START-UP NATION CENTRAL: FINDER INSIGHTS SERIES

ISRAEL'S CYBERSECURITY INDUSTRY IN 2017

START-UP NATION CENTRAL

Nir Falevich
Cybersecurity Sector Lead

EXECUTIVE SUMMARY

Throughout 2017, major data breaches and devastating ransomware campaigns made headlines all over the world. Three global-scale ransomware campaigns hit individuals and organizations across the globe, resulting in billions of dollars of damages, but only representing the tip of the iceberg of criminal activity in the cyber domain in 2017. Individual hackers are now armed with state-level cyber-attack capabilities, making cyber risks ubiquitous.

Simultaneously, the Israeli Cybersecurity sector has solidified its position as a source of innovation for cyber defenders all over the world. 2017 saw more multinational companies and governments making a strategic decision to engage with the Israeli cybersecurity industry, leveraging the local talent and spirit of innovation to help protect them from cyber threats.

The Israeli cyber ecosystem has continued its long-term growth with another record-breaking year in investments: a total of $815M, 16% of global private investments in the cybersecurity industry (an increase of 28% over 2016). While we saw fewer investment deals by early-stage start-ups, the size of the average seed investment increased to exceed the average in the US. We also saw a growth in the activity of foreign investors, who participated in two of every three funding rounds of Israeli companies in 2017. Furthermore, 2017 saw fourteen exits totaling more than $1.4B, exceeding the number and value of exits by Israeli cybersecurity companies in 2016.

The Israeli cybersecurity sector demonstrates clear signs of maturity. Three of the five largest investment deals over the past few years happened in 2017, more late-stage investment deals than ever before, and one IPO on NASDAQ by an Israeli company, all of which indicate the growing layer of pre-growth and growth cybersecurity companies.

2017 will be remembered as the year when the cybersecurity sector, both worldwide and Israeli, began to invest highly significant effort in defending IoT and Connected Devices, as well as in specific IoT segments, including medical devices, automotive systems, and industrial control systems. IoT Security accounted for 30% of newly-founded start-ups in 2017. Further positive trends can be seen in the Security Operations and Endpoint Security subsectors. The Network Security and Anti-Fraud solutions subsectors experienced reductions in the number of new companies established and in funding, in comparison to previous years.

Start-Up Nation Central is proud to present its annual Cybersecurity report, which offers a comprehensive and up-to-date analysis of the state of the Israeli cybersecurity ecosystem and its trends. Below, we review the major global developments of 2017, and analyze the performance and activity of cybersecurity companies in Israel, including by subsector. We utilize the data we collect on the Israeli cybersecurity industry, some 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, and investors, and provides accurate information on more than 5,800 companies across dozens of industries.

THE GLOBAL SCOPE

In 2017, cybercrime continued to dominate global headlines, following several high profile breaches, which demonstrated clearly that no organization is immune to cyber attacks. Furthermore, these attacks show that breaches are growing increasingly harmful to organizations, and also to society as a whole.

For example, Equifax, the American credit-reporting service, was subject to a major data leak in May 2017, which was revealed to the public only months later. The source of the breach was a malicious outsider, who exploited a known and unpatched security vulnerability in a web application. This resulted in the theft of 143 million identity records that included names, addresses and social security numbers, making this cyber attack seemingly the worst and most harmful ever.

Another extremely severe leak targeted the CIA. In March 2017, a group of hackers named The Shadow Brokers published a data trove on Wikileaks, containing secret information regarding cyber warfare, and operational information regarding surveillance activities and capabilities. This included source-code for hacking tools and zero-day exploits, which the CIA and the NSA had acquired over the years. Making these tools and techniques available to the public, the leak strengthened the commoditization trend of advanced hacking tools. What used to be exclusively the domain of strong states became available to a large number of individual hackers. Despite having less technical expertise, individual hackers and organized groups can now execute costly cyber-attacks.

The severity of this leak became very clear a month later, with the appearance of the WannaCry ransomware campaign. On May 12, 2017, a malware worm spread into more than 200,000 computers across 150 countries, using an exploit that was revealed following the leak from the CIA, commonly known as EternalBlue. EternalBlue allows the malware to propagate inside networks from one Microsoft Windows computer to another, rendering any computer that is unpatched, or has an unsupported old version of Windows, extremely vulnerable. Among the victims of WannaCry malware was England's National Health Service (NHS), which found itself temporarily unable to provide medical services.

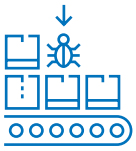
A few weeks later, on June 27, 2017, another type of ransomware called NotPetya spread internationally, using the very same EternalBlue exploit. The NotPetya attack was far more harmful than the WannaCry attack, since it employed a highly destructive file encryption methodology, which modified the master boot record (MBR) of the hard drive, leaving computers unable to recover. The spread of this destructive worm negatively impacted the operations of several giant companies, including FedEx TNT, the Danish shipping company Maersk, and the American pharmaceuticals manufacturer Merck, costing billions of dollars in lost sales.

Overall, during 2017, ransomware continued to be a serious concern for cyber defenders. According to research carried out by Accenture, in 2017, 27% of the companies surveyed experienced ransomware attacks (up from 13% in 2016),[2] and ransomware payments exceeded $2B.[3] Additionally, several new industry verticals experienced ransomware attacks. For example, in an Austrian hotel, all guests were locked out of their rooms following a ransomware attack on the key lock system.

2 2017 Cost of Cyber Crime Study, Independently conducted by Ponemon Institute LLC and jointly developed by Accenture (2017), 23.
3 2017 Ransomware Report, Bitdefender (2017).

In summarizing the state of cyber threats and cybercrime in 2017, we can identify five main trends:

Advanced hacking tools and techniques that were once affordable only to large and rich entities (chiefly governments), are now **easily accessible to the public**. Prolonged APT[4] campaigns are no longer the exclusive realm of nations and states.



Supply chain as a common threat: It is becoming clearer that even trusted supply chain vendors and third-party software providers are being used by hackers to penetrate their clients' networks. An example is the attack on CCleaner which came to light in September 2017, where hackers added a piece of malicious code to the commonly used PC-maintenance software, which gave them the ability to install malware at the customer endpoint.

The rising number and severity of data breaches: According to Gemalto,[5] there has been a significant increase in the number of data breaches, and the amount of records stolen. The most troubling fact is that only 4% of the stolen data was properly encrypted. The most noticeable data breaches of 2017 were those experienced by Equifax and River City Media.

The rapidly increasing adoption of IoT devices, and implementation of connectivity capabilities to traditional devices, reflects an exponentially growing surface area of potential attacks. With an estimated annual growth of 12% in the number of connected IoT devices worldwide,[6] this IoT security risk is not only a threat to the corporate network, but can also be harmful to industrial OT networks, smart grids, connected cars, and to the internet infrastructure itself, as illustrated by the September 2016 Mirai botnet DDoS attack.[7] This raises a huge challenge in the management of networks, and in the development of smart devices.

Increasing adoption of public cloud services: Migration of IT infrastructure to the cloud results in more assets that require protection by the enterprise. New types of relevant infrastructure and platforms, such as serverless computing and containers, involve handling new and unfamiliar forms of cyber risk.

Undoubtedly, cyber incidents will continue to affect a great many aspects of our lives and businesses in the future. As decision makers in the corporate world begin to comprehend the destructive potential, the impact of cyber attacks on their business, and the resulting loss of revenue, they will spend more on security.[8]

In addition, policymakers are becoming more concerned with the effect of cyber breaches on individual privacy, and are starting to enforce safer data management. The General Data Protection Regulation (GDPR) that will take effect from May 25, 2018, targets any business that holds private information on EU residents, and may lead companies to handle personal data with a higher standard of care.

Furthermore, we have identified that the global cybersecurity industry is focusing its efforts on two methodologies to better handle and mitigate these cyber risks:

- Executing basic security measures in a more effective way, including extensive use of encryption in the network and data stores, security orchestration, better incident response, and improved software patching management.
- The development of disruptive security solutions using artificial intelligence (AI) and machine learning to scale-up the process of detection of malicious activities over the network and at endpoints, and effect automatic incident response. AI has been used in the cybersecurity industry for several years, but only now is being adopted into off-the-shelf security products. Other technologies that security vendors are expected to adopt over the coming years are blockchain-based solutions and quantum computing.

> *"In today's hyper-connected world, internet-enabled devices, such as industrial machinery and cars, are more susceptible to cyber attacks than ever before. This digital transformation is expanding the potential attack surface and increasing the potential damages these cyber attacks might inflict. Complex cyber threats, once thought to be science fiction, are now a gloomy reality for major enterprises, manufacturers and service providers around the world, which are faced with a decision whether to acquire top talent and innovative solutions or risk their most valuable assets."*
>
> Arik Kleinstein, Co-Founder & Managing Partner, Glilot Capital Partners

4 According to a definition by Symantec, APT (Advanced Persistent Threat) "uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term."

5 Breach Level Index by Gemalto.

6 The Internet of Things: A movement, not a market, IHS Markit (2017).

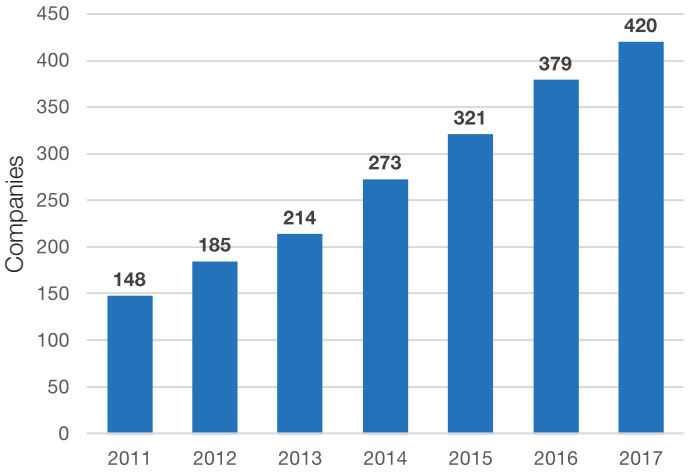
7 Mirai is a type of malware commonly found in IoT devices, converting them into a network of controlled bots. On October 2016 this network of controlled devices was used to execute a DDoS attack targeting the DNS provider Dyn and caused large internet services including Twitter, Amazon and Netflix to be unavailable.

8 Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017, Gartner, Inc. (2017).

THE ISRAELI CYBERSECURITY INDUSTRY

As the demand rises for innovative cybersecurity solutions, the Israeli cybersecurity industry continues to be at the forefront of the war against cybercrime. By the end of 2017 there were 420 active cybersecurity companies in Israel (70 new), and 30 multinational companies from various industries, including automotive systems, financial institutions, professional services, and internet, that have cybersecurity-related R&D centers in Israel.[9] A large cadre of highly trained and experienced professionals with a background in cyber technology , combined with a rapidly rising demand, and the spirit of innovation and entrepreneurship, comprises the strong foundations of the Israeli cybersecurity industry.

Figure 1: Active cybersecurity companies



In 2017, the Israeli cybersecurity industry continued to be vibrant, dynamic and attractive to both investors and multinational companies. 70 start-ups were founded during 2017, a slight decrease from the 84 that were founded in 2016. Several new international players entered the local industry, and opened R&D and cyber innovation centers, including Symantec, TD Bank, Renault, Daimler AG, and Harman. Over the past year, there were also several international collaborations between large Israeli companies and various governments, including Cyberbit's training centers in Japan and Maryland, CyberGym's training center in Australia, and a contract to set up a national cyber center between The Israeli Cyber Companies Consortium (IC3) and a Latin American country.

Additionally, the establishment of the Israel-US bilateral cyber working group, led by White House cybersecurity coordinator Rob Joyce, and the National Cyber Directorate, indicates the high level of trust in the Israeli cyber industry and talent pool. The international collaborations and knowledge-sharing initiatives built over 2017 strengthen Israel's position as a key player in the global war against cybercrime.

The remaining sections of the report concentrate on analyzing trends and performance of the Israeli industry in terms of investments and exits during 2017.

> *"We see a strong correlation between the global trends in cyber security and the Israeli cyber ecosystem, while most of the activity in our industry is still being led by the US and Israeli ecosystems. The cyber security market is driven by a combination of technical skills and innovation, with a good alignment to the main trends within the wider IT landscape such as the migration to Public Cloud, artificial intelligence and automation."*
>
> Alon Kantor, VP Business Development, Check Point Software Technologies

9 All figures regarding the Israeli high-tech industry are calculated according to Start-Up Nation Finder statistics, unless otherwise stated.

Strategic collaboration with Israeli innovation

As the Israeli cybersecurity ecosystem becomes one of the clear leaders of the global industry, multinational companies are increasingly making the strategic decision to engage. Leading multinationals are collaborating with early and late-stage Israeli cybersecurity start-ups, fully realizing that their cutting-edge developments and ideas answer the challenges of today and tomorrow. Similarly, many large security vendors are attracting Israeli talents and ideas, to develop future products. Start-Up Nation Central, an authoritative source on the Israeli innovation ecosystem, over the past two years has helped dozens of multinational CEOs, CIOs and CISOs to realize the potential of collaboration with the local ecosystem, learn various ways to connect, and take their first steps in Israel. Collaborations take several forms:

Affiliations – multinational corporations organize, participate and sponsor conferences, hackathons, challenges, competitions and meetups held in Israel, as a first step to engage their organization around the strategic decision for a more extensive collaboration with the Israeli ecosystem. For example, international partners from various industries take an active part in the major cybersecurity conferences held in Tel Aviv throughout the year.

Strategic partnerships – collaboration with local players including investors, large companies, start-ups, and academia. The main purpose of these partnerships is to gain knowledge and increased familiarity with innovations in the cybersecurity domain, which could result in investments and POCs, commercial agreements, joint ventures and so on. The multinational companies do this by partnering with existing accelerators or by operating accelerators themselves, investing in local VCs that specialize in cybersecurity, participating in design partnership platforms (such as Team8's Global Cyber Syndicate), and engaging a local scout.

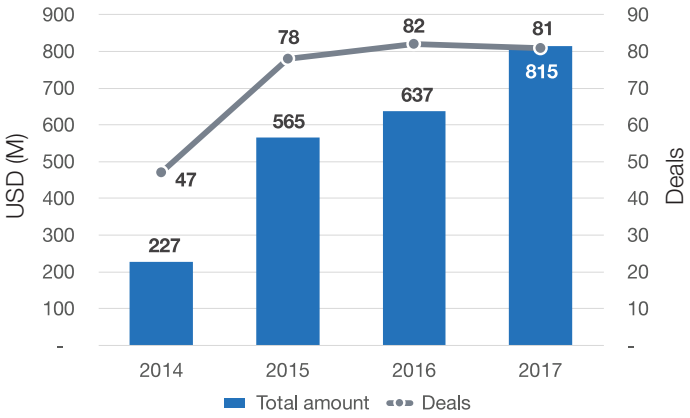
Local presence – certain multinational companies that identify the unique added value of a presence in Israel, have decided to invest resources in establishing a range of extensive operations in Israel. Security vendors, including Palo Alto Networks, Proofpoint, Gemalto and others, are fairly typical examples. Other software vendors and internet services, including Paypal and Microsoft Azure, also placed their security R&D centers in Israel. In 2017 we saw various manufacturers establish cyber R&D centers, including Mercedes-Benz. Most of those companies manifested their activity in the Israeli cyber ecosystem through the acquisition of start-ups to facilitate the initial recruitment of talent, although certain companies made the decision to open their centers from scratch. Alternative types of activity in Israel include corporate VCs investing in cyber technologies (Singtel Innov8), acceleration programs, design partnerships (Citi Ventures) and cybersecurity innovation labs (TD bank).

FINANCING IN 2017

Israeli cybersecurity companies raised a total investment sum of $815M in venture capital money and private equity, a record-breaking amount for the third year in a row, exceeding 2016 investments by 28%. In comparison to the global cybersecurity industry, the Israeli industry comes second only to the US, having taken 16% of the overall cyber investments worldwide, slightly increasing its share from 2016 (15%).[10] This impressive amount was raised over 81 investments (roughly the same as in 2016). The frequency of investments declined towards the end of the year, similarly to 2016.

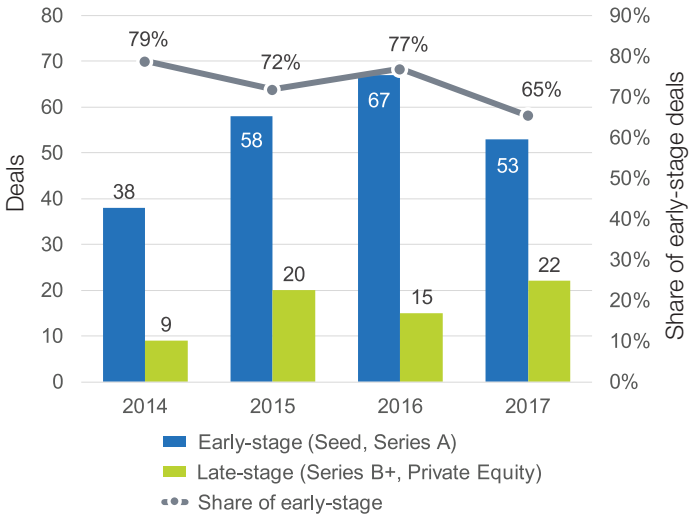
Three large deals accounted for 40% of the amount: Skybox Security ($150M), Cybereason ($100M) and SentinelOne ($70M), representing three of the five all time largest investment deals in Israeli cybersecurity.

Figure 2: Israeli cybersecurity investments



Upon taking a closer look, we can identify noteworthy changes that happened in 2017. While the majority of the investments were early-stage investments (Seed and Series A), their share declined from 77% in 2016 to 64% in 2017. This was due to a significant drop in the number of early-stage investment deals and an increase in late-stage deals (see Figure 3). The drop in early-stage investments aligns with the global trend of reduction in early-stage venture capital activity.[11]

Figure 3: Number of investments - early vs. late stage



10 Based on Pitchbook data and Start-Up Nation Finder.

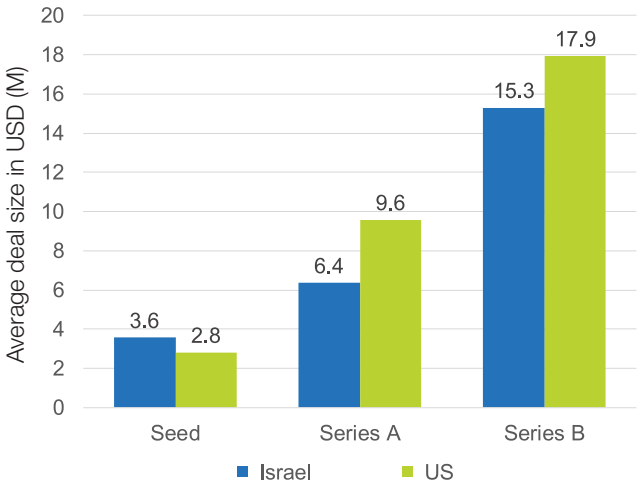
11 There's an implosion of early-stage VC funding, and no one's talking about it, TechCrunch (2017).

The average size of investment deals increased in 2017, particularly for seed rounds: $3.6M on average, almost twice the size of seed rounds in 2016. The increase in size of early-stage funding rounds is consistent with Start-Up Nation Central's earlier report, suggesting that the Israeli high-tech industry is becoming more mature.[12]

The increase in late-stage investments (Series B+ funding) in 2017 also indicates the increasing maturity of the Israeli cyber industry, as Israeli cybersecurity companies gain more opportunities to grow, become profitable, and position themselves as industry leaders. Companies such as SentinelOne, Cybereason, Checkmarx, and Cato Networks are good examples of the layer of pre-growth and growth companies that raised considerable amounts of funding for scaling up size and operations.

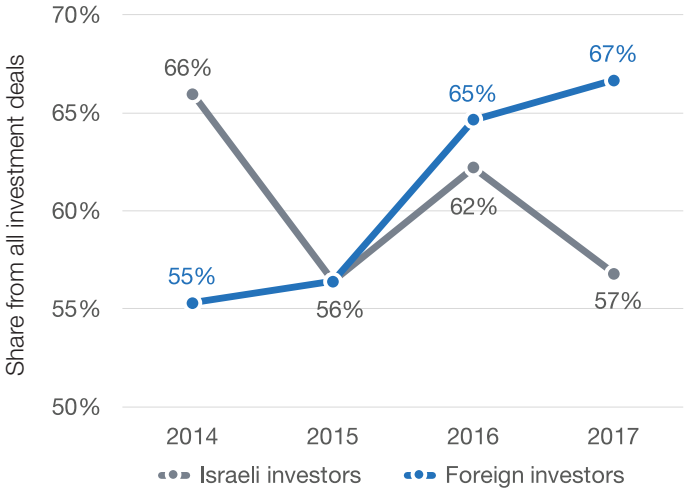
The average size of investments in Israeli cybersecurity companies in 2017 stands at $10.8M, 26% higher than the 2016 average. In addition to three large deals (over $50M), some of this growth is due to larger seed investments, as mentioned previously. In comparison to the US cybersecurity industry,[13] Israeli companies were relatively more successful in raising larger seed investments (see Figure 4). The investment amounts that early-stage start-ups receive is one indicator of the comparative advantages of the Israeli industry, which is characterized by high levels of innovation, and the development of deep and disruptive technologies.

Figure 4: Average deal size in 2017



When analyzing investors in Israeli cybersecurity, one notices a significant increase in the presence of non-Israeli investors. In 2017 there were more funding deals in which international investors participated than those in which Israeli investors played a part – further proof of the growing recognition of Israel as a global leader in cybersecurity.[14] Concurrently, we saw slightly less activity of Israel based investors, including angels. Among the most active investors in 2017 were YL Ventures and JVP Cyber Labs, each with four investments in cybersecurity, and Glilot Capital Partners, Maniv Mobility, Blumberg Capital, and Microsoft Ventures, each with three investments.

Figure 5: Investor types



12 In Israel, Early-Stage Venture Slump Is a Good Sign, Ha'aretz (2017).
13 Based on Pitchbook data and Start-Up Nation Finder.
14 Israeli and international investors can participate concurrently in the same funding deals.

EXITS

Fourteen exits (first-time deals, including IPOs and buyouts) took place during 2017, of which twelve totaled $1.4B, while the valuation of another two has not been disclosed. This exceeds the number and value of exits by Israeli cybersecurity companies in 2016. Of the fourteen exits, eleven were acquisitions. One of the exits was an IPO by Forescout on NASDAQ, breaking the long absence of NASDAQ IPOs by Israeli cyber companies. The large increase in the value of exits was due to the acquisitions of Argus Cyber Security (by Continental for an estimated $450M), Skycure (by Symantec for $280M), and Fireglass (by Symantec for $250M).

Earlier in this report, we mentioned the growing investment in late-stage companies, creating a more significant layer of growth-stage cybersecurity companies in Israel. Some of these companies will be targeted by the largest internet, software, and security companies, as well as by the connected devices manufacturers (including automotive and control systems), and we therefore predict that the acquisitions activity in Israel will intensify in 2018. At the same time some companies will prefer to remain private and even consider an IPO.

Figure 6: Exits 2014-2017

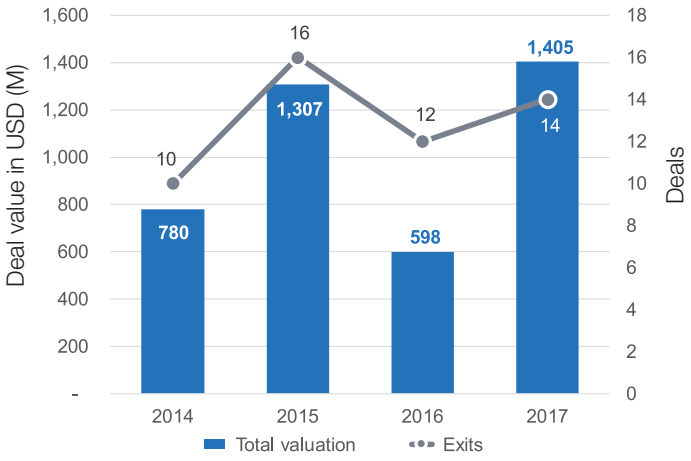
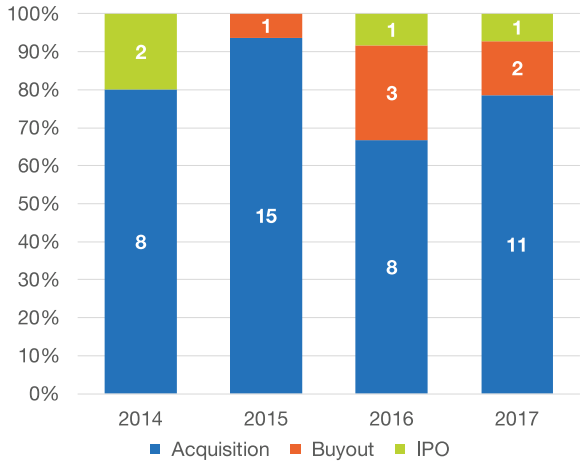


Figure 7: Exit types

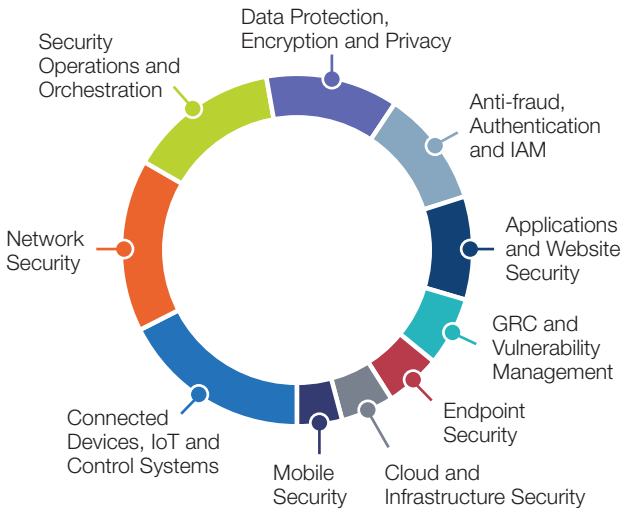


SUBSECTORS

In this section, we partition the cybersecurity sector into specific segments, identifying trends regarding how the Israeli cyber sector addresses global challenges. We classify cybersecurity companies as follows:

- **Data Protection, Encryption and Privacy**
- **Network Security:** prevention of APT, visibility solutions, isolation and deception (for the enterprise network).
- **Endpoint Security:** all anti-malware and anti-ransomware solutions, and Endpoint Detection and Response (EDR).
- **Cloud and Infrastructure Security:** solutions for securing 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)
- **Applications and Website Security:** security measures for software and web applications, including code review, bot detection, 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:** 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 incident response, forensics, SIEM, alert management, threat intelligence, and penetration tests.
- **Mobile security**

Figure 8: Active companies by subsector



SUBSECTOR TREND ANALYSIS

In the following section, we discuss subsectors in which a positive trend was identified:[15]

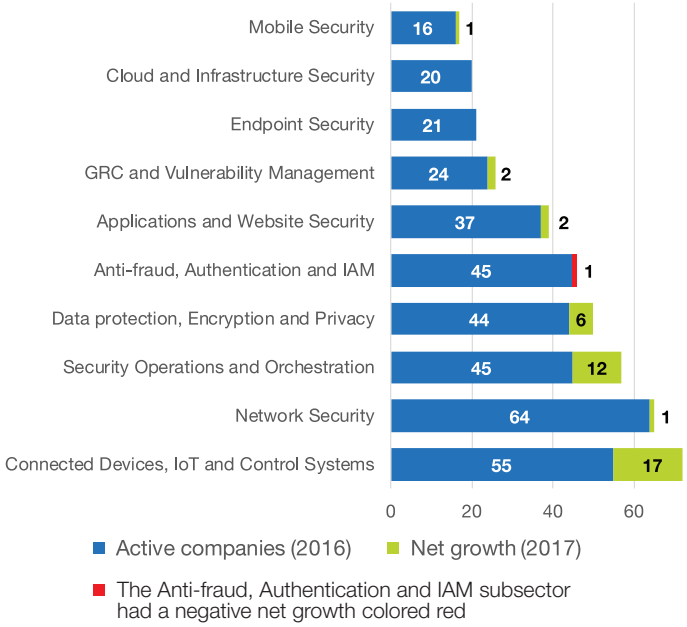
- **Connected Devices, IoT and Control Systems**
- **Security Operations and Orchestration**
- **Endpoint Security**
- **Cloud and Infrastructure Security**
- **GRC and Vulnerability Management**

Negative trends were identified in the subsectors of Network Security and Anti-fraud, Authentication and IAM.

POSITIVE TRENDS

In terms of the number of companies founded, the most dominant subsector is **Connected Devices, IoT and Control Systems** – representing the growing awareness of the risks of severe cyber attacks in this domain. There are 72 active companies in this subsector (17% of the Cybersecurity sector). For the first time, **Connected Devices, IoT and Control Systems** is the largest subsector, exceeding **Network Security**. Twenty companies were founded in this subsector during the past year, equaling 30% of all companies founded in 2017. This subsector enjoyed seventeen investment deals in 2017. Within this subsector, the security providers for connected cars and automotive systems had a very impressive year, with Upstream Security and Karamba Security raising $11M and $12M respectively, and Argus Cyber Security being acquired by Continental for an estimated $450M. Additionally, within the domain of security for industrial control systems, SCADAFence raised $10M and NextNine was acquired by Honeywell. Furthermore, a new segment identified this year was security solutions for healthcare providers' networks and medical devices, with four new companies founded in 2017, and other established companies offering unique solutions for healthcare providers' use cases.

Figure 9: 2017 net growth by subsector



Another growing subsector is that of **Security Operations and Orchestration**. As time progresses, the challenges of running security operations become increasingly severe,[16] and comprise both the rising number of incidents as well as the difficulties in employing security professionals.[17] Several Israeli companies, including Demisto, IntSights, SafeBreach, and many others, offer innovative solutions for SOC (Security Operations Centers) teams and IT management, that make such tasks as monitoring, incident response, forensics, penetration testing and threat intelligence more efficient and even automatic. Twelve new companies were founded in 2017, and 14% of companies in the subsector raised funds (see Figure 10).

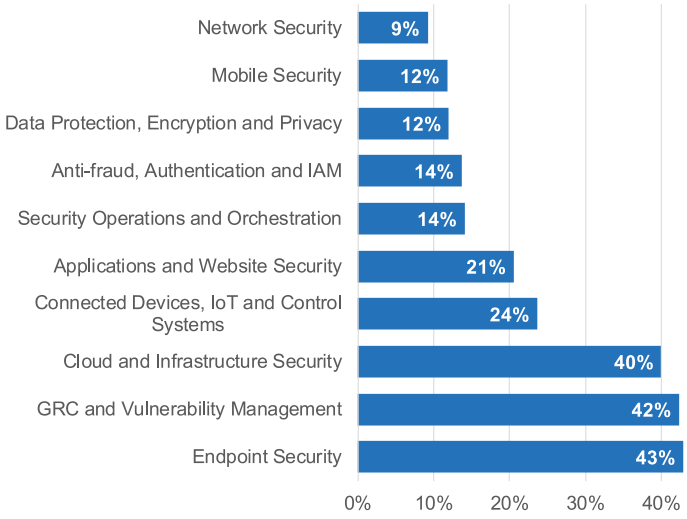
The **Endpoint Security** subsector did not see any new companies founded in 2017, however 43% of the existing companies had an investment deal: the two largest being Cybereason, ($100M), and SentinelOne ($70M). Some companies in this category aim to disrupt traditional anti-malware solutions by introducing Endpoint Detection and Response (EDR), utilizing machine learning and anomaly detection capabilities to identify malicious activities (such as ransomware attacks) at the endpoint.

Other subsectors that enjoyed a successful year in terms of investments include **Cloud and Infrastructure Security**, with no new companies established, but considerable financing activity (four deals of over $10M: Twistlock, Guardicore, Dome9, and Aqua Security), and **GRC and Vulnerability Management**, with 42% of companies raising funds, reflecting rising global concern about GDPR and challenges faced by cyber insurers in the underwriting process.

NEGATIVE TRENDS

Network Security, the second largest subsector, faced a stagnation with only three new companies being founded in 2017, plus a very low 9% of companies succeeding in raising investments. **Anti-fraud, Authentication and IAM** (Identity and Access Management) also had an unimpressive year, with more companies being closed than founded, and only 14% of the remaining companies succeeding in raising funds.

Figure 10: Financing activity per subsector



15 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.

16 The State of Incident Response 2017, Research conducted by Virtual Intelligence Briefing (VIB), sponsored by Demisto (2017).

17 Cybersecurity Jobs Report, Herjavec Group and Cybersecurity Ventures (2017).

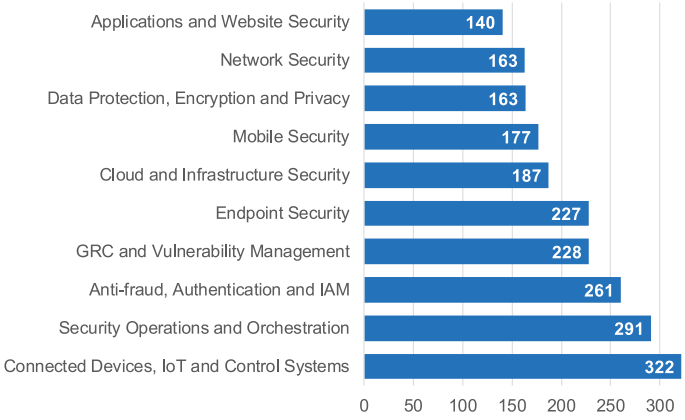
START-UP NATION CENTRAL AND THE CYBERSECURITY SECTOR

Start-Up Nation Central is committed to helping global corporations engage with Israeli innovation, which will generate significant value for them, while creating business opportunities for the Israeli innovation sector, and for cybersecurity in particular. Over the past few years, we have hosted senior executives from dozens of giant multinational corporations, senior government and NGO officials, and investors, and introduced them to the most relevant people and technologies. These highly customized and expertly-curated visits are carefully prepared to identify and address the corporations' most pressing challenges and needs. In the process, Start-Up Nation Central has connected more than a hundred Israeli cybersecurity companies with potential customers and strategic investors. Some of these connections have already evolved into POCs, investments, and strategic collaborations, while in many other cases the dialogue continues.

Analyzing the fields of interests expressed by our clients, we can infer the challenges facing global corporates in 2017, in securing the cyber domain. Approximately half were interested in IoT security solutions, either for their own corporate networks, the OT (Operational Technology) networks, or for their customers, reflecting a growing interest in the subject in comparison with 2016. We detect increased interest in solutions for security operations (threat intelligence, incident response, SIEM integration and so on), as well as in risk management and compliance domain, driven by the introduction of the General Data Protection Regulation (GDPR), which comes into effect in May 2018. The clients showed less interest in network security solutions in 2017, which matches the industry investment trend identified in the previous chapter of this report. Financial institutions hosted by Start-Up Nation Central were mostly interested in anti-fraud and authentication solutions for mobile devices.

Another way in which we create opportunities is through Start-Up Nation Finder, our online platform mapping Israeli innovation, where anyone can locate information on all cybersecurity companies and investors in Israel, and contact them directly. During 2017, the term "cybersecurity" was the most popular search in the platform, with Automotive, Fintech and IoT as the most popular subsequent searches (when combined with "cybersecurity"). On average, cybersecurity company profiles had 220 unique visits (50% of which originated from outside Israel), higher than any other sector in Finder. Figure 11 presents the average number of unique visits per profile by subsector.

Figure 11: Average of unique visits per profile



Profiles in the following subsectors had the highest average number of unique visits: **Connected devices**, **IoT and Control Systems**, **Security Operations and Orchestration**, and **Anti-fraud, Authentication and IAM**. Profiles in **Applications and Website Security** had fewer visits on average.

2018 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 2017.

In the pipeline for 2018:

Cybertech TLV
(January 29–31, Tel Aviv)

Israeli Cyber Security Showcase
The Israeli Delegation to the RSA Conference, hosted by the Israeli Economic Mission and the Israeli Export Institute
(April 16–20, San Francisco)

Cyber Week 2018
held by Blavatnik Interdisciplinary Cyber Research Center (ICRC) and the Yuval Ne'eman Workshop for Science, Technology, and Security
(June 25–29, Tel Aviv)

Israel Cyber & HLS 2018
held by The Israel Export and International Cooperation Institute
(November 12-15, Tel Aviv)

ABOUT START-UP NATION CENTRAL

Start-Up Nation Central is an Israel-based non-profit that serves as a gateway to Israeli innovation. An authoritative source on the Israeli innovation ecosystem, the organization leverages its in-depth knowledge to help identify the best solutions for demanding corporate and government challenges. Start-Up Nation Central is a non-profit organization, funded entirely by philanthropy, fueling Israel's innovation engine, convening thought leaders to help shape policies which support it, and enabling companies and technologies to grow. Start-Up Nation Central designs highly customized engagements for business leaders, governments, NGOs, and academic institutions across the globe, connecting them to Israeli problem-solving innovations that address their critical needs. It has curated the largest and most up-to-date innovation discovery platform of Israeli companies, R&D centers, investors and academics, (Start-Up Nation Finder), which provides accurate information on more than 5,500 companies across dozens of industries.

To read Start-Up Nation Central's Cybersecurity Report 2016, see **http://bit.ly/2D12ARR**

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 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. Investment 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.

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

START-UP
NATION
CENTRAL