DIGITAL TRANSFORMATION AND CYBERSECURITY:

Safeguarding Banks and Financial Institutions

xiid

CONTENTS

Trend Toward Digital Transformation

The banking industry places great emphasis on digital transformation to enhance operational efficiency, reduce costs, and improve the customer experience. However, increasingly relying on digital systems increases cyber risk and makes strengthening cybersecurity protections and reducing enterprise network attack surface imperative.

Digital banking transformation empowers banks and credit unions to thrive in a swiftly evolving financial landscape. The banking industry has recently witnessed intensified competition from fintech companies and non-conventional participants, including major technology firms. Further, bank employees are increasingly working from home in the wake of the COVID-19 pandemic and, even while at the office, are using Remote Desktop Protocol (RDP) and VPNs to securely access critical internal tools.

As financial institutions increasingly rely on digital systems and technology both internally and externally, they face an ever-evolving threat landscape that demands robust protection measures. In addition, compliance with industry-specific regulations is of utmost importance for banks and financial firms. These regulations serve as crucial guidelines to ensure the security, privacy, and integrity of financial transactions and customer data.

The consequences of cyber-attacks on banks can be far-reaching, affecting not only financial stability but also eroding customer trust and confidence. Therefore, it is imperative for the financial industry and banks to stay ahead of emerging threats, strengthen their cybersecurity protections, and shrink their enterprise network attack surface.

Cybersecurity Impact on Banking & Financial Firms

Cyberattacks can have serious consequences for the financial industry, affecting not only the targeted institution but also the broader economy and public trust. The potential impacts of successful cyber-attacks on financial institutions range from financial losses and reputational damage to regulatory penalties and compromised customer data. Even the possibility of a bank failure resulting from a major cyberattack is not implausible. Understanding these implications underscores the urgency for robust cybersecurity measures in the financial sector.

Almost all financial institutions have experienced a cyberattack in one form or another, and the number of attacks is only increasing. Some recent attacks include:

- **Capital One Data Breach (2019)**
  Capital One, a major U.S. financial institution, experienced a data breach where a former employee of a cloud services provider gained unauthorized access to the bank's systems. The breach exposed personal information of over 100 million customers, including names, addresses, credit scores, and Social Security numbers.
- **Flagstar Bank Data Breach (2022)**
  One of the largest financial providers in the United States, Flagstar Bank, suffered a massive data breach in June 2022, leaking the Social Security numbers of almost 1.5 million customers. The breach is the second such attack on the Michigan-based online banking giant in as many years.
- **Morgan Stanley Client Data Breach (2022)**
  US investment bank Morgan Stanley disclosed that a number of clients had their accounts breached in a Vishing (voice phishing) attack in February 2022, in which the attacker claimed to be a representative of the bank in order to breach accounts and initiate payments to their own account. This was, however, not the fault of Morgan Stanley, who confirmed its systems "remained secure".
- **Experian (2020)**
  A threat actor claiming to be a representative for one of Experian's clients convinced a staff member of the Experian South African office to relinquish sensitive internal data. According to one of the authorities involved in investigations, 24 million customers and almost 800,000 businesses were impacted by the breach.
- **Desjardins (2019)**
  A disgruntled employee of Canada's largest credit union, Desjardins, gained unauthorized access to 4.2 million members' data (SSN, Names, Email Addresses, Transaction Records) with an intent to cause harm to the company. Six months after the event, it was revealed that the breach impacted 1.8 credit card holders outside of Desjardin's member base and likely contributed to approximately $108 million in estimated damage costs.

Financial institutions face distinct challenges when it comes to cybersecurity due to the sensitive nature of their operations and the vast amounts of valuable data they handle. This is why the financial sector is the one of the leading groups targeted by cybercriminals, ranking second only to healthcare.

Sources

https://www.upguard.com/blog/biggest-data-breaches-financial-services
https://tech.co/news/data-breaches-updated-list

Banks and financial institutions must navigate a complex and evolving landscape of requirements along with a proactive approach to security throughout the organization. Key issues include:

- **Balancing User Experience and Security:** **providing a seamless user experience (UX) and ensuring robust security, all while managing complex authentication and verification processes**
- **Increasing Sophistication of Cyber Threats:** **adapting security measures to address evolving cyber threats, such as social engineering, advanced malware, ransomware, and state-sponsored attacks**
- **Legacy Systems and Infrastructure:** **managing outdated legacy systems that cybercriminals state-sponsored actors can exploit; updating and securing systems while minimizing disruption to operations**
- **Insider Threats:** **striking a balance between granting employees necessary and convenient access and implementing controls to prevent abuse or unauthorized access to sensitive data**
- **Third-Party Risks:** **collaborating with third-party entities necessitates effective management and security measures to protect sensitive information**
- **Regulatory Compliance:** **navigating a complex regulatory landscape and ensuring adherence to multiple compliance requirements while maintaining effective cybersecurity practices**

As banks navigate through the challenges of this stressful landscape, their manual and digital systems continue to experience both a surge in usage as well as deviations from traditional patterns. Simultaneously, cyber and anti-fraud teams are diligently implementing temporary rule changes in transaction monitoring and surveillance systems. This wave of heightened activity, coupled with the temporary rule modifications, increases the probability of malicious activities by cyber adversaries going undetected.

In light of these circumstances, banking and financial institutions must proactively take action to mitigate or eliminate their risk exposure.

Key Takeaways

- Increasing digital transformation of banks often increases banks' risk of major cyberattacks
- Cyberattacks undermine consumer confidence and can be extremely expensive for banks to recover from
- Distinct cybersecurity challenges for financial institutions include UX, state-sponsored threats, legacy systems, insider and third-party threats, and regulatory compliance

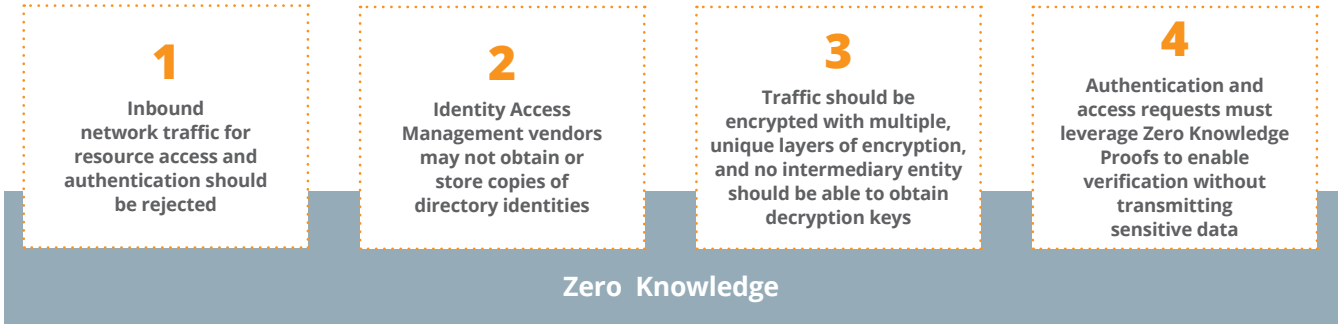
Zero Knowledge Networking Cyber-Defense

Xiid Zero Knowledge Networking (ZKN) solutions have been specifically designed to offer essential security enhancements tailored for banks and financial institutions. These solutions prioritize the protection of sensitive information, ensuring secure authentication, and reinforcing data exchange processes.

Zero Knowledge Networking guarantees that all parties – the endpoints and the vendor in-between – have no excessive knowledge of each other's sensitive data or location, eliminating vulnerabilities in a way that's proactive, rather than reactive.

Since Xiid's entire platform works outbound-only, institutions can block all inbound traffic and dramatically shrink the enterprise network attack surface.

While Zero Trust Network solutions in the market largely utilize "break-and-inspect" and AI-enabled firewalls to react to incoming attacks and exploits, ZKN fundamentally re-architectures the network to be naturally and proactively resistant to a wide range of attacks.



Zero Knowledge Networking Framework Tenets

To be considered Zero Knowledge, networks must adhere to the following tenets regardless of the type of network traffic.

Inbound network traffic for resource access and authentication should be rejected

Client devices and the enterprise private network should not require open inbound firewall ports for authentication or resource access. Attackers frequently target open ports for vulnerabilities. All access to resources, no matter the resource, should be achieved using outbound-only traffic on both endpoints. Further, since all traffic is outbound-only, neither endpoint should require or need to share a public IP address.

Identity Access Management vendors may not obtain or store copies of directory identities

Authentication requests should be processed and carried out efficiently without federation to a third-party service. Copies of sensitive identity information in Identity Access Management (IAM) vendors' data centers are extremely risky and dramatically increases the enterprise attack surface. Taking this risk should not be necessary for an organization to securely authenticate its users.

Traffic should be encrypted with multiple, unique layers of encryption, and no intermediary entity should be able to obtain decryption keys

All traffic should be encrypted with multiple layers of encryption, with the encryption algorithms used varying across the layers. This variation is key, as is it far more difficult for an adversary who can defeat one type of encryption to defeat multiple. There must be at least two layers of encryption, and one of the inner layers must use an Authenticated Encryption with Associated Data (AEAD)-type encryption method.

The Xiid Solution

Identity Access Management

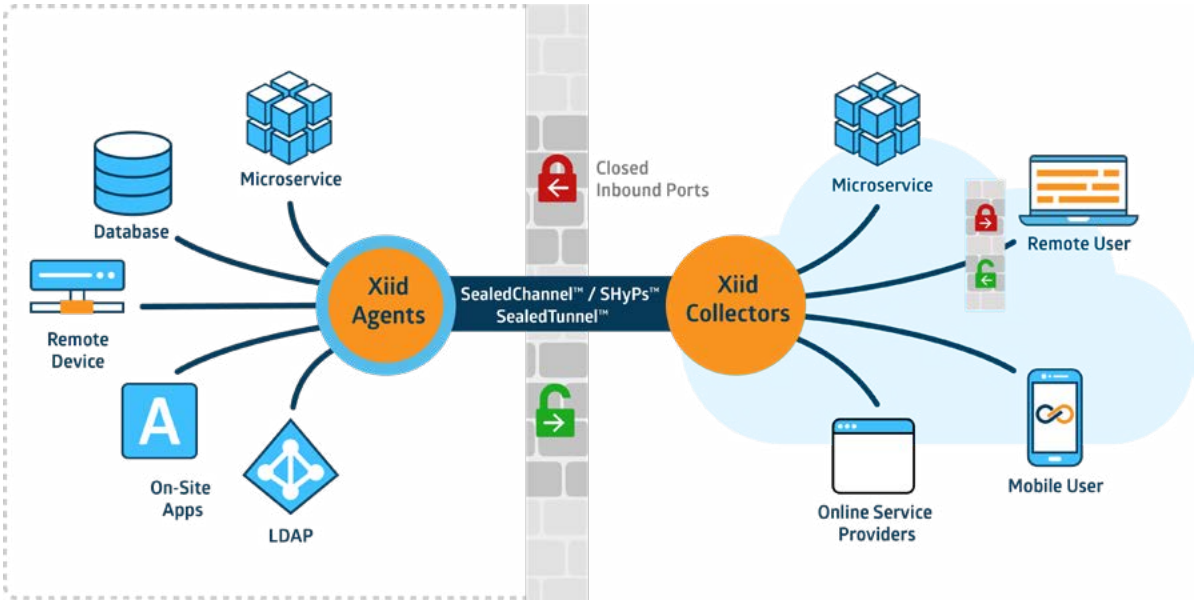
Xiid's Zero Knowledge IAM solution offers a unique, credential-less authentication process that leverages Zero Knowledge Proofs, eliminating the need for stealable, traditional usernames and passwords. Instead, it leverages advanced cryptographic techniques to verify user identities securely through the XOTC™ authenticator. All authentication requests can be serviced without any open inbound ports or risky third-party directory federation.

Xiid's XOTC™ authenticator application also serves as a comprehensive solution for mobile device checks. It performs thorough assessments to identify any indications of device compromise, such as the presence of malware, jailbreaking, rooting, and other security vulnerabilities. If the XOTC™ authenticator detects any signs of device compromise during the authentication process, it will refuse authentication and deny access to the requested resource. This proactive approach ensures that only secure devices are granted access, minimizing the risks associated with compromised endpoints.

By embracing credential-less authentication, banks can strengthen their security posture while reducing their reliance on vulnerable credentials and minimizing the impact of common cyber breaches. This approach not only enhances trust and confidence but also secures and future-proofs the enterprise network in an evolving threat landscape.

SealedTunnel™ Tunneling and Resource Access

Xiid's SealedTunnel solution establishes a highly secure, outbound-only, double-encrypted communication channel that remains unseen to potential intruders.



Without requiring open inbound ports, the SealedTunnel secures any internet or intranet traffic while making the enterprise network appear virtually invisible from the outside. Unauthorized access attempts and eavesdropping are effectively thwarted, ensuring the protection of sensitive financial data and key internal applications.

Bank networks are further protected by using SealedTunnel's process-to-process connections rather than traditional VPNs that connect endpoints to entire networks. This makes the enforcement of microsegmentation much easier, as segmented machines and servers can close all inbound firewall ports and still be reachable by the SealedTunnel.

Encryption and Data Protection Measures

Xiid offers robust encryption measures to enhance the security of financial processing. The platform ensures that all communication to and from endpoints is safeguarded by multi-layer encryption. This approach significantly strengthens the confidentiality and integrity of data transmission.

Xiid's encryption framework is designed to support various encryption methods within the elliptic curve family. This flexibility allows the platform to accommodate different encryption algorithms. By leveraging this framework, Xiid enables organizations to utilize encryption techniques that align with their specific security requirements and preferences.

Bank and Financial Use Cases

Secure Remote Access for Employees

With the increasing trend of remote work, employees in the banking and financial sector often need to access sensitive information and systems from outside the organization's network. The Xiid Zero Knowledge IAM solution with the XOTC authenticator provides secure remote access by implementing one-time credential-less authorization, adaptive access controls, and continuous monitoring that together largely eliminate the risk of credential theft or unauthorized access.

For example, a bank could deploy the Xiid IAM solution and require employees to authenticate themselves before accessing critical applications or databases. The solution continuously monitors user behavior and evaluates the risk associated with each access request. This approach ensures that only authorized and authenticated employees can access sensitive financial data, regardless of their location.

Employees could then use the SealedTunnel to access key resources and internal applications, rather than VPNs, allowing them to connect only to the resource they need while protecting the wider enterprise network from attacks.

Customer Identity Protection

Xiid's IAM solution plays a vital role in customer identity protection by implementing strict access controls and identity verification measures.

For instance, a bank may implement the Zero Knowledge IAM solution to verify customer identities before making online banking transactions or when accessing financial services. This approach minimizes the risk of account takeovers or identity theft by ensuring that only legitimate users can access their accounts or perform sensitive transactions, improving customer trust and reducing costs associated with identity theft resolution and mitigation.

Summary

As financial institutions increasingly move towards digital solutions, both for their customers and employees, their risk of damaging cyberattacks may increase. Zero Knowledge Networking (ZKN) has emerged as a proactive defense solution, prioritizing secure authentication and protecting sensitive information. This allows financial institutions to proactively mitigate cybersecurity risks to ensure a secure digital transformation in a dynamic financial landscape.

Engineered by longtime industry cybersecurity experts, Xiid offers the leading framework for secure access to an organization or agency's most sensitive assets from anywhere in the world.

xiid®

xiid.com