


Unlock the Power of Digital Identity in Financial Services



Accelerate Digital Transformation, Drive Digital Banking Adoption, and Modernize the Connected Financial Services Ecosystem

Introduction	2
Unlock the Power of Digital Identity in Financial Services	3
Accelerate Digital Transformation	5
Drive Digital Banking Adoption	8
Modernize the Connected Financial Services Ecosystem	11
Summary	13

Introduction

As an industry leader, you are well aware of the forces driving change across financial services (FinServ). The emergence of disruptive technologies, increasing prominence of trusted-third party providers (TTPs), and expansion of the FinServ ecosystem are uprooting traditional business models and competitive boundaries. Customers are demanding more control, greater access, and omnichannel personalization. Providers are embracing new ways of thinking and increasing investments in value-added offerings. The regulatory landscape in many parts of the world is accelerating adoption of open standards, open financial-grade application programming interfaces (FAPIs), and consent-based privacy. Meanwhile, cybersecurity risks continue to become more pervasive by the day.

The scale, scope, and pace of this paradigm change, further accelerated by the COVID-19 pandemic, creates new opportunities and risks for FinServ organizations. Digital transformation must move rapidly to improve customer experiences yet avoid disrupting business strategy and operations. Self-managed legacy systems posing greatest security risks must be sunset expeditiously without inhibiting the wider IT change agenda. Digital identity needs to protect

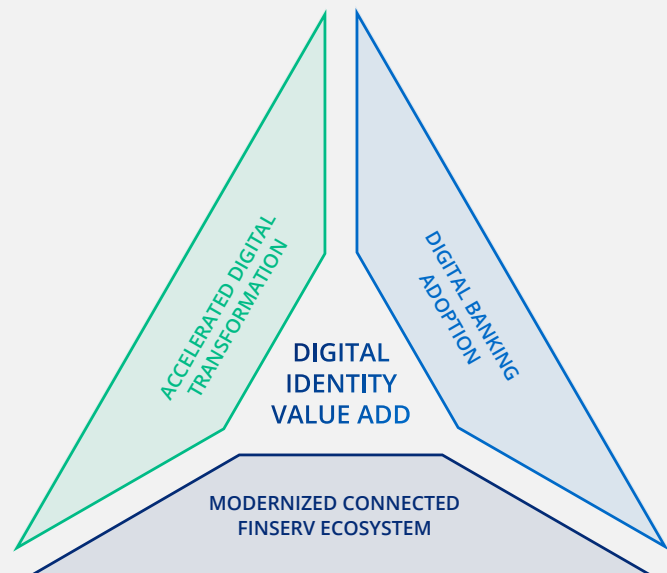
access to sensitive resources, applications, and data while avoiding unnecessary friction for customers. The wider FinServ ecosystem must be flexible enough to withstand demand- and supply-side shocks yet be sufficiently resilient to mitigate emerging cybersecurity risks. End-to-end digital journeys must continuously evolve to fuel customer acquisition, conversion, and retention while ensuring that customers are in control of their data. Standing still is no longer an option as the entire industry is being reimagined.

This eBook explores how ForgeRock helps organizations unlock the power of digital identity to help their customers, workforce, trusted third parties (TTPs), partners, and non-human identities safely and simply access the connected FinServ ecosystem. ForgeRock's capabilities and continuous track record of delivering value for financial services customers puts us in a unique position to help you:

- Accelerate digital transformation
- Drive digital banking adoption
- Modernize the connected financial services ecosystem

“By simplifying our legacy systems and consolidating them on the ForgeRock Identity Platform, we can get faster implementation and introduction of new services, reduce onboarding costs, and provide digital IDs to customers that are secure and easy to use. We are placing digital identity at the heart of our systems.”

Alan Chiew
Executive Director and Head of Technology,
Standard Chartered



Unlock the Power of Digital Identity in Financial Services

ForgeRock helps people safely and simply access the connected world. We strive to meet this mission by enabling exceptional digital experiences, no-compromise security, and comprehensive functionality at any scale with simple and flexible implementations in self-managed, any cloud or hybrid environments.

But how can digital identity help to simultaneously mitigate risks and harness opportunities facing today's FinServ organizations? Understanding this requires a deeper look at the challenges facing the industry.








Accelerate Digital Transformation: The Challenge

The FinServ industry is in the midst of the most disruptive transformation since the advent of payment cards in the early 1960s. Market-driven change in North America and regulatory-driven change in Europe and Asia-Pacific, as well as disruption spurred by emerging financial technology (FinTech) startups have mobilized technological innovation. The global FinTech market is expected to grow from [\\$127.66 billion in 2018 to \\$309.98 billion by 2022](#), at a compound annual growth rate (CAGR) of 24.8%. While many incumbent FinServ organizations see these changes as existential threats, others see an opportunity to deliver personalized experiences capable of upselling value, without the need to build-and-deploy in-house. This not only helps to enhance business agility and continuous deployment of new features, but also helps FinServ organizations tap into the latest FinTech innovation.

The emergence of the Open Banking movement in the European Union (EU), triggered by the General Data Protection Regulation (GDPR) and the revised Payment Services Directive (PSD2), as well as the Consumer Data Right (CDR) in Australia, have pushed the industry to adopt new business models, realign investments in banking platforms, embrace cloud-native strategies and, most importantly, embed TTPs at the core of the FinServ ecosystem. These capabilities give organizations the means to deliver hyper-personalized, value-added offerings to customers at pace. It's no surprise that the Open Banking market is projected to increase sixfold, from [\\$7.29 billion in 2018 to \\$43.15 billion by 2026](#). As FinServ organizations in these regions align with

Percentage of Banks Planning to Enable and Exploit open FAPIs.

	2020	YoY Change
 US	92%	+23%
 UK	85%	+17%
 Singapore	87%	+1%
 Hong Kong	89%	-
 France	87%	-1%

[Finastra](#)

regulatory requirements, they look to scale their capabilities, learning, and ecosystems in the quest to deliver hyper-personalized digital experiences and value-added offerings across the emerging Open Finance landscape.

In other regions, such as the U.S. and Canada, where transformation is driven by market forces and non-binding regulatory good practices, FinServ organizations continue to invest heavily in FAPIs, mobile banking capabilities, federated identity (OpenID Connect and OAuth 2.0), and cloud-native infrastructure. These investments help them to deliver personalized value-added offerings that directly address their customers' known and unknown financial needs and increase conversion rates, brand loyalty, and, ultimately, revenue. The onset of the COVID-19 pandemic has further encouraged traditional FinServ organizations to shift investments from physical/branch settings to digitally-focused channels. A significant percentage of these budgets are geared to moving U.S. FinServ organizations away from screen scraping¹ to secure FAPIs. This helps to mitigate the inherent risks associated with screen scraping, while giving customers more control over their personal data and privacy, further solidifying brand loyalty. In the post-pandemic era, FinServ organizations will increasingly seek to exploit these capabilities to insulate top-line growth from rising credit delinquencies and persistently low interest rates.

The confluence of these factors has pushed customers to demand streamlined, secure, personalized experiences across banking and non-banking services. With this, customers demand strengthened privacy, security, and the ability to control who and when their data is shared with and for what purpose. Meanwhile, the move to digital-first and hybrid physical-digital delivery channels has increased the prominence of omnichannel engagement. Indeed, [McKinsey](#) shows that over 71% of banking customers prefer these to traditional in-branch experiences, with 25% opting for pure digital engagement. The ability to deliver exceptional omnichannel experiences can make a difference between gaining and losing market share.

At the same time, the scale, scope, and sophistication of cyberattacks and identity fraud is increasing. The COVID-19 pandemic led to a [238%](#) rise in cyberattacks targeting banking organizations from February to April 2020 alone. Additional [data](#) shows that the financial services industry is 300 times more likely to be targeted by a cyberattack than other industries. This risk is further compounded by the growth of the FinServ ecosystem and the increasing attack plane this creates. Securing customer data, privacy, and the FinServ ecosystem has become essential to doing business. The most common cyberattacks stem from compromised authentication credentials and unauthorized access. Indeed, the [ForgeRock 2021 Consumer Identity Breach Report](#) estimates that over 43% of all breaches globally can be attributed to unauthorized access, with the average cost rising to \$8.64 million in the U.S., and \$3.86 million across the rest of the world.

Being able to fully harness and exploit the market and regulatory forces sweeping the FinServ industry can drive business agility, time to value, and top-line growth. This can, in turn, help organizations elevate customer experiences and shrink the growing cyberattack plane. Doing this successfully requires a comprehensive and scalable digital identity strategy and infrastructure at the core of your ecosystem.

¹https://en.wikipedia.org/wiki/Data_scraping



Accelerate Digital Transformation: The Solution

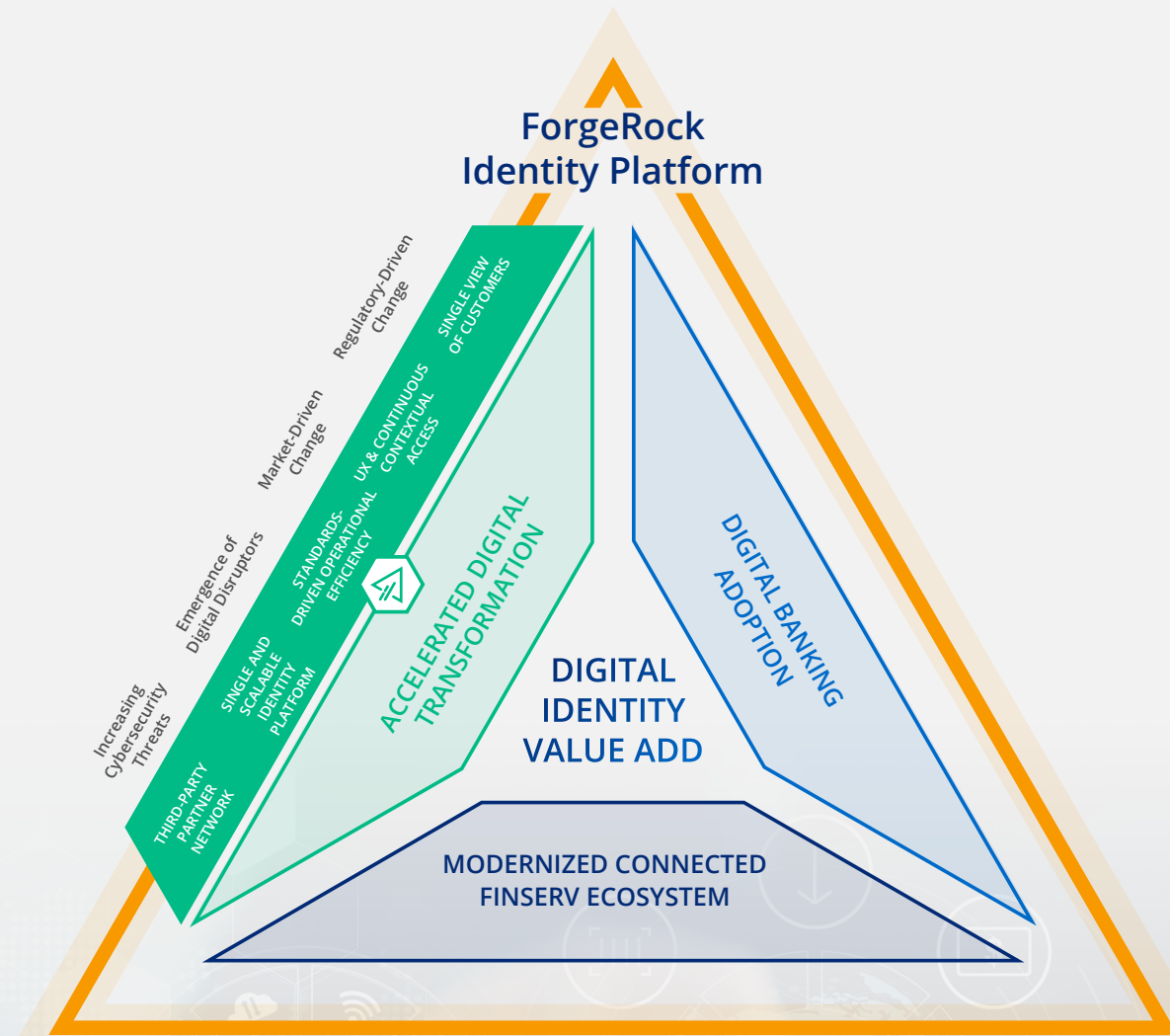
ForgeRock addresses these challenges through digital identity, which helps you accelerate digital transformation by:

- 1. Providing a Single View of Customers:** Bring together multiple identity sources to create a single view of customers' needs, enabling the hyper-personalization of value-added offerings while streamlining end-to-end customer journeys and experiences. Unify, scale, and secure directory stores to provide high performance and resilience across globally distributed services. Leverage best-in-breed identity management capabilities to automate the end-to-end identity lifecycle across billions of identities. Leverage extensive identity synchronization and reconciliation capabilities to provide a unified identity ecosystem enabling a real-time view of customer needs. ForgeRock can do all of this with a single platform.
- 2. Driving User Experience with Contextual and Continuous Access to Services:** Give customers and workforce a wide choice of authentication methods, including social and third-party proofed identities, to simultaneously improve user experiences and security. Integrate contextual signals into authentication journeys with an intuitive low-code, no-code drag-and-drop Intelligent Access interface to personalize and secure user experiences.
- 3. Improving Operational Efficiency with Open Standards:** Leverage a full suite of standards-based capabilities, including OpenID Connect, OAuth 2.0, Security Assertion Markup Language (SAML), and User-Managed Access (UMA) 2.0 to meet authentication, authorization, and regulatory needs. Provide customers and workforce with a unified, fluid single sign-on (SSO) experience to streamline access to multiple cloud-based applications. Secure APIs with data encryption in transit and at rest, rate limiting, configurable authentication, and authorization checks.
- 4. Leveraging a Single, Scalable Identity Platform for All Users:** Harness the rich capabilities of ForgeRock to unify and secure all digital identities (consumers, workforce, partners, things) in a hybrid self-managed and cloud environment. Deploy at a managed pace, and reduce time to value without being held back by legacy solutions.
- 5. Securing and Accelerating Third-Party Integration:** Harness the collective innovation of ForgeRock's digital identity partner network and ecosystem of pre-built, tested, and dynamic third-party integrations to leverage identity proofing, risk management, biometrics, and strong authentication capabilities while simultaneously securing and uplifting digital experiences.

"The great thing about ForgeRock is that it's so extensible: You can pretty much do anything you want with it, and if you can't, they will work with you to make it happen."

Sean Carrick,
VP, Identity Operations
and Engineering, LPL Financial

Accelerating your digital transformation with ForgeRock helps you maximize return on investment (ROI) in FAPIs, align with Open Banking and consumer protection regulations, and fully harness FinTech innovation to drive revenue, maintain competitive advantage, and mitigate cybersecurity risks.





Drive Digital Banking Adoption: The Challenge

The increasing adoption of smart mobile devices, the ubiquity of remote internet access, and the emergence of cloud computing have fueled exponential growth in digital challenger banking across the Asia-Pacific region, Latin America, Europe, and, to a lesser extent, North America. [Research](#) predicts that the digital challenger banking industry will grow from \$20.4 billion in 2019 to \$471 billion by 2027 at a compound annual growth rate (CAGR) of 48.1%. Sustained growth, however, is largely contingent on the ability of these banks to acquire and convert over [1.7 billion unbanked](#) consumers globally, as well as expand reach with underbanked consumers. In Indonesia, for example, over 81% of people own a mobile device, but only [48.9% have a bank account](#). In the U.S., underbanked consumers represent [over 16%](#) of the population. And [62%](#) of the European population are considering switching from physical banking to digital banking. Keeping ahead of the competition can mean the difference between sustaining investment funding for expansion, and becoming irrelevant.

Meanwhile, the growth of digital banking has spurred further growth of independent banks (neobanks), backed by established banking providers and FinTech start-ups aggressively looking to capture market share. These organizations continue to leverage best-of-breed cloud-native technologies, hyper-personalization, and innovative marketing strategies to deliver seamless end-to-end customer experiences that resonate with the Millennial, Gen-Z, and, increasingly, Gen-X and Baby-Boomer generations. By eliminating friction from user experiences, banks can deploy digital-first and mobile-centric experiences at [75% of the cost](#) borne by traditional retail banking providers. Despite the increasing demand for digital challenge banking, the industry continues to face systemic obstacles further amplified by the onset of COVID-19 pandemic.

Indeed, digital challenger banking organizations continue to struggle with monetizing and scaling value-added services away from transaction-based revenue models. Regulated FinTech start-up banks, on the other hand, continue to fund expansion through venture capital, while traditional banks hold back investments as the market inevitably moves to consolidate. To gain share in the unbanked and underbanked markets, traditional banks are instead spinning out digital challenger banks and moving into digital-first banking. This trend, further amplified by the COVID-19 pandemic, has forced banks to continuously

63%



of Asia Pacific customers are willing to switch to digital banks by 2025.

[IDC](#)

improve the digital experiences and value-added offerings they deliver to their customers. Capturing market share and diversifying revenue streams through secure, seamless, and hyper-personalized experiences are crucial to maintaining competitive edge.

Business models aside, perhaps the most significant challenge facing digital banks is being able to sustain customer trust. [Forty-five percent](#) of consumers think digital challenger banks will cease to exist in the short-term, and only 10% trust them to securely manage their data – compared to 41% trust in traditional banks. The reliance of digital challenger banks on identity proofing their new customers through opaque e-know-your-customer (eKYC) arrangements, ecosystem integrations with TTPs, and weak authentication and authorization policies create cybersecurity and identity fraud risks that threaten to compromise customer trust. The [ForgeRock 2021 Consumer Identity Breach Report](#) shows that attacks involving usernames and passwords have increased by 450% year-over-year, with financial services – including digital challenger banks – the most targeted industry, second only to healthcare.

Staying ahead of the competition in the rapidly changing digital banking industry is contingent on the ability to elevate end-to-end customer experiences by delivering and converting at pace value-added offerings that are personalized to the needs of unbanked and underbanked consumers. Doing this successfully requires a comprehensive and scalable digital identity strategy and infrastructure at the core of your ecosystem.



Drive Digital Banking Adoption: The Solution

ForgeRock addresses these challenges through digital identity, which help you drive digital banking adoption by:

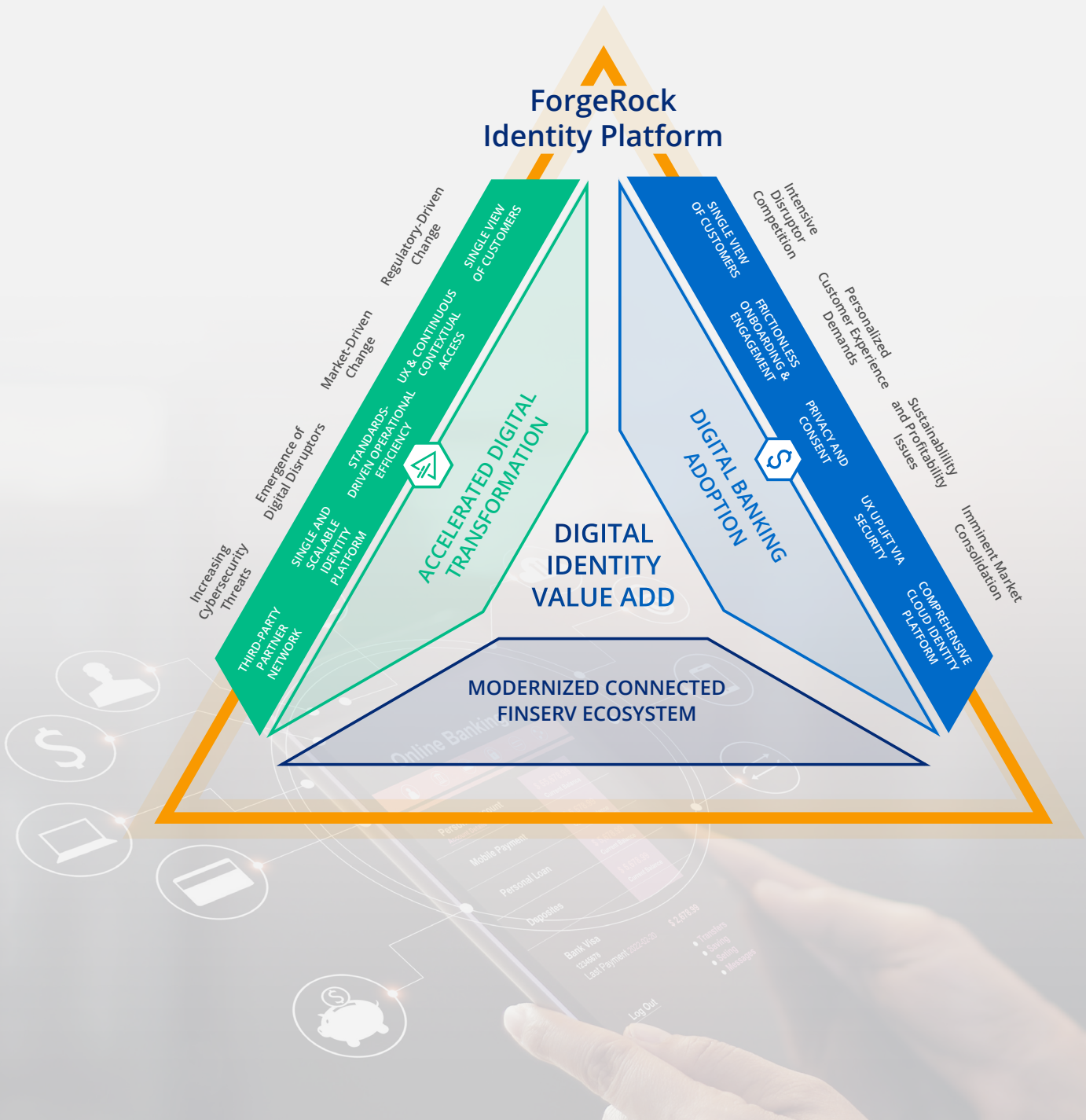
- 1. Providing a Single View of Customers Across Channels:** Build a unified view of customer needs, behaviors, and preferences. Hyper-personalize integrated, value-added offerings to drive upsell with existing customers and attract new underbanked and unbanked customers at pace. User journeys can be configured centrally and made available across every channel in a modern, consistent, and easy-to-consume FAPI-driven way, whether customers are using a smartphone, laptop, kiosk, voice, or any other device.
- 2. Enabling Frictionless Onboarding and Engagement:** Increase conversion rates by making registration easy with social registration options. Eliminate long-form registration forms and apply progressive profiling after login, enabling customers to provide rich information over time. Offer choices in how customers authenticate so they can interact with services and call centers faster. Offer easy-to-use self-service features, including password, security, marketing, profile, and privacy options.
- 3. Strengthening Privacy and Consent:** Giving consumers control over their data – from who has access to their accounts to managing profile and privacy settings – is essential for most customer-facing solutions. Privacy and consent management helps establish a closer relationship with customers because they can see what personal information a company holds and why. It also helps reduce customer support costs. ForgeRock provides a comprehensive, standards-based profile and privacy management dashboard. Users can manage who has access to their personal data, for how long, and under what circumstances. They can also manage their own profile details, the devices connected to their account, and applications they have consented to connect to their account.
- 4. Elevate Experience Through Security:** Deliver seamless, secure, and personalized customer experiences by enabling frictionless experiences with usernameless, passwordless, multi-factor, and device-based authentication. Leverage contextual signals, such as location, IP address, device type, operating system, and browser type to trigger adaptive authentication, protecting your customers while eliminating unnecessary friction in their journeys. Secure high-value transactions with context-based strong customer authentication and mobile push authorization workflows to amplify trust and security. Ensure customers' personal data is secured both at rest and in transit across your ecosystem, to mitigate the risk of breach and identity fraud.
- 5. Leverage Comprehensive Features of the Cloud Identity Platform:** Ensure that customers can benefit from a rapid continuous deployment of new features and offerings by leveraging the ForgeRock mobile software development toolkit (SDK) to integrate the powerful capabilities of the ForgeRock platform into customer-facing applications. Secure customer data with an FAPI security gateway across your hybrid IT environment to ensure customer trust and loyalty while aligning with regulatory requirements. Improve the performance of customer-facing applications with ForgeRock Identity Cloud, and meet demand spikes by benefiting from its modern customer-isolated, multi-tenant cloud architecture. Leverage ForgeRock's best-in-breed Hybrid Identity and Access Management platform capable of running, unifying, and securing all digital identities in a hybrid environment to minimize legacy burdens and accelerate time to value.

“Security is essential for quickly onboarding new customers and businesses, as well as providing an ideal digital experience. As the Customer Identity and Access Management (CIAM) solution for our Jenius applications, ForgeRock is helping us grow our business beyond our expectations.”

Joko Kurniawan, Senior Vice President,
IT Digital Service Enablement, BTPN Bank



Driving digital banking adoption with ForgeRock Identity Platform enables you to maximize your digital investments, hyper-personalize value-added offerings, and fully harness FinTech innovation to drive revenue, grow market share, and mitigate emerging cybersecurity threats.



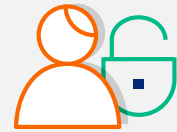


Modernize the Connected Financial Services Ecosystem: The Challenge

As both the scope and pace of digital transformation continue to grow, your ecosystem will inevitably become more costly and difficult to manage, extending your attack plane and susceptibility to emerging threat vectors. Managing an ever-growing list of workforce, TTP, partner identities, and access requests across the core and periphery of the FinServ ecosystem can overwhelm IT teams and create [entitlement creep](#). This can expose organizations to undue risk when scaling digital infrastructures, capabilities, and value-added offerings. Research shows that [most successful](#) digital ecosystems comprise an average of 40 partners/TTPs, with 77% of these spanning emerging markets and 83% extending across multiple industries. Securing and automating the end-to-end access management lifecycle with the latest artificial intelligence (AI)-driven technology can help to improve business agility, reduce costs, and ensure compliance with regulatory requirements, such as the General Data Protection Regulation (GDPR), the Consumer Data Right (CDR), the California Consumer Privacy Act (CCPA), and the Sarbanes-Oxley Act.

Managing entitlements, establishing segregation of duties (SOD), and preventing unauthorized access is becoming increasingly expensive and difficult to manage. The [2021 Varonis Data Risk report](#) for financial services shows that each employee in the industry has, on average, access to over 11 million files. Furthermore, an overwhelming 63% of organizations in the industry leave over 1,000 sensitive files open to every employee, with lack of basic access management and identity governance to minimize the risk that this poses. Meanwhile, [research](#) shows that 65% of compromised internal accounts have not been accessed for more than 90 days, suggesting that they are either dormant or in urgent need of de-provisioning. Centralizing, automating, and de-risking access across the FinServ ecosystem is more important than ever. Advances in AI, machine learning (ML), and the progressive adoption of cloud-based technologies have pushed FinServ organizations to increase investments in identity governance and administration (IGA) as well as internal access management (AM) capabilities. This enables them to effectively manage the end-to-end identity lifecycle, mobilize a wide range of SOD policies, security controls, and reduce entitlement creep to enhance their business agility, reduce costs, and achieve regulatory compliance.

43%



of all breaches are attributed to unauthorized access.

[2021 ForgeRock Consumer Identity Breach Report](#)

Unfortunately, aging identity and access management (IAM) technology presents roadblocks and causes delays. The prospect of ripping and replacing legacy IAM systems is daunting. A move away from legacy IAM is inherently risky for any organization. To mitigate these risks, FinServ organizations must find effective and rapid means of protecting their customers from unnecessary disruptions, insulating their business from cost overruns and potential internal compliance audit challenges. ForgeRock helps organizations accelerate identity migration by a factor of more than 30% with the ForgeRock Modernize IAM Accelerators. These can help organizations avoid a painful rip-and-replace experience and allow them to orchestrate a planned, purposeful migration into the ForgeRock platform to avoid customer disruptions, reduce costs, and accelerate time to value. More importantly, these can bring forward the ROI on digital modernization investments and help customers benefit from new features and offerings in days rather than months or years.

Standing still is no longer an option as your ecosystem scales to keep up with the competition. Embracing the growing “[identity fabric](#)” can help you enable a comprehensive set of digital identity capabilities to accelerate secure access for workforce, TPPs, and partners as a way of achieving regulatory compliance, mitigating risks, and reducing costs.



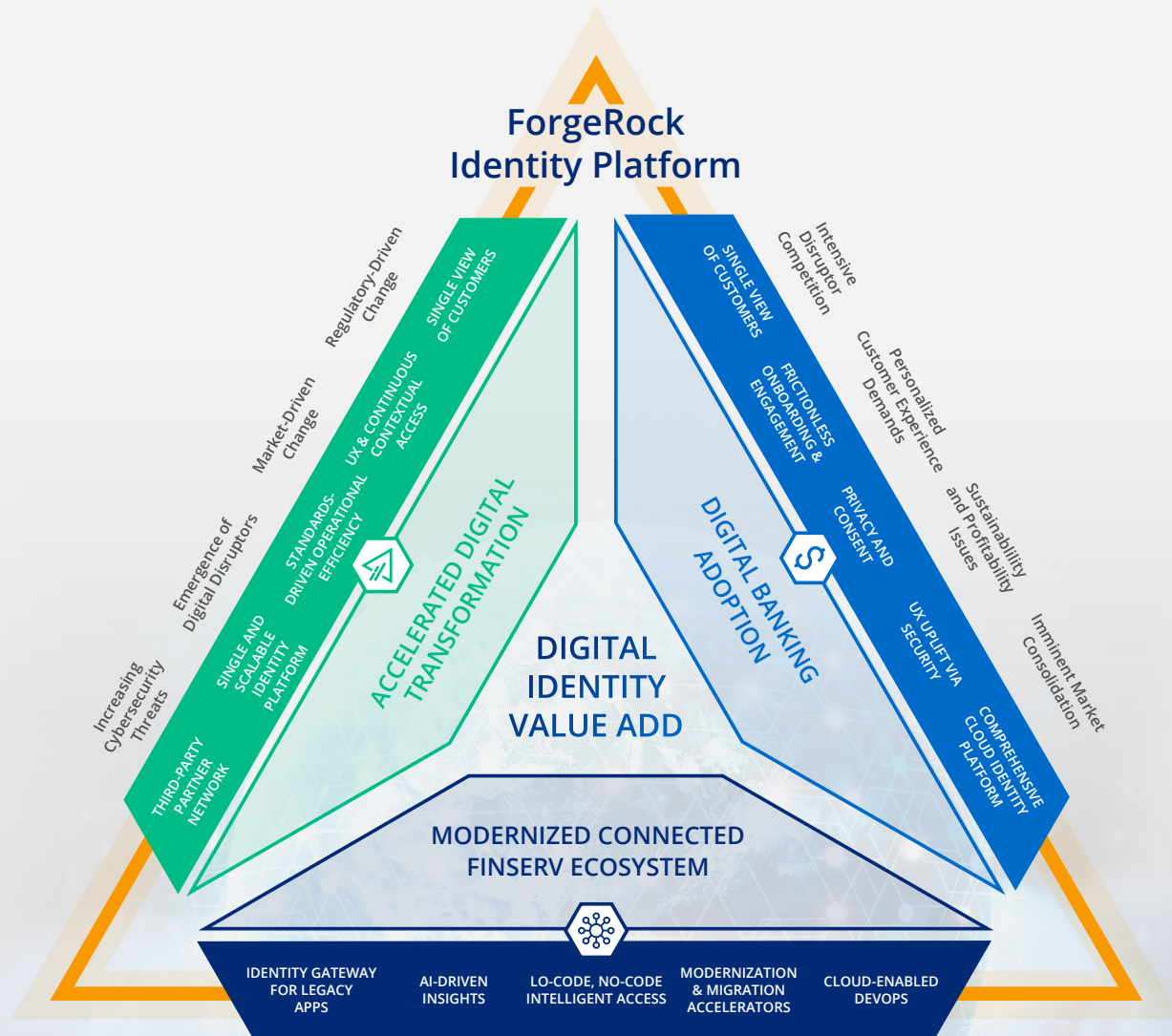
Modernize the Connected Financial Services Ecosystem: The Solution

ForgeRock addresses these challenges by enabling digital identity to help you modernize your connected financial services ecosystem by:

- 1. Leveraging AI Data Driven Insights:** Use AI-driven identity governance across the workforce, TTP, and partner ecosystem to achieve regulatory compliance, mitigate risks, and reduce costs. Automate high-confidence access approvals, recommend certification for low-risk accounts, and automate the removal of unnecessary roles to secure and optimize digital identity governance, eliminate entitlement creep, and minimize rubber stamping access certifications. Leverage existing legacy identity governance and administration (IGA) systems and investments and augment with an AI-driven engine to automate the end-to-end identity management lifecycle.
- 2. Accelerate Modernization and Migration Efforts:** Minimize the impact and risk of modernization by phasing the migration of complex IAM legacy using open-source Modernize IAM accelerator toolkits. Utilize a full range of accelerator options to support bulk or just-in-time user migrations with pre-configured templates available at no additional cost. Orchestrate the migration of identities from multiple identity management systems into the ForgeRock platform, enabling to leverage existing investments and streamline operations with zero disruption to customers. Facilitate rapid and secure opening of application programming interfaces (APIs) to support Open Banking and ecosystem expansion for onboarding, consenting, and access authorization workflows to fully leverage FAPI investments and agility.
- 3. Integrating and Securing Legacy Applications:** Simplify and secure how your workforce, TTPs, and partners authenticate into and access legacy applications by enabling comprehensive SSO and federation capabilities to accelerate digital transformation, reduce your time to value, and secure APIs. Leverage powerful Identity Gateway capabilities to protect your services and applications from distributed denial-of-service (DDoS) attacks, and monitor API traffic, throttle demand, and proactively detect anomalies.
- 4. Enabling Low-Code, No-Code Intelligent Access:** Use a powerful visual designer with a drag-and-drop interface to easily configure, orchestrate, and secure workforce, TTP, and partner journeys by quickly consuming a wide range of out-of-the-box authenticators. This eliminates the need for coding and significantly reduces time to value. Leverage an extensive ecosystem of third-party integrations to uplift strong authentication, behavioral biometrics, risk management, and identity-proofing capabilities. Integrate contextual signals, such as location, IP address, device type, operating system, and browser type into authentication journeys to improve experiences and security. Take advantage of AI-driven contextual signals, high-risk user access awareness, and remediation recommendations to introduce appropriate levels of access friction and to protect the FinServ ecosystem from unauthorized access.
- 5. Implementing a Cloud-Enabled DevOps Deployment Model:** Leverage the power of Docker and Kubernetes using the industry's fastest and most flexible multi-cloud IAM deployment options to accelerate time to market, deploy millions of identities in minutes on any cloud, and significantly reduce implementation costs. Protect workloads in any cloud, support multiple identity types, and enable rapid and repeatable solution development to support DevOps deployments. This provides scalability, increased flexibility, and, ultimately, helps to bring value to customers faster, at lower cost.



Modernizing your connected financial services ecosystem with ForgeRock will help you accelerate secure access for your workforce, TTPs, and partners to achieve regulatory compliance, mitigate risks, and reduce costs.



Summary

The confluence of market- and regulatory-driven forces, and emergence of customer-centric business models, ecosystems, and digital disruptors across the FinServ industry, mean that business agility is no longer a nice-to-have as you strive to maintain competitive advantage. Anchoring a comprehensive digital identity strategy at the heart of your digital investments can help you accelerate digital transformation, drive digital banking adoption, and modernize your connected FinServ ecosystem.

ForgeRock helps organizations unlock the power of digital identity to help customers, workforces, TTPs, and partners safely and simply access the connected FinServ ecosystem. Taking advantage of the industry-leading [ForgeRock Identity Platform](#) and [ForgeRock Hybrid Identity and Access Management](#) can help you accelerate digital transformation,

drive top-line growth, deliver great omnichannel experiences, secure your financial services ecosystem, and meet regulatory requirements.

ForgeRock is recognized as a leader in Customer Identity and Access Management (CIAM) by the 2020 [Forrester Wave](#), the 2020 [KuppingerCole](#) Leadership Compass for CIAM, the 2020 [Gartner](#) Magic Quadrant for Access Management, and is an overall leader in the 2021 [KuppingerCole](#) Leadership Compass for Identity Fabrics. ForgeRock is uniquely positioned to help FinServ organizations optimize their return on investment in digital transformation.

Get ahead of your competition by leveraging digital identity to its maximum potential with ForgeRock.

The AI-Powered ForgeRock Identity Platform

One Platform. All Identities. Any Cloud.

100+ inputs for identity, orchestration and dynamic access decisioning

Business Context

Transactions, Resources, Scopes

Security Context

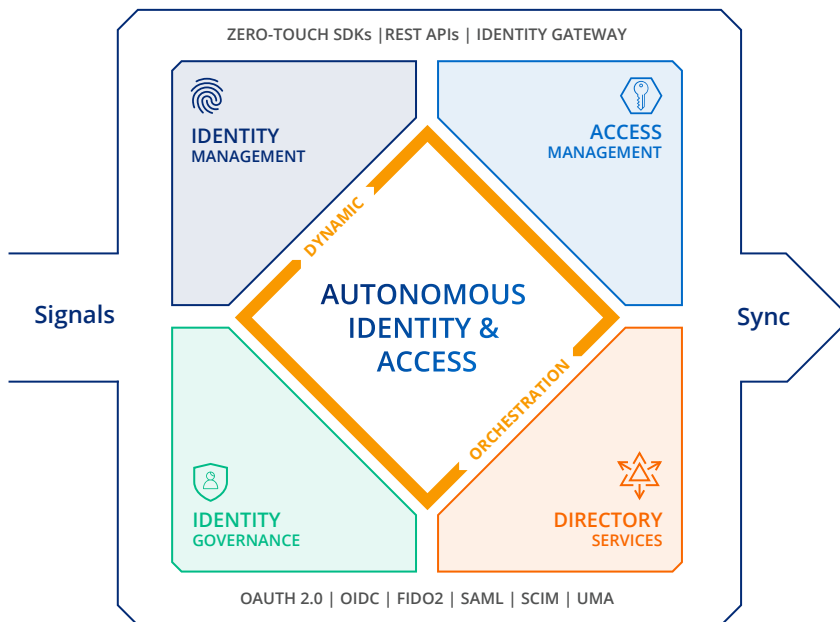
AI/ML, Fraud, Security, Behavior

Identity Context

Identity Proofing, Social

Relationship Context

User-User and User-Device relationships



Send rich signals throughout the digital enterprise for security and agility

Cyber Security Operations & SIEM

eKYC/Customer Profiling

Omnichannel Experiences

CRM, ERP, HR, and other business applications

Regulatory Compliance

Data Lakes and Data Warehouses

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit www.forgerock.com or follow ForgeRock on social media.

Follow Us

