White Paper

Open Banking Security-**Risks and Solutions**

Contents

Published by
Trend Micro

Written by
Satish Vagadia, Trend Micro
Suresh Kanniappan, AWS

About Open Banking

Open banking is a financial services term that refers to the use of open Application Programming Interfaces (APIs) to provide secure access to financial data and services.

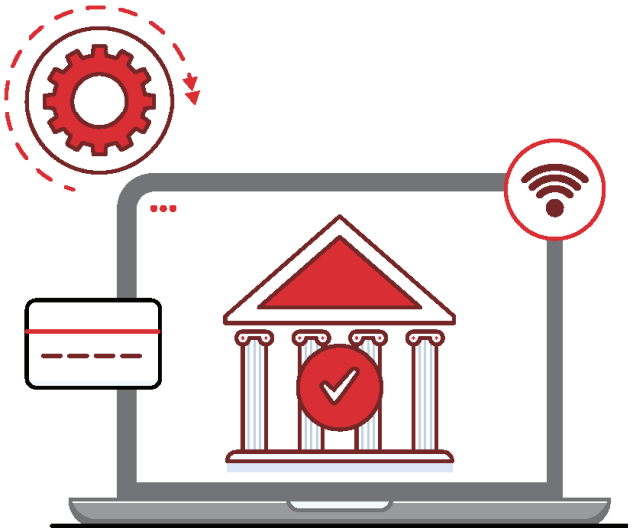
The main goal of open banking is to increase competition in the financial services sector by making it easier for third-party developers to create innovative financial products and services using data from banks and other financial institutions. This is done by allowing these third-party developers to access financial data and services through APIs, which are sets of rules and protocols that govern how different software systems interact with each other.

Open banking regulations and initiatives typically focus on giving consumers greater control over their financial data and providing them with more choice and convenience when it comes to managing their finances. The specific implementation can vary depending on the country or region, but they tend to require banks to make certain financial data available to authorized third-party providers (TPPs) under secure conditions.

Recent key changes in Indian Banking System

With Banking-as-a-Service gaining significance, most prominent institutions and upcoming ones are setting full-scale units for BaaS and digital banking with clear revenue and customer engagement targets. There is distinct movement on hiring as well as training the resources for this service. Open Banking is providing newer opportunities to develop business models like B2B2C or B2B2B or B+B2C and other combinations instead of straight business models like B2C or B2B.

- Regulatory movements
- Launch of Account Aggregator Platform
- Deepening of API banking platforms by banks
- Transformation of multiple payment / lending fintechs into neobanks
- Big Techs (like Google, Flipkart, Amazon, WhatsApp)
- Embedded Finance
- Launch of multiple neobanks
- Entry of international neobanks
- Enlarged funding rounds
- Talent & Organization Readiness



Increased Attack Surface Risks

Open banking, like any modern technology or system, introduces new risks and attack vectors for malicious actors to exploit and hence increases the risk of attack surface in a few ways:

1. Increased number of access points:

With open banking, Third-Party Providers (TPPs) are given access to financial data through APIs.
This creates additional access points that need to be secured and increases the likelihood that an attacker will find a weakness in the system.

2. Greater complexity:

Open banking systems are typically more complex than traditional banking systems, with multiple entities involved, including banks, TPPs, and consumers. This increased complexity can make it more difficult to identify and mitigate risks.

3. Dependence on third-party providers:

Open banking systems rely on the security practices of TPPs, and if these practices are not up to par, it can create additional risks. For example, if a TPP is compromised, an attacker could gain access to the financial data of multiple customers through a single attack.

4. Data Security Incident:

By accessing the data from several institutions, a compromise in a single institution can lead to wide-scale data security incidents.

However, despite these security measures, it is important to note that it is not possible to eliminate all risks associated with open banking, and companies should be prepared to respond quickly and effectively in the event of a security incident.

There are several cyber security risks associated with open banking, including :

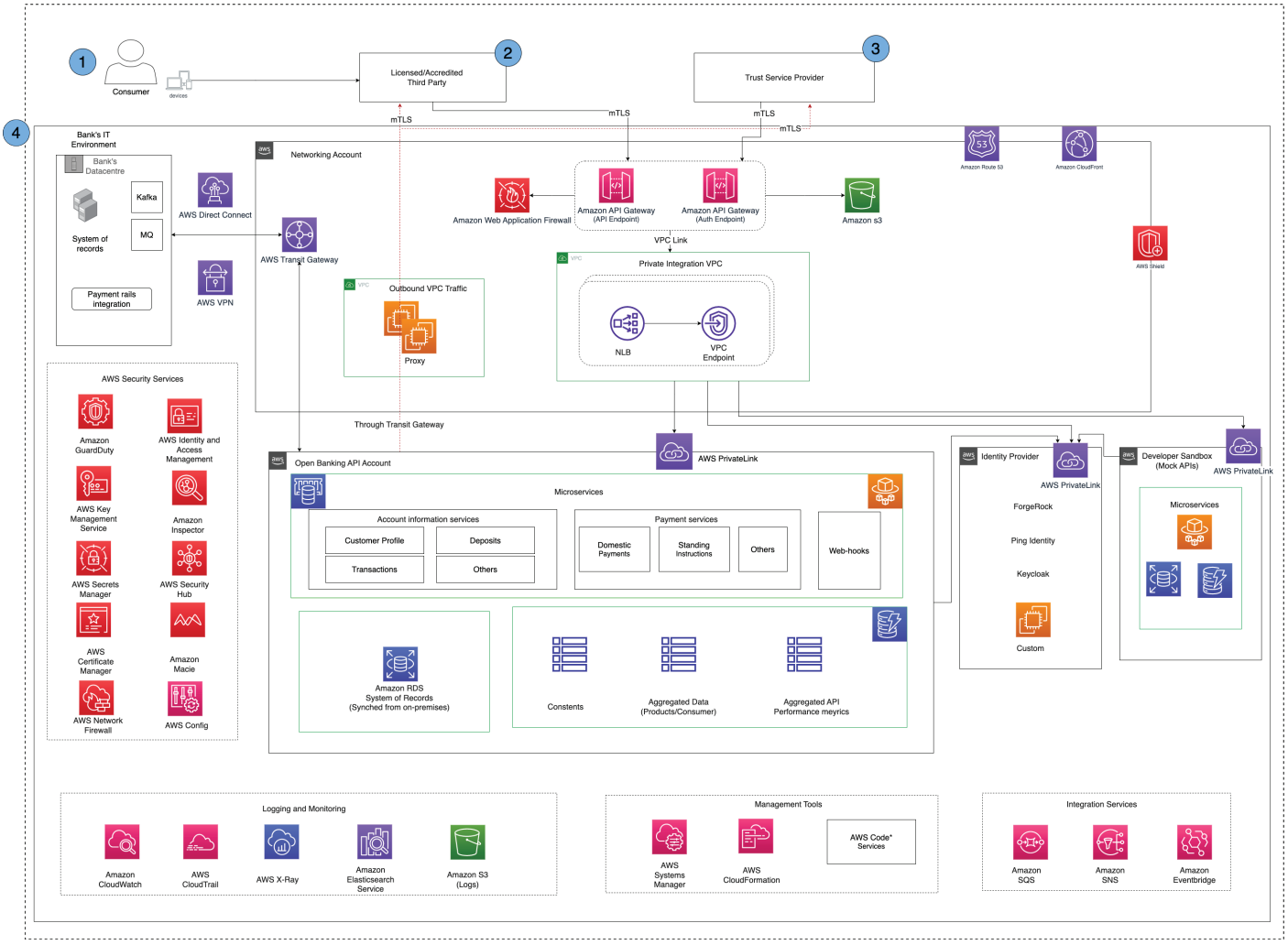
To mitigate these risks, regulatory bodies around the world are implementing strict security requirements for open banking systems, such as two-factor authentication, data encryption, and regular security audits. Additionally, companies that implement open banking are required to comply with regulations such as the EU's Revised Payment Service Directive (PSD2) and the UK's Open Banking Implementation Entity (OBIE).

Open Banking Reference Architecture on Amazon Web Services (AWS)

In Open Banking, banks use APIs to securely share their customer data with third-party developers and service providers – allowing automated and secure access to the functionality of their core banking platform. Banks are building open banking platforms in response to new regulations and customer demands. Banks that are building their open APIs choose AWS because of the scalability, cost effectiveness, and the services that AWS offers for analysing large volumes of new data.

Open Banking architectures supporting these use cases share the following characteristics:

- They use an OAuth 2.0 authorization standard.
- They have an API driven infrastructure and elastic and scalable environment.
- They provide instant or near-instant access to customer account data.
- They have tamper-resistant logging and audit capabilities.



Open Banking on AWS Reference Architecture

1. A consumer accesses the licensed or accredited third party application - and provides consent to the third party to access consumer data or make a payment submission request.

2. Third parties in Open Banking can be defined as authorized institutions that provide value-added services on top of the consumer's regular banking needs, such as accounts information (balance check, recent transactions, statements) and payments (payment to merchants, people and registered payees). This approach enables use cases such as spend analysis, credit decisioning, payments for ecommerce transactions, and more.

3. A Trust Service Provider (TSP) is a trusted entity authorized by a supervisory government body to verify the authenticity of banks and third parties, and issue digital certificates to third parties.

4. A bank's IT environment comprised of its AWS environment and data centers.

a. AWS security services help enhance security posture. For example, Amazon GuardDuty monitors for malicious activity and unauthorized behavior; AWS Security Hub provides a comprehensive view of security alerts and security posture across AWS accounts.

b. Amazon API Gateway provides the API management layer that exposes open banking APIs and Authorization APIs. AWS WAF (Web Application Firewall) integrates with the API Gateway for web protection. Amazon Simple Storage Service (Amazon S3) serves as a trust store, where public certificates of clients are stored for validating requests by API Gateway. Additionally, banks perform checks against a TSP to validate the authenticity and status of third parties.

c. Identity provider (IdP) for OAuth 2.0 implementation resides in separate AWS account so that other workloads in the bank can consume it securely. Customers can choose from AWS partners that provide IdP functionality or build a custom IdP.

d. Logs from all services are collected in Amazon S3 then analyzed and monitored by Amazon Elasticsearch Service

Strengthening India's Financial Ecosystem: Exploring the RBI Cybersecurity Framework and DPSC Directives

The RBI Cybersecurity Framework and DPSC directives form a comprehensive framework for boosting cybersecurity and protecting end user data in the banking sector. Adherence to these guidelines is essential in the context of open banking. By prioritizing these directives, it ensures the resilience and security of financial systems. These DPSC directives help regulated entities reap the benefits of open banking without compromising on data privacy and security and hence contributing to a robust and trustworthy banking and financial ecosystem.

Reserve Bank of India (RBI) Cyber Security Framework Mapping & Digital Payments Security Controls (DPSC) mapping

Major Directives

- Governance and Security Risk Management
- Generic Security Controls
- App Sec Life Cycle
- Fraud Risk
- Customer Protection, Awareness and Grievance Redressal
- Internet Banking, Mobile Banking and Card payments Security

Applicable to the Regulated Entities except Regional Rural Banks

RESERVE BANK OF INDIA

Scheduled Commercial Banks

- Public Sector Banks
- Private Sector Banks
- Foreign Banks

Small Finance Banks

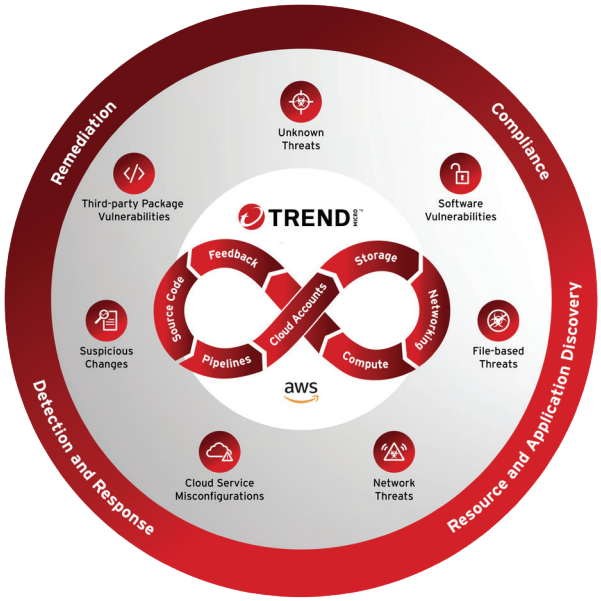
- Ujjvan SFB
- Utkarsh SFB
- Suryoday SFB

Payment Banks

- India Post
- PayTM
- Jio
- Airtel
- NSDL
- FINO

Trend Cloud One™ – Helping Adherence to compliance and Securing Open Banking on AWS

The Trend Cloud One™ platform provides comprehensive solutions for securing the complete application security lifecycle, including integration with various systems such as mobile payments, APIs, server workloads and container workloads. With the inclusion of behaviors analysis and detection capabilities, the platform leverages telemetry data to offer valuable insights through Trend Vision One™.



Applicable to the Regulated Entities except Regional Rural Banks

Application Security Life Cycle

- Vision One – Cloud Security Artifact Scanning
- Vision One – Container Security
- Vision One – Open Source Security
- Professional & Advisory Services
- Vision One – Workload Security

Mobile Payments and App Sec Control

- Vision One – Workload Security
- Vision One – Cloud Security Artifact Scanning
- Vision One – Container Security

Card Payments Security

- Vision One – Container Security
- Vision One – Cloud Security Artifact Scanning
- Vision One – Workload Security
- Apex One
- Vision One

Internet Banking Security Control

- Vision One – Cloud Security Artifact Scanning
- Vision One – Container Security
- Vision One – Workload Security

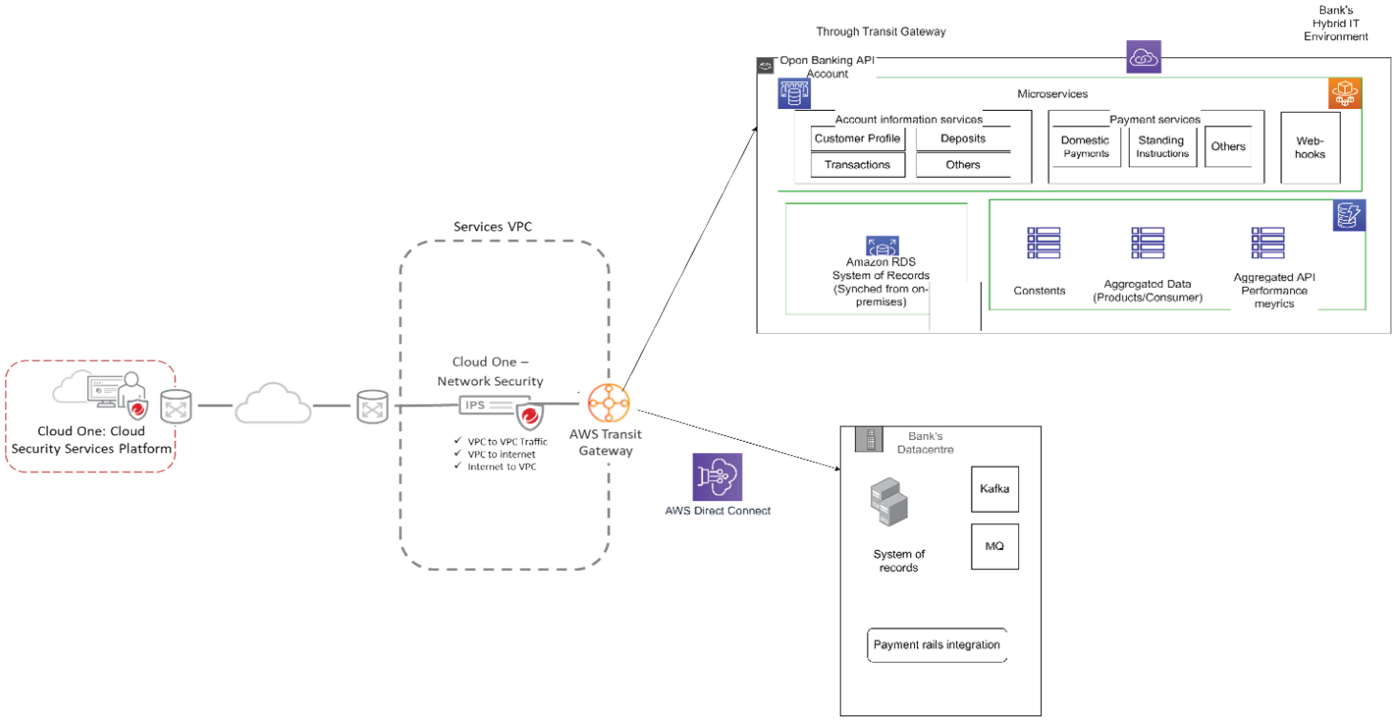
PCI DSS - 2020 Attested Solutions (Trend Cloud One™ – Container Image Security, Workload Security, Network Security)

GOALS	REQUIREMENTS
Build and Maintain Secure Networks and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Card Holder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information security Policy	12. Maintain a policy that addresses information security for all personnel

Trend Cloud One™ and Open Banking on AWS

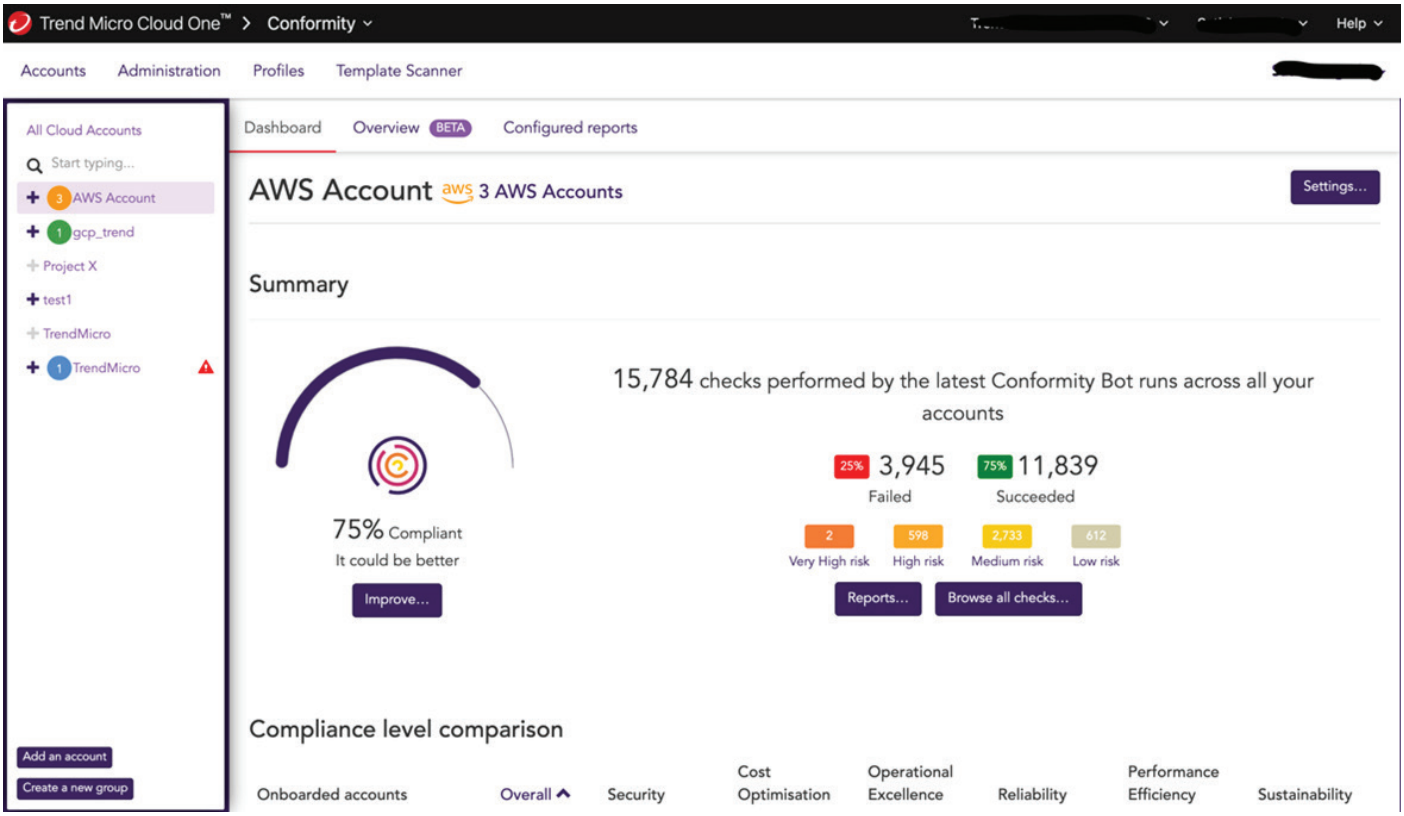
Regulated Entities should run automated Vulnerability Assessment (VA) scanning tools to scan all systems on the network

Solution is to use Trend Cloud One™ – Network Security with AWS Transit Gateway in as shown in diagram below. AWS Transit Gateway serves as the central hub on AWS to manage interconnectivity between workloads running in different AWS accounts. It shares the AWS Direct Connect and VPN connection with other workloads in the bank.



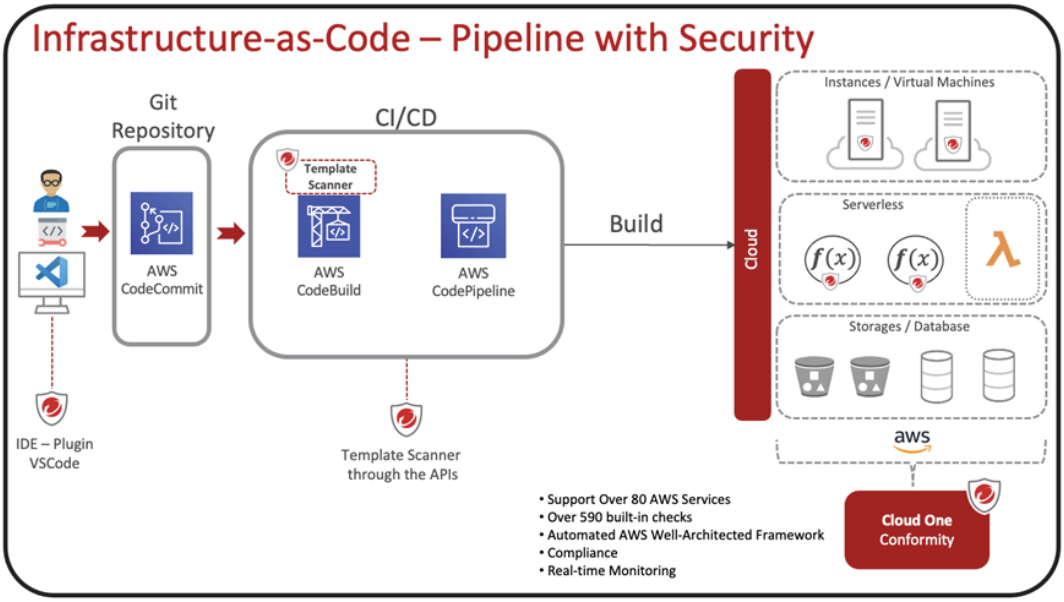
Regulated Entities shall follow a 'secure by design' approach

Our Cloud Security Posture Management technology - (Conformity™) provides comprehensive visibility of AWS accounts, and aligns with the DevSecOps approach of improving security and compliance posture through auto-remediation. It can also help organizations gain a coherent picture of security and compliance risks across multi-cloud environments.



Trend Cloud One™ – Conformity provides a number of tools to help organizations quickly assess their infrastructure's compliance posture against various compliance standards and frameworks, additionally there are templates available in AWS for aligning your environment to security controls. In AWS, by constraining the design on Identity and Access Management (IAM), AWS Key Management Service (KMS) and AWS CloudTrail, more granular control can be achieved.

Conformity offers reports for the following standards and frameworks. Each standard or framework is made up of controls that specify security and governance requirements. Conformity rules are mapped to these controls and the resulting checks can be filtered to display only the rules relevant to a particular standard or framework.



Regulated Entities shall implement multi-tier application architecture, sandbox and containerization approaches

Securing Containerized Environment – Complete Lifecyle by Trend Cloud One™ – Container Image Security on Amazon Elastic Kubernetes Service (EKS) and other container managed services ensures protection and enforcement are applied to container builds, deployments, and runtime workflows by integrating with build pipeline image and container registry scanning. The events are collected at central place for easy monitoring. This enables organizational governance and enforcement across container clusters in multi-cloud environments.

Regulated Entities shall adopt and incorporate a threat modelling approach

Trend Micro can help build Threat Modelling approach using its Cloud One products portfolio and AWS security services. We can build a honeypot network that can detect threats to the applications (web and Mobile) and provide mitigation capabilities from Cloud One products.

By having increased observability of multiple integrations in Trend Cloud One™ together with AWS threat modelling of the multiple features that make up a given AWS service to increase security observability posture. The cloud environment will be audited against hundreds of AWS best practices including SOC2, ISO 27001, NIST, CIS, GDPR, PCI DSS, HIPAA amongst others incorporated in Trend Vision One™ - Cloud Security to make your cloud infrastructure more reliable, secure and cost efficient.

Additionally the advanced XDR Capabilities with early and precise threat detection, rapid response and advanced threat correlation, Trend Vision One™ together with Amazon GuardDuty (Intelligent Threat Detection) & Amazon Inspector (Vulnerability Management Service) provides complete solution to security operations centre (SOC) analysts by quickly identifying critical threats to limit risk and damage to the organisation. In a recent Forrester Wave XDR evaluation, Trend Vision One™ was named a Leader and scored the highest ranking in the current offering category, further demonstrating our industry leadership position.

Next Steps

AWS and Trend Micro offerings on security controls help customers to secure the banking application and thereby meeting the compliance like PCI-DSS and regulatory guidelines such as Reserve Bank of India (RBI) Cyber Security Framework Mapping & Digital Payments Security Controls (DPSC) mapping.

The security controls help to secure the following critical banking applications:

- Core Banking Software
- Lead Management System (LMS)
- Loan Origination System (LOS)
- Loan Management System
- Customer Relationship Management (CRM)
- Payment & Credit Card Systems
- Collection Systems
- Mobile & Internet Banking

The customer shall reach out to AWS team via https://aws.amazon.com/contact-us/ & Trend Micro via https://www.trendmicro.com/en_in/business/get-info-form.html to have a deeper conversation on this front.