ADVANCING DIGITAL MATURITY IN FINANCIAL SERVICES

ACHIEVING ONLINE SECURITY AND CUSTOMER EXPERIENCE EQUILIBRIUM
Taking Trust to the Next Level

Customer relationships begin with trust. Whether you’re a bank, asset management firm, credit card company, payment provider, insurance carrier, or financial information service, trust is a prerequisite for any interaction — especially digital. The financial services (FS) industry has invested heavily in robust security and established proven leadership in protecting high-value customer data. But managing cybersecurity risk is just one component of online business success.

When customers entrust your organization with their sensitive financial and personal information, not only do they expect you to keep it safe, but they also demand the same fast, convenient online experiences they’ve become accustomed to on the web and mobile devices. For today’s FS organizations to stay competitive and grow revenue, digital security and customer experience (CX) can no longer be mutually exclusive.

Customer experience isn’t just a nice-to-have; it’s a business imperative. Customer experience leaders grow revenue faster than CX laggards, drive higher brand preference, and can charge more for the same products.

Forrester
What Does Your Digital Transformation Look Like?

The years that followed the global economic crisis did not create a climate for innovation in the financial industry. North American companies pulled back on new digital initiatives to focus on getting business back on track. As a result, the financial industry lagged on improving online experiences – compared to other industries such as commerce – and businesses and consumers developed low expectations for CX.

Digital transformation has sparked a dramatic shift not only in the way customers bank and invest, but also how financial organizations interact with customers, compete for market share, and attract and retain talented employees. In 2018, Nielsen Scarborough reported that the number of Internet users who banked online on a smartphone increased from 39.93 million in 2013 to 86.04 million in 2017 (an increase of 115.48%). Those numbers have climbed with the widespread adoption of mobile devices and even the most conservative clients now embracing technology. As forces inside and outside of financial organizations demand the agility and access that cloud adoption and CX-focus drive, the push toward digital maturity can no longer wait.

64% of U.S. consumers use mobile devices to perform banking activities.

Mercator Advisory Group
<table>
<thead>
<tr>
<th>Business Transformation</th>
<th>Business Engagement</th>
<th>User Experience</th>
<th>Technology Transformation</th>
<th>Cybersecurity Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rebranding</td>
<td>Percentage of</td>
<td>Instant Web</td>
<td>Investment in Care Systems &amp; APIs</td>
<td></td>
</tr>
<tr>
<td>Restructuring</td>
<td>Transactions</td>
<td></td>
<td></td>
<td>Always Available</td>
</tr>
<tr>
<td>Digital-First Approach</td>
<td>Self-Service</td>
<td>Instant Mobile</td>
<td>Always Secure</td>
<td></td>
</tr>
<tr>
<td>Digitally-Savvy Senior Management</td>
<td>Bot Management</td>
<td>Anytime</td>
<td>Protect the Customer</td>
<td></td>
</tr>
<tr>
<td>Follow eCommerce</td>
<td>Aggregator Strategy</td>
<td>Anywhere</td>
<td>Protect the Enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Robo-Active &amp; FinTech</td>
<td>Measurement &amp; Analytics</td>
<td>Protect the Company</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is Digital Maturity?

Digital maturity occurs when security and CX are sufficiently intertwined and understood as complementary. A Forrester digital maturity survey of over 350 companies commissioned by Akamai found that companies struggle to balance security with digital experience. Of the five categories assessed in the survey — security, strategy, digital experience, cloud, and general technology — most executives reported their firm is strongest in security and weakest in digital experience maturity.

The research found that executives recognize the potential negative impact a customer data breach would have on their business — damage to brand reputation, customer trust, and revenue. But they don’t fully grasp how to prevent future revenue loss. In digital experience, the survey found that firms are likely to optimize for speed, reliability, and security, but put the burden on customers for feedback on performance.

Investment firms that neglect the functionality and usability of digital touchpoints are ignoring one of the most important drivers of investors’ experience.

Forrester
Managing Digital Experience And Risk

The time has come to view security as a strategic enabler for your business, to mitigate risk and maintain trust, while you build customer loyalty with better online experiences. By adopting CX practices that leverage the data you already safely collect and retain, you can provide customers with the right offerings, at the right time, in the right place. Continuously monitoring, optimizing, and validating online performance – with a strong security underpinning – will provide the insight you need to deliver the digital experiences that users expect and desire.

You can make simple changes such as deploying a real user monitoring (RUM) solution to understand user behavior on your website, utilizing a content delivery network (CDN) for faster page loads, and adjusting images for more engaging content on any device. Ultimately, you can make more fundamental shifts in business strategy such as developing a digital roadmap for web and mobile platforms, embracing the cloud for all digital content, and adopting more agile security operations policies to support growth.

Companies with a high growth rate maximize experience and security.

Forrester
Meet Your New Customers

*Millennials* are 80 million strong and will inherit $41 trillion by midcentury. This next generation of customers represent vast amounts of wealth, have grown up with more services, are less loyal and more brand-oriented, and require organizations to meet them where they are – at a variety of mobile touchpoints.

The mobile app is only one touchpoint, and customer experience is only one of several factors that contribute to overall business results. Yet for a growing number of investors, particularly younger ones, the mobile app is the customer experience. And customer experience drives customer loyalty and revenue growth across industries.

*Forrester*
MONITOR

Understanding online interactions that drive user behavior
Data shows that 53% of visits to mobile sites are abandoned if pages take longer than 3 seconds to load. With the proliferation of new financial services solutions, you cannot afford to wait until customers identify a problem with your website or application.

Some organizations use Apdex as a measure of how they are engaging with their audiences. Apdex score is just one metric of satisfied customers, with no detail on what generated the result – a page load error, content not served up quickly, website difficult to navigate? **Digital maturity demands better insight from your online data.**

Real user monitoring (RUM) is an essential monitoring tool for CX. Augmenting web analytics with real user data helps you understand how performance is impacting user experience. For example, it can tell you which pages users are spending the most time on, how long they are willing to wait for content to load, and the factors affecting performance, such as large images or third-party services.

**Enhanced monitoring also improves security analysis and response as well as the effectiveness of security measures.** Online data is ultimately funneled into security information and event management (SIEM), where correlated events are processed and reviewed by risk teams. Integrating real user data into SIEM, and consolidating this information into digital and security operations centers, helps alert your organization to issues before customers do, for faster resolution. It also identifies when security controls are blocking legitimate traffic or slowing customer interactions, diminishing business results.
Understanding real user experiences and behavior on your digital properties aligns the organization – IT, marketing, executives – with performance data that translates into business results. By setting up key performance indicator (KPI) metrics that map to business imperatives and revenue – such as accounts opened, loan applications completed, or transactions processed – you can make data-driven decisions about technology and marketing investments that improve the bottom line. RUM alerts for missed KPIs, so you can prioritize performance problems with the most business or customer impact.

CASE STUDY

Building a Better Digital Wallet Experience

A major credit card company embarked on a strategic initiative to develop its digital wallet offering – a complete departure from business as usual. This effort called for a cloud-based approach to providing secure scalability of API traffic to increase reliability and responsiveness. To preserve their security posture in the cloud, the company leveraged Akamai’s cloud security solutions for protection against online attacks and credential stuffing. Akamai also helped maintain performance by controlling user experience and shaping customer traffic to ensure the digital wallet stayed responsive during peak events such as merchant promotions. For more insight into performance, the credit card company also started using real user monitoring (RUM) to understand the experience that users were having engaging with their service to maximize customer experience (CX) and satisfaction.
OPTIMIZE
Improving user experiences to promote growth
Security teams and measures are often siloed in a variety of groups, disciplines, and vendors, but it is important that they operate under the same charter – to enable, not impede, the business. Security cannot be a barrier for customers or negatively impact the business. With that in mind, you can proactively ensure advanced security measures don’t cause unnecessary friction.

For example, customers might view the inconvenience of two-factor authentication to be greater than the additional security it provides – make it optional. Or developers might struggle to sufficiently secure applications, either because they don’t know how to apply effective protection or find that the process negates agile cycles. To unburden developers without increasing your attack surface, deploying cloud-based web application firewall (WAF) and bot management solutions outside the scope of development applies, and manages security controls before traffic reaches applications.

**Security controls shouldn’t block or slow down legitimate traffic.** As the Forrester digital maturity data highlights, security and CX are not an either-or consideration.

---

To ensure security is not becoming a barrier to CX, you can optimize sensitive content with:

- An integrated global caching solution to minimize latency after initial security validations
- Web and mobile acceleration for both unauthenticated and authenticated users
- Asset optimization for research documents as well as upsell and cross-sell materials
Today’s users want real-time quotes, charts, and video clips with financial news or investment advice. Images and videos are key to user engagement, but delivering a rich user experience without the performance to drive it is a bad outcome. Front-end optimizations, including adaptive image compression and device characterization, can help to improve performance to provide a positive experience on mobile, tablet, and desktop.

To keep pace with business and market events, real-time controls enable, manage, and block online activities. These controls prompt critical conversations between business, application, and security groups about balancing CX and risk – a topic that falls to the chief risk officer in some organizations.

What is the acceptable balance between CX and latency or limitations inherent in security controls? What does the security team require to remain effective by improving intelligence? What is the potential revenue exposure if content – or worse, customer data – is stolen?
Cloud delivery solutions provide the security controls, real-time operating abilities, and intelligent CX automation to deliver the content users expect without compromising the business. If the marketing team runs a promotion, a stock market event drives trading, or a natural disaster prompts user logins, business stakeholders can be confident that security services are monitoring and acting against malicious activities, CX automation is offloading content acceleration and optimization as new information is published, and that there are ample real-time controls.

Real-time controls are essential for:

- URL rewrites and forwarding to create user-friendly links and the option to update campaigns
- Phased content releases across time zones
- Content targeting for resources available to relevant users or those with specific access privileges
- Device characterization to restrict certain transactions by device – for example, some website functionality might not be available on mobile
- Visitor or API prioritization to ensure consistent experiences, and waiting rooms for delays
It’s critical to accelerate and secure application program interface (API) activities beyond standard web content and requests. **APIs are a requirement for digital transformation** – publishing and consuming them opens new revenue streams and enables better user experiences. But to iterate quickly, developers must work the way modern apps are created, using technologies such as microservices and single-page applications. Cloud delivery solutions enable scripted and automated API management controls, allowing developers to **integrate CX improvements and application security into existing DevOps toolchains**, while securing deployments with robust API protection and cloud-based security.

**CASE STUDY**

**Enabling Business Success with a Multi-Cloud Approach**

One of the largest mutual fund companies in the U.S. empowered its application teams to utilize the cloud to best serve customers, regardless of platform. This multi-cloud approach allowed teams to select the right technology to achieve their business goals, rather than the other way around. To maintain consistent web performance and security across multiple cloud platforms, the company used cloud-agnostic web performance and security solutions from Akamai for centralized IT and security to scale, support, and respond to changing business needs. With this approach, IT was able to support application teams without putting the company at risk, allowing security to enable business progress.
VALIDATE
Delivering reliable performance without interruption
A period of market volatility in February 2018 caused investment apps to slow down. According to Reuters, major investment firms “reported service slowdowns on their websites amid heightened demand from clients.” Rising smartphone use, richer graphics and video, and heavy online traffic contributed to the slowdowns as users repeatedly checked apps, expecting instant market updates.

Availability is a top concern for FS organizations. Back-end systems must keep up with front-end improvements. Managing complex digital delivery of rich experiences and heavier pages is crucial. To confirm that the impactful, interactive, and personalized experiences you deliver aren’t going to negatively affect performance, and that CX initiatives are working, you need to test them at scale.

Load testing — against browser, device, and location — provides the confidence that your website and apps won’t fail users. The insight delivered by RUM helps you create test plans based on real user paths, to ensure the right pages, on the right platforms, in the right geographies are vetted before users interact with them. RUM also supports testing in production to safely validate performance without adversely impacting users.

Lab testing allows you to push the system to the breaking point, identify capacity limits, and learn how to recover from failure. However, some common performance complications — such as bandwidth constraints, network configuration problems, and CDN readiness — can only be found in real-world situations. Testing early and often at scale — in the lab and in production — allows you to make infrastructure improvements, change regional server distributions, adjust load balancers, and cache important content in advance of peak traffic periods, so users don’t experience an outage.
But what about the traffic spikes you don’t anticipate? The FS industry is a constant target for high volumes of bot traffic, ranging from mild – such as competitor price-scraping for the lowest rates – to severe – such as credential abuse or large-scale distributed denial of service (DDoS) attacks. You need to ensure that your infrastructure can not only handle the load from legitimate use, but remains responsive even with the additional strain of an attack. Ongoing monitoring with RUM, security analytics, and SIEM will help you brace for impact. This insight allows you to model the level of activity to test, as well as confirm that anti-fraud, anti-bot activities are working and not deterring real users.

**CASE STUDY**

**Taxing the Website for Tax Day**

With millions of U.S. taxpayers filing tax returns online, a best-selling tax preparation software company wanted to confirm that its website was able to support high continuous use as well as occasional surges in user traffic as the tax filing deadline neared. The company selected CloudTest load testing, now offered by Akamai, because it provided the ability to replicate anticipated user load for its website quickly and precisely. With scalable cloud testing, the company reached virtual traffic volumes never before attained – even as real customers accessed the production site – simulating 200% of anticipated peak load for confidence in site performance on Tax Day.
SECURE
Investing in security and CX innovation
If you don’t keep an eye on the changing security landscape, any investment in CX will be cancelled out by the negative impact of a data breach. Security should support new business initiatives, consider user experience needs, and find ways to maintain protection without slowing progress.

The financial industry saw a strong increase in the number of DDoS attacks, experiencing 298 DDoS attacks against 37 distinct organizations in the last three months of 2017, according to the Akamai State of the Internet / Security report. DDoS is a pervasive threat, requiring ongoing protection. Don’t get complacent – continue to review runbooks with vendors and playbooks within your organization on a regular basis to gauge security partner efficacy. Understand the value of DDoS solutions – the technology, the staff, and the service level agreement (SLA) terms – before you come under attack.

The report also found a sharp rise in credential abuse, with more than 40% of login attempts being malicious. Credential abuse is a bot problem, but blocking bots causes them to morph and strengthen into DDoS attacks or adapt to evade detection, and CAPCHAs aren’t effective. A bot management solution with advanced machine learning technology and accurate behavior anomaly analysis will help you mitigate bots, while minimizing performance impact and false positives that block legitimate users.

The security landscape is continually changing, as criminals take advantage of new attack surfaces.

State of the Internet, Akamai
The connections and integrations users demand for convenience create additional entry points for cyber attacks and fraud. It is a constant push and pull between enabling API integrations and agile development, and preventing exposure to threats. As you transition to the cloud, it is critical to consider security for all access points – both incoming and outgoing requests, as well as data in motion.

Securing the corporate perimeter is an increasing challenge, requiring FS organizations to rethink legacy attitudes of on-premises security for on-premises infrastructure. Cloud-based security services protect Internet-facing applications from cyberattacks, but also effectively secure internal and SaaS application access and guard against malware, ransomware, and phishing exploits.

A layered approach to security enhances your organization’s security intelligence practice with the best technology and solutions to create levels of defense from the outside in.

Layered security includes:

- Network management for handling traffic, securing Internet access points, and absorbing attacks
- Domain name system (DNS) protection for fast domain name and IP address resolution
- Application security such as a WAF to shield against threats
- Bot management that goes beyond just blacklisting or whitelisting IP addresses
The best way to protect from increasingly sophisticated cybersecurity attacks is to contract with expert partners that have automation, robust policies for management, and developer tools to integrate, backed by professionals conducting continuous research, providing 24/7 support, and offering the option of managed services. Managed services are vital, freeing your organization to focus on introducing the features and functionality that differentiate your business and keep it competitive.

CASE STUDY

Securing Online Credit Applications

One of the nation’s premier consumer financial services companies, offering private label and co-branded credit cards for leading retailers, found its online credit application under DDoS attack. It engaged Akamai and, within hours, stopped the attack and secured the application. After the incident, the company immediately realized the value of Akamai security solutions, tapping them again to safely move data centers as well as protect online properties from cybersecurity threats. The company also expanded beyond protection to include performance optimization from Akamai. Akamai accelerated the online credit application, bill pay, digital card, mobile wallet, and reward offerings – caching traffic to keep digital products secure and responsive. With Akamai, the company increased the performance of its applications, maximized online resources, saved costs, and improved customer experiences.
Adopting a Trusted Domain Name

To help users easily identify legitimate financial online destinations, you can adopt a financial top-level domain (fTLD) – .BANK or .INSURANCE – to signify your site has been verified and committed to implementing additional mandatory security requirements beyond existing standards. Only verified institutions in the industry are eligible – cybercriminals are identified in the application process and denied domains.

35% of users listed unsecured apps and websites and potential misuse of data as a reason for not using a digital banking channel.

Edelman
Staying Competitive in a Digital Market

To meet customer expectations, you must develop and design experiences that not only provide fast, secure interactions, but deliver them how and where customers want to engage — all the while, keeping pace with technology innovation in online security to maintain vigilance in data protection and preserve customer trust. Financial institutions need to care just as much about CX as security, and the best way to achieve both is by using cloud-based services.

Akamai’s cloud delivery platform is trusted by seven of the top 10 global banks for transactional and sensitive financial web traffic. In banking, asset management, insurance, and other FS segments, many of the world’s largest companies trust Akamai for the security and performance of their web and mobile sites and applications. Over $1 trillion in financial transactions are executed annually on the Akamai Intelligent Platform™.

Akamai’s industry-leading technology is designed to help companies overcome Internet bottlenecks across the globe and protect businesses and their users from advanced security threats. With a complete digital performance management offering, Akamai delivers real user insight to identify and prioritize where to act, integrated tools to optimize performance, and scalable testing to simulate realistic scenarios for the confidence that your applications will meet user expectations. Akamai’s global cloud delivery network helps you get closer to and more available for every user interaction to ensure the most seamless user experiences, wherever they are in the world.
As the world’s largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai’s massively distributed platform is unparalleled in scale, giving customers superior performance and threat protection. Akamai’s portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7/365 monitoring. To learn why the top financial institutions, online retail leaders, media and entertainment providers, and government organizations trust Akamai, please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. Published 07/18.