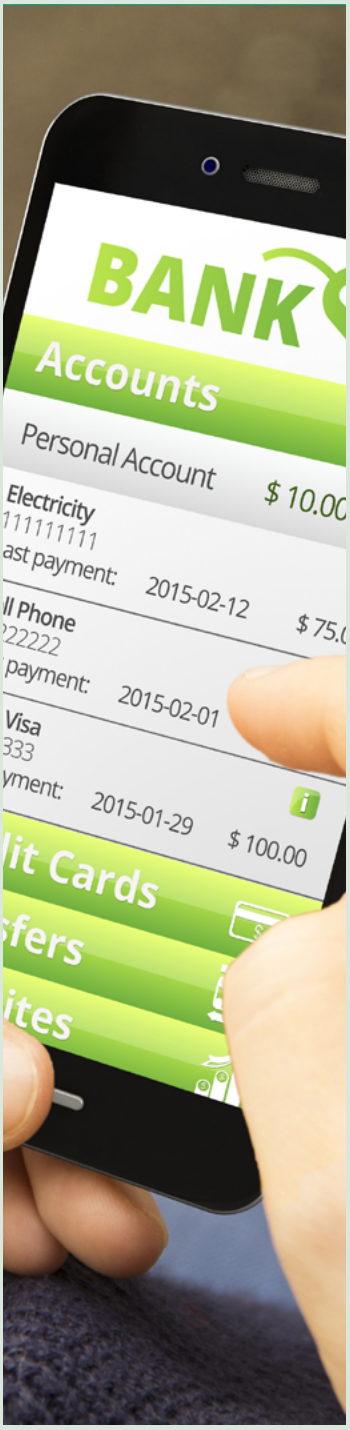
WHITE PAPER




# HELPING BANKS SECURE DATA DURING AND AFTER DIGITIZATION

An Infosys solution

Infosys®
Navigate your next

## Abstract

The banking industry is adopting digital technologies to renew how they deliver services to customers and increase efficiency in back-end operations. However, leveraging emerging technologies such as mobility and cloud solutions expose banking organizations to new vulnerabilities that plague the digital landscape. This white paper examines the right approach and the key elements of a successful data security strategy. It also describes an Infosys solution that helps banks protect their data from external threats.

## Introduction

Banking digitalization plays an important role in catering to consumer demand for instant multi-channel access to any banking service or product. Additionally, there are a slew of technologies that are making in-roads into the banking industry to help organizations sustain their edge, retain customers and increase loyalty.

However, adopting digital comes with its own challenges, particularly in terms of security. It opens new doors for security breaches, posing greater risk for data theft. Compared to traditional banking, online banking is increasingly vulnerable to such attacks as customer data is available online across multiple channels and players. In fact, reports indicate that 33% of attempted breaches against financial services and insurance companies are successful[1].

The three main threat avenues for online banking are:

- **Mobile malware** – Trojans, viruses and rootkits infect devices from unsecured third-party online sites that are accessed from mobiles, enabling easy information theft
- **Third-party apps** – Downloading third party applications to mobile devices from untrusted sources or without verified information is a key threat
- **Unsecured Wi-Fi** – Unsecured wireless networks allow entry for fraudsters into mobile devices either to seize control of or gain access to account information. This is a threat for customers who opt to store bank or card details on third-party websites when they choose the option 'save details for future transactions'. Successful hacks on such third-party sites or mobile applications enable identity theft of registered customer data

As cyber threats becoming increasingly sophisticated, there is a pressing need to upgrade security systems and implement intelligent threat monitoring and protection solutions. These solutions track the threat landscape, political climate, third-party risk, insider threat, and more. Thus, to combat threats to security and data during and after digitization programs, banks must first develop and implement a comprehensive and fool-proof cyber security strategy.

## Enabling end-to-end fool-proof data security

Banks that go digital should have a well-defined strategy for data security to deepen customer trust and loyalty. The three key elements of such a strategy are:

- **360-degree defense** – Banks need a holistic and robust defense mechanism to detect breaches immediately. This is a critical need as 59% of respondents in a recent study stated that it takes months to detect a security breach[2]. Timely threat identification requires latest technologies that are programmed to monitor and detect existing and new threats, intrusions and abnormal behavior. Organizations can also prevent data theft by separating systems, data and applications. Finally, data encryption and network segmentation helps minimize nefarious use of stolen data.
- **Strong resilience** – Resilience to cyber attacks is an important aspect of a bank's recovery process. It limits negative outcomes of any breach and allows the organization to return to normal operations quickly with minimal impact on customers and services. To enable strong resilience, banks need clear defensive actions such as proactive controls, testing of crisis response protocols, cyber security assessments, and penetration testing.
- **Service assurance** – To ensure uninterrupted services, it is necessary to incorporate strong defense and resilience protocols into daily business activities. Further, banks should periodically test their cyber defense mechanisms, track adherence to security norms and procedures and conduct employee cyber education to highlight risky behavior. Developing a clear methodology that identifies strengths and areas for improvement is strongly recommended.

## A holistic approach to cyber security

Implementing the above three elements requires a comprehensive approach spanning tools, solutions, internal training, and a security-driven organizational mindset. A recent study reveals that 78% of respondents are confident that the right cyber security program will yield valuable outcomes[2]. Here are some ways banks can ensure their cyber defense strategy meets all the necessary requirements to mitigate risk, respond to threats, recover from attacks, and comply with security regulations:

- C**hoose the right security applications and tools to tackle security threats** – Currently, banking institutions spend an average of 8.2% of their total budget on cyber security[3].To maximize value, banks must identify and implement the right network infrastructure. They should invest in fool-proof cyber security solutions and tools to handle security breaches and avert potential attacks. At this stage, it is important to identify the right technology partner and collaborate with anti-virus, anti-spyware and endpoint protection partners to reinforce security.
- **Regard information security as an organizational issue** – Cyber security cannot be relegated to a single department that functions in a silo. To protect data as it travels across the enterprise, banks must first re-evaluate existing back-office and front-end controls and processes. They should include additional verification layers and security systems with multi-level checks to ensure safe transactions across different channels. Finally, banks should maintain robust control processes to track, identify and report suspicious activities.
- **Fuse security into product development** – Innovation is a continuous process and security must be embedded across all stages of innovation. Thus, cyber security assessment and planning should be an integral part of product development and service launches. Dedicated security teams should be included in core product teams to ensure that all products and services are secure from threats.
- **Train internal employees on appropriate behavior** – Banks should integrate cyber-security into the business by training their employees to follow the right procedures. This will ensure that security is built into every workflow and eliminate risky behavior that allows hackers to gain access into internal systems. The importance of such training is significant when one considers that 48% of banks report that the greatest security impact comes from malicious insider threats[4]. When it comes to internal security, banks should also institute robust registration and secure login processes and journeys. This includes upgrading login access by opting for Digipass and PIN entry processes.
- **Leverage advanced threat protection solutions** – Advanced threat protection (ATP) is a combination of multiple security solutions designed to prevent hackers from stealing private and sensitive data. It includes solutions for malware protection to safeguard network devices, email gateways and endpoint agents as well as a centralized management platform. ATP solution suites leverage digital technologies such as AI and self-learning machines to prevent, detect and mitigate threats that may compromise the bank's data, thereby bolstering security efforts and minimizing risk.

## Cyber security solution by Infosys

The Infosys Cyber Security Practice provides data privacy and security solutions that meet the varying needs of clients from different industries. Our cyber security service offerings are delivered through the security operations center (SOC) that has a global reach. The main services offered are data discovery and classification, data masking, data loss prevention (DLP), data encryption, digital rights management, and data activity monitoring.

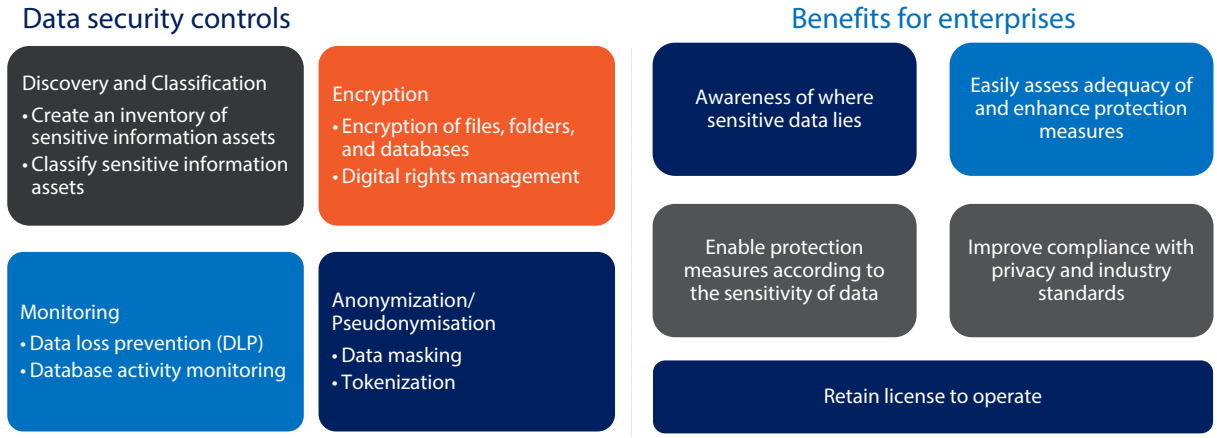
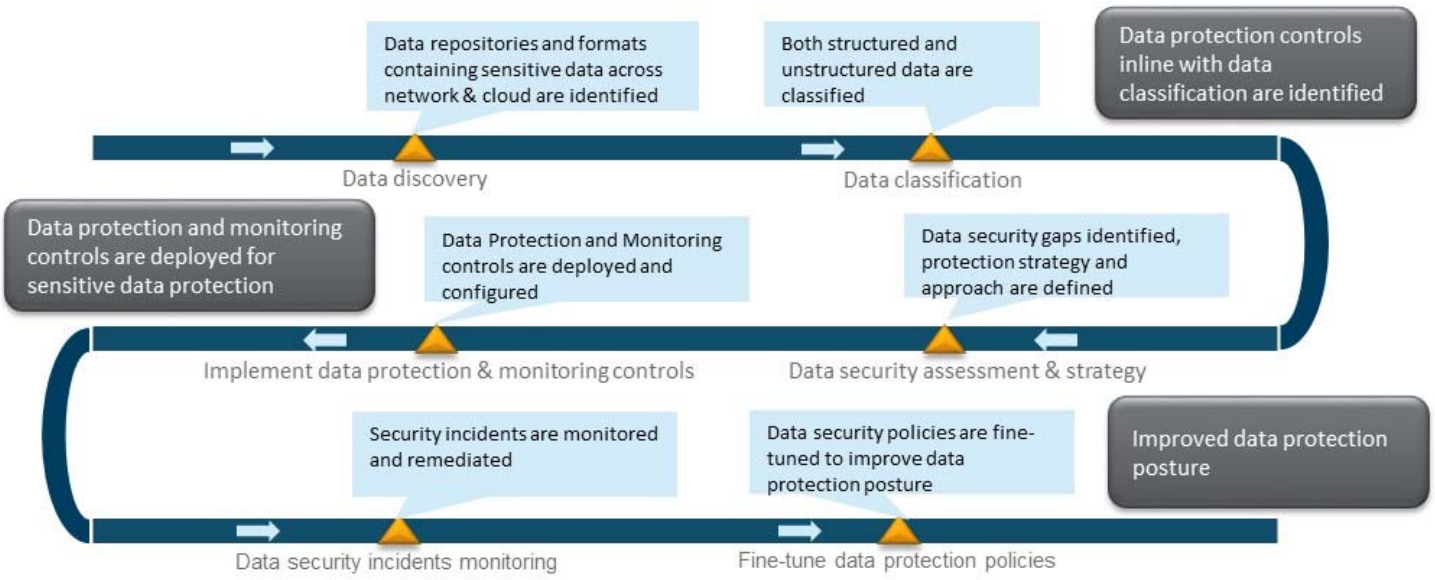



*Fig 1: Types and benefits of data security controls*

Our methodology for data protection begins by identifying and classifying data based on its importance and sensitivity. Classified data is encrypted and monitored for any loss or change. The data is finally passed on to the respective gateway channel. Each stage of this process is designed to ensure the highest level of data protection through stringent monitoring.




Data discovery, classification, security incident monitoring, and policy fine-tuning are continuous processes. New threat vectors and risks will necessitate periodical assessment and improvement of data security posture. This is an ongoing journey.

*Fig 2: Infosys methodology for data protection*

Infosys also provides an integrated data security solution that monitors data flow through several endpoints. The solution ensures that all sensitive data is classified, masked and passed to the respective gateway channels.

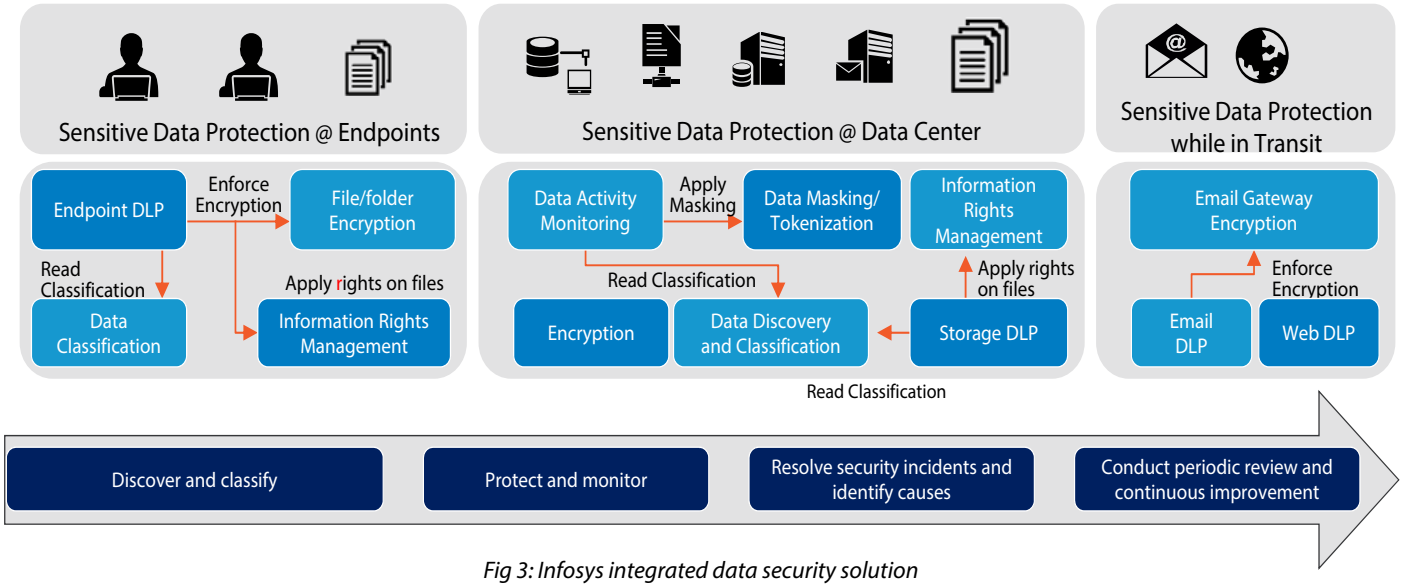
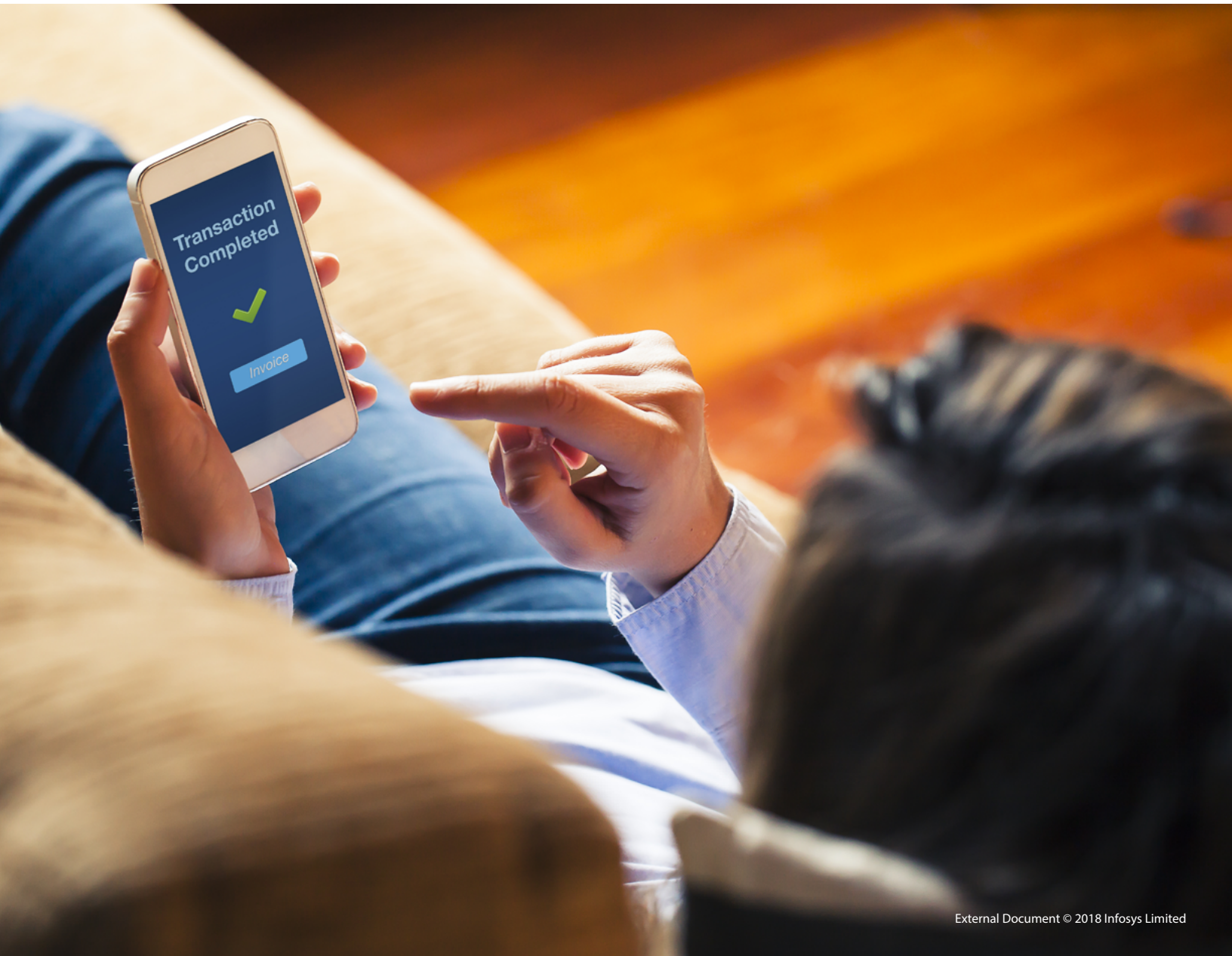



*Fig 3: Infosys integrated data security solution*



## Conclusion

Digitization is becoming a key driver for banks to sustain their business. While digital transformation offers several innovative capabilities to improve products and service delivery, it also exposes banks to a higher number of cyber threats. Thus, the topmost priority when embarking on a banking digitization journey is a robust and comprehensive data security strategy that enables 360-degree defense, strong resilience and service assurance. Infosys Cyber Security solution helps banks upgrade their security systems and protocols to ensure safe data transfer within and outside the organization. With capabilities such as data masking, encryption, and protection, the Infosys solution allows banks to confidently adopt digital, sustain their edge, and cement customer loyalty through secure banking platforms.

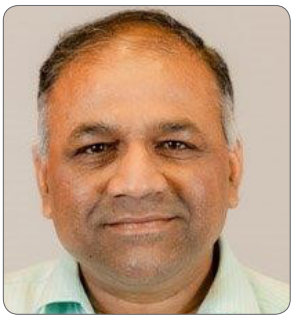
## About the Authors

**Senthil Rajkumar Shankar**

*Senior Consultant*

Senthil is a Senior Consultant with Domain Consultancy Group at Infosys. He holds MBA in Information Systems, a Bachelor of Applied Science Information Technology, and has over 13 years of experience in Core Banking System implementation of Retail as well as Corporate banking operations for major banking clients across US, UK, Europe and APAC regions.

Prior to Infosys, he worked with ABN Amro NL and Ford Business Services.



**Venkataramana R**

*Principal Consultant*

Venkat is a Principal Consultant with the Infosys - Financial Services – Domain Consulting Group providing consulting services to Banks in strategic transformational journeys. His prior experiences include stints as a Senior Retail branch head for 12 years, heading the Bank's information technology division for 5 years and leading a global Core Banking product group's activities in an IT major for 6 years He has strong expertise in Retail banking, Core banking and surround solutions. Some of the key transformational programmes supported in large global banks across US and Europe are across areas in Core Banking, Retail lending, Branch transformation, Dealer lending, Test data management and ICB Ring fencing program.

## References

1. https://authentic8.blog/five-must-read-reports-for-it-security-leaders-in-financial-services/
2. https://www.infosecurity-magazine.com/news/banks-confident-about-cybersecurity
3. https://cybersecurityventures.com/cybersecurity-market-report-q3-2015/
4. https://economictimes.indiatimes.com/industry/banking/finance/banking/one-in-three-cyber-attacks-in-banks-are-successful-report/articleshow/58396453.cms

For more information, contact askus@infosys.com

Infosys®
Navigate your next