START-UP NATION CENTRAL:
FINDER INSIGHTS SERIES

ISRAEL'S CYBERSECURITY INDUSTRY IN 2018

START-UP NATION CENTRAL

Nir Falevich
Cybersecurity Sector Lead,
Start-Up Nation Central

EXECUTIVE SUMMARY

By now, it is commonly understood that there is little safety and security in today's hyper-connected world. Nations and businesses are aware that cyber threats are here to stay, likely to intensify, and are not merely a technological problem waiting to be solved. These threats affect almost all aspects of life and business. This year witnessed the disclosure of several severe vulnerabilities and data breaches. Cyber criminals have become more professional, and are utilizing advanced hacking techniques by shifting to targeted attacks, and acting as business-like or military-like entities.

As defenders deal with the ever-changing landscape of threats, they eagerly seek innovative solutions that will keep them one step ahead. In 2018, Israel's Cybersecurity sector solidified its position as a global center of innovation. Israeli companies continued to demonstrate excellence in identifying new challenges and threats facing the world and developing new solutions to address them. Investors from all over the world are increasingly showing confidence in the local industry: 2018 ended with $1.19Bn of investments in Israeli companies, a 47% increase from 2017. According to the preliminary numbers, it constitutes almost 20% of the global VC investments in Cybersecurity.

The year saw more early and late stage investment deals, with an increased participation of non-Israeli investors. The growth of the cybersecurity industry can also be seen through the increase of 13% in number of employees, and of 12% in total annual revenue reported by the local industry, between 2016-2017.

In 2018 the IoT Security segment continued to grow, with many new start-ups and investments. The Data Protection and Privacy subsector was the fastest growing subsector, in light of the General Data Protection Regulation (GDPR) and countless large data breaches over the past few years.

Start-Up Nation Central is proud to present its annual Cybersecurity report for 2019, which offers a comprehensive and up-to-date analysis of the state of the Israeli Cybersecurity ecosystem and its trends. It reviews the major global developments in 2018, and analyzes the performance and activity of Cybersecurity companies in Israel, including by subsector. We utilize the data we collect on the Israeli Cybersecurity industry, much of which is displayed in Start-Up Nation Finder.[1]

1 Start-Up Nation Finder is the largest and most up-to-date innovation discovery platform of Israeli companies, R&D centers, investors and academics, and provides accurate information on more than 6,100 companies across dozens of industries.

THE GLOBAL SCOPE

2018 will not be remembered for any unique mega-incident, such as the "NotPetia" and "WannaCry" ransomware campaigns of 2017, or the Equifax data breach. However, many events did remind us how prevalent cyber risk is in our modern life. Just as 2018 began, the world discovered a new class of security vulnerabilities called speculative execution attacks, affecting any device with some of the most common CPUs in the market. This family of vulnerabilities, among them Spectre, Meltdown and Foreshadow, could potentially be used to steal sensitive information stored inside personal computers or third-party clouds, putting at risk any desktop, laptop, smartphone and data centers, with this, common, yet vulnerable, CPU hardware.[2]

2018 may also be remembered as the year when citizens in countries around the world began to be much more vocal about their digital privacy, as vendors collect, analyze, and monetize more personal data on their customers than ever before. This extensive data collection puts our personal sensitive information at risk of cyber attacks, particularly since in most cases there is a lack of transparency as to what vendors do with our data, and how they safeguard it, if at all.

Stolen data could be harmful, whether used for fraudulent and criminal activity, for profit, or for political or terrorist motives. In March 2018 it was revealed how Cambridge Analytica harvested private information from the Facebook profiles of more than 50 million users without their permission, to influence public opinion during President Trump's election campaign. The story led to a decline in Facebook's stock price and calls for tighter regulation of tech companies' use of data. In parallel to the heated public debate, 2018 also saw large-scale data breaches, such as the theft of Marriott's data on 500M guests, and that of Cathay Pacific's data on 9.4M customers (leading to a 6.5% drop in its market value after the disclosure). British Airways and Delta Air Lines also experienced the loss of hundreds of thousands of payment records during 2018. These are only part of a very long list of incidents of compromised consumer data during 2018, including Under Armour's MyFitnessPal, Quora, and MyHeritage, among others.

All these episodes lead us to question whether enterprises and online services are doing enough to keep our personal information safe. Although the General Data Protection Regulation (GDPR) went into effect in May 2018, the EU has not yet exercised its new powers. The immediate effect was a surge in reported breaches during 2018, which may imply that the new regulation did have an effect on how enterprises see themselves as liable in the handling of sensitive data. It will be interesting to see what happens when enterprises start receiving fines, which could be up to 4% of their annual sales, according to the GDPR.

There were some very interesting developments in the state of cyber-crime during the past year. First of all, the distinction between criminal and adversary nation-state activity in the cyber domain has become increasingly blurred, as state-sponsored and criminal hacking teams, with mixed financial and geopolitical motivations, share the same tools, capabilities, and even victims.[3] Attacks have become better targeted and more sophisticated than ever before, which has made them far more harmful.

Troublesome ransomware campaigns also showed their full and devastating potential when used in a targeted fashion rather than indiscriminately: During 2018 more than 60 organizations, mainly in the U.S., were compromised by the SamSam ransomware group, disrupting critical systems' operations of public institutions and healthcare services. The City of Atlanta was deeply disrupted during a ransomware attack in March 2018 and was unable to deliver basic services. Estimations are that the attack resulted in damages of $30M, while the cost of recovery exceeded $9M. Later that year, two Iranians were charged with running this campaign by the FBI.

In addition to this, it was revealed that another devastating targeted attack was experienced by a Saudi petrochemical plant, with the aim of "sabotaging the firm's operations and triggering an explosion"[4]. It was later revealed by FireEye researchers that much of the effort and coordination of the attack originated from within a state-owned Russian scientific institute.[5]

There was a significant decrease in the number of ransomware families and samples in 2018 as a whole,[6] after the 2017 Ransomware Rush. One explanation for the decrease in Ransomware popularity is that criminals have adopted a more lucrative business model – Cryptojacking. Cryptojacking is the method of using dedicated malware and webpage scripts to utilize victims' computing power for unauthorized "mining" of crypto assets, which allows attackers to remain undetected for long periods. According to a report by McAfee[7], the use of Cryptomining malware (which is the most popular method for crypto-jacking) has grown by more than 4000% in the past year. However it is not only malware: cyber-criminals take advantage of stolen credentials for cloud services that install cryptomining bots over cloud instances, and spread malicious docker images, as well as secretly mining cryptocurrency from unknowing victims.[8] Attackers also turn low-CPU devices (such as routers and IoT devices) into miners, utilizing a very large number of these unprotected devices.

---

2 For more information regarding speculative execution attacks, visit Meltdown and Spectre, and Foreshadow.
3 2018 CrowdStrike® Global Threat Report, CrowdStrike (2018).
4 A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try, The New York Times.
5 Hack of Saudi Petrochemical Plant Was Coordinated From Russian Institute, The New York Times.
6 McAfee Threats Report: December 2018, McAfee (2018), p.8.
7 Ibid, p.10.
8 Cryptojacking invades cloud. How modern containerization trend is exploited by attackers, Kromtech Security Center (2018).

The direct harm caused by cryptojacking activity is much lower than traditional ransomware, which encrypts data and sometimes deletes it. Instead it causes higher electrical bills and expenditure on cloud services, and decreases the productivity of computer equipment. More importantly, it means that the attackers have a presence and control over the network and sensitive assets of an enterprise, pointing out the flaws of current security arrangements which could result in far more devastating outcomes in the future.[9]

Cyber defenders in 2018 have had to deal with this landscape of ever-changing threats, which are growing ever more challenging. Many of the Cybersecurity vendors have developed various families of solutions based on artificial intelligence and machine learning, from identifying unknown attacks and vulnerabilities, to security operations and risk assessment. However, AI also has the potential to attack, and in the future we are likely to witness the widespread use of AI by cybercriminals, making attacks more harmful, and harder to detect. Another major trend is the movement of security tools and solutions to the cloud. For more than a decade cloud services were increasingly adopted for efficiency and new opportunities in IT management and software development. Over the past few years we have seen that security professionals also perceive the cloud as an opportunity for risk mitigation. By using security products as-a-service, or by designing cloud native applications and IT architecture, security teams are able to better mitigate and manage cybersecurity risk.[10]

Cybersecurity professionals must face an increasing number of challenges including:

- The widening shortage of Cybersecurity talent, which puts organizations at risk of not meeting the security challenges they currently face.[11]
- The uncertainty and complexity of regulation and compliance.
- Business growth and innovation sometimes conflicts with security requirements, which can result in security teams inhibiting product development and digital transformation.
- Ongoing patching and vulnerability management.
- Risks involved in third-party vendors and supply-chain.
- The growing use of unsecured IoT and connected devices.
- Perimeter-less enterprise networks in the era of hybrid cloud strategy and employees working remotely.

CISOs and other security decision makers are overwhelmed not only by the amount of issues to resolve, but also by the number of security vendors in the market. This raises the bar for all vendors, especially the traditional players, and forces them to create innovative next-generation security solutions. In turn, this creates a very strong incentive for enterprises and enterprise-class[12] security vendors to collaborate and incorporate innovative technology developed by start-ups. New players that enter this industry are creating new families of solutions (e.g., Endpoint Detection and Response, Software-Defined Perimeters, Breach and Attack Simulation, Security for blockchain and cryptocurrencies). These start ups are usually niche players, often targeting either a specific problem or a market segment. The collaboration between enterprise-class vendors and niche players has led to consolidation within the industry either in the form of M&A or integrations.

> *"With the rapid expansion of cloud and IoT, organizations face even more diverse and ubiquitous cyber threats. Israel is a global source of Cybersecurity innovation yet innovators are challenged with reaching decision makers globally and with being yet another small and essential piece in the Cyber defense puzzle. We are all essentially competing over the CIO/CISO time. This reality requires innovators to invest great efforts in market reach and creates collaboration and consolidation opportunities in the market."*
>
> Alon Elie
> VP of Corporate Development,
> Check Point Software Technologies

9 For more reading on this topic and how to remediate the risks, please visit our blog post - A Guide To The Latest Hacker's Business Model And How To Beat it

10 Clouds Are Secure: Are You Using Them Securely?, Gartner (2018).

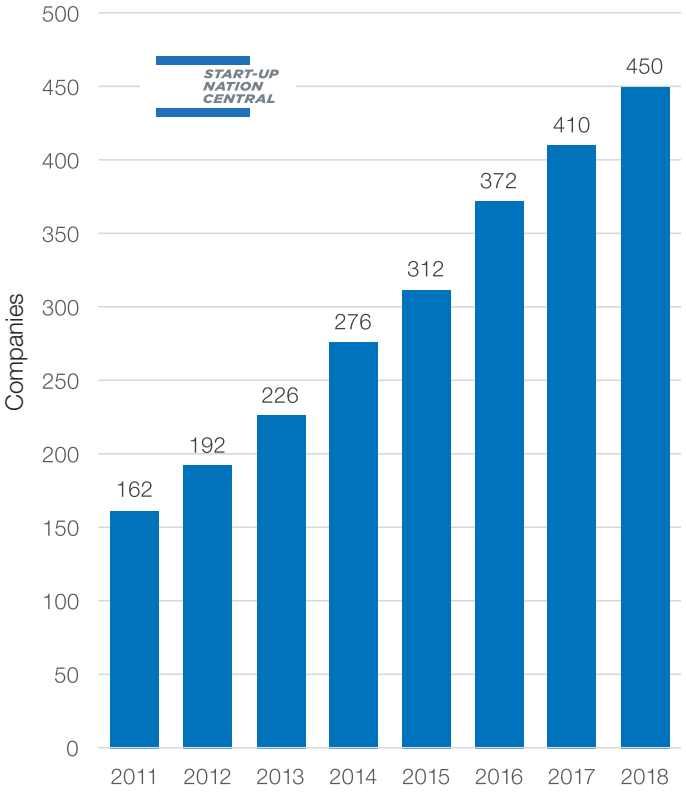
11 (ISC)² Cybersecurity Workforce Study, (ISC)² (2018).

12 According to the ESG report (2017), enterprise-class Cyber Security vendors are vendors "positioned to offer a broad array of increasingly integrated products and services to large organizations", e.g. Cisco, IBM, and Microsoft.

THE ISRAELI CYBERSECURITY INDUSTRY

Israel's longstanding position as a leader in the global effort to prevent cyber crime remains indisputable. By the end of 2018 there were 450 active Cybersecurity companies[13] (see Figure 1), 60 of which were founded during the past year (compared to 75 companies in 2017).

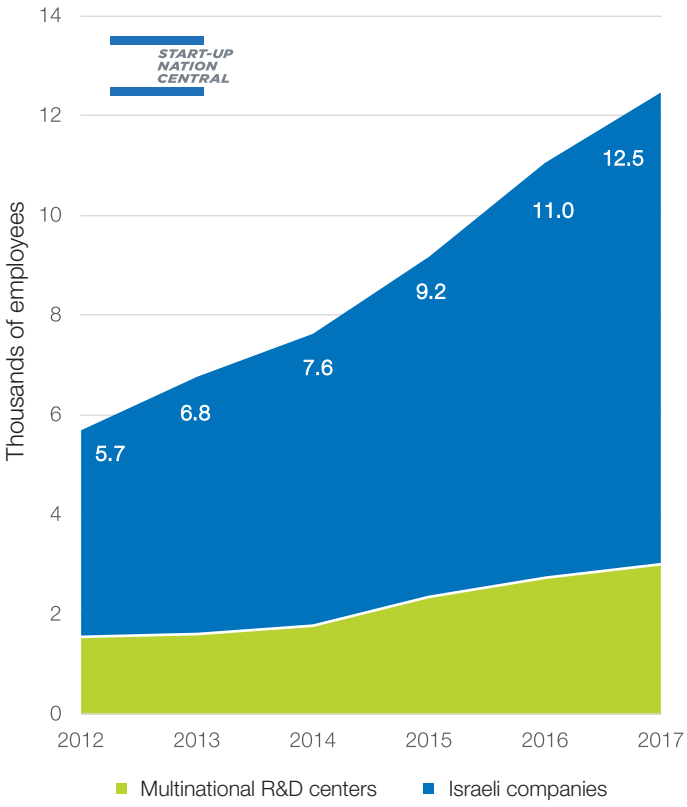
Figure 1: Active Israeli Cybersecurity Companies



REVENUE AND EMPLOYMENT

As part of a continuous collaboration between Start-Up Nation Central and the Central Bureau of Statistics (Israel), for the first time we are able to shed light on certain aspects of the industry growth and value. From the universe of 580 active and non-active Cybersecurity companies and R&D centers of multinational companies (MNCs) in Start-Up Nation Finder, the CBS identified records of 344 companies and MNCs that reported revenues on a standalone basis between 2012-2017.[14] [15] This sample of companies generated annual revenues of more than $3.5B in 2017 – a 12% increase since 2016. We also observed a 13% increase in the number of employees between 2016 and 2107, reaching a total of nearly 12,500 employees.[16]

Figure 2: Number of Employees in the Israeli Cybersecurity Industry



Source: Start-Up Nation Finder and The Central Bureau of Statistics

The sector consists largely of small companies with no significant revenue, although in this sample, 35 companies exceeded $10M in revenues in 2017, compared with 32 in 2016.

Figure 3: Revenues of Israeli Cybersecurity Companies

2014	2015	2016	2017	% change 2016-2017
Revenues in USD (Bn):				
2.6	2.86	3.17	3.55	**12%**
Number of companies with annual revenue >$10M:				
24	24	32	35	**10%**

Source: Start-Up Nation Finder and The Central Bureau of Statistics

13 All figures regarding the Israeli high-tech industry are calculated according to Start-Up Nation Finder statistics, unless otherwise stated. In general, and for the purpose of this report, Start-Up Nation Central recognizes an Israeli Cybersecurity company as any company that sells and develops products, whose founders are Israeli and at least part of the R&D is based in Israel.

14 Based on a list of entities that Start-Up Nation Central identified as Cybersecurity companies and R&D centers. The sample does not include service providers, consultancy firms, integrators, defense companies, and large companies with a Cybersecurity unit (IAI-ELTA, RAD, NICE Systems, Verint Systems and ECI Telecom)

15 By the time the report was written the data for 2018 is not yet complete, therefore our analyses in this section refer to the period ending in December 2017.

16 These numbers do not include service providers, consultants, integrators, and Cybersecurity professionals employed by businesses (security analysts, researchers, architects, penetration testers and others).

There are 47 MNCs with Cybersecurity-related operations in Israel. Most engage with Israeli Cybersecurity by establishing an R&D center that develops security products or components within their existing products and services. Others have adopted a variety of models, innovation labs being the most common. Such labs create strategic partnerships and engagements between Israeli start-ups and various business units within the enterprise. Some MNCs have moved their internal security operations teams to within Israel, which can act as incident response, red-teams, or provide penetration testing services (see Figures 4 and 5).

Figure 4: MNCs Cybersecurity Centers in Israel - by Vertical

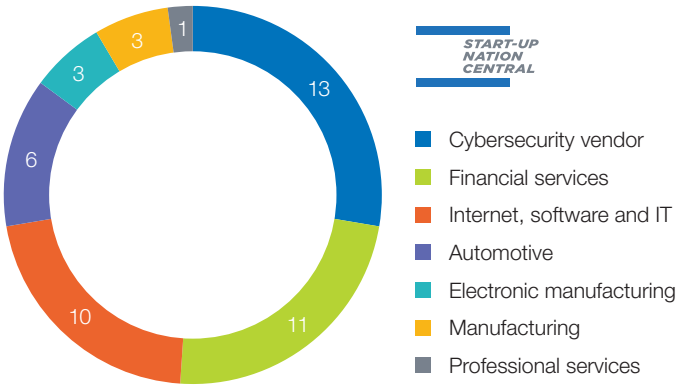
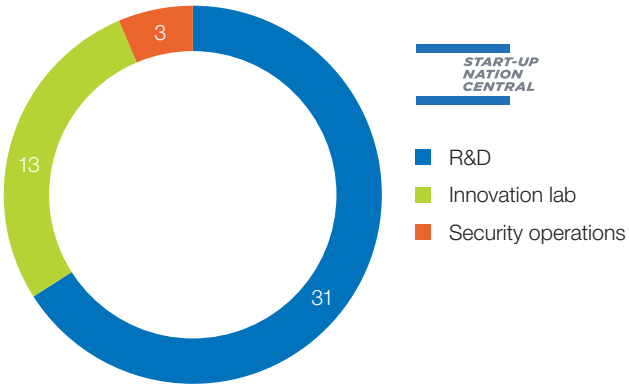


Figure 5: MNCs Cybersecurity Centers in Israel - by Model



Source: Start-Up Nation Finder

The success and recognition of the strengths of the Israeli Cybersecurity industry stem in part from the collaboration between Israelis and entities all over the world, in both the private and public sectors. A notable 2018 event was the choice of the JVP VC fund, together with SOSA, to establish a New York City hub focused on developing Cybersecurity technologies, in partnership with New York University, Columbia University, and Cornell Tech. A co-operation accord was also signed between Japan and Israel for the two nations to share research and development resources and capabilities, information and training programs.

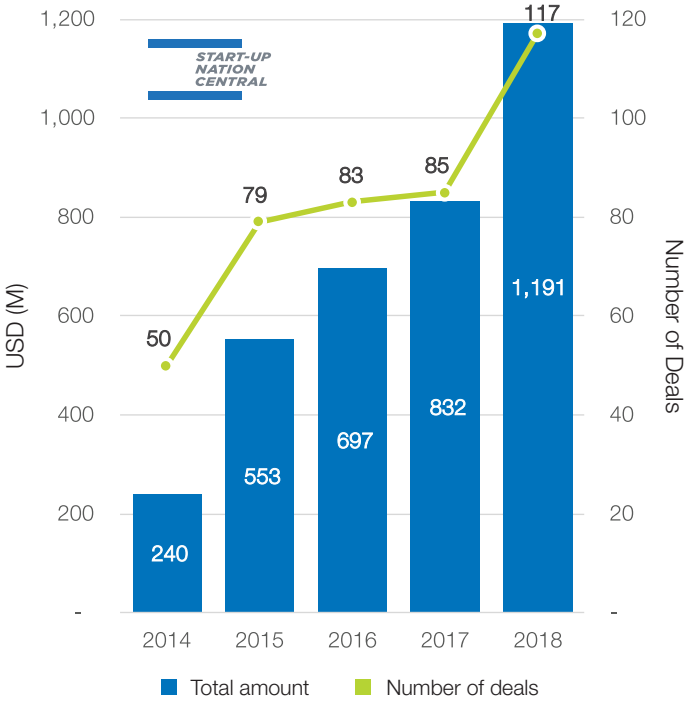
FINANCING

Israeli Cybersecurity companies raised a total of $1.19Bn in equity, a record-breaking amount for the fourth year in a row, exceeding 2017 investments by 47%, and showing a five-fold increase since 2014. As in previous years, in comparison to the global Cybersecurity industry, the Israeli industry comes second only to the US, having taken 20% of the overall cyber investments worldwide, increasing its share over 2017 (16%).[17] This amount was raised in 117 investment rounds (39% more deals than 2017).

The dramatic growth in the amount of funding is not due to a few "mega-funding rounds" compared to previous years. There were only three investment deals of more than $50M, which accounted for less than 15% of the total amount invested in 2018, as opposed to three deals that accounted for 40% of the total in 2017.

> *"Israeli Cybersecurity companies are maturing and more companies are in a position to expand and become meaningful global players, compared to previous years. As investors, we also see more companies that are focused on holistic solutions for a specific vertical, rather than coming up with new techniques to solve a known problem in the traditional large enterprise segment."*
>
> Barrel Kfir,
> Senior Associate,
> JVP

Figure 6: Israeli Cybersecurity Equity Investments



17 Based on Pitchbook data and Start-Up Nation Finder

The median size of investment rounds continued to grow in 2018, and currently stands at $6M, compared to $3.5M in 2017. In comparison to the global Cybersecurity industry, Israeli start-ups succeeded in attracting larger investment rounds, especially in Seed and Series A rounds.[18]

Although the absolute number of both early and growth/late-stage investments grew, the share of early-stage (Seed and Series A) investment rounds continued to decline slightly (see Figure 7), while the number of series B+ rounds increased. This indicates that more companies are maturing and attracting larger investments to maintain their growth.

The median size of investments grew at all stages (see Figure 8). Israeli early-stage start-ups received larger Seed, and Series A rounds than in the US. This could indicate Israel's competitive advantage in both the development of solutions based on deep technology, and that of more innovative solutions. At the same time, Israeli later stage companies attracted smaller investments than their counterparts abroad. The total amount, as well as the number of early-stage investments in Israel, grew in 2018, in contrast to the global cross-sector trend of fewer early stage investments since 2016.[19]

Figure 7: Number of Investments - Early vs. Late stage

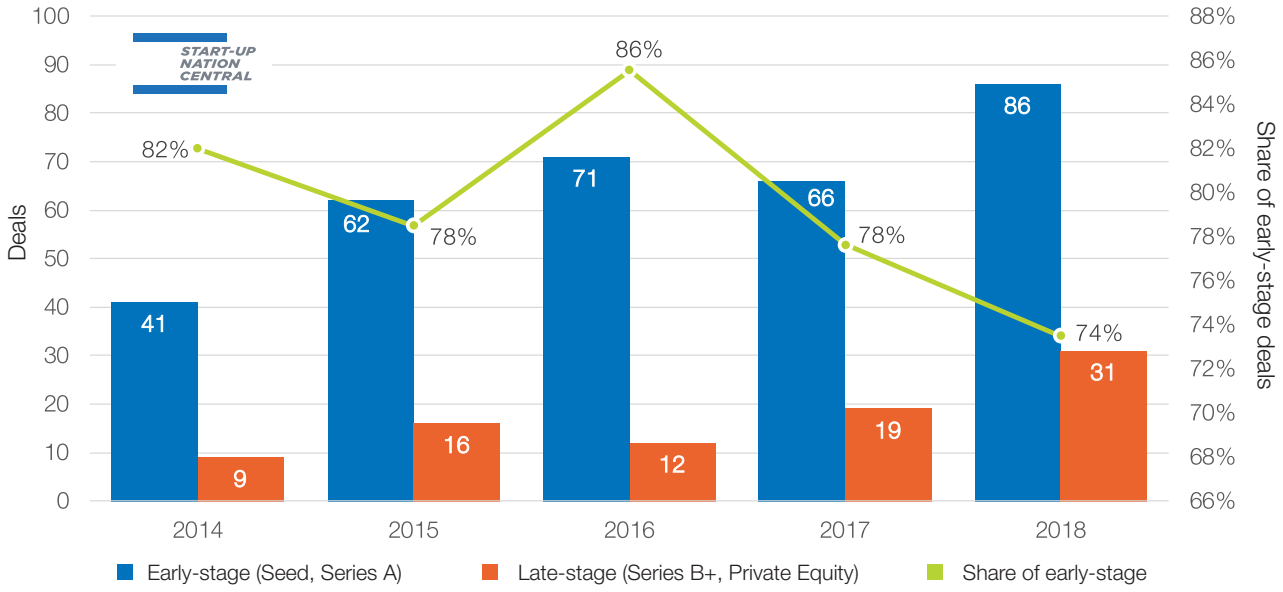
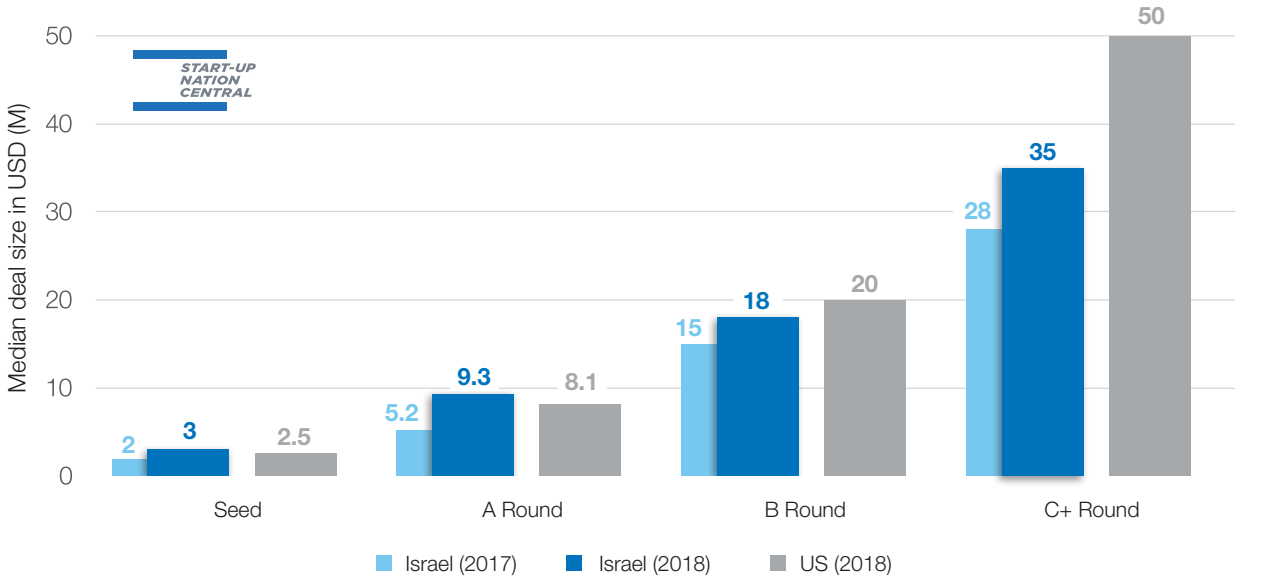


Figure 8: Median Deal Size



Source: Pitchbook data and Start-Up Nation Finder

18 Based on Pitchbook data and Start-Up Nation Finder

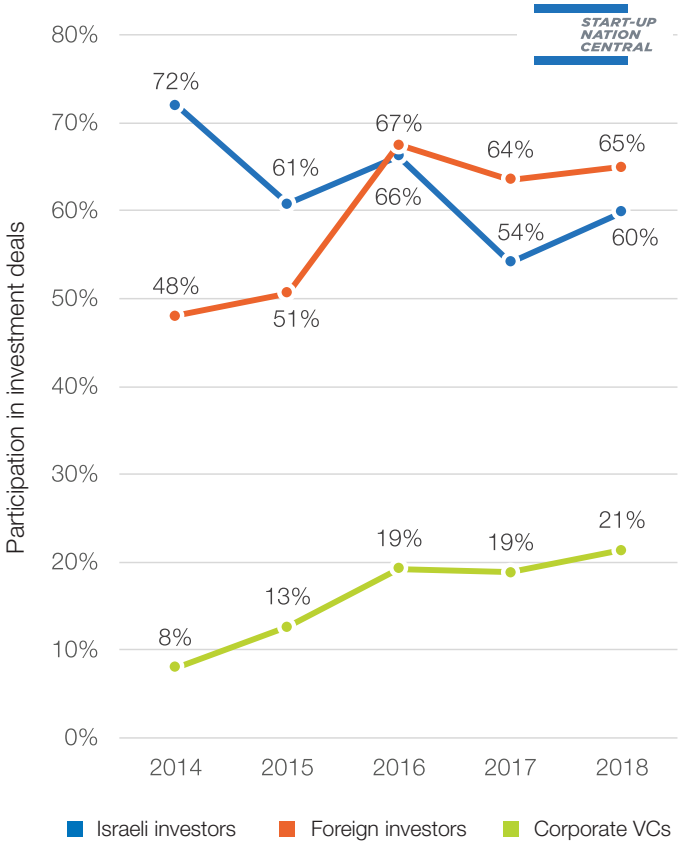
19 The 3Q VC Valuations Report, PitchBook (2018)

Non-Israeli VC investors continue to be the dominant players in the industry, participating in 65% of investment deals (See Figure 9).[20] At the same time, large corporates increased their engagement with Israeli Cybersecurity start-ups by investing in them. This is consistent with the broad global trend of corporate engagement with start-ups.[21]

The leading investors in Cybersecurity this year were Glilot Capital Partners, an Israeli VC Fund, and ClearSky Security Fund, a US-based investment firm, each with six investment deals. By becoming the most active investor, ClearSky Security represents two major investment trends in the local industry: the growing involvement of investors from abroad, and that of more capital being raised in Series B+. This is in contrast to previous years, when the leading investors were always early-stage Israeli VCs.

Other very active non-Israeli investors were Blumberg Capital, Boldstart Ventures, Intel Capital, and Sequoia Capital, each with four investments. The Israeli investors Team8, 83North, JVP, OurCrowd and Elron Electronic Industries also each invested in four companies during 2018.

Figure 9: Investor types



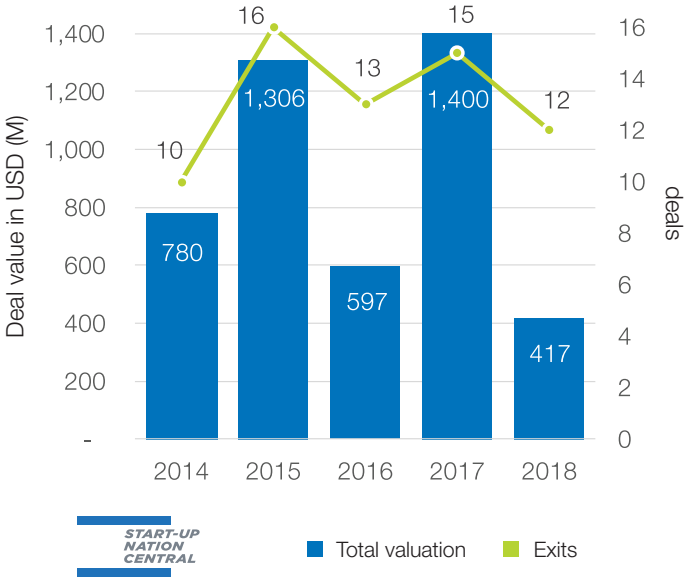
EXITS

2018 saw twelve exits (first-time deals, including IPOs and buyouts), the total of six of which was $418M, (the values of the other six have not been disclosed). Relative to previous years, this is a decline in numbers. We see a similar decline across all sectors which could be interpreted as a sign that more companies are choosing to stay private longer and grow their business, rather than look for an early exit. Another possible reason for the slowdown in M&A activity is that many of the top-tier global security vendors have already established local R&D centers, therefore they are less inclined to "acqui-hiring".

The largest deals were: Dome9 Security acquired by Check Point (for reportedly $179M), and SECDO acquired by Palo Alto Networks (for reportedly $100M). For the US-based Palo Alto Networks, this was the fourth acquisition in Israel over the past five years. Sygnia, a Team8 company that offers consulting and incident response support services, was acquired by Temasek, and although this acquisition was not included in our aggregation,[22] this deal may indicate the growing demand for Cybersecurity services that support any technology and product.

In 2018, there was a very prominent trend of consolidation between vendors in the global Cybersecurity industry. Private equity fund Thoma Bravo acquired four large companies in one year – one of which was the Israeli company Imperva. This could indicate a future trend of combining assets of different vendors into one Cybersecurity vendor with a broad portfolio of solutions. In addition, Cisco's acquisition of Duo, a leading provider of unified access security for $2.3B, and Blackberry's acquisition of Cylance for $1.4B, serve as good indicators of the popular trend of consolidation in the Cybersecurity industry. All of the above offer an incentive for Israeli start-ups in their growth stages to continue investing in expansion, rather than being bought at a relatively early stage.

Figure 10: Exits 2014-2018



20 In most investment deals, different entities with different characteristics (i.e. Israeli/Foreign, Angel/ VC/CVC) co-invest in an investment deal. As we lack the data regarding the lead investor in any specific deal, one deal may be defined as including the participation of both Israeli and non-Israeli investor, as well as Corporate VCs. Therefore, shares will add-up to more than 100%. In addition, deals with the participation of non-Israeli Corporate VCs are also considered to be deals with the participation of non-Israeli investors.

21 EULA out, equity in: Why startups are now a part of larger companies' security budgets, CyberScoop (2018).

20 According to Start-Up Nation Central's methodology, companies considered for this report pursue R&D activities in Israel, and are not service providers. Sygnia does not meet these criteria.

SUBSECTORS

We partition the Cybersecurity sector into 10 subsectors that correspond to challenges they address. These are:

Data Protection, Encryption and Privacy

Network Security: prevention of APT, visibility solutions, isolation and deception for the enterprise network.

Endpoint Security: anti-malware and anti-ransomware solutions, and Endpoint Detection and Response (EDR).

Cloud and Infrastructure Security: solutions for securing cloud services, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), container-based virtualization and serverless computing.

Anti-fraud, Authentication and IAM (Identity and Access Management)

Mobile Security

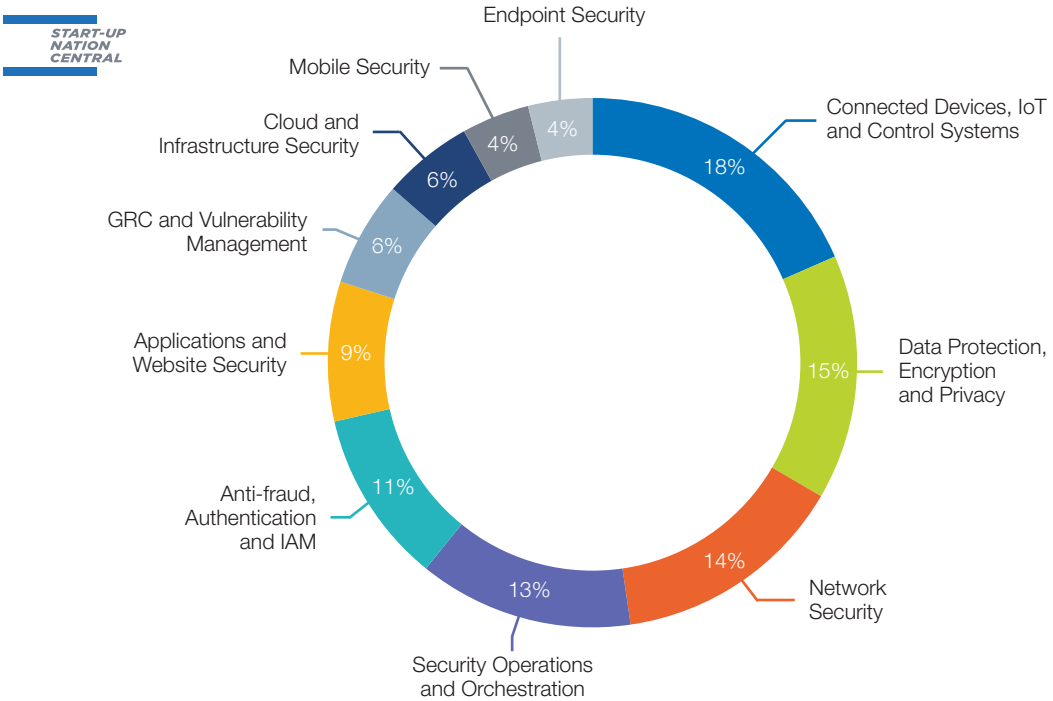
Applications and Website Security: security measures for software and web applications, including code review, bot detection, DevSecOps, web application firewall (WAF) and DDoS prevention.

Connected Devices, IoT and Control Systems: solutions for security challenges when using connected devices, from IoT network and mobile device management, to connected cars, industrial control systems, and medical devices.

GRC and Vulnerability Management: cyber-risk and vulnerability management, solutions for cyber insurance, supply-chain monitoring, and compliance audit.

Security Operations and Orchestration: all operational measures required to protect an enterprise network, including Security Orchestration, Automation and Response (SOAR), forensics, SIEM, alert management, threat intelligence, security analytics, and penetration tests.

Figure 11: Active Cybersecurity Companies by Subsector



SUBSECTOR TREND ANALYSIS

We have identified positive trends in:[23]

Connected Devices, IoT and Control Systems

Security Operations and Orchestration

Cloud and Infrastructure Security

Data Protection, Encryption and Privacy

In terms of the number of companies founded during 2018, the most dominant subsector is **Data Protection, Encryption and Privacy** – representing the growing awareness and fear of data breaches. Thirteen new start-ups were founded during 2018 in this veteran subsector (more than in any other subsector), adding up to 65 active companies (15% of the cyber sector), and sixteen investment rounds (14% of the total). The growing demand for privacy, plus a vocal public debate and the need for GDPR compliance, are attracting entrepreneurs and investors to next-generation solutions including AI-based data governance solutions, and advanced cryptography. A good example of this vibrant domain is BigID, a Machine-Learning-based solution for privacy protection and management of customers' personal data, which raised $44M in two funding rounds last year, and was named the "RSAC Most Innovative Startup 2018" of the RSA Conference Innovation Sandbox Contest.

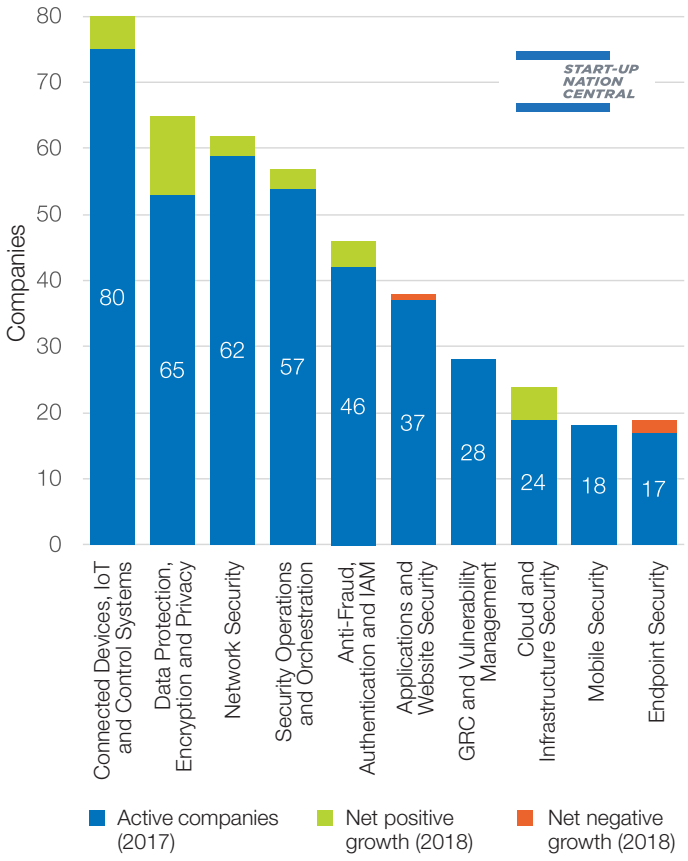
The **Connected Devices, IoT and Control Systems** subsector continues to attract a great deal of investor and customer attention. It remains the largest subsector with 80 companies, of which eight were founded in 2018. 25 companies in this subsector had an investment round during 2018, totaling $218M (compared to $66M in 2017). Four of the largest investments in this subsector in 2018 were raised by companies that provide solutions to Industrial IoT, control systems, and critical infrastructure: Claroty ($60M), and Indegy, CyberX and Radiflow ($18M each). Armis, offering an IoT security platform for enterprises, raised another $30M.

This year, more than ever before, we saw collaborations between top-tier information security vendors (such as Check Point, or Palo Alto Networks) and IoT security vendors. IoT security products are being consolidated into broad portfolios of solutions. ForeScout's acquisition of the Netherlands-based company, SecurityMatters, may give a hint regarding the future direction of the subsector – from segregated domains offering solutions for niche products and families of devices (medical devices, industrial control systems and networks, automotive, etc) to a more holistic approach at the enterprise network level. Another growing area of innovation concerning the risks of connected devices is reflected in companies that offer solutions for embedded security layers in devices, and secure development of IoT devices, focusing on OEMs as their main customers. VDOO, for example, raised $13M in 2018.

The **Security Operations and Orchestration** subsector continues to address the problems of the lack of Cybersecurity personnel. According to a recent study by ICS2, 63% of organizations suffer from staff shortage, and 59% of the respondents said that their organization is at extreme to moderate risk as a result.[24] As this shortage becomes more acute, enterprises are investing more resources in automating manual security operations and incident responses. Furthermore, Cybersecurity managers understand the value of threat intelligence as an efficient preventive measure. Of 57 Israeli start-ups in this subsector, 18 raised investments, totaling an impressive $298M. KELA Group raised $50M, and Demisto raised $43M. The Breach and Attack Simulation family of solutions has also gained popularity over the past two years, and some of the fast-growing companies in this segment are Israeli, including XM Cyber, which raised $22M, and SafeBreach, which raised $15M.

The **Cloud and Infrastructure Security** subsector showed strong growth in 2018, with ten companies raising investments totaling $96M. More companies are offering security solutions in cloud-native environments that allow DevOps, IT and cloud teams to operate seamlessly and develop secure apps. These solutions not only lower the security risk involved in cloud environments, but also serve to enable new software-based business models and make security teams less of an inhibitor in software development.

Figure 12: Active Companies by Subsector



23 We classified the local industry into ten subsectors and examined their performance over the past year according to two categorizations: number of new companies, and number of funding rounds compared to the size of the subsector. Further to this, we refer to the absolute size of the subsectors and the amount raised, but due to the large variance in subsector sizes and funding round sizes, these stats are less effective when analyzing trends.

24 (ISC)² Cybersecurity Workforce Study, (ISC)² (2018).

Network Security dropped to third place in terms of the number of companies (after being the largest in 2016), with only 9 companies (10%) raising an investment round this year. One reason for the slowdown is the strong consolidation trend (as discussed earlier in this report). Large traditional vendors, which tend to hold a rich portfolio of solutions for network security, are more likely to collaborate with start-ups that address non-traditional challenges and threats in order to enrich their portfolio of services.

Mobile Security also had an unimpressive year, with no new companies, and very little investment activity.

The smallest subsector, **Endpoint Security**, also saw a slight fall in the number of active companies and far fewer investments in 2018 compared to the previous year (mainly due to three large investments during 2017: Cybereason, SentinelOne and Deep Instinct).

Figure 13: Financing Activity Per Subsector

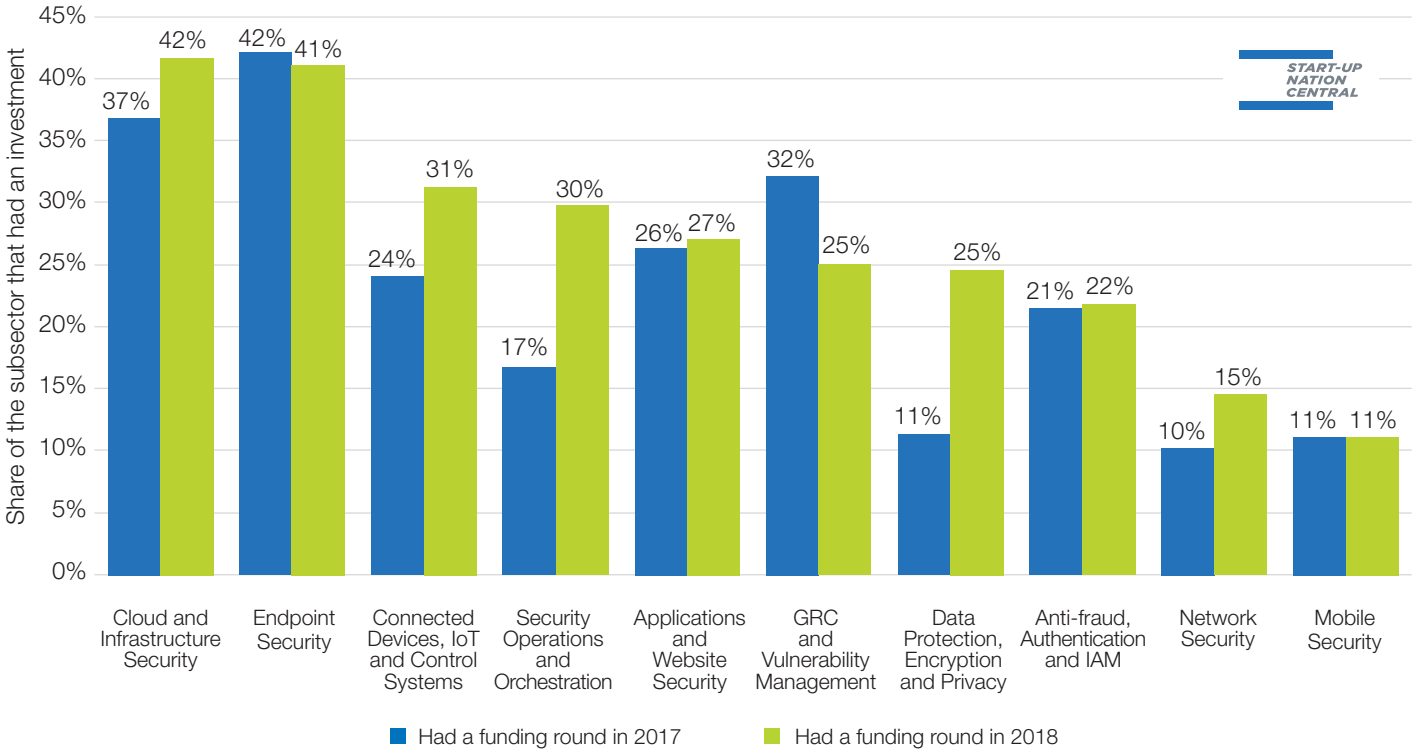
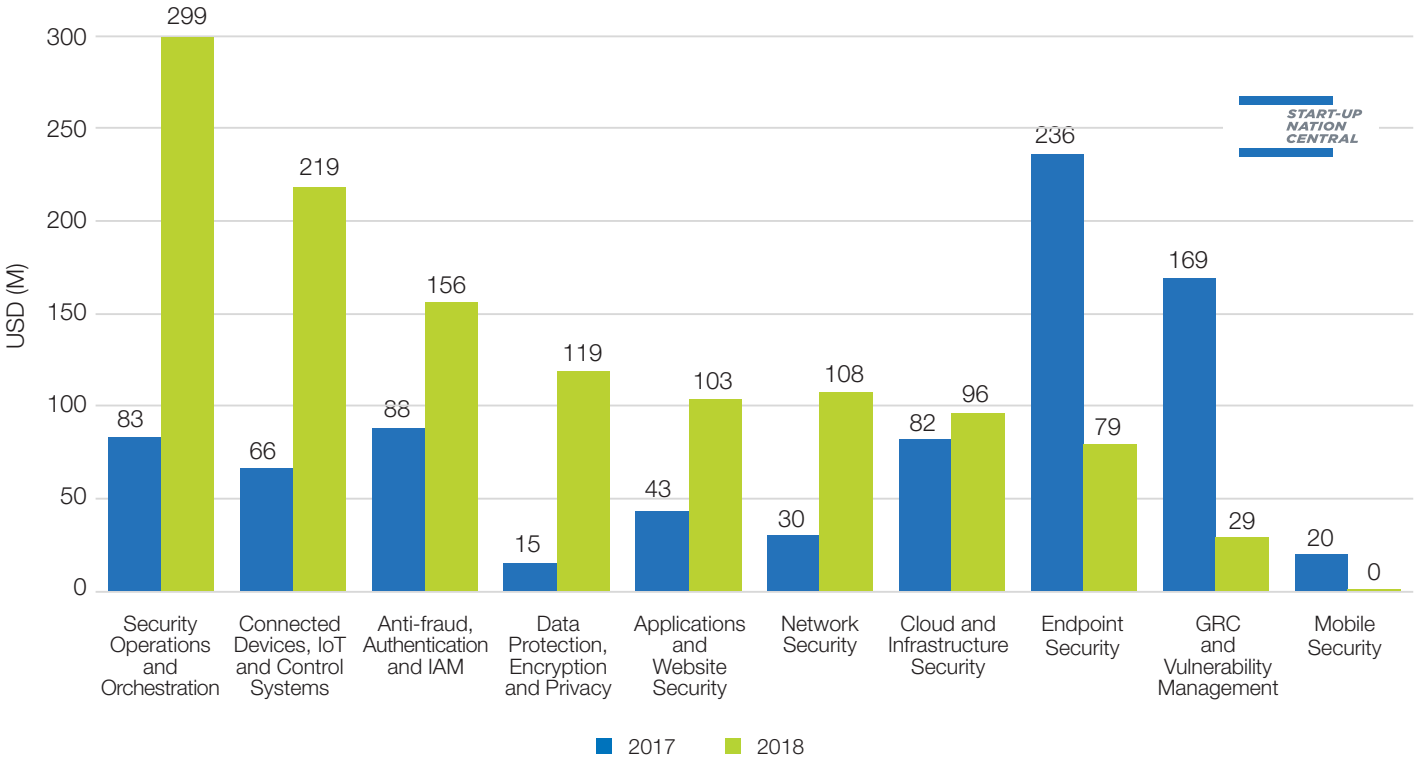


Figure 14: Total Investment per Subsector



START-UP NATION CENTRAL AND THE CYBERSECURITY SECTOR

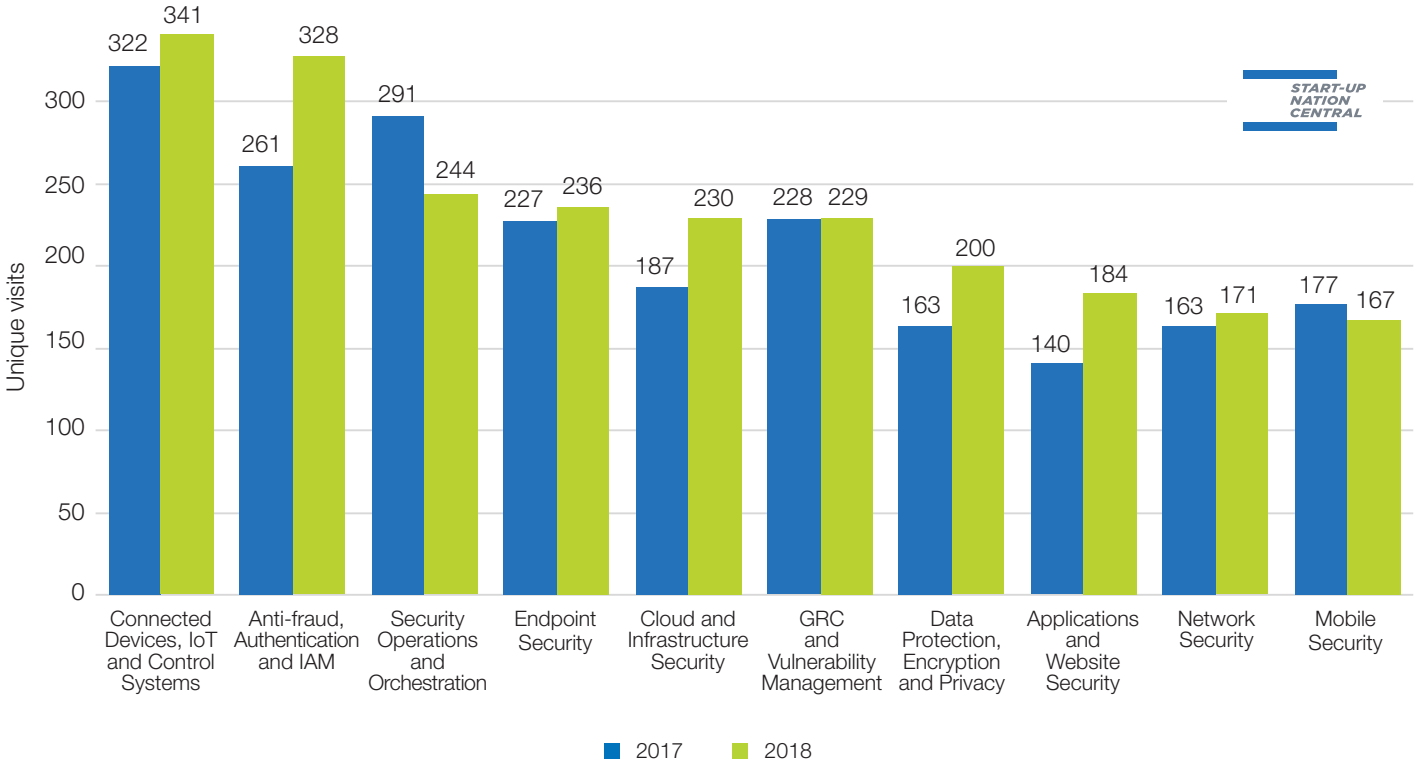
Start-Up Nation Central is committed to helping global corporations generate significant value by engaging with Israeli innovation in general and with Cybersecurity sector in particular. Aiming to facilitate mutual business opportunities, we have hosted senior executives from dozens of giant multinational corporations, senior government and NGO officials, and investors, introducing them to the most relevant experts and technologies; so far connecting more than one hundred Israeli Cybersecurity companies with potential partners, customers and investors. These highly customized and expertly-curated visits are carefully prepared to identify and address our partners' most pressing challenges and needs. Some of these connections have already evolved into POCs, investments, and strategic collaborations, while in many other cases, the dialogue continues.

In June 2018, as part of Cyber Week, Start-Up Nation Central partnered with Tel Aviv University and Team8 for the CyberMatch networking event. The event was designed with the aim of creating a unique opportunity for dozens of CISOs visiting Israel to engage with Israeli Cybersecurity start-ups that best answer their needs. Based on our prior communications with the CISOs, and our subsequent understanding of their workplans and the challenges they face, Start-Up Nation Central assigned meetings for each CISO with specific start-ups.

Not surprisingly, 80% of CISOs were interested in **Security Operations and Automation**, specifically in Patching Management, Vulnerability Remediation and Security Orchestration, Automation and Response (SOAR) solutions. **Enterprise Identity and Access Management** aroused strong interest among 65% of the participating CISOs. There was also significant demand for **Application Security**, **Code Quality and Security**, for **DevSecOps** in particular, and for **Data Protection**, **Privacy and Encryption**, **Deception Technology**, and **Security for Microservices**, and **Security Solutions for Online Banking Apps**.

Start-Up Nation Central also creates many opportunities through Start-Up Nation Finder, our innovation discovery platform, in which anyone can search for information on Cybersecurity companies, technologies and investors in Israel, and can contact them. During 2018, the term "Cybersecurity" was the third-most popular search within the platform, after Fintech and Digital Healthcare. The most popular subsequent searches (when combined with "cybersecurity") were the terms **Fintech**, **Automotive**, **Industry 4.0** and **IoT**. Cybersecurity company profiles received 277 unique visits on average across the whole of 2018 compared to 220 in the previous year). Figure 14 presents the average number of searches per profile by subsector.

Figure 15: Average of Unique Visits per Profile



STRATEGIC COLLABORATION WITH ISRAELI INNOVATION

Start-Up Nation Central has helped dozens of multinational corporations realize the potential of collaboration with the Israeli innovation ecosystem, and understand the various ways in which to engage with what it has to offer. Collaborations take several forms:

Affiliations – Multinational corporations organize, participate in and sponsor conferences, hackathons, challenges, competitions and meetups held in Israel, to expose their interests in innovation. This form of engagement can be a long term strategy or serve as a first step to a deeper commitment. . For example, many MNCs from various industries take an active part in the major Cybersecurity conferences held in Tel Aviv throughout the year.

Strategic partnerships – Commercial collaboration with local players, including investors, large companies, start-ups, and academia. Such partnerships provide extensive learning about the capabilities of the Cybersecurity domain, increase familiarity with its innovations. These, often result in investments, POCs, commercial agreements, joint ventures and so on. MNCs frequently partner with local accelerators and incubators (for example AlphaC Incubation Program together with NEC Corporate of America and Innogy Innovation Hub); invest in Israeli VC funds that specialize in Cybersecurity, and participate in design partnership platforms (such as Team8's Global Cyber Syndicate).

Local presence – Certain multinational companies have realized the unique added value of an on-the-ground presence in Israel. In some cases this has been done by establishing an R&D center in Israel: security vendors, including Palo Alto Networks, Proofpoint, Gemalto; online services providers, including Paypal and Microsoft Azure, manufacturers and OEMs, have all established such facilities. Most of these centers were established through the acquisition of an Israeli cybersecurity company (acquihire), although certain companies made the decision to open their centers from scratch (greenfield).

Other forms of on-the-ground engagement are also prevalent. Corporate VCs investing in cyber technologies (Singtel Innov8) run acceleration programs and design partnerships (Citi Ventures), Security Operations (Novartis), and Cybersecurity innovation labs (TD bank and Sompo). Due to the scarcity and the rising cost of hiring Cybersecurity professionals in Israel, many MNCs increasingly prefer to engage in Open Innovation in Israel by soliciting and implementing external ideas and products, largely through collaboration with start-ups.

The Israeli government supports certain types of on-the-ground engagements by MNCs, especially the Open Innovation model.

2019 CYBERSECURITY EVENTS IN ISRAEL

Israel hosts some of the most influential international Cybersecurity conferences, attended by world leaders, key players in the industry, academics and tech experts. **Cybertech**, **ICRC's Cyber Week**, and Team8's **Rethink Cyber**, are just a few examples of events that attracted thousands of visitors from Israel and abroad in 2018.

In the pipeline for 2019:

Cybertech - https://cybertechisrael.com/

Israeli Cybersecurity Showcase at RSA - https://israelatrsac.com/

The Israeli Delegation to the RSA Conference, hosted by the Israeli Economic Mission and the Israeli Export Institute

CyberWeek - https://cyberweek.tau.ac.il/2019/

Hosted by the Blavatnik Interdisciplinary Cyber Research Center (ICRC) and the Yuval Ne'eman Workshop for Science, Technology, and Security

ABOUT START-UP NATION CENTRAL

Start-Up Nation Central is an Israel-based non-profit that serves as a gateway to Israeli innovation. As an organization, we leverage our in-depth knowledge of Israel's innovation sector to draw insights and act on them, working in partnership with individuals and organizations in Israel and around the world, to help this sector expand and flourish.

Start-Up Nation Finder is Israel's definitive innovation discovery platform, provided as a free online resource. Mapping more than 6,500 innovative companies, investors, hubs, technology transfer offices, and multinational R&D centers, Start Up Nation Finder is a widely utilized source of information and insights. Based on its success, Start-Up Nation Central has also launched a Global Finder network that allows growing innovation hubs across the world to map and connect all the relevant stakeholders.

The success of the Israeli innovation ecosystem is the motivation behind Start-Up Nation Central's activities. We engage corporate, government, and NGO leaders from across the globe with Israeli innovation, creating customized and curated experiences where they connect to the relevant people and technologies that can address their most pressing challenges. We help start-ups build practical tools and expand their skillsets, regardless of their field, while paying especial attention to the development of the Agritech, Digital Health and Industry 4.0 sectors. We support tech communities, increasing collaboration and knowledge-sharing within the ecosystem.

Start-Up Nation Central's mission is also to help the tech innovation sector remain strongly rooted in Israel, and to this end, we have become an important voice on policies relating to this, together with creating innovative solutions to achieve this aim. We convene diverse thought leaders to help shape long-term strategy for the country, as well as directly addressing the issues of human capital shortage and development of regional ecosystems. Utilizing its knowledge and its connectivity within the community, Start-Up Nation Central promotes Israeli innovation at home, and across the globe.

To read Start-Up Nation Central's 2018 Cybersecurity Report, go to https://lp.startupnationcentral.org/Cybersecurity_report_2018/

METHODOLOGY

DATA SET

Amounts and definitions relating to Israeli innovation and entities accord with those of Start-Up Nation Finder. Companies considered for this report were founded by Israelis and pursue R&D activities in Israel, and are not service providers. This report organizes Israel's Cybersecurity sector into subsectors. Subsector division organizes the relevant companies into an inherently simplistic regimentation. Some companies offer multifaceted technologies and therefore could be assigned to multiple subsectors. But for the sake of deriving investment and tech trends, we associate each company with only one subsector, that which reflects the company's major focus. Figures representing numbers of companies and investments in Israeli Cybersecurity and its subsectors are likewise exclusive, e.g. we do not associate one company with multiple subsectors.

FINANCING

Refers to any equity transaction (e.g. VC, corporate, or angel investments; private equity in growth stage), but excludes full or major liquidity events (those are considered as Exits). In the cases where companies receive investments from incubators conjointly with grants from the Israel Innovation Authority, the latter are included in the funding amounts and are not specified. Fundraising amounts entail only the value invested in a given time period; even if a deal includes terms for future obligations, we do not include the pending conditions in the amounts listed in this report. Some investment figures may include funding that does not appear to the public on Start-Up Nation Finder. These amounts reflect data that Israeli companies disclosed to Start-Up Nation Central in confidence, which they prefer to remain inconspicuous while still factored into aggregates.

DIFFERENCES FROM PREVIOUS EDITIONS

There are slight changes in the statistics and measures from last year's report, due to continuous collection of data. In addition, we changed the way we measure the number of active companies each year (as seen in Figure 1) to represent the number of active companies by the end of each year, while excluding companies that were closed during the year.

AUTHOR

Nir Falevich,
Cybersecurity Sector Lead
Nir.falevich@sncentral.org

CONTACT

For more information on the Israeli Cyersecurity sector and the companies cited in this report, please visit:
finder.startupnationcentral.org

Find out more about your
next business opportunity
using our innovation discovery platform

Start-Up Nation Finder

finder.startupnationcentral.org

START-UP
NATION
CENTRAL