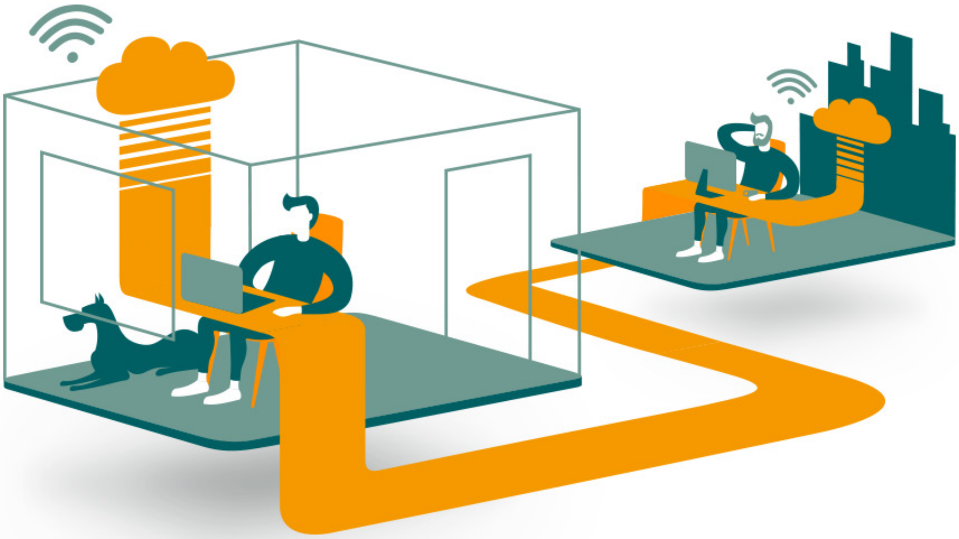
YL VENTURES
The CISO Current

The CISO Current Report

Q2, 2020



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 $270 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, CISOs and U.S.-based technology companies as advisors, prospective customers and acquirers of its portfolio businesses. The fund'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 fund is also dedicated to providing unmatched hands-on value-add support for 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 85 security professionals from leading multinationals, including Microsoft, Intuit, Zscaler, Kraft Heinz, Walmart, Netflix, Nike, Spotify, Aetna, Optiv and more. 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 continuous support across a multitude of functions throughout their life cycles. In return, network members benefit from exposure to pre-vetted Israeli cybersecurity innovations and receive direct exposure to a market second only to the U.S. in cybersecurity innovation.

Portfolio

satori
Secure Data
Access Cloud
www.satoricyber.com

cycode
Source Code Control,
Detection & Response Platform
www.cycode.com

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

VULCAN mind the gap
Continuous Vulnerability
Remediation Platform
www.vulcan.io

Hunters.
Autonomous Threat
Hunting Platform
www.hunters.ai

MEDIGATE
Securing the Internet
of Medical Things
www.medigate.io

orca security
Full Stack Cloud
Visibility Platform
www.orca.security

RIDE VISION
Predictive Vision
for Motorcycles
www.ride.vision

AXONIUS
Cybersecurity Asset
Management Platform
www.axonius.com

Acquisitions

Twistlock
Acquired by
paloalto NETWORKS

HEXADITE
Acquired by
Microsoft

FIRELAYERS
Acquired by
proofpoint.

Seculert.
Acquired by
radware

BlazeMeter
Acquired by
ca technologies

Clicktale
Exited to
Amadeus Capital Partners

AcceloWeb Click. You're there.
Acquired by
Limelight NETWORKS

UPSTREAM COMMERCE
Acquired by
Walmart

About the CISO Current

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 Current', an initiative under which we publish reports containing gathered intelligence for general use.

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

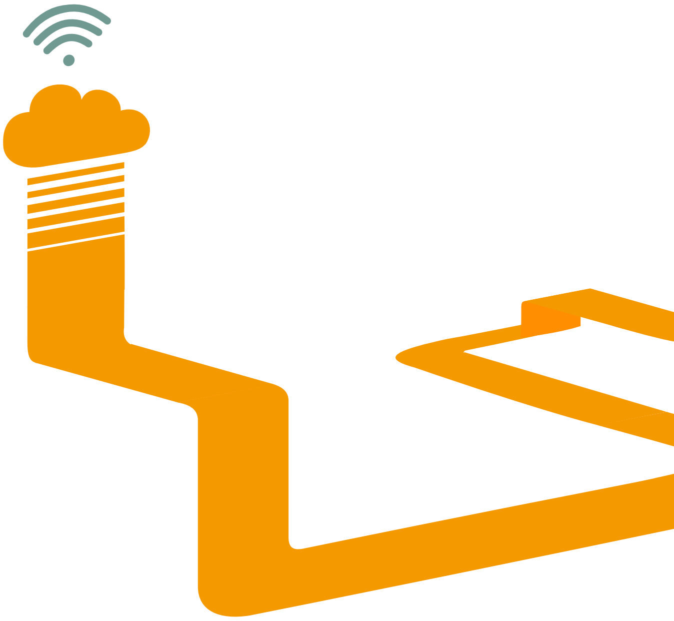


Table of Contents

Introduction

This document constitutes the fourth edition of the CISO Current report and contains data gathered from direct interviews surveying almost 50 cybersecurity executives at leading enterprises from YL Ventures' Venture Advisory Board.

The surveys were conducted in the form of short-form questionnaires and longer-form interviews. In order to obtain the most candid data possible, and with respect to the sensitive nature of some of the information shared, we anonymized the names of our respondents and their associated organizations.

Industry-wide, it is largely accepted that COVID-19 accelerated the inevitability of digital transformation and cloud migration. More specifically, it accelerated the need for security executives to integrate policies and solutions that secure remote workforces, a growing issue over the last few years that has become an immediate priority in the aftermath of recent events. Though shelter-in-place orders have gradually been lifted across the globe, it remains unclear when, if ever, the previous order will be restored. With companies such as Twitter and Google announcing more permanent company-wide remote work policies, it appears that supporting remote workforces may very well remain the status quo. To this end, many are discussing "the new normal" and endeavouring to prepare for what that may entail.

With the support of YL Ventures' CISO-in-Residence and Chief Technology Officer, our research team set out to understand how the new reality of dispersed employees, vendors, contractors and customers has impacted CISO priorities, enterprise security operations, budgets and security postures. The team further explored how the massive shift to completely remote workforces across the world has impacted enterprise acquisition and adoption of cybersecurity solutions and processes.

Our distinguished survey participants, hailing from a full spectrum of verticals and company sizes, responded to a series of questions (see Appendix) that provided meaningful insights into the cybersecurity industry's most pressing issues and promising opportunities. Chief among our findings was a heightened concern over data exfiltration due to increased phishing incidents, insider threats, third party security threats and use of personal devices, as well as the inherent vulnerabilities of downgraded controls.

The opportunity to exploit individuals that no longer operate inside well defined security perimeters has led to increased cybercrime. Reported phishing and fraud attacks have risen sharply since this outbreak began to spiral. Moreover, corporate VPNs have opened up a myriad of security vulnerabilities for enterprises that were unprepared for the unprecedented influx of workers logging in from home. All of these vulnerabilities have necessitated greater enterprise cybersecurity protection and are consequently top of mind for industry stakeholders. The deployment of additional remote work security introduced an additional layer of challenges to many of our experts by creating a new attack surface for malicious actors to exploit. This is further exacerbated by the security gaps inherent in exceptions granted to accommodate the new scale of remote work.

To these ends, there is a growing demand for seamless solutions that can demonstrate value to cybersecurity leaders quickly while supporting remote operations. This demand encompasses solutions that streamline, simplify and strengthen basic security controls, a core demand pervading the pushback against bloated security stacks. However, digital transformation brings with it new threats and concerns that add inevitable complexity to enterprise security stacks. Vendors must help cybersecurity leaders strike the right balance between addressing these new threats without exacerbating the already critical complexity and bloat they manage on a daily basis.

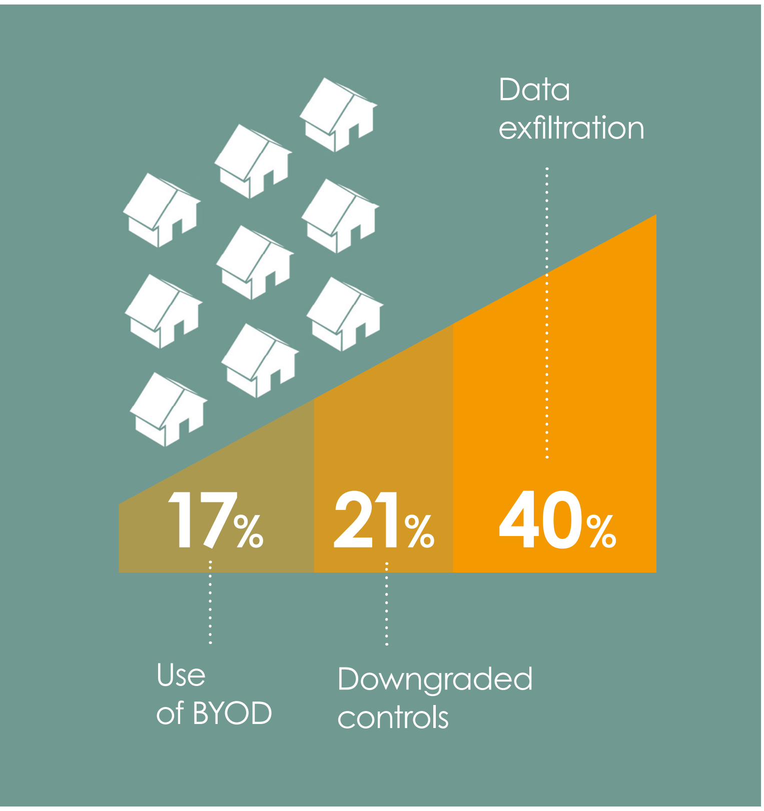
The Threat Landscape

Top Concerns for Securing a Remote Workforce

40% of the experts we consulted cited data exfiltration as their current primary concern. Meanwhile, 21% cited downgraded controls and 17% were concerned over expanded use of non-corporate-issued devices and networks for professional purposes—or "bring your own device" (BYOD).

Downgraded Controls

By necessity, some of our experts have been forced to relax their policies in the wake of the crisis. Prime examples include the extension of VPN time-outs as well as a relaxation of security measures around daily office tasks, including contract signing and printing, to enable remote productivity. This downgrade of controls raises the question of how exceptions are to be tracked and revoked to prevent exposures ripe for exploitation once they have been forgotten.



Use of BYOD

More people are using their own devices on their home networks as they shelter-in-place. This is allowing them to store and handle organizational data without running their activities through enterprise security controls that give our experts monitoring capabilities. Mobile device management has become particularly complicated as the number of devices owned per individual increases, broadening the attack surface security executives must protect. Upon distilling these vulnerabilities, the lack of visibility that has accompanied the rise in BYOD accounts for the majority of executive concern.

Data Exfiltration

With the aforementioned two factors combined, an increase in data accessed remotely and decrease in visibility have primed our experts to pay more attention to the threat of data exfiltration. The rise in cybercrime, especially phishing attacks, is only exacerbating these concerns. Our experts are also concerned about how the psychological impact of this crisis may increase the threat of insiders exfiltrating data, as well as how the paradigm shift of remote work requires a new approach to an old problem. To this latter point, our experts highlighted how sharing practices are shifting and how employees must take more ownership over their own cybersecurity postures.

The risk profile has consequently changed, which in turn affects the processes by which cybersecurity leaders must mitigate threats, track shared accounts and detect data theft across their user base. Because this issue surpasses the security gaps solved by firewalls and intrusion detection systems, some of our experts feel as though they are working blind.

Of those that cited data exfiltration as their main concern, 47% stated that it will remain so long as remote work continues at its current scale.

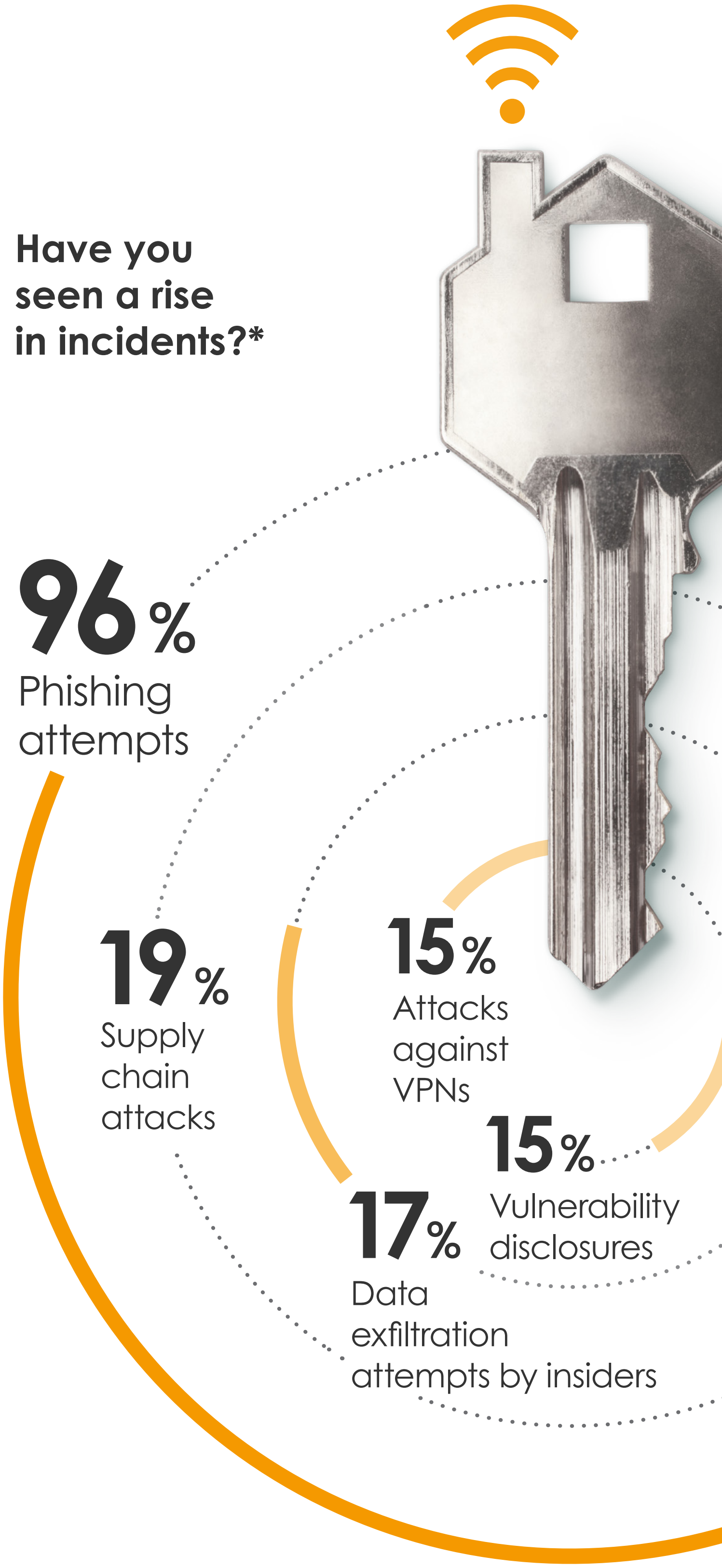
Our experts are concerned that the usage of and migration to SaaS applications will only exacerbate data exfiltration. Native security capabilities of commonly used SaaS apps have been deemed insufficient, leaving them in need of solutions that can provide more control over organizational data. A number also voiced interest in leading-edge solutions for SaaS monitoring that can provide systematic insights into stored data and the roster of those who can access it.

While some are pursuing DLP-type solutions, others conceded that they alone may not be able to prevent data loss at scale, given their inherent issues in scalability and prioritization. Many moreover brought attention to the fact that existing solutions in today's market only address already classified data. This renders DLPs inaccessible to many, as it is difficult to find talent willing to carry out the manual work around data classification, while automated solutions for data tagging, labeling and classification are not yet sufficiently advanced. Therefore, cybersecurity leaders facing these issues are primed for systems to help automatically classify the data they have and prioritize their sources.

Increased Incidents Since COVID-19

Times of crisis often see a rise in crime, and cybercrime is no exception. The fear and uncertainty of the times provide plenty of opportunity for exploitation by cybercriminals. As a result, 96% of our experts have seen a rise in phishing, 19% in supply chain attacks and 17% in data exfiltration attempts by insiders. According to 15% of our experts, attacks against VPNs and vulnerability disclosures have also increased. Overall, this data reveals that our experts are five times more concerned about external attackers than internal malicious actors.

Have you seen a rise in incidents?*



*Figures represent the percentage of respondents that saw an increase

Phishing Attempts

Phishing incidents have increased in both frequency and sophistication since the outbreak of the crisis. An age-old problem in the industry, experts currently have little options to work with outside of employee education and a select group of detection and prevention solutions.

The sophistication of the attacks is improving as cybercriminals hone in on widespread fear and anxiety surrounding the virus, as well as the infrastructural changes taking place to secure remote workers. Given the spike in VPN adoption, malicious actors are exploiting this transition with targeted phishing emails. Other targeted emails specifically seek to exploit the psychological difficulties caused by COVID-19 by posing as official bodies of health and tapping into the desire for clarity and information.

64% of our experts expressed their belief that phishing attempts will continue at higher rates so long as remote work continues to operate at its current scale.

Supply Chain Attacks

The rise in supply chain attacks have forced some of our experts to rethink how they interact with third parties—a primary source of data exfiltration and malicious activity. To these ends, some believe that providing their suppliers with corporate-sanctioned technologies may improve their enterprise's security while maintaining productivity.

Attacks Against VPNs

VPNs have gained a great deal of popularity over the years, inspiring cybercriminals to develop creative methods for exploiting their vulnerabilities, including VPN encryption key theft. VPNs represent another attack surface for our experts to secure—one that is expanding, given the need to scale them during the crisis. This has led to recent adoptions of newer architectures, such as network-centric Zero Trust Network Access solutions and application-centric Secure Access Service Edge solutions.

VPN attacks were already taking place before COVID-19, leading many of our experts to have taken early protection measures. Among them were "VPN profile cleanups", which entailed case-by-case reviews of the access required by individual workers and providing the very minimum stipulated by those assessments. This primed their environments to cope with remote work on large scales.

Vulnerability Disclosures

Our experts have seen an increase in the disclosure of vulnerabilities in devices and infrastructure. Many devices used for organizational purposes have not yet been configured or set to work in remote environments. This means that they have been left unmanaged and unpatched.

Budgeting

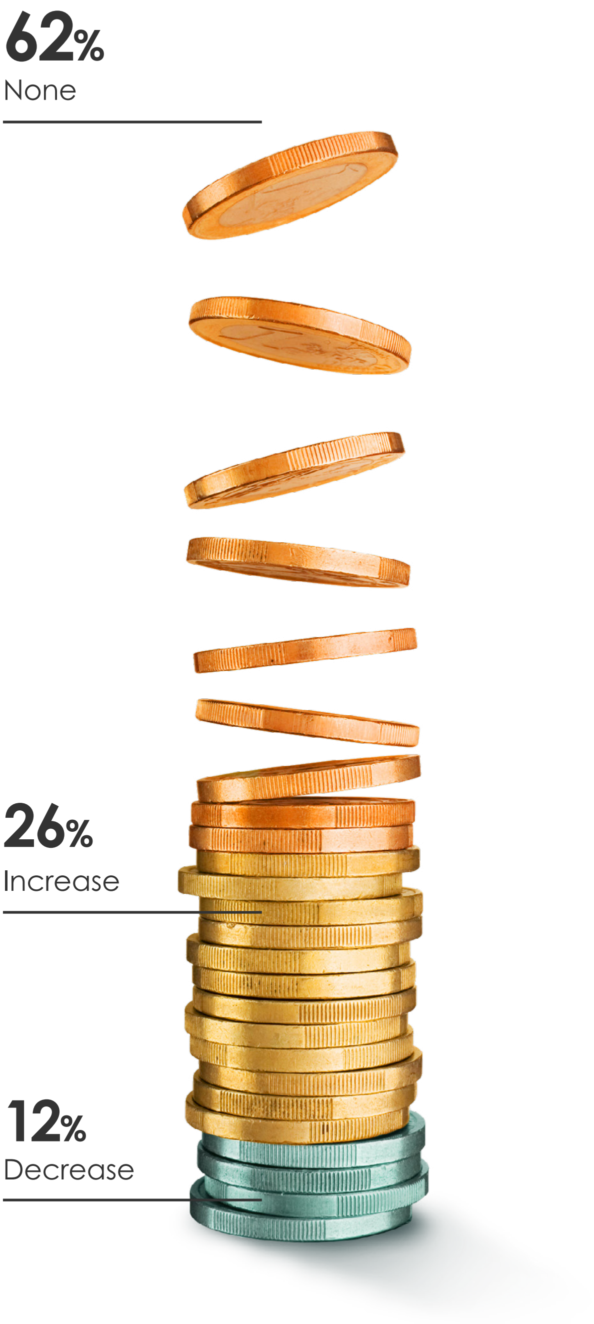
Though steadily recovering, many enterprises are remaining cautious in response to the market's volatility between February and July. This is an important contributing factor to the rise in unemployment, as enterprise budgets have been cut or frozen worldwide to enable business continuity.

However, as indicated by prior research carried out by YL Ventures, cybersecurity has achieved a new degree of appreciation among the c-level suites of many organizations. As a result, many executives hold the view that cybersecurity is a core business necessity. To this end, only 12% of our experts saw a decrease in budget, 62% saw no change or a temporary freeze and 26% actually enjoyed a budget increase to contend with the changing threatscape.

Budget increases may indicate that demand for strong cybersecurity postures will remain high in the "new normal". Many experts associate it with the acceleration of Zero Trust solutions. Though cost-scrutiny remains widely practiced, funds saved and surplus funds are being reinvested into other solutions. Some cybersecurity branches are even receiving funding out of other departmental budgets due to how closely they are tied to the organization's core business activities.

Nonetheless, market uncertainty has also led to precautionary freezing on spending, despite readily available budgetary allocations. Many cybersecurity executives admit feeling pressured to keep costs low, requiring "belt tightening" and a heavier emphasis on expenditure prioritization. This has led to project freezes on resource-intensive initiatives.

Budgetary changes



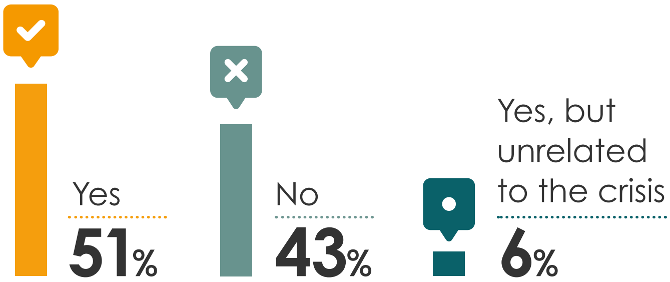
Security Posturing

Some of our experts implemented measures to manage remote workforces before the COVID-19 outbreak. Others were well ahead in their digital transformation from the outset, providing a significant advantage once shelter-in-place orders came into effect.

Acquisition of New Security Solutions

51% of our experts have acquired new technologies since the COVID-19 outbreak to accommodate remote workforces. 43% reported that they had not acquired any new solutions and 6% shared that, while they had acquired new ones, they were unrelated to recent events.

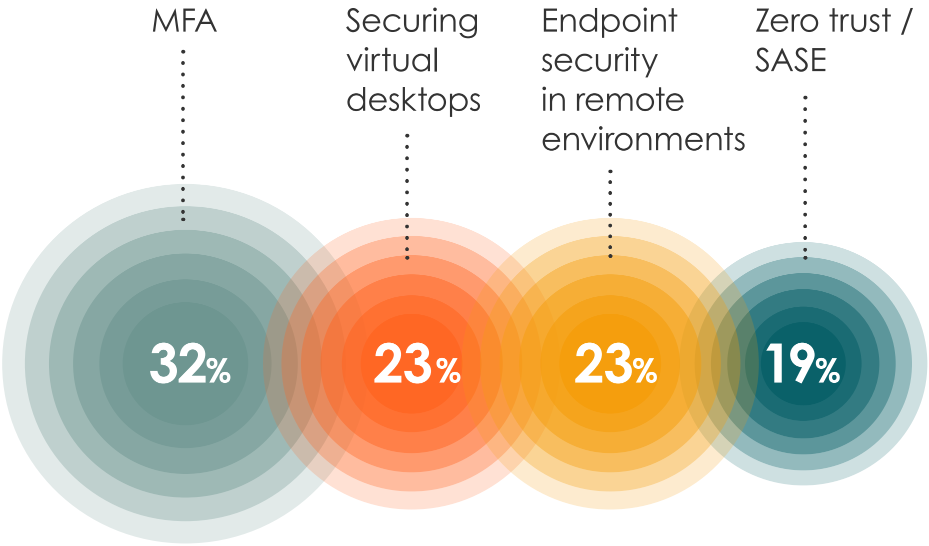
Have you acquired new security solutions?

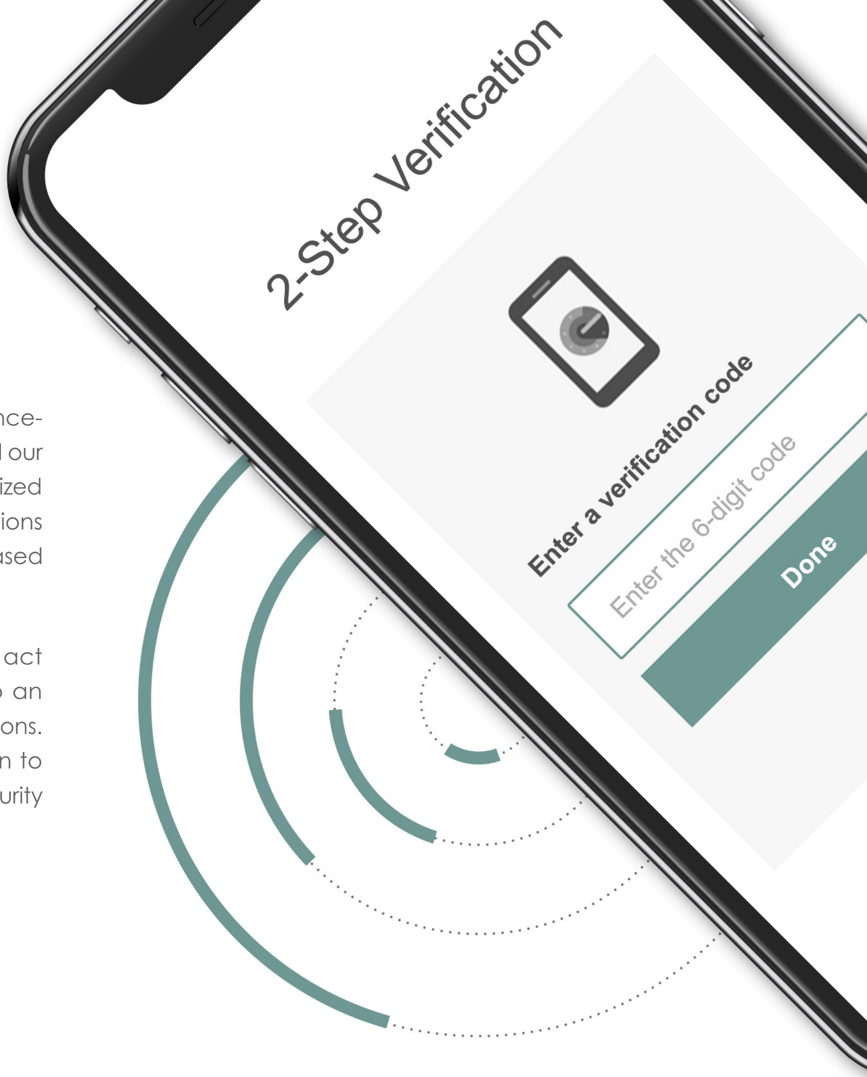


Solutions Acquired

Of the new solutions acquired, 32% addressed multi-factor authentication (MFA) while 23% respectively addressed security for virtual desktop environments and endpoint security for devices outside of corporate environments. Zero Trust and Secure Access Service Edge (SASE) made up another 19% of the solutions our experts introduced into their environments.

Which new solutions have you acquired?





Current circumstances have rendered physical presence-based authentication mechanisms moot. This has forced our experts to consider alternatives to ensure that only authorized users have remote access to corporate data, applications and devices. This has led to a dramatic rise in identity-based solutions—predominantly MFA.

The pandemic has moved cybersecurity leaders to act on their BYOD concerns more vigorously, leading to an increase in the implementation of endpoint security solutions. These implementations target corporate devices given to employees and the roll out of corporate-sanctioned security products for private devices.

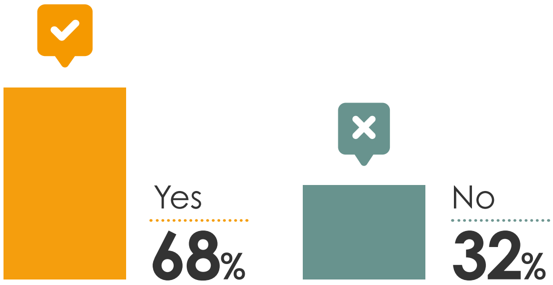
Of those citing endpoint security as one of their most pressing concerns, 21% state that endpoint security will remain so as long as remote work continues at this scale.

The need to provide the same level of security for those working at home as those in the office has accelerated the adoption of Zero Trust solutions and entrenched it into standard security practice. Our experts concede that existing VPNs provide insufficient security on their own, while perimeter-based controls fail to account for the vast majority of threats that originate from the outside. To this last point, it is worth noting that the corporate perimeter has significantly eroded over the last few years, given that network-based security controls have been rendered all but ineffective.

Adoption of New Security Policies and Processes

In order to secure scaled workforces, 68% of our experts implemented new policies and processes. 32% reported that they have not implemented any new policies and processes since the outbreak.

Have you adopted new security policies?



Policies and Processes Adopted

Of the new policies and processes adopted, 47% addressed remote onboarding, 28% introduced policy relaxation and exceptions, 26% addressed the use of BYOD and personal equipment for organizational use, and 21% secured split tunneling.

Which new policies have you adopted?

47%
Remote onboarding

28%
Policy relaxation & exceptions

26%
BYOD

21%
Split tunneling

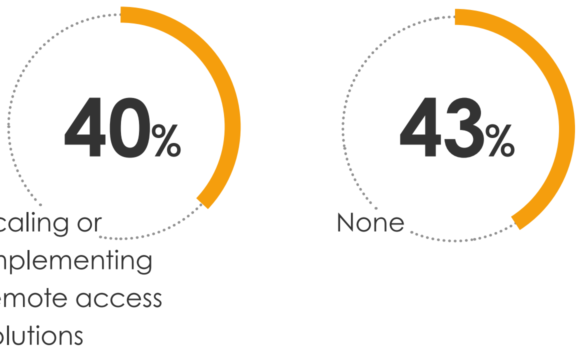
Our experts are struggling to securely onboard new employees to corporate networks, applications and users remotely. They are facing further difficulties onboarding existing employees to new VPNs, VDIs and Zero Trust solutions required to secure remote work. In cases where onboarding processes require physical presence to obtain login credentials, security personnel are now forced to issue information via less secure channels, such as personal emails. This allows attackers to leverage compromised accounts from the onset, which is very difficult to detect.

Despite the rise in phishing incidents, few experts are deploying new solutions or introducing new policies to counter them. This may indicate that current phishing solutions in place are viewed as sufficient to meet the rise in alerts and contain the threat. Conversely, efforts to secure BYOD and endpoints are taking the foreground of new solutions and policy implementation, indicating that existing solutions have been insufficient and that this concern remains top of mind. Insofar as BYOD is concerned, new policies mainly pertain to whitelisting devices.

Third Party Access

40% of our experts implemented change for third party access by scaling and implementing solutions such as VPNs, VDIs and Zero Trust, as well as MFA. In isolated cases, some even introduced remote browsers to isolate access to corporate resources. 13% implemented new types of endpoint security for third parties. The rise in third party access solutions correlates with the rise in concern over supply chain attacks, again in stark contrast to the few new solutions adopted to counter phishing attacks.

Changes to accommodate third party access

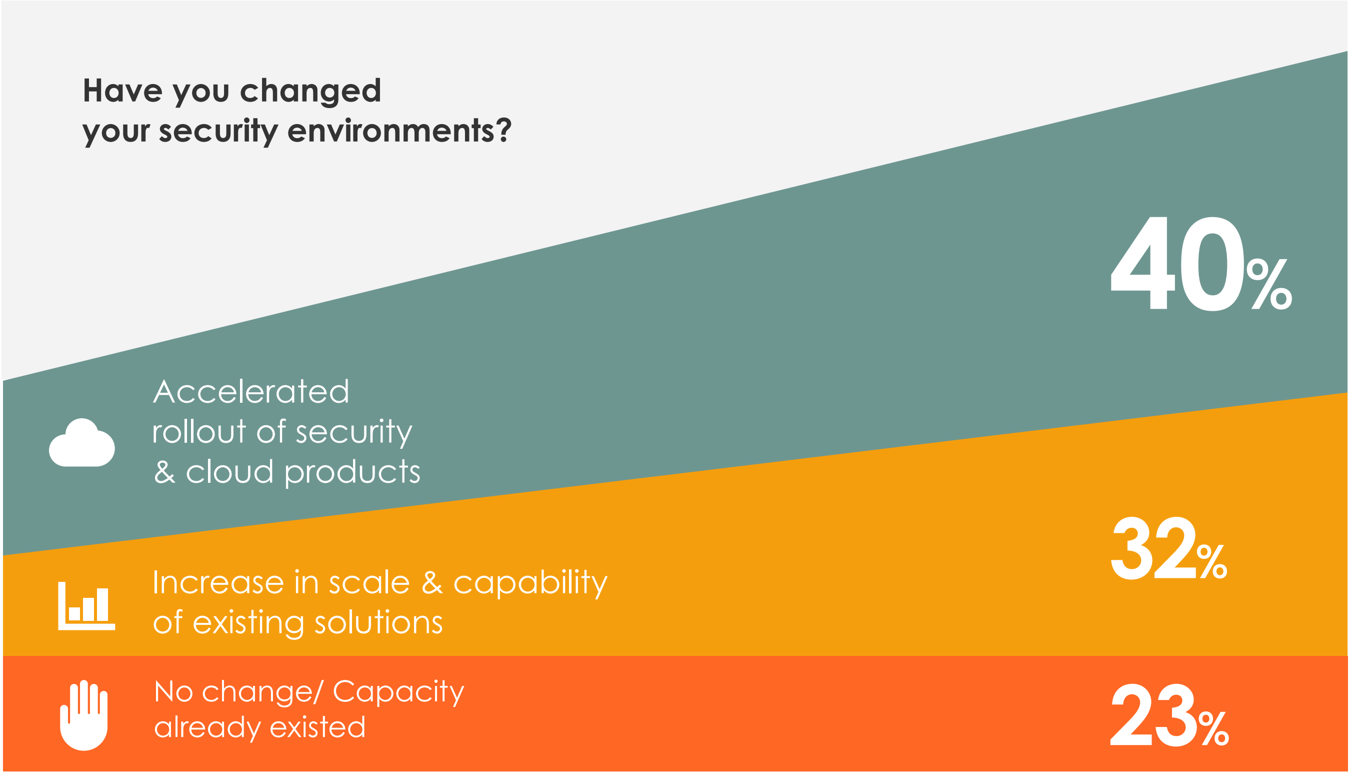


Scaling

Accommodating Scaled Remote Workforces

Many organizations already had varying degrees of remote workforce security infrastructure in place. However, only 23% of the experts we interviewed had the capacity to support the current scale of their remote workforce before the pandemic. 40% accelerated the rollout of security and cloud products. This can be explained by the fact that half of the experts surveyed implemented new security solutions—largely the rollout of authentication solutions like MFA for devices. This is also reflected in the aforementioned implementation of MFA in a third of our experts' environments. Moreover, a number of our experts also implemented solutions to provide increased visibility into their large and complex environments.

32% found themselves having to bolster the scale and capabilities of their existing solutions. This included broad assurance over the proper installation, configuration and management of solutions across all attack surfaces while increasing the availability of security products.



Solutions that Failed to Scale

Of the existing solutions our experts had in place, 23% experienced failures within their network-based controls during the crisis while another 6% of participants mentioned that remote access tools failed to scale as well.

Privacy

Privacy saw very little change throughout the crisis despite dramatic changes across operational structures and increased collection of Personally Identifiable Information (PII). However, 45% of our experts do not monitor their employee data at all. 19% of those that do claim to practice their monitoring with total transparency. 32% admitted to having no privacy controls in place.

A number of our experts are handling privacy concerns with routine assessments. These assessments survey the impact of privacy and data protection of every individual business process in their organization with the aim of minimizing the data collected and stored to support it. This ensures that only necessary data is used while the rest is deleted.

Many of our experts have also limited their endpoint monitoring to security-related events. Employees sign off on this as a condition of their employment. Some even sign separate remote working agreements upon joining. Even those with more comprehensive monitoring access still ensure clear policies with defined limitations for actions like code pushing and secret management.

The New Normal for Vendors

Given that projections for the "new normal" see no near end to largely remote workforces, the next generation of cybersecurity solutions would do well to cater to the new set of needs it produced. However, our experts are interested in built-in capabilities and warn vendors against rushing to "tack them on" for the sake of meeting this need.

Though cybersecurity executives have used this experience to introspect and bolster their security fundamentals, many are looking to further enable large-scale remote workforces and migrate to Saas if they have not already. To these ends, they are looking for positive control over their data in SaaS solutions and are particularly interested in DLP for data stored in the cloud and leading-edge cloud-SaaS monitoring. This is especially true where operational management tools are involved.

To make up for their loss in visibility, our experts are interested in new approaches to resolving their concerns over data access and management. A keen eye is being kept on solutions that leverage user-behavior analytics to alert them to anomalies and potential insider threats. Solutions that provide parity over IaaS, such as network monitoring and Privileged Access Management (PAM), are also top-of-mind.

Finally, as cybersecurity executives refocus on endpoint protection, many are realizing that their current approaches are insufficient for the threats they face in the wake of extensive remote work. Their solutions are not aligned to the cloud, necessitating solutions that provide prevention and detection models for endpoints that use cloud services.

Final Observations

Above all, this report reveals that cybersecurity executives managing remote workforces in the wake of COVID-19 are primarily preoccupied with the threat of data exfiltration. This is largely due to a significant rise in phishing attempts, insider threats, use of BYOD and third party security threats in combination with security control downgrades.

Those already in the cloud or in transition to cloud were far better prepared to secure newly remote workers than digital transformation laggards. Nonetheless, they are still in need of solutions to better protect VPNs and endpoints. Those catching up have been more prone to security control downgrades, increasing their vulnerability to both internal and external threats.

The market is primed for solutions to facilitate remote work security ahead of the new normal, which will likely see people continue to work from home well after shelter-in-place orders have been lifted. The crisis has accelerated already pressing needs in the cloud migration and digital transformation space, which still lack sufficient cybersecurity solutions.

Above all, cybersecurity leaders are most likely to embrace startups that address the threat of data exfiltration caused by the inherent vulnerabilities of dispersed workforces. The key, however, will also lie in communicating value with low-cost implementation and the potential to help CISOs streamline their stacks.

Outreach and Contact Information

This report was compiled with Israeli cybersecurity entrepreneurs in mind. If you are an Israeli-based start-up looking for guidance for seed-stage funding, we invite you to contact:

YL Ventures Partner & Head of Israel Office | Ofer Schreiber
ofer@ylventures.com

We would like to sincerely thank all of the CISOs that participated in this report. If you are an industry expert and would like to be interviewed for the next edition of the CISO Current, please contact:

YL Ventures Partner | John Brennan
john@ylventures.com

We also invite any questions relating to this report to be directed to:

YL Ventures Associate | Naama Ben Dov
naama@ylventures.com

Appendix

Survey Questions

Multiple choice questions

1. What is your top security concern as a result of employees transitioning to remote work? (Pick 1 answer)

- Use of BYOD
- Compromised home networks
- Increase in data exfiltration opportunities
- Downgrading security controls to allow remote workers
- Other:

2. What type of incidents have you detected increases in since the COVID-19 outbreak? (Pick multiple answers)

- Phishing attempts
- Vulnerability disclosures
- Data exfiltration attempts by insiders (accidental or intentional)
- Attacks against VPNs
- Supply chain attacks
- Other:

3. (Follow-on question) If you saw an increase in incidents in Q2, to what extent did they increase? (Pick 1 answer)

- <1.5x
- 1.5x
- 2x
- 2.5x
- 3x
- >3x
- Other:

4. Were you required to set up new security solutions since the COVID-19 outbreak?

- Yes
- No
- Other:

5. (Follow-on question) If so, what new security solutions were you required to set up? (Pick multiple answers)

- Zero trust / Secure Access Service Edge
- Security of SaaS
- Security of IaaS
- 2FA
- Security for Virtual Desktop environments
- Endpoint security (on corporate machines) that operates in non-corporate environments (e.g., home)
- Other

6. Were you required to set up new security policies or processes?

- Yes
- No
- N/A
- Other:

7. (Follow-on question) If so, what do these new security policies or processes address? (Pick multiple answers)

- Remote onboarding
- BYOD / Use of personal equipment for business purposes
- Password sharing policies
- DLP exceptions
- Relaxing 2FA requirements
- Split tunneling
- Approval of new software and services without completed vetting
- Printing
- Other:

8. Has your response time to events / incidents been affected?

- It hasn't
- 0-10% increase in response time
- 10-30% increase in response time
- 30-50% increase in response time
- Over 50% increase in response time
- Other:

9. How, if at all, has the security budget been affected by the new needs of the COVID-19 era?

- Budget has increased
- Budget has decreased
- Budget hasn't changed
- Other:

Open-ended questions

1. What security concerns and threats rose due to the increase in remote access?
2. How did you change your security environment / systems to allow remote work?
3. What controls have failed or not performed up to expectations due to the shift in use or remote-work?
4. How are you dealing with providing remote access to third parties (e.g.,call centers and contractors needing to access sensitive data)?
5. How are you monitoring remote workers and not infringing on the privacy of employees?
6. How, if at all, has the security budget been affected by the new needs of the COVID-19 era?