Digital Banking and UEM

Building a robust security for online banking system

WHITE PAPER

hexnode

TABLE OF CONTENTS

Introduction

Banks have been fulfilling an important role in the society for decades. They are critical to a country's economic growth because they influence the government's monetary policy. The introduction of mobility in banking industry has eliminated old working patterns and significantly changed the industry's working style.

Over the period, banks have adapted to new ways of functioning. However, among all the innovations shaking up the banking sector, mobility is the one that is causing the most substantial alterations across the board. Mobility means assisting organizations in meeting consumer expectations, increasing staff productivity, and lowering the cost of day-to-day activities performed manually.

It has helped businesses stay linked to the rest of the globe while speeding up the process. With mobility, the transaction procedure is automated, requiring no human intervention. As a result, customers are becoming more accustomed to and at ease with doing basic financial transactions on their mobile devices. Nowadays, they desire total control of their cash while investing their money to grow with trusted and effective financial services.

1

Emergence of Digital Banking

Banks are using more digital tools, so cash usage has decreased but savings has increased. Furthermore, long-term sustainability have become a top priority for the authorities.

The expanding number of internet users and a change from traditional banking toward digital banking are the primary factors driving the market's rise. While the banking business stays a constant in society, it evolves as new trends emerge. One of the most popular contemporary banking trends is internet banking, allowing account users to access and manage their cash from home via computer. With internet banking, payment mobility has changed customer behavior and habits. Furthermore, it has also changed how new marketing campaigns are developed to accommodate the new payment method.

The industry is increasing as more cloud platforms, and online payment systems are adopted, allowing for more scalability. This has enabled organizations and people to make low-cost, secure, and fast cross-border payments.

Also, greater usage of artificial intelligence and machine learning in digital banking, and an increase in sophisticated banking services and corporate investors, are expected to drive market growth. Several banks and financial organizations utilize artificial intelligence-based banking systems to provide consumers with faster and more effective customer support.

Talking about digital banking, one cannot forget the digital currency market, as cryptocurrencies have been proving their worth in recent years. To validate transactions, cryptocurrency uses distributed ledger technologies like blockchain. Furthermore, increased use of cryptocurrencies for cross-border transfers is likely to boost industry growth due to lower consumer prices and exchange rates. The increasing number of companies that accept cryptocurrency as an official payment option is one of the primary factors fuelling the rise of cryptocurrencies.

$7.9 trillion

Worth of the global digital banking market in 2021

$10.3 trillion

Estimated worth of the global digital banking market by 2028

Source: Facts & Factors

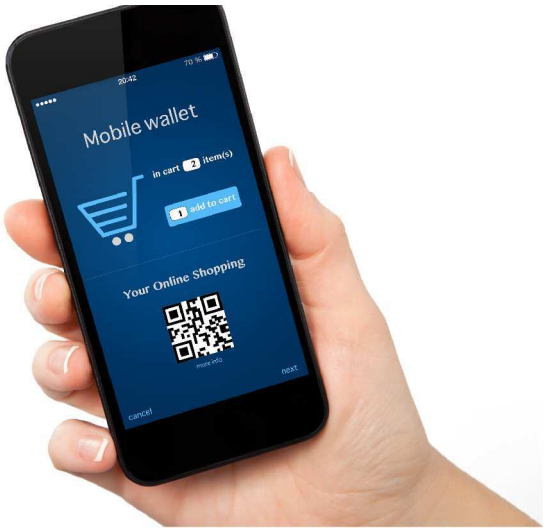
COMPONENTS OF DIGITAL BANKING

Elevating experiences with the cloud

Banks can improve flexibility and speed by leveraging cloud technology to expand their services according to demand. This guarantees that consumer complaints are addressed as fast and efficiently as possible. Simultaneously, this enables banks to rapidly adapt to changing customer demands by offering a uniform, straightforward, and accessible experience across all channels. Banks establish the basis for their digital strategy by assessing which digital interaction techniques are essential to clients and getting capacity in line with demand.

Online payments and mobile wallet access

Before online payments, people had to go to the banks and carry out transactions physically. With the emergence of online payments, you can transfer money between your bank accounts as well as from your account in one bank to another account in another bank. The mobile wallet was beneficial when users wanted to skip the delay in payment caused due to the bank servers. Applications like Samsung Pay and Cash App allow customers to store money in the app wallet and use it when needed without having to go through multiple payment steps.



Technological competency

To make a sustainable infrastructure, banking applications must have a proper frontend layer, middleware layer and a backend layer. The frontend layer includes the website, the application, the SMS, emails, etc. In the middleware layer, the security, authentication, messaging, rules, integration and orchestration of processing is taken care of. The backend layer stores transactional data, customer information, and APIs to integrate third-party services.

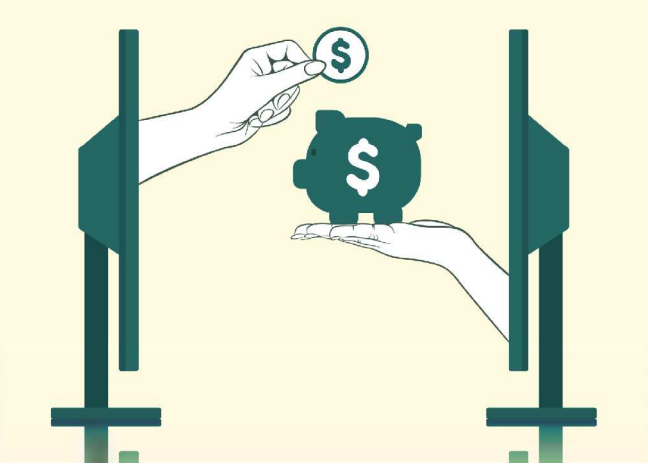
Increased customization

Artificial intelligence (AI) and Machine Learning(ML) help develop complex digital banking software personalization tactics. As a result, banks can provide clients with relevant financial solutions, interactive elements, and educational resources immediately. Budgeting software, expenditure statistics, savings reminders, and a variety of other tools assist in informing and engaging clients.

BENEFITS OF DIGITAL BANKING

Savings on expenses

Traditional banks devote significant time and money to verifying and accounting. By eliminating redundant back-office procedures, digital banking software drastically reduces operating expenses.



Digital banking systems save banks time and money by automating daily transaction operations. Furthermore, digitalization lowers the number of processes and employees involved in transactions and minimizes the likelihood of costly financial blunders.

Enhanced usability

Through integrated KYC and AML processes, digital banks and clients may open accounts in minutes from any device that has access to the internet. As a result, banks can serve consumers promptly and simply using ID verification systems and risk assessments.

One significant benefit of digital banking is that it is always accessible. This implies that clients may conduct any transaction and access various services anywhere.

Security through authentication

One of the most critical components of digital banking is security. Banks must make sure that only the authorized person is making the payments. For this, they use various multi-factor authentication (MFA) techniques.

2

Challenges of digital banking

The digital banking business is growing, but digital lending platforms have security and regulatory challenges. The issues are crucial not just for banks that provide online banking, but also for their consumers, who rely on the institutions to function properly.

LACK OF AWARENESS

The older generation of consumers is skeptical about mobile banking and other cutting-edge financial products. They still choose conventional banking because they believe it is safer and more secure. This hesitation is now one of the most significant barriers to implementing mobile banking.

To address this, banks and other financial institutions must educate their consumers about the advantages of mobile banking. Furthermore, they must promote the simplicity and security of mobile banking to increase usage.

PARTNERSHIP MODEL

Banking apps must handle a variety of partners, including social media outlets, telecommunication companies, merchants, data analytics firms, payment networks, smartphone makers, and so on. They also need to build partnerships with businesses and promote mobile payment options.

They must also educate them on the advantages of deploying POS terminals that enable clients to make payments straight from their mobile phones loaded with NFC chips.

PLATFORM SCALABILITY

Another barrier to the widespread use of mobile banking is platform scalability. To address this issue, third-party online banking application makers and banks must create a software program that can handle numerous mobile operating systems, including Android, Windows and iOS. Furthermore, the software must be interoperable with various communication protocols and form factors.

COMPLEX INTEGRATION

Banking applications must interconnect with all current bank systems and payment hubs to achieve operational efficiency and maximize growth possibilities. It might sound simple, but it is not. The application has to maintain a transaction's consistency, isolation, atomicity and durability.

DEVICE MANAGEMENT

It is crucial to manage the corporate devices used for these financial services efficiently. The challenge is maintaining the device and data security in every possible way.

These devices must be protected from malware attacks and should not give away sensitive information, even in case of theft. IT admin must be able to monitor the device remotely and troubleshoot them if required.

3

Securing digital banking with UEM

The approach of centrally managing endpoint devices from a single place is known as Unified Endpoint Management (UEM). UEM solutions are becoming increasingly significant as more businesses migrate to partially or entirely remote work and implement BYOD rules in their offices.

WHAT IS A UEM?

Unified endpoint management is more than just endpoint management. It offers a single console for deploying, managing and securing business endpoints and applications. It also has provisioning, deployment, troubleshooting, and updating capabilities. UEM software gives IT and security departments access to assets and end users through a single management dashboard.

In addition, UEMs can facilitate malware identification and clean-up on infected devices. With Unified Endpoint Management systems, administrators can monitor and control practically all of your mobile devices, applications, and content.

BENEFITS OF UEM

Enhanced visibility

Gaining visibility throughout the company network is the first step in delivering comprehensive security. UEM increases visibility across all endpoint devices and associated networks, allowing businesses to monitor inventories, data use, vulnerability systems, and other factors. Continuous visibility assists security professionals in being attentive and informed of potential threats.

Enhanced user experience

the primary purpose of installing a security solution is to improve user experience and efficiency without compromising security. It removes the need for numerous tools to manage endpoints, resulting in a consistent user experience and increased productivity.

Low IT management costs

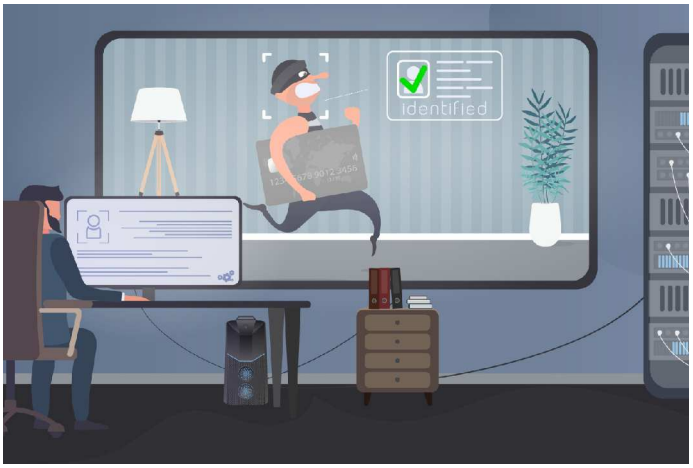
To reduce IT overhead costs and hardware prices, you may automate numerous IT operations and duties, such as endpoint tracking, provisioning, auditing, and data loss services.

Improved business decision making

It allows administrators or asset managers to monitor and evaluate the vast amount of data produced by endpoint devices. It provides diagnostic and predictive tools for analysts to analyze and evaluate data. This data is later utilized to detect threat occurrences and prepare for consequences. Decision-makers may track data, develop customized reports, and make educated decisions with complete visibility and insights.

Monitoring and mitigation of security threats

Security threats may target every endpoint in an enterprise's architecture, so security solutions must monitor every business device for attacks and notify your IT staff if one is detected. Many UEM products include security threat monitoring, which allows you to scan every endpoint in the organization for security flaws and malware. In addition, if the UEM solution has mitigation features, it can also deploy corrective remedies when it detects a hazard. As a result, the UEM tool may prevent or reverse a threat's impacts.



4

Hexnode UEM in digital banking

With cyberattacks and other crimes targeting the banking sector on the rise, implementing tight security measures in all aspects of banking has become more of a need than an option. Dealing with money frequently need a structure that is both safe and adaptable. Hexnode UEM seeks to simplify the entire procedure.

WHAT HEXNODE OFFERS?

Bulk hands-free enrollment

To secure a device with UEM, it must first be enrolled in the UEM console. Enrollment registers a device with your business, assigns it to users, and grants them access to work resources from nearly anywhere. Thus, IT admins would be able to apply regulations and limitations to registered devices, optimizing device operation to save downtime and increase user productivity. Hexnode supports conventional enrollment techniques, Android Zero-Touch Enrollment, Apple Business Manager, Samsung Knox Mobile Enrollment, Android Enterprise Recommended, and G Suite. This method securely onboards corporate-owned devices without configuring each one individually.

Integration with directory services

Active directory domain services store all directory information and manage all user-domain interactions. Hexnode eliminates the need to connect each of your corporate devices manually. From the Hexnode interface, you can easily connect your devices to the Active Directory domain. As a result, there is no need to create new user accounts for each device, and users can log in to their devices using their Active Directory credentials. Apart from Active Directory integration, Hexnode also supports integration with Apple Business/School Manager, Zendesk, SCCM, Okta, G Suite, etc. These integrations not just help in device enrollment but help to unlock additional capabilities as well. For example, Okta is an Identity and Access Management software hosted in the cloud. Using Hexnode, organizations can benefit from its Single Login-On (SSO) solution that enables users to sign in to multiple accounts from a single location.

Separate work and personal space

The entry of personal gadgets into the office may provide enterprises with convenience and increased productivity. Organizations cannot impose stringent security standards on employee devices since doing so may generate privacy issues. Performing a thorough clean on a compromised device frequently requires workers' permission. Organizations frequently employ containerization technologies to organize the packaging, isolation, and encapsulation of work data on distinct partitioned user spaces within the device. It lets corporate and personal apps and data coexist on a single device while remaining inside their respective boundaries. Deploying containerization with UEM technology allows you to mandate the usage of strong authentication and encryption and selectively delete business data from lost or compromised devices while leaving personal data unaffected.

Reports and notifications

Hexnode allows you to produce a variety of reports on the spot, including whole device reports and detailed reports based on particular actions. Hexnode allows you to produce reports at any time or on a daily, weekly, or monthly schedule, depending on your requirements. Admins have to provide the scan's start time and the email address to which the data should be provided. It continually monitors your company's endpoints through compliance checks and status reporting.

Crisis control actions

As devices are essential to businesses, one should treat device challenges and solutions seriously. Any failure to do so might result in device downtime, which can result in severe business losses. So, diagnosing device faults as they arise is critical to guarantee that employees have uninterrupted working conditions. Administrators may remotely inspect and monitor devices from the Hexnode UEM console using a remote view. Furthermore, it enables you to diagnose device faults in real-time quickly. In addition to troubleshooting, Hexnode may remotely erase a device if it is stolen.

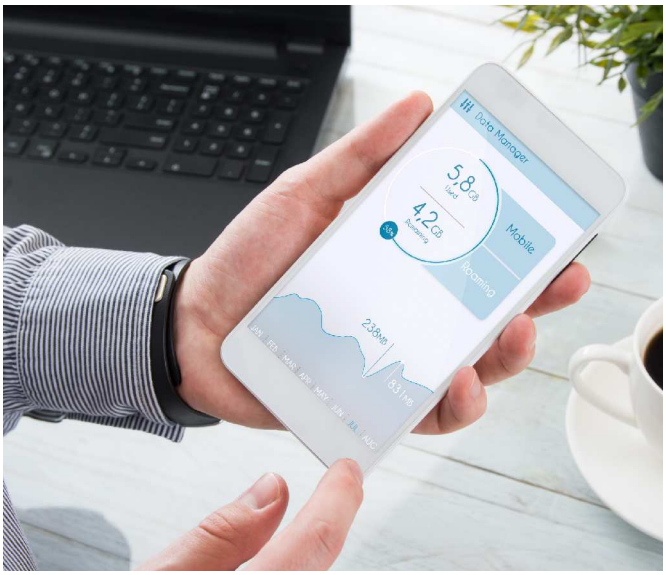
Secure app management

With the banking industry's push toward digitalization, applications have become essential in facilitating transactions and keeping track of their accounts. As more mobile banking apps emerge, ensuring they are safe and adequately protected against vulnerabilities is becoming increasingly important. The Hexnode console makes it simple to administer and install a wide range of applications remotely. The Hexnode interface also provides information on your apps, installation, uninstallation, and updates. Not only that, but you've got everything covered with app blocklisting and allow listing, in-app customizations, and permissions.

Data limiting

Hexnode UEM allows you to easily monitor and manage your company devices. To detect, monitor, and restrict per-app mobile data usage, Hexnode's Network Data Usage Management policy may impose app-level constraints.

For example, while all applications on Android devices can be tracked, only apps loaded with Hexnode UEM on iOS devices may be observed. Admins can set data limits using Hexnode, which notifies them via email if the data limit is exceeded. Additionally, managers can monitor mobile data and Wi-Fi data consumption independently, providing for complete data analysis.



Location-based policies

When businesses need to discover missing or lost devices or maintain track of the location travelled by the device, Hexnode's location tracking comes in helpful. This allows you to preserve accurate logs of the device's location history, making it more straightforward to locate the gadget if it is misplaced. Some specific built-in remote tracking tools make finding your misplaced smartphone a breeze.

Android, iOS, macOS, and Windows devices all support Find My Device. If you enable the functionality, you can find your device by signing into your Google, iCloud, or Microsoft account. Hexnode makes this process seamlessly easy. You may now lock or erase your missing device in a single click by browsing to actions under your particular device, in addition to discovering it with Location monitoring.

Security features

Security is fundamental is in the banking industry. With cyberattacks and other crimes impacting the banking sector, implementing tight security measures in all aspects of banking has become more of a need than an option. You may use Hexnode to enforce strong password restrictions on devices, reducing the possibility of penetration. Furthermore, you may remotely deploy security measures like encryption, VPN, and Wi-Fi rules to protect yourself from external dangers. IT admins can also set up configurations for access control using Identity & Access Management (IAM) feature. Hexnode's lost mode is a security feature that protects your data if you lose your business data-containing devices.

Kiosk lockdown

Hexnode simplifies the process of restricting your devices to the applications that your business trusts. This keeps the user from being distracted by potential diversions and tampering with device settings. With app-based and browser lockdowns, you can restrict your device to a few programs or websites. You may surf safely when the device is locked in kiosk mode using Hexnode's Kiosk browser. This also allows the organization to grant users access to select websites that have been allow listed.

A GLIMPSE ON HOW HEXNODE HELPED VARIOUS FIRMS IN DIGITAL BANKING

The features mentioned above are not speculations or fairy tales. On the contrary, these technologies have benefitted firms; below, you can read about them.

The crypto story

DigitalMint is a cryptocurrency service provider that allows customers to buy Bitcoin and other cryptocurrencies through kiosks and teller windows. DigitalMint distributes bitcoin to customers using iPads as point-of-sale (POS) terminals. However, DigitalMint's leadership team was concerned about the POS's security and deployment.

After implementing Hexnode UEM, they were able to:

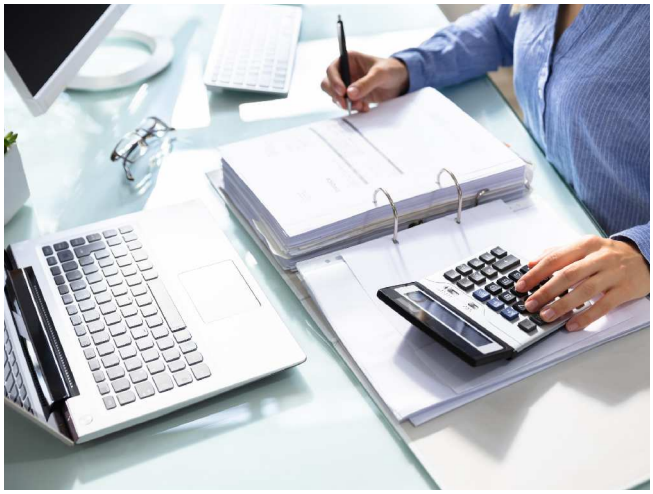
- Ensure POS security with their kiosk lockdown solution.
- iPads may be easily restricted to specific applications, ensuring they are not abused.
- Devices might be restricted to a single or numerous applications.
- Manipulate device settings selectively based on necessity.
- Application distribution across devices in bulk.
- Using app catalogs to create a personalized app store to deliver apps to specific consumers.

Helping CTI

Corporate Tax Incentives (CTI) is a financial services firm that specializes in providing tax solutions for businesses by assisting them in maximizing the tax benefits to which they are entitled. CTI provided iPhones to workers to help them do their business activities efficiently. Ernest Vannorsdell, the Senior Information Technology Manager of Corporate Tax Incentives, owned and controlled these equipment. He had several difficulties when manually handling the equipment. After registering for the trial, he realized Hexnode could match their criteria and was an excellent fit for their firm. He could effortlessly and quickly distribute the app on all iOS devices.

They were able to do the following with Hexnode:

- Execute inventory management and application deployment efficiently. They also enforced fundamental management skills such as password compliance.
- Ensure that access is only granted to authorized users.
- App deployment alternatives that are easier to use and enable for the rapid delivery of programmes to devices.
- Device misuse was reduced.



Conclusion

Today, digital transformation is a top priority for all financial organisations. Furthermore, banks may now provide clients with substantial financial solutions, interactive technologies, and educational materials to enhance their experience.

Security cannot be allowed to take a backseat. So, Hexnode UEM solution helps maintain device security and reduces IT admins' workload.

Tomorrow's market-leading banks will recognize that technology will not restrict what is possible. Instead, they will use digital technology to put the consumer in complete control of their destination and choose a method of engaging with their bank or other service providers. As long as security is maintained, the market will only get bigger with time.

Mitsogo Inc., United States (HQ), 111 Pine St #1225,
San Francisco, CA 94111
Tel: Intl +1-415-636-7555, Fax: Intl +1-415-646-4151