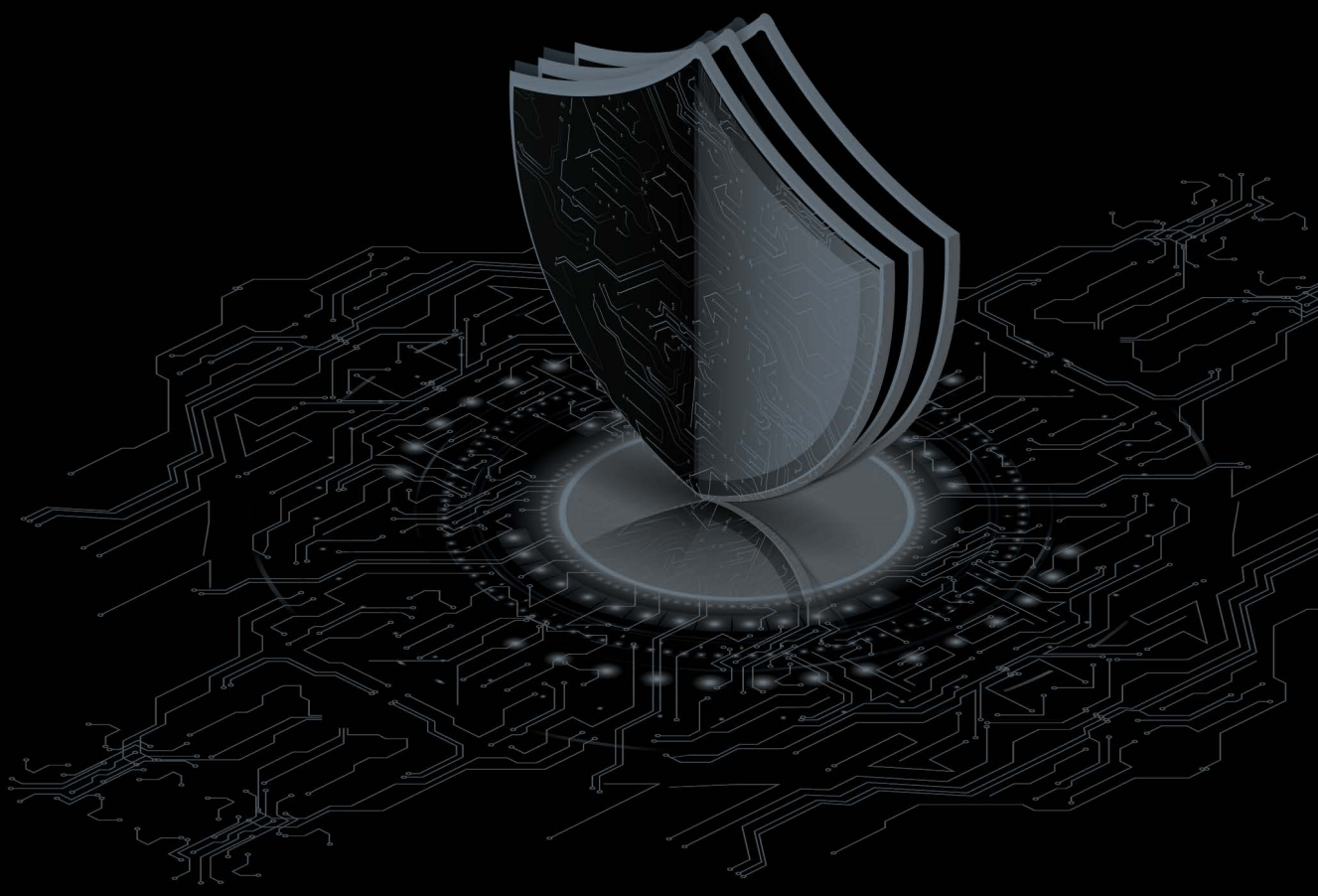
The SpyCloud **Ransomware Defense Report**

An annual benchmark of organizations' preparedness and strategies to close the gaps

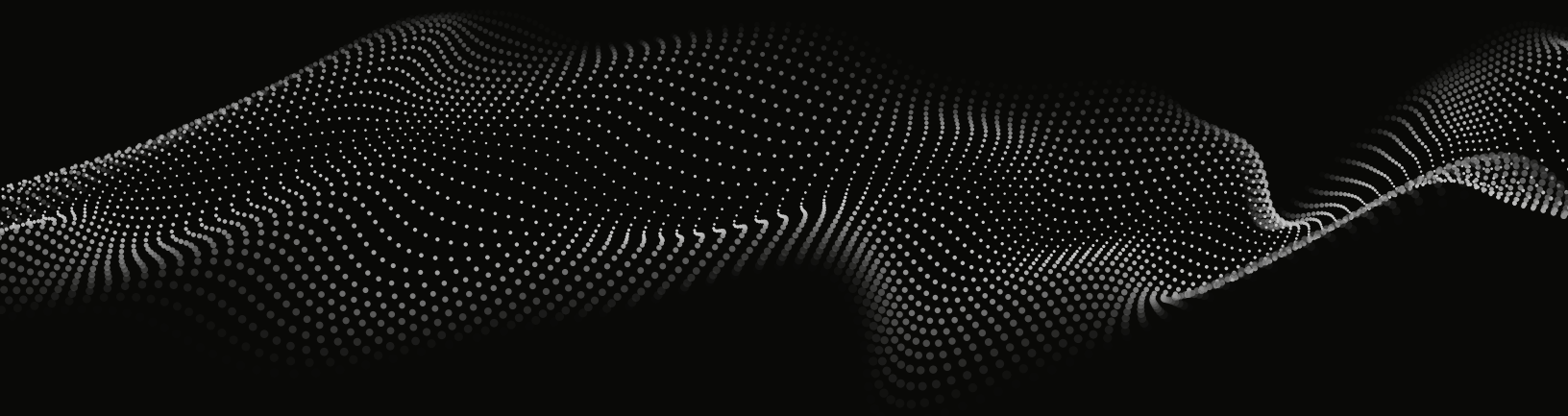
2022



SpyCloud

SpyCloud

Table of Contents



The Escalating Ransomware Problem

Within the past 12 months, ransomware attacks have forced a 157-year-old college to close its doors, a leading automaker to halt operations for a day, and an entire nation to declare a state of emergency. After dominating the headlines for several years, these kinds of stories may feel like old news by now. Yet the escalation of the ransomware threat into a global crisis keeps it at the top of the cybersecurity agenda for many organizations.

A recent SpyCloud sponsored survey of enterprise CISOs found that ransomware is the most concerning issue they face today. And for good reason: 66% of organizations **were hit by ransomware in 2021, compared to 37% in 2020.**

Not only is ransomware more prolific but threat actors also have gotten savvier – they succeeded in encrypting data in 65% of attacks last year, up from 54% in 2020. Adding to the injury is the fact that the majority of ransomware schemes now involve double extortion, with attackers stealing data first and threatening to leak it if the ransom isn't paid. Just two years ago, only one gang used this tactic while today it's present in 77% of attacks.

In last year's Ransomware Defense Report, we learned that organizations felt pessimistic about their prospects of avoiding an attack. Only 18% of those surveyed believed a ransomware incident wasn't likely to happen to their organization, while 22% believed it would likely happen multiple times. We wanted to see how things have changed since then – and this year's survey found that **organizations feel even less confident today in their ability to fight back.**

As we discuss in this report, ransomware remains a broad, persistent, and complicated problem to solve. To help organizations gain a more holistic understanding of this threat, we also discuss the often-overlooked aspects of ransomware attacks and how organizations can address them.

About the SpyCloud Survey

Following the 2021 Ransomware Defense Report, SpyCloud wanted to learn how security leaders and practitioners' perceptions about the threat have changed and what they're doing differently, if anything, to defend against ransomware. This year, we surveyed 310 individuals in active IT security roles at US, UK, and Canadian organizations that have at least 500 employees.

We examined areas such as:

- The prevalence and impacts of ransomware attacks
- Countermeasures that organizations currently have in place and/or plan to add
- The greatest risks and biggest obstacles related to ransomware

In addition to highlighting the survey findings, the report offers insights into how you can boost your organization's ransomware defenses. We encourage you to use this actionable data as a benchmark for your organization's preparedness and for making decisions on how to close your preparedness gaps.

Key Findings

1. **The prevalence of ransomware attacks is on the rise.** Year over year, we saw a significant decrease in the number of organizations that *haven't* been hit by ransomware in the past 12 months (10% in 2022 vs. 27.5% in 2021) and a significant increase in the number of those that have experienced multiple attacks (50% were hit two to five times in the past year vs. 33.5% the previous year, and nearly 78% were hit between two times and 10+ times in the past year vs. nearly 52% the year before).

Survey Demographics

SpyCloud solicited responses from individuals whose roles range from IT security analysts and architects/ engineers, all the way to the executive suite. The majority of the 310 participants came from senior levels: 34% are CIOs, CISOs, and security executives; and 50% are security directors, managers, or team leads (Figure 1).

We surveyed a cross-section of organization sizes (Figure 2), from small (500-999 employees) and midmarket (between 1,000 and 9,999 employees) to large enterprises (with 10,000 or more employees). The biggest cohort (46%) represents employers with 1,000-4,999 workers, followed by 23% from small companies (500-999 employees) and 18% from companies with 5000-9,999 employees. Respondents from the largest enterprises (10,000+ employees) comprise 12% of respondents.

Survey participants by IT security role

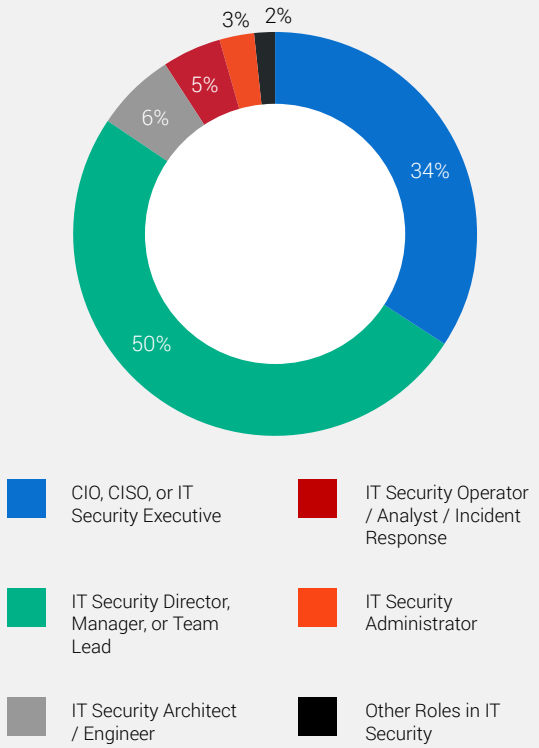


Figure 1

2. **Organizations feel less confident about their defenses this year.** We found a slight across-the-board decrease in the number of organizations indicating their existing ransomware mitigation solutions are in good shape, and an uptick in organizations looking to upgrade or add new security technologies. Additionally, more organizations have implemented "Plan B" measures this year, from opening cryptocurrency accounts to purchasing ransomware insurance riders. These findings suggest that organizations realize threats are slipping through their defenses and a ransomware attack is inevitable.

3. **The combination of unpatched vulnerabilities, phishing emails, and unmanaged devices creates the highest risks.** Survey participants ranked these three vectors as the riskiest entry points for ransomware. It's important to understand that all of these entry points are interconnected – and together, they greatly increase the risk of a successful ransomware attack.

4. **Organizations are leaving gaps in their layered defenses.** We weren't surprised to learn that organizations see data backup as their most important countermeasure and 67.8% are satisfied with the performance of their solution. Likewise, user awareness and endpoint detection are among the other typical defenses at the top. We were surprised, however, to see how many organizations overlook other important defenses. For example, monitoring for compromised web sessions is perceived as the third least important countermeasure. This and other gaps in organizations' layered defenses give ransomware operators more opportunities to gain access.

5. **Lack of visibility into true compromises creates bigger exposure.** Although unpatched vulnerabilities, phishing emails, and unmanaged devices deserve attention as risky attack vectors, the riskiest entry points that security teams can't see result in an even bigger vulnerability. Devices infected with malware, for example, create one of the biggest exposures to ransomware, and without visibility into those devices and into the resulting accounts compromised through malware-siphoned data, organizations don't have the complete picture of their risk.

Survey participants by size of organization

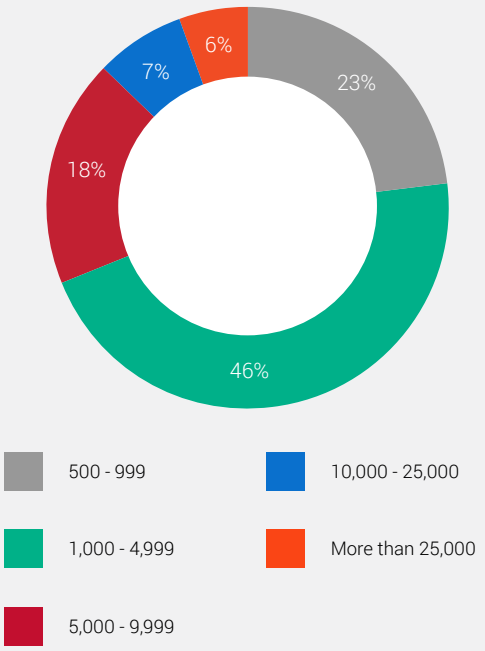


Figure 2

Section 1 | Losing Ground to Ransomware

A Bleak Picture

Research from the past year overwhelmingly points to the ransomware problem continuing its upward trajectory. Once again, it was the top threat in 2021, as observed by IBM Security researchers in their latest report. The 13% growth seen in ransomware-related breaches in the past year is "as big as the last five years combined," according to the latest Verizon Data Breach Investigations Report (DBIR).

Going into our survey, we expected to find similar results – and we did, including a jump to **90% in the number of organizations affected by ransomware at least once in the past year**, compared to 72.5% the previous year (Figure 3). Several other year-over-year changes indicate that organizations are losing ground to ransomware:

- Only 10% of respondents said their organizations weren't affected, a significant decrease from previous year's 27.5%.
- There was a big jump in the number of those affected two to five times, to 50% this year from last year's 33.5%; and in the number of those affected six to 10 times, to 20.3% from 13.1%.
- Overall, 77.7% of surveyed organizations reported being hit between two times and 10+ times vs. 51.7% in the previous year's survey.

Past Frequency of Ransomware Incidents (YOY)

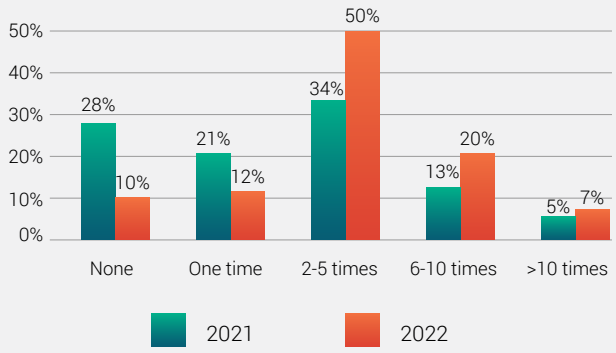


Figure 3

Size Doesn't Matter

While smaller organizations often think that ransomware attackers target the better-healed large enterprises, that's simply not the case. Our research shows that no size of organization is immune.

This year, the percentage of companies affected in each size category is spread very closely, with a range between 82.4% for the largest enterprises and 91.5% for organizations with 1,000-4,999 employees (Figure 4). But the smallest organizations seem to have it slightly worse than the largest ones, likely due to having fewer security resources – which means they need to look for cost-effective technologies that level the playing field.

Affected At Least Once (By Organization Size)

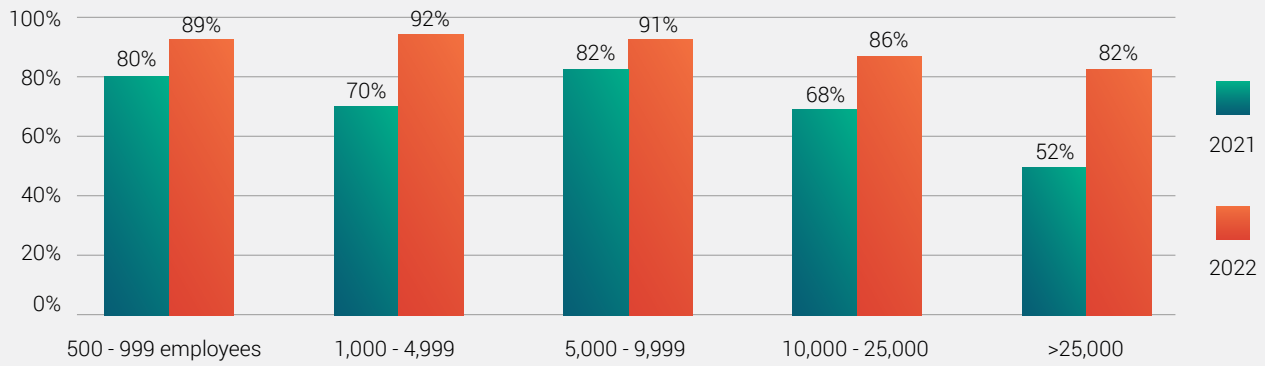


Figure 4

To Pay or Not to Pay?

Among those hit by ransomware in the past year, 65% ended up paying the ransom (Figure 5). But that doesn't mean they recovered their data. We found that of those that paid, slightly more than half recovered their data fully and roughly a third succeeded in partial recovery. Of those that didn't pay, 92% managed to recover their data through means such as data backups. This may seem like good news on the surface but it's not necessarily so – those organizations cannot be sure if the stolen data was already shared on the dark web prior to retrieval, making it available to other cybercriminals.

Response and Outcome of Ransomware Attacks

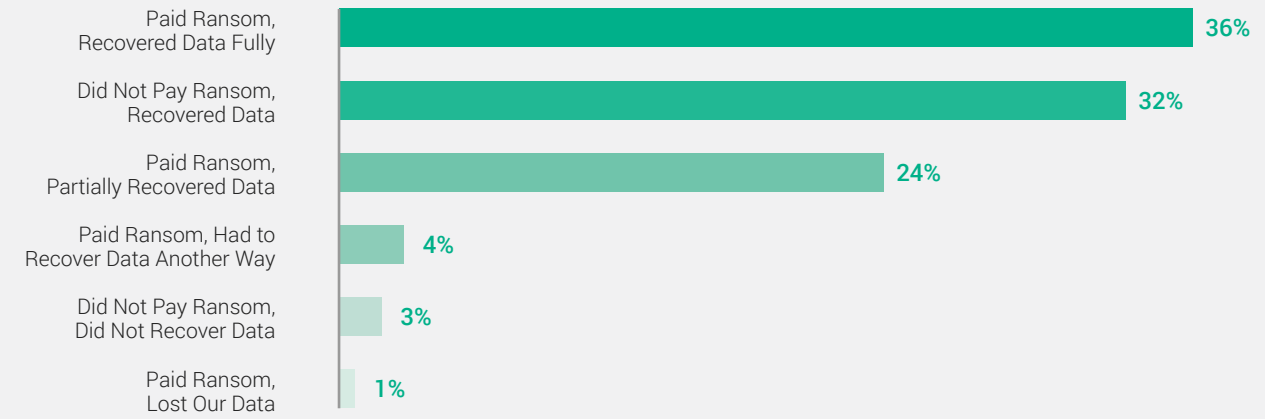


Figure 5

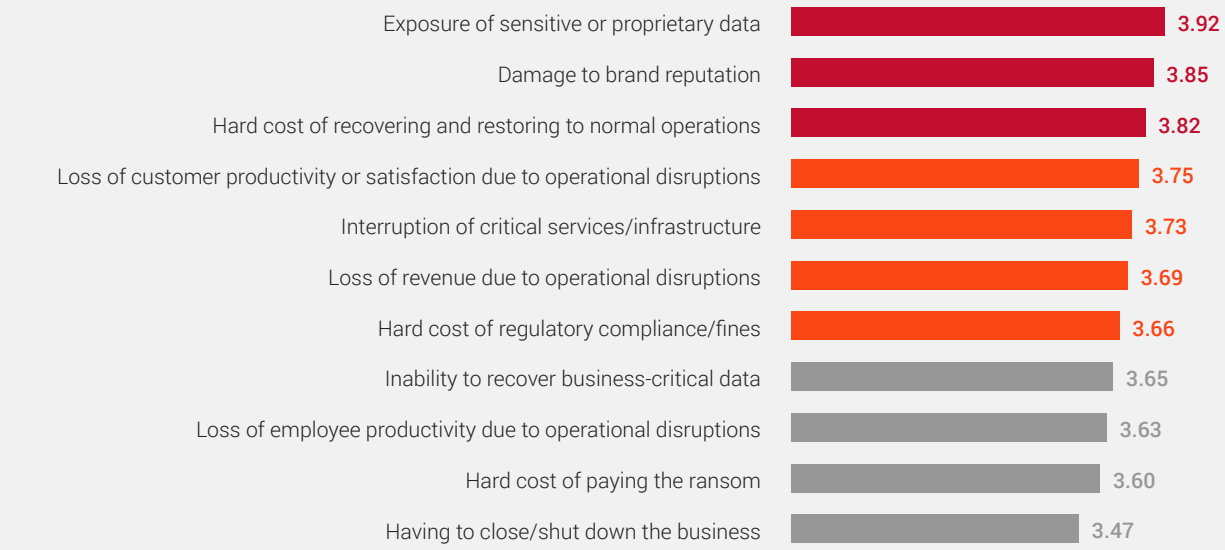
Keep in mind that the ransom is only a small part of the total cost of a ransomware attack. Even if the attack doesn't result in encrypted or stolen data or in paid ransom, there's a variety of other implications, including mitigation time, impact to customer-facing services, and loss of employee productivity. In the private sector, 86% of companies report losing revenue as a result of a ransomware incident and 90% say they lost their ability to operate. Additionally, 37% report having to lay off employees and 35% say they experienced C-level resignations. And while the impact depends on the nature of the business, the overall costs are far reaching. While the average ransom was $812,360 globally last year, the average cost of remediation was much higher – $1.4 million.

Perception Is Everything

This year, we also wanted to know what organizations are concerned about the most as a result of a ransomware attack. Four of the top five concerns – exposure of sensitive or proprietary data, damage to brand reputation, loss of customer productivity or satisfaction due to operational disruptions, and interruption of critical services/infrastructure – relate to external perceptions (Figure 6). These outward-facing concerns likely stem from a combination of factors:

- Through their double-extortion campaigns, criminals are advertising their actions.
- Even if cyberattackers aren't vocal about it, a ransomware attack is much more visible to stakeholders and potentially to the public, compared to other types of cyber incidents.
- Brand reputation is instrumental to growing a business, and thus of great concern.
- Boards have a heightened sensitivity to ransomware attacks, and they're growing more aware about the immense business implications.

Greatest Impacts of Ransomware Attacks to Your Organization



On a scale of 1 to 5

Figure 6

Losing Confidence in Prevention and Defense

Year over year, we found a decrease across the board in the number of respondents satisfied with their existing security technologies and an increase in those planning to upgrade or add to their toolset (Figure 7). This shift indicates organizations are aware that threats are slipping through and realize that gaps remain despite those layers of defense.

With ransomware attackers gaining ground, it's understandable that organizations feel less confident in their defenses. Clearly, they see room for improvement – and want to dedicate more effort to get there. The key is to ensure that any upgrades or additions to the security stack approach ransomware risk holistically and fill the cracks in the security posture, rather than creating more legwork that has limited impact.

Security Technologies Planned for Ransomware Mitigation

Already in good shape

Data backup	61.9%
Email security (with phishing detection)	52.4%
Multi-factor authentication (MFA)	50.5%
Endpoint/device protection	45.9%

Plan to Upgrade

Deception technology (e.g., virtual honeypots)	37.9%
Intrusion detection system (IDS)	33.3%
User and entity behavior analytics (UEBA)	33.1%
User awareness/training	32.9%
Patch & secure configuration management	32.8%

Plan to Add

Threat intelligence service(s)/sharing platform	25.6%
Monitoring for compromised credentials	24.3%
User and entity behavior analytics (UEBA)	23.8%
Deception technology (e.g., virtual honeypots)	23.5%
Endpoint/device protection	22.8%

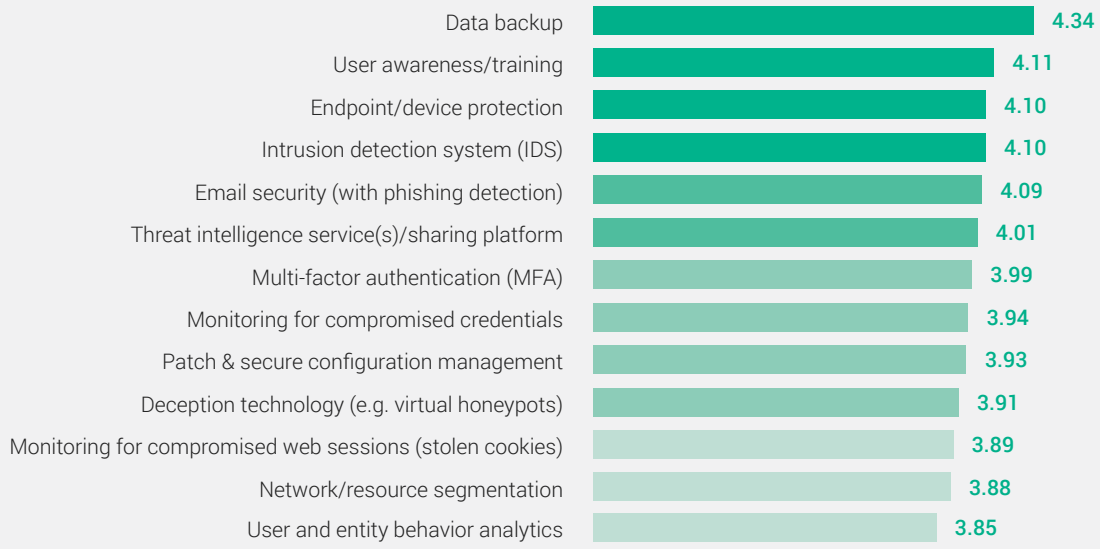
Figure 7

Section 2 | Visibility Gaps and Ineffective Countermeasures Creating Greater Risk

Are Countermeasures Truly Working?

Survey participants ranked data backup, user awareness, endpoint security, intrusion detection systems, and email security as the most valuable countermeasures against ransomware (Figure 8). This approach gives them blanket coverage for people, data, endpoints, network, and email, which have been the most important or highly targeted assets.

Most Important Countermeasures for Mitigating Ransomware Attacks



On a scale of 1 to 5

Figure 8

Yet, as discussed earlier, it appears that these technologies do not solve the problem effectively. Organizations are preparing for the inevitability of a ransomware incident, and more have implemented alternative measures this year, including opening a bitcoin account and creating response plans for ransomware incidents (Figure 9).

Preparations for Ransomware Incidents

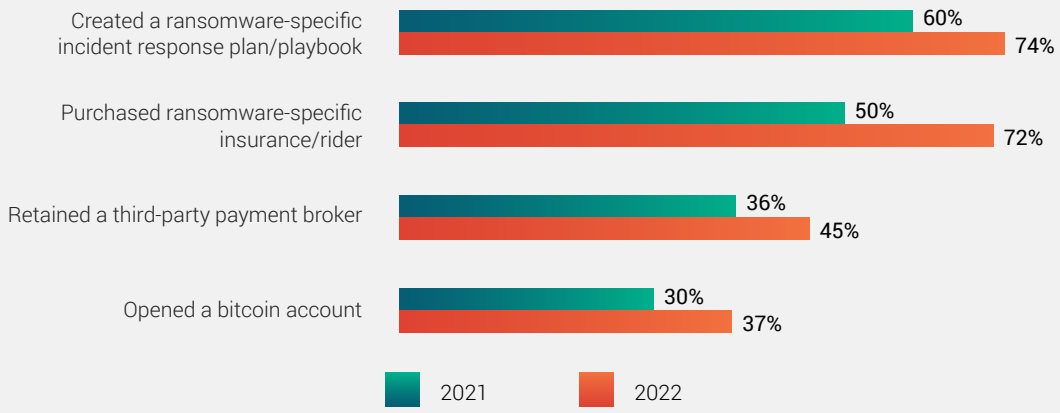


Figure 9

The highest jump was in ransomware-specific insurance riders, from 50.4% last year to 72.3% this year. This leap reflects the overall growing interest in cybersecurity insurance in recent years – 64% of companies have purchased it in 2022 compared to two years ago.

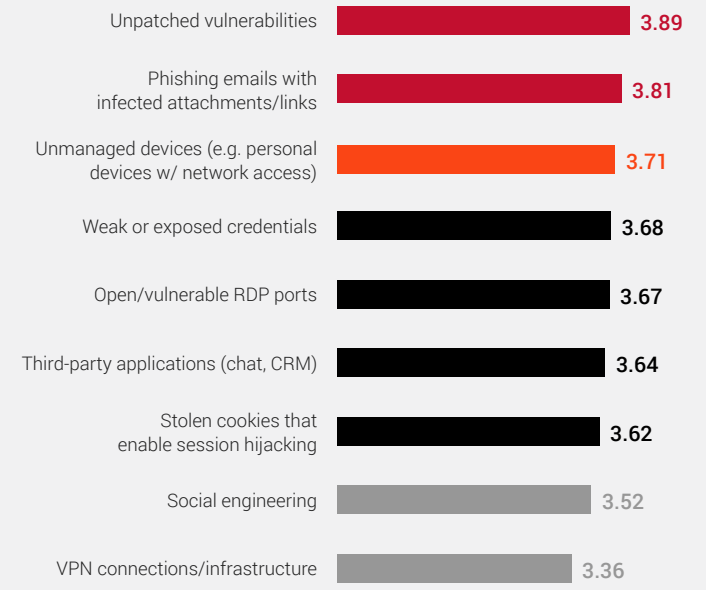
Shifting some of the risk to an insurance carrier may be a prudent move in many cases. However, it doesn't solve the underlying issue of inadequate prevention and, therefore, it's a temporary rather than long-term answer to preventing an attack in the first place. Think of it like buying car insurance. If you get in an accident, the insurance will cover some of your expenses, but that doesn't mean you should be driving around recklessly without a seatbelt. You should still rely on good driving habits to prevent an accident. And just like with auto insurance, if you have too many claims, your premiums quickly shoot up – or worse, you could lose coverage altogether.

The Riskiest Entry Points

Compared to last year, participants ranked all potential ransomware entry points as more concerning. Unpatched vulnerabilities, phishing emails, and unmanaged devices are perceived as the riskiest vectors (Figure 10). It's not surprising to see unpatched vulnerabilities at the top, as they're a common tactic for attackers, who often infiltrate an organization by infecting a device with malware. Ransomware is a malware problem – last year, ransomware was present in 70% of malware-related breaches, according to Verizon's DBIR.

Likewise, phishing, unmanaged personal devices (or even shared family devices that are used to access work applications), weak or exposed credentials, and any other of these entry points increase exposure to malware. Each of them creates a risk individually, but together, they act as force multipliers. Additionally, threat actors target these vectors not only during initial entry but also during multiple stages of an attack, enabling them to escalate privileges, move laterally, and carry out their ultimate objective.

Riskiest Points of Entry for Ransomware



On a scale of 1 to 5

Figure 10

What organizations perceive as their biggest risks doesn't always reflect the full picture, either. Typically, threat actors must take a series of intermediate steps before deploying the ransomware, and malware infections are often a precursor to ransomware attacks. Malware-infected devices, in particular, are extremely risky because cybercriminals can siphon data such as credentials, browser fingerprints, and session cookies, enabling them to impersonate an employee, bypass multi-factor authentication, and launch an attack. The risk is massive because one infected device could access dozens and potentially a few hundred corporate applications – and every application compromised by malware, whether it's a CRM database, collaboration platform, or SSO instance, creates an entry point from that single infected device.

Unmanaged devices pose the greatest concern because the lack of visibility means they can't be monitored for threats such as malware and third-party application exposures. Security teams seldom have this visibility into their attack surface and therefore often underestimate their malware-related risks.

How Malware-Infected Devices Make Your Organization a Target

Many ransomware operators outsource the first stage of their attack – the initial entry – to a specialized group called initial access brokers. These brokers use a variety of tactics to infiltrate an organization, but typically they look for ways to impersonate an insider rather than trying to break through firewalls and other intrusion prevention technology. To impersonate an insider, they need data such as credentials to log in or cookies that enable session hijacking – and that's where malware-infected devices come in.

Using infostealers – malware specifically designed to harvest information from a device – cybercriminals siphon data like credentials and browser fingerprints (which serve to authenticate a user) straight from the endpoint. Even if you detect the malware and wipe the device clean, the damage is done because the stolen data is most likely already on its way to the criminal underground.

Data from malware-infected devices is valuable to initial access brokers because it's current, accurate, and they can log into your network with a greater degree of success.

Data siphoned by malware also puts your organization on the attackers' radar in the first place. Like any other cybercriminals, ransomware gangs don't always target specific organizations but are rather looking for opportunistic targets. They may simply ask initial access brokers for any potential targets with easy access, such as compromised credentials and cookies, that fit their desired profile. If your company is on that list, your likelihood of being the next target skyrockets.

The Growing Concern Over Credential-Stealing Malware

This year, we asked survey participants if reports of credential-stealing malware, such as RedLine Stealer, have elevated their organization's concern of unmonitored personal devices being a potential entry point for ransomware. We weren't surprised to find that, indeed, it does, with 87% of respondents in agreement (Figure 11).

Concerned About Credential-Stealing Malware?

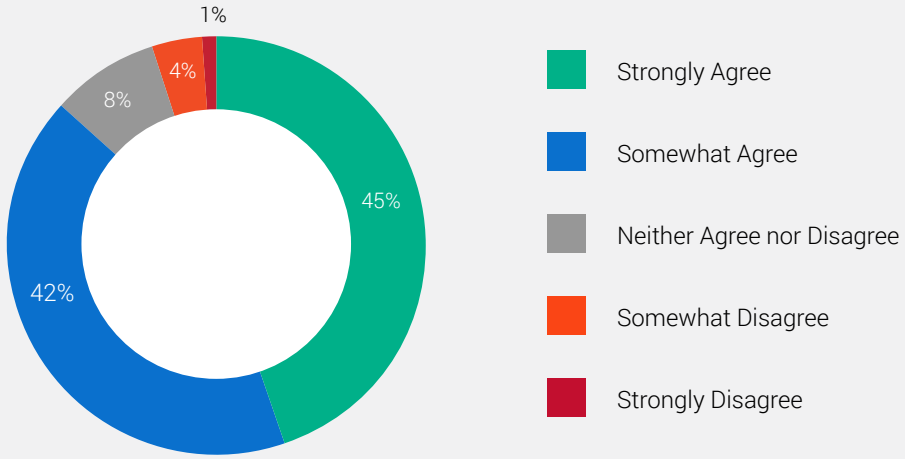


Figure 11

As the name implies, credential-stealing malware is a type of infostealer that harvests credentials. In the past year, RedLine Stealer was one of the most widely used infostealers for Windows devices. Often distributed through phishing campaigns, this malware steals, among other things, data from browsers. The stolen data includes stored passwords, browser fingerprints, and session cookies, which threat actors can use to log into corporate applications and systems, bypassing MFA, to launch a ransomware attack.

RedLine Stealer can masquerade as legitimate Windows updates and other software, making it difficult to detect. The infostealer also poses a big risk for unmonitored personal devices that employees use to access the corporate network and applications. Without any visibility into those devices, security teams have no way to monitor for malware infections and risky employee behavior such as accessing critical third-party applications from their infected endpoints.

Section 3 | Overcoming Barriers and Improving Preparedness

People: The Top Barrier to Effective Defenses

Lack of budgets and board support were major hurdles for security teams in the past. Business leaders' wide-spread awareness about the ransomware problem, however, created a silver lining: budget allocations and board involvement are no longer obstacles. In fact, board support grew from the previous year, likely a testament to the high-profile, high-impact nature of the threat. Other research from the past year shows that 86% of organizations have increased their security budgets to fight ransomware.

The top three barriers called out by our survey participants are lack of skilled personnel to implement solutions, difficulty implementing related tools or technologies, and low security awareness among employees (Figure 12). In other words, the biggest barrier is people.

Obstacles to Establishing Effective Ransomware Defenses

On a scale of 1 to 5

Figure 12

The talent gap retains the top spot from last year, a recurring theme that's been vexing the security industry for many years. The Great Resignation exacerbated the challenge as all sectors experienced a revolving door of employees leaving their jobs. In the US, for example, cybersecurity job openings grew 29% in the past year, more than double the pre-pandemic growth rate.

A 2022 survey of security operations center (SOC) analysts found that 69% of teams are understaffed and workloads have increased for 60% of them in the past year. But the problem is likely to get even worse – 71% said they're experiencing job burnout and 64% said they're likely to switch jobs in the next 12 months.

One way to alleviate the shortage of people is by automating workflows as much as possible. Select your security stack thoughtfully so you avoid inducing alert fatigue. By choosing solutions that bring definitive answers rather than producing more alerts, you can reduce both security team workload and burnout.

In terms of employee awareness, consider creating a safety net that protects your organization when employee awareness doesn't. Humans will inevitably make mistakes, and even the savviest employees (including security practitioners) can fall for a crafty fraudster's tricks. Even if you have a strong employee awareness program, implement solutions that help mitigate risks created by human behavior. Better yet, look for tools that both encourage positive security behaviors and reduce the risks of inevitable human error.

Worth noting is that "other conflicting priorities" moved from last year's fourth spot to the bottom of the list of hurdles. Perhaps the magnitude of ransomware has escalated to such a degree that it placed all the other types of threats firmly in its shadow.

Common Defenses

The top solutions **already in place** among surveyed organizations are data backup, MFA, user awareness training, network/resource segmentation, email security, and patching and secure configuration management (Figure 13). This is an appropriate set of technologies, given how ransomware operates. The primary focus for security teams is on stopping malware and its related entry points while also preparing to restore and recover data when an incident inevitably takes place.

Top Security Solutions in Place

	Already have it
Data backup	87%
Multi-factor authentication (MFA)	77%
User awareness training	76%
Network/resource segmentation	75%
Email security	74%
Patch & secure configuration management	74%

Figure 13

Of these five technologies, data backup (62%), email security (52%), MFA (51%), and endpoint/device protection (46%) also made the list of solutions that organizations feel are **already in good shape**, with credential monitoring (45%) rounding up the top five in this category (Figure 7). Data backup, however, had a slight drop in the "good shape" score and an uptick in planned upgrades, which could signal that some organizations made hasty investments in subpar solutions and are now working to rectify the situation.

Changes in Password and Authentication Practices

Among password and authentication practices specifically, MFA is now table stakes. We discovered a 71% jump (from 56% in 2021 to 96% in 2022) in the number of organizations that have MFA in place or plan to implement it (Figure 14). Another big jump was in monitoring for compromised employee credentials, from 44% to 73%.

These two changes show organizations now realize that credentials are at the forefront of protecting employee identities. Additionally, with the exception of single sign-on (SSO), we found an increase in every authentication practice this year. That's great news in today's threat landscape - where the problem of compromised, weak, and reused credentials is rampant.

In 2021 alone, SpyCloud recaptured 1.7 billion exposed credential pairs from the criminal underground. We also discovered a 64% password reuse rate for users with more than one password exposed in the last year. By placing a bigger emphasis on password and authentication measures, you are in a better position to prevent the risk of compromised logins and to protect identities – and consequently, greatly improve your organization's ability to prevent ransomware incidents.

Password and Authentication Practices

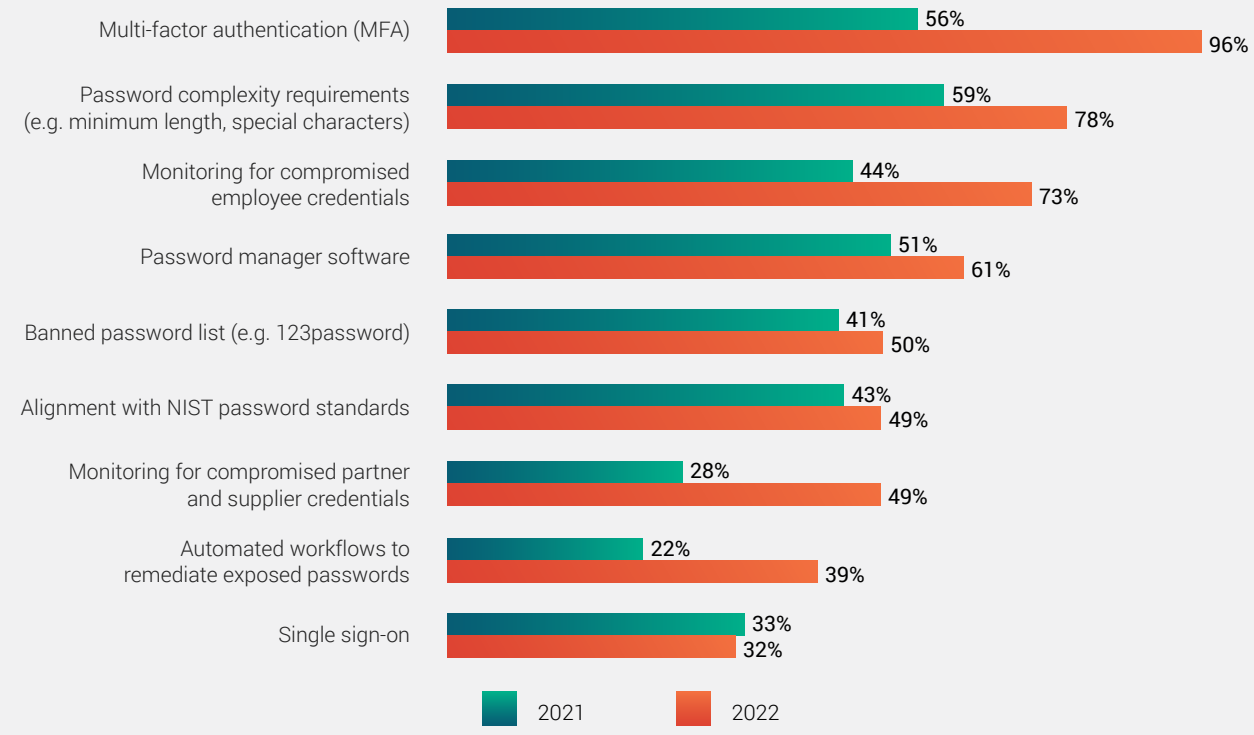


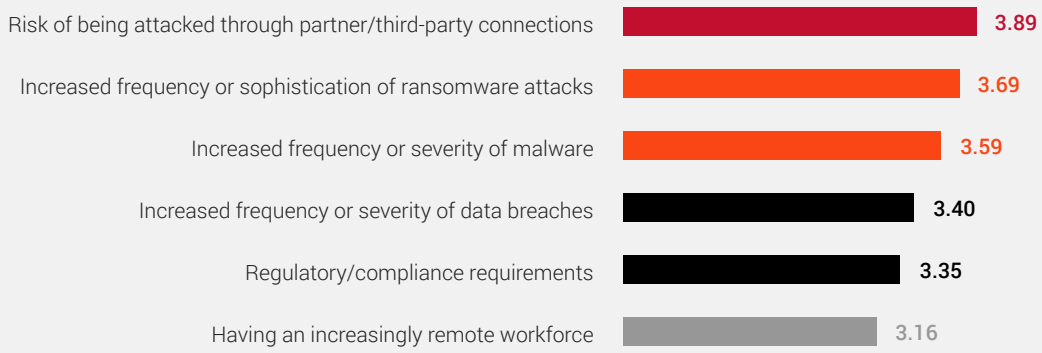
Figure 14

And finally, the third existing or planned password and authentication practice that saw significant year-over-year growth is monitoring for compromised partner and supplier credentials (75% increase). Several high-profile supply chain attacks in the past two years exposed how vulnerable all organizations are to third-party risk, and this concern is now top of mind for CISOs. Supply chain attacks ranked as the third greatest concern in the CISO survey sponsored by SpyCloud, while third-party vulnerabilities and risks were the highest-ranked type of vulnerability. Recognizing that partners and vendors are a weak link, organizations are taking additional measures to minimize this risk.

Future Plans to Improve Defense

Concern about third-party risk is so great that it surpassed ransomware in our survey as the factor impacting upcoming security investments the most – moving to the top from last year's fourth spot (Figure 15).

Greatest Impact to Cybersecurity Plans



On a scale of 1 to 5

Figure 15

The increased severity of malware and data breaches are the third and fourth biggest factors driving planned investments in the next 12 months. Data breaches dropped to fourth place from last year's second. Keep in mind that data stolen in breaches can facilitate new malware and ransomware attacks, so think of data breaches not simply as an outcome but as a source of further compromises. Worse, data breaches create a perpetual attack cycle because cybercriminals leverage the freshly stolen data to launch new attacks. Essentially, breaches are another force multiplier that boosts the odds of a successful attack for threat actors.

Consider all the factors that drive your risk and think holistically when you make security investments – especially when economic factors are at play and you're under pressure to cut expenses and maximize revenues. While you may feel tempted to halt the purchase of new security tools to fill those gaps, the financial and other impacts a breach can have on your organization will outweigh the small savings from downsizing security investments.

Remote Work Loses Importance

Remote work dominated much of security teams' attention in 2020 and 2021, but organizations have moved on to other priorities. The remote workforce has the least impact on investments planned for the coming year, according to our survey respondents. This shift is likely due to organizations embracing the new reality created by remote and hybrid work and realizing that protecting the network is no longer enough. The new approach is to protect identities, and this strategy is the best way to solve challenges associated with ransomware attacks.

The new hybrid workplace creates an environment in which unmanaged devices and unmanaged cloud applications generate many new places where workers can accidentally expose data or give criminals entry points, yet security teams still aren't focusing sufficiently on these vulnerabilities. Additionally, your attack surface is much broader than in the past. Even if your remote workforce is shrinking, the attack surface is not – and many security teams don't have the visibility they need.

Upgrades and Additions to the Security Stack

As noted earlier, organizations are more dissatisfied in general this year with their security stack and more of them plan to update or upgrade their technologies (Figure 7). If we look at the growing dissatisfaction through the lens of the higher number of organizations affected by ransomware, we suspect that organizations had a misplaced confidence in their security last year but have seen the shortcomings since then.

Moreover, solutions that have been less considered before, such as monitoring for compromised web sessions, are among the top countermeasures planned for addition. This suggests that organizations are looking to extend protection to other areas as threat actors, confronted with the more traditional defenses, shift their focus to other vulnerabilities that are less often or less thoroughly protected. Major attacks in recent months also served to drive up malware concerns, sparking further interest in additional security layers.

Monitoring for malware-compromised devices or web session cookies is an effective way of preventing ransomware incidents because you're proactively protecting vulnerable employees before threat actors can access their accounts through session hijacking. Armed with this data, attackers can use "anti-detect" browsers to bypass MFA and even newer browser fingerprinting anti-fraud technologies. This type of monitoring helps you identify employees whose endpoints have been infected by infostealers so you can invalidate their active web sessions and take further post-infection remediation steps.

Post-infection remediation (Figure 16) is a critical yet frequently overlooked step in malware incident response. Wiping & reimaging an infected device doesn't mitigate long-term ransomware risk created unless all compromised applications are also properly remediated. And for that you need a complete picture of the exposed credentials, stolen session cookies, and other data that could allow ransomware operators to "walk right in." With information about each exposed device, application, and user, you can accelerate remediation and significantly shorten the enterprise exposure window.

Post-Infection Remediation

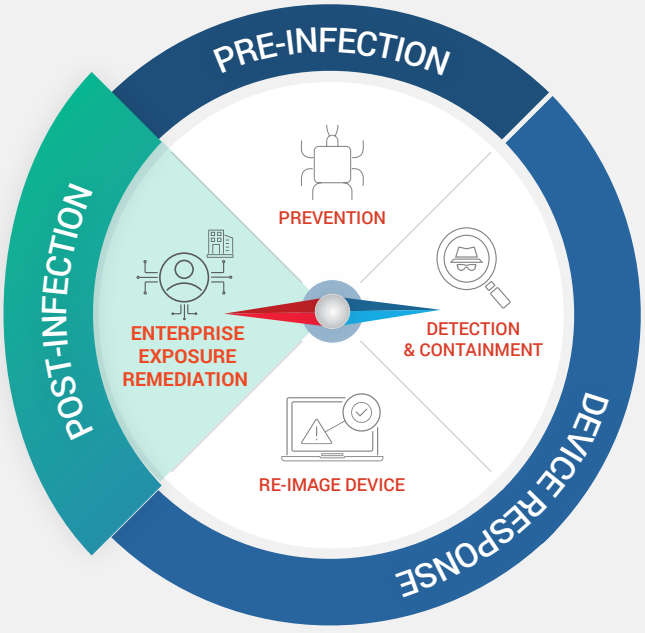


Figure 16

SpyCloud

Focus on Prevention to Boost Resilience

The findings of this year's report may feel discouraging as they illustrate that ransomware gangs continue to experience widespread success in their nefarious endeavors. However, the data from this report can help you look at the ransomware problem from a different perspective. The incomplete understanding of the hidden ransomware risks and vulnerabilities is a big reason why organizations are falling further behind the attackers. Use the report as an opportunity to understand the hidden risks and weaknesses, such as hard-to-detect malware infections and unmanaged devices, that may be affecting your own organization.

While you continue to strengthen and expand your defensive layers, you should place an equal, if not bigger, emphasis on prevention. The cost of effective ransomware prevention is much lower than the cost of response and recovery from an incident. Any proactive measures that you implement for ransomware prevention and early detection also help you fight other threats, boosting your organization's security posture — and, most importantly, improving your overall resilience to cyber threats.

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.

Enterprise Protection

Prevent account takeover that can lead to ransomware.

Learn More

Consumer Protection

Combat account takeover and online fraud.

Learn More

Investigations

Unmask criminals attempting to harm your business.

Learn More

Data Partnerships

Enhance your solution with SpyCloud's data.

Learn More

SpyCloud