WHITE PAPER

Securing the Digital Revolution of Healthcare

Digital Healthcare's Mass Expansion

Create common security and performance policies across your application portfolio to decrease risk and improve customer experiences.

The rapid transition to remote work prompted by the COVID-19 pandemic has dramatically accelerated digital transformation. This shift can be seen not only in industries such as e-commerce and financial services, but also in healthcare, where providers and payors are rapidly spinning up new digital infrastructure. This rapid response is necessary not only for continuity of care via digital telehealth and virtual healthcare, but also to support the business side of healthcare, with payments and business processes performed digitally through online portal accounts, digital payments, and the transfer of protected health information (PHI) over digital channels and health data aggregators.

ACCORDING TO THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, HEALTHCARE DATA BREACHES CATEGORIZED AS A "HACKING/IT INCIDENT" AFFECTED:

- 16.8 MILLION INDIVIDUALS IN 2020
- ALMOST 40 MILLION INDIVIDUALS IN 2021

Virtual healthcare has quickly become a dominant modality of care, allowing more patients, providers, and payors to manage healthcare digitally through their portals. A key lesson from the expansion of digital healthcare is that with more accounts, logins, and data comes an exponentially larger cyber threat landscape and, subsequently, more security breaches that lead to fraud.

As cybercriminals continue to target the healthcare sector, there's now evidence that vulnerabilities are being sold and organizations are being compromised using a Cybercrime-as-a-Service model. Medical information is considerably harder than financial information to recover after it has been compromised. Stolen credit card data can be retired; healthcare data cannot. This makes PHI a particularly valuable target for fraudulent sales and other deceptive practices. Healthcare fraud is gaining speed and momentum in the U.S. Of the $5.6 billion civil settlements and judgements involving false claims and fraud against the U.S. government in 2021, more than $5 billion—nearly 90%—involved healthcare sector entities.

Bad actors use the massive amounts of PHI with other personally identifiable information (PII) on the dark web to commit credential stuffing for account takeover, then submit fraudulent medical claims for payment. Some use malware to steal PHI or ransomware targeted to healthcare organizations, but cybercriminals increasingly turn to malicious automated bots to inflict large-scale healthcare fraud.

The Pervasiveness of Fraud

Understanding the vulnerabilities

Healthcare organizations are targeted by threat actors because of the vast amounts of valuable personal information they hold. This includes PHI, PII, and financial information, all of which are valuable in part because the different types of data can be divided and sold in different markets. In fact, the U.S. Department of Health and Human Services reports that in 2021, almost 40 million individuals were affected by breaches classified as "hacking/IT incident"—and that doesn't include incidents reported as "theft."

Identity protection is the first line of defense against fraud, and it faces the full brunt of assault with attempts such as synthetic identity creation and account takeover. But to maintain continued online access to healthcare, everyone needs to use credentials—patients, employees, administrators, insurance agents, suppliers: the entire ecosystem. Fraudsters are on the lookout for these credentials to help them circumvent security controls and commit fraud.

It's difficult to constantly adapt security and fraud defenses to keep up with rapidly evolving attack tactics—and if you are not keeping up, then you are falling behind and creating victims. The impacts to the healthcare industry can include:

- Questionable data integrity (PHI, IoMT, FSA and HSA card credentials)
- Bottom-line operational losses
- Poor business and patient care insights
- Damaged brand and lost stakeholder trust
- Regulatory fines (e.g., HIPAA/HITRUST)
- M&A infrastructure challenges in digital transformation
- Low network latency due to automated bot attacks
- A poor customer and stakeholder experience—patients, physicians, pharmacists, and associated costs for call centers

Improving security at the perimeter is a key opportunity for lowering fraud losses. To reduce these losses, we need to first understand how cyberattacks evolve into or enable fraud. Only then can we begin to decrease fraud losses that plague the healthcare system.

The implementation of better security upstream can lower the burden on fraud investigators downstream. Improving collaboration between fraud and security teams allows the development of better security solutions, reducing the financial burden of fraud and improving the customer experience for healthcare consumers and other stakeholders.

DATA AGGREGATORS

HEALTHCARE AGGREGATORS CAN INCREASE THE RISK OF A BREACH. COMMONLY, THEY OFFER EMPLOYERS THE PROMISE OF LOWER HEALTHCARE COSTS TO INSURE THEIR EMPLOYEES. HEALTHCARE AGGREGATORS FIND LOWER HEALTHCARE COSTS VIA WEB BROWSER PLUG-INS THAT SCRAPE EXPLANATION OF BENEFITS (EOB) AND PRICING INFORMATION FROM PATIENTS' CURRENT HEALTHCARE PROVIDER.

AT RENEWAL TIME, THE HEALTHCARE AGGREGATOR WILL FIND THE LOWEST-COST HEALTHCARE PROVIDER BASED ON THE ACCUMULATED INFORMATION FROM MULTIPLE PATIENT USER ACCOUNTS. THEN HEALTHCARE PROVIDERS END UP LOSING CONTROL OF PHI AND THEIR PRICING INFORMATION TO THESE HEALTHCARE AGGREGATORS.

Fraud's entry point into healthcare

Through cyberattacks, credentials are stolen, and attackers have become increasingly sophisticated over the past decade. Well-resourced organized criminal gangs and nation states have the same skills, tools, and services at their fingertips as IT teams. This includes the ability to use artificial intelligence (AI) and machine learning (ML) to create sophisticated campaigns that adapt to mitigation efforts. These dynamic attack methods keep evolving as the value of the data gained continues to significantly outweigh the cost of carrying out the attack.

In particular, credential stuffing has evolved from simply attractive to downright lucrative, particularly in attacks against healthcare providers and insurers. Because we cannot change our health history in the way that we might cancel a credit card, the same PHI can often be used fraudulently and repeatedly—often in collusion within the ranks of payors and providers.

Account takeover (ATO), defined as gaining unauthorized access and control to a user's account with the intent of committing fraud, is the primary objective of credential stuffing attacks. Unlike brute-force password attacks, credential stuffing typically leverages already exposed usernames and passwords from breaches at websites and applications other than the attack target, making detection of successful account takeover that much more difficult.

What's in it for the fraudsters? Attacker economics

Automated attacks are proliferating against organizations around the globe—especially in e-commerce, financial services, and healthcare. As the cost to launch these attacks continues to plummet, healthcare organizations are increasingly targeted by credential stuffing attacks that can lead to portal account takeover, flexible spending account (FSA) and health savings account (HSA) credit card theft, and claims and payment fraud. Although credential stuffing attacks have been around for years, they're quickly becoming one of the most prevalent attack types.

Degrees of sophistication exist when it comes to credential stuffing. A bad actor can launch distributed, automated login attempts using freely downloadable, public breach data with a zero-dollar investment and few technical resources, while still seeing occasional login successes since many individuals re-use passwords across multiple locations. With slightly more effort, attackers can use free automation tools such as Selenium to script mouse and keyboard interaction patterns that introduce randomness and entropy, making the behavior seem human-like rather than repetitive and robotic.

By spending just a few dollars, attackers can incorporate low-cost CAPTCHA solving services such as Google ReCAPTCHA to bypass basic bot defenses and purchase higher fidelity lists of credentials for a specific target. Proxy and anonymization services can even enable bad actors to launch attacks from residential IP addresses in geographic areas relevant to the victim organization, preventing even firewall geo-blocking from being effective.

With such inexpensive, effective tools, criminal organizations can rapidly change their tactics when defenders try to improve system security. Defending against attacks can become an almost insurmountable problem without specialized tools and dedicated security teams.

Assume you're going to be attacked

In general, you should assume that every external-facing application holding anything of value, whether PHI or other data, will eventually be subjected to automated attacks. It happens to even the most well-defended organizations with securely coded and patched apps. That's because attackers aren't exploiting flaws; they're abusing logic in order to commit fraud.

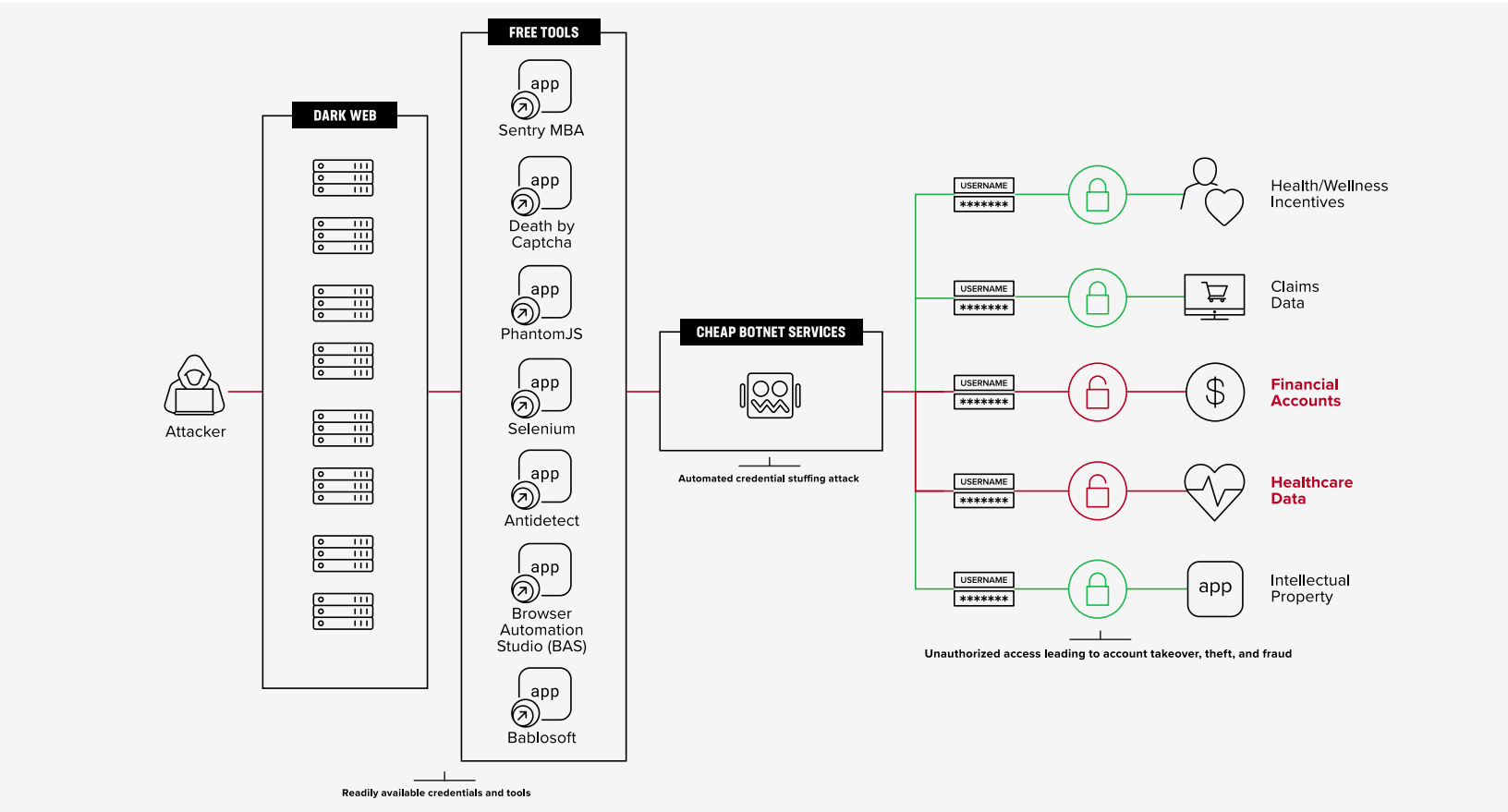

Figure 1: At a high level, this diagram shows how credentials, accounts, and a bevy of data products are obtained and used to gain unauthorized access that leads to fraud.

The ingredients required for these attacks—previously compromised patient or consumer credentials found on the dark web, tools to orchestrate an attack, and botnets to execute the attack—are becoming less expensive to buy, or even rent. As a result, successful credential stuffing attacks can net an attacker a consistent income. The decision to launch such an attack is a simple cost-benefit analysis that can all too easily tip in the attacker's favor.

In essence, cybercriminals have developed an industrialized attack lifecycle where application exploits and credential attacks are automated and weaponized.

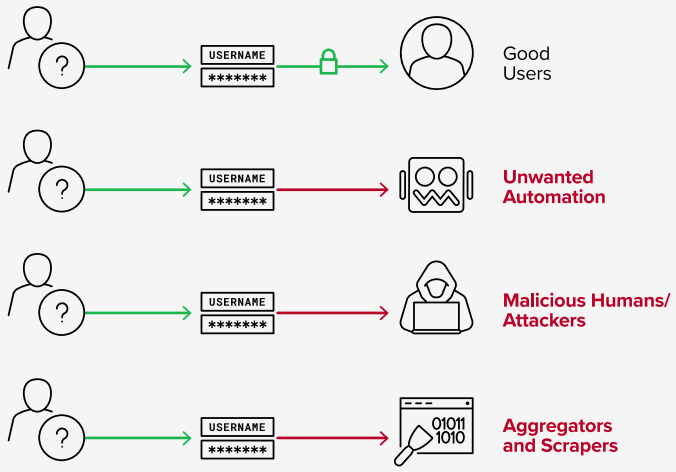

Figure 2: Attackers use victim profiles and automation frameworks to imitate real human traffic. By doing so, they're abusing inherent functionality to conduct automated and manual fraud.

Monetizing account takeover

Most organizations understand that if attack costs are low and the financial rewards for cybercriminals are high, they're sitting ducks for attacks. Automated attacks such as credential stuffing that target healthcare provider and payor organizations are designed to steal and sell PHI so that fraudsters can profit from account takeover, theft, and fraud. For example, having credentials for provider accounts, criminals might carry out the following fraudulent activities:

- Bulk prescription ordering (e.g., pharmacy account takeover)
- Provider billing (fraudulent claims and competitive price scraping)
- PII and PHI theft to feed into automated bot attacks or human attacks that break through secure perimeters
- Taking over member/patient portal accounts including individual prescription theft (e.g., modified shipping address and fraudulent claims)

If credential stuffing attacks on your applications have a high probability of success, the chance of attack escalates. On the flip side, if the chance of success drops due to the cost of penetrating the application security defense mechanisms you've put in place, this can severely diminish the attackers' ROI and they may decide it's not worth the effort and target another organization.

For the threat actor, it's simply a cost-benefit analysis. As long as the value outweighs the cost, the attack continues and evolves.

Figure 3 shows how the attack-value chain works.

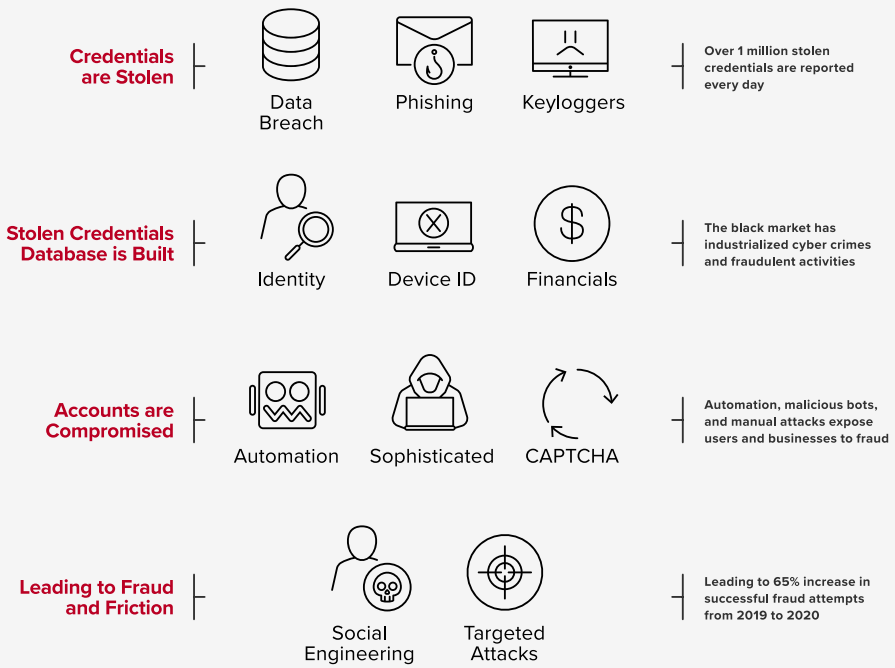

Figure 3: The attack-value chain: The accelerated attack lifecycle starts with unwanted automation, is sold through the black market, and results in account takeover and user friction to authenticate.

These schemes translate into cyberattacks. Figure 4 illustrates the threat landscape that leads to account takeover—through automated bot attacks, human attacks, and sophisticated fraud schemes.

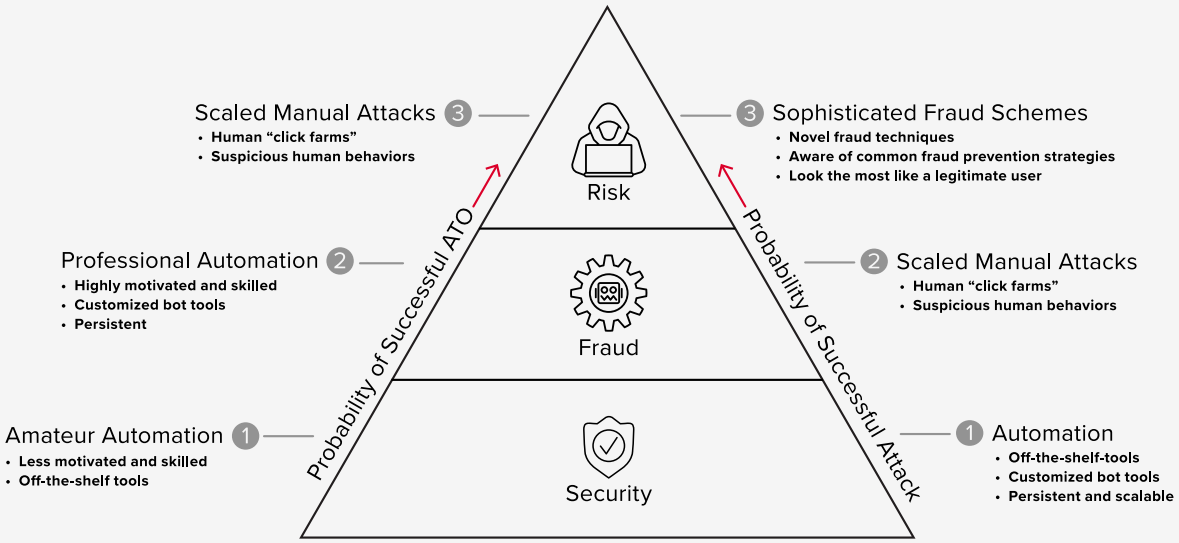

Figure 4: How fraud attacks move from security to fraud to risk: Credential stuffing, malicious bots, and human attacks progress in levels of sophistication to achieve account takeover.

WEB AND MOBILE APPLICATIONS FACE AN ONSLAUGHT OF SOPHISTICATED ATTACKS WITH ONE COMMONALITY: INSTEAD OF EXPLOITING APPLICATION VULNERABILITIES, ATTACKERS ABUSE AN APPLICATION'S OR PORTAL'S FUNCTIONALITY. IMITATION ATTACKS SIMULATE HUMAN BEHAVIOR USING HIGHLY SOPHISTICATED AUTOMATED TOOLS, THEREBY CONDUCTING FRAUD OR UNAUTHORIZED ACTIVITY AT SCALE.

Bot Detection and Management

Bots automate repetitive tasks, raise brand awareness, and engage users early in their digital journey. But in the wrong hands, bots and automation are powerful tools that can be used to compromise user accounts—resulting in account takeover and fraud. Forrester Research defines bot management as: "Solutions that identify and analyze the intent of automated traffic directed at an application, rejecting and misdirecting traffic from malicious bots and managing good bots, such as the ones from partners, to increase attacker costs while not affecting performance for paying customers."

The way to counteract automated and malicious bot attacks is through a sophisticated bot management solution—one that uses machine learning to adapt to attackers' tactics as they evolve. Enterprise Management Associate's recent bot detection research reported that the top three bot defenses in use by respondents include web application firewalls (55%), dedicated bot mitigation (51%), and CAPTCHA (48%).

As a counter-offense, the goal with a bot management solution is to build defenses that increase the attack cost, as discussed earlier. This will deter attackers who aren't able to

reach an ROI on their attack investment and block the path to fraud. To achieve this, the solution must classify real humans, good bots, and bad bots to allow legitimate users, and identify new attack techniques to ultimately reduce the costs of fraud and improve the user experience.

The attack lifecycle: It starts with credential stuffing

It makes sense that bot attacks and credential stuffing go hand-in-hand. Credential stuffing is a type of cyberattack that uses credentials obtained from previous, unrelated breaches to take over existing accounts on other web or mobile applications. For a more in-depth description of credential stuffing and its impacts, refer to the F5 Lab piece on how credential stuffing works.

Credential stuffing attacks include the following key steps:

- An attacker obtains leaked credentials (i.e., a username and password pair, a social security number, or a patient unique identifier) from prior cyberattacks.
- The attacker uses a software tool to automate the testing of stuffing these credentials against various healthcare websites and mobile applications.
- If a credential set is successfully authenticated, then it is flagged as a valid account—whether of a patient, healthcare worker, or even a payor portal login.
- The attacker can now take over the account and extract any value, including PHI, HSA/credit card information, and stored value (such as medical records), as well as access email, make fraudulent claims, and resell the account for further fraudulent activity.

Credential stuffing attacks have become incredibly easy and inexpensive. One only has to search for “combo list for sale” on the public internet to uncover the ecosystem built on buying and selling breached credentials. (A combo list is a text file that contains a list of leaked usernames and passwords usually obtained from different breaches and collectively stored within a file in a specific format.) Beneath the surface, on the dark web, is a thriving market as well, including combolists-as-a-service, where bad actors use a subscription model to continually provide freshly stolen credentials and other PII/PHI.

Once credentials are obtained, a credential database is built and then attack tools such as bots are employed to compromise accounts. The goal? Healthcare fraud in its numerous permutations. The final consideration is the havoc this wreaks on legitimate users trying to log in to their healthcare or insurance applications, creating a poor customer experience.

Account takeover prevention

As stated, the goal of credential stuffing is account takeover to commit fraud. ATO continues to be the most prevalent and expensive attack targeting financial institutions, e-commerce and many other organizations.

Our healthcare system can't function without portals and applications to provide services, perform diagnostics, run all Internet of Medical Things (IoMT) funneling through networks, and transfer payments with integrity. These applications must be readily protected to keep our healthcare system safe and secure, while providing ease of use for all the stakeholders using the systems and applications they rely on to deliver care. This system is under attack with every payor, provider, and patient as victims of the attack lifecycle.

The accelerated attack lifecycle starts with unwanted automation and ends with account takeover and application fraud. Just like in e-commerce and financial services, account takeover is growing at an alarming pace in healthcare and other industries. And the complexities of all the entry points and stakeholders in healthcare payors, providers, and patient pools make it an even more lucrative target. According to Javelin Strategy and Research in its 2021 Identity Fraud Study, account takeover fraud resulted in over $6 billion in total losses in 2020.

Preventing account takeover requires a set of countermeasures that rely on network, device, and user telemetry. These include solutions that in an integrated fashion can stop automated credential stuffing attacks, adapt to attacker retooling, and simplify and consolidate access.

"ATO has been an increasingly significant source of anxiety among fraud executives for years. Like application fraud, the root cause driving much of the growth has been the proliferation of the raw material that makes the fraud accessible to bad actors. The pace of data breaches that produce that raw material shows no sign of slowing and has also proved resistant to the environmental conditions that have disrupted virtually every other commercial enterprise. In fact, many fraud executives have made the argument that, if anything, the environmental conditions brought about by the pandemic will only accelerate the output of fraudsters' industrial-scale data-mining operations. … Add to this consumers' habit of reusing credentials, the unfortunate trend among fraudsters toward automation, and the ever-evolving nature of digital-first payments platforms, and it's not hard to see why ATO has been among the top three pain points for fraud executives for several years running."

- Aite Group, "Key Trends Driving Fraud Transformation in 2021 and Beyond," December 2021

DIGITAL GIANTS SUCH AS AMAZON AND APPLE, ALONG WITH BIG-BOX RETAILERS SUCH AS BEST BUY, WALMART, AND CVS HEALTH HAVE INCREASED THEIR INVESTMENTS IN HEALTHCARE OVER THE LAST THREE YEARS. THEY ARE FOCUSING ON DIGITAL, CONVENIENT PRIMARY CARE, AND CHRONIC DISEASE MANAGEMENT.

NEW CHALLENGERS ARE SEIZING ON THE FACT THAT CONSUMERS HAVE BECOME INCREASINGLY "DIGITAL FIRST" AND THAT HEALTHCARE INCUMBENTS CONTINUE TO SERVE FRAGMENTED, FRICTION-FULL EXPERIENCES CHARACTERIZED BY AN OVER-RELIANCE ON BRICK AND MORTAR AND AN UNDERUTILIZATION OF DIGITAL.

WHILE ANY SINGLE MOVE BY BIG-BOX RETAIL AND DIGITAL GIANTS MAY NOT BE SIGNIFICANT, THE SUM TOTAL OF RETAIL AND DIGITAL HEALTH INVESTMENT ACCELERATES ALREADY-IN-MOTION INDUSTRY TRANSFORMATION EFFORTS. IT ALSO HEIGHTENS THE PRESSURE ON HEALTHCARE CIOs TO DELIVER BETTER CONSUMER EXPERIENCES.

Client experience is just as important

The proliferation of account takeover will adversely affect legitimate users' experience through the inconvenience of identity authentication and authorization. In well-intentioned efforts to boost defenses, healthcare organizations are part of the growing trend to apply multiple methods to verify that users are who they say they are. And for those who are, they are put through the paces to prove it. This creates friction at the login transaction—leading to frustration and possible abandonment of service.

Therefore, the ongoing emphasis on improving the client experience affects which digital transformation initiatives may be prioritized. While loss prevention is the priority among fraud and risk executives, according to a recent Aite Group report, the same perspective is not necessarily shared by the leaders of other lines of business, channel and product strategy teams, and operations units, who are playing increasingly influential roles.

Let's consider all stakeholders:

- Patients logging in to healthcare portals
- Insurance consumers
- Payors
- Providers
- Suppliers such as pharmacies, medical device manufacturers, etc.

With these and more stakeholders in the healthcare ecosystem, weeding out those who aren't who they say they are is a complex undertaking. Consider that there are just three questions to understand whether a user is legitimate:

- Are you human?
- Are you good or bad?
- Are you who you say you are?

As shown in Figure 5, as the traffic volume of your applications rises, so does the friction to catch malicious attacks.

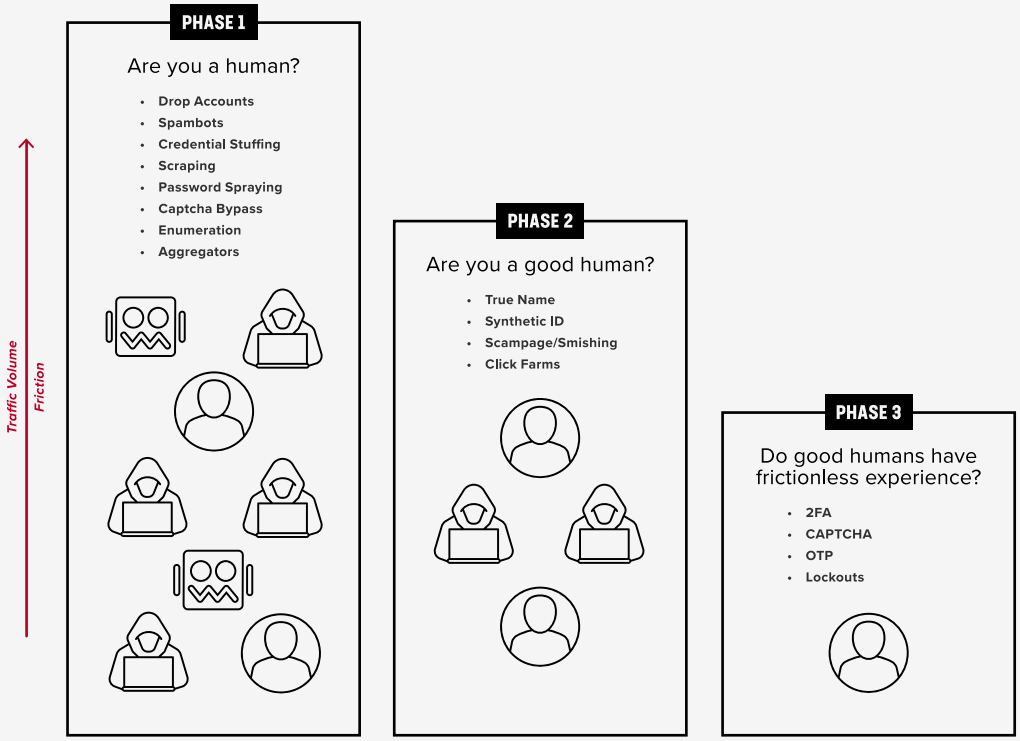

Figure 5: The more you know about your traffic (and users), the less friction you need to introduce.

There are solutions available to classify application logins while removing friction for good humans. To prevent account takeover while maintaining stakeholder trust, security teams can work closely with fraud teams to find an optimal balance between user experience and risk management, reducing frausters' success.

Some proven measures to prevent account takeover fraud and keep stakeholder trust include:

- Collecting the right telemetry signals
- Hardening your JavaScript and SDK
- Using human-assisted AI/ML to perform Stage II analysis
- Minimizing feedback to fraudsters
- Understanding how fraudsters evolve
- Not relying on any form of CAPTCHA
- Identifying user intent
- Using two-factor authentication sparingly
- Aligning security and fraud teams

Aligning the security and fraud teams is of utmost importance. Read on for the best path forward to build this collaboration in order to minimize the impact of security breaches that develop into large-scale fraud.

Security and Fraud Teams Working Together

Healthcare security roles, by definition, are destined to fail at preventing fraud. NetOps teams are tasked with monitoring and responding to network alerts, documenting daily tickets, and repairing the infrastructure. SecOps teams monitor and respond to security alerts and automate and orchestrate security measures. Fraud analysts focus on incident response—for example, investigating suspected fraudulent payments—and tune authentication rules based on false positives and false negatives.

Their collective failure isn't that they don't cover everything, but that they often don't overlap. Each team operates in its own silo while fraudsters, knowing this, conduct their business in the spaces in between those siloes. Fraud teams, for example, may have zero visibility into the security incidents that can signal potential fraud before it occurs, like an automated credential stuffing attack that leads to account takeover.

As a result, fraud teams spend unnecessary time on reactive analysis and mitigation efforts that could have been avoided if security and fraud teams had simply reached across lanes to share intelligence. The harsh reality is that many fraud and security job descriptions couldn't be more advantageous to fraudsters if they'd written those descriptions themselves.

All of this results in a siloed attack defense, which isn't nearly as effective as a highly coordinated defense strategy.

Breaking down the siloes improves risk management

While most healthcare and insurance leaders are aware of the need for a more unified approach to solving problems such as account takeover that span security and fraud controls, there is often resistance when trying to align disparate teams. However, the traditional siloed approach to security and fraud creates redundancies and limits agility to deliver care and reduce fraud losses in claim payments. Ultimately, the ability to respond to nascent threats and changing technology gets bogged down due to complexity, maintenance overhead, and headcount constraints.

As the world becomes more digital, healthcare organizations that provide the best customer experiences—whether those customers are patients, suppliers, providers, or insurers—will dominate their respective markets. The opportunity exists to align security, fraud, and digital team priorities around low-friction customer and stakeholder experiences that maintain security by eliminating bots and preventing account takeover.

Detecting online fraud throughout the healthcare ecosystem

With secure login processes and monitoring capabilities that provide visibility into human users, good and bad automated bots, device IDs, and other telemetry, you can detect fraud earlier to better utilize your fraud investigation resources on high-stakes case management.

Bot management and account takeover prevention solution vendors deliver value across a range of capabilities and orchestration. But in choosing a vendor, it's critical to give all stakeholders in your healthcare ecosystem a streamlined account access and management experience whether they're a payor, provider, supplier, or patient. Moreover, minimizing false positives will prevent you from adversely affecting the user experience or over-taxing already over-burdened special investigation units.

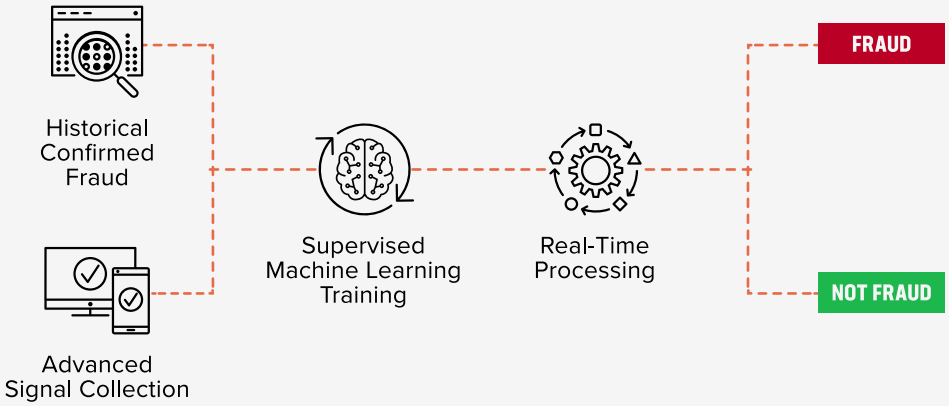

Figure 6: Solutions that apply these methods make it possible to identify good, returning users.

The goals are to safeguard PHI, eliminate fraudulent bulk prescription ordering, prevent account takeover and malicious aggregators, and ensure payment integrity to avoid fraud investigations after the money is paid out ("pay and chase"). This is indeed a tall order for the healthcare industry, but it is possible. To reduce fraud as an outcome, realize that the security vendors you use to fight fraud must be able to adapt to the changing tactics of very motivated bad actors.

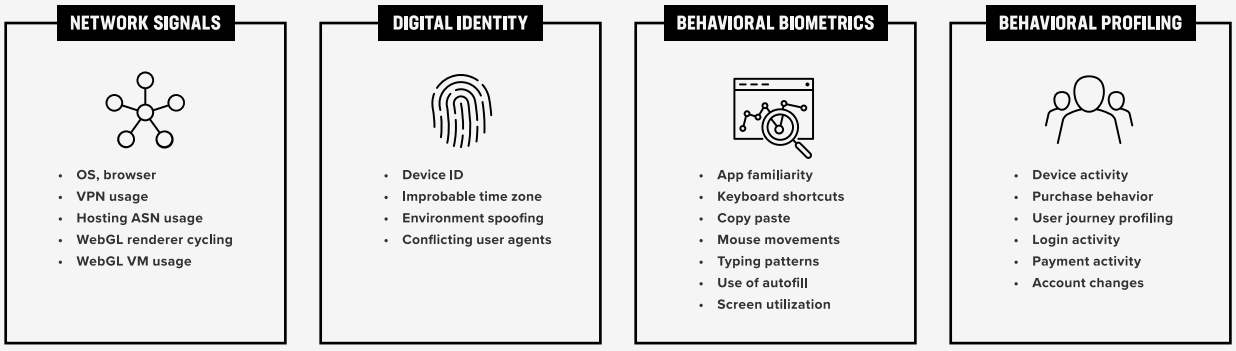

Figure 7: To reduce fraud, the security vendors you use must be able to adapt to changing attacker tactics.

A RECENT FORRESTER TOTAL ECONOMIC IMPACT™ STUDY REVEALED THAT F5'S BOT DEFENSE SOLUTION:

- REDUCED COSTS OF FRAUD FROM BOT ATTACKS BY 30%
- LOWERED COSTS FROM CREDENTIAL STUFFING ATTACKS BY 96%
- DECREASED ACCOUNT LOCKOUTS AND THEIR COST TO SUPPORT BY 88%
- ELIMINATED MANUAL BOT PROTECTION PROCESSES AND REDUCED RULE-SETTING WORK BY 40%
- IMPROVED COLLABORATION OF SECURITY AND FRAUD TEAMS TO IDENTIFY FRAUD PATTERNS AND OTHER MISSED FRAUD

Finally, in your efforts to safeguard patient data and healthcare records or EOBs, it's critical not to put users through an agonizing experience as they log in to applications. It's possible to identify good, returning users using methods such as:

- Monitoring traffic levels and success rates on your key application flows—including password reset and account creation
- Anticipating attacker evolution, knowing that the most motivated attackers will retool
- Encouraging collaboration across siloes to avoid gaps in security, fraud, and identity
- Considering a Sofware as a Service (SaaS) model to ease the burden on your security, fraud, and development teams

How F5 Can Help

F5's solution for mitigating malicious bot and human traffic provides data analytics and controls for security and fraud use cases across healthcare. It also uses AI and human intelligence to continuously improve efficacy, enabling you to stay ahead of the evolving attacks of bad actors.

F5's fraud and risk solution goes beyond traditional bot mitigation. By defending the world's largest companies for multiple years, F5 has developed expertise in not just identifying whether the request was made by a bot or human, but whether the request was made with malicious or benign intent. This provides healthcare enterprises full context into the user's transaction flow, enabling real-time fraud prevention.

The service also delivers advanced protection against credential stuffing and account takeover attacks:

- Proprietary signal collection about the visitor's web browser, PC, or mobile device, interaction pattern and network request structure enable F5 to uniquely identify attack infrastructure and inorganic behavior patterns, regardless of anonymization tactics and human-mimicking scripted actions.
- Backed by specialized human analysts and highly trained machine learning systems, F5 identifies new attack patterns and develops countermeasures when bad actors retool their scripts or infrastructure to avoid detection.
- F5's 24/7 Security Operation Center (SOC) tracks both the health and traffic patterns for F5 customers, acting as an extension of the organization's security team.
- Flexible deployment models enable protection to be incorporated as an inline or out-of-band security layer, regardless of your underlying infrastructure.

F5 offers a proven approach for solving security and fraud challenges throughout the healthcare industry so that you can identify good and returning users and reduce fraud as an outcome.

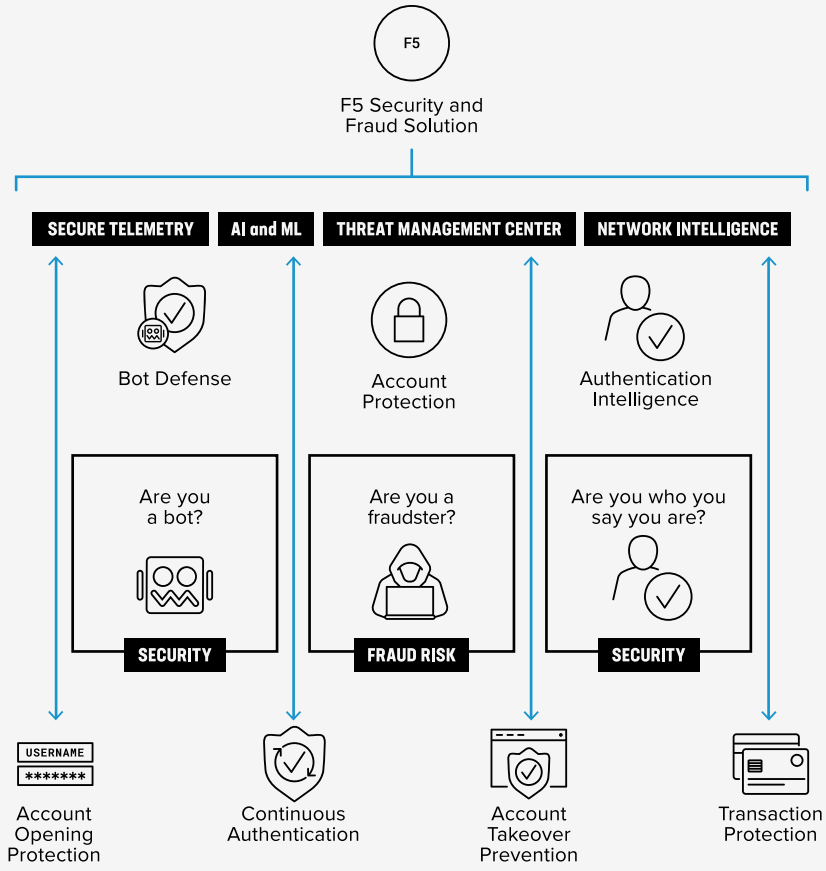

Figure 8: The pillars to a comprehensive fraud and security defense: Bot defense, account protection, and authentication intelligence answer the three critical questions to reducing attacks, fraud, and user friction.

Using this advanced solution, healthcare organizations can stop unwanted automated requests, control the flow of PHI, and protect their stakeholders. F5 can also identify healthcare aggregators and allow or deny access to member information.

Conclusion

As more healthcare providers digitalize their operations and services, they're striving to increase efficiency and improve the user experience while ensuring application security. Unfortunately, however, this has led to an expanded cyber threat landscape, and thus more security breaches and fraud. Healthcare organizations are an especially attractive target for bad actors because of all the PHI they hold along with other data.

To reduce their risks while maintaining a positive user experience for their entire ecosystem of patients, employees, administrators, and others, healthcare providers need to stay ahead of fraudsters as they launch increasingly sophisticated attacks. By adopting an advanced security and fraud solution that continuously improves its feedback loop using AI and human intelligence, healthcare organizations can protect their assets against malicious human and bot traffic—and focus on delivering the highly seamless digital experiences their stakeholders need and desire.

For more information read Gartner: Market Guide for Online Fraud Detection and Forrester's study, The Total Economic Impact™ Of F5® Distributed Cloud Bot Defense.