SpyCloud

RANSOMWARE DEFENSE REPORT

2023

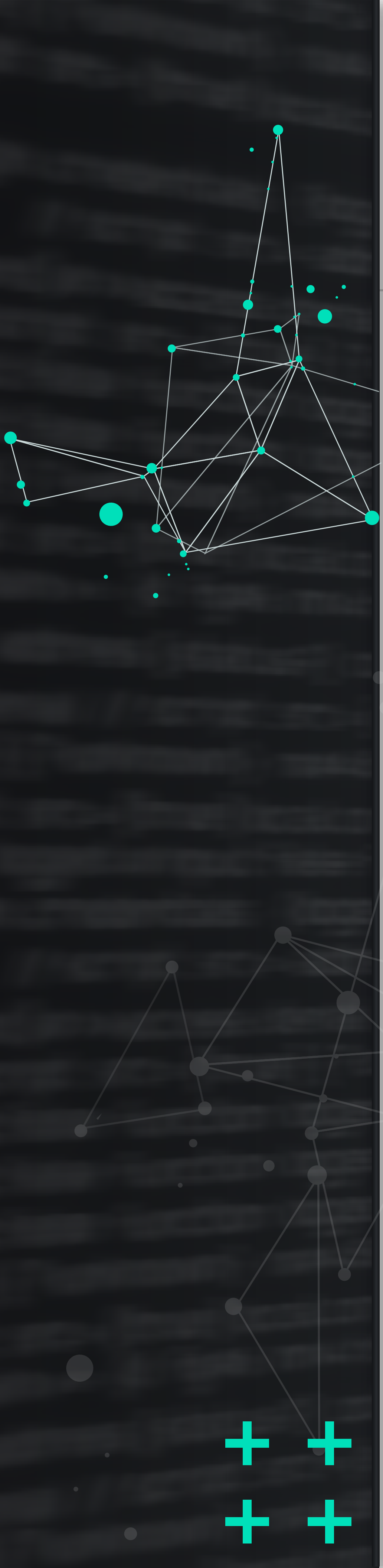


TABLE OF CONTENTS

WHAT TO EXPECT IN THIS YEAR'S REPORT

▽

Last year, we found that organizations were losing ground and felt less confident about their defenses than before. **This year's Ransomware Defense Report** examines how security frontline and leadership perceptions, practices, and priorities have changed since then, and how SecOps teams are doing in their fight against ransomware.

INTRODUCTION

For the last several years, we've watched our workplaces digitally transform, making the convenience of working and collaborating from anywhere the rule rather than an exception. Many organizations have welcomed this new reality, but they've struggled to keep their security defenses in step with the fast pace of digital growth and an expanding attack surface.

Cybercriminals, however, haven't had any problem staying current with a digital-first, cloud-first environment. As they quickly pivot to next-generation tactics for exfiltrating data and access, security operations (SecOps) teams are falling farther behind – while exposure to cyberattacks like ransomware is at an all-time high.

Some Background Before You Dig In

After the release of our last Ransomware Defense Report in September 2022, ransomware attacks showed some promising signs of slowing down. Criminals tested other tactics and government agencies cracked down, with the number of attacks **leveling off** by the end of year. But that glimmer of hope fizzled quickly, with attackers picking up the pace so fast in 2023 that we're headed toward the **second-most costly year** for ransomware in history.

Even through that ebb-and-flow, the sophistication and impact of ransomware attacks has grown. At least one new ransomware group with double-extortion abilities **surfaced** every month last year, while the average cost of a ransomware attack escalated to **$5.13 million** – surpassing the average cost of a data breach.

And one thing hasn't changed: ransomware is one of the toughest cybersecurity challenges organizations of all sizes and industries continue to face. In SpyCloud's **2023 Malware and Readiness Defense Report**, security leaders and practitioners ranked ransomware as the top threat to their organization's security.

WHY WE DO THIS SURVEY

As we note in our findings, ransomware defenses are not keeping pace with cybercriminals. We do this survey to shine a light on one of the contributing causes: an emerging threat that could be an early warning sign of a ransomware event – information-stealing malware, or infostealers.

Criminals are using infostealers to siphon authentication data – including logs with information that enable access to enterprise networks and applications – and selling the data to ransomware operators. And through a deep analysis of recaptured infostealer logs, we've uncovered that the presence of infostealer malware is related to the likelihood that a company will experience a ransomware event in the near future.

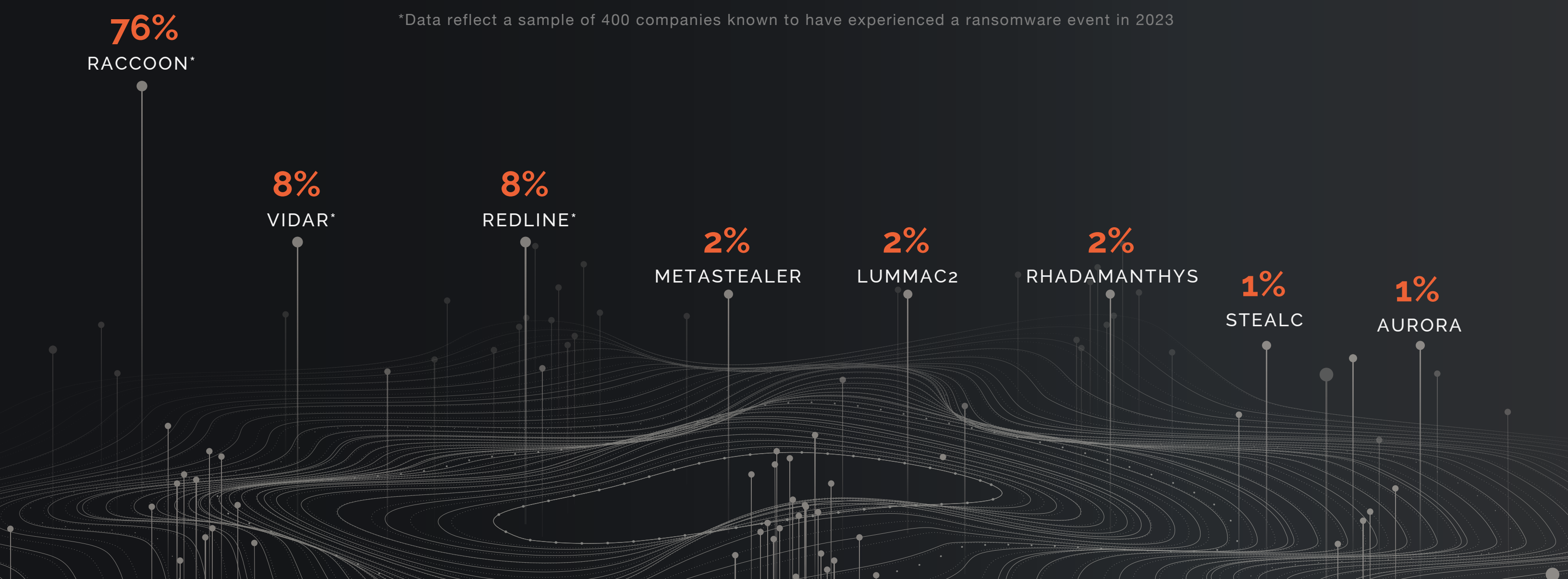
THE INFOSTEALER-RANSOMWARE CONNECTION, BROKEN DOWN

SpyCloud researchers conducted a detailed analysis using ransomware event data from **ecrime.ch** and our own database of recaptured records from the criminal underground. **Of 1,831 North American and European companies victimized by ransomware in 2023, 22% had at least one infostealer infection prior to being attacked.**

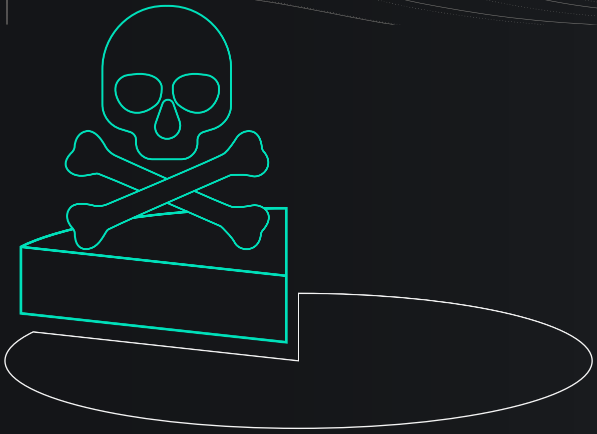
Our analysis also showed that the presence of specific infostealer infections – Raccoon, Vidar, and Redline – increases the probability that a company will experience a ransomware event.

THE MOST PREVALENT INFOSTEALER FAMILIES ASSOCIATED WITH RANSOMWARE VICTIM COMPANIES

Companies with Raccoon, Vidar, and Redline infostealers experienced a ransomware event within an average of 16 weeks post-infection.



*Data reflect a sample of 400 companies known to have experienced a ransomware event in 2023



IN 2023, MORE THAN A FIFTH OF NORTH AMERICAN AND EUROPEAN RANSOMWARE VICTIM COMPANIES HAD AN INFOSTEALER INFECTION PRIOR TO BEING ATTACKED.*

*Data reflect a sample of 1,831 companies known to have experienced a ransomware event in 2023.

Many organizations fail to fully remediate infostealer and other malware infections, focusing primarily on protecting the infected device and skipping critical remediation of exposed credentials and active session data, leaving them exposed to follow-on attacks. In addition to presenting survey results in this report, we offer insights about how comprehensive **Post-Infection Remediation** can help prevent ransomware attacks – and ultimately enable security teams to get ahead of attackers.

About the SpyCloud Ransomware Report

Since 2021, SpyCloud has gathered insights from security leaders and practitioners about ransomware's impact on their organizations and their defensive practices. In this third year of the report, we continue to analyze the trends related to the evolution of this costly cyber threat.

We surveyed 316 individuals in active cybersecurity roles within organizations in the US, Canada, and the UK with at least 500 employees. **We asked them about:**

1

TOP CONCERNS
about ransomware for their business, including financial impact

2

THE MOST COMMON
defenses their organizations have in place or on their roadmap

3

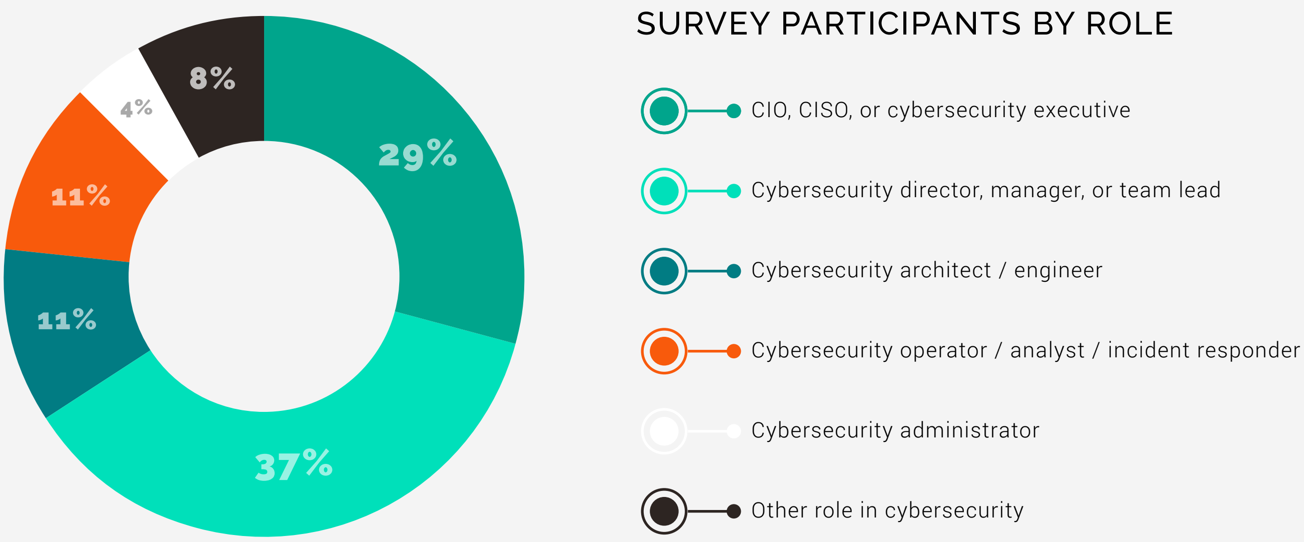
KEY GAPS
that may be leaving their organizations exposed

The report also provides insights into next-generation strategies that support a more complete remediation cycle. We encourage you to look at these trends and learn how best practices are evolving to keep pace with new ransomware tactics, techniques, and procedures (TTPs).

Survey Demographics

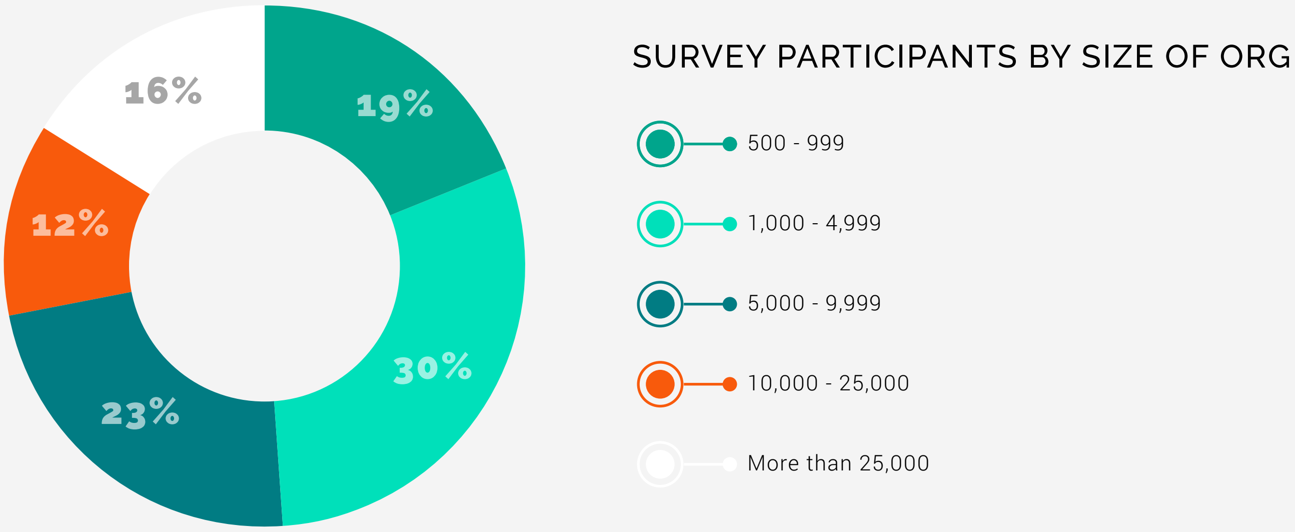
SpyCloud solicited responses from individuals whose roles range from cybersecurity analysts to C-suite security executives. The majority of the 316 participants come from leadership levels: 37% are cybersecurity directors, managers, or team leads; 29% are CIOs, CISOs, and security executives (Figure 1).

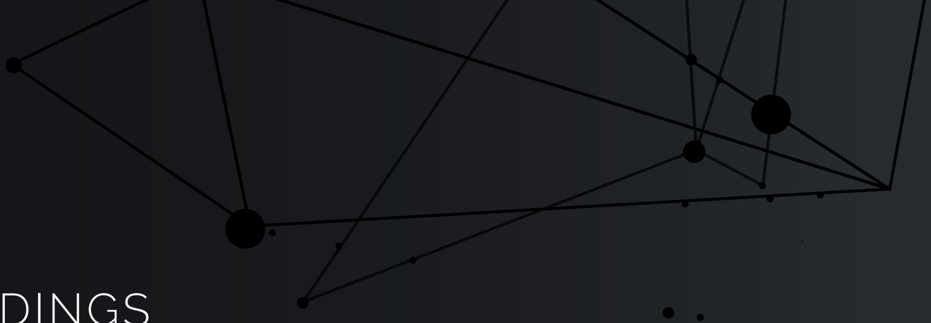
SpyCloud Figure 1 ▶


SURVEY PARTICIPANTS BY ROLE

The cross-section of surveyed organizations ranges in size from small (500-999 employees) and midmarket (between 1,000 and 9,999 employees) to large enterprises (with 10,000 or more employees). The two biggest cohorts represent mid-sized employers: 30% with 1,000-4,999 workers and 23% with 5,000-9,999. The largest enterprises (10,000+ employees) comprise a total of 28% of respondents (Figure 2).

SpyCloud Figure 2 ▶

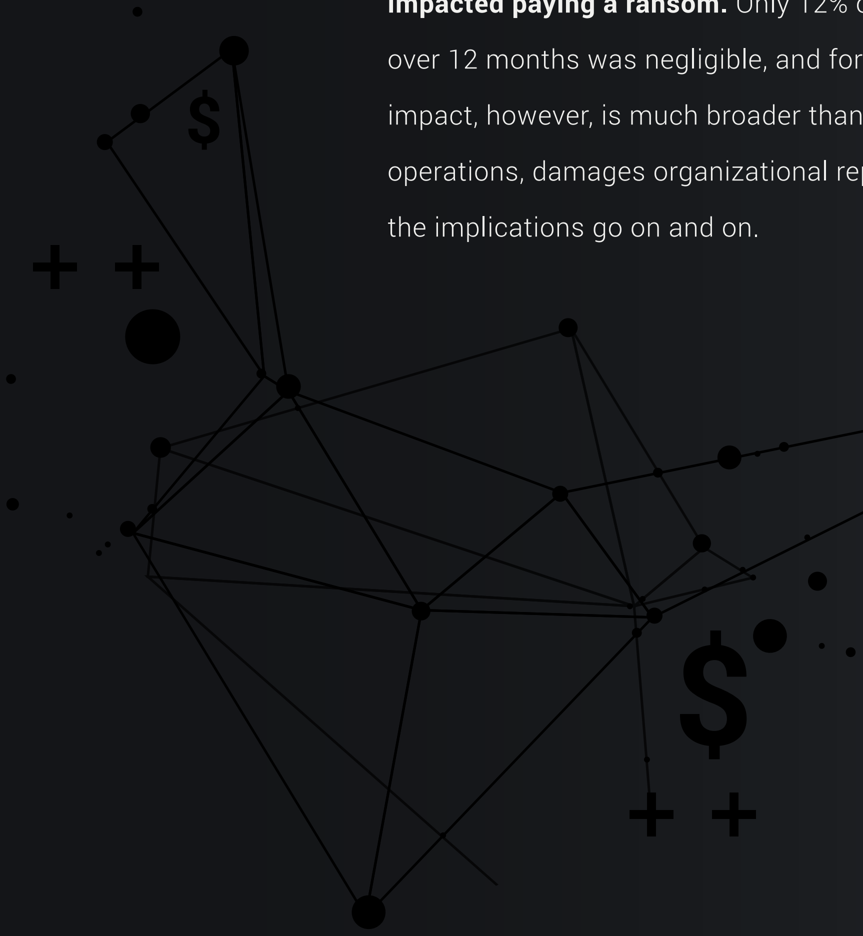

SURVEY PARTICIPANTS BY SIZE OF ORG



KEY FINDINGS

1. Despite some positive developments, the impact of ransomware attacks remains high.

The good news? We found a drop in the number of organizations affected by ransomware and in the number paying ransom compared to the previous year. This likely reflects the temporary slowdown of ransomware activity in the later part of 2022 before things ramped up again in the first half of 2023. **Overall, however, impact from ransomware remains high, with 81% of surveyed organizations affected at least once in the past 12 months, and 48% of those that were impacted paying a ransom.** Only 12% of those affected said the cumulative cost over 12 months was negligible, and for 39%, the cost was at least $1 million. The impact, however, is much broader than financial losses. Ransomware also disrupts operations, damages organizational reputation, and drains SecOps resources – and the implications go on and on.



2. Security teams are changing how they defend their riskiest entry points – but will need to keep pivoting to combat new attack vectors.

Survey participants ranked phishing and social engineering as the riskiest entry points for ransomware attacks again this year. With human behavior an ongoing issue, security teams are changing their approach – shifting from user awareness and training to technology-driven countermeasures to mitigate the inevitable human-driven risks.

As teams rely more heavily on tooling, they agree that automated workflows would significantly improve their ransomware defenses and overall security posture. This is a necessary shift to make, but more adjustments are required. **The majority of respondents ranked data backup and endpoint device protection as primary mechanisms for defense, but those countermeasures are insufficient as cybercriminals increasingly target unmanaged devices and steal authentication data that allows them to impersonate users and gain access to organizations' networks and critical business applications.**

3. Infostealer malware is a precursor for a ransomware event, but teams aren't worried about it – and they aren't prioritizing malware remediation.

Organizations are optimistic about their ransomware prevention capabilities, with 79% of surveyed security professionals expressing general confidence in their ability to prevent a full-blown ransomware incident. But their optimism may be misplaced, since only 19% of organizations are prioritizing improved visibility and remediation of exposed credentials and malware-exfiltrated data. Additionally, respondents ranked monitoring for compromised web session cookies and tokens as the third least important countermeasure. **With infostealer malware infections preceding more than a fifth of ransomware attacks this year, these findings tell us that many organizations' post-infection remediation efforts are leaving the door wide open for follow-on attacks.**

THE SHIFTING RANSOMWARE TRENDS

As we noted, ransomware took a roller-coaster ride in the past 12 months. Some industry research showed a positive trend for 2022, with the number of attacks **leveling off** or even **decreasing**, and ransomware revenue dropping **40%**. But the reprieve was temporary. During the second quarter of 2023, ransomware attacks **skyrocketed** – and ransomware payments approached **record levels** by June.

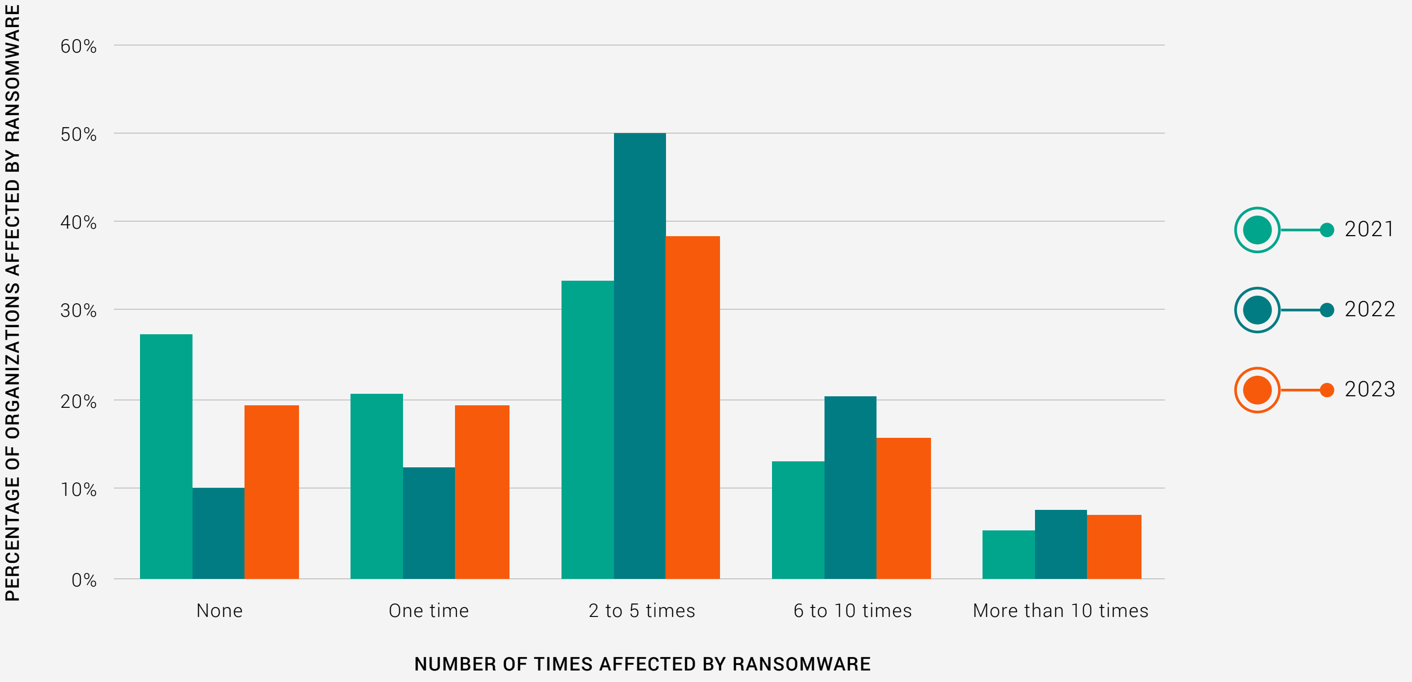
SpyCloud's survey reflects these shifting trends. Although some of our indicators moved in a positive direction, upon digging in, we found a bleaker picture than appears on the surface.

On the Positive Side, We Saw Fewer Organizations Affected...

First, the positive news. We found a slight decline in the number of organizations affected at least once by ransomware in the past 12 months: 81% in this year's survey vs. 90% last year. Additionally, we saw a year-over-year drop in the number of organizations affected at least once or multiple times (Figure 3). It's important to note that 'affected' doesn't necessarily mean a business was impacted by a successful ransomware event; rather, that they were impacted to some degree that required business resources.

SpyCloud Figure 3 ▶

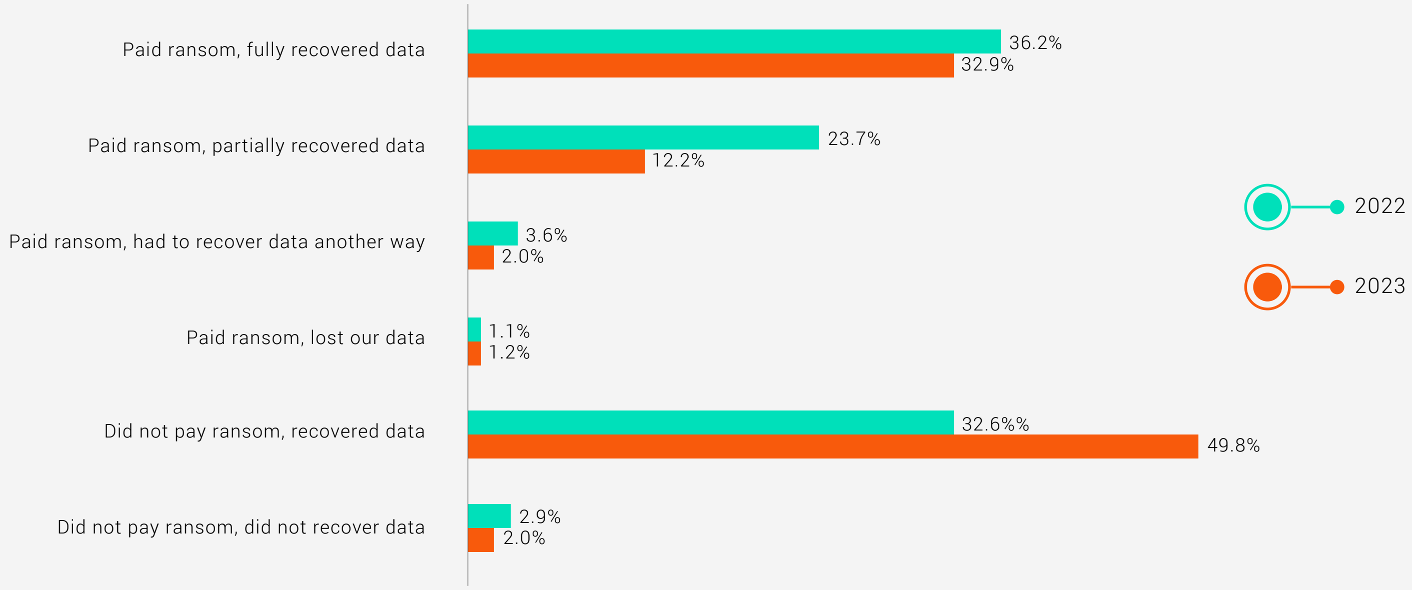
PAST FREQUENCY OF RANSOMWARE INCIDENTS (Y-o-Y)



Contributing to some good news for organizations on the financial front is a decline in the number of organizations paying a ransom (48% in the past 12 months compared to 65% the previous year) and a slight uptick in the number of those that recovered data at least partially if not fully, whether paying or not – 95% in this year's survey vs. 93% last year (Figure 4).

SpyCloud Figure 4 ▶

RESPONSE AND OUTCOME TO RANSOMWARE ATTACK



…But the Impact Remains Immense for Entire Organizations

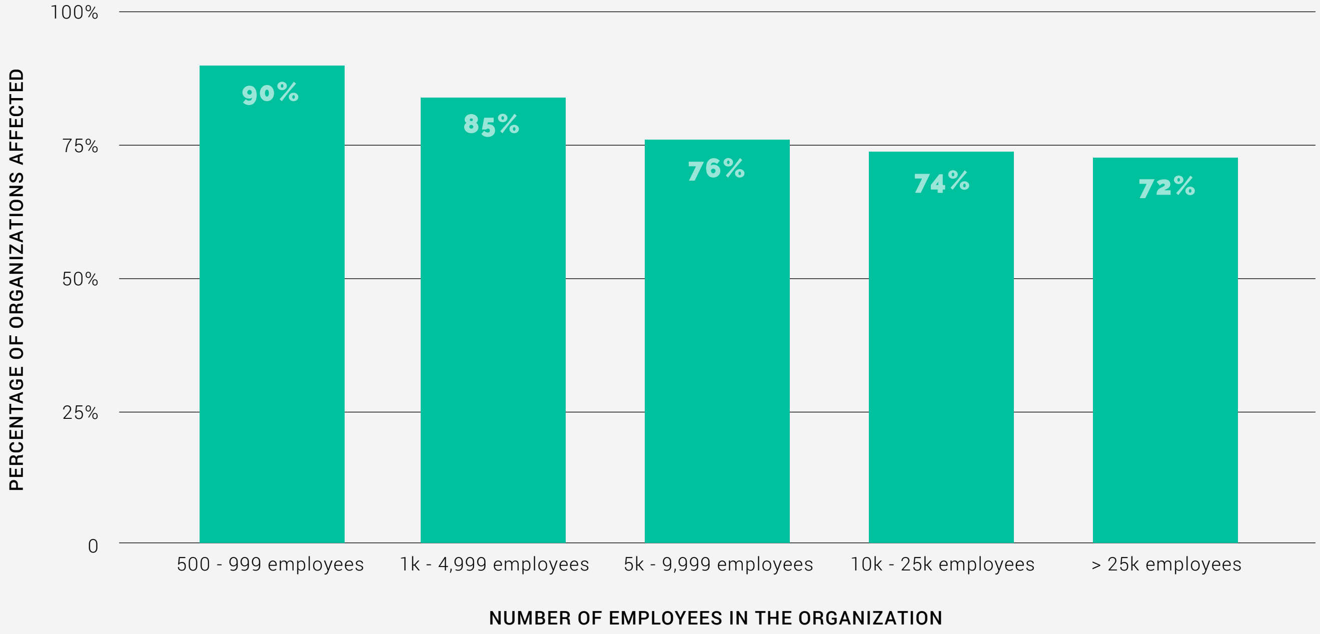
Despite some positive trends, ransomware remains a huge problem for organizations of any size, given that the majority are affected.

While the prevailing assumption is that larger organizations are in a better position to defend themselves given budgets and resources, our data shows that large enterprises with 10,000 or more employees were affected just as much as mid-sized organizations, with more than 72% reporting being affected at least once. Smaller organizations, however, weathered the worst impacts, with 90% affected (Figure 5).

AT LEAST 81% OF ALL ORGANIZATIONS SURVEYED REPORTED BEING AFFECTED BY RANSOMWARE AT LEAST ONCE IN THE PAST 12 MONTHS

SpyCloud Figure 5 ▶

AFFECTED BY RANSOMWARE AT LEAST ONCE
(BY ORGANIZATION SIZE)

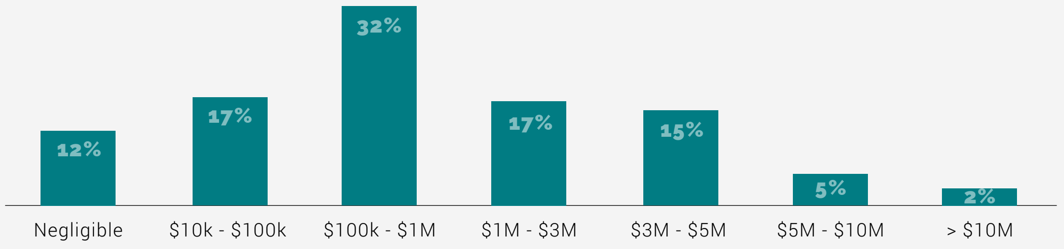


The Cost Is Climbing, Too

Last year, security researchers found **an increase** in average ransom demands across many sectors, possibly because attackers were trying to make up for the lower payee count. Even when victims choose not to pay, they still see financial losses that go far beyond the ransom. Fewer than 12% of our surveyed organizations that were hit described their costs as negligible. **For 39%, the price tag was over $1 million** (Figure 6).

SpyCloud Figure 6 ▶

CUMULATIVE COST OF RANSOMWARE ATTACKS
(FOR THOSE ATTACKED IN THE PAST 12 MONTHS)

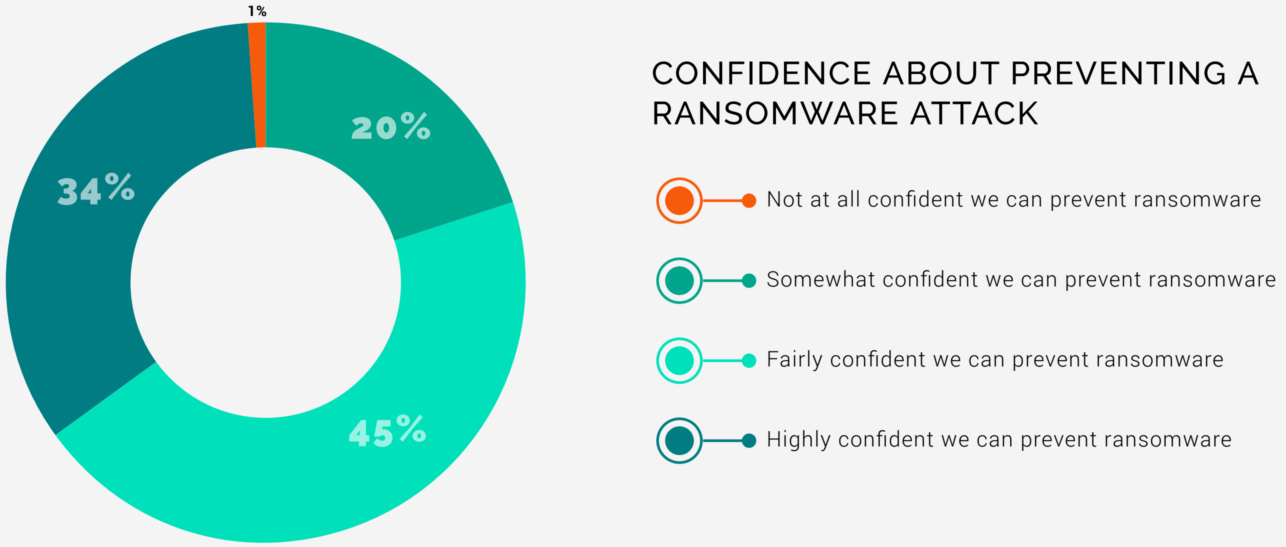


The harder-to-measure costs, from reputational damage to impact on operations and drain on resources, can be just as high or higher than the ransom itself. For example, SpyCloud's **data** shows that multiple core teams across the organization, not just SecOps, are involved in traditional malware incident response. Considering that recovery times **grew longer** last year in many industries, the expense of response alone can quickly add up.

A False Sense of Confidence

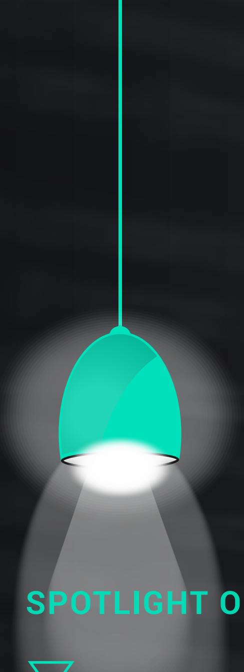
The positive developments we noted perhaps explain why **79%** of surveyed security professionals feel fairly or highly confident about their capabilities to prevent a full-blown ransomware attack in the next 12 months (Figure 7). After all, perceptions are colored by past experiences.

SpyCloud Figure 7 ▶



79% OF RESPONDENTS SAID THAT THEY ARE GENERALLY CONFIDENT IN THEIR ABILITY TO PREVENT A RANSOMWARE INCIDENT – BUT THEIR OPTIMISM MAY BE MISPLACED

Measuring confidence based on the past or the current state breeds complacency – which is especially dangerous since attackers are constantly innovating. Security practitioners understand this better than security leaders: executives expressed much higher general confidence than practitioners in preventing an attack. For example, only 71% of responding SecOps practitioners agreed they're highly or fairly confident in this ability, compared to 91% of executives (Figure 8).



SPOTLIGHT ON SECTORS

Our survey found that the two sectors most affected by ransomware at least once in the past 12 months were retail (93%) and technology (91%) (Figure 9). This isn't surprising, considering these sectors also lead in the amount of exposed data available on the criminal underground. SpyCloud's recent **Fortune 1000 Exposure Report** found, among other things, that:

TECHNOLOGY

Had the lion's share of compromised session cookies (1.26 billion of the 1.54 billion total), and nearly 68,000 malware-infected employees.

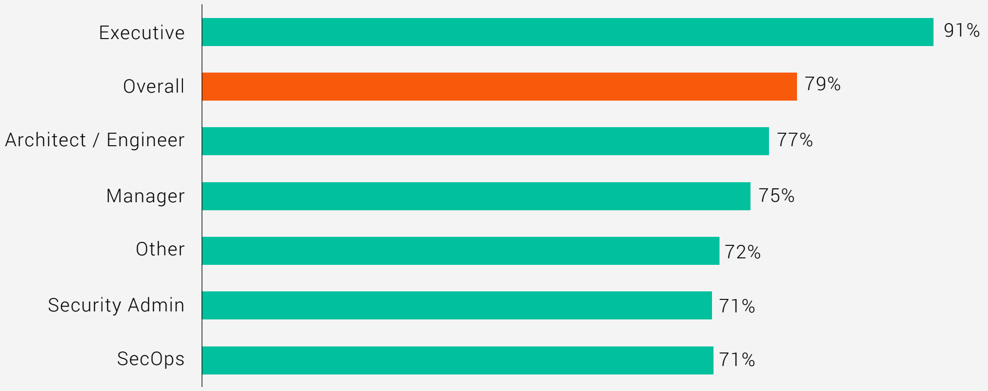
RETAIL

Had 5.88 million compromised cookies and 11,950 malware-infected employees.

This authentication data, exfiltrated from devices infected by infostealers, enables cybercriminals to easily impersonate employees and infiltrate the company.

PERCENTAGE OF RESPONDENTS GENERALLY CONFIDENT IN ABILITY TO PREVENT RANSOMWARE

(BY TITLE)



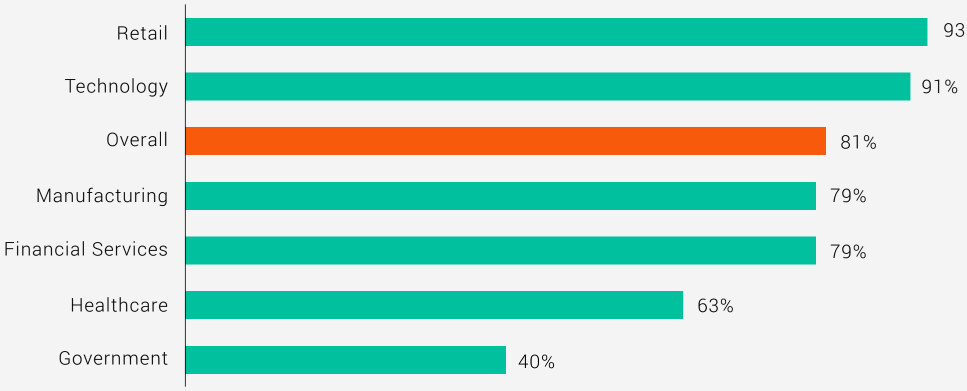
SpyCloud Figure 8 ▶

Another factor that may have contributed to the false sense of optimism in the past twelve months was a temporary slowdown in activity, as several ransomware syndicates experienced chaos. Governments doubled down on dismantling high-profile groups such as **Conti** and REvil. But the cybercriminals quickly rebounded. REvil, for instance, **resurfaced within months** with an attack on a multibillion-dollar manufacturing company.

In the meantime, multiple new groups popped up. Among them were **Play**, which uses self-propagation techniques; and **Black Basta**, which launched a widespread campaign using a banking trojan to steal credentials. In the second quarter of 2023 alone, at least **14** new ransomware-as-a-service groups emerged. As these developments illustrate, the actors are multiplying, tactics are evolving, and the speed of criminal innovation is no match for current defenses.

INDUSTRY BREAKDOWN

ORGANIZATIONS AFFECTED AT LEAST ONCE



SpyCloud Figure 9 ▶

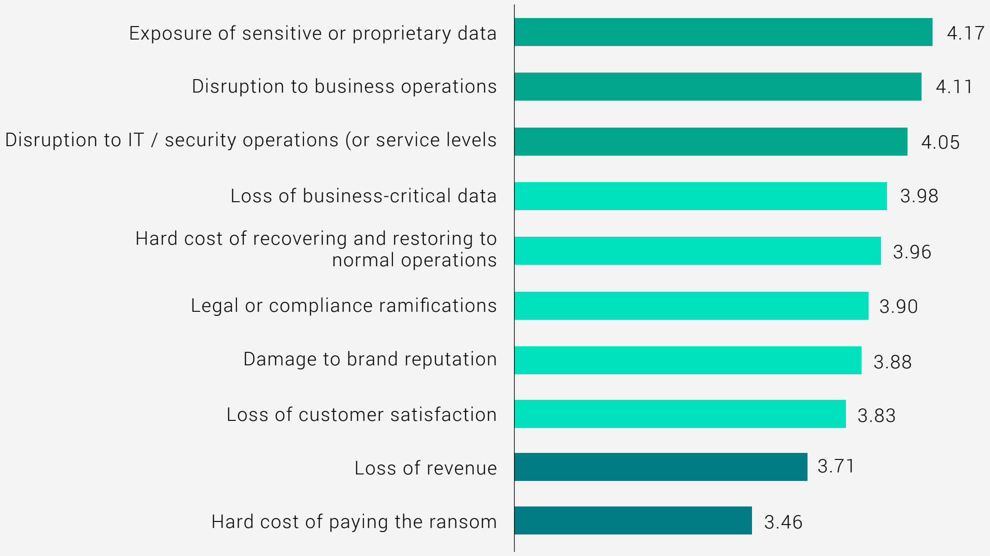
Stolen cookies/tokens are especially insidious because cybercriminals don't even need employee credentials – with a still-valid authentication cookie, they can bypass any authentication method, from multi-factor authentication (MFA) to passkeys, and walk right into corporate systems and networks without raising any alarms.

We were surprised, however, that our survey identified the healthcare sector as the second-least affected industry. Although healthcare-specific cyberattacks don't seem to appear as frequently in headlines as of late, the **FBI's Internet Complaint Center** data shows more ransomware attack reports were received from healthcare organizations in 2022 than any other critical infrastructure sector.

RANSOMWARE IS MORE THAN A SECOPS PROBLEM

Although some organizations may not see big, immediate financial impact from ransomware attacks, they recognize that the exposure due to data loss creates just as much risk, if not more. **Participants ranked exposure of proprietary and sensitive data as the greatest potential impact of ransomware, followed by disruption to business operations and disruption to IT and SecOps** (Figure 10).

The concern over data exposure maintained its lead from last year, reflecting the prevalent double-extortion trend. With **89%** of ransomware attacks incorporating data exfiltration, organizations realize that they need to worry about much more than being locked out of their encrypted systems or data.



PERCEIVED GREATEST IMPACTS OF RANSOMWARE

ON A SCALE FROM 1 TO 5

SpyCloud Figure 10 ▼

THE IMPLICATIONS OF EMERGING NEXT-GEN ACCOUNT TAKEOVER

For years, compromised credentials (username + password combo) were considered the highest risk for cybercrimes such as account takeover (ATO). Today, with access as the new currency, session hijacking or next-generation ATO is emerging as a new tactic.

Session hijacking originates from the takeover (or "hijack") of an active browser or application session using a stolen, still-valid authentication cookie where the criminal appears as a verified clone of a legitimate employee. This method goes beyond traditional credential exposure and expands the data criminals can now use to assume the access of an authenticated user.

Criminals leverage these active sessions to exfiltrate data, and monitor and mimic user behavior patterns.

RANSOMWARE
ATTACK
$
5.13
MILLION
AVERAGE COST ACCORDING TO 2023 IBM COST OF DATA BREACH REPORT

Where SecOps and BizOps Collide

As we've discussed, ransomware is not just a SecOps problem. It affects business operations by hoarding resources across the organization, often involving a minimum of **seven internal departments**, and can quickly result in damaged brand reputation or loss of business. **IBM's annual Cost of a Data Breach Report** shows a painful price tag for an organization due to a ransomware attack: $5.13 million on average, not including the ransom itself.

But the burden to proactively protect business operations does generally fall on security teams working in the trenches, and these teams are often bringing the proverbial knife to a gunfight. Simply put, traditional malware remediation processes stop short of complete **Post-Infection Remediation**, keeping the door open for attackers to come back by leaving that stolen data out for the taking and available to use until it's invalidated.

SpyCloud's **Malware Readiness and Defense Report**, released earlier this year, found that 92% of security leaders and practitioners are extremely or significantly concerned about malware-stolen data leading to future attacks. Unfortunately, it also revealed that incident response today often lacks the crucial steps to negate the consequences of that exposed data – and, as we uncovered in this survey, it's still much the same.

To prevent ransomware attacks and protect business operations, SecOps teams must remediate applications and users compromised by malware infections. A machine-centric process of isolating and reimaging the infected device only cuts the connection to the malicious intruder. It doesn't address the stolen credentials, cookies, and other authentication data making its way to darknet markets, where it can be leveraged by initial access brokers selling guaranteed access to ransomware gangs.

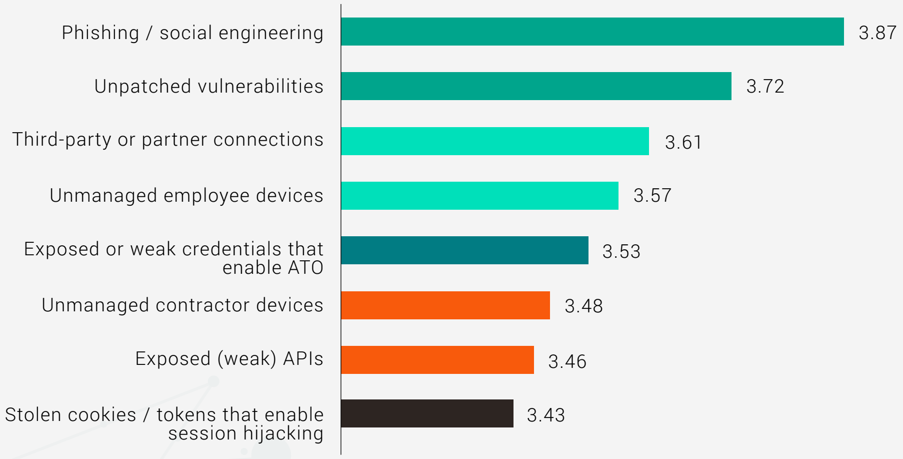
Last year alone, SpyCloud researchers recaptured 22 billion stolen cookie records, which indicates criminals are shifting tactics to steal, buy, and trade this highly accurate and highly valuable data – minimizing their need for larger breach datasets that may be clouded with old, outdated, and for their purposes, somewhat useless data.

For ransomware attackers, session hijacking is a highly successful tactic, yielding much better return on investment – and we expect to see it become mainstream as a way around passwordless technologies (like passkeys).

BATTLING RANSOMWARE ON MULTIPLE FRONTS

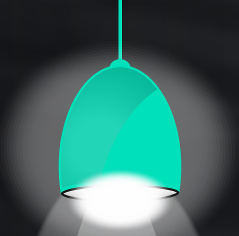
Phishing and social engineering, along with unpatched vulnerabilities, once again ranked as the riskiest entry points for ransomware (Figure 11). This was expected, since ransomware is often preceded by human behavior that results in a malware infection, which can then enable a ransomware attack. Similarly, respondents to our **malware defense survey** identified phishing and spear-phishing as the second greatest threat to their organization's security overall, with ransomware as the top threat.

PERCEIVED RISK OF ENTRY POINTS FOR RANSOMWARE
(ON A SCALE FROM 1 TO 5)



SpyCloud Figure 11 ◄

We were surprised, however, to see stolen cookies/tokens rated as the least risky entry point, suggesting that understanding of this new threat is just beginning. This entry point is an especially high risk in passwordless environments, which many view as the future of authentication. While passkeys are a tremendous improvement over passwords, cybercriminals are simply **working around passwordless authentication** with session hijacking attacks.



SPOTLIGHT ON SECTORS' PERCEIVED RISKY ENTRY POINTS

▽

Not all sectors view their riskiest entry points through the same lens, with some placing higher emphasis than the average across all industries on risks such as stolen cookies and unmanaged or undermanaged devices. For example:

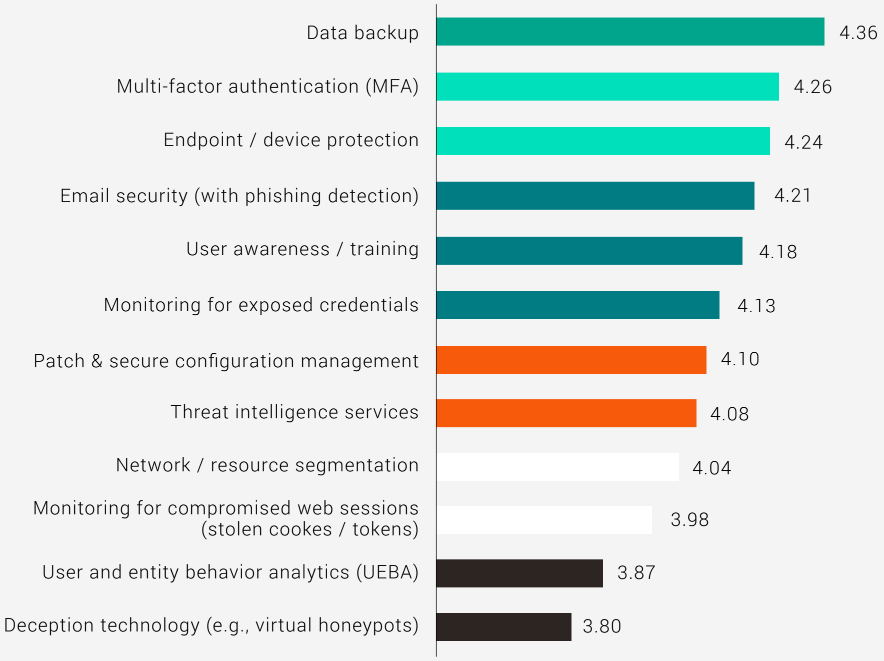
- **WEAK APIs** are a bigger concern in retail, manufacturing, and technology
- Manufacturing, Technology, and Healthcare view **COOKIES** as riskier compared to the average
- Across sectors, retail cybersecurity professionals are the most concerned about **UNMANAGED EMPLOYEE DEVICES**

The bottom line is that each of these entry points is risky, but together they're a force multiplier. This means teams must focus on all of them, including third-party, unmanaged, and undermanaged devices, and weak APIs. The use of unmanaged, undermanaged, and third-party devices, for instance, has exploded in the digital-first environment, yet they create blind spots for security teams. Likewise, the use of APIs has skyrocketed in recent years, and many organizations don't pay enough attention to the security implications of vulnerable and improperly designed APIs and stolen API keys, which are another form of access being exfiltrated from malware-infected devices.

Countermeasures Misaligned with New Ransomware Tactics

Year over year, data backup has remained the most important countermeasure for organizations (Figure 12). We highlight this as concerning because it shows that defenses are not adjusting to the shift in ransomware tactics. Backup was effective years ago when data encryption was the biggest problem, but it doesn't mitigate the risks of modern ransomware – which relies heavily on malware-exfiltrated authentication data.

MOST IMPORTANT COUNTERMEASURES IN PRACTICE TODAY
(ON A SCALE FROM 1 TO 5)



SpyCloud Figure 12 ▲

The importance of MFA grew significantly year over year, which may be contributing to organizations' false sense of security. Although organizations should deploy MFA as one of their critical defense layers, they must also take the steps to identify malware-infected employees and invalidate stolen cookies that enable authentication bypass and session hijacking. As stated earlier, MFA and passwordless technology such as **passkeys** are not sufficient fixes because session hijacking bypasses any form of authentication.

Since technology and tools are only one part of the defense equation, we also asked the security pros about their operational and organizational countermeasures. Most feel that they adhere well to basic hygiene practices such as patching and applying least privilege techniques (Figure 13). While the majority already have strategies like ransomware-specific incident response in place, plenty of work remains to be done, with a good number of respondents noting they are considering or are only in the planning stages of implementing upgrades to their existing strategy.

SpyCloud Figure 13 ▶

STATUS OF RANSOMWARE COUNTERMEASURES

	ALREADY IN GOOD SHAPE	PLAN TO UPGRADE	PLAN TO ADD	NO PLANS
Adhere to security hygiene best practices (e.g., frequent patching, least privileges)	60%	21%	17%	2%
Cyber insurance that includes coverage for ransomware attacks	48%	27%	17%	8%
Ransomware-specific incident response team	48%	32%	19%	4%
Ransomware-specific incident response training or exercises	45%	30%	23%	2%
Ransomware-specific incident response plan / playbook	42%	33%	23%	2%

It's worth noting that there is a significant disconnect between the high confidence in operational practices and the high number of organizations that were affected by ransomware in this year's survey. **This gap tells us that either the combination of technology and processes isn't working – or organizations are overly optimistic about their controls.**

THE IMPOSSIBLE HUMAN FACTOR

Organizations recognize that human behavior plays a major role in the ability to defend against ransomware, but they're shifting from user awareness to technology-based measures. Unfortunately, these measures only work if SecOps teams have complete visibility and control across all users, applications, and devices connecting to the network and accessing sensitive data – and that's not the case today. In recent **findings**, we learned that:

36%

OF ORGANIZATIONS

allow unmanaged **personal devices** to access business applications and systems

54%

OF ORGANIZATIONS

struggle with **shadow IT** due to employee adoption of applications and systems without IT's consent

28%

OF ORGANIZATIONS

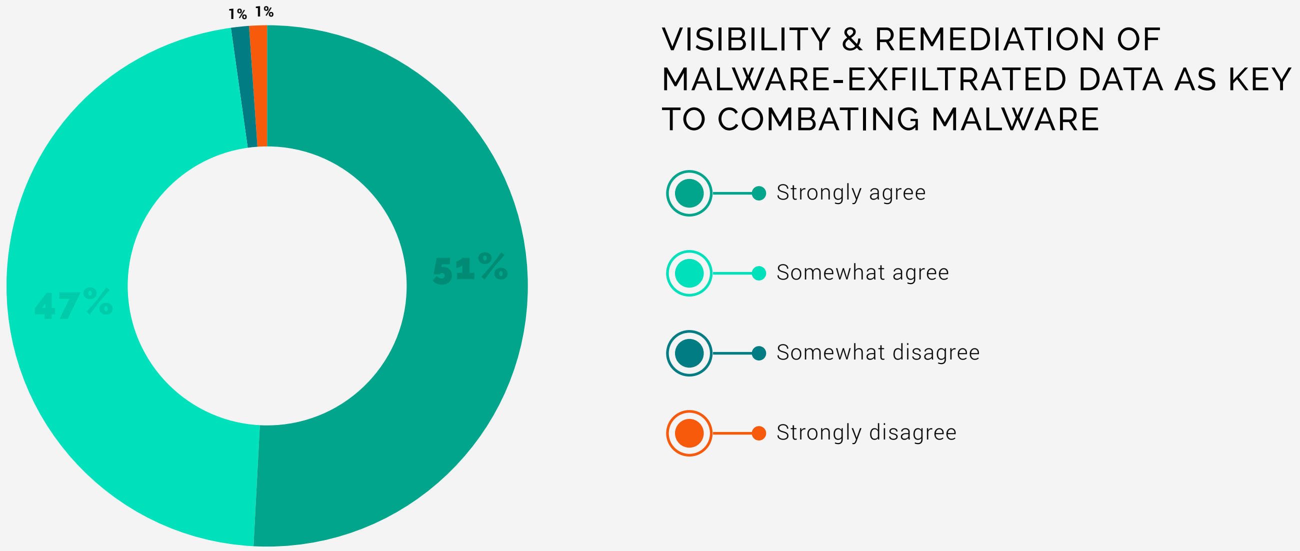
allow **unmanaged third-party devices** to access business applications and systems

These risky practices illustrate that SecOps teams are struggling to keep up with the evolution of the digital workplace and often lack visibility into their sprawling attack surface.

FUTURE DEFENSE PRIORITIES SHOW DISCONNECT

Lack of visibility, the inefficiency of manual tasks, and cumbersome or false alerts are recognized problems in cybersecurity. Survey participants overwhelmingly agree that better visibility of malware-exfiltrated data, along with automated remediation workflows, would improve their ability to combat ransomware and improve overall security posture (Figure 14).

SpyCloud Figure 14 ▶


VISIBILITY & REMEDIATION OF MALWARE-EXFILTRATED DATA AS KEY TO COMBATING MALWARE

98% OF RESPONDENTS AGREE THAT BETTER VISIBILITY INTO MALWARE-EXFILTRATED DATA AND AUTOMATED REMEDIATION WORKFLOWS WOULD IMPROVE THEIR OVERALL SECURITY POSTURE

This sentiment, however, contradicts respondents' views on the importance of session cookies, which they ranked in their bottom three countermeasures, as noted earlier. It also doesn't align with reported authentication practices that are in place: automated workflows to remediate compromised session cookies/tokens and automated workflows to remediate exposed passwords are among the bottom three authentication practices that organizations are currently using (Figure 15). However, it's clear that this is an area of increasing focus, as automation for remediating those two threats is at the top of priorities for the next 12 months.

SpyCloud Figure 15 ▶

AUTHENTICATION PRACTICES IN USE OR PLANNED FOR IMPLEMENTATION/UPGRADE

ALREADY IN GOOD SHAPE

Password complexity requirements	64%
Monitoring for exposed employee passwords	59%
Banned password list (e.g., 123password)	57%
Single sign-on	54%
Password manager solutions	53%
Passwordless authentication solutions(biometrics, passkeys)	48%
Monitoring for exposed contractor, partner, and supplier passwords	46%
Monitoring for stolen partner and supplier session cookies / tokens	41%
Other authentication solutions	40%
Monitoring for stolen employee session cookies/tokens	39%
Automated workflows to remediate compromised session cookies / tokens	37%
Automated workflows to remediate exposed passwords	35%
Hard tokens for MFA	34%

PLAN TO UPGRADE OR ADD

Password complexity requirements	35%
Monitoring for exposed employee passwords	39%
Banned password list (e.g., 123password)	39%
Single sign-on	38%
Password manager solutions	43%
Passwordless authentication solutions (biometrics, passkeys)	46%
Monitoring for exposed contractor, partner, and supplier passwords	48%
Monitoring for stolen partner and supplier session cookies / tokens	53%
Other authentication solutions	58%
Monitoring for stolen employee session cookies/tokens	59%
Automated workflows to remediate compromised session cookies / tokens	60%
Automated workflows to remediate exposed passwords	63%
Hard tokens for MFA	55%

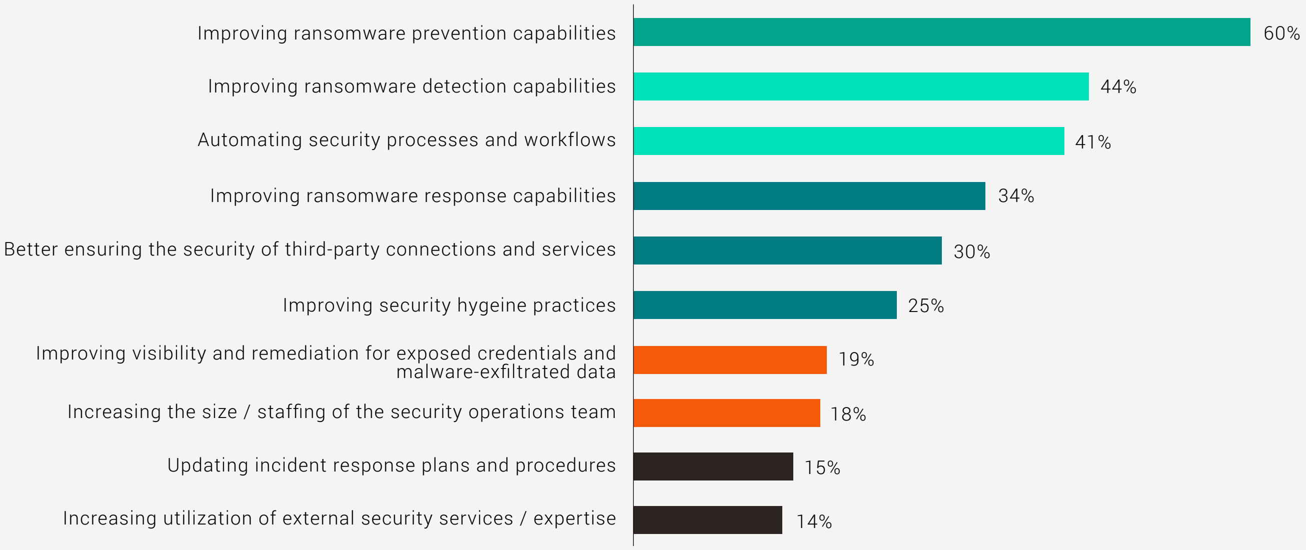
However troubling the disconnect, these findings are consistent with those from SpyCloud's malware defense survey, in which 98% of security professionals also agreed that better visibility into business applications exposed by an infostealer infection would increase security posture. This lack of visibility hinders progress in the fight against ransomware, and SecOps teams have to figure out this problem in order to effectively reduce the risk of malware exposure.

All Eyes on Prevention and Automation

Proactive prevention is just as important as strengthening defenses and response capabilities, and our respondents agreed when asked to pick their top three defense priorities. Improving ransomware prevention capabilities is the top priority for organizations in the next 12 months, followed by improving ransomware detection capabilities and automating security processes and workflows (Figure 16).

SpyCloud Figure 16 ▶

TOP SECURITY PRIORITIES



Although prevention and detection are in the top three priorities for both security leaders and practitioners, the two sides place different importance on automation. Executives identified automation as their second priority, while admins and analysts/incident responders ranked it third, and managers and architects fourth. In contrast, automation is the top overall security priority identified in **our Malware Readiness and Defense Report**, reflecting a growing industry trend of organizations automating processes as much as possible to not only combat the talent gap crisis but also boost SecOps efficiency.

The average duration of a ransomware attack – the time between initial access into the organization and the ransomware deployment – has plummeted more than **94%** in the span of just two years. **What used to take attackers more than two months now takes less than four days**. This accelerated timeline illustrates how cybercriminals are making headwinds at a dizzying pace, underscoring the need for SecOps teams to automate remediation processes.

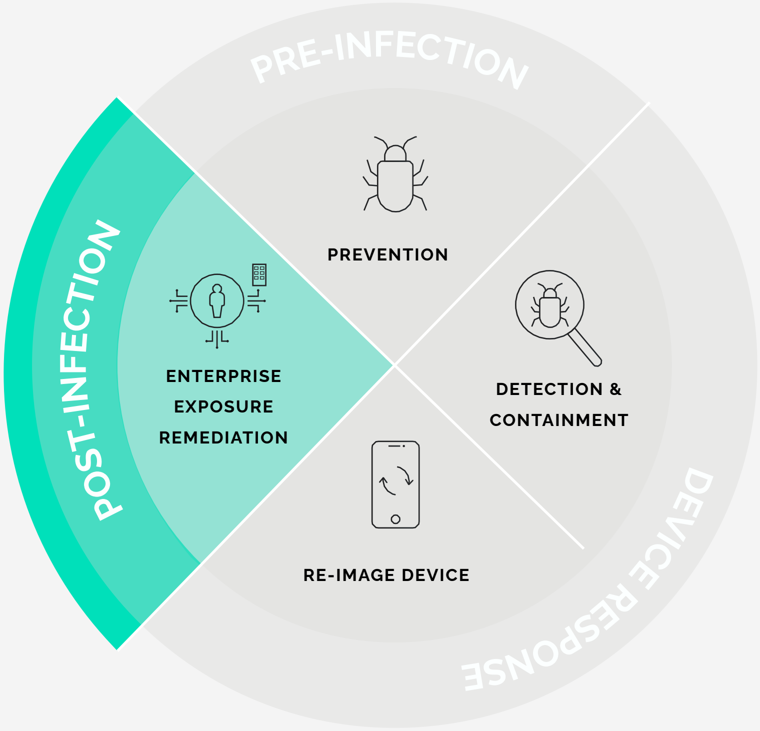
ADAPTING RANSOMWARE DEFENSES FOR STEALTHIER ATTACKS

We found that ransomware prevention is consistently at the top of the priority list for organizations, not only across all security roles but also regardless of an organization's size. So, what does proactive prevention look like in the face of evolving threats?

Ransomware is a malware problem at its core, which means that preventing ransomware attacks must start with proper and robust malware remediation. Bad actors are exploiting infected systems to exfiltrate data they can use to aid an attack, identify potential entry points to corporate resources, and deliver executable files.

Traditional malware response, however, doesn't address the risk of the stolen data from an infected device. By the time malware is detected and the device has been reimaged, the data is already in the hands of criminals. Some infostealers can siphon data in mere seconds. Non-persistent malware can vanish with little or no trace, which means teams don't know it was ever there to begin with. SecOps workflows and processes have to evolve to include a critical addition to their next-gen incident response: **Post-Infection Remediation**.

MALWARE RESPONSE MUST INCLUDE POST-INFECTION REMEDIATION

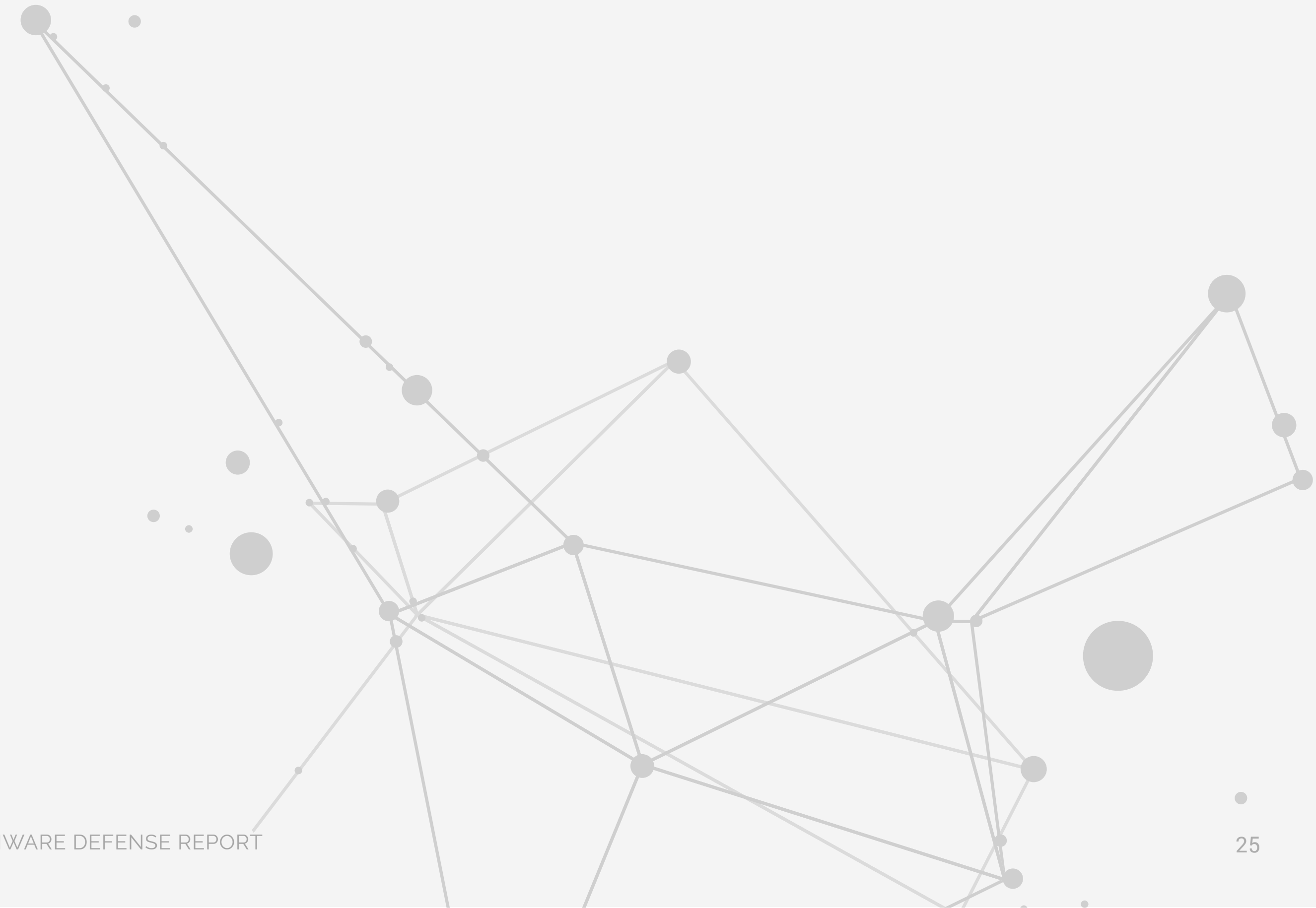


Today's attack surface includes users and applications, not just devices. **And Post-Infection Remediation is a paradigm shift from the current machine-centric response to a more comprehensive identity-centric response that takes that growing attack surface into greater consideration.** While traditional machine-centric remediation simply clears a device, Post-Infection Remediation takes additional measures to reset stolen credentials and invalidate active web sessions of exposed applications. This approach adds the necessary steps to protect an organization from additional entry points for a ransomware attack.

SecOps teams can't take these extra steps without visibility into the entire attack surface to start with. Incident responders need to know what authentication data has been stolen, and which users and corporate applications have been exposed, so they can focus efforts (ideally in an automated fashion) in the right areas.

Yet, as our report reveals, visibility is a universal struggle. The proliferation of unmanaged, undermanaged, and third-party devices perpetuates blind spots for security teams. Shadow IT and shadow data exacerbate the problem because unsanctioned applications and data stored in them are not traditionally governed by corporate security policies.

The only way for defenders to gain ground and stay a step ahead is by embracing next-generation malware remediation practices – and this is where Post-Infection Remediation comes in. **By adding Post-Infection Remediation to their playbooks, SecOps teams can greatly improve their ransomware prevention outcomes and move faster to close the door on attackers, all while minimizing the cross-team resources that full-blown incidents consume.**



FINAL THOUGHTS

Our biggest takeaway from this year's survey is that SecOps teams have not yet embraced a key piece of the ransomware defense puzzle – remediating malware-exfiltrated authentication data – **which means that many organizations may be more vulnerable than they realize**. With an infostealer infection as a precursor to more than a fifth of ransomware events in 2023, teams can no longer ignore this rising threat.

While many respondents noted feeling confident in their ability to avoid a ransomware attack in the next 12 months, their current practices and future priorities don't support that optimistic outlook:

Organizations view phishing and social engineering as the riskiest entry point for ransomware, and have shifted their focus from changing behaviors through user awareness and training to technology-driven controls. **Yet they lack important visibility into authentication data that has been exfiltrated from unmanaged, undermanaged, and third-party devices, which greatly limits the impact of any new defensive mechanisms.**

Respondents overwhelmingly agree that better visibility of malware-exfiltrated data and automated remediation would improve their ransomware defenses and overall security posture. **But they view monitoring for compromised cookies as one of the least important countermeasures.** They're also least likely to have or implement automated workflows for remediating exposed passwords and cookies, compared to other authentication practices.

Ransomware prevention is the biggest priority for security leaders and practitioners alike. **However, without complete malware remediation, any prevention efforts will remain limited.**

As workplaces continue to digitally transform and organizations adapt how they do business, human behavior continues to add to a sprawling attack surface. And threat actors are paying attention. They're modifying their TTPs for a landscape where access is the new currency and finding quick ways to circumvent authentication layers, from MFA to passkeys. For SecOps teams that want to outmaneuver ransomware attackers, SpyCloud's enterprise protection solution offers automated detection of malware infections across devices and fuels remediation workflows powered by comprehensive and actionable data.

Stolen credentials via malware-siphoned data give cybercriminals the upper hand – **isn't it high time to use the same data against them?** By gaining full visibility into malware infections and acting quickly, SecOps teams can truly gain confidence in their ability to keep the business safe.

SpyCloud

PROTECT YOUR ENTERPRISE FROM RANSOMWARE **WITH SPYCLOUD**

THE FIRST LINE OF DEFENSE IS PREVENTION

Act on known points of compromise to shut down targeted attacks like ransomware. With SpyCloud, you get actionable insights and high-fidelity alerts that let you stop a malware infection from becoming a full-blown ransomware event.

SPYCLOUD ENTERPRISE PROTECTION

ABOUT 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, protect their business from consumer fraud losses, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to nearly 200 cybersecurity experts whose mission is to make the internet a safer place.

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