacks:

- **Phishing, infostealer malware, and third-party users and devices** are among the greatest threats that survey participants have identified, and all these threats work in tandem to compound the risk of ransomware.

- The most effective capabilities for complete malware remediation, including **identifying applications exposed by malware infections and invalidating compromised web sessions**, are areas where organizations can make the most improvements.

- Just over half of organizations take steps like **reviewing logs of potentially exposed applications and terminating open sessions for applications** – and without those steps, they remain exposed.



HEROES CAN'T WIN THE FIGHT IF THEY DON'T HAVE THE RIGHT RESOURCES →

Today's SOC should not be left to fend off modern threats with old and tarnished tools. They deserve better – a solution befitting their adversaries, something designed and built to beat the enemy. A single powerhouse that can turn the tides. The upper hand on whatever surfaces from the underground next.

› **ENTER SPYCLOUD**

SpyCloud transforms recaptured darknet data to protect businesses from cyberattacks. Its products operationalize Cybercrime Analytics (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, successful phishes, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include more than half of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to make the internet safer with automated solutions that help organizations combat cybercrime.

To learn more and see insights on your company's exposed data, visit **spycloud.com**.