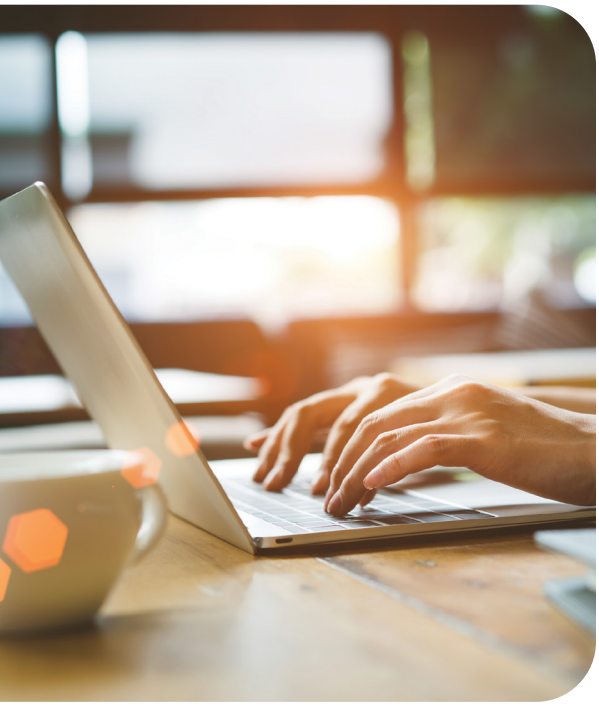
APITURE®

Beyond Features and Functionality

Five Critical Questions to Ask When Evaluating Digital Banking Solutions



When evaluating the strength of a digital banking platform, financial institutions typically begin with a review of the features and functionality available to support consumer and business needs. Ensuring that a particular solution provides the innovative, fully featured capabilities your user base demands is an important first step, but the evaluation shouldn't end there. Understanding a solution's performance capabilities and constraints is equally important to ensure a positive user experience.

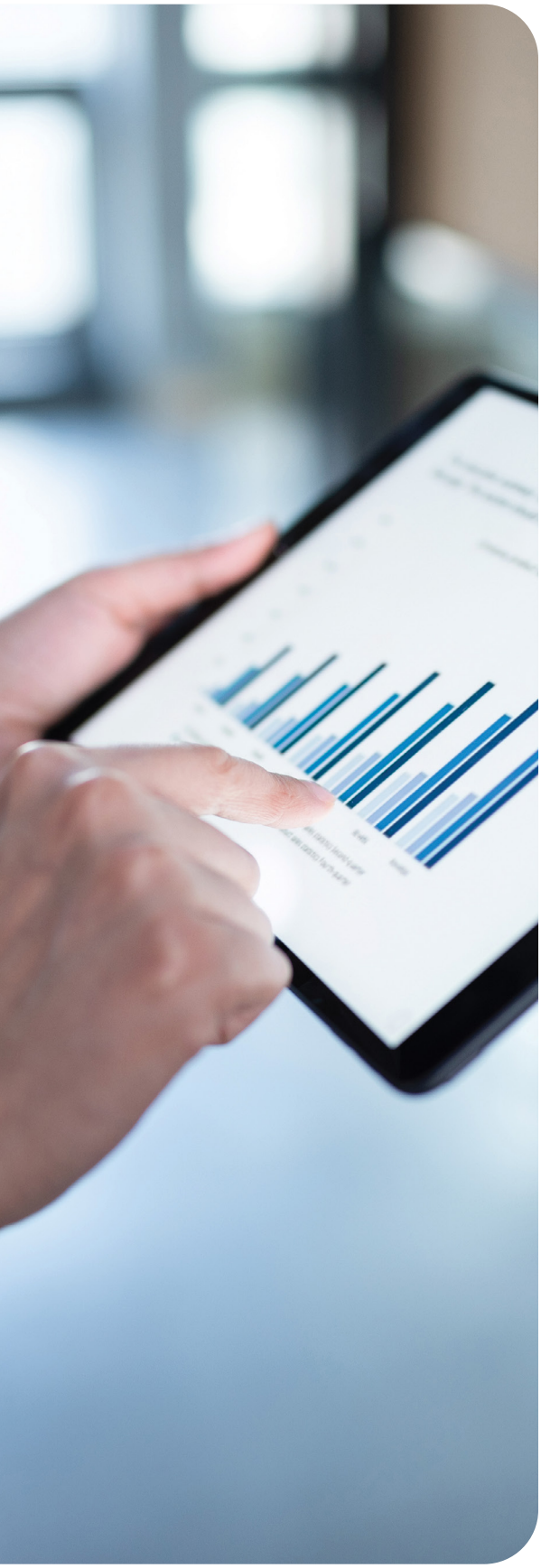
The following are key questions to ask as you assess your existing provider and evaluate potential alternatives.

1 What tools are in place to identify and block security threats?

In today's world, having systems that keep security at the forefront is paramount as financial institutions seek to protect their customers' highly sensitive financial information—and a single breach can have a dramatic impact on brand loyalty and reputation. Understanding the degree to which a potential provider can identify and halt or prevent various threats is critical.

Security is a wide-ranging topic, and you should understand what tools and processes a provider has put in place to prevent breaches. For example, vulnerability testing conducted prior to releasing new code into production is an important internal security practice. **In addition, consider the following topics to understand how a provider mitigates attacks:**

Credential Stuffing: This is a form of brute force login attack, where bad actors test millions of known compromised credentials from other sites, generally from the dark web, against banking and other sites to see if they can successfully log in. A large percentage of users use the same username and password combination across many of their accounts. By performing "credential stuffing," fraudsters can identify a small percentage of working logins to sell on the dark web as working banking credentials. Your digital banking provider should demonstrate it has the tools in place to detect and block these attacks.



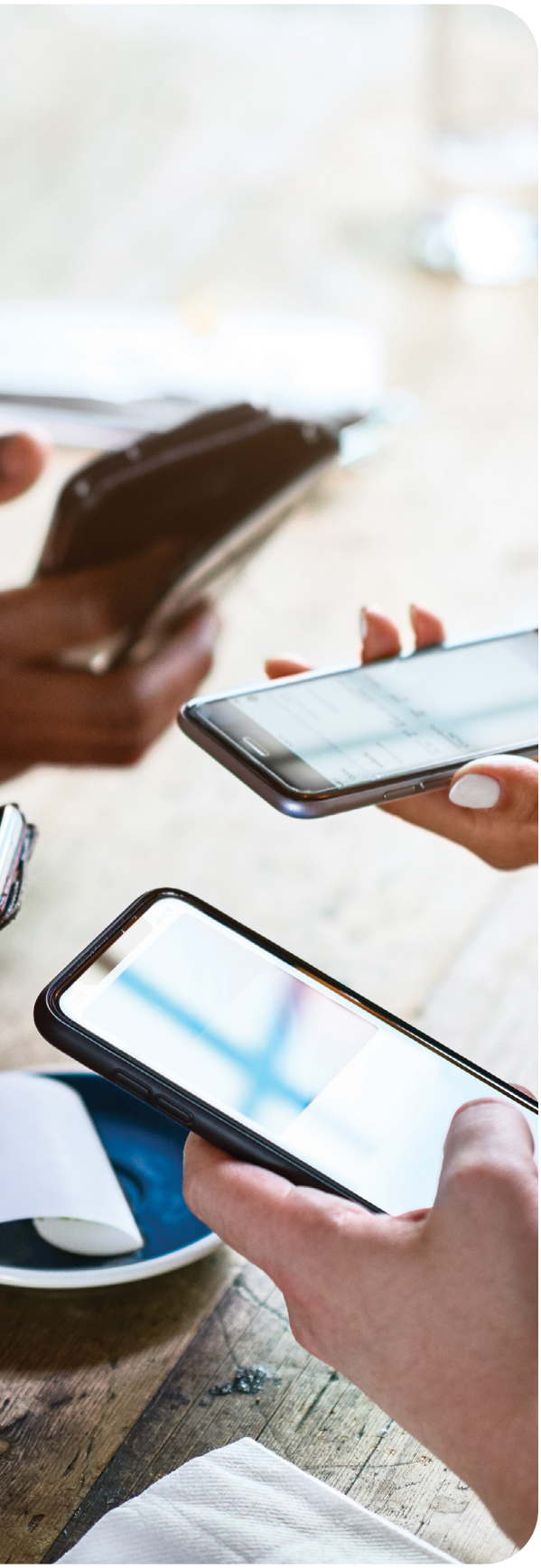
Distributed Denial of Service (DDoS) Attacks: This type of attack represents an ongoing concern for financial institutions. Occurring when a cybercriminal seeks to slow down or block access to a website by flooding it with more traffic than it can handle, DDoS attacks impact financial institutions more than any other industry, according to F5, which says the finance sector was the target of more than 25% of all attacks in 2021. Ask your potential solution provider to demonstrate how its network infrastructure is equipped to detect and route good traffic while blocking DDoS traffic, thereby preventing a slowdown, or worse, a potentially lengthy network outage.

Injection Attacks: As one of the most threatening classes of attacks, an injection attack can result in significant loss or damage to an application's data. There are several types, but in general, a bad actor "injects" malicious scripts or code to an application to change its normal operation or to force it to execute specific commands. Your vendor should be able to articulate specific measures used to prevent injection attacks, such as enforcing least access privilege controls to allow only those privileges that are necessary and implementing processes for validating the code and security of applications.

2 What is the digital banking platform's availability track record?

Downtime has a significant impact on a positive customer experience, so it's critical to understand a provider's availability track record. In today's climate, news of an outage can spread quickly, causing reputational damage that can be hard to repair. For example, a November 2021 outage suffered by Singapore-based DBS—the biggest in more than a decade—was widely publicized internationally. Likewise, Bank of America suffered an outage lasting several hours in October 2021 that resulted in more than 12,000 complaints and extensive media coverage.

Most recently, in May 2022, VyStar Credit Union suffered a digital banking outage lasting over a week following its planned conversion to a new online and mobile banking solution. Citing performance issues with the new platform, VyStar dealt with frustrated members who were unable to complete even the simplest transactions like balance inquiries without visiting a branch. The outage was widely publicized, and the credit union notified customers that digital banking channels were unavailable on its website and even through a YouTube video, truly a worst-case scenario.



When evaluating different vendors' availability data, compare the following:

- **Uptime percentage:** Look for solutions with uptime exceeding 99.9%.
- **Total downtime:** How many total minutes of downtime did users experience?
- **Number of outages:** How many different outages occurred?
- **Response time:** Once an outage occurred, how long did it take the provider to restore the system (minimum, maximum, and average response time in minutes)?
- **Data loss:** Did the provider lose any data following an outage? How much? Were they able to restore it?

A digital banking solution that is based in a public cloud environment like Amazon Web Services (AWS) is likely to result in significantly higher availability than one maintained in a vendor's private data center environment. This is because a cloud-based solution has access to a large network of servers that can protect against failure, while a private data center is limited to the hardware dedicated to a single organization.

Note that while being hosted in the public cloud has advantages, how the provider has architected the solution within this environment is also critical in differentiating one solution from another. Be sure a provider's code is operating in multiple availability zones, with multiple data centers within each, to ensure that if servers go down, they are automatically relaunched quickly. Redundancy is the key to a strong failover and disaster recovery plan.

3 How does the provider ensure stability when introducing changes?

Stability and availability go hand in hand. When new code is released, particularly when numerous changes take place at once, a provider can introduce instability that can significantly impact uptime and the user experience. For example, code changes may result in latency issues that lead to slowdowns or outages.

Choosing a provider with demonstrated software development process maturity is critical here. Vendors should have well-defined performance testing processes, for example, with automated scans that evaluate stability before code is released into production.

Being able to proactively assess, diagnose, and mitigate issues within minutes, often before clients know something is wrong, is often a function of experience. Look for a team with appropriate monitoring tools and the background to know what to watch for and how to react when trouble arises.

Beyond monitoring to confirm your digital banking system is up and servicing, you should also understand a provider's ability to monitor the back-end systems your financial institution connects with. Around-the-clock support will ensure someone is monitoring your systems even when you are not.

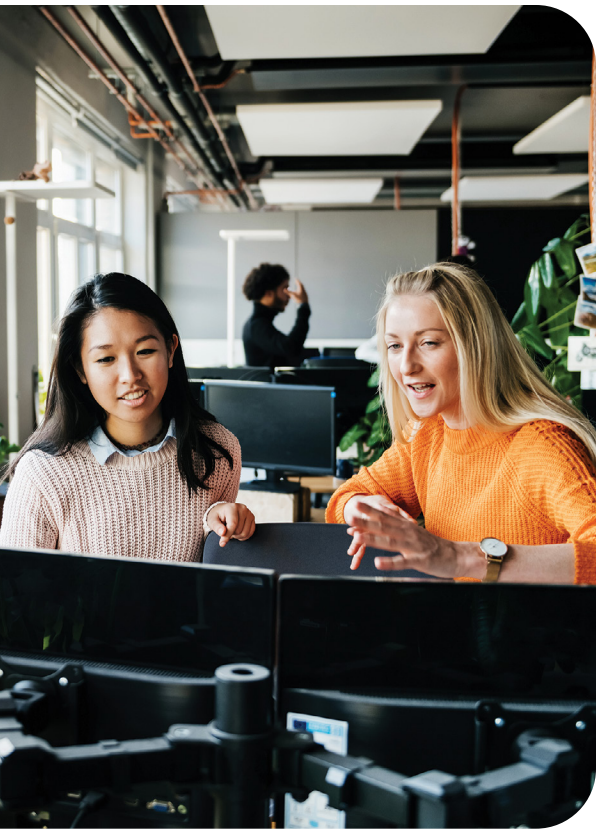
4 How resilient is the digital banking platform?

Having resiliency built into your digital banking solution is essential to ensure your system provides a strong user experience even when disruption occurs. This is particularly important when considering systems to which your digital banking solution connects. If your core banking provider is responding slowly, for example, will the digital banking solution preserve functionality to minimize impact to the user?

5 Can the solution scale effectively?

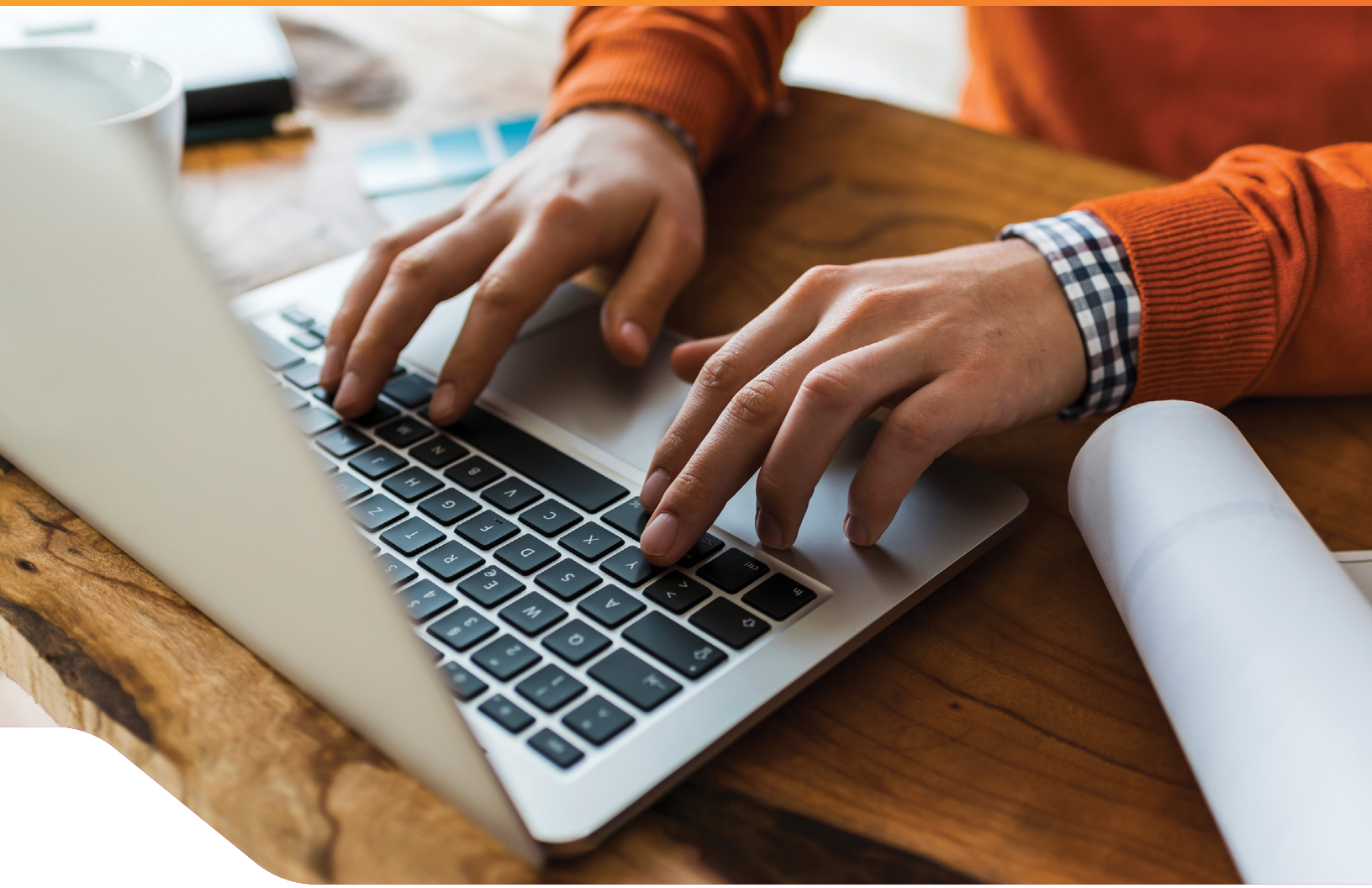
It's critical to understand whether your digital banking solution can scale on demand as your needs change, within a given period or over time. For example, if you were to acquire a new financial institution that doubles your account size, you would need a solution that could support your growth without significant disruption. During periods of peak traffic, such as tax day or the date of stimulus check release, you need a platform–and an experienced team–that can handle higher traffic without bottlenecks that impact the user experience.

At the other end of the spectrum, certain time periods inevitably see lower traffic. While solutions based in a public cloud environment are well suited to scale up or down based on specific traffic needs, those operating in a private data center are limited to the capacity available through existing servers–and pricing models may result in you paying for capacity you don't routinely need.



Optimizing Your Solution

Consumers and businesses are relying on digital banking more than ever before. As you determine the best platform for you and your customers, it's critical to balance the need for features and functionality with strong performance to ensure a positive user experience. Likewise, evaluating the performance characteristics of the systems with which your digital banking platform connects—such as your core banking solution, imaging vendor, and other systems—will bolster the strength of your platform and your overall brand.



About Apiture

Apiture delivers award-winning digital banking solutions to banks and credit unions throughout the United States. Our flexible, highly configurable solutions meet a wide range of financial institutions' needs, from leveling the playing field with larger banks to enabling unique, digital-only brands. Through our API-first strategy, our clients can maximize the capabilities of their platform while preserving a seamless user experience. Our exclusive focus on digital banking means we're dedicated to delivering innovative solutions that meet the unique needs of our clients while providing a level of support that's unmatched in the industry. Apiture is headquartered in Wilmington, North Carolina, with offices in Austin, Texas.

To learn more, visit www.apiture.com

0003_22wp