DECALIA
INVESTMENT FUNDS

INVESTMENT INSIGHTS

March 2022

CYBERSECURITY
THE HOTTEST AND MOST DANGEROUS AREA TO INVEST

CONTENT

- Antivirus
- The Corporate Security Castle is dwindling
- The problem is you
- How do we secure alpha?

Written by Quirien Lemey, Co-Lead PM of DECALIA Sustainable SOCIETY

CYBERSECURITY

THE HOTTEST AND MOST DANGEROUS AREA TO INVEST

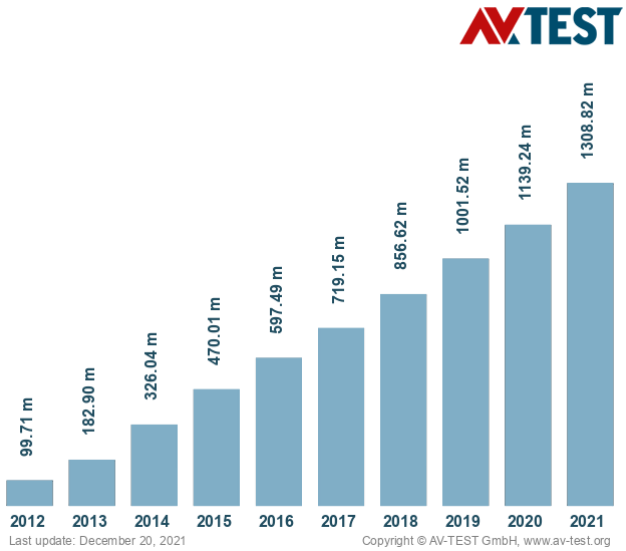
In 1999, 15-year-old James Jonathan was able to hack and shutdown NASA's computers for 21 days. August 2013, account information of more than three billion of Yahoo customers had been accessed by a hacking group, in what is still one of the largest cybersecurity hacks of all time in terms of users impacted. WannaCry, one of the biggest ransomware attacks of all time, took place in 2017, and affected over 230,000 computers in more than 150 countries. This outbreak had a massive impact across several industries. A third of NHS hospital trusts were affected by the attack. Even ambulances were reportedly rerouted, leaving people in need of urgent care. It was estimated to cost the NHS a whopping £92 million after 19,000 appointments were canceled as a result of the attack. A few weeks later, a malware called NotPetya wreaked havoc on 7000 companies globally. It locked access to systems that A.P. Moller-Maersk uses to operate shipping terminals all over the world and took two weeks to fix and cost the Danish shipping giant $200 million to $300 million. The list just goes on and on. As can been seen from the picture below, the amount and severity of global attacks are increasing over time.

Given our society is becoming increasingly digitized and the number of connected devices exploding, we believe this trend will only continue. Cybersecurity is one of the biggest challenges our society faces in the years to come. Companies worldwide face not only reputational risk when being hacked but also business disruption, IP theft, heavy repair costs and even fines by governments. Nations are increasingly engaging in cyberwars as is recently painfully demonstrated by Iran and Israel, who widened their cyberwar to target civilians on a large scale. Iran accused Israel of being behind a cyberattack on the country's gas stations, knocking them out of service for a week. Days later, an Iranian-linked hacking group, Black Shadow, targeted an Israeli hosting company, temporarily shutting down a number of websites and stealing user data from "Atraf," an Israeli LGBT dating site. Concurrent with the increase in the number of cyberattacks, the number of listed cybersecurity companies have also increased dramatically in the past decade, in our estimates growing to a combined market cap of more than $400bn. In what follows we look at how cybersecurity is evolving, look at some key players and what investors should pay attention to.

Antivirus

The most familiar type of cybersecurity is of course the antivirus software like Norton, Trend Micro, McAfee. Once ubiquitous, traditional endpoint security software has seen a sharp decline in popularity due to its limited protection capacity. Legacy solutions rely on databases of signatures, unique values of code that are associated with specific types of malware, in order to identify and prevent future attacks of similar type. These solutions are limited by nature as they can only prevent against attacks that use malware that has been previously identified and stored in the database. Already many years ago it became clear that legacy approaches were failing, as signature databases could not be updated at the same rate that new malware was being created (see graph below). It is almost impossible to catalog the hundreds of thousands new malware variants that emerge each day.

Total malware



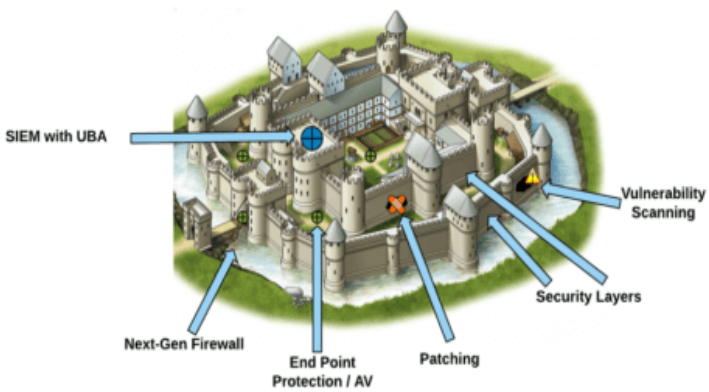
It is due to this failure we have seen new next generation vendors come to the forefront which use machine learning and artificial intelligence to help organizations prevent against unknown, or what is referred to as zero-day attacks. But the so-called Endpoint Detection and Response (EDR) market goes a step further from prevention to also detect and respond to malware that has already made its way onto the endpoint. Crowdstrike and SentinelOne are two listed providers of next generation EDR solution with a cloud native platform. Although one can theoretically make money with any stock we always try to avoid disrupted incumbents. Although the anti-virus space is no different than any other space in software where the incumbents are moving towards cloud native solutions to better compete, it is also no different that it typically pays to stick with the cloud native disrupters… The flipside is the typical high valuation these companies tend to trade on. For this particular market we would also avoid exposure to consumer end markets as less and less individuals tend to pay for an antivirus and Microsoft even incorporates their antivirus into their Window software. We do like the corporate end market as data continues to proliferate and this software helps customers protect workloads running on a variety of endpoints including laptops, desktops, servers, virtual machines, and IoT devices across on-premise, hybrid, and cloud environments.

CYBERSECURITY

THE HOTTEST AND MOST DANGEROUS AREA TO INVEST

In The Corporate Security Castle is dwindling

Traditionally enterprises organized their security as a typical castle-and-moat framework. This means they consider the headquarters as the castle where, once inside, anyone can freely roam the premises wherever they want. Outside the castle nobody is trusted and hence a moat is constructed to keep out unwanted visitors. This moat is the typical firewall product in the security world. These are appliances, meaning software bundled on hardware, servers, to host this software. Some traditional firewall providers are Cisco, Checkpoint and Palo Alto Networks. These firewalls can then be complimented by many additional solutions such as vulnerability management (Tenable, Qualys are some listed companies in this space), endpoint protection (discussed in the article above) and SIEM (Security Identification and Event Management, Splunk is the leader here). Employees outside the headquarters that need to connect to the internet or to internal applications are then typically connected via VPN (Virtual Private Network) or MPLS (Multi-Protocol Label Switching) technology. All traffic from remote employees or corporate branches would be rerouted back to the headquarters where all security checks and company policies can be applied.



Source: atmosera.com

Just like cloud native players Salesforce.com and Workday (and many more later on) entered and disrupted the traditional ERP software world dominated by SAP and Oracle more than a decade ago, this is happening all over again in the cybersecurity world today. Cloud native cybersecurity players like Zscaler and Cloudflare are disrupting traditional players and traditional architectures (more on this below). As it turns out, cybersecurity can be provided via the cloud, removing the need to buy expensive hardware. Some would even argue cloud-based security can be even more secure than traditional on-premise appliance-based security. On top of this, employees are increasingly outside the headquarters and using more and more devices to do so (think phones and iPads), rendering the castle-and moat approach increasingly inefficient, expensive and cumbersome. Evidently, this evolution got a massive boost from the Covid pandemic as employees suddenly had to work from home proving corporate IT departments with security and performance headaches.

The problem is you

It is very funny how many people think "how stupid one must be to open that mail or click on that link", referring to an obvious email scam of some sorts. However, according to the Verizon 2021 Data Breach Investigations Report, credentials are the primary means by which a bad actor hacks into an organization, with 61 percent of breaches attributed to leveraged credentials. Hackers' methods and tools are often very creative and sophisticated, but their success is the result of the "human element." We reuse the same passwords over and over, we access corporate applications on unprotected personal devices, and we refuse to adopt multi-factor authentication, and yes, we have all clicked on mails we never realized are malicious. Next to the move to cloud native securities, we also believe there are areas within cybersecurity that will grow in importance the next couple of years. One of these areas is Identity and Access Management, software used to manage user identities and regulate user access within an organization. Okta is the market leader in the Single Sign- On segment, and Sailpoint and CyberArk are best-of-breed vendors in the Identity Governance and Privileged Access Management segments respectively. Ping Identity and Forgerock are more recent IPOs in this area.

Given that humans are the most commonly exploited attack vectors, another area we believe will see increased importance in the years to come is security awareness software, that enables organizations to train employees to identify and prevent social engineering attacks. KnowBe4 is a recent IPO and market leader here.

Given that companies are becoming increasingly digital, utilizing hybrid and multi-cloud environments, adopting more cloud-based applications, dealing with a proliferation of devices and having employees that are increasingly operating outside the core corporate network, this has all given rise to a new set of buzzwords. Zero Trust Security and SASE (Secure Access Server Edge) are two examples of concepts that most companies mentioned in this article frequently speak of. Instead of assuming everything behind the corporate firewall is safe (inside the castle), the Zero Trust model assumes breach, and the main concept behind is "never trust, always verify". The Zero Trust framework requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration before being granted access to applications and data.

CYBERSECURITY

THE HOTTEST AND MOST DANGEROUS AREA TO INVEST

Effectively what we are seeing is a move away from the traditional castle and moat architecture to Zero Trust Architecture. A more recent buzzword is SASE, which boils down to the convergence of network and network security services into one, mostly cloud delivered service. Zero Trust is seen as an integral part of this. We view SASE as the current ultimate model where companies need to transition to. Given the hype around SASE, the number of vendors claiming to offer SASE has increased significantly, but not every vendor claiming to offer a SASE product currently delivers all of the required and recommended SASE capabilities, and the capabilities offered by different vendors are not at the same level of functionality and maturity.

So how do we secure alpha?

For potential investors, one must try to identify the winners and losers in these transitions. The complexity not only lies into understanding the many different technologies, there's also the existence of hybrid environments. For example, we prefer to avoid exposure to traditional on-premise firewalls, but this segment is still a growing segment. Although companies are moving towards zero trust and cloud-based security architectures, there is still an increasing amount of data flowing through traditional firewalls, increasing the need for these products as well... There is a massive installed base (read investments in hardware and software) which is not going anywhere anytime soon. On top of this, products and companies are evolving, to give just one example, Palo Alto is now providing a cloud-based version of their firewall... And to make things even more frightening, technologies themselves rapidly evolve and rendering older ones obsolete.

At Decalia cybersecurity is one of the seven main themes of our Sustainable SOCIETY fund (the S stands for security). We approach our investments in cybersecurity through a research and expertise driven, diversified, barbell approach. We invest in the most disruptive and innovative, cloud-native business models such as Zscaler. The issue with these companies is that they are typically expensive, so we also invest in less expensive, but still well positioned companies. On top of this, we apply a proprietary subsector based ESG framework to all our themes and subthemes to better understand and avoid risks associated with our investments.

Written by Quirien Lemey,
Co-Lead PM of DECALIA Sustainable SOCIETY