VOLUME 1

TRUST HAS A NUMBER

THE 2019 TRUST REPORT

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

Trust Runs Deep

All brands, whether explicit or not, make promises to their customers. How a brand delivers on their promises determines our level of trust in them.

Amazon, who consistently scores very well in consumer trust sentiment polls, was built upon shoppers' faith in the eCommerce giant to provide selection and customer satisfaction. Volvo buyers' loyalty is about drivers' trust in the carmaker's safety record. And every pizza that Domino's sells is a reflection of customers' trust in the brand's "30 minutes or free" delivery promise.

Executives already know that when a brand consistently succeeds in delivering on its promises, consumers respond by trusting—and by buying—more. However, any disruption of service (or breach) that undermines a brand's core promise can be damaging just as much or more so than a data breach because the business is inhibited and the brand cannot uphold its promise. The trust that these beloved brands have worked to build up over time with their customers can be wiped out in an instant. Because of this, security can no longer be viewed as a back office expense; it needs to be considered as a huge factor that determines a company's value. Trust must be built into a business by design.

When Trust is Lost

While consumers want to trust companies, research shows that today's institutions aren't holding up their promises.[1] One glaring failure is security: many well-established brands are being breached and exposing their consumers' personal data - all at a cost to trust in their brands. In fact, 2018 witnessed 81% more breaches than 2017, totaling 2,216, and many millions of consumers affected.[2] The Starwood/Marriott breach affected 500 million accounts (one of the most widespread of all time); MyFitnessPal affected 150 million users; Quora affected 100 million users; MyHeritage affected 92 million users; Newegg, Panera, and more round out the largest breaches of last year.

Unfortunately, as life becomes more and more digital, consumers are re-evaluating their assumptions about whom they trust and why—and companies have to re-evaluate how they uphold their brand promises. Following the privacy and data breach scandals that Facebook suffered in 2018, some 74% of adults on Facebook downgraded their use of the platform in some way, including a startling 26% who outright deleted the Facebook app from their mobile devices.[3] Equifax lost $5.2B in market cap following its data breach the previous year, a loss that, two years later, it has yet to fully recover.[4] It's clear that trust is becoming a strong differentiator of choice for consumers; organizations should view security as a value center for their brand, not a cost burden as traditionally conceived.

---

1 Edelman Trust Barometer 2019, https://www.edelman.com/trust-barometer

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

3 "Americans are changing their relationship with Facebook," September 5, 2018. http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/

4 "Equifax's stock has fallen 31% since breach disclosure, erasing $5 billion in market cap," September 14, 2017. https://www.marketwatch.com/story/equifaxs-stock-has-fallen-31-since-breach-disclosure-erasing-5-billion-in-market-cap-2017-09-14

CISO as Brand Protector and Trust Builder

In response, companies should no longer think of security as just an IT issue—it's a trust issue, one that massively affects a company's brand. From loss of revenue and reputation to lawsuits, remediation costs and cleanup, and cyberattacks can debilitate a company's brand and business.

This dynamic places the CISO, ironically not the CMO, as the primary protector of the brand—and security as the most strategic weapon in their arsenal. As a result, CISOs have to put the right technologies, controls, and metrics in place to set their programs up for success; not to mention selecting the right vendor partners that are right for their organizations (from more than 3,000 security vendors operating today[5]).

However, this process—building trust, and security, by design—takes time. The first step is diagnosing how far along an organization is in the process, followed by analyzing where the industry is going, and putting a plan in place to get there.

The Synack Trust Report: Trust Has a Number offers a starting place. This first-of-its-kind report begins to quantify how trusted our organizations are at an asset level using proprietary data. The report and Synack's Trust Score offer security executives and boards a realistic sense of brands' performance against their promises and actionable recommendations for making progress over the next year. Let's start building trust by design by taking this first step together.

JEFF HANCOCK
PROFESSOR OF COMMUNICATION, STANFORD UNIVERSITY
FOUNDING DIRECTOR, STANFORD SOCIAL MEDIA LAB

> *"Trust is the glue of life. It's the most essential ingredient in effective communication. It's the foundational principle that holds all relationships."*
>
> STEPHEN R. COVEY

5 "Momentum Cyber's Mid-year Market Review has Cybersecurity Industry on Track for Best Year Ever with IPOs, VC & PE Financings and M&As at Record Levels," August 6, 2018. https://www.businesswire.com/news/home/20180806005229/en/Momentum-Cyber%E2%80%99s-Mid-year-Market-Review-Cybersecurity-Industry

PART 1

IT'S ALL ABOUT MEASUREMENT

Synack

To begin to build trust by design, CISOs have to know whether their security investments are actually working.

To begin to build trust by design, CISOs have to know whether their security investments are actually working. In light of increasing breaches and the expanding security budgets they beget, Synack's 2019 Most Trusted CISO, Ethan Steiger of Domino's, puts it this way: "Now, in 2019 more than ever, I need to prove to my board, executives and customers that they can trust that our security is working, and therefore trust our brand."

However, this measurable, trustworthy security is not something that's achieved overnight. It requires changing our thinking about security from something that's a static, point-in-time effort to something that is dynamic and approached in a continuous way, just as modern digital organizations approach their development. Just as trust is not a one-time thing, but an ongoing, long-lasting effort that is built into a business by design, so must security be.

Historically, it's been difficult to measure an organization's security strength and improvement over time. There aren't many metrics by which to measure security health, and those that do exist are not well-adopted or universal. Metrics that have worked for security teams, such as the number and severity of vulnerabilities or scores produced by scanner outputs, don't necessarily translate well in a boardroom full of business executives. The board and executive team want to know, holistically and at a high-level, how the company's security is positively or negatively affecting the risk to the business.

To calculate trust so that the board can get a sense of an organization's security strength, we must consider many factors. Those factors include: the size of an organization, that organization's breach history and how they've responded to incidents, security risks that the organization is exposed to and risk mitigation tactics being utilized. Together, these inputs help us put a number on trust: the Synack Trust Score—a single, one-of-a-kind metric that provides a holistic measurement of an organization's performance upholding their brand promise and designing trust into every level of the business, starting with security. The Synack Trust Score is calculated from Synack's massive database of penetration test performance data across industries. It uses empirical, not theoretical, data and is all the more powerful as a result.

> *"It's all about measurement. CISOs need a way to present security to their executive team and board in a way that clearly demonstrates and measures the business risk to the organization. The executive team doesn't want to talk about security—they want to talk about risk.*

STEPHEN WARD
CISO, HOME DEPOT
REMARKS MADE AT SYNACK STUDIO DURING RSA 2019

The Synack Trust Score provides

Confidence

Confidence in a company's ability to live their brand promise to their customers

Performance

An overall measure of security performance for the board

Resistance

An actionable measure of attacker resistance by asset for the CISO and security team

The most trusted organizations design trust into the core of their businesses by integrating security and integrity into the principles and products on which their businesses are built.

That's why, at the core of Synack's Trust Score, is the patented Synack Attacker Resistance Score™ (ARS™).

This is where we begin our Trust Report series. In subsequent volumes, we will continue to explore the remaining inputs of trust and broaden our focus. This first-of-its kind report series, based on proprietary data, from the Attacker Resistance Score, is intended to share important takeaways for modern CISOs to help them build up their security and get to trust.

> *"Today's consumers are getting more and more sophisticated; they want to know who is collecting their data and how their data is being used. They want more controls, more protection digitally. With the passage of GDPR and CA Consumer Privacy Act, it signals that more rights are being established for consumers and there is a greater expectation for organizations to use information in a trustworthy manner, and they will be held accountable.*

AMIT ELAZARI
GLOBAL CYBERSECURITY POLICY, INTEL & LECTURER, UC BERKELEY
REMARKS MADE AT SYNACK STUDIO DURING RSA 2019

The Number at the Core of Trust: the Attacker Resistance Score

The Attacker Resistance Score is based on a complex calculation[6] of Attacker Resistance Scores from the Synack Crowdsourced Security Platform, which harnesses the most talented and trusted ethical hackers in the world and pairs them with AI technology to deliver the most rigorous penetration test an organization can find. By mimicking real-world attacks through a hacker-powered, AI-enabled model, Synack is able to assess how well an organization and its assets could resist an actual attack by a malicious actor. Aggregating and anonymizing this information at the industry level gives companies a benchmark of how they are performing relative to their competitors.

By probing and testing continuously with hackers and AI tools, Synack continuously calculates an Attacker Resistance Score between 0 and 100 for every asset, assessment, and organization that Synack tests. Synack has conducted thousands of tests across security-conscious organizations ranging from the Global 2000 to high-growth companies to government agencies. The higher their scores, the higher their attacker resistance, and the higher the trust a customer can have in these organizations. Score data inputs from testing activity include†:

6 See Appendix for the methodology of how the score is calculated.

† Note: Data inputs continue to roll into future releases. Remediation is factored into Attacker Resistance Score for Crowdsourced Continuous Tests only. Please see the Appendix to understand the methodology for each calculation.

In general a higher Attacker Resistance Score 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.

> *When you have a quantifiable measure, you can then start to improve your situation. Unless there is a common metric and benchmark, however, it's hard for all of us to do our jobs well. Trust takes time and you need to be able to measure your progress. Historically, this has been extremely difficult to do, but the Attacker Resistance Score has presented CISOs with a new tool and opportunity.*

JAY KAPLAN
CO-FOUNDER & CEO, SYNACK

PART 2

TRUST STARTS HERE

Synack

It's time to give credit where credit is due.

Now that we can truly measure our security performance, we can show where our security program is succeeding and where we need to apply more resources in order to build more trusted systems, services, and products. This report explores how organizations' trust, from a hacker's perspective, is trending and what organizations can do to improve. No marketing predictions—just straight facts and statistics from the industry's only model of Attacker Resistance. Our Data Science team explain how the model works (distilled down to one page) in Appendix 1: Methodology.

Here's what the data say:

TRUST TAKES TIME

200%

Up to 200% higher Attacker Resistance Scores among those organizations that work to improve their attacker resistance for 2+ years vs. <1 year.

TRUST MUST BE PRACTICED CONTINUOUSLY

43%

43% higher Attacker Resistance Scores on average among organizations that practice continuous security testing vs. point-in-time testing.

ORGANIZATIONS WITH THE HIGHEST SYNACK ATTACKER RESISTANCE SCORES ARE:

01 Making it harder for attackers to find vulnerabilities

02 Integrating security testing into DevOps to reduce the cost of vulnerabilities

03 Remediating security issues quickly

PART 3

TRUST IMPROVES OVER TIME

Synack

Good news: Overall, we see a more positive picture for Attacker Resistance Scores than a year ago. In fact, the average Attacker Resistance Score for organizations has continued to improve year over year since the start of the score.

JANUARY 2018

55.2

Average Attacker Resistance Score

JANUARY 2019

57.2

Average Attacker Resistance Score

And that makes sense, because better metrics mean better insight. With the introduction of security platforms that combine Human Intelligence (HI) with Artificial Intelligence (AI), security teams have a more realistic, hacker-powered perspective of their security. They can now focus their resources on the assets that need the most remediation support.

And the effort pays off. Individual industries can improve their average Attacker Resistance Score by up to 200% over two years when conducting crowdsourced penetration testing with Synack.

FIGURE 1: 2019 ATTACKER RESISTANCE SCORES BY INDUSTRY

Industry†	Mean Attacker Resistance Score	Median Attacker Resistance Score	# of Incidents / Breaches‡
Manufacturing and Critical Infrastructure	65	69	582 / 89
Financial Services	61	68	598 / 146
Federal Government	57	64	22,788 / 304
Healthcare	56	57	750 / 536
Retail	54	61	317 / 169
Technology	53	60	1040/109*
Consulting/Business & IT Services	50	47	7,728 /165
State, Local and Education	49	53	22,788 / 304
eCommerce	45	47	1040/109*

Source: Synack proprietary data. Breach data from 2018 Verizon DBIR Report

† See Appendix 2 for Industry Definitions. Synack's sample size is based on thousands of crowdsourced security tests across security-conscious organizations in the Global 2000, high-growth sector, and governments. As industries evolve, so will their definitions. For example, while Retail is defined as companies for whom brick and mortar is a significant sales channel of their consumer goods and/or services business, this industry is increasingly evolving into the eCommerce sector. Today, Retail still includes companies such as food delivery businesses who have brick and mortar stores, in addition to delivery apps.

‡ This metric adds context to industry Attacker Resistance Score mean and median.
Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.
Breach: An incident that results in the confirmed disclosure— not just potential exposure—of data to an unauthorized party.

* eCommerce and Technology combined Incidents/Breaches

INDUSTRY TRUSTEES

Some industries are in a better position than others when it comes to trust.

Manufacturing and Critical Infrastructure lead the industry with an Attacker Resistance Score in the highest quartile. The sector has had to adopt a more proactive approach to securing their infrastructure because the industry is a top target for attacks by governments and large entities or "state actors"[7]. In turn, they are more mature in their testing than other industries. Not surprisingly, they've also kept the annual number of reported breaches in their industry down to double digits (See 2019 Synack Attacker Resistance Scores by Industry).

On the other hand, eCommerce lags other industries with an Attacker Resistance Score below average. Given digital forces pushing the industry to take its businesses online, it's not surprising that fast development cycles and frequent releases are creating new vulnerabilities. Agile development is healthy, but it necessitates agile security testing to keep pace. As a result, many organizations in these industries are upping their testing cadence from point-in-time to continuous testing.

CAMPAIGN FOR CULTURE CHANGE

The State, Local, and Education sector, in particular sees a dramatic improvement in Attacker Resistance Scores between organizations using trusted crowdsourced security testing less than one year and those using it over two years. This sector's security has undergone a high degree of scrutiny over the past few years, driven by everything from attacks on election systems to breaches at prominent universities. And in these cases, a new awareness brought about a new commitment to improving attacker resistance and rebuilding stakeholder trust.

7 "Why 'secure' isn't secure enough in the utilities sector", December 27, 2017, https://www.utilitydive.com/news/why-secure-isnt-secure-enough-in-the-utilities-sector/513205/

PART 4

THE BUILDING BLOCKS OF TRUST

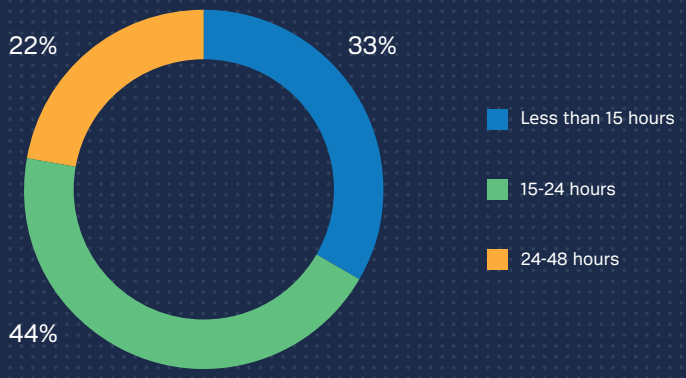
INCREASING THE COST OF ATTACK

Synack

Increasing the Cost of Attack

As part of the Attacker Resistance Score[8], the **Attacker Cost** component measures how much effort is required for a malicious actor to find undermining vulnerabilities in your organization. On average, it takes a researcher on the Synack Red Team less than one day (22.8 hours) to find an exploitable vulnerability, from the time they find an exploitable path. In a test environment, that means fast results. In a real-life scenario, that could mean your barrier to being damaged by a breach is less than a day.

FIGURE 2: DISTRIBUTION OF AVERAGE TIME TO FIND A VULNERABILITY BY A SYNACK RED TEAM MEMBER



Source: Synack proprietary data.

On average, it takes a researcher on the Synack Red Team less than one day (22.8 hours) to find an exploitable vulnerability, from the time they find an exploitable path.

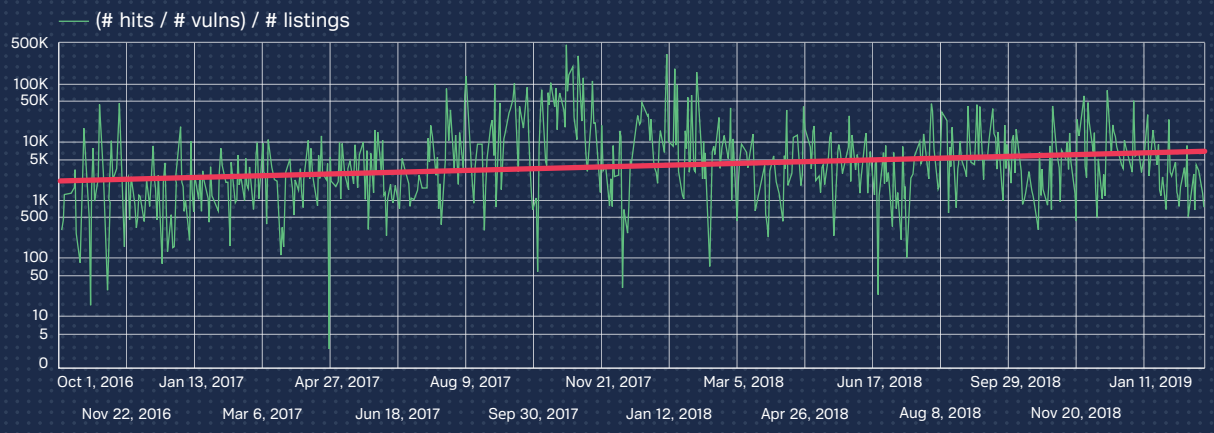
8 Please note that the formula to calculate these components is quite robust; this section shows simplified data. Please see the Appendix for the methodology on how the Attacker Resistance Score is calculated.

Increasing the Cost of Attack (cont'd)

Another component of **Attacker Cost** is the hits/vulnerability ratio, or how many attacker hits on an asset it takes to find an exploitable vulnerability (if any).

Synack's crowdsourced approach to security testing has helped its customers harden their assets over the past few years. From 2017 to 2019, Synack customers have increased their average hits/vulns ratio by 112%, meaning they increased the cost of attack and made it more effort-intensive for attackers to find vulnerabilities. Customers' assets are becoming more difficult to penetrate.

FIGURE 3: AVERAGE HITS/VULNERABILITY RATIO OVER TIME



From 2017 to 2019, Synack customers have increased their average hits/vulns ratio by 112%, meaning they increased the cost of attack and made it more effort-intensive for attackers to find vulnerabilities.

COSTLY ATTACKS

The average time to find a vulnerability in Technology is significantly higher than other industries. The longer the time to find a vulnerability, the higher the cost to the attacker and the less attractive the target. This is in line with other trends we've seen within the Technology industry to take a proactive approach to security.

PART 5

THE BUILDING BLOCKS OF TRUST

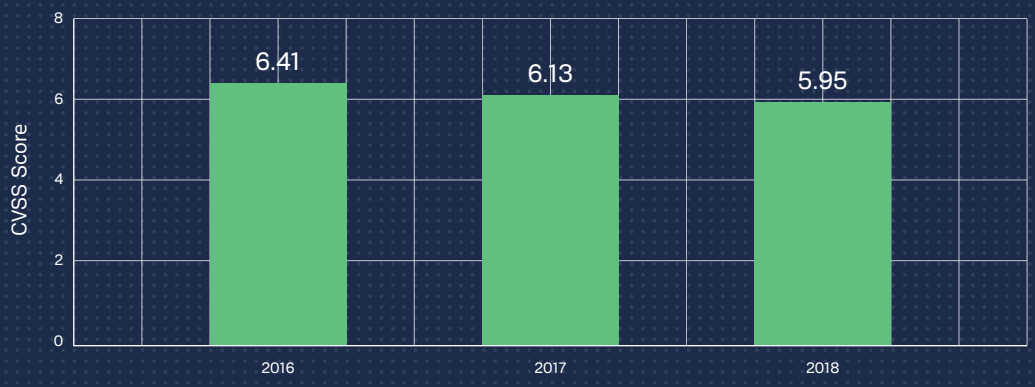
KEEPING SEVERITY OF FINDINGS TO A MINIMUM

Synack

In addition to requiring more effort to find vulnerabilities, the severity of the vulnerabilities discovered by the Synack Red Team is decreasing.

The **Severity of Findings** component of the Attacker Resistance Score measures both the quantity and quality of vulnerabilities found in your organization that put your brand and business at risk. The good news here is that the average Common Vulnerability Scoring System (CVSS) score of vulnerabilities discovered by the Synack Red Team among Synack customers has declined at a compounded annual growth rate (CAGR) of -4% over the past two years:

FIGURE 4: AVERAGE CVSS SCORE OF VULNERABILITIES DISCOVERED BY THE SYNACK RED TEAM OVER TIME



This decline aligns with the hard work by customer security teams to shift security left, find vulnerabilities earlier, and reduce the severity of findings.

Synack's Technology sector customers helped drive this decline, reducing industry average CVSS by 9% in the last year, and 11% overall in the past two years. The National Vulnerability Database is seeing a similar decline in CVSS in line with Synack's trend, likely due to the improvement that Synack's crowdsourced security testing is driving among some of the largest G2000 organizations.

In terms of types of vulnerabilities, both Synack and the National Vulnerability Database cite XSS as the #1 most common vulnerability type.

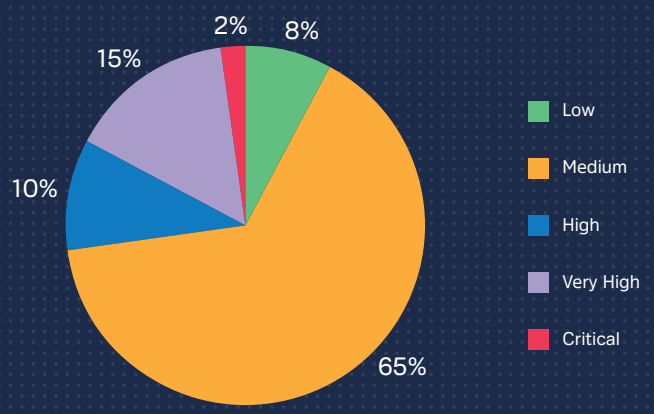
FIGURE 5: VULNERABILITIES DISCOVERED BY THE SYNACK RED TEAM BY TYPE

Vuln Type	% of Total, 2018
Authentication Session	8%
Authorization Permission	19%
Brute Force	2%
Content Injection	5%
Cryptography	<1%
DoS	<1%
Functional Logic	7%
Information Disclosure	16%
Insufficient Transport Protection	<1%
Other	<1%
Remote Execution	2%
Server App Misconfiguration	2%
SQL Injection	5%
Cross-Site Request Forgery	7%
Cross-Site Scripting	26%
Grand Total	**100%**

Some industries deserve honorable mentions for their proactive approach to security through testing for vulnerabilities, remediating them, and making the adjustments necessary to instill long-term, cultural changes to improve security posture. The results reflect that. For example, Financial Services has significantly fewer Authorization Permission vulnerabilities than average. This speaks to the industry's focus on security in this area. To their credit, many financial institutions have proactively adopted stronger controls around authentication and authorization to make it harder for attackers to find their way in. That being said, there is still room for improvement.

Synack finds 150% or more breach-worthy vulnerabilities, such as SQL Injection, in Financial Services and Federal Government than the cross-industry average. In eCommerce in 2018, Synack found 10% more XSS vulnerabilities in eCommerce than on average across other industries. Vulnerabilities found by Synack Red Team are typically unknown, i.e. not in the National Vulnerability Database. With the increasing pace of transaction digitization and software development, the discovery of these types of vulnerabilities, which are commonly associated with web apps, is not surprising.

FIGURE 6: VULNERABILITIES DISCOVERED BY THE SYNACK RED TEAM BY SEVERITY



Synack finds 150% or more breach-worthy vulnerabilities, such as SQL Injection, in Financial Services and Federal Government than the cross-industry average.

PART 6

THE BUILDING BLOCKS OF TRUST

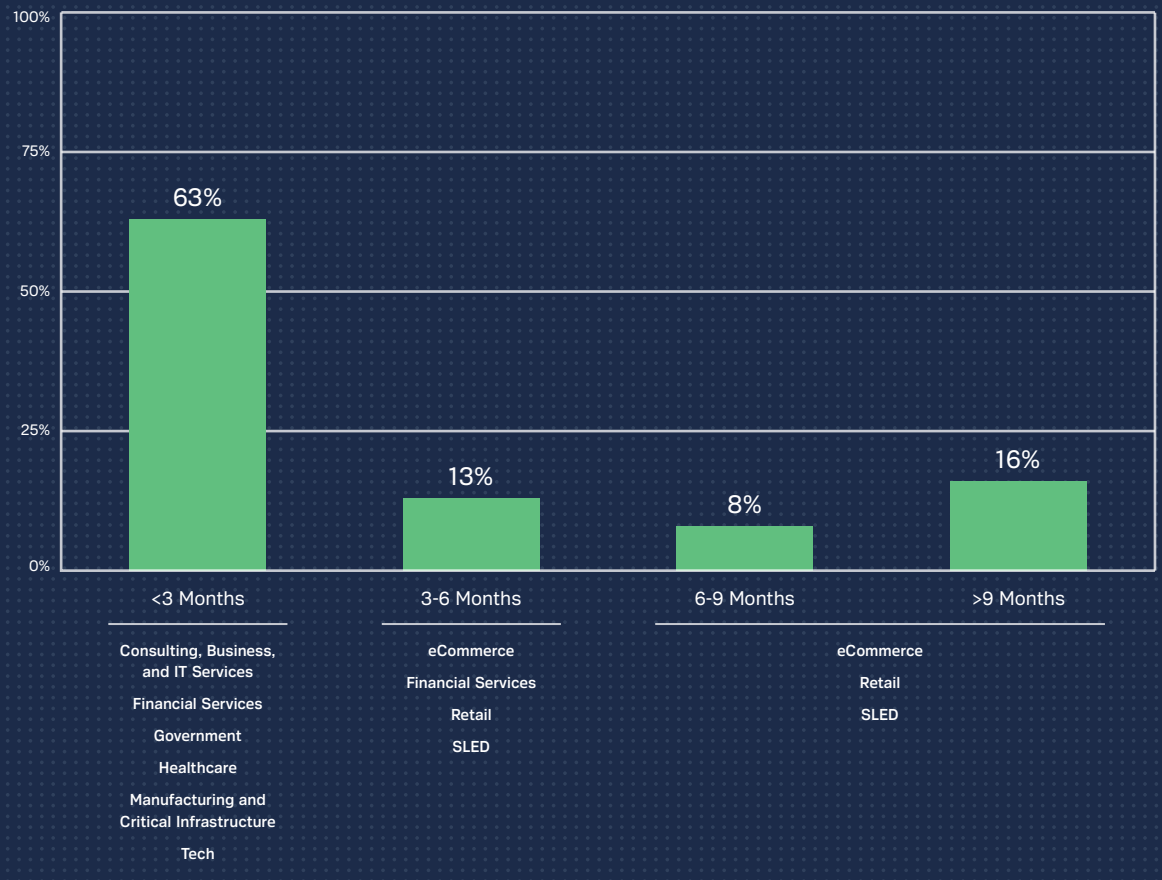
REMEDIATING EFFICIENTLY WITH DISCIPLINE

Synack

In general, Synack found that the majority of vulnerabilities are closed and remediated in less than 3 months.

However, this varies by industry. **Remediation** is completed 57% faster in Manufacturing and Critical Infrastructure than other industries. Their proactive approach means they are quick to patch once a vulnerability is found. Not coincidentally, the Manufacturing and Critical Infrastructure Attacker Resistance Score is the highest among all industries.

FIGURE 7: TIME TO REMEDIATE A VULNERABILITY BY INDUSTRY*



*The chart shows the distribution of average time to remediate a vulnerability during 2018. The industries highlighted in each segment account for the majority of vulnerabilities in that segment.

PART 7

TRUST REQUIRES A CONTINUOUS LIFESTYLE

Synack

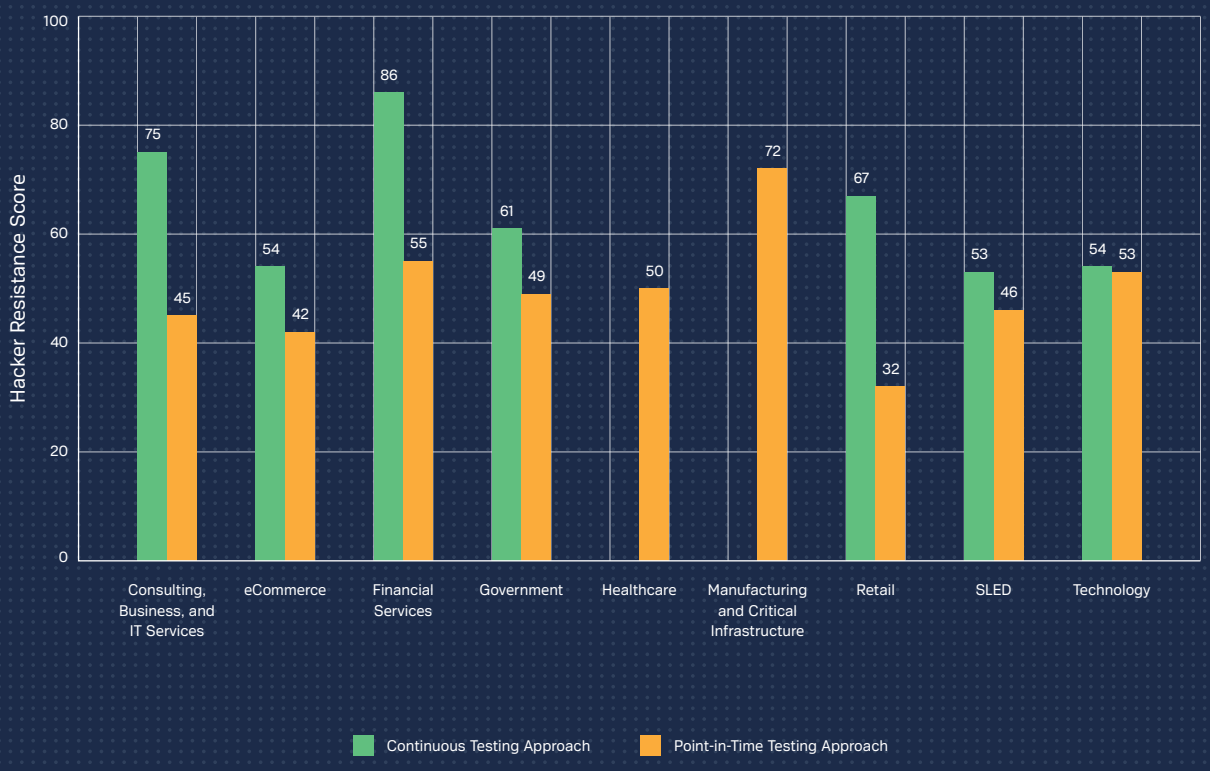
The data speak for themselves—building real trust takes not only time but continuous engagement.

It takes time for attacker resistance to build, just as it takes time to build a brand and build trust with customers. It should come as no surprise, then, that **organizations that conduct security testing continuously have 43% higher Attacker Resistance Scores on average than those that test on a point-in-time basis**. Security should be a continuous practice and these organizations tend to remediate faster and build security earlier in their development life cycle. These are the organizations that never stop looking for vulnerabilities that could undermine their operations, businesses, and brands. Kevin Fielder has adopted this practice as CISO at Just Eat. Kevin believes that:

> *"Building a security lifestyle into your organization gets you to trust. This means integrating security into the development lifecycle on a continuous basis from the onset of product development. By growing customer trust in the product, Security enables the business and the bottom line.*

KEVIN FIELDER
CISO, JUST EAT
REMARKS MADE AT SYNACK STUDIO AT RSA 2019

FIGURE 8: AVERAGE ATTACKER RESISTANCE SCORE BY TESTING CADENCE



Manufacturing and Critical Infrastructure and Healthcare still tend to rely on a point-in-time model. However, we expect this to change by next year. Continuous vulnerability discovery alone isn't enough to elevate the Attacker Resistance Score, however—it must be accompanied by continuous remediation. Even in industries that conduct security testing continuously, those industries that have longer remediation times, such as eCommerce, SLED, and Tech, also have lower overall Attacker Resistance Scores. On average, 16% of patches fail the first time around—patch verification and rapid remediation are critical to reduce the lifetime of a vulnerability.

Five Suggestions for Improving Security and Trust

Your ability to fully live up to your brand promise can be an enormous asset, and security is a central part of that commitment. Trust is a strong differentiator, and as such, security should be viewed as a strategic advantage and value center. Your entire company has a stake in building trust and should look for opportunities to leverage security to build brand value. Here are five suggestions to help you improve security and trust:

01 Security is Core to the Brand

Security is essential to protecting your organization's brand; working across your organization with other executives can also be very useful as a strategic differentiator as part of your brand to build trust. In the age of data breaches, privacy issues, and increasing regulation, showing your customers you take these issues seriously can have a positive effect on how they perceive your brand.

> *"At the core of trust between consumers and businesses is economics of convenience. Every customer must determine their threshold of comfort for sharing their private data in order to gain a convenience or bypass a hardship. Once that trust is broken many consumers will not continue to utilize the service because it is no longer worth the risk to continue to utilize that service.*

DAVID COHEN
BROWNSTEIN HYATT FARBER SCHRECK
PREVIOUSLY CHIEF ADMINISTRATIVE OFFICER AT CLEAR
REMARK MADE AT SYNACK STUDIO AT RSA 2019

02

Get an Outsider's Perspective on Your Security

Do you know how attackers perceive your organization? You won't know unless you've performed rigorous security testing. A crowdsourced approach provides the most realistic simulation of an attack. The good news is, if a crowd of security researchers sees your organization as difficult to attack, it will be easier for the board and your customers to trust that your security is working.

03

Adopt a Continuous Security Approach

Integrate security into your DevOps to keep pace with product innovation. Combining human intelligence with artificial intelligence can often give you the most realistic assessment of your security landscape. The earlier security testing takes place in the SDLC, the shorter the lifetime of a vulnerability, which helps keep upward pressure on Attacker Cost and downward pressure on Severity of Findings. Meanwhile, if you are the target of a breach, remediate as quickly as possible to increase the cost to your attackers and deter them from waging war on your brand and business.

04

Don't Just Find—Also Fix

Getting proactive about finding vulnerabilities is just part of the equation in building trust. The insights and intelligence derived from crowdsourced testing will allow you to pinpoint exactly where to focus your remediation efforts so you prioritize and execute well. Efficient remediation of vulnerabilities, just like rapid response to an auto or drug recall, is critical for minimizing damage and upholding the brand promise. Getting good intelligence from a combination of security experts and smart AI security tools is key to moving fast and avoiding a breach. Using a sound process will enable your remediation efforts and integrate with your development management systems.

05

Build a Security Ecosystem around Your Organization

You can do this by extending your talent pipeline through training partners and trusted crowds, the right technology and processes. And don't be shy about it: tell your employees and customers about your continuous security journey as part of building security into the brand. Remember: trust is vital to your business and brand, so make it part of your corporate story.

> *"Today, we have a trust deficit. It's a matter of when, not if, an organization will be breached. When you find yourself in that situation, the first question is not what do we do, but what do we know. Leaders that take time to diagnose their security, measure their progress, and invest in trust will stand out from the rest.*

DAVID DEMAREST
CEO, ASPENLINE REPUTATION STRATEGIES
LECTURER, STANFORD GRADUATE SCHOOL OF BUSINESS
FORMER BRAND AND COMMUNICATIONS EXECUTIVE AT:
THE WHITE HOUSE, BANK OF AMERICA, VISA

As CEO of AspenLine Reputation Strategies and former White House Communications Director, David Demarest, remarks, understanding your security health is the first step in building trust. And, now there's a way to measure how your security investments are working: through the Attacker Resistance Score. Use this as a benchmark to track your performance year-over-year and promote it to customers, the board, and the Street to prove that your business takes security seriously and is indeed trustworthy.

Next Steps

Read more about the **Attacker Resistance Score** on our website.

Learn more about the **Synack solution** by visiting our Products page.

Contact Synack to find out how our industry-first, innovative approach to exploitation discovery and management can work for your business.

About Synack

Synack, the trusted leader in crowdsourced security testing, helps organizations protect themselves from cyber attacks. By leveraging the world's best ethical hackers and an AI-enabled platform, Synack helps organizations find and fix critical security issues and provides valuable security intelligence on digital assets. The Synack platform delivers data-driven insights to help organizations understand their risk from a hacker's perspective and then mitigate that risk with a hacker's help. These insights secure critical infrastructure and leading brands and businesses around the world—Synack's crowdsourced penetration testing protects leading global banks, DoD classified assets, and close to $1 trillion in Fortune 500 revenue. For more information please visit **www.synack.com**.

Note: Data inputs continue to roll into future releases. Remediation is factored into Attacker Resistance Score for Crowdsourced Continuous Tests only.

Synack's proprietary Trust Score, or Attacker Resistance Score (ARS) is a measurement of how hardened your assets are against an attack. The overall Attacker Resistance Score provides a comprehensive view of an asset's susceptibility to attack based on a patented algorithm developed by Synack's data science team. It is a function of Attacker Cost, Severity of Findings and Remediation Efficiency. ARS is calculated by bringing together the following data inputs in a weighted combination, as detailed on the next page.

ATTACKER COST

This variable answers the question: "How much effort was required to try to penetrate your attack surface and discover vulnerabilities against your assets?" The Attacker Cost input is calculated using the full packet capture data collected by LaunchPoint®, our secure gateway technology. The raw testing traffic data details all Synack Red Team testing activity for a given assessment.

To calculate Attacker Cost, first, we isolate the assessment-specific penetration testing traffic data to understand its underlying structure. Then, using this structural information, we calculate the amount of "power," or work over time, that was expended to either successfully discover the vulnerability by the researcher or to probe the assessment leading to no discovery. The amount of attacker "work" is estimated by counting the number of "hits" (i.e. HTTPS requests for web apps or network packets sent for host networks) against the assessment location. Time is measured from the researcher's first login to LaunchPoint and hit on the assessment location to the time the potentially discovered vulnerability was submitted or a reasonable amount of time had elapsed. In this manner, an individual Attacker Cost is computed whether the effort expended leads to a vulnerability or not. Next, scores are normalized to a range of 0–100 using raw Attacker Cost values across the organization. Finally, Synack determines the Attacker Cost for each asset by averaging the Attacker Cost over all such efforts on that particular asset that may or may not have led to discovered vulnerabilities, where lack of discovered vulnerabilities indicate the assessment's resistance from cybersecurity risk.

SEVERITY OF FINDINGS

Derived from the severity and quantity of vulnerabilities discovered against your targeted assets. Similar to Attacker Cost, the Severity of Findings input is calculated for each vulnerability. In particular, the severity of each discovered vulnerability is measured on a CVSS scale of 0–10 where 0 and 10 denote the least and most severe vulnerabilities, respectively. Based on the number and severity of discovered vulnerabilities, a family of linear models are used to generate the Severity of Findings input on a per vulnerability basis, which is further aggregated to arrive at per asset input.

REMEDIATION EFFICIENCY

Measures how quickly and effectively an organization resolves identified issues in their environments. Post discovery of vulnerabilities on the customer's target, the vulnerability data are shared with the customer for mitigation and remediation. Post patch, we measure the patch efficacy and application time to estimate Remediation Efficiency. We also take into account the numerosity and severity of the vulnerabilities for which patches have been applied or have not been considered to further refine Remediation Efficiency.

APPENDIX 2: INDUSTRY DEFINITIONS

CONSULTING/BUSINESS & IT SERVICES
Organizations that derive the main source of their revenue from selling their expertise and professional services rather than a product

ECOMMERCE
Companies that sell the majority of their products electronically through the Internet

FINANCIAL SERVICES
Companies that manage money for individuals and other businesses, specifically credit unions, banks, credit-card companies, insurance companies, consumer-finance companies

FEDERAL
Federal government agencies that administer, oversee, and manage public programs such as branches of the military and other executive departments

HEALTHCARE
Companies that provide medical services for both patients and practitioners, manufacture medical equipment or drugs, or provide medical insurance

MANUFACTURING AND CRITICAL INFRASTRUCTURE
Production of merchandise for use or sale using labour and machines, tools, chemical and biological processing, or formulation. Their products are mainly sold to other manufacturers or retailers. This sector also includes energy and utilities companies.

RETAIL
Companies selling consumer goods or services to customers through multiple channels of distribution, but mainly focused on brick and mortar

SLED
This market represents five unique levels of government: state, city, county, education and special districts

TECH
Companies whose primary business is selling technology or tech services

---

Note: Synack's sample size is based on thousands of crowdsourced security tests across security-conscious organizations in the Global 2000, high-growth sector, and governments. As industries evolve, so will their definitions.