VOLUME 3

MEASURING THE VALUE OF SECURITY AMIDST UNCERTAINTY

THE 2020 TRUST REPORT



Trust is Critical.

Delivering smart penetration testing at scale. Synack's platform harnesses the world's most talented ethical hackers plus machine intelligence to deliver on-demand, continuous coverage with actionable results.

We are Synack, the world's most trusted Crowdsourced Security Platform.



Table of Contents

Foreword	4
Part 1: Measuring Up	6
Part 2: Key Trust Findings in 2020	9
Part 3: Security Amidst Uncertainty	13
Part 4: Building Blocks of Security Testing	17
Part 5: Conclusion	28
Part 6: Methodology	30

C-SUITE EXECUTIVES ARE ASKING:

"How can I accelerate the digital transformation of my company and be sure that these new digital systems are secure?" "Can I trust that my organization is properly designing cybersecurity into our systems while under pressure to deliver quickly?" "How can I be sure that applications developed in the rapid continuous deployment of Agile DevOps are secure?" "How secure are my systems and applications compared to my competitors and other industries?" "Can the board trust that the digital transformation they authorized me to implement is secure and they will not see our company's name on the front page of the newspaper?"

The cybersecurity of your organization's digital assets is as important as the health of your body. Ninety-eight percent of US citizens have not been infected by COVID-19; however, if you are one of the 2 percent who have been, you have suffered. Ninety-seven percent of the US citizens who have been infected with COVID-19 have fully recovered; however, 3 percent have not. The probability your company will suffer severe damages from a cyberattack is small – but if it does happen, the repercussions can be devastating. Many of us have always protected the health of our bodies by getting annual physical exams. Many of us have found problems in those exams that we could correct before they became serious. In my own case, my doctors discovered a 90 percent blocked coronary artery during a cardiac stress test. Thankfully, I'm now the proud owner of a "stent" and not a heart attack statistic.

In this time of COVID-19, we have seen that testing has saved hundreds of thousands of lives.

AS A CYBERSECURITY PRACTITIONER FOR OVER 30 YEARS, I CAN TELL YOU THAT PENETRATION TESTING HAS FOUND VULNERABILITIES THAT, WHEN FIXED, HAVE SAVED TENS OF THOUSANDS OF COMPANIES FROM BEING BREACHED, PREVENTED BUSINESS INTERRUPTION, LOSS OF INTELLECTUAL PROPERTY, CLASS ACTION LAWSUITS, BEING DRAGGED THROUGH THE PRESS, AND WORSE.

FOR THE "CYBER-HEALTH" OF YOUR DIGITAL ASSETS, THE ULTIMATE STRESS TEST IS THE PENETRATION TEST.

Standard vulnerability scanners will help you to find some of the common, lower criticality vulnerabilities, but smart penetration testing can find those "90% blocked arteries" that could kill you. The 2020 Synack Trust Report makes it clear that companies surviving the continuous barrage of cyberattacks are the ones that frequently test as many of their digital assets as possible with the appropriate depth and breadth to the criticality of that asset.

I have always found it ironic that the same digital technology that we use to drive our businesses, to reduce costs, increase sales and profits, and drive employment is simultaneously increasing our cyberattack surface. In today's environment we are implementing Agile DevOps with new versions of our software being put into operation every few weeks. In other words, the testing we did last month had a different attack surface, rendering last month's test and fixes insufficient. How can I trust that this month's system has not introduced new cybersecurity vulnerabilities?

Synack provides an established, proven, market-leading smart penetration test platform used by thousands of the world's preeminent organizations to find vulnerabilities in their digital assets that others can't. That's enabled them to fix the vulnerabilities and, in some cases, eliminate risk. Behind the platform, Synack's researcher vetting methodology brings together the highest quality, most skilled security researchers around the world.

Synack's game-changing approach to penetration testing enables both scalable as well as continuous testing of digital assets as new code is deployed. Its platform combines what an automated scanner can find with high confidence, triaged by

expert human researchers for confirmation, and expert security researchers using their skills and experience to find more critical vulnerabilities that automated scanners cannot. Because all vulnerability detections are fully triaged, confirmed by expert researchers, and detailed in actionable vulnerability reports, false positives are severely reduced and remediation is swifter and more efficient.

This approach has significant benefits. First, it discovers vulnerabilities that are created over time, either by changes in the production system, or by accidental misconfigurations. Second, having the variety of security researchers participating in the penetration testing, you get a much more comprehensive view of your vulnerabilities – like having a cardiologist, hematologist, and neurologist determining the root cause of an illness. Finally, the Synack platform offers a pragmatic analysis of how easy or difficult it is for a cyberattacker to penetrate your critical systems and what kind of damage could occur if that attacker is successful.

Synack calls this quantifiable analysis its Attacker Resistance Score (ARS)™ Metric. ARS helps your C-Suite determine how secure their assets are relative to your peers and competitors as well as those in other industries to give you a real world perspective on security risk. In other words, if ARS indicates your assets are attackable even by a script kiddie in a few minutes, then you would want to invest significantly more in your security posture. If ARS indicates you are closer to Fort Knox, then you can safely trust that your existing investment and security practices are keeping you secure.

THE 2020 SYNACK TRUST REPORT IS A MUST-READ FOR ANYONE WHO HAS EVER BEEN ASKED BY THEIR C-SUITE, CEO, OR BOARD: "CAN I TRUST OUR DIGITAL SYSTEMS? AND HOW DO WE COMPARE TO OTHER COMPANIES?" TWO OF THE MOST OFTEN ASKED QUESTIONS I HEAR FROM HUNDREDS OF COMPANIES.



MICHAEL CODEN
GLOBAL LEADER CYBERSECURITY PRACTICE, BCG PLATINION
BOSTON CONSULTING GROUP

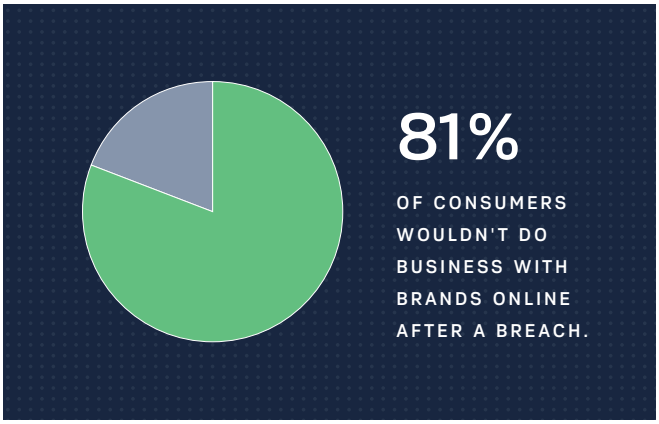
PART 1

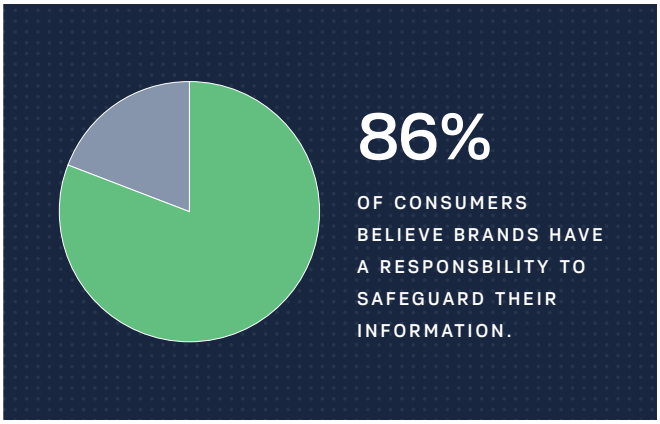
MEASURING UP

Synack

Trust has never been more important.

In 2020, as we face unprecedented challenges to our communities, global economies and the environment, consumers expect their favorite brands to be agents of positive change, provide stability and safety amidst uncertainty and develop innovative solutions to build healthier communities and a more equitable future.





SEVENTY PERCENT OF CONSUMERS BELIEVE BRAND TRUST IS MORE IMPORTANT THAN EVER, according to the Edelman Trust Barometer Special Report: Brand Trust in 2020. It matters for everything from major purchases to everyday buying decisions. When families order pizza via mobile apps, they count on their favorite restaurants to safeguard personal and financial data all while delivering fresh, hot pizza on time.

DISTRUST CAN SPREAD QUICKLY.
One of the fastest ways is a data breach. Eighty-one percent of consumers said they wouldn't do business with brands online after a breach. PwC's Consumer Intelligence Series found that 86 percent of consumers believe brands have a responsibility to safeguard their information. It's not just consumer trust that matters, either.

UNFORTUNATELY, BREACHES REMAIN ALL TOO COMMON PROBLEMS.
The carnage that results can require costly and monumental repair work. The price tags for the massive British Airways and Marriott breaches topped $100 million. Executives who mishandle breaches are often fired and can face criminal charges. Beyond breaches, reports of significant and harmful vulnerabilities—even when they aren't exploited—can lead to reputational damage, lost revenue, diminished confidence and government action against global tech companies.

The 2020 Trust Report is Synack's essential guide for CISOs, CIOs, executives, and other security professionals to understand how industries and sectors of the economy measure up when it comes to security preparedness.

The report is grounded in data from the patented **Attacker Resistance Score (ARS)™ Metric**[1] and draws information directly from the Synack Crowdsourced Security Platform based on thousands of security tests run through July 2020.

ARS scores range from 0 to 100. The higher the score, the more likely an organization is to successfully defend itself against a cyberattack. When it's lower, organizations face greater risk.

In 2020, the average score across all industries was 53, slightly down from last year's average of 54, but the details throughout the 2020 Trust Report show how scores can change year to year. While some organizations can receive an ARS as high as 100, scoring above 70 is a strong indicator of excellent security practices. Synack customers put a premium on security testing and proactively analyze new assets and digital applications. That means even if an ARS score periodically drops, these organizations can rapidly address new issues and therefore be better positioned to defend themselves than the competition. The goal is not to achieve the highest score and then move on, but to continuously measure how well new technologies and assets can withstand attacks. While some organizations may score higher or lower than the industry average, scores fluctuate for even the most proactive organizations.

1 Synack's proprietary Attacker Resistance Score (ARS) Metric is a measurement of how hardened your assets are against an attack. The overall ARS provides a comprehensive view of the target 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. Additional detail on the ARS metric available in the appendix.

ATTACKER RESISTANCE SCORE™ METRIC

A Realistic Metric Based on a Robust Model

Attacker Resistance Score Metric

=

Attacker Cost

The level of effort exerted by the Synack Red Team to penetrate the attack surface and find vulnerabilities

+

Severity of Findings

The severity and quantity of vulnerabilities discovered in an asset

+

Remediation Efficiency

How efficiently an organization resolves identified issues in their environments

PART 2

KEY TRUST FINDINGS IN 2020

Synack

FIGURE 1: 2020 ATTACKER RESISTANCE SCORES BY INDUSTRY				
Industry[2]	2018 (Trust V1)	2019	2020[3]	Incidents/ Breaches (Verizon DBIR Report)[4]
Government	57	47	61	6843/346[5]
Financial Services	61	57	59	1509/448
Healthcare	56	60	56	798/521
Technology	53	46	55	5471/360[6]
SLED	49	46	50	819/228[7]
Consulting/Business & IT Services	50	53	48	7463/326[8]
Ecommerce	45	48	47	5471/360[9]
Retail	54	45	46	287/146
Manufacturing/Critical Infrastructure	65	70	45	1070/407[10]
Average	**56**	**54**	**53**	

Government Agencies Bolster Cyber Defenses

It has been a difficult year for many sectors due to the unprecedented changes required to help fight the COVID-19 pandemic. That has been especially true within government agencies and departments globally. But this global sector also showed that continuous testing and speedy remediation are critical to effective and best in class cybersecurity.

Government bodies outperformed all other sectors evaluated in the 2020 Trust Report with an average score of 61. In the U.S., the new Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 19-02, which required federal agencies to remediate critical vulnerabilities within 30 days, caused agencies to move swiftly to address critical flaws. That made a key difference. Overall, agencies reduced the time to fix flaws by 73 percent, driving up the overall score for the sector.

In 2020, Synack worked with many government agencies throughout the pandemic to marshall the Synack Red Team, our community of the world's best ethical hackers, to ensure they were well protected when rushing out new technologies to meet growing and urgent needs. Many of their assets were critical to the pandemic response that would help our nation perform vital functions.

2 More detailed Industry descriptions can be found in the appendix

3 January 2019- July 2020 (We extended our analysis through COVID)

4 2020 Verizon DBIR Report

5 2020 Verizon DBIR Report: Public Industry

6 2020 Verizon DBIR Report: Information

7 2020 Verizon DBIR Report: Educational Services

8 2020 Verizon DBIR Report: Profesional, Scientific, and Technical Services

9 2020 Verizon DBIR Report: Used Information category

10 2020 Verizon DBIR Report: Manufacturing, Utilities

> *"Our crowdsourced pen-testing has been the main component of our response. Over 14,000 hours of testing – that measures out to 350 full days each year."*



JANET VOGEL
CISO
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Manufacturing and Critical Infrastructure At Risk

Other sectors faced a tougher year. The ARS for Manufacturing and Critical Infrastructure dropped to 45 in 2020 from 70 in 2019. The 36 percent decline is the largest reduction for any sector in the 2020 Trust Report. Within this sector, organizations did score as high as 90 and many of the highest scoring organizations are using a continuous approach to testing. Manufacturing and Critical Infrastructure have been under tremendous pressure due to rapid shifts needed to comply with guidelines to reduce the spread of COVID-19 and that strain is evident in their weakened security posture, as they continue to face a constant barrage of attacks. The 2020 Verizon Data Breach and Investigations Report analyzed 469 large incidents affecting Manufacturing, mostly the result of financially motivated and nation-state attacks. Unfortunately, critical industries often aren't well protected, as they often rely on legacy systems. According to a recent survey of critical infrastructure organizations by Greenbone Networks, just 36 percent of those surveyed said they have reached a high degree of cyber resilience.

Healthcare Threat Surface Expands Amidst COVID-19

Innovation in the Healthcare sector has been key to help defend against the pandemic. That rush to develop and deploy new apps would also lead to cybersecurity challenges. Additionally, law enforcement agencies worldwide reported an increase in attempted cyberattacks on hospitals. Despite those issues, the sector had the third highest average score as research and manufacturing organizations stayed vigilant and continuously tested their digital assets. While some organizations increased their scores as they prioritized testing and remediation throughout the pandemic, the average score for the Healthcare sector dropped to 56 in 2020 from a four-point uptick to 60 in 2019. The SRT tested numerous technologies directly related to those efforts. Overall, actual breaches at hospitals are down, a key indicator that thorough security testing is having an impact.

Ecommerce Making Progress as Digital Demand Surges

Retail and Ecommerce sectors have endured major changes to business as usual. With the surge in demand for online shopping and home delivery, the average ARS for Ecommerce jumped two points from 2018 and increased 7 percent during COVID because organizations prioritized testing for new apps and quickly remediating vulnerabilities. Meanwhile, the Retail ARS decreased 15 percent, reflecting a more challenging transition to all-digital commerce over the past six months.

Financial Services Endure Massive COVID-19 Disruptions

In spite of the massive operational undertaking to shift operations from office buildings to Zoom chats, Financial Services had the second highest ARS this year coming in at 59, just behind Government.

Financials Services adapted quickly through the pandemic to help employees adjust to their new remote work realities and ensure customers could continue doing business as usual when banks and brokerage firms closed temporarily. Continuous security testing played a significant role in the sector's higher ARS. Synack customers that adopt a continuous approach to testing score 18 percent higher than other organizations.

Digital Transformation Leads to Drop for Consulting and IT Services

The ARS dropped for Consulting and IT Services to 48 in 2020. In the cases of this sector, it appears that digital transformation continues to create growing pains. Organizations are testing more assets and deploying more technology, leading to an increase in vulnerability findings. This can affect overall scores.

But the journey toward trust isn't linear. It takes trial and error and quickly fixing to affect change. Many organizations within this category have successfully navigated digital transformation and continue to see their scores increase, some scoring as high as 96. The leaders in this sector score above the average, setting an example of proactive security testing for others in their industry. For example, government consultants have been hard at work to secure our national supply chain and proactively test these assets.

PART 3

SECURITY AMIDST UNCERTAINTY

Synack

The global pandemic put tremendous pressure on CISOs and other security professionals. As consumers rushed to adopt work-from-home platforms and video conferencing apps, they expected — and demanded — that companies would protect their security and privacy. Brands that couldn't maintain that trust faced real and measurable consequences.

Zoom is a prime example. It saw a surge in usage this spring as schools and corporations everywhere shifted to working remotely. But its credibility suffered from headlines in The Wall Street Journal and The New York Times about major vulnerabilities and the mere potential for hackers to exploit the platform. "Zoom bombing" became a real problem for schools and universities. Its stock tanked as a result. Companies such as SpaceX, Google, and the U.S. military banned its use and investors sued over the privacy and security problems. "Zoom backlash" became a common and trending catchphrase.

Zoom executives responded with a vigorous PR campaign and brought in well-known security experts to serve as security consultants. The CEO carried out a major apology tour. It even bought a cybersecurity firm. Zoom has surged back with a market valuation above $100 billion in August but the unforeseen vulnerabilities and the potential of other security issues opened the door to a crop of aggressive competitors at a critical time when enterprise customers need to maintain trust with their customers.

But organizations don't need to be caught off guard by major vulnerabilities that can cost them invaluable trust in the marketplace. Continuous testing is a remedy for those kinds of unpleasant — and damaging — surprises.

ARS Changes During Shelter in Place

Soon after the first stay-at-home orders went into effect across the U.S., ARS scores fell for some key industries such as Retail, Manufacturing and Critical Infrastructure. Also, quarantine requirements led to more time the Synack Red Team spent searching out customers' vulnerabilities. The time the SRT spent researching assets between March and April 2020 increased 70 percent compared to the same period last year.

> *"One positive note about the COVID-19 pandemic is it's clear that security is an enabler of the business.*



GREG MCCORD
GLOBAL HEAD OF INFORMATION SECURITY
CalAmp

FIGURE 2: ARS METRIC CHANGES DURING COVID-19

Industry	Change in ARS during COVID-19†
Consulting/Business & IT Services	-3.88%
Ecommerce	6.72%
Financial Services	-11.64%
Government	13.46%
Healthcare	-0.74%
Manufacturing/Critical Infrastructure	-6.59%
Retail	-7.15%
SLED	26.16%
Technology	6.38%

† Synack proprietary data from March 1,2020- July 1, 2020

> *Trust is absolutely critical. That means we prioritize our product security to keep our customers' trust. As a current CEO and former CISO, I leverage crowdsourced penetration testing to get realistic, adversarial insights on my attack surface. I choose Synack for that purpose. Synack's SaaS portal makes my actionable results easily accessible. They make my life easy by owning triage and patch verification, and they also let me check the compliance boxes that you know I need to check.*



MICHAEL COATES
CO-FOUNDER & CEO, ALTITUDE NETWORKS
FORMER CISO, TWITTER

Time to Double Down on Security

Throughout the pandemic, CISOs have focused on ensuring core business operations aren't interrupted by attacks. In fact, 70 percent of organizations surveyed this spring said they planned to spend more money on cybersecurity. At the same time, business leaders are looking more to the cloud as an essential part of their operations. The Boston Consulting Group found that 45 percent of companies surveyed expected migrating apps to the cloud to be a major priority over the next year or two.

That's a major security concern. A 2020 IBM Security and Ponemon Institute survey found that 19 percent of organizations do not scan during cloud migration. Even more troubling, 57 percent of those surveyed admitted that their organizations don't know which vulnerabilities pose the biggest dangers.

PART 4

BUILDING BLOCKS OF SECURITY TESTING

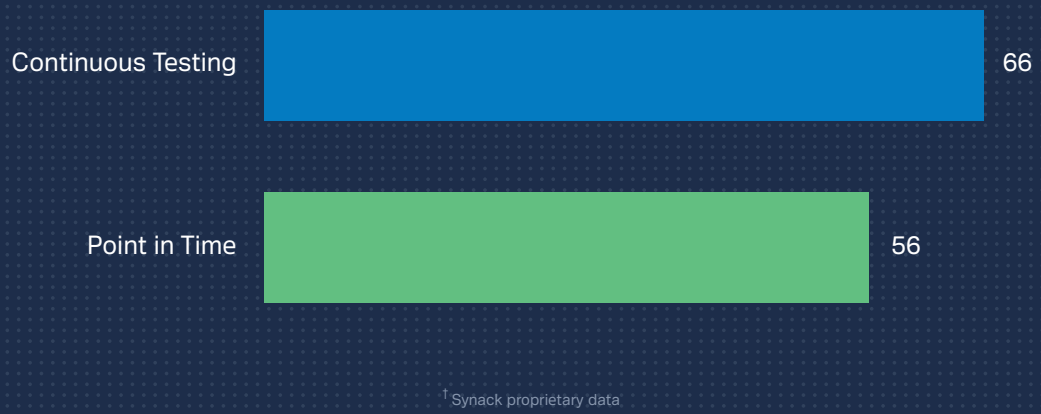
Synack

Security testing serves a simple purpose: find potentially devastating vulnerabilities, fix them quickly and learn from the process to build better code.

But the process is complex. It requires diligence and expertise. It takes the world's best ethical hackers to do it right and continuous testing from smart, AI enabled technologies. It needs attention and consistency to make a real difference.

Organizations that adopt a continuous approach to security testing have an 18 percent higher ARS on average than organizations that use point in time testing.

FIGURE 3: ARS METRIC FOR CONTINUOUS VERSUS POINT IN TIME TESTS†



† Synack proprietary data

Continuous Testing Increased ARS by up to 23 Percent

Businesses don't need to be caught off guard. There's a better way.

Organizations that adopt a continuous approach to testing see 18 percent higher ARS on average with some organizations up to 23 percent higher ARS than those that conduct only periodic tests. Organizations that test their assets regularly for three years decreased:

33.3%
IN SQL INJECTION VULNERABILITIES

30%
IN REMOTE EXECUTION VULNERABILITIES

57%
IN XSS VULNERABILITIES

> *"As we shift security left in our DevOps process, we begin to uncover vulnerabilities we hadn't seen before and we discover new vulnerabilities faster. To support this shift, we had to build an ecosystem around security so the dev teams would then remediate at pace.*



RONALD ULKO
DOMINO'S
INFORMATION SECURITY MANAGER

Types of Testing

SCANNING
The use of software and artificial intelligence to search for vulnerable or unauthorized systems and services.

PENETRATION TESTING
Evaluating systems for common vulnerabilities leveraging the Open Web Application Security Project (OWASP) or other standards body.

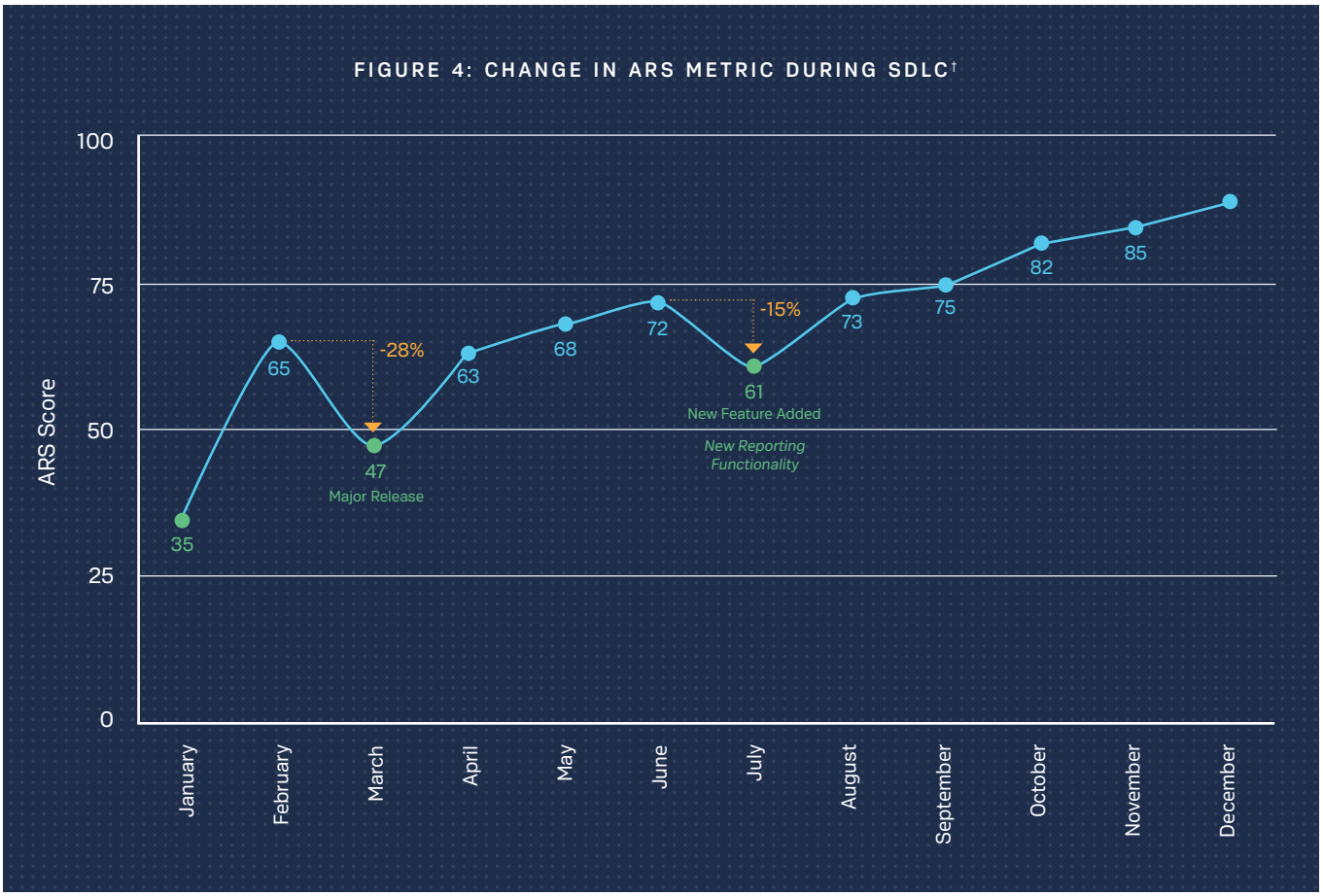
BUG BOUNTY TESTING
Researchers are allowed to attack the asset in their own creative ways, incentivized by bounties.

CROWDSOURCED SECURITY TESTING PLATFORM
A process that combines the best elements of the other three categories—this is the next generation of pen testing.

THE JOURNEY TO TRUST ISN'T LINEAR.

The increase in agile teams and frequent code releases means that point-in-time testing will fall short. Assets with frequent updates and sensitive data require continuous testing. It's the only way to achieve a comprehensive view of an organizaiton's testing environment in real time. That means assets can be evaluated when they are deployed and vulnerabilities discovered and fixed before attackers can exploit them.

FIGURE 4: CHANGE IN ARS METRIC DURING SDLC†



† Synack proprietary data based on numerous use caes

Increasing the Cost of Attack

WHY IT MATTERS

FIGURE 5: AVERAGE TIME TO FIND VULNERABILITY†	
Industry	Average Time to Find (hours)
Healthcare	15.5
Retail	16.0
SLED	16.7
Ecommerce	18.3
Financial Services	19.0
Consulting/Business & IT Services	19.8
Manufacturing/Critical Infrastructure	21.4
Technology	29.2
Government	30.1
Grand Total	**21.0**

† Synack proprietary data

The most secure companies — the ones that have scored the highest in the Trust Report — make carrying out attacks on them costly and timely. This means that attacks will look for easier targets. Digital crooks typically don't want to expend time, energy and money to penetrate targets. To increase resistance to attack, an organization must increase the cost of the attack.

Attacker cost is a component in the ARS model in which we measure and quantify effort required by a hacker to find a vulnerability. The average time to find a vulnerability decreased slightly from 22.8 hours in last year's report to 21 hours. Organizations are testing a wider variety of assets and some that include more sensitive information. Researchers are becoming effective and augmented tools are helping them more efficiently find vulnerabilities. Overall, attacks are getting cheaper. And that's a problem. A recent study found that attackers can execute a cyberattack for as little as $34 per month. Some criminal cyber operations cost only $3,800 a month to operate but can result in up to $1 million per month in profits.

The Technology sector had one of the highest time-to-find a vulnerability metric compared to other industries. As many technology companies adopted agile development and focused on security earlier in the process, their assets hardened due to regular testing. That meant developers left fewer vulnerabilities in the code. It also meant that discovering the more severe vulnerabilities took longer.

FIGURE 6: AVERAGE CVSS OF VULNERABILITIES FROM 2018-2020

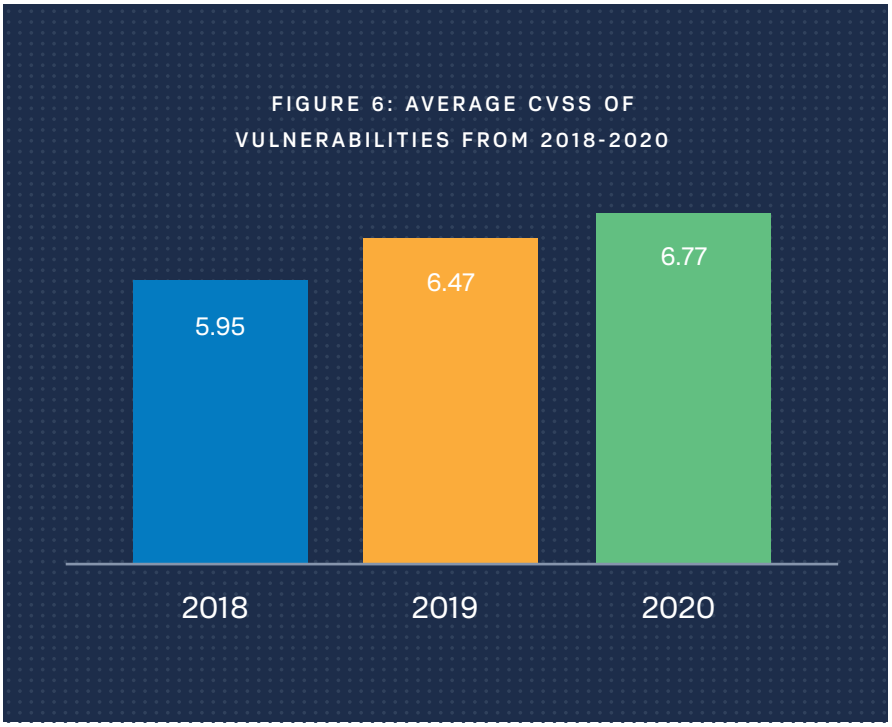


FIGURE 7: AVERAGE CVSS BY INDUSTRY

Industry	Average CVSS
Retail	6.13
Ecommerce	6.13
Technology	6.26
SLED	6.33
Financial Services	6.41
Consulting/Business & IT Services	6.48
Healthcare	6.66
Government	6.92
Manufacturing/Critical Infrastructure	6.96

Note: Figure 6 and 7 based on Synack proprietary data from 2018 through July 2020

Understanding the Severity of Findings

Assigning vulnerabilities a Common Vulnerability Scoring System (CVSS) rank helps organizations and CISOs understand the severity of flaws and it's one component of the ARS calculation. CVSS scores provide valuable information, but they're just one part of realizing overall risk. Even vulnerabilities that aren't highly rated can lead to devastating breaches. Hackers are able to compromise companies with even basic attacks.

Severity of Vulnerabilities

THE AVERAGE CVSS HAS INCREASED, BUT THE SPREAD OF SEVERITY HAS REMAINED FAIRLY CONSISTENT.

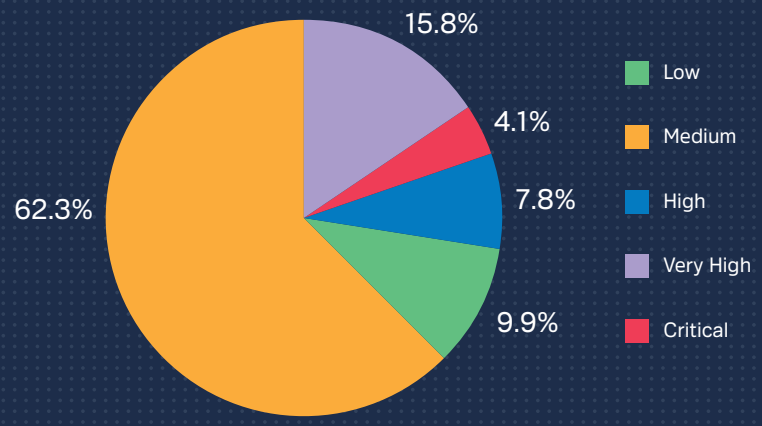
Organizations are increasingly testing a variety of assets including more host infrastructure tests. Host assets average CVSS, 7.75, is higher than both web and mobile.

FIGURE 8: AVERAGE CVSS BY ASSET TYPE

Asset Type	Average CVSS
Host	7.75
Mobile	5.68
Web	6.6

FIGURE 9: DISTRIBUTION OF VULNERABILITIES BY SEVERITY

The average CVSS has increased, but the spread of severity has remained fairly consistent.



Note: Figure 8 and 9 based on Synack proprietary data from 2018 through July 2020

The Distribution of Vulnerabilities by Category

FROM 2018 TO 2020, THE DISTRIBUTION OF VULNERABILITIES THAT SYNACK HAS SEEN OVER THOUSANDS OF SECURITY TESTS:

FIGURE 10: DISTRIBUTION OF VULNERABILITIES BY CATEGORY†

Vuln Type % of Total	2018	2019
Authentication/Session	8%	6%
Authorization/Permission	19%	22%
Brute Force	2%	2%
Content Injection	5%	3%
Cryptography	<1%	<1%
CSRF	7%	4%
DoS	<1%	<1%
Functional Logic	7%	7%
Information Disclosure	16%	14%
Insufficient Transport Protection	<1%	<1%
Other	<1%	<1%
Remote Execution	2%	4%
Server/App Misconfiguration	2%	5%
SQL Injection	5%	8%
XSS	26%	23%

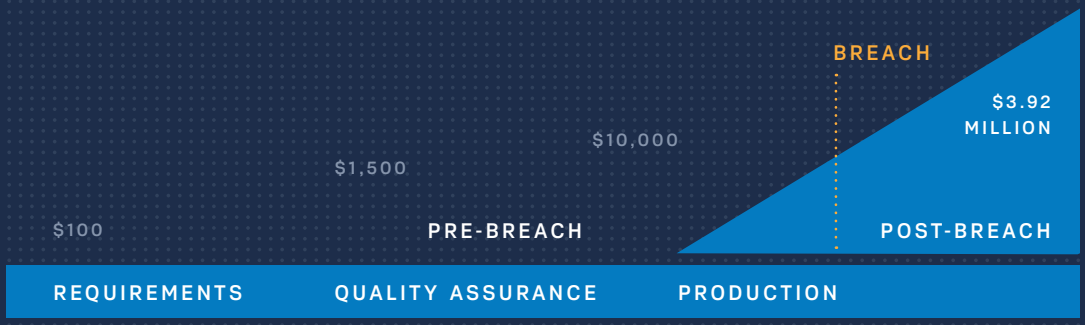
† Based on Synack proprietary data

Earning Trust Requires Speed

FIGURE 11:

Why testing early helps

THE COST TO FIX GOES UP THE LATER THE VULNERABILITY IS FOUND.



Source: Celerity/IBM System Science Institute+Data Breach Report- IBM Ponemon 2019

Organizations in the top quartile of ARS metric fix vulnerabilities on average within 30 days. Remediating vulnerabilities is just as important as finding them in the first place. Finding and fixing them early reduces costs significantly.

Remediation is the third component in Synack ARS metric and critical to reducing risk. As the number of vulnerabilities increases it becomes difficult for teams to keep pace and remediate all vulnerabilities. We recommend a three-step process to more effectively eliminate risk:

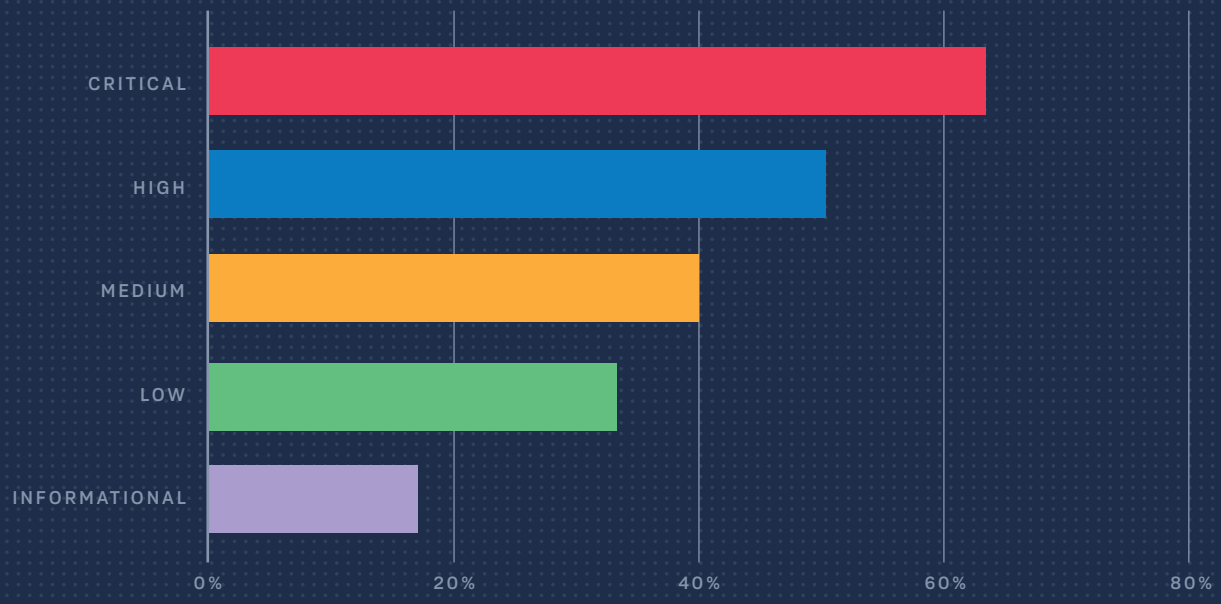
01 Prioritize the most critical vulnerabilties.

02 Follow a manageable, repeatable remediation process.

03 Build speed into your security lifestyle—it's an ongoing effect.

Critical Vulnerabilities Patched First.

FIGURE 12: % OF VULNERABILITIES FOUND THAT ARE PATCHED



Source: Based on Synack proprietary data through July 2020

Not surprisingly, critical vulnerabilities are patched at a higher and faster rate than ones with lower ratings, according to Synack's own data. Thousands of new vulnerabilities are disclosed every year, so knowing which ones to immediately patch or mitigate is a major challenge. Unfortunately, just 21 percent of respondents to the IBM Security and Ponemon Institute study on patching vulnerabilities said their organizations effectively patched flaws quickly. In some cases, according to the survey, it can take a month to address a critical or high-risk vulnerability.

Prioritizing vulnerabilities can help teams move quickly, but focusing only on the critical flaws ignores the possibility of attackers chaining together several lower-risk vulnerabilities. This is a common and dangerously effective tactic attackers use to gain administrator privileges—the "keys to the kingdom."

PART 5

CONCLUSION

Trust is Fragile. Protecting it is Critical.

Consumers need to trust the brands they rely on every day. They need to find it in their institutions, too. Without it, the best brands will struggle in the market and institutions can't perform vital critical functions like providing health services or even carrying out elections. Trust is paramount across all aspects of society — and maintaining in the face of increasingly severe digital threats is a daunting task.

It's also critical that CEOs trust their systems and the teams charged with keeping their organizations safe and secure. As we've seen this year, news of dangerous vulnerabilities and massive breaches can cause immense reputational and financial damage. Hacks and breaches can also lead to serious fines, government action and lawsuits. A proactive approach to cybersecurity is more vital than ever before.

That's the CISO's mandate. The ARS is the insight they need to ensure organizations are secure, avoid costly breaches and vulnerabilities, protect their customers and partners and maintain lasting trust and loyalty.

PART 6

METHODOLOGY

Synack

Methodology Summary

Synack's proprietary Attacker Resistance Score (ARS) metric is a measurement of how hardened your assets are against an attack. The overall ARS provides a comprehensive view of the target 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, SRT Skill, and Remediation Efficiency. ARS is calculated by bringing together the following data inputs in a weighted combination:

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.

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 to enterprise organizations and government agencies.

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

ENERGY/UTILITIES
Companies that produce and supply energy. This sector includes companies involved in the exploration and development of oil or gas reserves, oil and gas drilling and refining, or integrated power utility companies including gas, electric, and water.

ENTERTAINMENT/LEISURE
Companies that are focused on recreation, entertainment, sports, and tourism-related products and services including talent agencies and music publishing companies.

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.

STATE, LOCAL, AND EDUCATION (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.



© 2020 SYNACK, INC. ALL RIGHTS RESERVED.