CYBER SECURITY HUB

Securing Enterprise Authentication Without Sacrificing User Experience

Striking the Right Balance as Threats and Customer Turnover Risks Rise

In Partnership With

COMARCH

MAY 2020

Executive Summary

Transaction-based industries face increasing threats from fraud and identity theft because bad actors are constantly evolving their tactics, the number of devices accessing accounts is growing, and the current methods of transaction authentication are riddled with false positives and poor confidence scores. Businesses cannot afford to contact customers every time a transaction appears to be suspicious because the cost is too high and more importantly, customers would lose trust in the business and likely decide to find a new partner.

Despite the difficulties that transaction-based fraud presents, today's customers expect immediate gratification. False positives slow transaction times and customers find it troublesome to prove their identity.

Since no single data set can accurately predict the probable validity of user authentication, many businesses have implemented 2FA. However, the methods used to validate the second authentication factor may have an unsatisfactory success rate. When personnel must validate a transaction because there is a lack of trusted indicators, the process is typically time-consuming and expensive. In fact, many factors can be used to assess an individual's credibility. However, not all possible authentication methods are practical for every business and industry.

Both businesses and their customers want a quick and secure method of ensuring the validity of transactions. What is needed is an anti-fraud and anti-identity theft solution that simultaneously achieves high levels of trust and customer convenience.

This white paper explains what security and IT leaders should consider when attempting to balance their company's security requirements with customer experience.

Table Of Contents

Transaction-Based Industries Face Increasing Threats From Fraud and Identity Theft

The number of device types and applications capable of facilitating transactions continues to increase with mobile, the Internet of Things (IoT), and the Industrial Internet of Things (IIoT). Meanwhile, bad actors continue to modernize their attack methods which has a growing financial impact on businesses.

For example, CyberSecurity Ventures predicts that cybercrime profits will reach $6 trillion by 2021, up from $3 trillion in 2015. Yet, market research firm Gartner estimates that cyber security spending will grow at a compound annual growth rate (CAGR) of 8.5% from 2018 to 2022, reaching $170.4 billion by 2022. Despite the increase in cyber security spending, cyberattack prevention and management represent less than 6% of cybercrime profits.

The economic disparity between cyber crime and enterprise cyber security spending is most evident in high-profile breaches, though many more breaches fail to make headlines. According to the the Ponemon Institute's 2019 Cost of a Data Breach Report sponsored by IBM Research, a single data breach costs U.S. companies $8.2 million on average with each lost record worth $242.

Meantime to Discovery (MTTD) is critical, but many companies are falling behind. In fact, the SANS Institute's 2019 Incident Response survey reveals that only 52.6% of respondent organizations had an MTTD of less than 24 hours. Once an incident has been detected, 68.7% said they had a Meantime to Response (MTTR) of less than 24 hours.

The growth of transaction volumes is outpacing the ability to hire or afford personnel to perform the necessary authentications. Yet, end users expect immediate gratification 24/7/365 from anywhere using any device.

> "If you're a doctor or a nurse, you don't have time to memorize your password with this capital letter and that symbol. You need to find out what the patient's condition is. If I don't understand what the end user really does, there is no identity management solution that will work. They'll walk in, tell someone to login, and they'll piggyback on another person's session."
>
> **Ross Leo**
> Chief Information Security Officer
> ObservSmart Invisalert Solutions

Customer Expectations and Mobile Device Use Are Rising

Today's customers are extremely fickle. Companies like Amazon and Uber have differentiated themselves by providing a better user experience which includes delivering the outcome of a transaction more immediately than their traditional counterparts.

Over the past several years, there has been a trend toward increased mobile transactions as organizations supplemented their websites with mobile apps that provide anywhere, anytime convenience. The mobile trend has resulted in greater IT ecosystem complexity and an expanded attack surface through which hackers can launch attacks. The additional end points also provide ways for insiders to ignore security mechanisms or find a workaround.

At the same time, mobile device popularity has increased the number of channels through which users seek to access sensitive information. Thus, any enterprise user authentication strategy must span both fixed and mobile communication channels.

Threats Play Out Differently in Different Industries

There is always tension between the security posture a business must have and whether employees or customers will accept the security methods an organization has decided to use. While user ID and passwords are common across industries, the actual methods of authentication, and the number of factors utilized, depend on the use case. What works in an office setting may not work well on a manufacturing shop floor, out in the field, or in a work from home setting, For example.

“MFA can always be a bit tricky, which is why adoption is not as high as it should be. I think in large part, users need to understand there will always be a little bit of friction when it comes to authentication. The basic rule of thumb is increasing security, accuracy, and reliability equals greater levels of friction and less end-user adoption. In previous research interviews, this finding was found to be consistent among both higher and lower-level employees. Surprisingly, some vendors mentioned that a large portion of manager[s]/directors failed to address standard MFA rules introduced by their respective IT departments.”

Dimitrios Pavlakis
Digital Security Analyst, ABI Research

» Threats Play Out Differently in Different Industries

Application Security

Application security is at the top of every organization's list because application vulnerabilities are so common, they are frequently exploited. One mistake is to apply the same security mechanisms across different types of applications when the risk profile of each application differs. It is also important to understand which users and applications are accessing, using, or manipulating what data.

Mobile Banking

Banks now encourage customers to do more mobile banking because it provides customers with 24/7/365 account access while lowering the bank's HR overhead. Hackers exploit mobile banking in several ways including device cloning and man-in-the-middle attacks. So, banks are using additional authentication factors, such as a one-time code in addition to user ID and password.

Remote Access

Companies recently discovered that their remote access policies and related security measures would be tested by the COVID-19 pandemic. Suddenly, security teams were forced to question whether their methods of authentication, authorization, and identity lifecycle management were still effective. Some organizations had trouble adjusting role and access permissions, as necessary to provide reliable access to IT resources and to delegate privileges.

Credit Card Fraud

Credit card fraud is a growing problem. According to a 2018 report by the U.S. Federal Trade Commission (FTC), credit card fraud is the most common form of identity theft. Like insurance fraud, credit card fraud can be hard to detect, albeit for different reasons. For example, some fraudsters will charge a nominal amount, such as one dollar, to test a card's validity which results in a false negative. A pattern of false negatives (if undetected) can add up an expensive true positive across many accounts. Conversely, false positives result in delayed or denied transactions with actual customers which can cause brand reputation issues and customer turnover. Here, AI is used for anomaly detection and subtle, suspicious behavior evade rules-based systems.

Threats Play Out Differently in Different Industries

Field Service Fraud

Telecom companies manage physical assets that require maintenance and repair, such as cellular towers. Employees or contractors may provide false reports that degrade or interrupt the delivery of services to customers. This type of fraud can increase asset management and maintenance costs as well as customer service and customer retention costs. Increasingly, telecom companies are using AI to detect fraudulent field service reporting by comparing the data submitted with data acquired from other sources such as satellite data, geolocation data, and timestamp data.

Loyalty Card Fraud

Loyalty cards help consumer-facing businesses increase the value of individual transactions and customer lifetime value. Since accrued points can be redeemed for free products and services, they're an attractive target for hackers. Hackers also know that loyalty cards are not protected like other forms of payment and that accounts contain customers' sensitive information. When points are stolen, businesses have two choices which are to risk losing customers by admitting their points were stolen or keeping the customer by replacing the stolen points which increases loyalty program costs. AI and machine learning can help identify fraudulent behavior and identify the root cause of threats and IT ecosystem vulnerabilities.

Telecom Fraud

More types of telecom fraud have emerged with VoIP and mobile. Bad actors are stealing customer IDs, breaching network security, cloning devices and SIM cards, hijacking services, and commandeering prepaid accounts. Customers blame service providers for service overcharges, lost credits, and other account-related issues. AI and machine help pinpoint patterns that suggest suspicious device, equipment, service, and account tampering or use.

Insurance Fraud

Insurance fraud is rampant in several industries. A major issue many companies face is rules-based conformance. Specifically, if an insured person or a fraudster files a claim and the data conforms to the automated claims processing system's field values, then it is automatically approved. To reduce the possibility of fraud, insurance companies need to authenticate the insured individual and the transaction.

Current Authentication Methods Are Personnel Intensive and Create User Friction

No single authentication method is perfect, which is why organizations tend to use 2FA or MFA. A common problem with various point solutions is that the disparate systems tend to result in more overhead and higher costs, as well as gaps in a security fabric which open the door to compromised systems and breaches.

Regulatory requirements require strong authentication, but that takes extra time and tends not to be user friendly because it involves additional hardware or software. For example, EU-based companies must comply with the General Data Protection Regulation (GDPR) and/or Payment Services Directive (PSD2), depending on the type of data they're processing. Those regulations coupled with growing organizational and IT ecosystem complexity can make IAM complicated, time-consuming, and labor-intensive. However, user-friendly approaches do not achieve cyber security requirements, so there is an opportunity for a user-friendly authentication method that does not sacrifice security.

As is evident from everyday consumer and work experiences, current authentication methods tend to fall short. From a customer experience perspective ,that may mean a transaction has been interrupted, requiring the user to provide yet another form of identification such as answering a pre-selected question, successfully completing a CAPTCHA challenge, or providing a live agent with a code word.

What's needed is a user-friendly authentication method that does not sacrifice customer experience quality. Since the definition of "strong enough" measures varies based on the industry, the company, and use case, the technical and user experience requirements must be balanced accordingly. Therefore, the solution must meet all the technical requirements while providing a range of options that have different impacts on user experience. For example, retina scans tend not to be used outside of high security environments because that level of security is unnecessary and involves a lot of overhead. So, it may make more sense to authenticate an individual using facial recognition or a fingerprint.

> "Just relying on the asset-based MFA option is not adequate anymore. You need to get into attributes. That is where risk-based [authentication], anomaly detection, and behavior analysis come in."
>
> **Vijay Vedanabhatla**
> Director, Information Security, UPS

Credibility And Reputation Scoring Can Be Established Using Multiple Threat Detection Techniques

Many enterprises do not realize the total scope of threats they face, so their security posture is weaker than it should be. Other organizations prioritize security audits, including risk assessments and penetration tests, so they can proactively minimize the possibility of breaches, legal action, and regulatory fines.

On a day-to-day basis, several threat detection methods should be used to assess user and device credibility including:

Device Recognition:

Is the request coming from a trusted device? Is the request occurring in a known or previous location? Has the SIM been swapped since the last transaction? Has root mode been detected? When a device requests access to a specific resource, it should be compared with other devices used by the same individual, if the data is available. It should also be checked to determine whether the device is associated with known fraud attempts.

Behavioral biometrics:

Is this request similar to this user's previous requests? Can a human user's request be distinguished from the request of a machine? Is it possible to identify an individual based on keystrokes, taps on the screen, and/or mouse movements? Organizations should monitor user behavior and continuously authenticate users in a transparent way so that a high level of security and end user convenience can be achieved simultaneously. Given the widespread use of bots and AI, it's important to be able to distinguish between authentic users and synthetic ones, and to be able to identify unique users.

Identity cloning:

Are the user credentials associated with known compromised accounts? Are payment/loyalty card details being replaced on the same device in a manner representing credential stuffing? Is the credit card, loyalty card, or email address temporary? Identity clones live their lives as another person, acquiring assets, amassing debts and otherwise placing another person's reputation, livelihood, health and/or legal status in jeopardy. These fraudsters often use temporary cards, email addresses, and telephone numbers to avoid identification by businesses and law enforcement.

Malware detection:

Has the website been infected with malware? Has developer mode been activated? Obfuscation detection is important to hide hackers' attempts to hide malware injections.

An assessment utilizing these techniques enables the establishment of a credibility score. However, business practices and use cases vary so there are different thresholds of acceptable credibility scores that can be applied to determine the next course of action such as approval, rejection or escalation. By continuously monitoring user and device activity, organizations can achieve unique scoring for authentication, authorization and more.

>>

Credibility And Reputation Scoring Can Be Established Using Multiple Threat Detection Techniques

For example, if the assessment yields a high credibility score, the user may automatically proceed with their request. In contrast, a low credibility score may require escalation for additional validation.

The outcome from a risk and credibility assessment and threshold tuning determine when incremental authentication is necessary, which enables an enterprise to build dynamic integrity into its transactions and reduce false positive triggers, streamlining customer experiences so they involve less friction. Rather than creating barriers to successful transactions, businesses can focus on growth while continuous authentication mechanisms operate in the background.

> “Most device trust mechanisms leverage software and/or services to a certain extent. They are not as secure as hardware-based mechanisms, but they are cheaper and easier to implement (including retroactively – not always so for hardware). A cheaper option is often less secure. This is not always the case, and it depends on how it is used. A good software-based device trust mechanism, coupled with continuous monitoring, threat intel, [and] risk assessment can be more secure than something that is hardware based but never activated or leveraged.”

Michela Menting

Digital Security Research Director, ABI Research

A Solution is Available That Mitigates Risk For The Organization And Improves The Usability For The Customer Base

Businesses must balance the need for enterprise security and frictionless customer experiences. Using a single solution to do both, the enterprise can build integrity into its transactions, reduce false positive triggers and streamline customer experiences. Organizations that take no action to simultaneously address enterprise and customer requirements risk reputational harm, competitive disadvantage, shrinking customer bases, non-compliance, and potential legal action.

The speed of MTTD and MTTR are essential to reduce the cost and impact of fraudulent activity, although effective remediation needs to be coupled with proactive anticipation of the most likely threats which is best accomplished using a cyber threat protection platform that secures transactions and detects cyber threats. Rather than creating barriers which impede customers' regular activities, businesses can focus on growth through continuous authentication. A centralized IAM solution helps simplify privilege delegation as well as changing role and access permissions. It can also make remote access easier to manage generally and under extreme circumstances.

Importantly, an IAM solution should be transparent to end users so they do not need to take any actions or install any additional tools. That way, they can focus on the task at hand versus finding a security workaround that exposes the organization to risks.

Meanwhile, security professionals can exercise greater control over enterprise wide IAM using a single solution dedicated to and supported on both fixed and mobile devices. The IAM solution's mobile device capabilities should include tamper detection which verifies the device's operating mode, identifies the installation of unsecured software packages, executes processes in simulator mode, and more.

Finally, flexibility is important as threats evolve, enterprise ecosystems change, and customer experience expectations shift. Security and IT professionals need a solution that is comprehensive enough to support whatever combination of IAM methods make sense from the simplest and most traditional to the latest and most sophisticated. Importantly, a comprehensive cyber threat protection, can help organizations balance the need for strong security with customers' user experience expectations.

COMARCH

Comarch is one of the biggest software houses in central Europe, employing over 6000 people. We were founded in Kraków, Poland, and have been around for more than 25 years.

At Comarch Financial Services, a business sector within the Comarch Capital Group, we specialize in developing software and IT systems for major financial institutions in banking, insurance and capital markets.

Our primary advantage lies in the extensive domain knowledge. A growing number of implementations, know-how of our engineers and long-term relations with the leading banks and insurers help us improve the results of what we do all the time, every time. One of our top priorities is innovation.

Our expertise

- *Digital banking (www & mobile)*
- *Trade finance*
- *Factoring*
- *Credit management*
- *Cash management*
- *Digital insurance*
- *Loyalty for banking*
- *Wealth management*
- *Cyber security*
- *Transaction protection*
- *Identity & access management*
- *Fraud prevention & detection*
- *Anti-money laundering*

Our highlights

- *Over 15 000 users of the Comarch Loan Origination system*
- *3.7 mln transactions (+67% y/y) completed through the Comarch Corporate Banking mobile app in one of the largest Polish banks (2019)*
- *One of the largest loyalty programs for banking in Brazil – 19 million participants*

Our commitment

We don't just make software and security hardware. Apart from that, we offer consulting services in terms of security issues, authentication tools, centralized user management, system integration, or IT infrastructure administration. In other words, we take end-to-end responsibility – from solution design and implementation up to maintenance. Just so our clients are confident that whatever happens, we're there for them. We pride ourselves on creating a family of cryptographic tokens designed to protect customer and transaction data by providing 2-factor authorization and authentication. They can be easily integrated with identity and access management software that controls the access to company applications and resources. We also constantly develop our solutions for user and device monitoring that help guard firms and institutions against online frauds.

Our competitive edge

- *Large domain expertise in research and development. Innovation is our primary focus. More than 1100 of our IT engineers are directly involved in R&D in several locations in Europe*
- *Software and design in one package*

Our potential does not go unnoticed, and is highly regarded, by world-renowned research companies

- *Analysys Mason*
- *EU Industrial R&D Investment Scoreboard*
- *Gartner*
- *Forrester*
- *Celent*
- *IDC*
- *TOP200 IDG*
- *Truffle 100*

Read more on www.comarch.com >

CYBER SECURITY HUB

About Cyber Security Hub

The Cyber Security Hub is an online news source for global cyber security professionals and business leaders who leverage technology and services to secure the entire perimeter in their enterprise.

We're dedicated to providing the latest industry news, thought leadership and analysis in the cyber security space. Cyber Security Hub's expert commentary, tools and resources are developed through obtaining data and interviewing end users and analysts throughout the industry to deliver practical and strategic advice.

Our editorial team surveys and monitors the latest trends in cyber security and creates news articles, market reports, case studies and in-depth analysis for a captive audience consisting of C-Level executives, VPs and directors of cyber security and information technology.

CYBER SECURITY HUB

Dorene Rettas
Managing Director,
Cyber Security Hub
Dorene.Rettas@CSHub.com

Rosecley Morishita
Editorial Director,
Cyber Security Hub
Rosecley.Morishita@iqpc.com

Barry McIntyre
Marketing Director
Barry.McIntyre@iqpc.com

Seth Adler
Editor
Cyber Security Hub
Seth.Adler@iqpc.com

UPCOMING MARKET REPORTS

JUNE: Zero Trust: Inverting The Authentication Model

SOCIAL MEDIA INFORMATION:

Facebook:
CSHubIQPC

Twitter:
CSHubUSA

LinkedIn:
Cyber Security Hub -
Enterprise Security Professionals