5 ways fintech security teams can protect digital trust

Securing customer data in an industry beloved by cybercriminals

LACEWORK

Financial technology — otherwise known as “fintech” — is a burgeoning industry. Over 20 years, the digital transformation of banking has moved from in-person banking to online banking and to, now, cloud-native banking on internet applications, separate from any brick-and-mortar locations.

The rise of cloud computing has driven these changes. It has changed how financial organizations develop, build, and manage infrastructure and applications. Yet navigating the tools to secure innovation in the fast-paced fintech industry is anything but easy. And in this industry where sensitive financial data abounds, there are attackers eager to exploit this data for their own financial gain.

At its most foundational level, consumers trust fintech companies with their financial integrity. And these organizations must protect that trust at all costs — even in the face of rising cyberattacks.

This eBook offers some practical ways fintech companies — and financial organizations, in general — can maintain customer trust and continue innovating safely and securely.

40% of consumers between the ages of 21 and 55, subscribe to fintech services, with half spending $10 or more each month, for a total of $13 billion annually.[1]

Fintech on the rise

Up to 75 percent of consumers across the globe use at least one fintech service — a number that is expected to grow.[2] Forty percent of consumers between the ages of 21 and 55 subscribe to fintech services in some capacity, with half spending $10 or more each month. And 30 percent of Americans within this same age range consider a fintech company as their primary checking account provider, as opposed to a traditional bank.[1]

Cloud adoption has driven the rise of fintech. Although initial cloud adoption in finance was slower than other industries, 83 percent of financial services organizations now say that cloud initiatives are already underway or are in the foreseeable future.[3] The IDC sees cloud spend within this sector growing 16 percent per year for the next two years, totalling $77B by 2024.[4]

The cloud opens up unlimited opportunities for both traditional brick-and-mortar banking institutions and digital-native fintech startups. Cloud computing offers lots of benefits, including speed, scalability, accessibility, and unlimited storage capacity. Perhaps most appealing are the cost savings from not having to maintain hardware and only having to pay for what cloud resources are used.

But on the flip side, cloud computing brings about a certain amount of risk — especially in the financial services industry, which has historically been a prime target for cybercriminals.

$112.5B
Fintech Market in 2021

$332.5B
Fintech Market in 2028[5]

The great data heist

Unsurprisingly, financial services is a perpetual leader in cybercrime. According to IBM Security, finance and insurance was the second most attacked global industry in 2021 (22.4% of attacks), eclipsed only slightly by the manufacturing industry (23.2% of attacks). And while the industry's rate of attack dropped incrementally year-over-year (down .6%),[6] the forecast looks grim. According to a VMware survey, 80 percent of financial institutions reported a cyberattack increase over the past year, and 82 percent indicated that the perpetrators are clearly becoming more sophisticated.[7]

As finance migrates to the cloud and fintech reimaginies financial services, cyberattackers continue to invent sophisticated ways to exploit personal financial management (PFM) tools and payment methods. The proliferation of connected networks and devices spanning multiple platforms provides an ideal attack vector for cybercriminals to go unnoticed. With the advent of online banking and the benefits of big data on global markets, hackers take advantage of organizations that are not continuously monitoring their users, data, and infrastructure. Adding to the lure is the dark web and the abundance of accessible financial data to capitalize on.

Phishing Attacks

Phishing was the most common infection vector for financial services in 2021.[6] Attackers trick consumers or organizations into handing over sensitive information to penetrate bank networks and use it to impersonate or defraud.

Account Takeover

Fraudsters will stop at nothing. From password sharing, credential stuffing, or cryptojacking, they work to gain access to accounts to use or sell them for profit.

Identity Fraud

Malicious tactics make it easier for cybercriminals to hide in the cloud with stolen payment care data and stolen identities.

98% of fintech startups are vulnerable to web and mobile application attacks.[6]

Don’t break what isn’t easily fixed

For fintech companies, the most important asset stolen by cybercriminals isn’t data — it’s customer trust.

Much like healthcare, finance is an industry where companies are dealing with livelihoods. Mishandling this heavy responsibility can have an immense negative impact on a business. In fact, one recent study showed that nearly 25% of American adults named financial services as the industry where trust is most important to them. The only other industry that surpassed financial was, unsurprisingly, healthcare (40%). The next closest industry to the two was food and beverage, with less than 10% of the votes.[9]

In the past year, three large consulting firms each independently sponsored research around trust and finance — with a specific focus on fintech. And, independently, each research firm seemed to land on two interconnected truths: in finance, 1) trust is difficult to earn but 2) trust is easy to break.

1. **Trust is difficult to earn.**
   - **30%** of American consumers stated that trust was the primary factor for considering a financial institution.[10]
   - **87%** of consumers said that their trust of financial institutions hinged on their ability to secure personal data.[9] Similarly, according to Ernst & Young, the biggest driver of financial trust is confidence in securing customer data. This is the unanimous top driver across all age groups when choosing among 14 other drivers.[2]

2. **Trust is easy to break.**
   a. **66%** of consumers said that they would stop using a financial institution if there was a data breach affecting their data.[9]
   b. **21%** of consumers verified that they have, in fact, stopped using a financial service on account of a data breach.[9]

5 keys to locking the vault on customer trust

So, the bottom line? Exploited vulnerabilities can be fixed. Malicious actors can be identified and largely removed from environments. But the loss of trust is something that has staying power.

Because of this, fintech is an industry where the rewards are rich but the risks are many. An industry on the upswing, garnering mass adoption across demographics, with limitless potential in the cloud. But an industry where the trust that took so long to gain can be lost at the stroke of a key. And the odds aren't in favor of regaining that trust again.

Luckily, there are some practical steps fintech companies can take to make sure that their data — and their consumers' data, by extension — remains protected. These steps range from things that can be implemented as soon as closing this eBook to things that may require some time and effort to deploy.

Here are 5 tips to tighten your grasp on consumer trust at your fintech company.

1. Build a cautious culture

Phishing. Just reading that word may have put you on edge. Why? **Because, according to IBM, phishing was the most common infection vector in 2021, claiming 41% of all successful cyberattacks across all industries.** And phishing comes out just ahead of the average in financial services, where it claimed 42% of attacks.[6]

Phishing has caused some of the most destructive financial cyberattacks of all time. In 2014, JP Morgan Chase leaked the personal information of 76 million households and 7 million small businesses. The cause? One single successful phishing attack against an employee's personal computer.[11]

While phishing attacks are becoming more sophisticated, they have always preyed on the most widespread vulnerability — human error. And, for this reason, phishing is an issue that can never be completely solved. But with phishing leading the pack in 2021 for infection vector frequency, pushing past the previous year's leader (vulnerability exploitation),[6] it's worth trying to move the needle in the right direction.

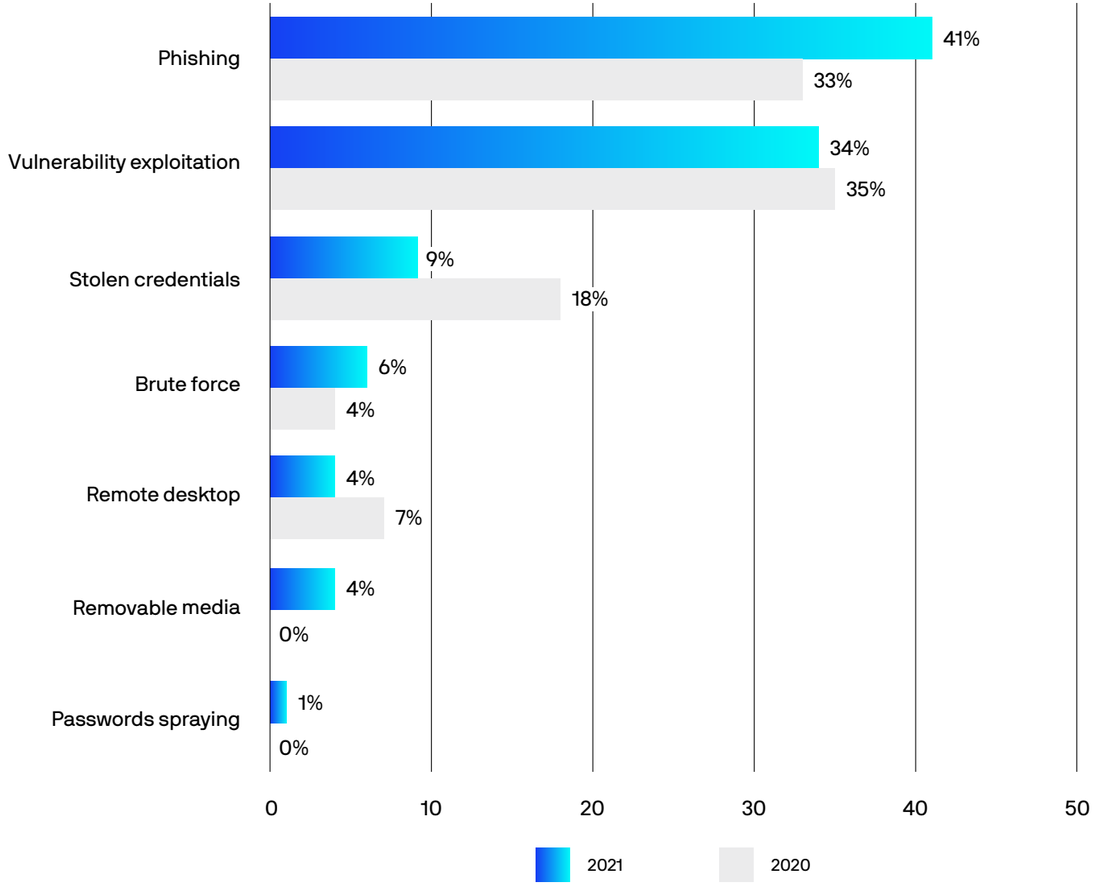
To fight against phishing, fintech companies can implement the usual suspects — email filters, VPNs, antivirus software. But, at the end of the day, education is going to be key in this sector. Why? Because, more than practically any other industry, finance is pinpointed by malicious actors. And fintech workers — and your own customers — should know that.

Educate your employees and your customer base on the fact that phishing is the most used infection vector for cyberattacks. That financial services is a perpetual leader — arguably *the* perpetual leader — in cyberattack frequency. Of the different ways attackers can successfully execute a phishing attack, beyond suspicious emails. Of your company's own security policies. And put this information in front of them early and often.

This is a practical tip you can act on, starting tomorrow.

Top infection vectors, 2021 vs. 2020

Breakdown of infection factors observed by X-Force Incident Response, 2020 –2021 (Source: IBM Security X-Force)



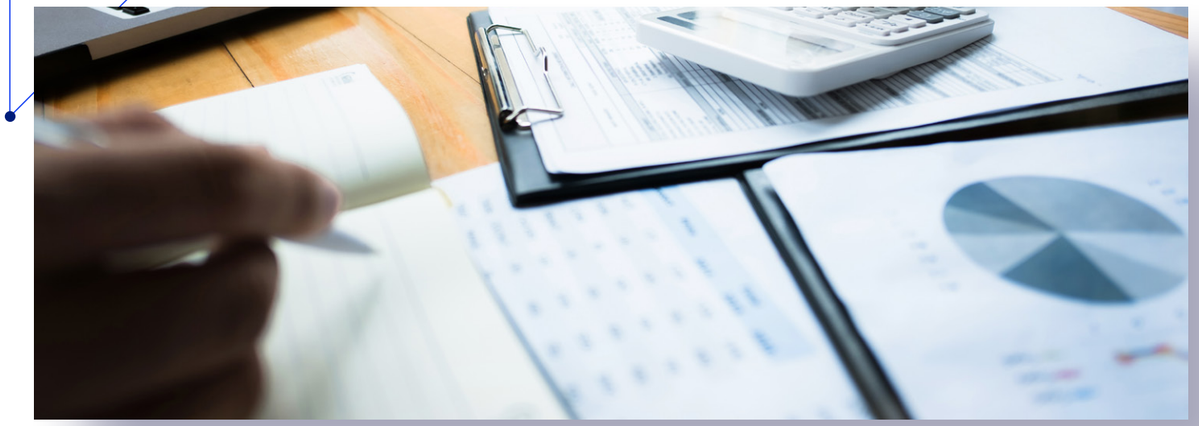
2. Fix your vulnerabilities (and avoid creating new ones)

In 2021, vulnerability exploitation was the second-most frequent infection vector, just behind phishing.[6] This should come as no surprise. While the cloud offers the ability to develop faster, more cost-effectively, and at scale, it can create an environment riddled with blind spots and gaps, leaving data at risk.

Organizations are encouraged to speed application development, embrace agile processes, and ship as soon as possible. These pressures can sometimes lead to accidental mistakes, misconfigurations, or security gaps that open the door for malware. Premature deployment can leave security teams scratching their heads, not knowing where infrastructure is deployed, what operating systems are being used, and more.

Fintech, specifically, is a highly competitive industry where time to market matters. Fintech companies can't afford to cave in to a "win at all costs" mentality, where speed is favored over security.

Fintech companies should consider modern approaches to security that allow development teams to not sacrifice security for speed. For utmost protection in a competitive industry, they should integrate security practices into the software supply chain and "shift left," allowing teams to spot and fix issues before they reach production. These technologies could include private image registry scanning, inline scanning within CI/CD pipelines, proxy scanners, and integrations with admission controllers.



43% of organizations note that faster development cycles of CI/CD is a top challenge for security teams because they lack visibility and control in the development process

46% of organizations admit to granting unauthorized access to applications and data, as a result of IaC template misconfigurations

68% of organizations consider the adoption of developer-focused security solutions and shifting some security responsibilities to developers to be a high priority[12]

3. Don’t bank on old tools

So let’s assume the worst has happened. Let’s say a fintech employee falls victim to a phishing attempt. Or perhaps a bad actor finds that vulnerability, as a result of a rushed code deployment. Traditional security tools that companies relied on for decades to protect their on-premise data centers and endpoints simply simply aren’t fit for the cloud.

Historically, companies have focused on protecting their systems from known threats by using Indicators of Compromise (IOCs). Unfortunately, this strategy depends on rules — on companies knowing exactly how they will be attacked and manually updating their cybersecurity defenses on those threats. Traditional rules-based solutions can’t detect unknown variants, making it impossible for them to detect attacks that have not previously been seen. They were designed to catch known attacks — not to proactively monitor for signs of trouble.

Rules-based security tools also can’t keep up with the cloud. These tools take considerable time and effort to configure, implement, and fine tune, especially when considering the size of a modern cloud environment. Tired security teams are forced to write new rules or edit existing rules, while faced with an unending queue of non-prioritized (and sometimes false) security alerts as the cloud grows and shrinks. If a pre-written rule is able to detect the intrusion, it’s likely to be buried underneath a barrage of other alerts. And once the alert is found, the investigation is likely time-consuming, as the alert lacks the proper context to point the practitioner in the right direction.

According to IBM, the average time to identify a security breach in 2021 was 212 days.[13] The amount of data captured in a tenth of that time could be catastrophic to a fintech company.

Fintech companies should consider cloud-native security solutions that were built specifically for the cloud. Rather than retrofitting legacy solutions for the cloud, modern security tools were built for the cloud and are able to handle the temporal and ever-evolving nature of cloud environments. These tools often feature anomaly-based, rules-optional approaches to cybersecurity. Rather than manually inputting rules to detect threats and vulnerabilities, modern tools learn the ins and outs of a cloud environment, then automatically surface anomalies — anything that looks out of the ordinary.

This way, security teams can surface risks in their environments immediately, whether known or unknown, with a drastic reduction in alerts.

4. Automate compliance as much as possible

The “pacing problem.” Even if fintech companies aren’t familiar with the exact term, the idea of the pacing problem is an all too familiar one. The pacing problem is the idea that technology and science is accelerating, yet governmental regulatory processes are slowing down. Or, at the very least, they can’t keep up.

But the pacing problem isn’t true everywhere. If fintech companies have a global scope, they will have to become familiar with multiple countries’ regulations and compliance needs. Some of these countries are quicker to evolve than others.

So fintech companies will likely find themselves in one of two camps. Either they will view compliance as a set of unnecessary and outdated “hoops” to jump through — hoops that throttle speed and innovation. Or they will view compliance as an ever-changing process that’s simply too complicated to fully meet with a lean security team — and doing so will, again, throttle speed and innovation. Or some combination of both.

Yet here’s the hard truth: **to succeed in fintech, companies must continue innovating, meet regulatory requirements, and establish ongoing security practices that extend well beyond these regulatory requirements. Yes, even with lean security teams.**

There are two things that fintech companies can do to stay on top of compliance needs, without sacrificing precious resources.

1. **Try to maintain an open channel of communication with regulators.** This step shows a good faith effort to stay on top of any late-breaking changes that may affect your technology, roadmap, or company goals.
2. **Invest in an automated compliance solution.** Modern cloud security solutions connect to your cloud environment and can assess your environment against pre-built or custom compliance frameworks. With these platforms, companies can both stay on top of compliance requirements and can generate compliance reports on-demand to fulfill auditor needs.

5. Build an airtight data policy

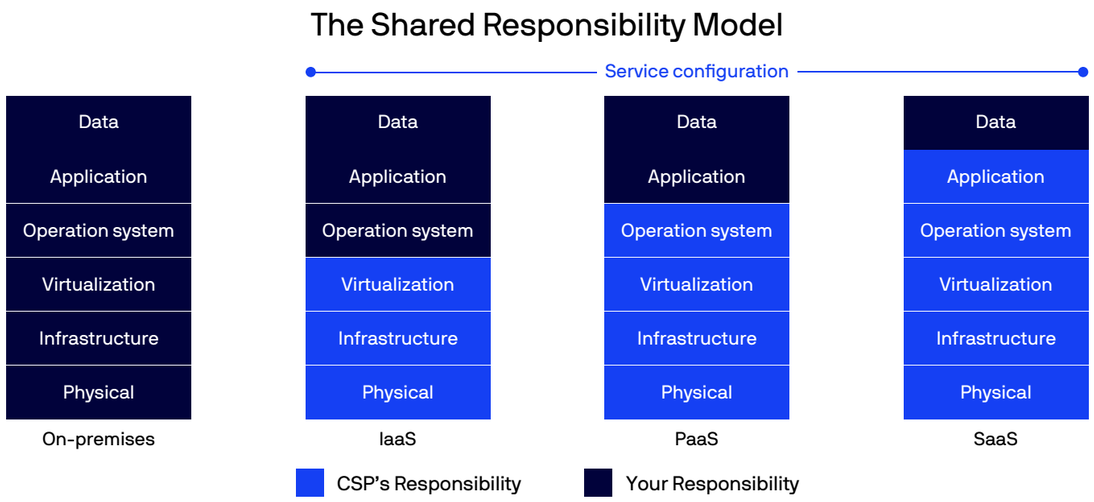
“Who is responsible for what?” This is an important question when it comes to cloud computing. But it’s even more important when it comes to the fintech industry.

Cloud data ownership presents its own set of challenges. Fintech companies need strict policies for who can access, create, modify, and delete data to ensure compliance with applicable regulations and standards, as well as technical and legal processes.

These policies are crucial for fintech companies. Fintech companies are often interconnected with actual banks and other financial institutions. And much like the Shared Responsibility Model which lays out roles and responsibilities between companies and their cloud service providers (CSPs), these financial institutions often pass responsibilities down to the fintech companies themselves, including the burden of data security.

Integration with these types of third-party banks and services — including non-financial services like social networks — introduce yet another way for hackers to steal private information.

For this reason, fintech companies must have data policies that are clearly communicated and agreed upon, from the top down. And these data policies should impact operations throughout the entire software lifecycle, from build time and into runtime.



Invest in a better solution

With consumer trust at stake, fintech organizations must invest in cybersecurity tools that move away from a traditional rules-based approach, consolidate disparate security tools, and embrace automation to speed detection, investigation, and response.

Short-staffed security teams don't have time to constantly configure, implement, and fine-tune rules. They need tools that provide the flexibility to add additional layers from build to runtime insights from a single platform for maximum value and security.

With Lacework, fintech companies can benefit from:

Security visibility

Deep observability into and across your cloud accounts, workloads, and microservices for better security control.

Threat detection

Identify threats that target your cloud servers, containers, and Infrastructure as a Service (IaaS) accounts so you can take action.

Anomaly detection

Detect and resolve anomalous behaviors across your workloads and IaaS accounts that indicate compromise or represent a security risk.

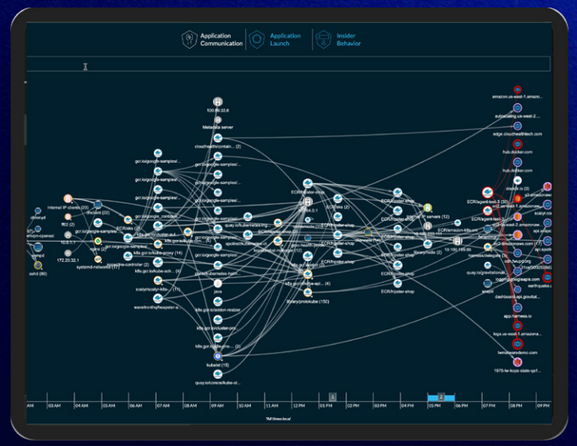
Host compliance

Achieve compliance standards such as SOC 2, PCI DSS, HIPAA, and more that require host intrusion detection (HIDS).

Configuration compliance

Spot IaaS account configurations that could put your company at risk and violate compliance and security best practices.

LACEWORK



Ready to chat?

Request a demo

Need to automate PCI-DSS compliance?

Read the solution brief

Lacework is the data-driven security company for the cloud. Founded in 2015 and headquartered in San Jose, Calif., Lacework is backed by leading investors like Sutter Hill Ventures, Altimeter Capital, D1 Capital Partners, Tiger Global Management, Counterpoint Global (Morgan Stanley), Franklin Templeton, Durable Capital, GV, General Catalyst, XN, Coatue, Dragoneer, Liberty Global Ventures, and Snowflake Ventures, among others.

Get started at www.lacework.com

LACEWORK

Sources

1. Shevlin, R. (2022, June 28). The revolution is alive and well: How Fintech has impacted banking. Forbes.
2. Lele, N., & Mannamkery, R. J. (2021, June 11). How financial institutions can win the Battle For Trust. Ernst & Young.
3. Maufe, Z. (2021, August 12). Financial Services, cloud adoption, regulators. google cloud blog. Google.
4. Silva, J., & Augustine, K. (2021, August). Banking on the cloud: Results from the 2021 cloudpath survey. IDC.
5. Vantage Market Research. (2022, May). Fintech market size USD 332.5 billion by 2028.
6. Singleton, C., DeBeck, C., et al. (2022, February). X-Force Threat Intelligence index 2022. IBM Security.
7. Aw, W. (2021, July 29). Fintech innovation and the cloud: Securely connecting the future of banking. FinTech Futures.
8. Drugeot, C. (2019, August 20). 98% of fintech start-ups exposed to cyberattacks. Software Testing News.
9. Principato, C. (2022, June). Most Trusted Brands 2022 - Trust in banking, investment and payments. Morning Consult.
10. Krivkovich, A., White, O., Townsend, Z., & Euart, J. (2021, January 19). How US customers' attitudes to fintech are shifting during the pandemic. McKinsey & Company.
11. SessionGuardian. (n.d.). The top 5 Fintech data breaches of the century, Broken Down. SessionGuardian.
12. Marks, M., Lundell, B., & Gahm, J. (2022, June). ESG Research - Developer Security Survey. ESG, a division of TechTarget.
13. IBM. (2021, August). Cost of a Data Breach: A view from the cloud 2021. IBM.
14. Application Security Series. (2019, August 20). State of Application Security at top 100 Global Fintech Startups. ImmuniWeb.