2019 TRUST REPORT IN PRACTICE

TRUST AT SCALE

Synack

Trust is Everything.

Delivering comprehensive penetration testing with actionable results.

Securing continuously with the world's most skilled ethical hackers and AI technology.

We are Synack, the most trusted Crowdsourced Security Platform.

Synack

Table of Contents

Key Findings

Data from hundreds of thousands of hours of security tests across companies in every industry show that the most trusted organizations are able to build trust at scale and practice **more efficient and effective security** by leveraging both human intelligence (HI) and artificial intelligence(AI). By utilizing this optimal combination of HI and AI, these security organizations are able to keep pace with the growth of their business and the evolving cyber threat landscape. 2019 Trust Report in Practice: Trust at Scale shows that a combination of HI and AI results in security with more:

Coverage and Scale: While humans are ~2x more impactful than a machine at finding and fixing security vulnerabilities, an augmented combination of the best security talent in the world and AI-enabled technology results in **20x more effective attack surface coverage** than traditional methods.

Efficiency: Humans can gain **up to 73% efficiency in evaluation time** by using AI-enabled technology to discover and evaluate vulnerabilities for exploitability.

Effective Remediation: By combining HI + AI, companies are able **to find and close critical vulnerabilities 40% faster**, than when HI + AI are used separately. Security teams are armed with the information they need to prioritize and remediate the most severe vulnerabilities and reduce their lifecycle.

Foreword: Augmenting Trust

Today's businesses run on trust. After all, the most successful brands are built on promises to their customers. We trust our favorite brands to fulfill those promises.When those promises are broken, so is that trust.

For modern businesses, trust is a value center. For them to flourish, that trust must be woven into the fabric of an organization by design. As businesses continue to modernize, that fabric becomes increasingly digital, vast, and complex.

Over 17 billion devices[1] are connected to the internet today, and that number is growing rapidly. As enterprises migrate to the cloud, accelerate their development cadences, create and ingest troves of data, naturally their digital footprints are proliferating. Growing technology stacks provide a multitude of new opportunities—but also, new risks.

What looks like a sophisticated technology portfolio to a CIO unfortunately appears as a target-rich attack surface to malicious cyber actors. In the next five years, $5.2 trillion in global value will be at risk. This translates to 2.8 percent in lost revenue growth the next five years for a CISO at a large global company[2]. Now more than ever, security teams must become proactive, bolster their defenses, prove that boards and customers alike can trust in their brand—and do all of this at a fast pace and on a large scale.

Trust is now the imperative of every business executive and every security executive. Our current global spend on security defenses is just short of $140 billion[3]—a far cry from the trillions in global value at risk. Companies simply will not be able to scale their security investment by simply investing more dollars across multiple vendors. To build trust at scale, we need to work smarter, not just harder.

In the 2019 Trust Report, we explored how organizations can work to build trust and realistically measure their progress using a Trust Score. In this Trust Report update, we look at trust in practice. We explore how Global 2000 companies, government agencies, and high-growth mid-sized companies are successfully deploying effective security practices at scale across their expanding attack surfaces to increase their Attacker Resistance Scores. These companies are increasing their resistance to attack by harnessing top human talent—an invaluable resource in security—and augmenting that human talent using machines and artificial intelligence. They have realized that we, as humans, trust humans and machines to do different things. They utilize the optimal combination of using humans for what they are best at—creativity and critical thinking—and using machines for what they are best at—efficiency. They pair them together in an augmented intelligence model to get the most effective, efficient, and trusted outcomes.

To scale trust, trust must be augmented, and this report, Trust At Scale, shares the data to support that. By combining human intelligence with augmented intelligence to build trust by design into organizations from the ground up, enterprises can ensure that their brands will grow and flourish at the same pace as their digital transformation. Let's dig in.

---

1 Knud Lasse Lueth, "State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating," IoT Analytics, August 8, 2018, https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

2 "Securing the Digital Economy: Reinventing the Internet for Trust," Accenture, January 17, 2019, https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf#zoom=50

3 "Forecast: Information Security and Risk Management, Worldwide, 2017-2023, 3Q19 Update," Gartner, October 3, 2019, https://www.gartner.com/document/3969990?ref=TypeAheadSearch&qid=ce9d09081691e56bca7e6bb8add

Scale: A CISO's Imperative

Security leaders sit between a number of huge, and somewhat new, challenges: an active (and continually evolving) threat landscape, agile software development becoming the norm in most development organizations, and digital transformation initiatives at the corporate level beginning to take effect. To say security teams are overwhelmed is a massive understatement. Frankly, security today requires the ability to analyze and respond at a volume and pace that far exceeds the ability of most security programs as they function now. Today, software development is a continuous process that constantly pushes out new updates. This can make getting a realistic view of your threat landscape extremely difficult, if not impossible. In addition, this trend increases the potential not only for new vulnerabilities, but also a higher number of them with each new and frequent release. That's why security's greatest challenge today is the ability to scale. Security teams need top talent, but talent is finite, requiring time and additional resources to recruit and retain top talent. Technology, such as vulnerability scanners, has been available to try to alleviate this burden; however, it's unsophisticated. Security teams need a smarter solution.

Human security talent, or security researchers, are critical to finding the most severe vulnerabilities (as compared to scanners), replicating malicious human behavior, and providing context, insights, and analysis into the findings. However, the rapidly evolving pace and severity of the cyber threat landscape has demonstrated that humans alone are not enough.

- **3.5 million cybersecurity positions** are projected to go unfilled by 2021.[4]
- **Only 14% of IT Managers** believe they have the cyber skills they need on staff.[5]
- Alert management can be burdensome and overwhelming for security analysts, with analyst spending up to **15 minutes every hour** on triaging and reviewing false positives.[6]
- Meanwhile, security teams also manage on average **more than 70 security vendors** and more than a third support multiple builds per day by their development organizations.[7]
- It's no wonder that the number of breaches continues to rise: in fact, 2018 witnessed **81% more breaches** than 2017.[8]

Instead, we need to augment our security teams with a smart, efficient solution—one that provides both quality talent and scalable coverage. Scaling our defenses to the magnitude of the threat requires a dynamic solution, leveraging the best security researchers in the world augmented by smart technology—an approach where human intelligence (HI) is augmented by artificial intelligence (AI).

---

4 Steve Morgan, "Cybersecurity Jobs Report 2018-2021," Cybercrime Magazine, May 31, 2017. https://cybersecurityventures.com/jobs/

5 https://cybersecurity.arcticwolf.com/Dark-Reading-Surviving-It-Security-Skills-Shortage.html

6 Ericka Chickowski, "Every Hour SOCs Run, 15 Minutes Are Wasted on False Positives," Bitdefender Business Insights Blog, September 2, 2019. https://businessinsights.bitdefender.com/every-hour-socs-run-15-minutes-are-wasted-on-false-positives

7 Asha Barbaschow, "Security landscape plagued by too many vendors: Cisco", ZdNet, November 2016 https://www.zdnet.com/article/security-landscape-plagued-by-too-many-vendors-cisco/

8 Verizon Data Breach Investigation Reports, 2017 and 2018. https://enterprise.verizon.com/resources/reports/dbir/

AI can scale the work of humans by taking on:

- **Repetitive tasks** where AI can find the most common types of cyber threats.
- **Evolving security threats and anomaly detection** where AI can conduct reconnaissance to build a more in-depth threat landscape; and
- **Cybersecurity data analysis** where AI can complete tasks with consistently higher accuracy than human analysts.

Scaling security defenses starts with a continuous diagnosis of security health based on rigorous and realistic security testing. Only by knowing where our security vulnerabilities are and fixing them before the adversary can exploit them can we stay ahead of the threat and minimize vulnerability risk. By adopting an augmented approach to security testing that leverages the absolute best of both human intelligence and technological advancements, organizations are able to find and remediate vulnerabilities faster, more effectively, and at scale, increasing their resistance to malicious attacks. The data show this too. Results from thousands of crowdsourced security tests show that humans can gain up to **73% efficiency in evaluation time and up to 40% efficiency** from reducing the number of days to close vulnerabilities by using AI-enabled technology, according to data from Synack, the most trusted Crowdsourced Security Platform. Taken together, the combination of human intelligence and artificial intelligence can yield better security outcomes, enabling great trust at scale.

The most optimal security testing: 1) finds and fixes vulnerabilities as effectively and efficiently as possible and 2) provides you with data about the strengths and weaknesses of your organization's attack surface and how it changes over time. This helps make your organization more resistant to attackers, and helps you build trusted products and brands even in the midst of constant change and threats. Above, we've tried to paint a picture of the security landscape today and the challenges that exist for security leaders who want to build and maintain trust with consumers now and also in the near future. In the sections that follow, we dive deeper into what "Trust in Practice" means for today's organizations and leaders. We will consider how a vast array of industries are currently utilizing artificial intelligence and our biases in regards to how we trust humans and machines differently. We will also explore the respective strengths and weaknesses of human and machine intelligence and propose a framework for how they can work together to optimize and scale current security practices to build trust by design at scale.

> *"A 'security by design' approach builds trusted systems; however, the ability to scale that security is one of today's biggest challenges*

STEFAN MANGARD
PROFESSOR, GRAZ UNIVERSITY OF TECHNOLOGY;
SPECTRE & MELTDOWN VULNERABILITY RESEARCH TEAM

Trust at Scale Requires a Dynamic Approach

The security threat landscape is evolving quickly—humans and artificial intelligence individually cannot keep up. Scaling trust begins with scaling security. Security teams need a readily available arsenal of tools to manage the ever-expanding threat landscape, especially given how busy security teams already are, juggling internal deliverables and updates to their applications and infrastructures.

Without humans, AI alone falls short. Where AI falls short:

- AI-based cybersecurity detection methods can produce quite a bit of noise and false positives. A single algorithm is still not better than a crowd of many researchers.
- AI can be limited in following business logic, which is better handled by the creativity of human beings.
- Hackers can use AI to carry out attacks as well. "Similar to ethical hackers and cybersecurity experts that use AI for cybersecurity, black hat hackers can use AI to test their own malware. Cybersecurity professionals are needed to stay ahead of the malicious attacks."[10]

In other words, human researchers are needed to help improve their AI in order to keep up with attackers' AI. Moreover, reliance on a single source of truth is dangerous, and can lead to openings in an attack surface.

THE BUSINESS CASE FOR USING AI TO AUGMENT HUMANS IN CYBERSECURITY

Enterprises are already seeing the value of combining human intelligence with artificial intelligence in cybersecurity, especially when it comes to **increasing efficiency when human security talent is limited**. For example:

Three out of four executives say that using augmented security solutions allows their organizations to respond faster to breaches.

Three in five firms say that using AI improves the accuracy and efficiency of cyber analysts.

A majority of organizations say that augmented solutions lower the cost of detecting and responding to breaches by 12%, on average.[9]

9 "Reinventing Cybersecurity with Artificial Intelligence," Capgemini, 2019. https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

10 Naveen Joshi, "Can AI Become Our New Cybersecurity Sheriff?" Forbes.com, February 4, 2019. https://www.forbes.com/sites/cognitiveworld/2019/02/04/can-ai-become-our-new-cybersecurity-sheriff/#57504ee836a8

Having said that, human beings alone aren't enough either. In a world without AI, human security experts simply cannot match the speed and scale at which AI software can accomplish repetitive tasks. While many humans are creative, the ones with creativity and security acumen are finite are finite, and require augmented intelligence to scale. By utilizing augmented intelligence, humans can scale across larger attack surfaces and focus their efforts on the most creative complex tasks. The benefits of scaling security testing with augmented intelligence are:

Coverage: AI can highlight any changes or modifications in attack surface in real time, with 24/7/365 monitoring of the entire attack surface.

Prediction Analysis/Forecasting: AI can predict where there might be a threat or a vulnerability based on past experience and insights from analyzing large datasets.

Bias/Diversity of Skill Set: AI can help level the playing field for researchers by getting a full, neutral view of the threat landscape.

Augmented Intelligence in Practice

While the technologies powering artificial intelligence and augmented intelligence are the same, the goals and applications are different: AI aims to create systems that run without humans, whereas augmented intelligence aims to create systems that enable humans to be more effective and efficient.[11] In security testing, by leveraging the optimal combination of human intelligence and augmented intelligence, organizations can get 4x higher ROI than traditional penetration testing models. Synack's model crowdsources ethical hackers and augments them with AI-enabled technology to help enterprises understand how the attackers could breach their systems more effectively and efficiently than traditional methods.

11 Aaron Masih ,"Augmented Intelligence, not Artificial Intelligence, is the Future", January 2019 https://medium.com/datadriveninvestor/augmented-intelligence-not-artificial-intelligence-is-the-future-f07ada7d4815

Trust in Machines is Elastic

Research has found that when machines are more accurate than humans, trust in machines starts high, but falls fast if/when they err.[12] Trust in humans is less elastic than machines, but when they work together, the outcomes are more trusted and effective. For example, a research study showed that people were more likely to give their credit card numbers to a computerized travel agent than a human travel agent and then utilize the human agent to plan the logistics of their trip[13]. By the same token, Facebook uses humans to implement their policies more consistently and accurately.

Augmented HI + AI in Practice: Industry Case Studies

Manufacturing/Critical Infrastructure

Augmented Intelligence is already working in factory operations, performing real-time production monitoring, and improving the accuracy of key metrics including Overall Equipment Effectiveness (OEE), production yield rates, as well as production efficiency to help human workers be more efficient and make decisions in real time with data. A new generation of AI-enabled robotics capable of image and speech recognition are increasing precision operations in the factory, allowing human workers to undertake higher-level jobs such as programming, maintaining, and coordinating robotic operations.

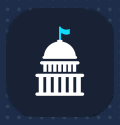
Financial Services

Credit scoring augmented with AI uses more complex and sophisticated rules compared to those used in traditional (human-run) credit scoring systems. This helps lenders distinguish between high-default risk applicants and those who are credit-worthy, but lack an extensive credit history.[14] AI in finance is a powerful ally for financial analysts when it comes to analyzing real-time activities in any given market or environment, because its accurate predictions and detailed forecasts are based on multiple variables and are vital to business planning.

12 Berkeley J. Dietvorst, Joseph P. Simmons, and Cade Massey, "Algorithm Aversion: People Erroneously Avoid Algorithms After Seeing Them Err," SemanticScholar.org, 2014. https://pdfs.semanticscholar.org/1463/09d561f0b373d0e3205a213f3336b0bdac68.pdf?_ga=2.126250509.1886561791.1569500649-1500989739.1569500649

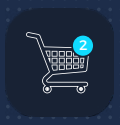
13 Ben Renner, "Is Artificial Intelligence More Trustworthy Than Humans When It Comes To Personal Info?" Presented at the ACM CHI Conference, May 2019. https://www.studyfinds.org/artificial-intelligence-more-trustworthy-person-info-other-humans/

14 Arthur Bachinskiy, "The Growing Impact of AI in Financial Services: Six Examples," Medium.com's Towards Data Science, February 21, 2019. https://towardsdatascience.com/the-growing-impact-of-ai-in-financial-services-six-examples-da386c0301b2



Federal Government

Civilian agencies have also been embracing AI technologies for a variety of use cases ranging from cognitive automation to AI-powered chatbots, and more. The General Services Administration (GSA) leverages AI within its Acquisition Process to accelerate human workstreams, and also during reskilling and upskilling the acquisition workforce.[15] In addition, Defense and Intelligence agencies have long been leaders when it comes to AI. In fact, the Department of Defense (DoD) recently launched the Joint AI Center (JAIC) with a mission to transform the DoD by accelerating the delivery and adoption of AI to achieve mission impact at scale.



eCommerce

Through AI, organizations are working to display customer-centric results that are relevant to their desired search. eCommerce websites are increasingly leveraging NLP (or Natural Language Processing) and Image Recognition to better comprehend user language and produce improved product results. In addition, because customer reviews are an integral part of the sales cycle (87% of customers trust what they read without a second thought[16]), AI is increasingly being deployed to analyze and classify user reviews so they can address and better address their needs. For instance, Yelp has deployed a sentiment analysis technique to classify its review ratings.[17]

Using AI to Augment Humans for Smart, Effective Security Testing

Building trust at scale begins with smart, effective security testing to identify security weaknesses, harden them, and strengthen the business. With the increasingly complex threat landscape, researchers need help to efficiently and effectively get through the noise and focus on the critical vulnerabilities. We will always need the creativity of human intelligence to beat human adversaries. That's because security risks and threats are always evolving and artificial intelligence does not excel at higher-order tasks. AI can help reduce the noise of the cyber threat landscape and allow scarce human researchers to focus on the creative tasks required to fight threats. Let's take a closer look.

15 Kathleen Walch, "Government Leaders And Influencers Are Prioritizing AI," Forbes.com, August 6, 2019. https://www.forbes.com/sites/cognitiveworld/2019/08/06/government-leaders-and-influencers-are-prioritizing-ai/#3903b4ef6cc3

16 "Top 5 Use-Cases of AI in eCommerce," EngineerBabu.com, February 15, 2019. https://engineerbabu.com/blog/top-5-use-cases-of-ai-in-ecommerce/

17 Ibid.

Through thousands of crowdsourced security tests, we've seen that an augmented approach to security testing, with an AI-enabled scanner providing reconnaissance and vulnerability intelligence to a team of top human talent hunting for, triaging and verifying vulnerabilities, can reduce noise and help save time for security researchers. A recent study found that "a staggering 27 percent of IT professionals reported receiving more than one million threats daily, while 55 percent noted more than 10,000," with 52% of them being false positives, and 64% being redundant—exacerbating the burden on an already-overwhelmed staff.[18] AI reduces noise by reducing false positives and redundant alerts by up to 99.63% and humans reduce the remaining noise by 91.05%—for an overall noise reduction of 99.98%, according to Synack data). This is a perfect example of how human intelligence augmented by artificial intelligence is better together.

In fact, smart technology can help to make security teams find vulnerabilities faster, cover a wider attack surface, and speed up time to find and fix vulnerabilities—adding up to 400% more efficiency to security teams in penetration testing.[19]

> *"While humans can't scale, machines can't think. More than 70% of the vulnerabilities that our Synack Red Team find in digital assets aren't detected by a traditional scanner. We will always need the creativity of human intelligence. But to scale at the pace of the threats, we need to keep building augmenting technology to test 'smarter'.*

DR. MARK KUHR
SYNACK CTO AND CO-FOUNDER

18 Tami Casey, "Survey: 27 Percent of IT professionals receive more than 1 million security alerts daily," Imperva Blog, May 28, 2018. https://www.imperva.com/blog/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/

19 Synack Proprietary Data

The results of a human + artificial intelligence approach to security testing are:

Effective: By leveraging HI + AI in security testing, more ground is covered and humans can focus on the higher severity vulnerabilities. According to Synack data, the average CVSS for vulnerabilities found by the Synack Red Team (a crowd of the top security researchers in the world) is over 4 points higher than those found by scanners—demonstrating that testing security with technology alone would miss impactful vulnerabilities found through a variety of methodologies. More than 70% of vulnerabilities found by humans would not be found by machines. By combining HI and AI, enterprises get the impact and creativity of human talent with the efficiency and coverage of technology.

Efficient: Humans can gain up to 73% efficiency in evaluation time by using AI-enabled technology to discover and evaluate vulnerabilities for exploitability, based on Synack data. By utilizing the reconnaissance data from AI-enabled technology, humans' time is more focused and effective and they can identify and triage vulnerabilities 73% more efficiently.

Fast: By combining HI + AI, companies are able to find and close critical vulnerabilities 40% faster, according to Synack data, than when HI + AI are used separately. AI-enabled scanning technology allows human testers to triage and find vulnerabilities faster, in turn providing security teams with information to prioritize and remediate the most severe vulnerabilities and reduce their lifecycle. Gaining up to 40% human efficiency combined with reducing the number of days to close (and a 73% increase in human speed in the evaluation process) frees up researcher time and allows them to cover a larger attack surface faster.

90%

Humans finds on average 90% more severe vulnerabitlies than those found by scanners

76%

More than 70% of vulnerabilities found by humans would not be found by machines

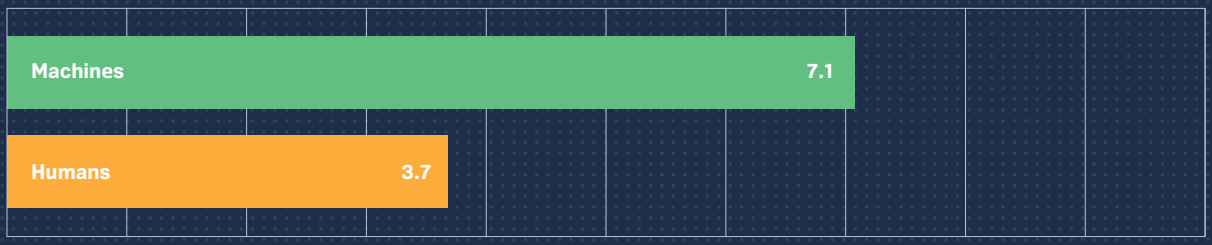
73%

Humans can gain up to 73% efficiency in evaluation time by using AI-enabled technology

40%

By combining HI + AI, companies are able to find and close critical vulnerabilities 40% faster

AVERAGE CVSS OF VULNERABILITIES DISCOVERED BY HUMANS VS MACHINES



Average Vulnerability Severity

Humans are ~2x more impactful, but **when combined with AI enabled technology together they are 40% faster and more impactful**. In fact, when humans augment machines the average CVSS score of their findings goes up to 3 points.

> *"Humans and AI have vastly different skill sets; therefore, we trust them to do different things. To effectively augment humans with AI, we need this trust to be informed by their respective strengths and weaknesses.*

DR. PAULA BODDINGTON
SENIOR RESEARCH FELLOW, CARDIFF UNIVERSITY &
AUTHOR, TOWARDS A CODE OF ETHICS FOR ARTIFICIAL INTELLIGENCE

Augmenting ROI: Best Practices from Crowdsourced Platforms

An augmented approach is not unique to security alone. Across industries, humans are scaling their efforts by leveraging AI systems to speed up decision making when humans can define tasks where the AI can support human decision making with analysis and inferences.[20] Crowdsourced platforms, such as Lyft, Airbnb, and Waze have all successfully used AI to augment their humans to allow them to scale and get access to better insights, resulting in better fraud detection, traffic data, and search functionality. Subsequently, there has been an increase in training AI systems to detect malware and viruses to perform pattern recognition that helps identify malicious behavior in software and alert human researchers to vulnerabilities.[21] Taken together, the combination of human intelligence and artificial intelligence yields better security outcomes, enabling trust at scale.

"Over time we realized that moving to deep learning is not a drop-in model replacement at all; rather it's about scaling the system. As a result, it requires rethinking the entire system surrounding the model." [22]

20 Gagan Bansal, Besmira Nushi, Ece Kamar, Dan Weld, Walter Lasecki, and Eric Horvitz, "Updates in Human-AI Teams: Understanding and Addressing the Performance/Compatibility Tradeoff," AAAI Conference on Artificial Intelligence, January 2019. https://www.microsoft.com/en-us/research/publication/updates-in-human-ai-teams-understanding-and-addressing-the-performance-compatibility-tradeoff/

21 Naveen Joshi, "Can AI Become Our New Cybersecurity Sheriff?" Forbes.com, February 4, 2019. https://www.forbes.com/sites/cognitiveworld/2019/02/04/can-ai-become-our-new-cybersecurity-sheriff/#57504ee836a8

22 Kyle Wiggers, "Airbnb details its journey to AI-powered search," VentureBeat, October 24, 2018. https://venturebeat.com/2018/10/24/airbnb-details-its-journey-to-ai-powered-search/

To get the best results from AI, we recommend you use it to help your security teams focus on their most difficult creative tasks. For example, AI and crowdsourcing have evolved into a more pragmatic approach for companies and organizations, which access the crowd not only for their ingenuity and help with co-creation of products, but also as trainers for AI systems. AI has become a critical piece to augmenting crowds of human experts and scaling services. In fact, many crowdsourced companies that have gone public highlight their IP coming from humans and their scale coming from AI-enabled technology. **For example:**

- **Lyft** has leveraged artificial intelligence to help them improve rider experience. They have leveraged data from over one billion rides and more than ten billion miles to train models to improve the experience, such as by reducing arrival times and maximizing the available number of riders.[23] Lyft has also built AI models to augment their analysts to help them figure out how to attract more riders during otherwise slow periods and to detect fraudulent behavior.[24]
- **Airbnb** doesn't rely on just one AI system. They have built an "ecosystem" of algorithms to support their decision making that can predict the likelihood a host will accept a guest's request for booking to the likelihood a guest will rate a trip or experience highly. The in-house AI systems can turn design sketches into product source code and translate listing reviews into guests' native languages making their teams more efficient and allowing them to spend more time on building and improving their products. They have also used it to improve user search. Search is one of the first experiences users have with Airbnb. Most guests start with a search at Airbnb's website for homes available in a particular geographic region, and the company has enlisted AI to help increase the relevance of search results.[25]
- **Waze** combines anonymized navigation information crowdsourced from the 100 million drivers who use Waze with Waycare's proprietary, AI-driven traffic analytics.[26] This allows users to benefit from real-time crowdsourced traffic data and predictive traffic analytics to ensure they are driving on the most efficient route.

23 https://www.forbes.com/sites/tomtaulli/2019/03/31/lyft-ipo-what-about-the-ai-strategy/#10e6c2ec2862

24 https://www.engadget.com/2019/05/01/lyft-google-tal-shaked-machine-learning-ai/

25 Kyle Wiggers, "Airbnb details its journey to AI-powered search," VentureBeat, October 24, 2018. https://venturebeat.com/2018/10/24/airbnb-details-its-journey-to-ai-powered-search/

26 Catherine Shu, Waze Signs Data Sharing Deal with AI-based Traffic Management Startup Waycare, April 26, 2018. https://techcrunch.com/2018/04/26/waze-signs-data-sharing-deal-with-ai-based-traffic-management-startup-waycare/

Are Augmented Companies More Trusted?

We've seen how AI can augment the work of security researchers, but what does it mean in terms of organizational security and trust?

Attacker Resistance Scores: Building Blocks of Trust

Synack's Trust Score is based on a complex calculation of Attacker Resistance Scores (ARS) from the Synack Crowdsourced Security Platform. By mimicking real-world attacks through a crowdsourced, AI-enabled model, Synack is able to assess how well an organization and its assets could resist an actual attack by a malicious actor. In general, a higher ARS means it is more difficult to find vulnerabilities in an organization, the vulnerabilities that are found are fewer and less severe, and/or the organization is quick to respond and resolve the issues. Organizations with the highest Synack Attacker Resistance Scores:

- Make it harder for attackers to find vulnerabilities.
- Remediate security issues quickly.
- Integrate security testing into DevOps to reduce the cost of vulnerabilities.

Using an augmented approach to building trust and security testing at scale has a positive impact on each building block of ARS (as outlined in the 2019 Trust Report):

BENEFITS OF AN AUGMENTED APPROACH

20x

This augmented approach yields 20x more attack surface coverage than traditional methods

4x ROI

Increases ROI 4x over traditional methods of security testing with humans alone

40%

Reduction in time taken to find and triage vulnerabilities by streamlining processes

Attacker Cost

- An augmented approach to security testing increases attacker cost as Attacker Resistance Scores by increase up to 200% over two years.
- An augmented approach **increases ROI 4x** over traditional methods of security testing with humans alone.

Severity of Findings

- AI enables the Synack Red Team to focus on the more severe vulnerabilities, allowing your organization to be notified of severe vulnerabilities faster and reducing the lifecycle of vulnerabilities within your organization.
- An augmented approach optimizes for both quality and quantity of findings:
  - Humans find more severe findings.
  - AI finds cover more ground and potentially find more vulnerabilities in the same amount of time.
  - This augmented approach yields **20x more attack surface coverage** than traditional methods.

Remediation Efficiency

- An augmented approach accelerates remediation, reducing days to close a vulnerability by 40% by reducing the time to find and triage vulnerabilities and streamlining processes between researchers and your security teams. AI helps accelerate remediation efficiently—the faster you find, the faster you can fix. An AI-enabled scanner can remove up to **99.98% of the noise for security researchers**. (AI reduces noise by 99.63% and humans reduce the remaining noise by 91.05% by verifying and prioritizing vulnerabilities—for an overall noise reduction of 99.98%.)
- Humans can provide detailed remediation guidance to make the patch easier to develop and implement.

A Roadmap to Trust at Scale: How to Augment Your Security Practices

As you seek to scale trust within your organization, we recommend four key steps to augmenting your security organizations and building a solid foundation for trust:

01

Train Security Teams to Adopt an Augmented Approach: Always-On Trust and Security

Train cyber analysts to be AI-ready. Teams need deep knowledge of key processes within an organization to ensure that the AI algorithm can cover the attack surface. By training your team on your security testing tools, analysts can understand how to best leverage security tools—helping them to scale trust through better efficiency, resulting in improved security.

02

Build an Ecosystem of Trust: Collaborate Externally to Enhance Security Intelligence

Collaboration via crowdsourced platforms ensures your organization stays up-to-speed on the threats facing other security professionals; such a platform also plays an important part in improving the logic of AI algorithms so that it detects threats more efficiently. Getting a diverse set of perspectives on your security risk can help you to increase your resistance to attack and build trust in your organization's security practice at scale.

03

Select the Right Use Cases to Get the Most ROI

Understand when to use AI, when to use humans, and when it's optimal to use both. By using technology and humans in a way that leverages their strengths allows you to build trust in your security strategy and trust in your organization more efficiently and effectively.

04

Trust at Scale: A Continuous Practice

Continuous research and development in AI is helping the technology grow exponentially; this same mindset and practice should be integrated into your security practice and ecosystem within your organization. A continuous cadence to building trust is required to build it at scale and requires a commitment to continuous security testing in order to build trust by design.

Building trust at scale requires both human intelligence and artificial intelligence. By optimally combining them, the most trusted organizations are able to build trust by design into their DNA, helping them keep pace with the growth of their business and the evolving cyber threat landscape. As a result, organizations are more efficient and outcomes are more effective, resulting in improved security at scale.

How Synack Can Help

The Synack Platform combines the efficiency of machines and the creativity and depth of human insight to help security teams find and fix exploitable vulnerabilities at scale. The Platform includes:

Apollo, Synack's continuous learning engine that uses machine learning to automate repeatable tasks and augment detection with new insights, strengthened by our learnings from working with the Synack Red Team.

LaunchPoint+, a secure testing gateway with added researcher endpoint control and enhanced workspaces to support privacy for highly regulated environments.

Hydra is Synack's proprietary, AI-enabled scanner that provides smart, automated scanning, based on best-in-class scanning plugins and continuous data-gathering backed by Apollo. Harnessing this intelligence, Hydra automates the reconnaissance and prioritization phases for security researchers to provide scalability to human testers.

Together, the platform's new features and advanced technology seamlessly orchestrate the optimal combination of human and augmented intelligence for more effective, efficient security on a 24/7/365 basis. The platform leverages Hydra to help security teams increase their attack surface coverage and gain new insight by continuously scanning for suspected vulnerabilities and engaging the company's crowd of top security talent, the Synack Red Team, to validate them. This frees up time for the Synack Red Team to focus on creatively hunting for high-impact vulnerabilities. The augmented intelligence offered by Synack's Smart Crowdsourced Security Platform, if applied to all penetration testing, would add 400% more efficiency to security teams.[27]

If you'd like to learn more about how Synack combines the best of human intelligence and augmented intelligence to protect your environment, please contact us.

27 Synack Proprietary Data

About Synack

Synack, the most trusted crowdsourced security platform, delivers continuous and scalable penetration testing with actionable results. The company combines the world's most skilled and trusted ethical hackers with AI-enabled technology to create an efficient and effective security solution. Headquartered in Silicon Valley with regional offices around the world, Synack protects leading global banks, federal agencies, DoD classified assets, and close to $1 trillion in Fortune 500 revenue. Synack was founded in 2013 by former US Department of Defense hackers Jay Kaplan, CEO, and Dr. Mark Kuhr, CTO. For more information, please visit **www.synack.com**.