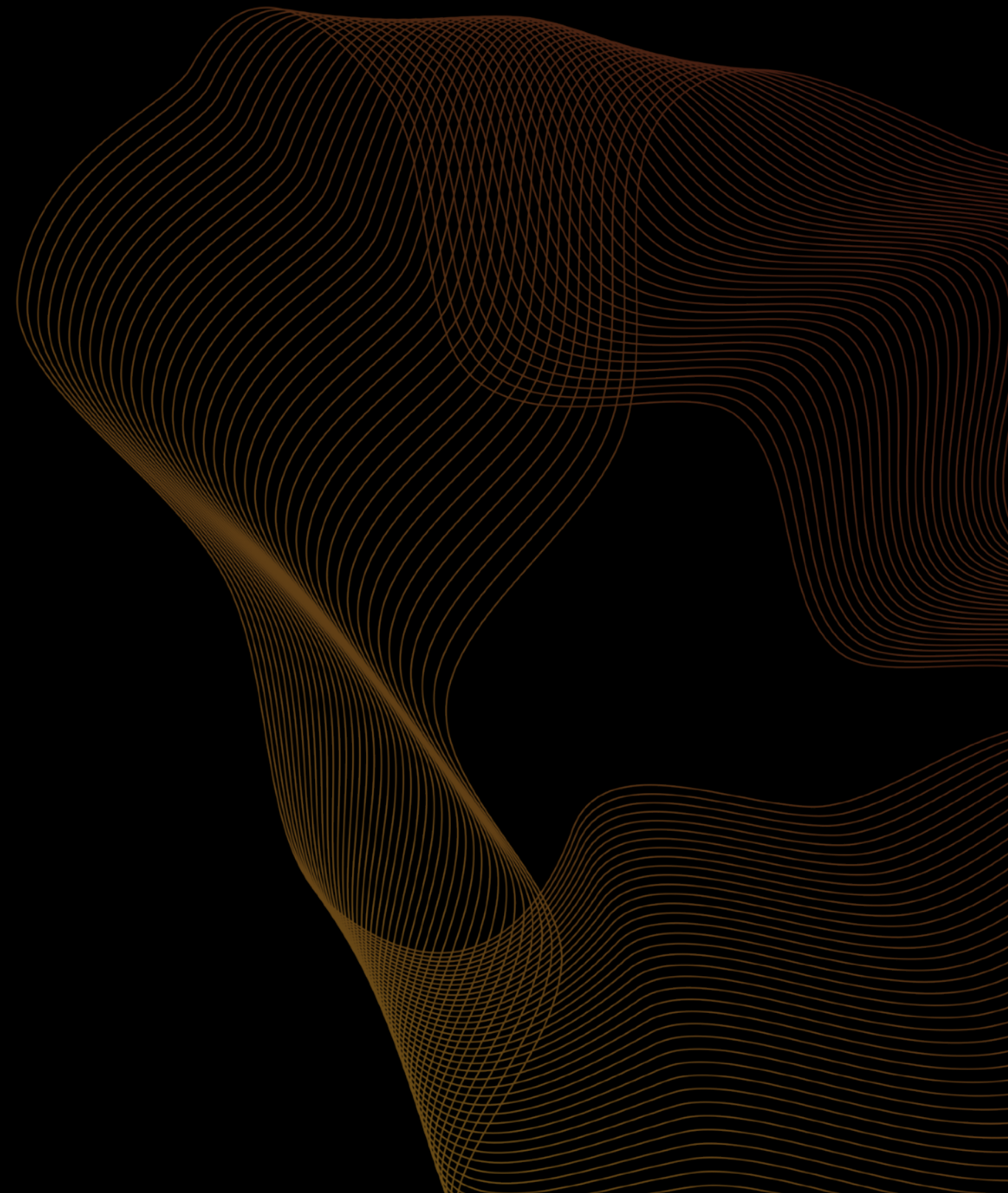SUMERU

How Sumeru helped fin-tech startup Onemoney to secure their business critical applications?

Sumeru Cyber Security Case Study

SUMERU

About the client

Onemoney, India's First Account Aggregator, licensed by RBI is building a sustainable, trust and consent based sharing of data between citizens and enterprises.

Championing data democracy, Onemoney is developing user experience tools and APIs for users and enterprises. With Onemoney solutions, citizens have control over their financial data and financial institutions have the power to safely share and receive consumers' data.

Sumeru helped Onemoney Onemoney management to understand their potential cyber risks and build a robust Security Program to tackle them.

SUMERU
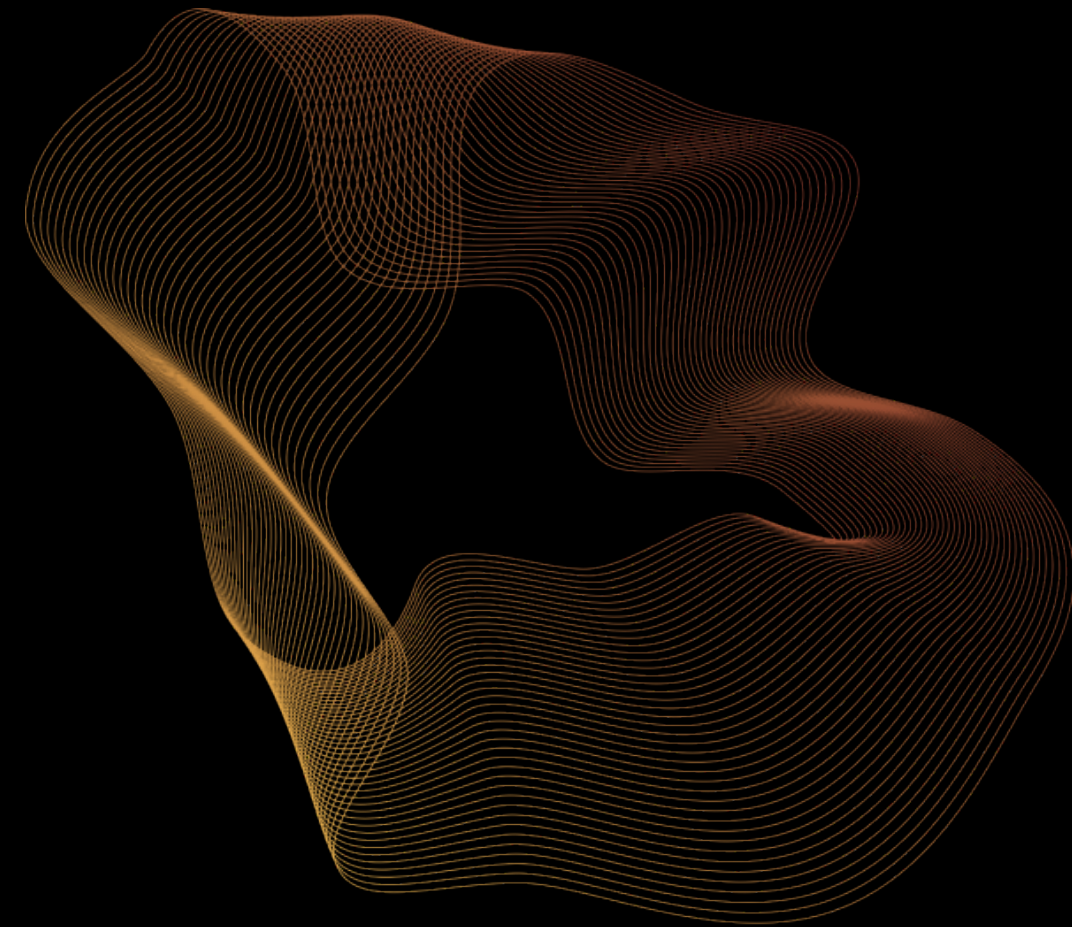
Sharply reducing the cyber risks by introducing security measures and protecting sensitive apps and information

Identifying and prioritising right security measures is a major challenge for a business institution like Onemoney. Malicious persons can leverage the vulnerabilities of the infrastructure and applications to compromise critical assets and steal sensitive data.

Sumeru helped Onemoney with a clear picture of their cyber risk posture and determine how much security they need. We started by looking at their current IT assets (hardware and software) as well as your business priorities to arrive at a security plan specific to their business. We helped Onemoney with…

- Security Advisory
- Application and Network Penetration Testing
- Secure Code Review
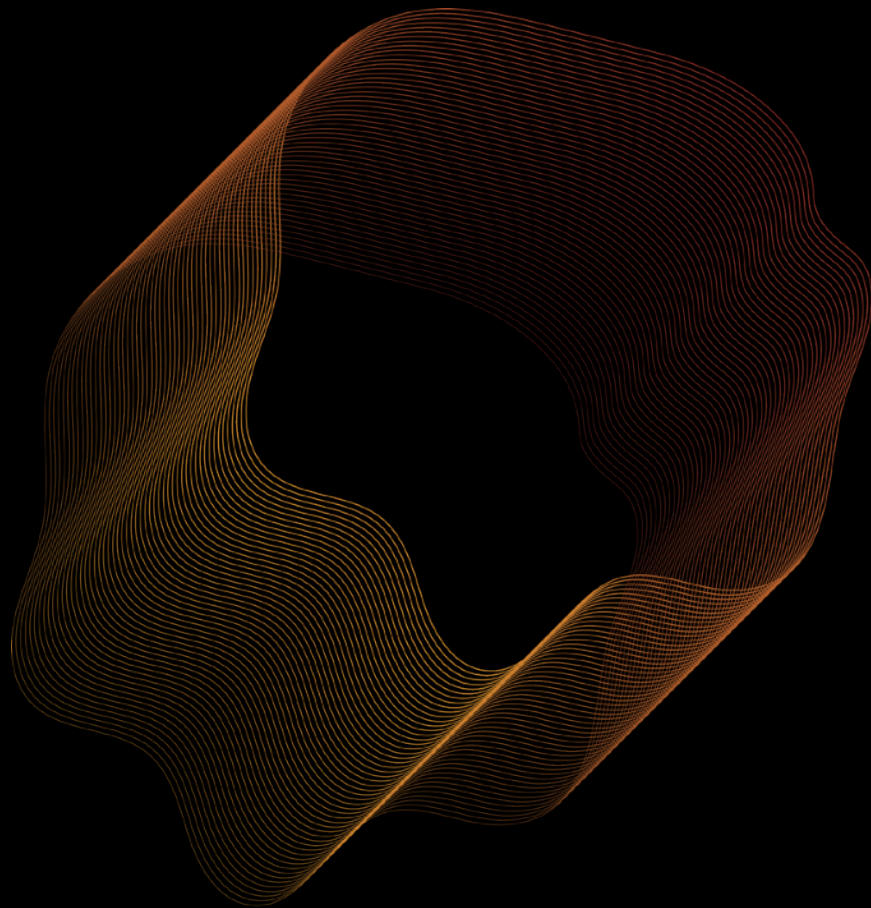
Business requirements

- A systematic security plan for Onemoney, implemented based on their business priorities

- Perform the security risk assessments for the business-critical web applications and network services

- Provide detailed recommendations on the improvement of information systems' security level

- Handhold inhouse teams to adapt to secure application development practices
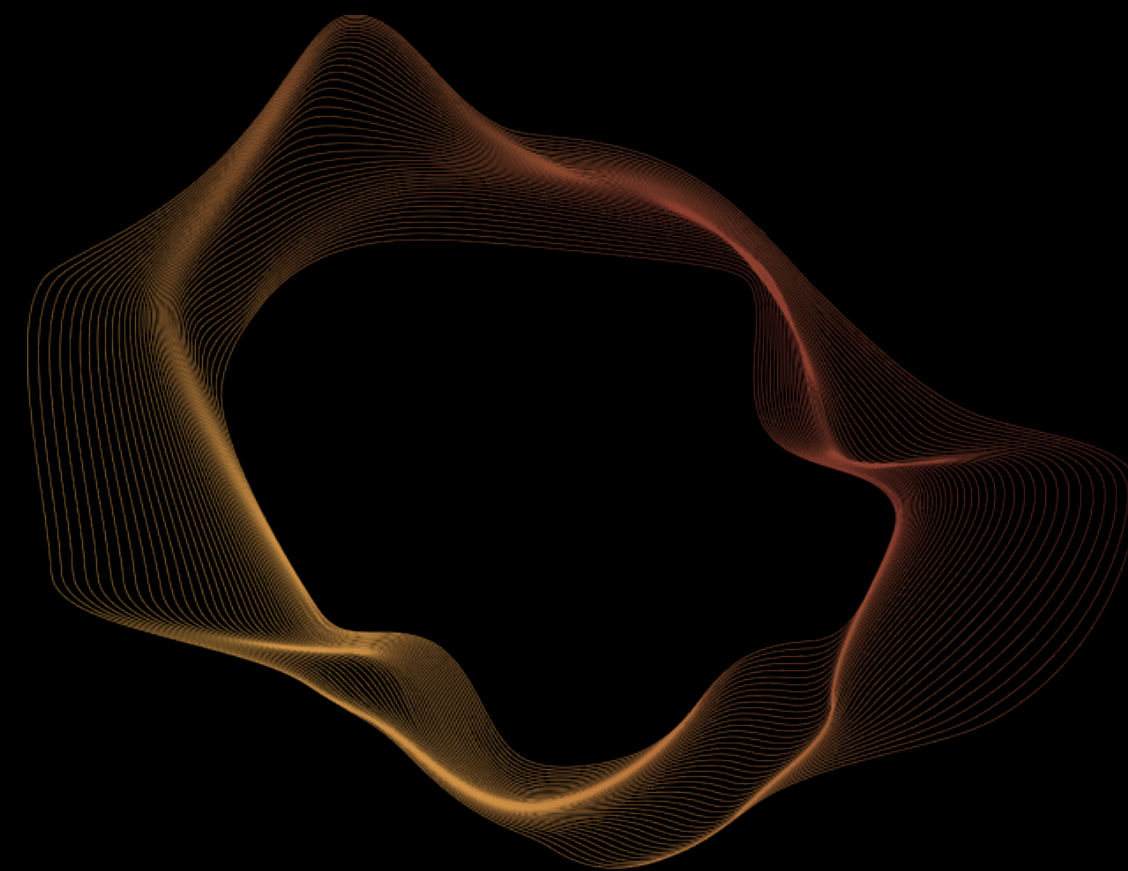
Challenges

- Demand of highly secure software applications and a robust IT infrastructure to handle sensitive financial information

- Meeting compliance requirements for handling classified information

- Lack of secure practices in development and operations

- A viable security program with complete visibility into their cyber risk and security posture
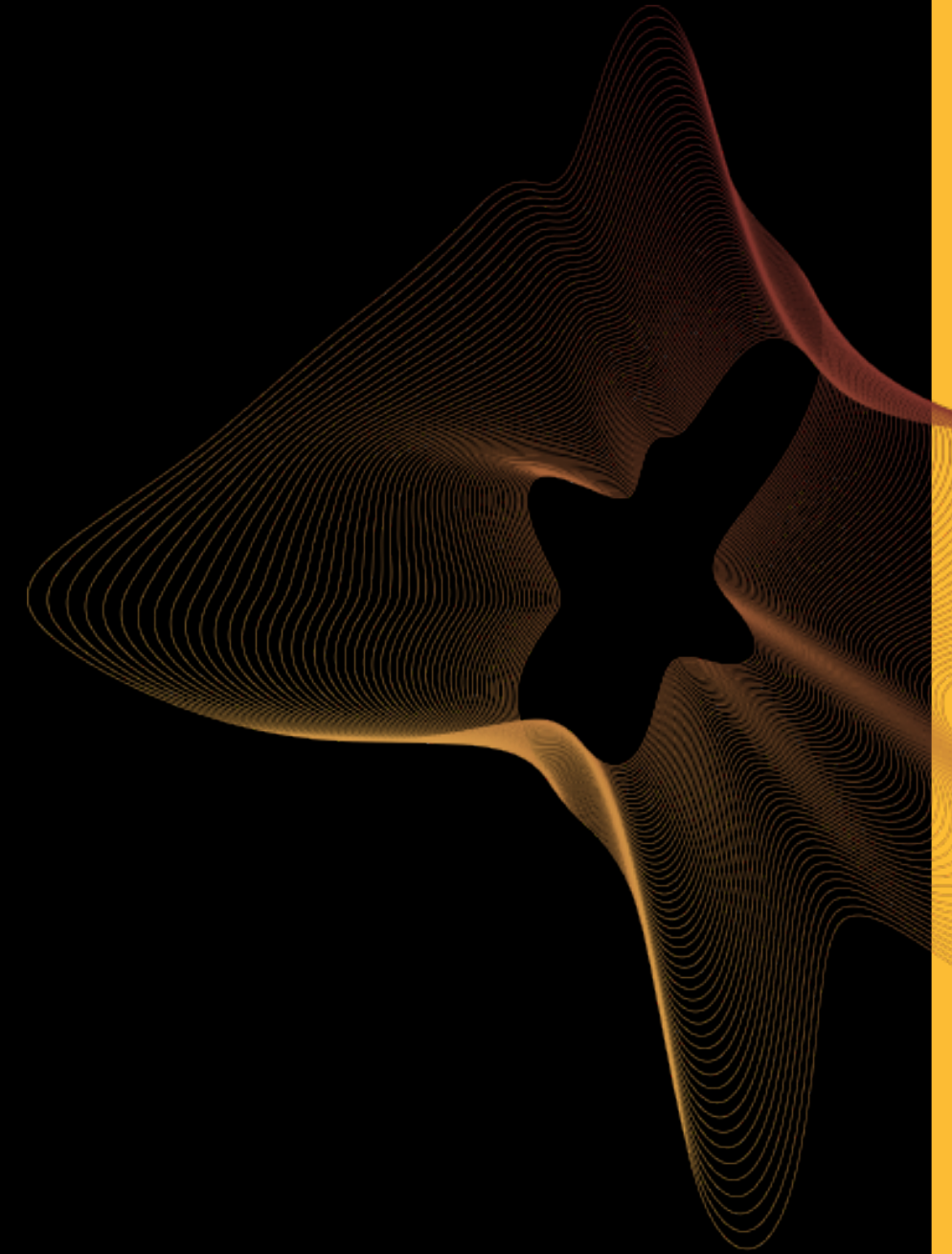
Our Solutions
Security Advisory

- Gap Analysis to understand the security gaps

- Creating a comprehensive security plan to protect assets, data and reputation

- Helping Onemoney management to identify and invest available information security budgets judiciously on the most important security activities

- Deploying the right team of seasoned, certified security leaders, analysts and testers to set and execute security program

- Introducing best of breed security products to take care of all aspects of people, process and technology

Reducing the attack surface

Sumeru focused on improving the security posture of Onemoney.
Here are the steps taken by Sumeru...

- Penetration tests to identify application and network vulnerabilities

- Enabling Application Security Verification Standard (ASVS) controls to help organizations develop and maintain secure applications

- Code Review to detect, validate and remediate vulnerabilities directly with development team

- Reported issues with recommendations

- Oriented developers on Secure SDLC process to help them avoid pitfalls in further development process

- Implemented security controls around their critical IT infrastructures to remain complied with different security standards

Business impact

We helped Onemoney to introduce Security Awareness and Assurance
into their IT infrastructure, app development and business operartion.
Our efforts brought some significant improvements in their security posture.

- Noticeable decline in product, web application and network vulnerabilities

- Helped the organization to successfully meet the business/regulatory requirement by developing secure applications

- Timely execution of vulnerability remediation as per deadlines

- Scale the development efforts by performing security testing early in the development lifecycle

- Enable developers to spot security issues early and fast

- Reduce development time and business resource

SUMERU

SUMERU

Sumeru Cyber Security
Everything, from soup to nuts.

Identify

- Phishing Simulation
- Cloud Security
- Application Security
- Infrastructure Security
- Security Architecture & Configuration Review

Protect

- Security Awareness Training
- DevSecOps
- CASB
- Web Application Firewall
- MFA
- Third Party Vendor Assessment
- Data in Rest & Transit Security

Detect

- SOC 1, SOC 2
- Threat Hunting
- Attack Surface Monitoring
- Office365 Security Centre
- Azure Sentinel
- AWS Guard Duty
- SIEM,Threat Intel & UEBA
- Endpoint detection and response

Respond & Recover

- SOAR
- Digital Forensic
- Incident Response
- Backup and data recovery

Comply

- ISO 27001 & ISO 9001
- GDPR/PIMS
- SOC 2 Type 1 & 2
- RBI Guidelines Audit for banks

SUMERU

*"They have been **top class professionals** when it comes to planning our security needs.." - **ADP India***

*"Top class **professionalism** has been **consistently shown** by Sumeru in planning, execution and report delivery of Information Security assignments.**" - Shangri-la***

*"Sumeru is our **Information security partner**! Their ability to align service delivery to business goals has directly helped us **add value to our customers.** It is this approach that makes Sumeru different from other vendors." - **TATA Power***

Let's explore possibilities.

Send us a friendly email with a little about what you're working on, and we'll be happy to help you figure out whether it's a good fit.

chidha@sumerusolutions.com

And meanwhile, check us out online : inservice.sumeru.com