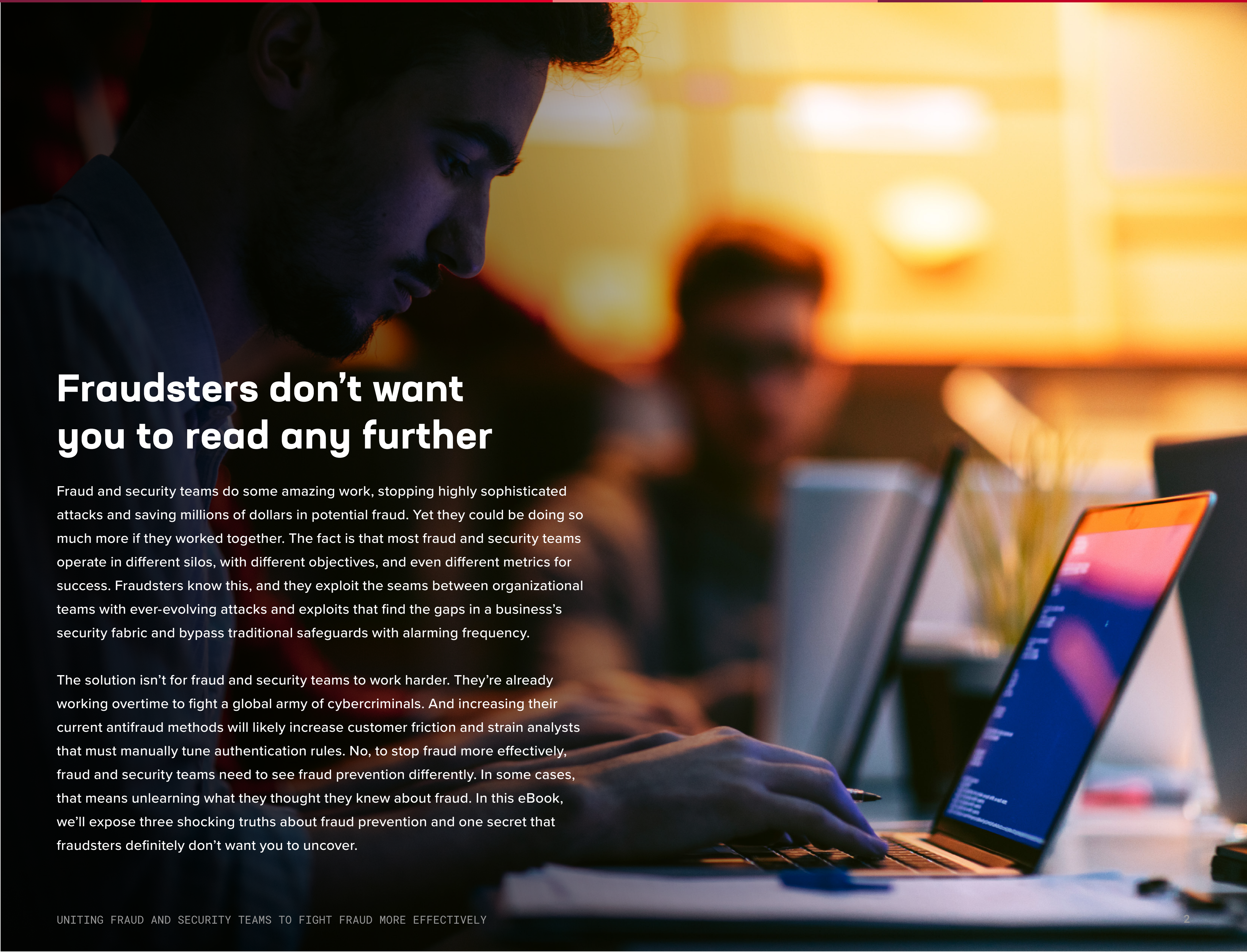
Uniting Fraud and Security Teams to Fight Online Fraud More Effectively

THE CASE FOR SECURITY AND FRAUD TEAMS TO UNITE



Fraudsters don’t want you to read any further

Fraud and security teams do some amazing work, stopping highly sophisticated attacks and saving millions of dollars in potential fraud. Yet they could be doing so much more if they worked together. The fact is that most fraud and security teams operate in different silos, with different objectives, and even different metrics for success. Fraudsters know this, and they exploit the seams between organizational teams with ever-evolving attacks and exploits that find the gaps in a business’s security fabric and bypass traditional safeguards with alarming frequency.

The solution isn’t for fraud and security teams to work harder. They’re already working overtime to fight a global army of cybercriminals. And increasing their current antifraud methods will likely increase customer friction and strain analysts that must manually tune authentication rules. No, to stop fraud more effectively, fraud and security teams need to see fraud prevention differently. In some cases, that means unlearning what they thought they knew about fraud. In this eBook, we’ll expose three shocking truths about fraud prevention and one secret that fraudsters definitely don’t want you to uncover.

Section 01

Separate lanes fail at stopping fraudulent transactions

Security roles, by definition, are destined to fail at preventing fraud. Network ops teams are tasked with monitoring and responding to network alerts, documenting daily tickets, and repairing the infrastructure. Security ops teams monitor and respond to security alerts and automate/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 don't overlap. Each team operates in its own lane while fraudsters, knowing this, conduct their business in the spaces in between those lanes. 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 (ATO). 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.

Fraud is a security issue first

By tracing the first steps of fraud, it's clear that fraudulent activity starts with a lack of security. Here are some examples of security attacks that can leave the door open for fraudsters to take out millions of dollars later.

Credential stuffing

Fraudsters rent a distributed botnet and leverage databases of stolen credentials to mount an automated attack on a login form and gain access to customer accounts, circumventing security countermeasures by emulating and exhibiting user behavior.

Content scraping

Fraudsters mount a targeted attack with bots to collect information (for example, scraping product pricing) that can be used later to disrupt advertising and revenue.

New account opening fraud

Fraudsters use social engineering and the dark web to create fake accounts with stolen or compromised personal identifiable information (PII), opening fraudulent lines of credit and initiating fraudulent transactions such as money laundering.

Aggregator attacks

Fraudsters open an aggregator account and attempt to link a bank account using compromised credentials to check if the account is active, see the balance, and monitor for deposits that may provide more insight into the customer. This allows them to obtain PII such as social security numbers and then use the data for subsequent schemes like synthetic identity fraud.

Section 02

You only need to answer three simple questions to stop fraud

Fraud and security teams are heavily reliant on rules to detect and block attackers. There are a litany of firewall and authentication rules designed to flag suspicious behavior. Fraudsters, however, make it their business to learn these rules and create methods to spoof them and bypass detection. They test the thresholds, avoid the alerts, and essentially fool the rules—all while working between the organizational seams.

For example, if a web application firewall rule sets a threshold for logins per minute, fraudsters can discover that threshold and stay below it. If browsing in incognito mode raises a fraud/risk score, fraudsters can discover this and avoid incognito mode during application access. If five minutes of browser inactivity triggers a rule for reauthentication, fraudsters can make the session seem active to avoid this.

We believe durable telemetry, and not rules, is the future of fraud prevention. Instead of anticipating what we think fraudsters will do (rules), durable telemetry provides descriptions of what fraudsters are actually doing. Ultimately, fraud detection should focus on answering three simple questions about the user:

1. Are they human?

For example, does their login behavior follow human characteristics or does it appear automated or machine-like?

2. Are they good or bad?

Are they browsing items for purchase or scraping information, potentially to buy out your stock and resell it at a higher price?

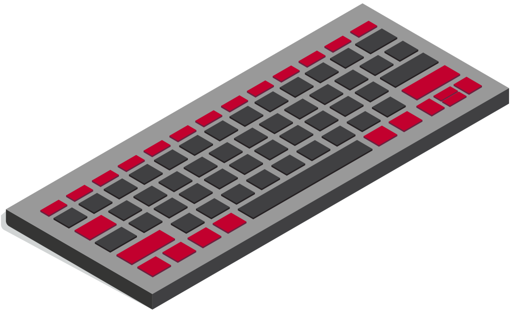
3. Are they who they say they are?

Do their device, environment, and behavior match expected patterns or do they depart suspiciously from their usual activity?

Spotting fraud signals

Advanced fraud detection solutions use artificial intelligence and machine learning to identify fraud patterns that human detection often misses.

For example, did you know that...



Fraudsters are **80x** more likely to use **keyboard shortcuts,**

250x more likely to use **Ctrl+V** when filling in account information fields,

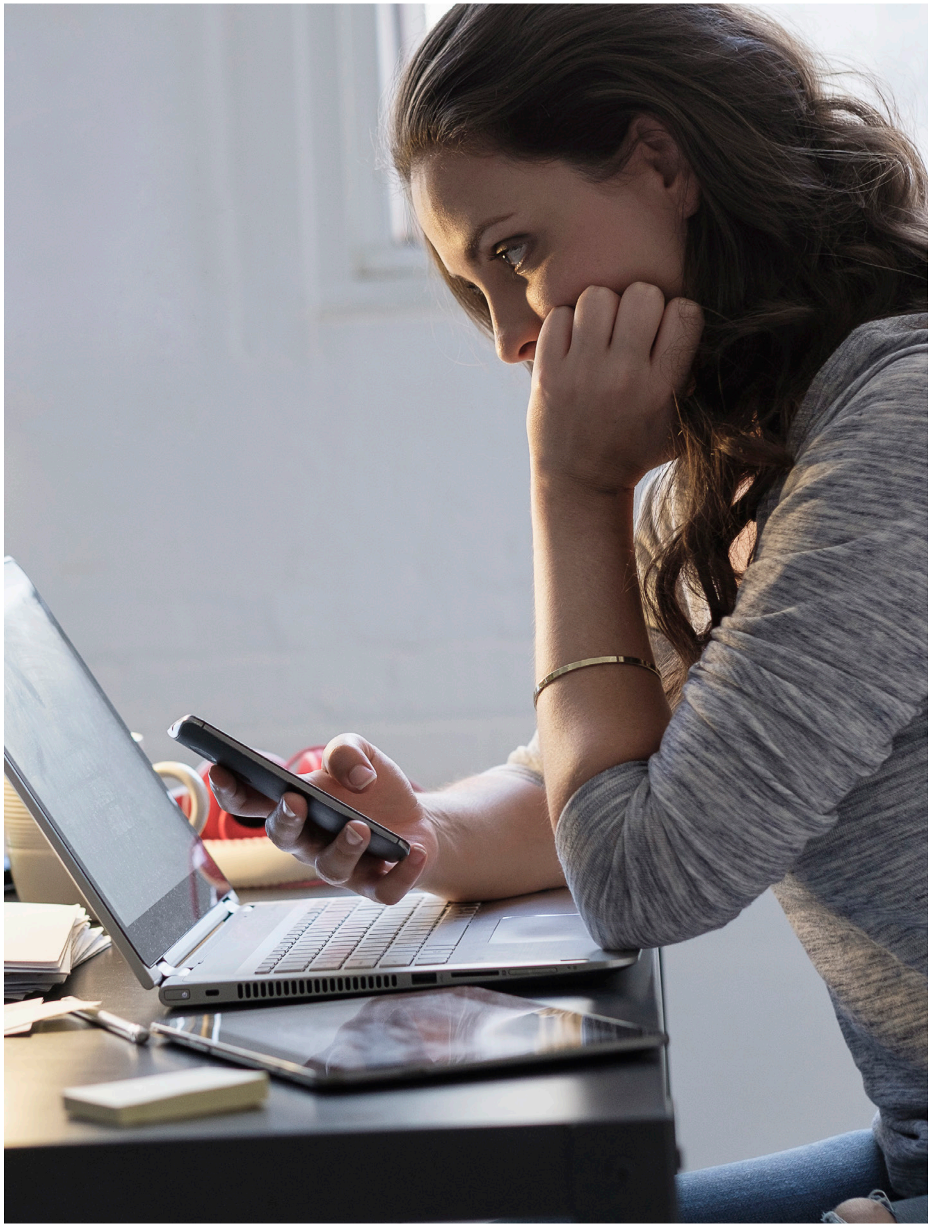
280x more likely to switch between browsers **during login**

Section 03

Multi-factor authentication only really succeeds when it fails

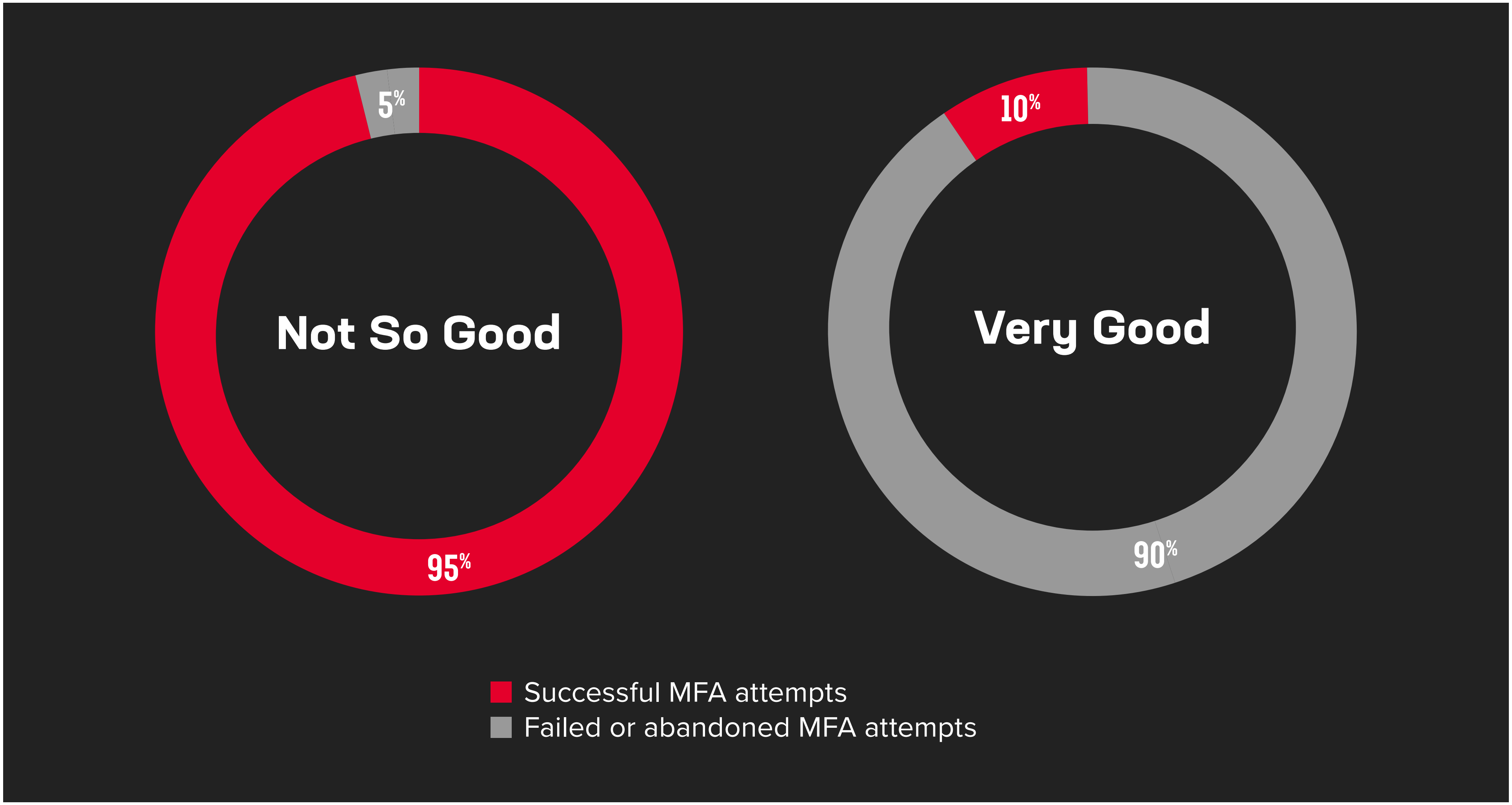
Multi-factor authentication (MFA) is regarded by most fraud and security teams as a best practice—but few companies are actually using it to their best advantage. A financial services company might execute hundreds of thousands of MFA requests in a single day, with 95% of those requests being successfully completed. A 5% failure rate for MFA is good, right? Wrong. In fact, you want your failure rate to be a lot closer to 90%.

Here's why: multi-factor authentication causes customer friction, which can lead to transaction abandonment, lost revenue, and reduced customer loyalty and retention. Presenting everyone with the same MFA challenge is like treating everyone as a fraudster. Instead, MFA should be used only in cases where the user has presented suspicious behavior, such as a new IP address, a different browser, or, as in our previous example, pasting their account information into the login screen with a Ctrl+V command. In addition, the most sophisticated fraudsters have ways to bypass MFA, such as gaining unauthorized access to service provider portals through social engineering, or by using Real-Time Phishing Proxies (RTPP).



Successful MFA requests mean a fraud detection failure

Multi-factor authentication means customer friction. If only a small percentage of your MFA requests lead to fraud, your fraud prevention isn't as "good" as you think.



Conclusion

Use AI to beat the bad guys

As you can see, siloed security, rule-based protections, and customer friction are only good enough to stop some of the fraud, some of the time—while requiring a lot of time from fraud and security teams to stay one step ahead of an increasingly sophisticated fraud industry. To outsmart criminals, companies need to equip themselves with a 360-degree view of fraud behavior and share that intelligence across fraud and security teams.

To achieve this goal, fraud and security teams have untapped and powerful weapons in their arsenal, including artificial intelligence (AI) and machine learning. An AI-driven fraud engine can understand how fraud occurs across the entire customer journey and stitch snapshots of behavior together into a full picture of fraud from beginning to end. As fraudsters adapt their methods, the AI fraud engine adapts with them, uncovering new signals that, when overlaid, reveal fraud with brilliant clarity.

An AI fraud engine can improve fraud detection and prevention by **80%** and reduce fraud investigations by **50%**

AI mechanisms don't replace the fraud analyst; they make the fraud analyst more effective by eliminating the tedious task of manually analyzing transactions, quickly correlating data and insights through complex algorithms, and minimizing the number of false positives. Results show that using an AI fraud engine can improve fraud detection and prevention by 80% and reduce fraud investigations by 50% while saving companies millions of dollars.

You can't fully prevent fraud alone. You need better tools and a broader perspective across fraud and security teams to do it. Learn how F5 Shape can help you double down on fraud through better collaboration and better intelligence.

ABOUT F5

For more informations on how F5 Shape can help your organization battle both automated and manual human-driven fraud, visit **f5.com/solutions/stop-online-fraud.**

US Headquarters: 801 5th Ave, Seattle, WA 98104 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com