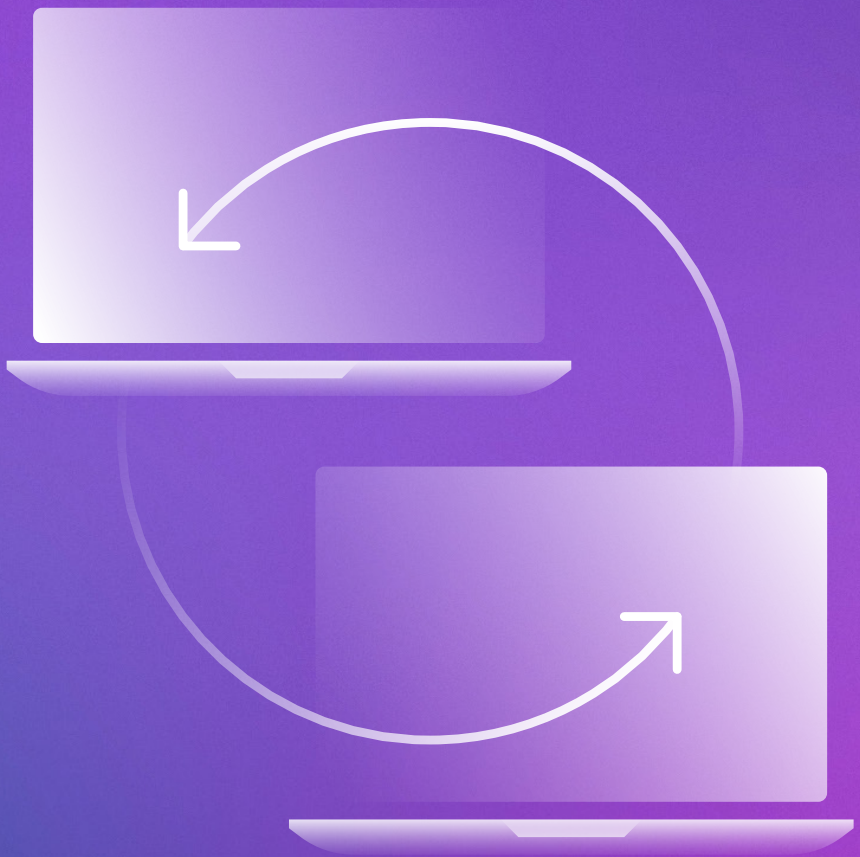
HUMAN

WHEN HUMANS MEET PERIMETERX

A MERGER TO BRING MODERN DEFENSE STRATEGIES TO DISRUPT CYBERCRIME & FRAUD



JONATHAN CARE & RICHARD STIENNON

SUMMARY

Human Security and PerimeterX are two market leading companies solving different parts of the bot, account abuse and fraud problem that is one of the most important and fundamental issues facing every enterprise and the internet today. Today, the companies announced they have merged under the HUMAN company name, and now serve more than 500 customers and have more than $100 million in ARR.

Both companies are recognized as industry leaders in protection against bot attacks, account abuse and fraud protection. This merger will offer enterprises a more comprehensive approach to safeguarding against these attacks from a single Human Defense Platform, put cybercriminals on notice and will give a substantial advantage over competitors.

INTRODUCTION

HUMAN Security, a New York based company, with Goldman Sachs being the largest shareholder, has announced it ismerging with PerimeterX, based out of San Mateo, Calif. HUMAN specializes in protection against abnormal bot behavior and fraud in the Adtech, performance marketing and cybersecurity space, while PerimeterX is a long-time participant in enterprise-focused bot detection and account abuse in the ecommerce space. Together, these organizations offer not only a well-matched set of complementary capabilities but also strengthen each other's products through significant additional threat intelligence and insight. The question on the minds of CISOs, investors and competitors alike must be what impact will this new company make in its chosen market, and how will it expand to adjacent markets.

BUSINESS LOGIC ABUSE (BLA): WEB ATTACKS THAT ABUSE PROCESS, NOT (ONLY) SOFTWARE FLAWS

The Open Web Application Security Project (OWASP) defines business logic abuse as *"ways of using the legitimate processing flow of an application in a way that results in a negative consequence to the organization."*

What this means is that attackers can cause business-impacting disruption without the usual attacks that a CISO expects such as SQL injection, Cross site scripting, and so on. In fact, many attack surface management and detection products will fail to see BLA attacks at all as they consist of apparently normal user activity. Only the intent and outcome indicate the hostility of the actor.

The Impact of this is that the highly technical attack-focused CISO may overlook BLA entirely, as it is not a direct attack on the organization. The Governance, Compliance and Policy based CISO may also overlook this attack as it does not violate any regulatory standards. In fact, awareness of this phenomenon usually surfaces when the CMO is examining business performance and discovers that website activity does not correlate with forecasted results. Even more seriously, in a hype-driven market the organization may have its attention drawn by sales quota restrictions imposed by the branded supplier. Many hype-driven brands are concerned about internet-enabled unauthorized secondary markets, from sneakers (and other sports leisurewear), to consumer electronics, and of course event tickets.

BLA is also apparent in other business processes, including loyalty programs, gift cards and promotions.

There is a real opportunity for the mature CISO to expand security activity to all business processes including those that are external such as the ones described above. By doing so, there's an opportunity to dramatically increase consumer sentiment and loyalty through improvement in Trust & Safety as a facet of the user experience. Mature management of this vulnerability serves organizational goals through protecting revenue and market share.

ABUSE	DESCRIPTION	IMPACT
Fake Engagement	Consuming online content (e.g. Music) to generate fees for the content creator	Loss of revenue to platform, and subsequent reduced payments to genuine creators
Scalping	Purchasing inventory of a hyped consumer item and creation of an unauthorized secondary market	Consumer dissatisfaction, Brand Damage, and sales quota limitation upon retail outlets
Denial of Inventory	Live Event spinning. Bot holds the ticket and resells at a higher cost site	Loss of availability to genuine customers leading to brand damage and consumer dissatisfaction
Carding	Testing payment cards for small values to check validation	Retailers are seen as high risk by the banks and credit card brands
Token Cracking	Entering gift card numbers until ones are found with a positive balance	Loss of revenue due to gift card theft and subsequent fraudulent purchases
Credential Stuffing	Using credentials from breaches and trying them on multiple other sites	Account Takeover
Scraping	Pulling pricing data or other intellectual property from an ecommerce website	Competitive Impact
Account Takeover	Attackers target web apps to steal, validate and use identity and account information to unlock stored value, create new accounts and commit fraud. Every attack plays a part in the cycle and has the potential to contribute to fraudulent activity, threatening customer loyalty, conversion rate and brand reputation.	

So, the purpose of any Bot Defense, account abuse and fraud protection product (whether in ad-space or in the enterprise space) is to detect undesirable or unwanted actor behavior and make it uneconomic for an attacker to misuse ecommerce processes. In order to make BLA an uneconomic proposition for an attacker, the bot defense product must disrupt their activity. Disruptions can be created by

1. *Defend*
2. *Drop*
3. *Deceive*
4. *Disable*
5. *Defeat*
6. *some type of challenge.*[1]

Clearly this disruption activity cannot create an unwelcome user experience which therefore means that a top key performance indicator for any vendor competing in this space is accuracy and to test the bot, not the human which is the fundamental flaw in any CAPTCHA based system. CISOs who are purchasing these solutions must be mindful of the needs of value proposition and business process owners who will not tolerate impediments to the genuine customer journey. Therefore a challenge to a sophisticated bot attack that does not impact the real-human customer yet complex for a bot, is highly beneficial. Also, older tools used to stop bot attacks, account abuse and fraud such as CDNs and WAFs may stop simple bot activity but a specialist like the combined company of HUMAN has demonstrated that they can detect, identify and actually disrupt sophisticated cybercriminals so they are taken out of operation for good.

IMPACT ANALYSIS

HUMAN Security CEO and Co-Founder Tamer Hassan stated:

This is a merger of two great companies and great teams to accelerate our ability to stop and win against cybercriminals. Bot attacks, account abuse and fraud is one of the most important and fundamental issues facing every enterprise and the internet today. In order to disrupt the economics of cybercrime, we wanted to accelerate our capabilities and bring together two amazing teams to change the way we approach protecting our customers and the internet. It's through modern defense —built on internet visibility, network effect and disruptions. By making it more expensive and the risks too high for cybercriminals, this merger changes the game and puts us in a position to win.

Furthermore, PerimeterX CEO added that:

When we started to talk many months ago, it became very clear how complementary our businesses are and how powerful it would be to combine them. You put our people and advanced products together on a single Human Defense Platform, it becomes something very powerful. The PerimeterX mission has been to protect the apps that power our daily lives with a portfolio of comprehensive application protection solutions that detect and stop the abuse of identity and account information on the web. With HUMAN's vision and successful approach to modern defense safeguarding enterprises and internet platforms from attacks, it's clear that we should be allies. HUMAN Security Inc. have announced that they will acquire PerimeterX in a play that is certain to engage interest in the Bot Defense market from investors, competitors and CISOs alike.

HUMAN (formerly known as White Ops) is best known for its adtech defense products, while PerimeterX has been a long-time incumbent in the enterprise-targeted defense of business logic abuse.

This merger combines service offerings and talent into one organization with a combined ARR[2] of over $100 million. of which will address many of the web security challenges faced by the modern enterprise. Tamer Hassan will continue as CEO of the company. PerimeterX CEO, Omri Iluz, will join the board and become President and general manager of the Enterprise security division, while PerimeterX's CTO, Ido Safruti, will join as CTO of the Enterpirse security division The merger has been approved by both companies' board of directors and has received regulatory approval. HUMAN has received a $100 million debt facility from Blackstone Credit that follows on the heels of a $100 million growth funding round led by WestCap and NightDragon earlier this year. Terms of the merger were not disclosed.

The Bot Management and Defense space is an interesting one. To many CISOs with a background in Network Security and Infrastructure Protection it would appear that this is a logical extension of the Web Application Firewall, a technology that is unfortunately appearing more and more beleaguered against the ever more sophisticated array of web application attacks and increasingly sophisticated fraudsters. BLA is one of the more pernicious attacks as there are no obvious indicators of compromise (IoCs). Therefore CISOs must carefully balance capabilities of products designed to fulfill the needs of this space vs more broader products that attempt to provide some functionality in the bot defense space.

Representative bot detection vendors include:

Google	DataDome
Radware	Cloudflare
Netacea	Akamai
HUMAN Security	Cequence
Arkose Labs	F5
PerimeterX	Kasada
Imperva	hCaptcha
	Reblaze

As can be seen, vendor sizes vary widely and so the merger of two leaders (HUMAN and PerimeterX) is likely to win approval from enterprise decision makers such as procurement & compliance.

Primary markets & use cases served by HUMAN:

MEDIA SECURITY

Ad Fraud	Fraud
Malvertising	Device/App/ SSA Spoofing
Click Fraud	Loyalty Program Abuse
CTV Fraud	Coupon Fraud
Paid Marketing Manipulation	Promotion Fraud
Lead Generation	

ENTERPRISE SECURITY

Account Takeover	Denial of Inventory
Carding	Digital Skimming
Client-Side Supply Chain Attacks	PII Harvesting
Credential Stuffing	Scalping
	Web Scraping
	Fake Account Creation

A formidable capability set such as the above leads to the opportunity to build more use cases that align with HUMAN's strategy of Modern Defense designed to increase the cost to attackers and lower the cost of collective defense. The opportunity is significant and cited as a c. $30 Billion TAM[3].

MERGER ANALYSIS: STRENGTHS, WEAKNESSES, OPPORTUNITIES & THREATS

STRENGTH

- Intelligence from each product complements the other. HUMAN gives insight into front-wave activity & identity through ad-tech signals whereas PerimeterX gives insight into BLA attack patterns
- Products combine and offer additional ancillaries such as data enrichment, pervasive behavioural identity and analytics
- Strong product portfolio attractive to both features-focused CIS and vendor-consolidation supplier managers
- Demonstrable thought and market leadership

WEAKNESS

- More complex product suite indicates increased resource requirement for development
- Most M&As trigger a period of inward focus where the new organization evaluates itself. This indicates a potential lack of external focus on the market
- Wider product portfolio increases the chance that elements of the portfolio will be in place in customer deployments, thus potentially increasing customer resistance.

OPPORTUNITY

- Build product portfolio through internal development and further acquisition. Adjacent areas such as fraud analytics, identity verification, and authentication.
- Stronger merged company more attractive to strategic partners
- Increased rich data is an asset that can be productised into new adjacent markets e.g.
- Transaction enrichment (VISA/ Mastercard), identity (SOCURE, LXNexis, etc)
- Pre-integrated portfolio to bring to market

THREAT

- Perceived as threat by the large complex vendors
- More complex product portfolio => slower customer decisions due to choice
- Point solution vendors try to differentiate on specific products

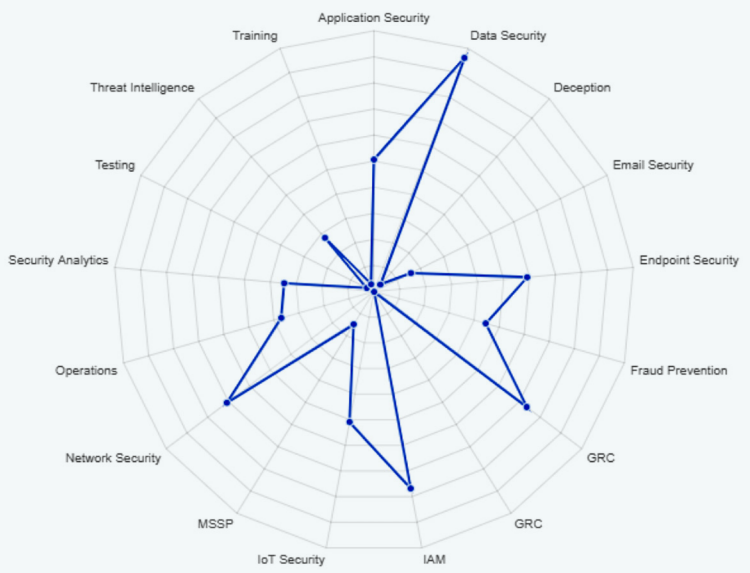


Figure 1: Global Cybersecurity investment by sector. Courtesy IT-Harvest https://it-harvest.com

As can be seen from figure 1 above. Fraud prevention investment (which includes Bot Defense) receives less investor enthusiasm than Data Security, Network Security and is on a par with Application Security. So the merger of HUMAN Security and PerimeterX has the potential to significantly affect this market, not only on purely technical capabilities but also by creating a strong competitive player.

A number of competitors to HUMAN and PerimeterX have already gone down the acquisition path, such as:

Vendor	Acquired By
Shape Security	F5
Distil	Imperva
Shieldsquare	Radware

The market is also under pressure from external entrants such as Akamai and Cloudflare, both of whom are actively marketing bot protection as a capability in their edge security solutions. However, edge solutions such as the above suffer from a structural flaw in that they are unlikely to be able to be tightly integrated with business application logic and so will suffer a lack of accuracy, a key performance metric for solutions in this space. It's also possible that we will see cloud providers also offering capabilities in this space either directly or through strategic partnerships. Future market moves could conceivably include a heavyweight network security vendor such as Cisco or Checkpoint seeking to complete their security portfolio through acquisition which could include existing pureplay bot detection vendors such as Arkose Labs, Netacea, DataDome, or Cequence Security. Certainly the differentials between sub-categories in Fraud Detection such as API protection, Behavioral Analytics, and Bot Detection are blurring as vendors in these spaces seek to expand the products and services they offer to their customers.

The new HUMAN organization will have a combined headcount of over 450 employees and expects to continue its pattern of sustainable growth on a global basis, reaching profitability in 2024. After the merger is closed, the combined companies will have more than $100 million in ARR and serve 500 customers.

IMPACT ON CUSTOMERS

Customer Acquisition Model
Customer acquisition models are very similar but are very complementary. PerimeterX has protected mostly ecommerce companies working with their security & ecommerce/ digital teams, and recently expanding into fraud operations. HUMAN has protected Ad Tech, Performance Marketing and cyber security/application security teams. Joining these silos means that customers will have a fully articulated solution addressing key business needs

Customer Retention Model
Customer retention models are very similar. Both organizations have Client Success Teams and dedicated sales leads that focus on retention. Marketing also plays a role in building strong relationships with customers and the Human Collective and the Satori Threat Intelligence Team brings together customers for investigations and disruptions. This all leads to high NPS scores (+72) and high retention rates.

Purchase Model
Purchase models are similar and will be combined over time, taking the best approach to serve customers and create satisfaction. The new product portfolio offered will be the entire suite of HUMAN and PerimeterX products.

Deal-size Model
Deal sizes are similar and are mostly based on scale of interactions safeguarded

This agreement unites two complementary market leaders that share a common vision and that together can deliver even greater value. The merged company, under the brand HUMAN, combines the modern defense capabilities of HUMAN with the comprehensive account protection capabilities of PerimeterX to disrupt the economics of cybercrime and delivers a formidable challenge to the cyber adversaries facing today's digital businesses.

HUMAN/PerimeterX enterprise security customer benefits

- Safeguard against more bot, account abuse and fraud use cases, enabling them to better protect e-commerce and cybersecurity applications. The more signal and visibility they have across the internet, the more they can safeguard everyone with collective protection.
- Invest even more in R&D and new products as part of their Human Defense Platform, directly protecting enterprise security across a variety of use cases, including: Account takeover, carding, client-side supply chain attacks, credential stuffing, denial of inventory, digital skimming, PII harvesting, scalping, web scraping and fake account creation.
- Be best suited to safeguard your entire company across advertising, marketing, e-commerce and cybersecurity from sophisticated bot attacks, account abuse and fraud.

HUMAN media security customer benefits

- Safeguard against more bot and fraud use cases, enabling them to better protect the advertising and performance marketing ecosystem. The more signal and visibility they have across the internet, the more they can safeguard everyone with collective protection.
- Invest even more in R&D and new products as part of their Human Defense Platform, directly protecting the advertising ecosystem across a variety of use cases including: Ad fraud, malvertising, click fraud, CTV fraud, paid marketing manipulation, lead generation fraud, device/app/SSAI spoofing, loyalty program, coupon fraud and promotion fraud.
- Be best suited to safeguard your entire company across advertising, e-commerce and cybersecurity from sophisticated bot attacks and fraud.

IMPACT ON THE NEW ORGANIZATION

The new HUMAN organization has a clearly defined purpose, i.e. *to disrupt the economics of cybercrime through Modern Defense*, where a single protection event for one is a protection event for all. The market opportunity based on the use cases that the combined companies now solve is more than $30 Billion. PerimeterX has raised $148 Million and HUMAN has raised $142 Million. Goldman Sachs is the largest shareholder in the company and HUMAN received $100 Million in funding in January 2022, led by West Cap and Night Dragon (The $100 M is part of the $142 M stated above).

Tamer Hassan commented:

> **"Our advanced technology, combined resources, mission-focused teams and industry-leading strengths, will enable us to create the most comprehensive Human Defense Platform that offers the most complete protection for enterprises and internet platforms across advertising, marketing, ecommerce and cybersecurity.**

[1]The most common type of challenge being a CAPTCHA. However, consumer sentiment is turning against "endless pictures of traffic lights" and so many vendors are innovating new ways of reliably identifying human actors, and impeding unwanted bot actors.

[2]ARR is an acronym for Annual Recurring Revenue, a key metric used by SaaS or subscription businesses that have term subscription agreements, meaning there is a defined contract length. It is defined as the value of the contracted recurring revenue components of your term subscriptions normalized to a one-year period. ARR is the less frequently used alternative normalization method of the two common ones, ARR and MRR. It is used almost exclusively in B2B subscription businesses. - Source: SaaSOptics

[3]Total addressable market (TAM), also called total available market, is a term that is typically used to reference the revenue opportunity available for a product or service. TAM helps prioritize business opportunities by serving as a quick metric of a given opportunity's underlying potential - Source: Wikipedia

[4]Net Promoter Score measures customer experience and predicts business growth. Source: Netpromoter https://netpromoter.com

About Us

HUMAN is a cybersecurity company that safeguards 500+ customers from sophisticated bot attacks, fraud and account abuse. We leverage modern defense—internet visibility, network effect powered by collective protection, and disruptions—to enable our customers to increase ROI and trust while decreasing end-user friction, data contamination, and cybersecurity exposure. Today we verify the humanity of more than 15 trillion interactions per week across advertising, marketing, ecommerce and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN. To **Know Who's Real**, visit www.humansecurity.com.