PEEL HUNT

MARKETING COMMUNICATION

13 January 2020

Technology

ANALYSTS

Damindu Jayaweera
+44 (0) 20 3597 8657
damindu.jayaweera@peelhunt.com

James Lockyer
+44 (0) 20 7418 8940
james.lockyer@peelhunt.com

Oyvind Bjerke
+44 (0)20 7418 8951
oyvind.bjerke@peelhunt.com

Redefining the future of cybersecurity

An arms race to detect harmful traffic has reduced the usability of essential business functions such as e-mail, web browsing and content sharing. In wanting to balance the inversely correlated security and usability in favour of better productivity, enterprises have become resigned to a state of insecurity. An approach termed 'Hardsec', which uses hardware to extract and verify harmless traffic, has the potential to overhaul this status quo radically. Defining what is 'good' is easier than trying to identify the ever-changing 'bad'. Doing so using simple hardware instead of complex software greatly reduces the risk of compromise.

Threat detection has been the focus of many cybersecurity advances. This has evolved from just being able to identify known-knowns (eg, virus signatures and website black-lists) to being able to identify known-unknowns (eg, sandboxing and behaviour analytics). Enterprises, however, continue to suffer attacks from unknown-unknowns (ie, threats we didn't even know that we don't know!). Between better-resourced attackers, ever-increasing threat surfaces (eg, IoT) and perennial human error, an easy-fix has proved elusive.

What if we focus on extracting and verifying harmless traffic instead of trying to detect harmful traffic? Conversely, this means all traffic is treated with zero-trust. The definitions of popular mark-up languages (eg, html and Word) are well understood, making it easy to detect harmless traffic. The first step is to 'transform' all relevant traffic into easily 'verifiable' formats (eg, a browsing session can be turned into a video stream or a complex Excel file can be rid of its unnecessary active content). A verification engine can then test for the content's purity before passing on to the user. This 'transform and verify' methodology is already in use within the UK's national security apparatus.

We can then solve the 'who polices the police' problem using hard-to-hack hardware. Simply implementing the aforementioned, conceptually elegant 'look for the good instead of the bad' methodology still leaves some attack-vectors open. Think of an international border that switches from identifying potential threats to only allowing pre-vetted people through. Despite the ease of management, the border control officials can be compromised. In cybersecurity, an Achilles' heel is typically the software implementation. This risk is reduced by using computationally simple hardware like FPGAs to implement the verification engine. This reduces the risk of compromise in the verification phase of the 'transform and verify' methodology. The use of hardware is the *secret sauce* of the methodology, and underpins pioneering implementations by the likes of Garrison and Deep Secure. Known as 'Hardsec', it opens an enterprise market worth cUS$7bn. In a world where every internet user is protected by 'Hardsec', the market could be worth a quarter-trillion dollars pa!

This document must be treated as a marketing communication for the purposes of Directive 2014/65/EU as it has not been prepared in accordance with legal requirements designed to promote the independence of research; and it is not subject to any prohibition on dealing ahead of the dissemination of investment research.

The problem with software

Much of cybersecurity innovation has been about advances in software. The progress here has been rapid, from traditional solutions that only dealt with known-unknowns (eg, signature-based malware detection) to a new generation that can deal with known-unknowns (eg, behavioural anomalies in the network using machine learning). To a large degree, these solutions have increased security while lessening the impact on usability. *However*, there remains a major weakness in this progress. Software, by its very nature, is burdened by:

- **Complexity –** The increasing complexity and size of code is making software more error-prone than ever. Think of any software product that you use, and how the necessity for constant 'updates' has grown over the years.
- **'Componentisation' –** Very few applications are built from the ground up, as it makes little sense to reinvent all the wheels. The result is the pervasive use of third-party components that are largely outside the OEM's control.
- **Ecosystems –** Any enterprise-grade software today sits within an ecosystem of other software, making for a higher likelihood of unstable, unpredictable and unintended interactions.
- **Malleability –** By its very nature, software encourages developers constantly to add features in through updates, potentially introducing new vulnerabilities to a secure product. This malleability also makes it extremely difficult to prevent completely software being modified post deployment.

This inherent weakness in software also means that software-based cybersecurity platforms are vulnerable by design, creating in essence the 'who polices the police?' problem. Unlike many other types of software, cybersecurity software, by necessity, has greater access to the deepest levels of an enterprise's IT systems. This means a piece of compromised cybersecurity can be one of the most dangerous attack-vectors.

Hardware to the rescue

While the boundary between hardware and software continues to blur ('software is eating the world'), hardware will always have 'some' advantages over software. Why some? As the reader will be aware, generic hardware designed for 'one-size-fits-all' functions will have vulnerabilities of its own (see Spectre and Meltdown exploits). This is the downside to the increasing complexity in hardware (and all technology). However, if the hardware can be functionally limited by design (as opposed to a CPU that can do 'anything'), the advantage over software can be extended. For example, any exploitable weakness due to design error will be very limited in scope due to the limited functionality.

Limited functionality hardware will likely conjure up images of custom semi-conductor chips that are prohibitively expensive to design and manufacture. This is where advances in technology and scale economies have changed things. For example, FPGAs (field-programmable gate arrays) have unlocked the ability to 'programme' hardware post manufacture, while smartphones have super-charged the economics of specialised hardware (eg, cheap image processing chips). This means we could economically make use of specialist, limited-functionality hardware that can be programmed. If these hardware-based systems can then be physically locked out of any further changes, we can be in possession of hardware-defined cybersecurity solutions that can overcome many of the software disadvantages.

The hardware in Hardsec

The Hardsec approach makes use of aforementioned FPGAs. They are particularly effective in implementing the verification stage. In order for those FPGAs to be secure, one must prevent them from being re-programmed once they have been deployed. Like any chip, these FPGAs have input and output pathways (think of pins in a microchip). However, unlike many chip variants, FPGAs also have a 'management' pathway that is used in programming the FPGA. Once programmed, this pathway can be physically blocked, introducing a physical airgap that prevents the FPGA from being re-programmed.

Take a web browsing session. Instead of sending across all the processing instructions to render a website, which can contain malicious code, its browsing session is rendered into a video stream. In a video stream, each frame is just colour instructions across a dense, two-dimensional grid, which can be verified by a FPGA. Given such a picture contains no processing instructions, it is difficult to think of a scenario in which the stream can be used to attack some security hole in the FPGA. The user will therefore experience the web browsing session as a harmless streaming video session. Commercial implementations have solved the keyboard/mouse interactions required to make the whole thing seamless. The method effectively creates an airgap between the website's instructions and the display of that website via the FPGA verification process that sits in between.

Making the jump from James Bond to 'enterprise' Joe Bloggs

Through the 'transform and verify' process, an enterprise is able to receive data, be they webpages, e-mails or even API calls, that are free from known, unknown and undetectable threats. This is a better balance between zero-trust security and usability. The methodology uses hardware with limited functionality, reducing the attack surface of the process itself. Use of well-entrenched technologies such as FPGAs allows for viable economics. This in essence is 'Hardsec', a methodology that is already becoming standard practice across multiple Western government security agencies worldwide. Companies like Garrison and Deep Secure are in the process of commercialising the methodology for the private sector. We think this foundational technology will be key to achieving a better balance between security and user experience in the enterprise. Even more important is the fact that increasing chunks of a nation's 'critical infrastructure' is today run by the private sector. It therefore becomes important for the private sector to adopt the same methodologies that are being used by security agencies.

Sizing the market

Technology is just a tool. In most cases, despite all the strategic posturing and the marketing buzz, it is treated as a cost rather than an investment. Cybersecurity spending, on the other hand, is thought of slightly differently given the everrising cost of data breaches. With the adoption of GDPR and similar regulations across the world, there is a fear-driven need to spend more to contain these costs.

Reports like 'Cost of a Data Breach Report' from IBM and 'Data Breach Investigations Report' from Verizon are treasure troves of data. Taking insights from those reports for 2019, we estimate that just across 25m Fortune 500 information workers, cost of breaches came to US$100bn. We think the principles behind Hardsec, productised to protect the information workers (eg, Garrison, Deep Secure), could help contain a third of these costs (cUS$33bn). Therefore, we think it is realistic to consider a market opportunity worth a fifth of that (cUS$7bn), implying a 4x return on investment. This is about a third of the investments that today go into securing the border between an enterprise and the wider internet.

Chart 1: Cybersecurity spend to be displaced by Hardsec

Source: Peel Hunt, Gartner (Secure Web Gateway, Secure E-mail Gateway, and Web Application Firewalls Software alongside Firewall Equipment End-User spend), Avast

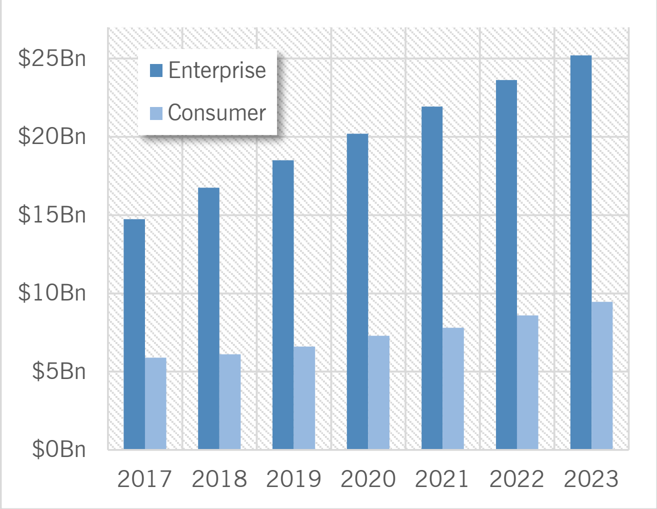
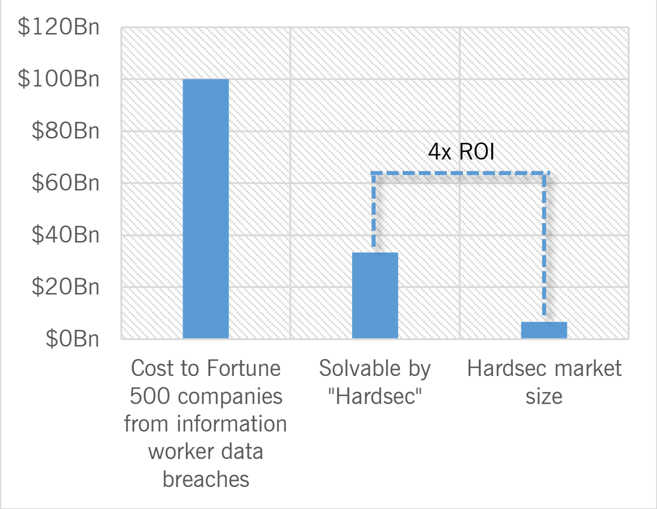


Chart 2: Bottom-up sizing of Hardsec market

Source: Peel Hunt, IBM, Verizon



This is only an estimation of the higher-end enterprise opportunity. We also think that the risk to the consumer, in an era where cyber privacy and security are dominant societal issues, is also great enough to create an opportunity for Hardsec. Here the assumption is that such technology will be deployed not at the consumer end-points, but at access gateways such as the internet service provider (a bit like how content filtering is used today) or cloud content solutions such as Office 365 and Dropbox. If we take Avast's (the world's largest consumer cybersecurity company by installed base) estimate of its addressable market as a guide, this opens up another cUS$7bn (Source: Avast IPO prospectus) opportunity for Hardsec.

The need for government-grade security has never been greater

In 2004 the cybersecurity market was worth US$3.5bn (Source: Cybersecurity ventures). By 2017, it had grown to 30x that size and has been growing at high single digits pa every year since (Source: Gartner). Despite this growing investment, the cost of breaches has also grown at the same rate since 2017

(Source: IBM's 'Cost of a Data Breach Report'). There clearly is a disconnect between current investments in cybersecurity and the continued deterioration of enterprise cybersecurity. In many cases, the enterprises are not even in total control of their cybersecurity estate. For example, there are instances of external technology infrastructure that enterprises rely on being found wanting when it comes to security (eg, ElasticSearch server exposing 1.2bn people).

Despite spending vast sums (JP Morgan alone spends US$600m pa), financial services, a vertical that takes security seriously, was still experiencing major attacks. First American, where a breach hit 885m sensitive financial records, and Capital One, where 106m customer accounts and credit applications were stolen, were notable examples from 2019. The costs of these breaches are also becoming more direct (BA fined £183m, Yahoo US$118m, Uber US$148m, Marriott £99m, Facebook US$5bn, Equifax US$700m, etc) due to new regulations like GDPR.

More worryingly, government-grade attacks are deployed in the consumer-facing cybersecurity space. Allegations include use of WhatsApp by Israel, and the iPhone by China. It will not be long before government-grade attacks go beyond monitoring of citizens and damaging physical infrastructure (Stuxnet targeting Iran's nuclear programme) to direct economically-motivated attacks on private enterprises. There has already been major IP (eg, Philips' medical research, Rio Tinto's prospecting secrets) and financial (eg, US$81m from Bangladesh Bank) theft by government-sponsored hackers. The only way to protect from such government-grade attacks is for the enterprises to adopt a similar security mentality to those of the government security agencies. ***This is perhaps the strongest case for Hardsec; the need to step up from enterprise-grade security that has been a sinkhole for investments to government-grade security, which, at least for now, has mostly kept to its mandate.***

Conclusion

Einstein's definition of insanity is doing the same thing over and over again and expecting different results. This definition can also be used to describe enterprise cybersecurity. This is why we have ended up in a world of increasingly complex, software-based, ineffective threat detection. Hardsec has a differentiated approach to this problem by treating all traffic as harmful (zero-trust). At its heart is a methodology used by the government security agencies to eliminate threats. Doing so using hardware that is harder to hack (FPGAs) reduces the risk of compromise and performance bottlenecks. This could, to start with, rewrite the playbook for established cybersecurity sub-domains such as 'web-isolation' and 'content disarm and reconstruction'. Longer term, it has the potential to deliver the reversal of the cybersecurity arms race in favour of the good guys. The price for doing so can be lucrative. There are 4.5bn active internet users in the world. How much will each of these users on average be willing to pay to adopt a zero-trust stance? Across the West, the average monthly cost of internet access is cUS$50. If they paid US$5/month on top for such safety, the market opportunity for Hardsec could be well over a quarter-trillion dollars!

Recommendation structure and distribution

	Recommendation distribution at 10 January 2020				All research published in the last 90 days	
	Corporate No	Corporate %	No	%	Corporate %	%
Buy	99	83	203	57	86	58
Add	11	9	48	14	9	13
Hold	8	7	79	22	5	22
Reduce	0	0	10	3	0	3
Sell	0	0	9	3	0	3
Under Review	1	1	5	1	0	1

Peel Hunt's Recommendation Structure is as follows:

Buy, > +15% expected absolute price performance over 12 months

Add, +5-15% range expected absolute price performance over 12 months

Hold, +/-5% range expected absolute price performance over 12 months

Reduce, -5-15% range expected absolute price performance over 12 months

Sell, > -15% expected absolute price performance over 12 months

Under Review (UR), Recommendation, Target Price and/or Forecasts suspended pending market events/regulation

NB The recommendation is the primary driver for analyst views. The target price may vary from the structure due to market conditions, risk profile of the company and capital returns

This research material (the "Report") is produced by Peel Hunt LLP, which is authorised and regulated in the United Kingdom by the Financial Conduct Authority ("FCA") and is a member of the London Stock Exchange. The Peel Hunt LLP analysts that prepare such are stated on the Report.

The Report must be treated as a marketing communications for the purposes of Directive 2014/65/EU as these have not been prepared in accordance with legal requirements designed to promote the independence of research. Although Peel Hunt LLP is not subject to any prohibition on dealing ahead of the dissemination of investment research, Peel Hunt LLP applies this prohibition through its internal systems and controls.

The analyst or analysts responsible for the content of the Report certify that:

(1) the views expressed and attributed to the research analyst or analysts in the Report accurately reflect their personal opinion(s) about the subject securities and issuers and/or other subject matter as appropriate. Information that is non-factual, interpretive, assumed or based on the analyst's opinion shall not be interpreted as facts and where there is any doubt as to reliability of a particular source, this is indicated; and

(2) no part of the research analyst's or analysts' compensation will be directly or indirectly related to the specific recommendations or views contained in this research report and, as far as they are aware, there are no relationships or circumstances (including conflicts of interest) that may in any way impair the objectivity of this recommendation, and that where any such relationship, conflict or circumstance exists concerning any financial instrument or issuer to which this recommendation directly or indirectly relates, this has been disclosed. This statement applies equally to any persons closely associated with such analyst.

Peel Hunt LLP has effective organisational and administrative arrangements set up within the firm for the prevention and avoidance of conflicts of interest with respect to research recommendations, including information barriers. For information regarding potential conflicts of interest and the general approach taken by Peel Hunt LLP in relation to conflicts of interest, please contact mar-disclosures@peelhunt.com.

The Report is for the use of the addressees only and is not intended for nor should be disseminated to Retail Customers as defined in Directive 2014/65/EU. The Report is directed at investment professionals, high net worth companies and/or high net worth individuals only in accordance with the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005. Persons who do not meet this description should not act on the Report. It may not be copied or distributed to any other person without the written consent of Peel Hunt LLP and may not be distributed or passed on, directly or indirectly, to any other class of persons, Peel Hunt LLP may in its discretion distribute this document to any other person to whom it could lawfully be distributed by an unauthorised person and without its content being approved by an authorised person.

Each Report has been prepared using sources believed to be reliable, however we do not represent it is accurate or complete. Neither Peel Hunt LLP, nor any of its partners, members, employees or any affiliated company accepts liability for any loss arising from the use of the Report or its contents. It is provided for informational purposes only and does not constitute an offer to sell or a solicitation to buy any security or other financial instrument. While Peel Hunt LLP endeavours to update on a reasonable basis the information and opinions contained herein, there may be regulatory, compliance or other reasons that prevent us from doing so. The opinions, forecasts, assumptions, estimates, derived valuations and target price(s) contained in this material are as of the date indicated and are subject to change at any time without prior notice.

The Report does not constitute a personal recommendation and the investments referred to may not be suitable for the specific investment objectives, financial situation or individual needs of recipients and should not be relied upon in substitution for the exercise of independent judgement. Past performance is not necessarily a guide to future performance and an investor may not get back the amount originally invested. The stated price of any securities mentioned herein is not a representation that any transaction can be effected at this price.

The date and time when the production of the Reports is completed is the date and time stated on the relevant Report. Additionally, unless specifically stated otherwise, the date and time for prices quoted for all stocks mentioned in the relevant Report is the same as that shown on the front page of the relevant Report. For further detail of when any relevant Report was first published, please contact mar-disclosures@peelhunt.com.

For further detail of our forecasts on any stock/company, please contact mar-disclosures@peelhunt.com.

Peel Hunt LLP's methodology for assigning recommendations includes (unless otherwise indicated) the following: market capitalisation, maturity, growth/value, volatility and expected total return. Target prices are derived from variety of valuation methodologies, which include (unless otherwise indicated), but are not restricted to, analysis of market risk, growth rate, revenue stream, discounted cash flow (DCF), EBITDA, EPS, cash flow (CF), free cash flow (FCF), EV/EBITDA, P/E, PE/growth, P/CF, P/FCF, premium (discount)/average group EV/EBITDA, premium (discount)/average group P/E, sum of the parts, net asset value, dividend returns, and return on equity (ROE). All investment recommendations provided are subject to changes in macro-economic information, such as GDP, unemployment and inflation. Micro-economic information about the issuer such as quantitative and qualitative factors may also be taken into account.

The time horizon for both recommendations and target prices is 12 months, unless otherwise stated in the relevant Report. For details of valuation methodologies, please see the relevant pages of each Report or previous Report.

The frequency of updates to Reports is not planned. Analysts endeavour to remain up-to-date on stocks at all times, and generally write regular (but not frequent) Reports. Analysts will usually write in the event of a significant development.

It should be assumed that any Report has been reviewed by the issuer/company for factual accuracy, and that changes will have been incorporated as a result of that review.

It should be assumed that for the purposes of Peel Hunt LLP's business, including Market Making, Peel Hunt LLP may hold 0.5%, or more, of the stocks it provides Reports in relation to. Financial instruments referred to in Reports where Peel Hunt LLP is not a market maker, it may be a liquidity provider and engage in transactions in a manner inconsistent with the recommendations in its Reports.

A list of recommendations made in the past 12 months by Peel Hunt LLP can be requested by contacting mar-disclosures@peelhunt.com.

Peel Hunt LLP, its partners, members, employees or any affiliated company may have a position or holding in any of the securities it researches, or in a related instrument. The Reports are approved for communication by Peel Hunt LLP in the UK and to EEA market professionals who have registered with Peel Hunt LLP to receive such information.

Unless otherwise stated, Peel Hunt LLP owns the intellectual property rights and any other rights in all material shown on the Portal. No part of any Report may be modified, photocopied or duplicated in any form by any means or redistributed, transmitted, published or derivative works created without the prior consent of Peel Hunt LLP. By accepting access to the Portal you agree that you have read the above disclosure and to be bound by the foregoing limitations / restrictions.

Not for onward distribution into the People's Republic of China.

US Disclosure: Peel Hunt LLP Reports are distributed to US investors by Peel Hunt Inc., which is a member of the Financial Industry Regulatory Authority ("FINRA") and the Securities Investor Protection Corporation ("SIPC"). Peel Hunt LLP accepts responsibility for the contents of this Report and it has not been altered in any way by Peel Hunt Inc. Peel Hunt LLP and/or its affiliates may hold 1% or more of any class of common equity securities in the issuer that the Reports cover. Disclosures in relation to Peel Hunt LLP and/or any affiliate's role in: (1) managing or co-managing a public offering of securities for the issuer; (2) receiving compensation for investment banking services from the issuer in the past 12 months; (3) expecting or intending to receive compensation for investment banking services from the issuer in the next three months; and, (4) making a market in the issuers securities; are set out in the main disclosure section of this publication.

Canada Disclosure: Peel Hunt LLP Reports may only be distributed by Peel Hunt LLP to Permitted Clients as defined in Section 1.1 of the National Instrument 31-103 Registration Requirements, Exemptions and Ongoing Registrant Obligations ("NI 31-103") in reliance on the International Dealer Exemption and International Adviser Exemption pursuant to subsections 8.18(2) and 8.26(3) and Notification to Clients of the prescribed information under subsections 8.18(4)(b) and 8.26(4)(e) of NI 31-103 in Alberta, British Columbia, Ontario and Quebec. Peel Hunt LLP is not registered in the local jurisdiction to provide advice on securities or to trade in securities. Peel Hunt LLP is: (1) registered in England and Wales with its principal place of business in the United Kingdom; (2) a member of the London Stock Exchange; and (3) regulated by the FCA. All or substantially all of the Company's assets may be situated outside of Canada. There may be difficulty enforcing legal rights against the Company because of the above. The Reports have not been prepared in accordance with the disclosure requirements of Dealer Member Rule 3400 – Research Restrictions and Disclosure Requirements of the Investment Industry Regulatory Organisation of Canada ("IIROC").

Republic of South Africa Disclosure: Peel Hunt LLP Reports may only be distributed to clients as defined in the FAIS Notice 37 of 2014 issued by the Financial Services Board. These Reports are distributed by Peel Hunt LLP under the exemption granted from section 7(1) of the Financial Advisory and Intermediary Services Act, 2002.

Australia Disclosure: Peel Hunt LLP Reports are distributed in Australia by Peel Hunt LLP under the exemption in Australian Securities and Investments Commission ("ASIC") Class Order [CO 03/1099] from the requirement to hold an Australia Financial Services Licence. This research may only be distributed to a "Sophisticated Investor" or a "Professional Investor" and a "Wholesale Client" (within the meaning of sections 708(10), 708(11) and 761G of the Corporations Act 2001 (Cth) (the "Act"), respectively), being a person to whom an offer of securities can be made without disclosure under Chapter 6D of the Act.

Peel Hunt LLP
Moor House
120 London Wall
London EC2Y 5ET
T: +44 (0) 20 7418 8900
F: +44 (0) 20 7305 7088