

ECONOMIC VALIDATION

Analyzing the Economic Benefits of HUMAN Security

HUMAN Security Reduces the Risk and Business Impact of Fraud, Bots, and Wasted IT Resources

By Nathan McAfee, Senior Economic Analyst
Enterprise Strategy Group

March 2023

Contents

Executive Summary	3
Introduction	3
Challenges	3
The Solution: HUMAN Security	5
Enterprise Strategy Group Economic Validation	6
HUMAN Security Economic Overview	6
Improved Profitability	6
Improved Visibility and Control	8
Reduced Risk	9
Conclusion	10

Executive Summary

Businesses are experiencing digital attacks, also known as cyber-attacks, at a rate that is escalating every year. These attacks are initiated by criminals that have a low barrier of entry to their crimes and very little chance of being caught and prosecuted. The criminals are growing in both numbers and in the sophistication levels of their attacks, while the costs of attacks increase with each new area that is targeted. In addition to the bottom-line costs of these crimes, companies are finding that illicit activities frustrate their customers and reduce the potential value of customer lifecycles.



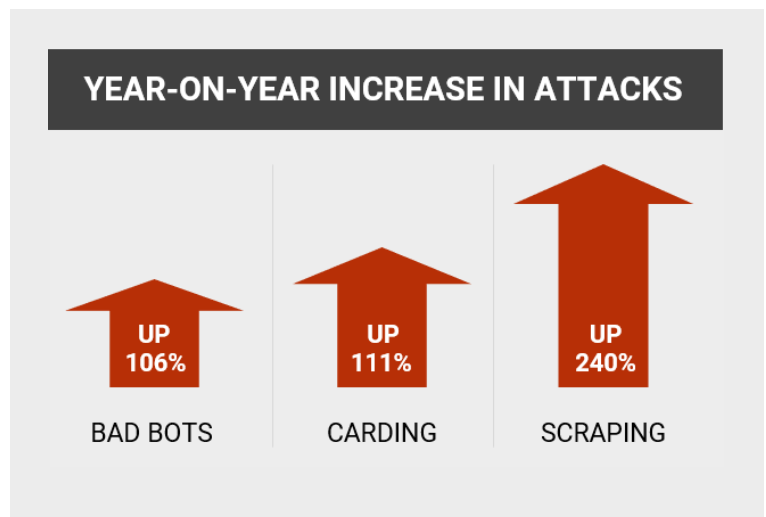
TechTarget’s Enterprise Strategy Group (ESG) analyzed the threat environment, challenges faced by organizations, and the impact that HUMAN Security can have to help businesses overcome these challenges and better reach their business and IT goals. ESG studied customer examples that show **900%+ ROI, 50% reduction in fraud, and 80% savings** in employee full time equivalent (FTE) time associated with monitoring and remediating internet-based threats. ESG also found that customers deploying HUMAN Security technologies realize **increased revenue and profitability**.

Introduction

This Economic Validation from Enterprise Strategy Group (ESG) focuses on the quantitative and qualitative benefits organizations can expect by deploying the capabilities of HUMAN Security to reduce or eliminate digital attacks. The insights in this analysis are the result of interviews with HUMAN Security customers, ESG research, study of existing information and case studies, and ESG analyst guidance.

Challenges

Businesses that rely on external connectivity are under constant attack. In addition to human-generated internet traffic, bots (short for robots or internet robots) are computer-generated operations that mimic human activity. Bots can work at a speed that is impossible for humans to match and at a far lower cost than most human-generated requests. While up to two-thirds of internet traffic may be bots, not all bots are malicious.¹ However, estimates of internet traffic that is generated by bots with illicit intent range from between 40-50%. The cyber-criminals and bad actors that initiate these attacks are becoming more organized and sophisticated with each passing month and are using technology that can easily overwhelm efforts to protect digital assets, portals, and workflows. As organizations continue to modernize their digital operations, they find their threat landscape is increasing, giving bad actors more areas to attack. 41% of organizations surveyed by Enterprise



¹ Source: TechTarget, whatis.com, [bot](https://en.wikipedia.org/wiki/Bot).

Strategy Group say that keeping pace with increasing threats is one of their biggest challenges with protecting their APIs.² The threats created by bad actors and bots can be grouped into three categories:

Theft

- **Carding** – Carding involves using bots to verify that stolen credit card numbers are valid. These validated numbers are then either used for large purchases or sold to criminals who will use them for illicit purchases. Carding impacts the legitimate cardholder, as well as merchants, through lost products, chargebacks, and fees.
- **Content scraping** – This is the extraction of content from one website to use on another. This activity is usually bot-driven and pulls content from another organization’s website to its own. This gives the scraping organization access to pricing information, provides them with competitive intelligence, and can give them a competitive advantage.
- **Account drainage** – This is an exploit in which cybercriminals gain temporary access to accounts or gift cards to spend or transfer available balances.
- **Inventory manipulation** – Inventory manipulation is used to either deplete a competitor’s reported inventory or purchase larger quantities of goods than would otherwise be available.
- **Malvertising** – In malvertising, when an ad exchange is compromised, advertisements that appear legitimate but contain malware can be pushed to the end user.

Fraud

- **Account takeover** – This is an attack in which bad actors take over someone else’s account by either using stolen credentials or brute force hacking of accounts.
- **Fake accounts** – In this attack, accounts are created with the intent of fraudulent activity.
- **Coupon abuse** – This represents the use of coupon discounts in a manner that is outside the intended scope.
- **Programmatic ad fraud** – Either driven by devices or content, bots can mimic authentic human ad impressions to raise cost-per-click income.
- **Content manipulation** – Using fake content, comments, or reviews, bad actors either bolster the appearance of their offerings or hurt the offerings and reputations of competitors.
- **Fake form fills** – Bad leads generated by fake form fills waste time, waste ad spending, and mask legitimate opportunities.

Business Operations

- **Increased infrastructure costs** – Depending on the industry, the need to overprovision capacity to handle bot traffic may cost more than what is needed to handle legitimate requests. Based on customer interviews, Enterprise Strategy Group saw examples where up to two-thirds of internet traffic was bot-generated, daily login attempts regularly exceeded 10 million per day, and advertising exchanges saw trillions of ad requests per month. The sheer magnitude of traffic requires companies to design infrastructure to handle the peak flow of wasted bot traffic, as well as the needs of actual customers.
- **Digital noise** – Too often, the line between bots and valid requests is blurred. In that blurred space, opportunities for growth and increased profitability are lost while time, money, and attention are spent fighting bots and illicit activities.
- **Brand damage** – Illicit activity hurts the bottom line, but even worse, it can prevent an actual customer from being able to conduct business. This results in customer churn, reduced value of a customer’s lifespan, and

² Source: Enterprise Strategy Group Research Report, [Trends in Modern Application Protection](#), July 2022.

lowered net promoter score (NPS).³ The ongoing damage to customer relationships and the brand as a whole often far exceeds that bottom line cost.

















The challenges are staggering. The criminals that create and use bad bots are increasing in numbers and the complexity of their attacks. The result is a double-edged sword: increased infrastructure and management costs and a decreased ability for organizations to reach maximum revenue potential. Every company that serves customers with external websites is at risk from illicit bots. However, the ability to protect assets while serving customers is unfortunately beyond the capabilities of most organizations. There needs to be a solution that offers clear and complete protection.

The Solution: HUMAN Security

HUMAN Security offers a portfolio of solutions that protect organizations against digital attacks. HUMAN Security provides extensive visibility into digital traffic while identifying and combating illicit bot requests and targeted attempts to hack workflows and credentials.

As seen in Figure 1, HUMAN Security works throughout all of the stages of the customer digital lifecycle to allow organizations to become proactive at preventing attacks, vigilant at protecting against active attacks, and supplied with the type of data to provide insight to protect against future attacks.

Figure 1. HUMAN Security Fights Fraud and Illicit Activity at Each Stage of the Digital Customer Journey

HUMAN Security Protects The Customer Digital Journey					
CUSTOMER PHASE	Initial interest	Lead generation	Account creation	Online account	Referrals
ATTACK VECTOR	AD FRAUD/ MALVERTISING	PAID MARKETING/ CONTENT MANIPULATION	DIGITAL SKIMMING/ COMPROMISED CREDENTIALS	ACCOUNT TAKEOVER/ TRANSACTION FRAUD	PROMOTION FRAUD/ COUPON ABUSE
HUMAN SECURITY	 MediaGuard  Bot Defender  Clean AD	 Bot Defender  MediaGuard  Code Defender	 Credential Intelligence  Account Defender  Code Defender	 Account Defender  Bot Defender  Code Defender  Credential Intelligence	 Bot Defender  Code Defender  Account Defender

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

³ Source: TechTarget SearchCustomerExperience, [Net Promoter Score \(NPS\)](#).

The HUMAN Security Portfolio consists of multiple technologies that span the digital lifecycle. The technologies studied for this analysis include:

- **Bot Defender** – analyzes bot behavior to distinguish between beneficial bots and those that were created with malicious intent. Bot Defender protects websites, apps, and APIs from bot-based attacks while reducing the infrastructure overhead wasted to service illicit bot traffic.
- **Code Defender** – provides granular insight into code-based vulnerabilities and behavior, giving companies clarity into application and script risks.
- **Account Defender** – protects against fake accounts and attempts to compromise authentic accounts.
- **Credential Intelligence** – prevents credential stuffing attacks to protect authentic accounts from takeover.
- **MediaGuard** – fights ad fraud and malware risk by ensuring that intended ads are safe and served to actual people.

Enterprise Strategy Group Economic Validation

Enterprise Strategy Group (ESG) completed a quantitative economic analysis on the impact that the HUMAN Security portfolio can have on organizations that rely on digital interactions to conduct business.

ESG's Economic Validation process is a proven method for understanding, validating, quantifying, and modeling the economic value propositions of a product or solution. The process leverages ESG's core competencies in market and industry analysis, forward-looking research, and technical/economic validation. ESG conducted in-depth interviews with end users to better understand and quantify how HUMAN Security has impacted their organizations, particularly in comparison with previously deployed and/or experienced solutions. In addition to having experience with HUMAN Security solutions, many of the customers interviewed had migrated to HUMAN from alternative solutions and were able to give detailed feedback about differences between their before and after states. The qualitative and quantitative findings were used as the basis for a simple economic model comparing the expected costs and benefits of HUMAN Security to those of alternative solutions.

HUMAN Security Economic Overview

Enterprise Strategy Group's (ESG's) economic analysis revealed that HUMAN Security provides its customers with significant benefits in areas, including:

- **Improved profitability** – Organizations are able to shift the focus of their resources toward activities that benefit their products and actual customers and reduce the costs of fraudulent activities.
- **Improved visibility and control** – HUMAN Security provides insight into internet traffic, bot interactions, and resource utilization that allow organizations to make decisions based on clear and accurate data.
- **Reduced risk** – By reducing fraudulent activities and improving overall governance, ESG found that HUMAN Security customers can substantially reduce the risks associated with internet-driven business.

Improved Profitability

Enterprise Strategy Group (ESG) found that organizations that adopted the different technologies offered by HUMAN Security were able to improve their profitability in multiple parts of the equation, increase revenue through the enablement of partnerships and authentic growth, reduce costs from a shift from reactive to proactive thinking, and reduce losses from fraud, waste, and customer churn.

- Reduced fraud** – Fraud looked different in every organization that ESG studied for this analysis, but one factor was consistent. Fraud directly and negatively impacted bottom-line profitability. ESG found that the customers interviewed for this study budgeted for an average of **2-3% of digital transactions to be fraudulent**, with some cases indicating **up to 50% fraud** for businesses that rely on limited edition products that create massive amounts of hype and traffic. With HUMAN Security, each customer reported that their fraud numbers decreased exponentially. This alleviated most of the 2-3% that was previously lost to fraud and enabled organizations to increase the lifetime value of customers, especially in the cases where HUMAN Security helped ensure that limited product offerings were placed in the hands of actual customers instead of bots or resellers. The co-founder and chief engineer of an online petition platform explained how their migration to HUMAN changed the way they could approach their day-to-day operations. He shared, **“Moving to HUMAN allowed us to proactively prevent fraud instead of reacting to occurrences”** and explained how the reputational cost of fraud far exceeded the dollars lost to fraud.
- Reduction in wasted infrastructure and media spending** – Companies pay money for traffic, as well as hardware, cloud services, and IT staff FTE, which must be maintained at a level to support incoming requests. However, when bot requests are inundating systems, much of that spending is squandered. A security team expert from an international health and wellness retailer shared, **“Bots tie up resources. We were at the point of resource exhaustion, bots were bogging down our growth. Not only were we able to cut the bot traffic to our portal in half, HUMAN helped us dramatically reduce the number of non-legitimate requests that actually got into our portal.”**
- Authentic growth and increased revenue** – ESG heard multiple customer stories of profitability being masked by bots overwhelming systems, leading to skewed reporting, inventory chaos, and wasted resources. While the level of increased revenue and profitability on overall revenue was variable across organizations studied, multiple customers shared a **return on investment (ROI) for HUMAN Security products of approximately 900%**, with ancillary benefits of improved customer satisfaction and a better roadmap for authentic growth. This authentic growth facilitates more accurate reporting and planning.
- Reduced customer churn** – Across the interviews that ESG conducted for this project, we heard examples of how bad bot traffic impacts customers. Before they deployed Bot Defender, one apparel manufacturer who sells footwear found that up to **80% of their limited edition inventory was being grabbed by reseller bots** instead of legitimate customers. This created up to 10 million requests per hour, which bogged their platform down and hurt usability. It also forced them to maintain inflated year-round infrastructure to try to support these limited events. Even with increased infrastructure costs, their main pain point was the disappointment of their customers trying to buy directly from them. The value of each of their customers could be tens of thousands of dollars over their lifespan, and they found that customers were getting discouraged because of the inability to buy limited editions direct from the manufacturer. In addition to diminishing the lifetime value of customers, they found these types of customers were active in social media communities and cast a negative cloud on the business because products were then only available on the secondary market. The impact of disappointed customers is amplified by their propensity to pass their negative experiences on to other potential customers, which lowers NPS scores and dwarfs the bottom-line loss of a single customer’s lifetime value.

“Just the FTE savings we saw with HUMAN’s Technologies gave us a positive ROI, but the true impact is the positive change it has had on our reputation and Net Promoter Score.”

- Co-founder, online petition platform

When shifting the view to companies that sell advertising, ESG found that fraud hurt customers in two main ways: by forcing those companies to charge higher prices because of programmatic ad fraud and mistakenly flag authentic transactions as fraud. One advertising sales business development manager shared, **“In the past, we would often flag ad requests as invalid traffic. This would turn off publishers, who**

are our partners. We saw a lot of customer churn because of flagging legitimate requests. HUMAN has had a substantial impact in reducing false-flagging and helped us retain our customers/partners.”

- **Facilitation of partnerships** – Very few companies exist on their own. Most take advantage of APIs that allow access to outside functionality. However, many APIs that could enhance offerings are not used. One interviewee explained, **“There are so many third-party APIs and trackers we could use, but we just couldn’t trust them. Code Defender helps us protect ourselves across all of our third-party code. We can use third-party functionality that we would have avoided in the past. This gives us full control over our marketing spend.”**
- **Shift to proactive from reactive** – ESG found that every company interviewed for this analysis reported the ability to shift focus from reactive activities to areas that increase profitability and uncover new business opportunities because of HUMAN Security. Multiple customers shared stories of spending far too much time using brute force to try to protect their traffic, and an average of **80% reduction in FTE hours** needed to monitor digital activities once they deployed HUMAN. A short-term financing company summarized it clearly, saying, **“HUMAN has allowed us to shift our focus from reactive thinking to proactive activities that reduce costs and enable revenue. This has helped us pull more profit out of existing business, as well as grow our revenue by expanding to areas that we didn’t have the time to explore in the past.”**

“Without Code Defender, we would have to limit the value our marketing teams can learn from our data. Code Defender gives us control and allows us to grow and fill our funnel.”

– IT Operations and Security Manager,
Finance

Improved Visibility and Control

Understanding what is happening with internet-based requests is a challenge that few organizations can master. The rapid increase in illicit traffic and attacks is outpacing the ability of most companies to find and retain the expertise needed to keep them ahead of and informed of both the risks and opportunities. Enterprise Strategy Group (ESG) found that HUMAN Securities can positively impact visibility and control through benefits, including:

- **Reduction of malicious login attempts** – It is widely known that stolen credentials are easy to find and purchase. HUMAN Security’s stats show that there are over 24 billion stolen credentials available for purchase on the internet and that over 65% of people reuse passwords for many of their accounts. Malicious logins cause multiple problems. Login systems can be overwhelmed, keeping legitimate customers from accessing their accounts; fake accounts can be created to operate outside the intended scope of the business; value can be drained through illegitimate logins; and accounts can be taken over from their actual owners. ESG found that customers that use Account Defender and Credential Intelligence can stop fraud before it happens by analyzing attempted logins, alerting them when accounts pose danger, and flagging credential breaches to limit attackers’ ability to commit fraud while forcing credential resets.
- **Reduction in bot traffic** – Bots can bog down networks and hinder profitability. Businesses must staff and maintain infrastructure to service their high-traffic spikes. When bot traffic that is not beneficial to a business is at high levels, this invalid traffic (IVT) forces companies to concentrate on the noise created by bad bots instead of focusing on actual business. ESG found HUMAN’s Bot Defender and Media Guard to have an immediate and substantial impact in reducing IVT, with multiple examples in this study showing a **90% reduction**. One Business Development Manager from an ad platform provider stated, **“Each percentage point of invalid traffic costs us approximately \$100K. With HUMAN, we have seen our IVT fall to below 2%, saving us millions.”**
- **Visibility into traffic** – HUMAN Security views approximately 20 trillion digital interactions each week and finds about 50% of overall internet traffic to be bot-driven (both good and bad bots). On average, HUMAN reports that about 90% of that bot traffic is not beneficial to the hosting organization. HUMAN’s visibility into bot traffic benefits all of its customers since a single attack can be analyzed and the remedy shared quickly across the entire customer base. HUMAN’s machine learning is rebuilt on a daily basis to inject protection gained

previously. As one customer shared, **“HUMAN gives us 24x7 visibility into our traffic. We sleep better at night knowing that HUMAN has our back.”**

- **Increased platform performance** – The reduction or elimination of non-genuine traffic allows platforms to run more efficiently. ESG found that many companies were experiencing resource exhaustion before adopting HUMAN’s technologies but are now experiencing higher and more predictable performance numbers.
- **Ease of use** – HUMAN Security’s platform simplifies extremely complex operations. One IT operations and security manager shared, **“With our previous solution we had to set rules by ourselves. We needed deep analytic skills to investigate and expensive skills to create and implement the rulesets, and it took too much time to react to changing threats. We are short-staffed as it is. With HUMAN, they take care of everything faster than we could have and better than we ever could.”**

Reduced Risk

All of the savings and performance offered by a platform are irrelevant if security isn’t at the forefront of a solution. It is clear that the threat landscape is rapidly increasing, both in volume and in the sophistication of the attack. Enterprise Strategy Group (ESG) found that HUMAN customers realize substantial improvements in reduced risk in areas that include the following:

- **Reduction in malicious inbound traffic** – In addition to the cost-benefit and improved operational clarity discussed above, HUMAN Security customers reported substantial benefits in their security posture due to reductions in malicious traffic.
- **Reduced fraudulent transactions** – Many types of internet-based fraud are too easy for criminals to resist with low costs to implement and a very small risk of being caught and prosecuted. Many customers shared in interviews that fraud had become a line item in their chart of accounts. It was inevitable, and their best efforts were unable to keep it from increasing each year. However, every person interviewed for this analysis reported a substantial and measurable reduction in the frequency of fraudulent transactions, as well as the impact of those occurrences.
- **Lowered risk of corporate espionage** – In addition to growing external threats, the risk of corporate espionage is increasing each year. ESG found that HUMAN Security customers were able to improve their level of governance through improved visibility into traffic, activity, and attacks. This governance, combined with a shift in focus that HUMAN enables, facilitates insight and control. Customers reported a lower risk of both internal and external espionage, as well as a reduction in the risk of captured credentials. Based on the 2022 Automated Fraud Benchmark Report, approximately **80% of security breaches** are caused by leaked credentials. Unfortunately, the average attack goes unnoticed for 60+ days.⁴ HUMAN Security lowers this risk.
- **Removal of accounts at risk** – HUMAN Security research estimated there was a 307% increase in account takeover (ATO) in 2021. Interviews with Account Defender and Bot Defender customers showed that these customers were able to identify the majority of at-risk accounts and either remove those accounts or **mitigate their risk** in most cases.
- **Proactive views of larger-scale attacks** – With the threat landscape increasing faster than most IT budgets and skillsets, the threat of large-scale attacks looms over most company leaders. While protecting each individual customer is the primary focus of the HUMAN Security Platform, HUMAN’s ability to recognize threats across their entire customer base and quickly eliminate risk for all customers helps prevent these larger attacks. A security team expert from a health and wellness retailer shared, **“Our CISO is extremely concerned with skimmer attacks. Before Code Defender, we had little visibility into attacks. Code**

“We don’t see static, dumb attacks anymore. We see attacks that change as they are blocked. There is no way we could keep in front of these attacks without HUMAN Security.”

– Director of Digital Operations, e-Commerce

⁴ Source: perimeterx report, [Automated Fraud Benchmark Report](#), 2022.

Defender helps us prevent and mitigate skimmer attack risk. I am able to put my leadership at ease and assure them we are protected because of HUMAN Security.”

- **Improved compliance** – Customers in compliance-based industries often find it hard to take advantage of some opportunities because they may rely on third-party functionality that doesn’t come with the level of transparency or assuredness necessary to satisfy regulations and auditors. ESG found that the granularity and control that HUMAN Security solutions like Code Defender provides increases the level of reporting and detail to open up these capabilities while still providing the insight needed for compliance.
- **Alleviated staffing challenges** – One of the top risks to the ongoing growth of most organizations is the challenge of finding and keeping top-tier security expertise. By passing the onus of internet security to HUMAN Security, ESG believes that organizations can alleviate this risk while focusing their efforts on their core business. As one interviewee stated, **“It is very hard to find security talent and even harder to keep those experts once they gain experience. We were always playing catch-up with our staffing. HUMAN has given us access to top-level experts that scale with our business.”**
- **The HUMAN Collective** – This invitation-only group provides a collaborative ecosystem to gain insight into the tactics of cybercriminals and develops best practices to protect all organizations. ESG believes that HUMAN’s leadership and overall involvement in this collective results in reduced attacks, fraud, and account abuse across the entire ecosystem.

Conclusion

Securing internet traffic is a challenge that constantly increases in complexity as cybercriminals become more sophisticated. In addition to the group of organized criminals, smaller bad actors can overwhelm organizations because the barrier to entry for cybercrime is low, the potential for success is high, and the risk of being caught and prosecuted is almost non-existent. Most companies find that they have to accept fraud as part of their revenue equation, and their best bet is to try to service their legitimate customers while filtering through all of the noise created by cyber thieves.

Enterprise Strategy Group (ESG) analyzed the impact that HUMAN Security technologies can have on digital attacks. ESG interviewed current HUMAN Security customers, utilized existing research, examined case studies and publicly available material, and relied on ESG analyst insights to understand the impact that HUMAN can have in reducing fraud, eliminating invalid network traffic, preventing data and account contamination, and improving end-customer experience.

ESG found that, while HUMAN was able to verify at a scale of **20 trillion digital interactions per week**, its technologies were able to provide granular and actionable insights that allow companies to substantially reduce the negative impact of bots, code and account attacks, and fraud. Customers interviewed shared stories of the immediate impact that deploying HUMAN technologies provided, as well as the value of being able to shift resources from monitoring and reacting to more strategic areas that **align with their core business**.

ESG verified that companies utilizing HUMAN Security technologies can reduce the risk associated with internet-connected operations; improve their visibility into internet traffic and control over account-based activities; and improve profitability through reduced fraud, increased customer value/satisfaction, and increased revenue.

If your organization engages in internet-connected activities and is looking to reduce risk while increasing profitability, ESG suggests that you explore the offerings from HUMAN Security and how they can change the way you approach your business and IT initiatives.


All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community. © TechTarget 2023.

 contact@esg-global.com

 www.esg-global.com