The CISO Circuit by
YL VENTURES

Top CISO Insights Edition 8

Ransomware Risk in 2022

About YL Ventures

YL Ventures funds and supports Israeli tech entrepreneurs from seed to lead. Based in Silicon Valley and Tel Aviv, the firm currently manages over $800 million and exclusively invests in cybersecurity.

YL Ventures is uniquely focused on supporting the U.S. go-to-market of early-stage companies and leverages a vast network of industry experts, Chief Information Security Officers (CISOs) and U.S.-based technology companies as advisors, prospective customers and acquirers of its portfolio businesses. The firm's focused strategy allows it to conduct rapid and efficient evaluations for early-stage entrepreneurs and guide founders through their ideation processes pre-investment. The firm is also dedicated to providing unmatched, hands-on value-add support to each of its portfolio companies, both strategically and tactically, across multiple functions post-investment.

The firm's global network and footing in the U.S. have always counted among its most powerful assets. YL Ventures bridges the gap between Israeli innovation and the U.S. market. The firm has formalized and amplified this core competitive advantage through the launch of YL Ventures' Venture Advisory Board.

YL Ventures' Venture Advisory Board is composed of over 100 security professionals from leading multinationals, including Microsoft, Google, Amazon, Intuit, Hearst, Kraft-Heinz, Walmart, Netflix, Nike, Spotify, and Zendesk. The firm's relationship with its advisors, as well as its extended network, is symbiotic in nature. The advisors bolster the YL Ventures investment due diligence process and provide the firm's portfolio companies with continuous support across a multitude of functions throughout their life cycles. In return, network members benefit from introductions to pre-vetted Israeli cybersecurity innovations and receive direct exposure to a market second only to the U.S. in cybersecurity innovation.

Portfolio

eureka
Cloud Data Security Posture Management
www.eureka.security

PIIANO
Privacy Engineering Infrastructure
www.piiano.com

valence
SaaS-to-SaaS Supply Chain Security
www.valencesecurity.com

grip
SaaS Security Control Plane
www.grip.security

enso
Application Security Posture Management
www.enso.security

satori
Secure Data Access
www.satoricyber.com

cycode
Software Supply Chain Security
www.cycode.com

orca security
Cloud Security
www.orca.security

HUNTERS
SOC Platform
www.hunters.ai

VULCAN.
Cyber Risk Posture Management Platform
www.vulcan.io

Karamba Security
Embedded Security for Connected Systems
www.karambasecurity.com

RIDEVISION
Predictive Vision for Motorcycles
www.ride.vision

Acquisitions

MEDIGATE Acquired by **CLAROTY**

build.security Acquired by **elastic**

AXONIUS Exited to **late-stage investors**

Twistlock Acquired by **paloalto**

HEXADITE Acquired by **Microsoft**

FIRELAYER Acquired by **proofpoint**

Seculert Acquired by **radware**

BlazeMeter Acquired by **ca technologies**

Clicktale Exited to **Amadeus Capital Partners**

AccelaWeb Acquired by **Limelight Networks**

UPSTREAM COMMERCE Acquired by **Walmart**

About the CISO Circuit

YL Ventures frequently confers with an extended network of prominent cybersecurity professionals, including our Venture Advisory Board and industry executives, to assess our portfolio prospects, inform market predictions and cultivate portfolio company business development. As such, we have established direct lines of communication with the global market's preeminent CISOs and cybersecurity experts for ongoing insights into their thoughts, priorities and opinions about the state of their organizational cybersecurity.

We recognize the value this information presents to entrepreneurs, especially those wishing to enter the U.S. cybersecurity market, and to the cybersecurity community as a whole. For this reason, YL Ventures launched "The CISO Circuit", an initiative under which we publish reports containing gathered intelligence for general use.

We hope the observations compiled in this report will prove useful to aspiring cybersecurity entrepreneurs and the rest of the cybersecurity community.

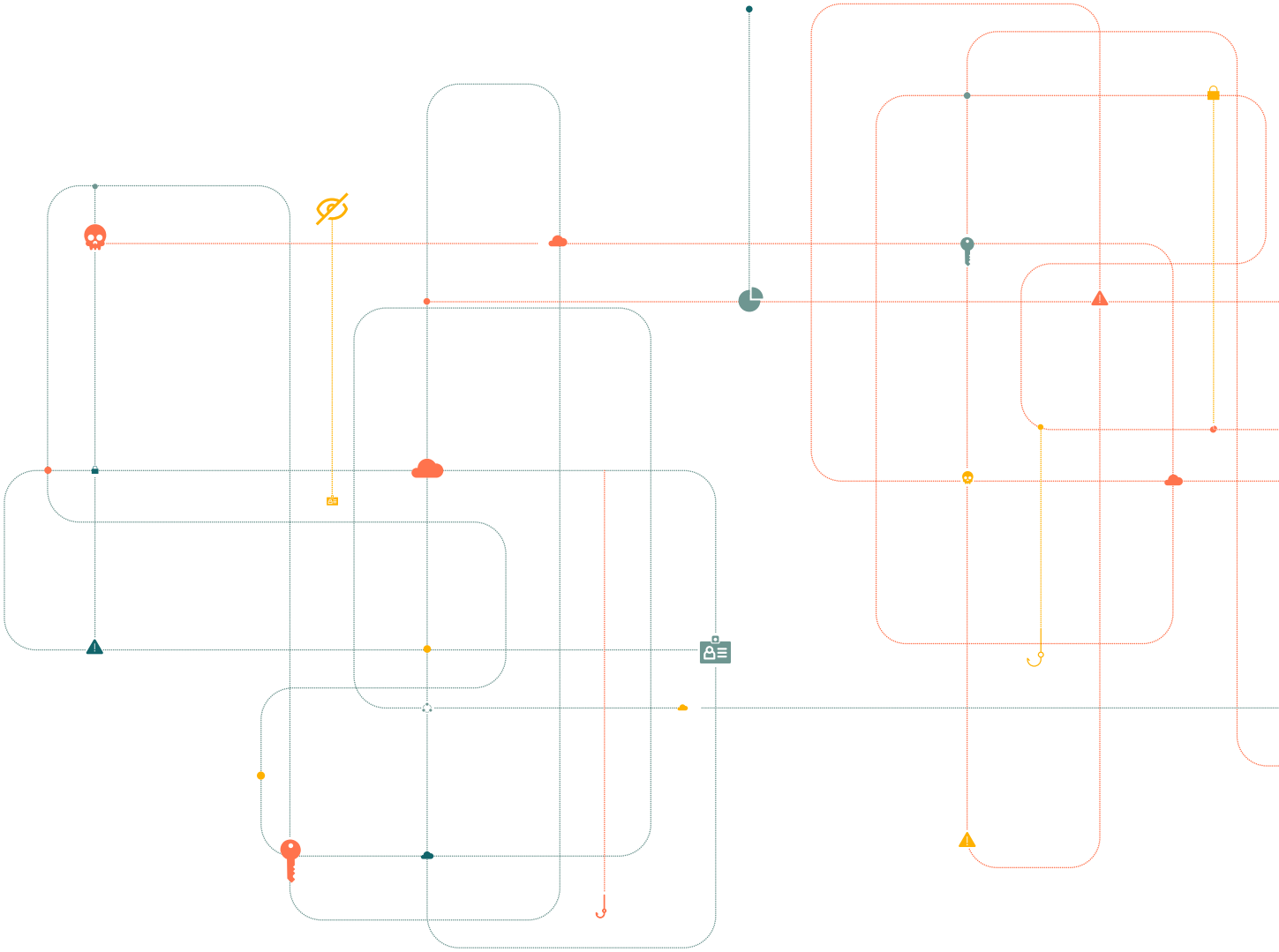


Table of Contents

Introduction 5

Ransomware Attacks 6

How Ransomware Works 6

Frequency of Ransomware 6

Current Best Anti-Ransomware Practice 7

Prevention 9

Backup and Recovery 10

The Future of Ransomware 11

Ransomware in the Cloud 11

The Expansion of Ransomware 12

Critical Infrastructure and Operations 12

Dedicated Ransomware Solutions 13

Conclusions 14

Outreach and Contact Information 15

Appendix 16

Introduction

In this report of the CISO Circuit, our team set out to understand the challenges ransomware presents to enterprise security teams. Over the course of 40 interviews with distinguished cybersecurity executives hailing from a wide spectrum of verticals and company sizes, we collected responses to a series of questions (see Appendix) about their most pressing ransomware concerns and current best ransomware mitigation practices.

Ransomware attacks are some of the most disruptive cybersecurity threats to enterprises across all industries today, topping security executive concerns. After cyber extortionists infiltrate an organization's system and hold its data hostage via encryption, victims of ransomware run the risk of total operational failure across any task reliant on the encrypted information. In a digitally-run economy dependent on data access and flows to operate, victims without the means to regain their information–especially mission-critical data–either through reliable backups or by buying it back, may lose their businesses entirely.

The effects of ransomware range far and wide. Unlike other types of attacks, ransomware can carry physical, as well as digital and reputational consequences, halting critical functions that include production, quality assurance, distribution, operations and customer support. This makes certain technologies, such as smart grids, autonomous vehicles, hospital networks and critical infrastructure, particularly dangerous targets. Only recently, SpiceJet was hit by a ransomware attack that left thousands of passengers stranded as a result. A similar, well-known incident took place in 2020 against navigation giant Garmin. Other high profile incidents over the last few years include the $5M extortion of fuel supplier Colonial Pipeline, the $11M extortion of beef-supplier JBS, the $40M extortion of insurer CNA Financial Corp and the $50M extortion of electronic giant Acer.

The financial disruption, privacy implications and occasional danger caused by ransomware attacks offer victims little choice but to heed their attackers. According to Sophos, recovery from a ransomware attack averages $1.85 million. Crowdstrike recently concluded that damages from ransomware are expected to reach $6 trillion this year, highlighting how valuable victim data and business continuity are to both adversaries and their victims. Our experts warn that the sophistication and disruptive potential of ransomware attacks are only expected to grow.

In fact, attackers are already carrying out double and triple extortion threats. Cyber criminals are always looking to maximize bottom lines and have leveraged many creative monetization strategies in the process. While ransomware has historically focused on encryption, many contemporary attacks involve "double extortion", in which attackers exfiltrate sensitive data before encrypting it within an organization's environment. They then demand ransom for both decrypting and not leaking the information. More recently, we have seen the rise of "triple extortion", in which bad actors also directly threaten their victim's clients and suppliers over information discovered about them from an attack. Further pressure may be applied in the form of DDoS attacks and direct leaks to the media.

In researching this topic, it is clear that the cybersecurity market still lacks a silver bullet for ransomware attacks despite the myriad solutions addressing different areas of ransomware risk. At this point in time, no enterprise can currently ensure full protection against bad actors taking their information hostage. Security leaders must instead rely on detecting ransomware attacks as early as possible, as well as building rapid response and backup plans to reduce their impact. Nonetheless, given the sheer volume of data stored by organizations, even today's most extensive backups cannot fully restore encrypted or stolen information in its entirety.

Moreover, as with any other kind of cybersecurity breach, post-attack solutions do little to mitigate the reputational damage and privacy harm that ransomware attacks produce. Finally, as organizations continue to digitally transform, we can expect ransomware attacks to migrate to the cloud as well. Expanding the threat beyond traditional endpoints, this gives CISOs yet another reason to stay up at night.

Ransomware Attacks

How Ransomware Works

Ransomware attackers traditionally access enterprise environments via phishing and other common attack vectors, such as gaps in identity management and zero-day exploits. Once inside, they identify valuable data and assess security controls in order to disable endpoint protection tools and delete or encrypt backups. Data is then possibly exfiltrated and later used for extortion before getting encrypted with malicious software known as ransomware.

It is worth noting that ransomware attacks are swifter than other advanced persistent threats. Where other attacks can take months to carry out, the first instance of malicious activity after a ransomware deployment averages three days. This speed lies at the heart of why traditional security tools often fail to mitigate ransomware attacks. Moreover, attackers often circumvent their security triggers, such as endpoint security's reliance on behavior-based detection.

Have you experienced a ransomware attack?

Frequency of Ransomware

Ransomware attacks have proliferated over the last decade as they have grown increasingly efficient and lucrative. This is in large thanks to "RaaS" ("Ransomware-as-a-Service"), a criminal business model that uses affiliates to deploy already-developed ransomware software as well as virtually undetectable penetration strategies. Critically, RaaS' specialization offers highly sophisticated technologies and services for specific elements of the ransomware attack supply chain. The RaaS model, which can include both fixed-fee subscription and ransom-based revenue sharing, has significantly widened the pool of bad actors behind ransomware attacks to include people with fewer relevant technical skills and experience to successfully execute end-to-end ransomware campaigns.

42% of our surveyed experts admitted to their organization falling victim to one or multiple ransomware attacks. Such a significant figure not only indicates how widespread ransomware incidents have become, but also how often they disrupt enterprises across all industries and sectors. It is moreover clear that the cybersecurity market and its leaders have yet to devise a reliable method for preventing these attacks.

Current Best Anti-Ransomware Practice

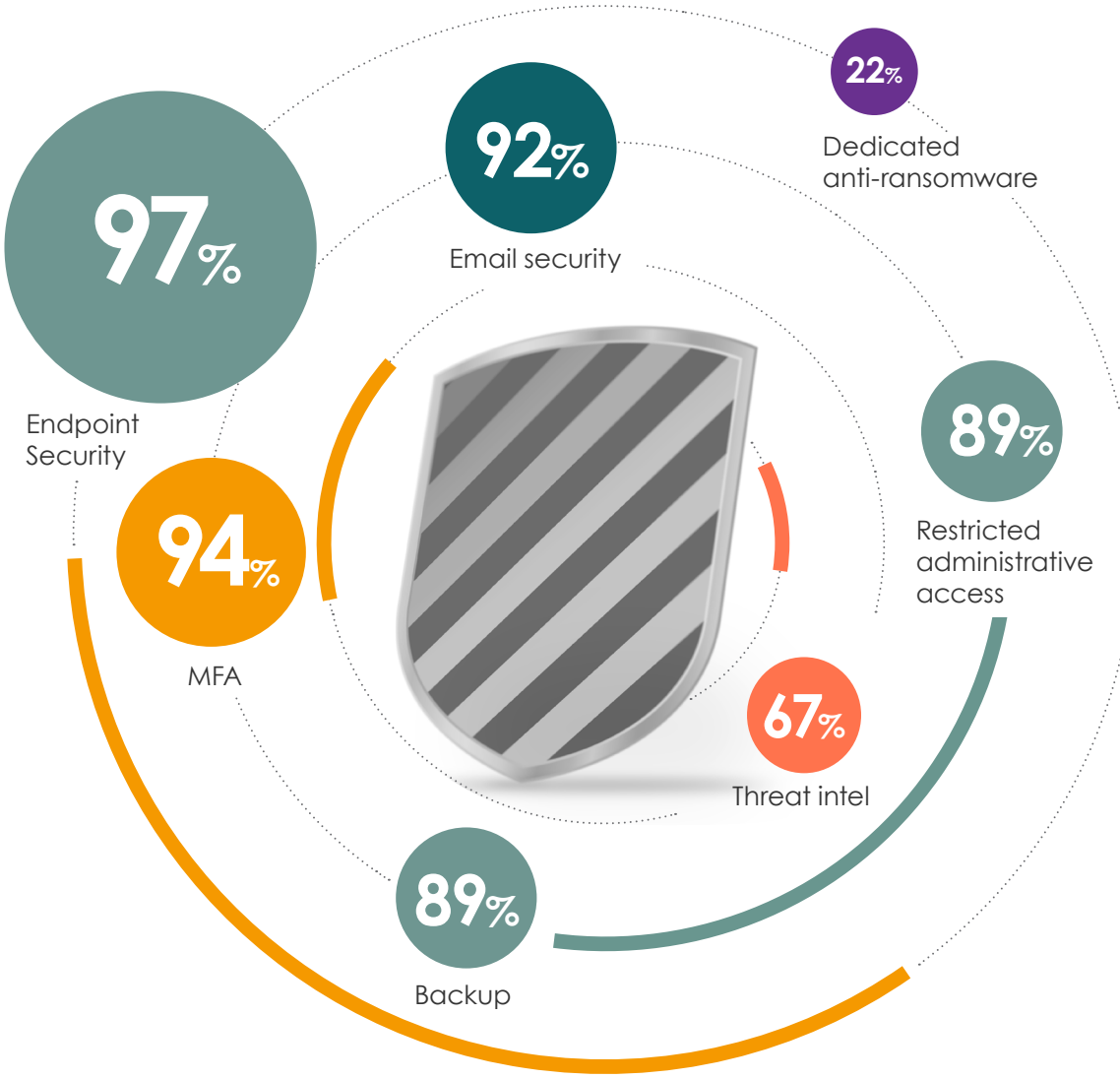
Security experts utilize two main approaches to tackle ransomware: The first stresses the importance of maximizing prevention, and the second requires recovery and response to nullify ransomware's ultimate risk of total data loss. The latter is dependent on early detection and most often refers to the employment of reliable backups.

Currently, security teams require a full security stack to mitigate the total threat of ransomware. Their anti-ransomware tool kits tend to primarily focus on preventative solutions (60% of allotted anti-ransomware budget), with a secondary focus on detection, recovery and response (40%).

Over 90% of respondents have four or more preventative solutions to manage ransomware risk. Of these solutions, 97% include endpoint security, 94% multi-factor authentication, (MFA) 92% email security, and 89% restricted administrative access. Additional, but far less common, solutions include threat intelligence, employee awareness training and 24/7 security operation centers.

22% of respondents reported employing a dedicated anti-ransomware solution. However, upon further investigation, we found that this tended to refer to anti-ransomware features offered by major endpoint security providers, rather than specific purpose anti-ransomware point solutions.

What do you currently have in place to manage ransomware risk?



These responses offer two important insights. First, enterprises see more value in protecting against and preventing ransomware attacks. No matter how reliable their recovery plan, security leaders still prioritize avoiding ransomware attacks from hitting them at all, insisting that preventative, or proactive, cybersecurity efforts are the most effective method of decreasing ransomware's ROI and disrupting attacks. Stressing the financial motivations behind ransomware attacks, they believe that attackers are far less incentivized to target hardened and prepared enterprises.

Second, enterprises do not believe that full protection against ransomware is possible, and insist that overcoming any defense is only a matter of time for motivated bad actors. This is especially poignant for enterprises that have more attack vectors than extant security teams can defend. It is thus unwise to invest entirely in prevention and instead necessary to organize a strong recovery plan, too.

Ransomware attackers mainly target endpoints, leaving our surveyed experts on a constant mission to keep them up to date and bolster defenses already in place.

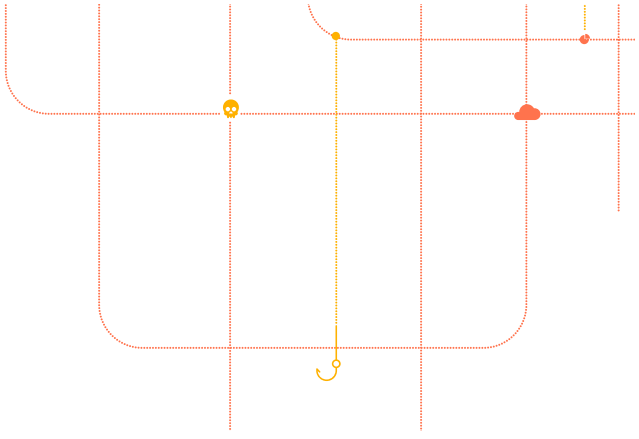
Prevention

By distinguishing their biggest areas of concern, we can better understand which domains CISOs focus on for preventing ransomware, as well as the best practices they employ for this area of enterprise security.

When asked which attack vectors cause them the most concern, the majority of responses included phishing and unpatched vulnerabilities. In fact, phishing was most often categorized as the highest level of risk by 70% of respondents. This is consistent with recent findings by TechTarget that 80% of cyber attacks in 2022 are expected to originate from phishing scams[1]. 56% of respondents categorized unpatched vulnerabilities as high, which is also consistent with recent findings designating them as a primary ransomware attack vector. Malware and supply chains were each ranked as high risk by 44% of respondents. Widespread privileged access was ranked next as a primary area of concern at 42%. Other areas of exposure, such as lacking segmentation and insider threats, factored much less significantly.

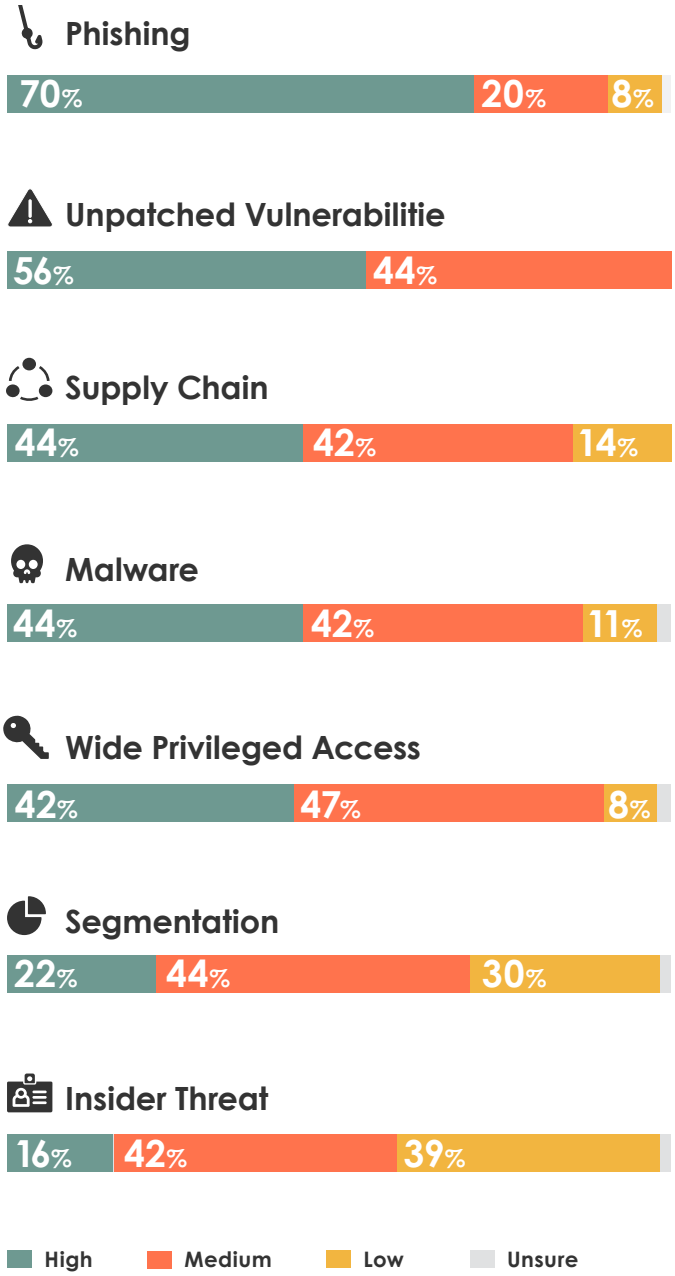
Ransomware attackers mainly target endpoints, leaving our surveyed experts on a constant mission to keep them up to date and bolster defenses already in place. CISOs typically accomplish this by employing Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR), as well as by automatically updating both solutions at every opportunity. 36% of respondents believe this approach to be mostly effective. Meanwhile, 19% rank it very highly, 17% moderately and 17% only occasionally helpful.

Surveyed CISOs moreover conduct regular vulnerability scanning to identify and address gaps across their environments to limit their attack surface–especially those on internet-facing devices. 33% believe this is an effective strategy, with 22% ranking it highly. 28% only moderately believe in it.



[1] Find additional data points on ransomware by Cobalt here

Which areas of exploitation qualify as high risk for ransomware attacks?



Risk management and cyber hygiene practices for third parties or managed service providers (MSPs) did not factor highly in this question, despite many of today's breaches originating from third parties. However, research by cyber risk intelligence provider Black Kite found that ransomware was the most common attack to result from third-party breaches in 2021. Our respondents' own experience confirms this, having sustained attacks from call centers and logistics providers connected to their networks. In one case, the vast majority of 26 ransomware attacks launched against a respondent over the past year were carried out via third parties.

Respondents appear conflicted over the efficacy of employee awareness and training programs to prevent ransomware, which often include guidance on how to identify and report suspicious activity (e.g., phishing) or other incidents. 53% give it a low or moderate score of importance, while 47% rank it highly. Those in favor of these programs argue that they are necessary, given that end users are typically perceived to be an enterprise's weakest security link. This is especially true for phishing. Awareness and training advocates believe it is imperative to make every enterprise employee an active participant and stakeholder in their company's cybersecurity posture, as even the best preventative technology can be rendered moot by faulty human behavior. Those who disagree with this strategy argue that no amount of training can prevent the inevitable click on a malicious link–and it only takes one to let ransomware criminals in.

Backup and Recovery

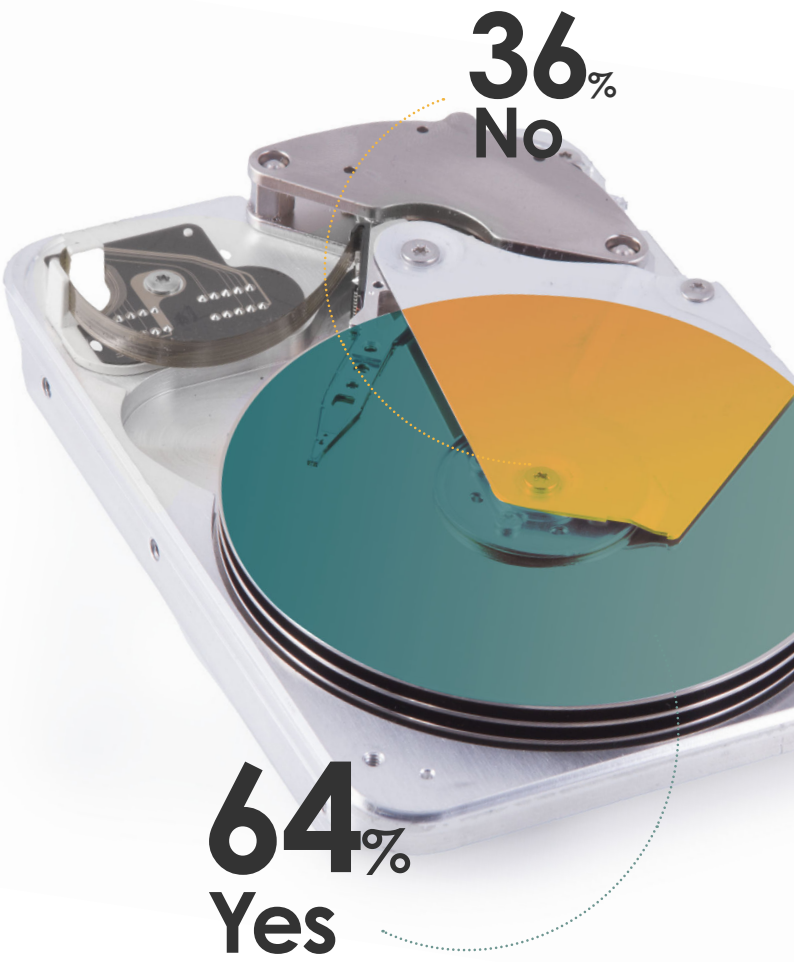
90% of CISOs have prepared for successful ransomware attacks with backup solutions. While all of our respondents insist that incident response plans for ransomware attacks are paramount for proper risk mitigation, only 64% have a documented, specialized ransomware recovery plan in place today. Among them, 88% carry out multiple ransomware response drills throughout the year.

Building an effective recovery program is highly challenging and resource-intensive, given that it must be kept updated and protected against ever-evolving threats. Such efforts must employ dedicated, experienced staff–a difficult task given today's ongoing talent shortage–and the required velocity can come at the heavy expense of other high-priority activities. Moreover, the industry has yet to agree on how to gauge the efficacy of these programs and measure their success. How should CISOs reliably assess whether or not their program has reached an acceptable threshold of risk mitigation?

When asked how to build an effective backup and data recovery program, 64% of respondents answered that they invest in restoration assurance. 60% use mixed data storage and data integrity assurance. 44.5% claimed to back up end-user systems. The rise of cloud-based solutions, such as OneDrive and Google Drive, help explain this. They ease pressure off of backing up local end-user systems. Thus, reliance on cloud storage curtails the need for endpoint backups because these services offer some of the most hardened datastores on the market. This does not, however, negate the ongoing importance of the shared responsibility model. Only 17% of participating CISOs still use manual backups.

Immutability tops the list of strategic considerations for backup solutions due to the criticality of maintaining data integrity. After all, this is the deciding factor of harm caused to enterprises when bad actors take information hostage. CISOs unilaterally recommend maintaining offline, encrypted backups of data and regularly testing their integrity. 50% of our respondents attributed very high importance to this while 17% believe it to be of general importance. The remaining 33% ranked its importance from moderate-low. This answer may be influenced by the impracticality of maintaining effective offline backups due to the sheer volume of data involved in today's data-driven economy. Many CISOs are faced with having to choose between limiting the volume of data they manage or investing in costly additional data centers.

Does your incident response plan have a documented, specialized ransomware recovery plan?



Building an effective recovery program is highly challenging and resource-intensive, given that it must be kept updated and protected against ever-evolving threats.

The Future of Ransomware

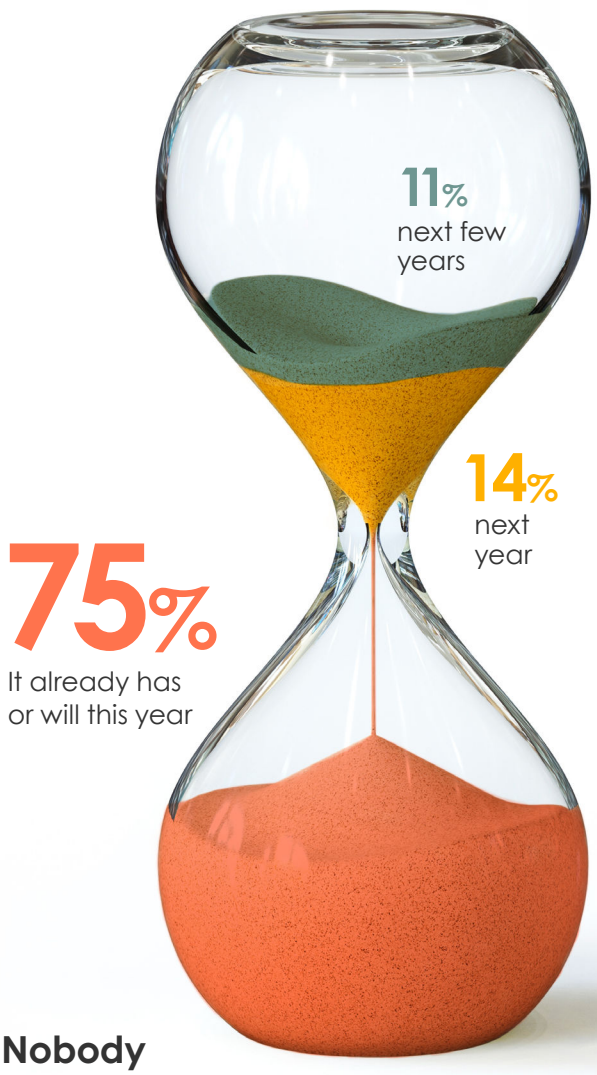
Cyber criminals are always looking for new means to profit and grow their profit margins. What does this mean for the future of ransomware as we shift our data to the cloud? Will the seeming impenetrability of cloud service providers dissuade them? Are cloud providers even as hardened as we think?

Ransomware in the Cloud

The rise of cloud infrastructure, with its many available attack vectors, holds great potential for cybercriminals. These troves of data are highly attractive targets, and our surveyed experts expect ransomware attacks in the cloud to increase in the coming years. Though current available literature on ransomware specifically in the cloud is sparse, 75% of our surveyed experts are confident that they have already taken place or will this year. They are also certain such attacks will only increase as ransomware attackers hone their craft within cloud environments to exploit misconfigurations and other cloud-specific vulnerabilities.

Attackers are highly incentivized to target the cloud. Digital transformation moved massive amounts of data to the cloud, nearly to the extent of nullifying any data-driven mission to attack endpoints. However, as previously mentioned, commercial cloud environments are reputed to employ some of the most reliable security in the industry, requiring attackers to put more effort into breaking in. Moreover, cloud environments tend to be easier to restore, thus making the data within them more resilient. Overall, the ROI of cloud attacks remains lower for attackers than continuing to target on-prem infrastructure–for now.

When do you think ransomware will hit the cloud?



What kind of innovations can we expect of bad actors looking to monetize stolen and encrypted data in the cloud?

Existing solutions offer little prevention or recourse against attacks targeting the cloud. Organizations will have to add yet another layer to their security stacks. Specifically, 57% of respondents believe that ransomware's expansion into the cloud will require some slight adjustments to existing solutions, whereas 23% believe it will require a complete new set of solutions. Only 14% feel already fully protected in the cloud. These numbers clearly indicate interest and need for innovation in the cloud ransomware space.

The Expansion of Ransomware

RaaS is also on the rise. Surveyed CISOs expect this out-of-the-box business model to mature in the coming years and largely replace the traditional practice of criminal groups carrying out ransomware attacks independently.

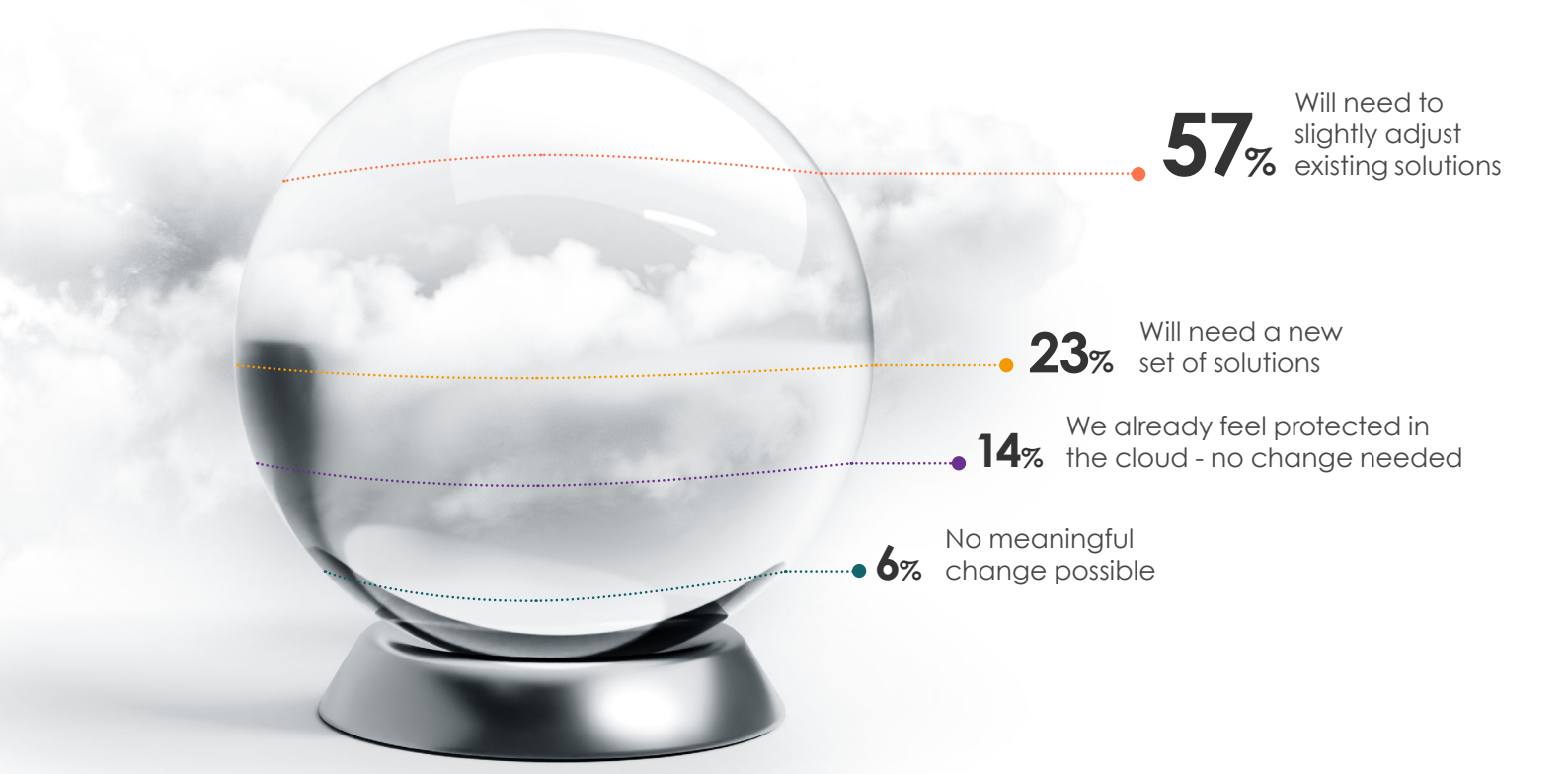
Given the growing reliance on data exfiltration as a method of extortion, we can expect bad actors to target backups and cloud services mitigating the full impact of their attack. Surveyed respondents are certain that this practice will continue to evolve alongside risk-mitigation efforts.

Critical Infrastructure and Operations

Many are wary of how cybercriminals will approach the next phase of monetizing cybercrime. It is important to recall that data is not the only high-value target in a ransomware attack. Our surveyed experts point out that today's black market data saturation has shifted ransomware's monetization focus to business continuity. **Ransomware can be an excellent means for disrupting critical services, such as clean water and healthcare.** Indeed, hospitals and oil refineries have been famously targeted by some of the highest-profile ransomware attacks over the last decade. The potential for harm in these incidents almost always incentivizes payment to nullify their threat as soon as possible. So long as this is the case, ransomware will continue to pose a growing threat to product manufacturers and distributors, as well as service providers.

It is worth noting that, despite its low popularity among surveyed experts, network segmentation is still one of the best practices for limiting the blast radius of a ransomware attack. This is seen as a reliable method for ensuring that only a fraction of machines fail instead of the full roster.

How will ransomware expansion into the cloud align/clash with existing ransomware solutions and best practices?



Dedicated Ransomware Solutions

Despite CISO preoccupation with ransomware attacks, no true, dedicated anti-ransomware solutions are available to them. Instead, their security stacks consist of many different security solutions, including some with anti-ransomware features. Many respondents are perplexed by the idea of a dedicated solution, given that ransomware is just one of many security risks mitigated by their multi-layered approach. For example, CISOs employ email security, multi-factor authentication and restricted administrative access to stop any kind of threat–not just ransomware.

20% of respondents believe that a point solution for ransomware would be impractical and a "hard sell" in the business for being too threat-specific. They instead recommend a full-featured security tool for the cloud that includes ransomware protection. 14% believe that a meaningful solution must focus on both preventing ransomware and halting its expansion within any network it gains access to. 17% hold that the true solution for ransomware lies in innovating response and recovery, thereby nullifying ransomware's inherent risk.

Possible alternatives are available on the market, and cyber insurance may offer the next best solution. However, as this sector remains highly underdeveloped, many of our experts feel that it must mature substantially before it can address the full scope of ransomware's risks.

Many respondents are perplexed by the idea of a dedicated solution, given that ransomware is just one of many security risks mitigated by their multi-layered approach.

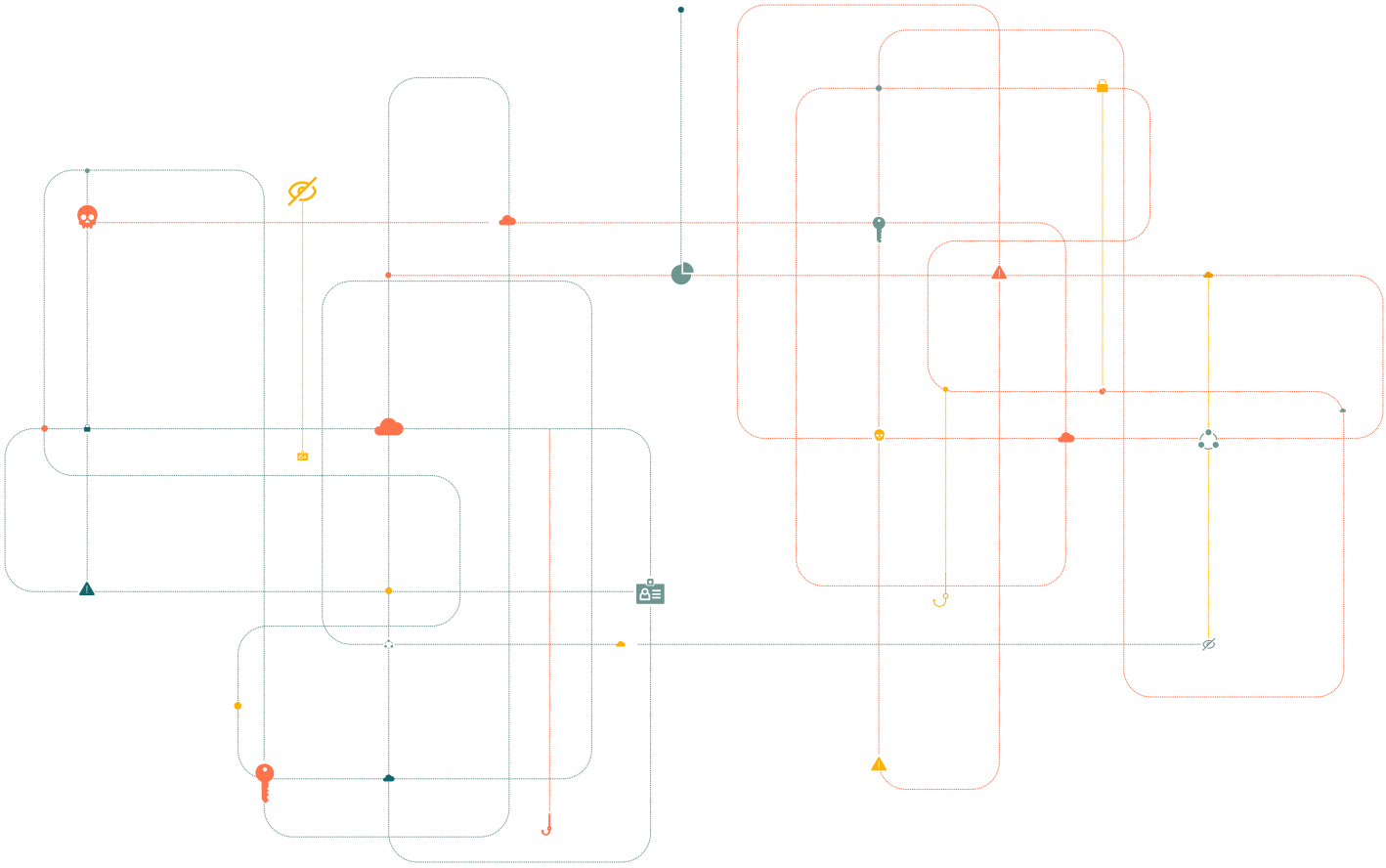
Conclusions

Ransomware is one of the cybersecurity landscape's most dynamic threats and effective means of cybercrime. As its monetization strategies continue to evolve and intensify, cybersecurity executives have no choice but to keep ahead of its risks. Current best practice demands multiple defenses to protect against ransomware, and many of our respondents doubt one solution will ever be able to cover the entire scope of its risk. Instead, they believe in utilizing a full security stack for a multi-layered approach that addresses many security concerns at once.

Without a point solution, security teams must continue to rely on the collective protection, response and recovery offered by their changing and growing security stacks. This holistic approach is necessary so long as ransomware cannot be fully prevented, though it is worth considering that perfect backup systems are not yet available, either.

As privacy continues to gain traction within C-Suite priorities, it is important to recall why victims of ransomware feel they must pay off their attackers. While many attackers pair traditional encryption with Doxware and third-party extortion that can threaten a company's perceived trustworthiness, the majority of businesses are most acutely affected by ransomware's disruption of business continuity. All affected operations are often forced to stop for at least a few days, even when the ransom is paid, given that employing decryption keys and properly restoring the entirety of stolen information are each highly complex and technical processes.

Our surveyed experts worry about what both attacks and recovery will look like once ransomware becomes more prevalent in the cloud. Housing critical operational data, from automated workflows to proprietary data, the stakes of ransomware attacks in the cloud are significant. It is thus expedient to address the budding demand for cloud-specific solutions to counter the inevitability of ransomware in the cloud.



Outreach and Contact Information

This report was compiled with Israeli cybersecurity entrepreneurs in mind. If you are an Israeli-based startup looking for guidance for seed-stage funding, we invite you to contact **Ofer Schreiber, Senior Partner,** at **ofer@ylventures.com**. We also invite you to direct any questions relating to this report to this address.

We would like to sincerely thank all of the CISOs who participated in this report. If you are an industry expert and would like to be interviewed for the next edition of the CISO Circuit, please contact **Michael Cortez, Partner,** at **michael@ylventures.com**.

Appendix

Survey Questions

1. **Have you experienced a ransomware attack?**

2. **What attack vectors are you most concerned about? Please attribute perceived level of risk for each**
   a. Malware
   b. Phishing
   c. Unpatched vulnerabilities
   d. Widespread privileged access
   e. Segmentation / zones of trust
   f. Supply chain / third-party access
   g. Insider threat

3. **When dealing with ransomware, which is a more important area of focus, prevention or response recovery? Imagine you have 10 points worth of effort to both total. How would you allocate them?**

4. **What do you currently have in place to manage ransomware risk?**
   a. Dedicated anti-ransomware
   b. Endpoint security
   c. Backup
   d. Email security
   e. Multi-factor authentication
   f. Restricted administrative access
   g. Threat intel
   h. Other

5. **Does your incident response plan have a documented, specialized ransomware recovery plan?**

6. **If you have an incident response plan, do you practice how you would manage a ransomware event?**

7. **What strategies do you use in building an effective backup and data recovery program?**
   a. Backing up client machines
   b. Mixed data storage (eg. on-prem and cloud, duplicated data etc)

8. **If your program isn't where you'd like it to be, what challenges are you facing?**

9. **How effective are these recommended best practices against ransomware? Please rank them in order of effectiveness.**
   a. Maintaining offline, encrypted backups of data and regularly testing your backups
   b. Creating, maintaining and exercising a basic cyber incident response plan and associated communications plan
   c. Conducting regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
   d. Implementing a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents.
   e. Ensuring that antivirus and antimalware software and signatures are up to date. Additionally, turning on automatic updates for both solutions.
   f. Taking into consideration the risk management and cyber hygiene practices of the third parties or managed service providers (MSPs) your organization relies on.

10. **When do you think ransomware will hit the cloud?**

11. **How will ransomware expansion into the cloud align/ clash with existing ransomware solutions and best practices?**
    a. We already feel protected in the cloud - no change needed
    b. Will need a new set of solutions
    c. Will need a new set of solutions
    d. No meaningful change possible

12. **What is the future of ransomware?**

13. **What advice do you have for founders looking to build a ransomware solution?**