The CISO Circuit by
YL VENTURES

SaaS Security

The CISO Circuit Q3, 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 over $300 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 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 90 security professionals from leading multinationals, including Microsoft, Intuit, Zscaler, Kraft Heinz, Walmart, Netflix, Nike, Spotify, Aetna and Optiv. 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 introductions 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

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

Hunters.
Knowledge-Powered XDR
www.hunters.ai

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

MEDIGATE
Medical IoT Security and Asset Management
www.medigate.io

AXONIUS
Cybersecurity Asset Management Platform
www.axonius.com

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

RIDE VISION
Predictive Vision for Motorcycles
www.ride.vision

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 Circuit

This edition, we are thrilled to introduce the 'CISO Circuit', the new nomenclature of our cybersecurity research and reporting initiative. This transition aims to better convey our mission to foster energizing connections between the cybersecurity ecosystem's various players and speaks to the multi-directional feedback that drives this industry's innovation forward.

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', now '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 a useful resource for aspiring cybersecurity entrepreneurs and the rest of the cybersecurity community.

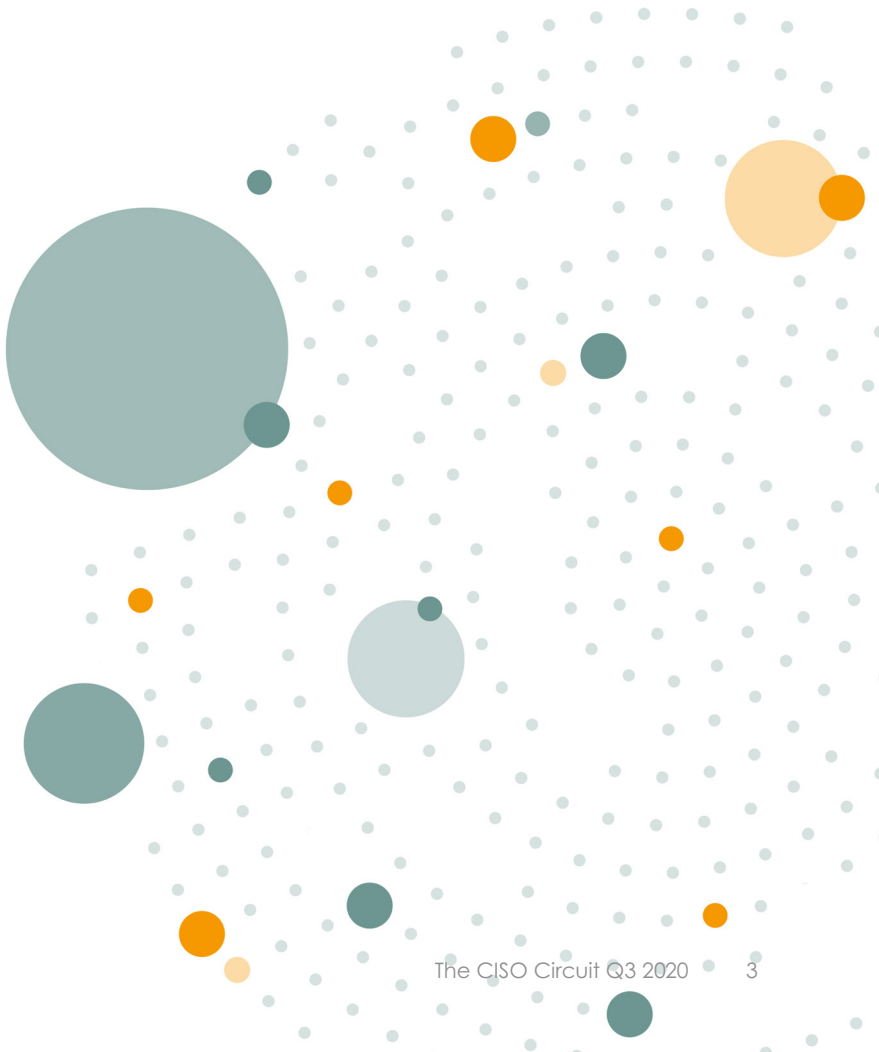


Table of Contents

Introduction

This document constitutes the fifth edition of the CISO Current report, hereby known as the 'CISO Circuit', and contains data gathered from direct interviews surveying 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.

This quarter, with the support of YL Ventures' CISO-in-Residence and Chief Technology Officer, our research team set out to understand the cybersecurity challenges posed by the rise of Software-as-a-Service (SaaS) solutions. Over the course of 50 interviews, we asked our distinguished survey participants, hailing from a diverse spectrum of verticals and company sizes, to respond to a series of questions (see Appendix) on their most pressing SaaS security-related concerns, strategies and needs.

SaaS solution adoption by enterprises of all sizes and industries is a natural corollary of their ongoing migration to the cloud. Many are drawn to the ease-of-use, scalability and productivity offered by SaaS solutions despite the known risks that accompany them. In the wake of COVID-19, many have been forced into SaaS adoption following wholesale transitions to remote workforces. Both trends have led to an unprecedented reliance on SaaS that, paired with a surge in cybersecurity attacks over the last six months, has underscored the serious threats posed by its inherent vulnerabilities. This has consequently generated demand for meaningful SaaS security solutions that the cybersecurity industry has yet to meet—let alone offer concerted best practices for CISOs to employ.

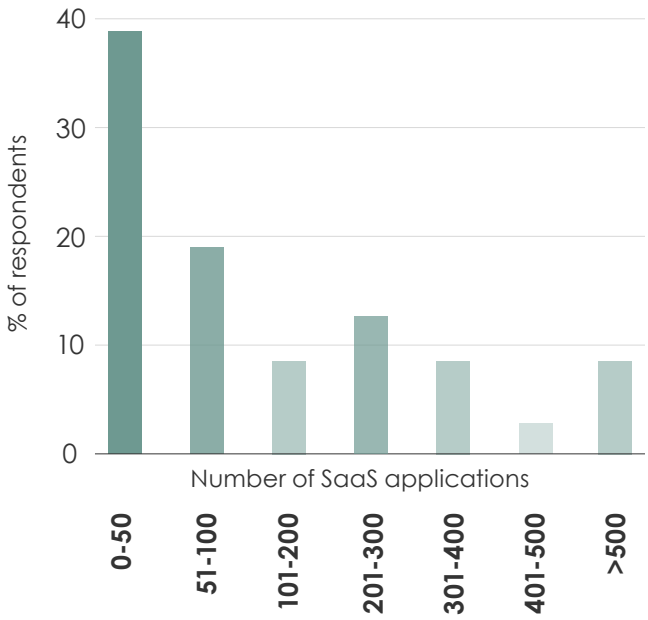
SaaS in Enterprise Environments

The majority (61%) of our survey respondents leverage over 50 SaaS applications in their enterprise environments while 43% leverage over 100 Saas applications.

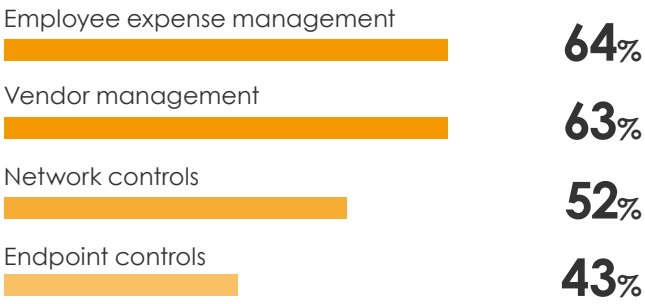
40% of all respondents claimed that 96% of SaaS applications were approved, while 43% still believed that they had authorized the majority of them. 2% intentionally abstained from putting any authorization measures in place. Most conceded to a high likelihood of unknown or unauthorized SaaS in their environments.

Of the controls available to them, the majority (64% and 63%) of our respondents utilize vendor management and employee expense management controls to provide visibility over the SaaS in their respective environments. The latter involves tracking SaaS-related billing from financial departments to create or complete an inventory of SaaS applications for security purposes. 52% responded that they use network controls while 43% use endpoint controls. In certain instances, CISOs have also been reported to monitor employee registration emails for SaaS vendors.

How many known SaaS applications are in your organization?



Which controls provide visibility over SaaS in your environments?



Of the controls available to them, the majority of our respondents utilize vendor management and employee expense management controls to provide visibility over the SaaS in their respective environments.

SaaS Adoption

SaaS adoption has risen sharply in recent years. According to the Ponemon Institute's 2019 study on Global Cloud Data Security Study, 91% of organizations reportedly used SaaS solutions in 2019.[1] To date, SaaS spending exceeds IaaS spending by an average factor of two. A Gartner release in April 2019 projected $110.5 billion in worldwide revenue of SaaS applications in 2020.[2] The same report also projected that SaaS applications will soon grow into the largest segment of general public cloud services. In fact, SaaS usage is so pervasive that many business applications are transitioning to SaaS-only delivery.

Cybersecurity executives remain skeptical over the current SaaS capabilities of network and endpoint controls, leaving them to more heavily rely on non-security tools and limiting their security posture.

Contending with largely ineffective controls to track SaaS solutions across environments and quantify their risks, CISOs find themselves plagued by "unknown unknowns".

Visibility

Out of our survey respondents, 63% listed vendor management or billing controls as their main means to a semblance of visibility. Cybersecurity executives remain skeptical over the current SaaS capabilities of network and endpoint controls, leaving them to more heavily rely on non-security tools and limiting their security posture. This has generated a demand for more reliable security-oriented SaaS visibility controls.

Against the backdrop of rising SaaS adoption, our survey respondents shared how often their hands were tied when interacting with new SaaS vendors. Many celebrate the mere implementation of Single Sign On (SSO) as a victory and lament penetration test authorizations as a distant fantasy.

The rapid adoption of SaaS compounds growing visibility concerns and frustrating inter-departmental dynamics. Many of these SaaS subscriptions cannot be attributed to a single billing owner or manager, and some continue to hold corporate data despite their lack of use. Moreover, employees seeking immediate productivity often bypass potential security approval bottlenecks to stealthily add shadow SaaS solutions to enterprise environments. Growing concern over privacy compliance introduces an additional point of tension and incentive to follow the shadow route.

As a result, many security teams have lost control over where corporate data sits. Contending with largely ineffective controls to track SaaS solutions across environments and quantify their risks, CISOs find themselves plagued by "unknown unknowns". Given that every connection to a SaaS application represents a growing attack surface, this disadvantage puts enterprises at very high risk.

[1] The Ponemon Institute, "Protecting Data In The Cloud 2019 Thales Cloud Security Study". White paper. 2019.

[2] Gartner, "Forecast: Public Cloud Services, Worldwide, 2016-2022, 4Q18 Update". Report. 2019.

SaaS Security Solutions

100% of the experts we consulted utilize identity and access management (IAM) or SSO to secure supporting SaaS. Meanwhile, 73% rely on native security capabilities, 41% on CASB and 20% on internally-built proprietary solutions.

73% rely on native security capabilities, 41% on CASB and 20% on internally-built proprietary solutions.

IAM and SSO

Our survey overwhelmingly established IAM and SSO as baseline enterprise SaaS security capabilities, with 100% of respondents utilizing them. However, our respondents were quick to highlight that many SaaS solutions fail to support SSO integrations, while many others only offer it for an additional fee or as part of a "bundle" with less desirable features. Colloquially, this is referred to as the "SSO Tax".

The "SSO Tax" is growing increasingly controversial to cybersecurity customers as SaaS vendors are responsible for introducing many new risks to enterprise environments. Our respondents insisted that SaaS vendors must share responsibility for this risk, claiming the premium counterproductive to all parties involved. Many moreover feel that this additional cost contradicts vendor claims about prioritizing customer data security.

The "SSO Tax" is growing increasingly controversial to cybersecurity customers, as SaaS vendors are responsible for introducing many new risks to enterprise environments.

CASB

This edition's respondents held mixed opinions over Cloud Access Security Brokers, or CASBs—the market's first solution addressing visibility and data security in SaaS applications. To date, the CASB market has exhibited little urgency to evaluate SaaS native security settings and permissions management. Our experts were quick to highlight the current CASB market's lack of appropriate granularity, transparency, analysis, authorization management and fail safes. Many tried and rejected CASB solutions after struggling with latency issues and discovering that they provided insufficient value when paired with large datastores.

Native Tools

Our survey findings also underscore a need for more native SaaS security offerings. To date, and with few exceptions, only the largest SaaS vendors (for example G-Suite, Office 365 and Salesforce) boast their own full stack of native security tools. Others, despite large customer bases, tend to lack key enterprise-grade features—such as data leak prevention, authorization capabilities or default configurations—that account for cybersecurity best practice. Our respondents further added that the availability of more robust native features directly impacted their preference for one solution over another.

Budgeting for SaaS Security

The overwhelming majority of experts we surveyed do not manage a dedicated budget line for SaaS security, highlighting its nascency as a field. They noted that SaaS security spend is often pulled from other budgetary allocations, including overall SaaS spend, human capital and cloud allocations. Some survey respondents enjoy a budget line for CASBs.

Top security concerns about SaaS usage

When asked why their SaaS kept them up at night, 82% of our experts cited managing access and permissions as their top SaaS usage security concerns, while 80% cited the prevention of data loss and 49% discussed the prevention and remediation of misconfigurations.

Access Management

Access management remains top of mind for our experts, who regard IAM and SSO as baseline SaaS security capabilities. The sudden influx of remote workers and need for flexible accessibility to workplace resources following COVID-19 has moreover rendered user-level access and credentials the only true set controls on SaaS. A growing number of CISOs are looking to centralize the management of these controls in a single tool that enables just-in-time authorization.

Data Leaks

Security professionals widely agree that data leaks and breaches comprise the most serious of SaaS security threats. Our respondents leverage two types of CASB deployments to prevent this: backend APIs that crawl for data leaks and proxies that can serve as a chokepoint for managing traffic. However, the cost and reported latency of CASBs often outweigh these perceived gains.

Top 3 SaaS usage security concerns

82% Managing access & permissions

80% Preventing data loss

49% Preventing & fixing misconfigurations

Misconfigurations

Misconfigurations also remain top of mind for cybersecurity executives, who remain largely responsible for setting and maintaining secure configurations. Many of our respondents voiced the need to reassess the shared responsibility model with SaaS vendors, arguing that solutions should be secure by default. However, they conceded that this may not withstand the market standard of flexibility, ease of use and expediency of business processes, which can be hindered by default security configurations. Unfortunately, this places the burden of further unwelcome risk on consumers.

Many of our respondents voiced the need to reassess the shared responsibility model with SaaS vendors, arguing that solutions should be secure by default.

This has led to the rise of SaaS Security Posture Management (SSPM), tools that continuously assess SaaS security risks and manage the security posture of SaaS applications.[3] Core capabilities include reporting the configuration of native SaaS security settings and offering suggestions for configuration improvements to reduce risk. Optional capabilities include automatic adjustment and reconfiguration to suit updated industry frameworks.

Top Unauthorized SaaS Security Concerns

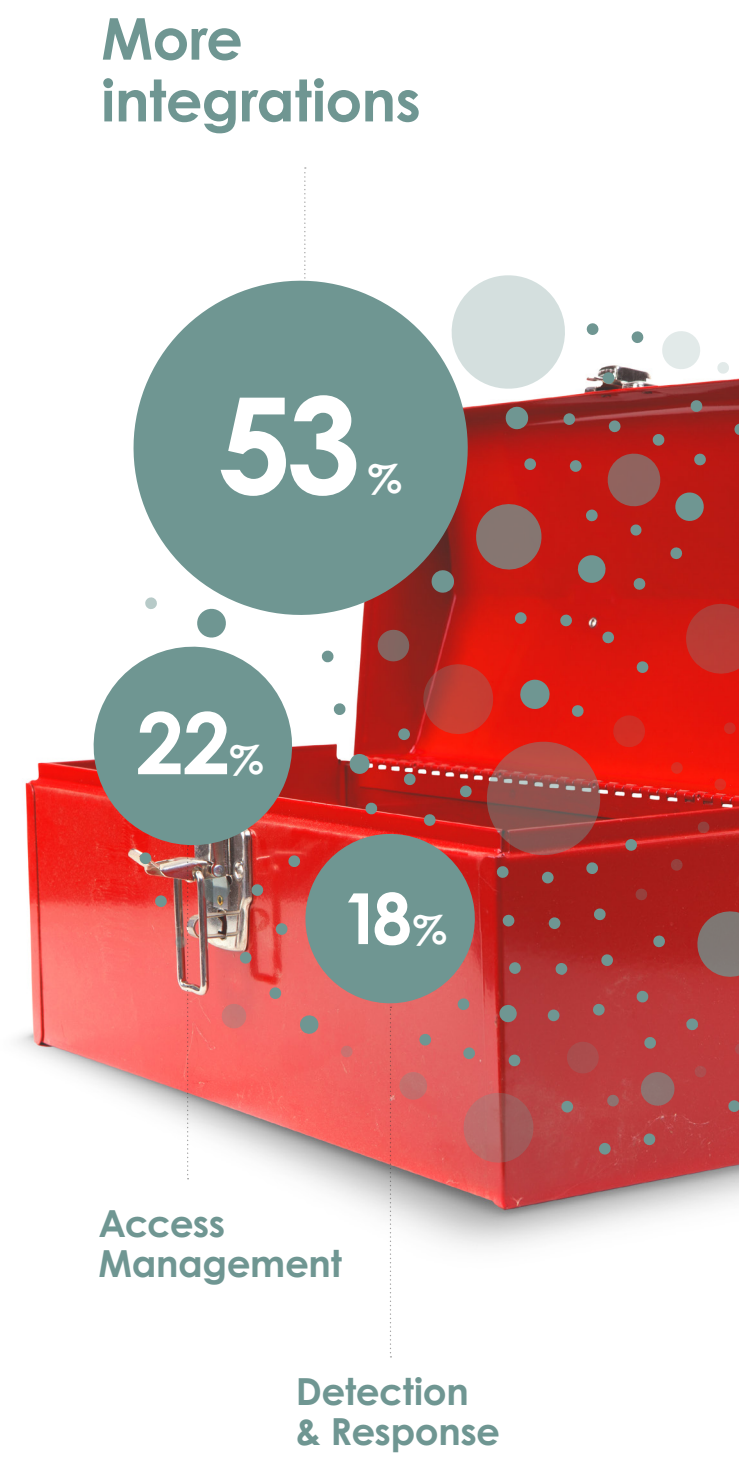
Our cybersecurity experts cited data leakage and access management among their chief concerns around unregulated SaaS. However, concerns over compliance, reputation and customer trust consistently superseded them.

The risk of non-compliance is indeed high. Enterprise employees can quite easily upload customer information consisting of personally identifiable information (PII) to an unknown SaaS—in clear violation of regulations like GDPR and CCPA—and security executives and privacy officers cannot prevent what they cannot see. In the meantime, some of our experts are leveraging GDPR-required data mapping to help prevent data leaks from unauthorized SaaS applications as well.

[3] Gartner, "Hype Cycle for Cloud Security, 2020". Report. 2020.

Capabilities Missing from SaaS Security Vendors

Among the capabilities felt most critically missing from existing SaaS security vendors, a strong majority (53%) of our experts responded with integrations, while 22% responded with access management and 18% with detection and response.



SaaS-Security Integrability for Visibility

SaaS vendors holding critical enterprise information do not provide sufficiently robust APIs for integrations with existing SaaS security solutions. The lack of extensive APIs limits customer ability to clearly understand where their data sits, how it behaves and the risks it faces. It further limits its ability to monitor employees activity and usage. This was found to be the case for both third party security solutions, which strive to connect to SaaS solutions in order to attain sufficient visibility into the security posture of SaaS-based data, as well as for internally-built solutions.

SaaS control remains elusive for even the most conscientious of enterprises. While popular SaaS applications present useful configurable security controls, many are difficult to discover and measure effectively.[4] However, this remains unimportant while existing SaaS fails to integrate with other solutions. Our respondents repeatedly alluded to a "single pane of glass" in this context with good reason—they require a single source of truth to inform their entire SaaS security posture. This single source should ideally include all security configurations and SaaS-vendor with normalized and filtered views.

This would also require better SaaS-to-SaaS integrations in order to provide a clearer picture of enterprise SaaS environments, activities and events. The data generated by a variety of SaaS applications can ultimately produce better insights than that generated by a single SaaS. It would also help address the need to track data "spillage" from one SaaS to another.

[4] Gartner, "Hype Cycle for Cloud Security, 2020". Report. 2020.

Our respondents repeatedly alluded to a "single pane of glass" in this context with good reason—they require a single source of truth to inform their entire SaaS security posture.

SaaS-to-SaaS Integrability for Access Management

Security executives are also prioritizing SaaS security solutions that can readily alleviate their access management frustrations. This would require the inclusion of dedicated controls around authorization, especially just-in-time authorization. Some advisors have built their own authorization solutions, some of which have even been open-sourced.

Detection & Response

Emerging vendors refer to detection and response capabilities primarily within the context of SaaS as "cloud detection and response (CDR)". CDR encompasses the approach to SaaS security that prevents access exploitation, account compromise and insider threats. The number of SaaS-native attacks rising in proportion to growing SaaS solution adoption has rendered detection and response capabilities fundamentally essential. CDRs provide insights, visibility and alerts around risks and threats through the continuous collection, normalization and analysis of configurations, SaaS activity, accounts and privileges. In the absence of similar offerings by CASBs, our cybersecurity experts are turning to this potential alternative for SaaS security instead.

SaaS Security Solution Prioritization

We asked our respondents to select the most optimal solution between the following two hypotheticals:

First, an in-depth solution that would only secure a small number of their organization's most crucial SaaS; second, a solution that would provide reasonable security coverage over the majority of their SaaS. There was little variance between the two responses, as 51% selected the focused solution while 49% opted for broader protection.

51%

In-depth security for a limited number of crucial SaaS

49%

Reasonable security over many SaaS

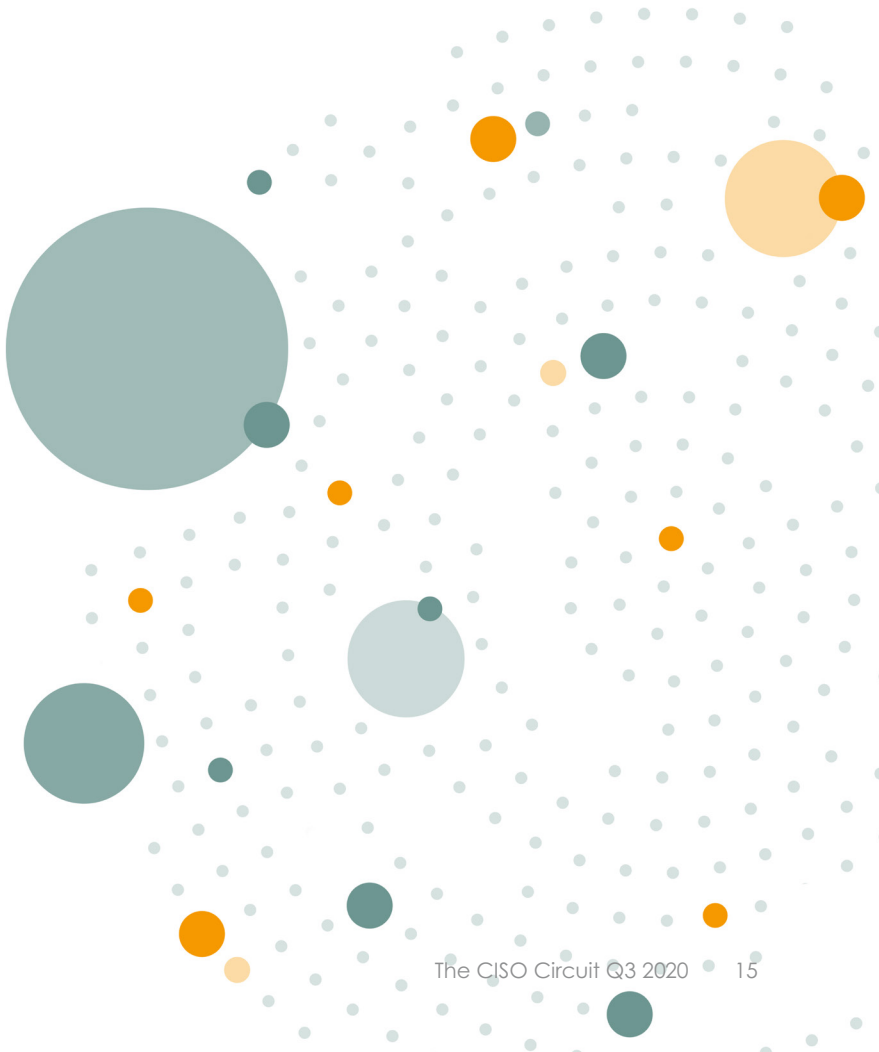
The responses to this question strongly correlate with the amount of SaaS in an organization and the variance indicates nearly equal support for either hypothetical. The more mature and SaaS-heavy the organization, the more strongly its CISO was inclined towards broader protection—even at the expense of a more in-depth security posture. Our research leads us to believe that numbers will increasingly skew towards this response in the coming years as SaaS adoption skyrockets.

As organizations continue to deploy more SaaS, the need to attain baseline visibility into their environments, and where their data sits, will take precedence over in-depth mechanisms. Ultimately, many of our advisors voiced a pressing need for both. In time, we may either see the emergence of two separate classes of SaaS security solutions to meet these respective needs or the maturation of an initially broad-protection market that comes to embrace more extensive security solutions like SaaS detection and response.

Final Observations

SaaS security is a growing unmet market following the increase in SaaS adoption to meet the demands of the 'New Normal'. Cybersecurity executives are keen to adopt a common layer of security across all of their SaaS applications to mitigate their increasingly widespread enterprise SaaS security gaps. Neither native nor incumbent third party tools currently provide sufficient or broad enough protection and visibility to do so. Enterprise SaaS security postures will remain vulnerable until security and privacy teams can enjoy visibility into all SaaS across their organizational environments.

Unclaimed and blurred SaaS security responsibility models are putting enterprises in further danger of security and privacy violations. Comprehensive security cannot exist until more SaaS vendors generate robust APIs for third party integrations. Robust APIs are an excellent way by which SaaS vendors can mitigate this vulnerability and demonstrate their commitment to security. Further, entrepreneurs would do well to innovate and rethink how to provide more expansive security, and in time, more in-depth security into SaaS.



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 Circuit, 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

1. How many SaaS solutions are used by your organization that you know of?
2. How many of these SaaS solutions are actually authorized for use?
3. What type of solutions do you have in place to secure SaaS?
4. How many of your SaaS solutions are protected by the security products mentioned?
5. What types of controls do you leverage to gain visibility into what SaaS is being used in your environment?
6. What percentage of your organization's overall SaaS spend is dedicated to SaaS security?
7. What are the top three most important concerns for you in securing SaaS applications?
8. What are your top concerns relating to the usage of unregulated/unapproved SaaS?
9. What capabilities are currently missing in existing SaaS security solutions? What capabilities would you like to see included in an ideal SaaS security solution?
10. What kind of SaaS security solution would you prioritize?
    a. An in-depth security solution for a limited set of your most crucial SaaS applications.
    b. A security solution that provides reasonable (albeit not in-depth) security over a large amount of SaaS apps.