

SECURING THE DIGITAL BANKING ERA



Table of contents

Cybersecurity imperatives in digital banking..... 02

NexGen banking core functions..... 03

Cyber threat landscape of hyperconnected banking..... 05

Reimagining NexGen security in banking..... 07

 Advanced network security..... 07

 Cloud, content and identity security..... 09

 SOC for banking resilience..... 11

 Governance, risk and compliance management..... 13

 Customer channel and endpoint security..... 15

Success stories..... 17

Strategic cybersecurity advantage for banks..... 19

Contributors..... 20

Cybersecurity imperatives in digital banking

The banking sector is rapidly shifting to digital-first models, driven by customer demands, fintech disruption, and regulatory change. This transformation expands the value chain but also broadens the cyber risk surface at every layer.

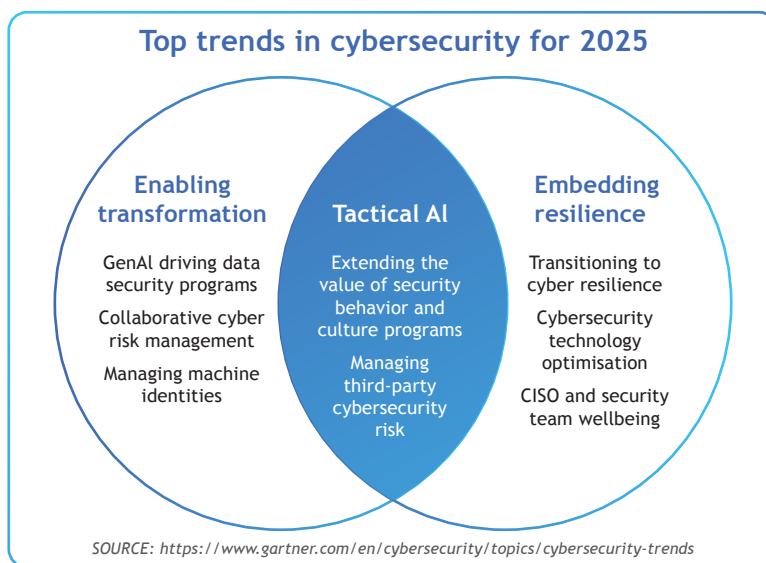
Banks have shifted from monolithic IT to dynamic digital ecosystems powered by cloud-native platforms, microservices, open APIs, embedded finance, and real-time transactions. Customer interactions now span mobile apps, internet banking, and smart ATMs.

Fifty-eight percent of boards would like to see their organisation take more technology risk, despite 81% viewing cybersecurity as a business risk.

SOURCE: <https://www.gartner.com/en/articles/2025-trends-for-security-and-risk-leaders>

Digital banking is no longer just “banking on a screen” — it has evolved into a partner-driven ecosystem where **banks, fintechs, SaaS providers, and lifestyle platforms** converge to deliver seamless financial experiences. Banks are no longer standalone providers but **orchestrators, embedding payments, credit, investments, and insurance** into everyday interactions — from checkout to mobile apps.

This transformation boosts agility and customer experience but also widens the attack surface. Cybercriminals now target cloud interfaces, partner APIs, payment systems, and endpoints, rendering the old “castle-and-moat” model obsolete. Banks must defend a porous, dynamic ecosystem with adaptive, intelligence-driven security. At the same time, regulators demand proof of resilience, not just controls. Compliance has become continuous, with global mandates like the EU’s DORA, Basel’s cyber guidelines, and the RBI’s directives setting new expectations for resilience, monitoring, and third-party governance.



Cybersecurity has become a strategic imperative — embedded across the entire banking ecosystem, shaping **resilience, trust, and long-term growth**.

To secure their digital future, banks must adopt a **holistic cybersecurity approach** that aligns with the Smart Banking Ecosystem:



Core technology

infrastructure, banks must secure cloud infrastructure, ensure third-party risk governance, and meet evolving regulatory requirements.



Operations and compliance

must protect core banking systems, transaction engines, and sensitive customer data from sophisticated attacks and internal threats.



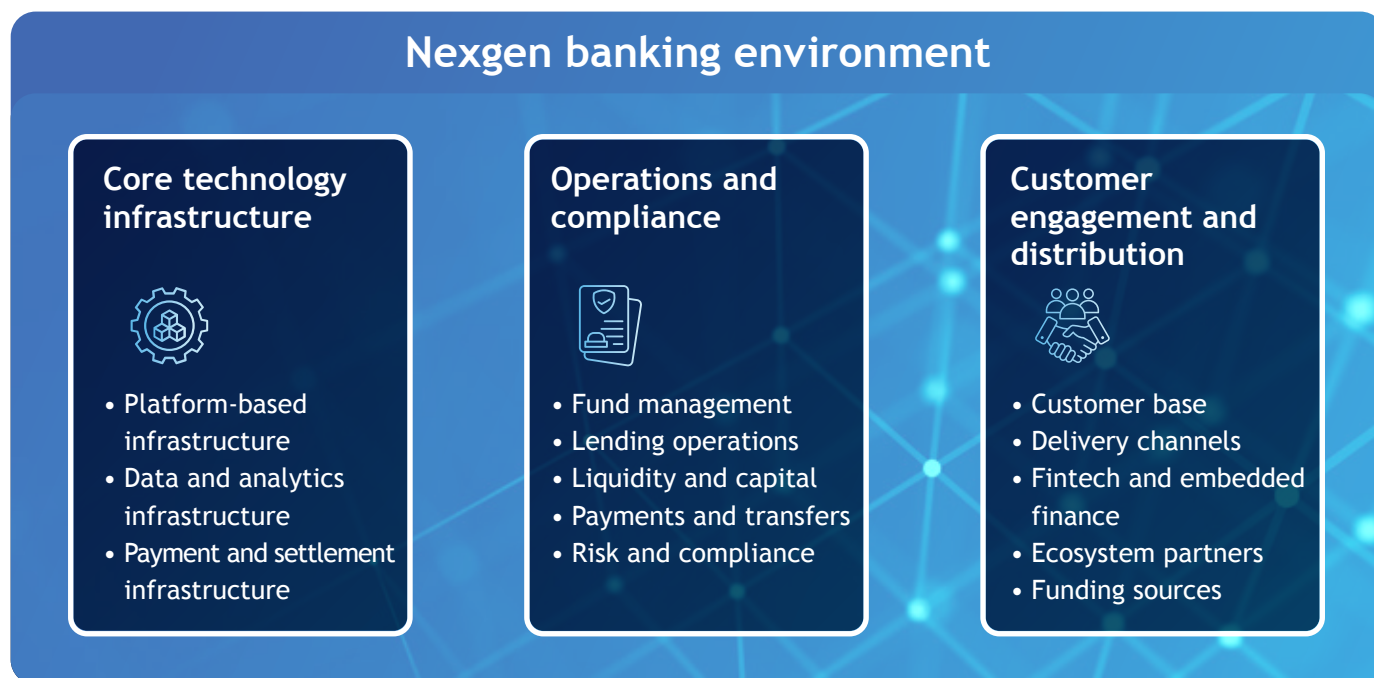
Customer engagement and

distribution- banks must harden digital interfaces, enforce strong identity controls, and safeguard trust at every customer and partner touchpoint across the ecosystem.

NexGen banking core functions

The emergent banking runs on an inter-connected value chain — from the underlying engines of infrastructure enablement, through the precision of operational execution, to the frontline of customer engagement.

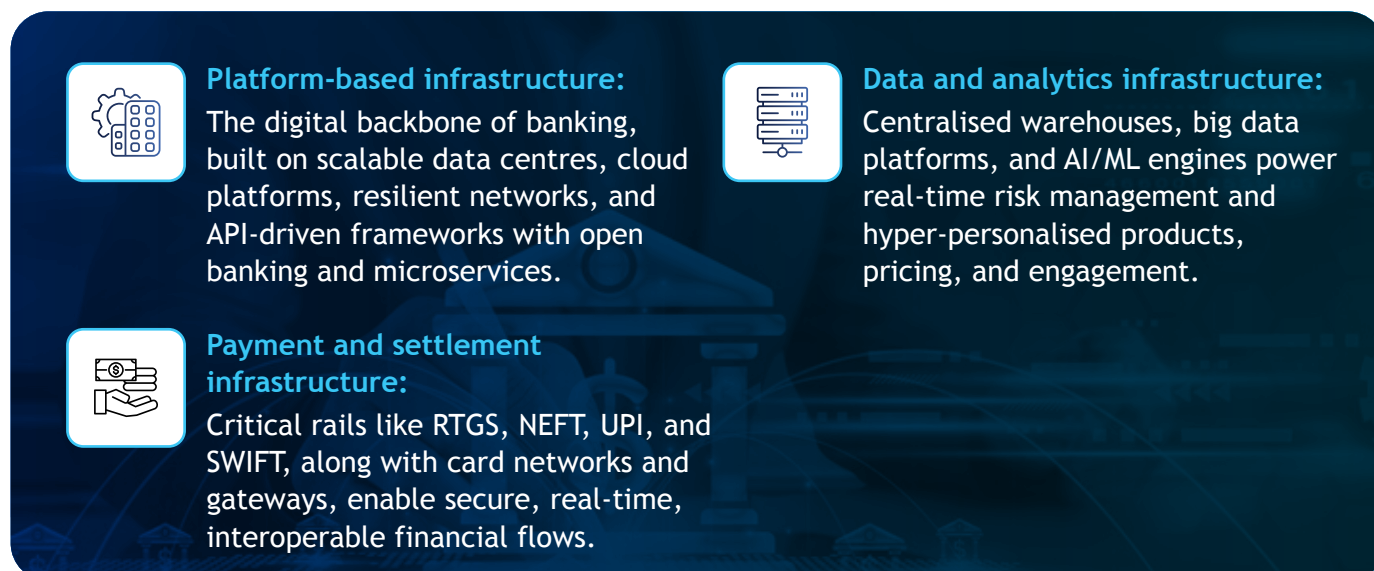
Understanding this structure is vital for banks to drive digital performance, ensure compliance, and gain competitive advantage.



Core technology infrastructure

This layer consists of critical enablers that provide the digital platform, data and payment infrastructure for banking operations.

Key functions:



Operations and compliance

At the heart of the value chain lies the core banking layer, where banks manage funds, create financial products, perform credit operations, and ensures regulatory compliance.

Key functions:



Fund management:

Allocating customer deposits, managing liquidity and interest risk.



Lending operations:

Retail, SME, and corporate loan origination and servicing.



Liquidity and capital:

Central bank funding, capital markets, inter-banking systems, securitisation.



Payments and transfers:

Interbank payments (e.g., SWIFT, UPI, RTGS), clearing, and settlement.



Risk and compliance:

AML/KYC monitoring, audit reporting, regulatory adherence.

Customer engagement and distribution

This layer represents the distribution points and external interactions through which financial services are delivered, consumed, or co-created.

Key channels:



Customer base:

Retail, SME, corporate, HNWIs, and public sector clients.



Delivery channels:

Branches, ATMs, mobile/internet banking, call centres, RM networks.



Fintech and embedded finance:

Digital wallets, BNPL platforms, open banking APIs.



Ecosystem partners:

Lifestyle platforms, Auto dealers, real estate brokers, e-commerce, insurance providers and continuously expanding web of value creating partners.



Funding sources:

Customer deposits, investments, and wholesale funding.

Cyber threat landscape of hyperconnected banking

In the hyperconnected ecosystem, universal connectivity and pervasive infrastructure drive embedded finance and AI-enabled personalisation for competitive advantage. Cyber threats now target every layer—APIs, third-party integrations, mobile apps, and cloud workloads—pushing banks toward Zero Trust, AI-enabled, integrated security. Proactive detection, real-time monitoring, and end-to-end data protection are essential to safeguard trust, ensure compliance, and maintain resilience.

Cybersecurity challenges in core technology infrastructure

Digital infrastructure has become both a catalyst for innovation and a source of systemic risk. This interconnected ecosystem calls for a resilient, end-to-end cybersecurity posture—one that evolves with tightening regulations and an accelerating threat landscape.

According to Gartner, by 2026, third party cyber risk program performance will become a standing agenda item for 50% of board committees globally.

SOURCE: <https://www.gartner.com/en/newsroom/press-releases/2023-12-13-gartner-survey-finds-45-percent-of-organizations-experienced-third-party-related-business-interruptions-during-the-past-two-years>

Key challenges:



Platform and network security threats:

Platform security: Multi-cloud infrastructure gaps, expanding API-based ecosystems widen the attack surface, while DDoS attacks keep service availability at constant risk.

Network security: North-South and East-West traffic breaches can significantly disrupt banking operations. This will include mobile banking, UPI, SWIFT, card gateways, while lateral movement can access core banking systems, payment rails, or customer data. Traditional perimeter defences are not adequate for preventing these types of network security challenges.



Data and analytics infrastructure security threats:

Banks' vast data warehouses, big data platforms, and AI/ML engines face risks from data breaches, insider threats, and insecure APIs. Sensitive financial and customer data is a prime target for theft, manipulation, and misuse.

Weak governance, inadequate encryption, and fragmented access controls amplify risks—turning data infrastructure from a strategic asset into a critical attack surface.



Payment and settlement infrastructure security threats:

The critical rails of banking—national payment systems, clearinghouses, and global card networks—are high-value targets for cyberattacks. From fraud, phishing, and malware on real-time channels (UPI, RTGS, SWIFT) to manipulation of settlement systems and large-scale card breaches, any compromise can disrupt the flow of banking transactions.

Operations and compliance security threats

Core Banking operations centrality and critical function make it a high-value target for cyber adversaries, including advanced persistent threats (APTs) and financially motivated attackers.

In 2024, application-layer DDoS attacks targeting APIs in the financial sector surged by 58% year-over-year, intensifying pressure on operational resilience and compliance efforts.

SOURCE: <https://www.akamai.com/site/en/documents/white-paper/2025/ddos-attacks-acrosst-the-financial-sector.pdf>

Key challenges:



Fund management and lending operations disruption:

Fund allocation, deposit management, and lending systems are prime targets for unauthorised access, liquidity disruption, and manipulation of retail, SME, and corporate loan platforms—directly endangering financial stability and customer trust.



Payments, liquidity and capital market threats:

Critical systems for liquidity, capital markets, and interbank flows depend on RTGS, UPI, SWIFT, and clearing networks. Cyberattacks here can derail settlements, stall securitisation, and spark systemic risks across the financial ecosystem.



Risk and compliance threats:

AML/KYC monitoring, audits, and regulatory reporting hinge on accurate data. Breaches, insider threats, or malware can corrupt records, weaken detection, and expose banks to penalties and reputational damage.

Customer-facing channels vulnerabilities

As digital banking expands into mobile, online, ATM, and smart devices customer-facing platforms have become the prime targets. Security gaps leave them exposed, making protection vital for data, trust, and compliance.

In the second quarter of 2025, 43.6% of all application-layer DDoS attacks targeted financial services firms, capturing the largest share among all sectors. These attacks specifically aim at web applications—such as online banking portals and payment interfaces—that directly interact with customers, making them particularly disruptive to service availability.

SOURCE: <https://www.itpro.com/security/cyber-attacks/application-layer-ddos-attacks-are-skyrocketing-heres-why>

Key challenges:



Channel-based exploits:

APIs, mobile apps, and internet banking portals are prime hunting grounds for DDoS attacks, API abuse, and session hijacking.



Weak authentication:

Flawed MFA setups and static passwords open the door for attackers, putting customers and their data at risk.



IoT and ATM security gaps:

Smart ATMs, kiosks, and PoS terminals demand hardened firmware and encrypted links—or they become easy entry points.



Customer confidence and brand risk:

One breach in downstream systems can shatter trust overnight, bringing legal fallout and reputational damage.

Reimagining NexGen security in banking

Banks are increasingly adopting 360° AI-powered, zero-trust cybersecurity frameworks to secure modern digital operations.

Advanced network security

Enterprises are moving toward cloud-delivered, Zero Trust-based network security to safeguard operations across distributed environments. Built to secure today's cloud-first, edge-driven ecosystems, our solutions provide multi-layered defence against evolving threats—whether on-premise, across clouds, or at the far edge.

Key capabilities



Massive DDoS defence:

Enterprises are increasingly deploying platforms with high ingestion capacity to defend against the largest volumetric cyberattacks and ensure continuity of operations.



Zero Trust framework:

Every user, device, and application is verified continuously, minimising insider risks and preventing lateral movement.



Multi-Layered protection:

Security extends from the core to the edge, covering networks, applications, and endpoints with unified visibility.



Cloud-Delivered agility:

Security services are deployed closer to users and workloads, enabling consistent protection across geographies and hybrid environments.

AI's role in network security for banking



AI-Powered channel protection

- **Use Case:** Safeguard mobile apps, internet banking, and APIs against abnormal traffic, DDoS, and session hijacking.
- **AI Enablement:** ML models analyse real-time traffic patterns to distinguish legitimate user activity from botnets or attack traffic, reducing false positives.



AI-Driven payment infrastructure defence

- **Use Case:** Protect RTGS, UPI, NEFT, and SWIFT from sophisticated attacks that can disrupt settlements.
- **AI Enablement:** AI correlates NetFlow records at massive scale to detect anomalies in transaction flows and flag early signs of coordinated attacks.



AI in open banking security

- **Use Case:** Secure APIs and third-party fintech integrations against data leakage and unauthorised access.
- **AI Enablement:** AI engines monitor API calls for unusual frequency, data access patterns, or credential misuse, enabling faster threat isolation.



AI-Enabled threat detection and fraud monitoring

- **Use Case:** Identify insider threats, fraud attempts, and account takeovers across customer and back-office systems.
- **AI Enablement:** Machine learning continuously learns from past incidents, spotting subtle deviations in user behaviour and preventing advanced persistent threats.



AI-Supported zero trust for hybrid workforces

- **Use Case:** Enforce least-privilege, context-aware access for employees, contractors, and branches.
- **AI Enablement:** AI evaluates device posture, location, and behavioural signals in real time to allow or deny access dynamically.



AI in compliance and audit readiness

- **Use Case:** Ensure adherence to frameworks like Basel III, PCI DSS, GDPR, and DPDP.
- **AI Enablement:** Automated AI-driven logs, anomaly reports, and compliance analytics reduce manual effort and improve audit readiness.

Business impact



Resilient services:
Always-on protection
at global scale.



Stronger trust:
Secures customer-facing
platforms and sensitive
data.



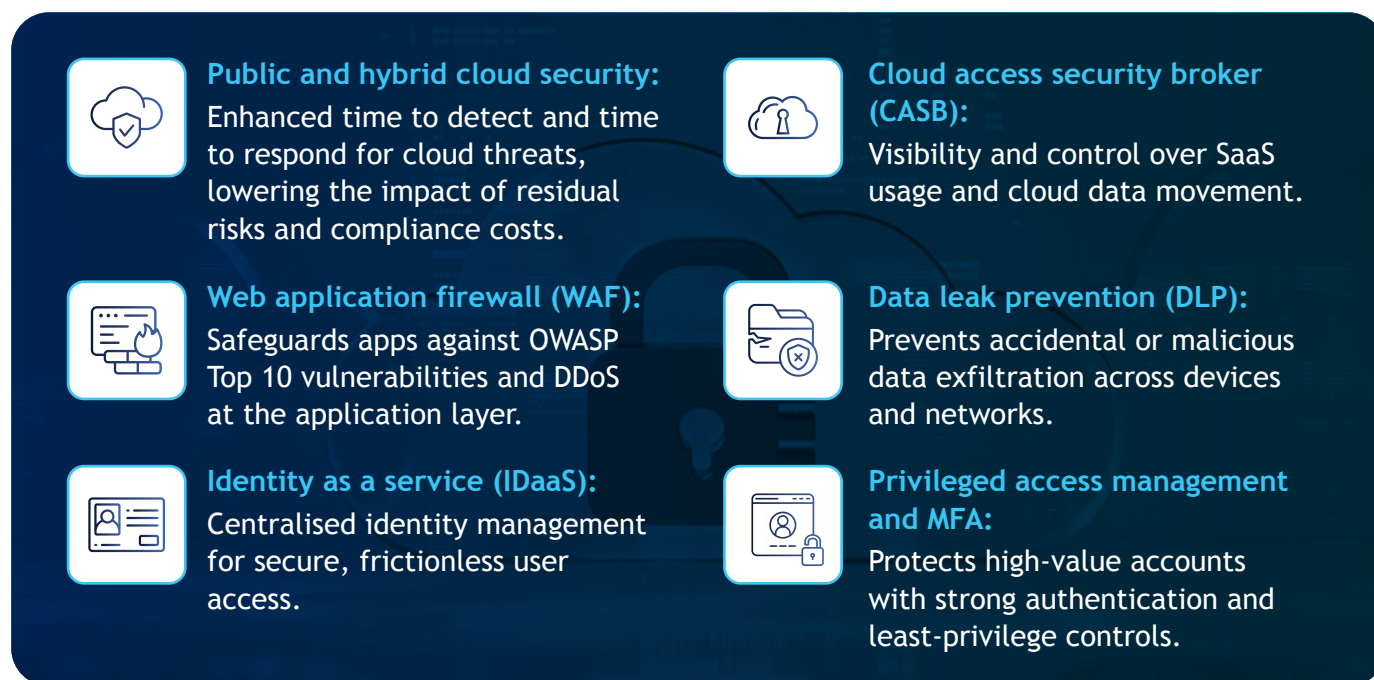
Future-Ready security:
AI-enabled intelligence
that evolves as fast as
threats.






Cloud, content and identity security

As cloud adoption and digital engagement accelerate, securing applications, content, and user identities is critical. Banks are adopting multi-layered cloud, content, and identity security frameworks to block application-layer threats, enforce granular access, and secure connectivity across hybrid and public cloud environments.

Key capabilities



AI's role in cloud, content and identity security for banking

- 
AI-Powered cloud security
 - Use Case:** Detect and mitigate misconfigurations, abnormal traffic, and advanced threats in public and hybrid cloud environments.
 - AI Enablement:** AI/ML models scan massive volumes of cloud logs and NetFlow data to identify unusual patterns, automate remediation, and reduce response time.
- 
AI-Driven content security
 - Use Case:** Protect web applications, portals, and content delivery from application-layer attacks (OWASP Top 10, DDoS, and bot traffic).
 - AI Enablement:** AI-based WAF continuously learns attack signatures and adapts to block new threats like zero-day exploits and automated bot campaigns.
- 
AI-Enabled identity and access control
 - Use Case:** Strengthen authentication and manage access rights across users, devices, and applications.
 - AI Enablement:** AI analyses login behaviours, device fingerprints, and geolocation to detect anomalies, enforce adaptive MFA, and prevent account takeovers.



AI-Supported Data Leak Prevention (DLP)

- **Use Case:** Prevent unauthorised or accidental data exfiltration across SaaS platforms, endpoints, and networks.
- **AI Enablement:** AI classifies sensitive data in motion and at rest, flags abnormal transfer attempts, and applies automated encryption or blocking policies.



AI in API and SaaS monitoring (CASB)

- **Use Case:** Control shadow IT, SaaS usage, and API interactions across the enterprise.
- **AI Enablement:** AI maps usage trends, detects suspicious API calls or excessive data access, and enforces granular access policies in real time.



AI for compliance and privacy assurance

- **Use Case:** Meet data protection and regulatory mandates (GDPR, DPDP) with proactive monitoring.
- **AI Enablement:** AI automates compliance reporting, identifies privacy risks early, and reduces manual audit workloads.

Business impact



Stronger compliance:

Simplifies adherence to GDPR, DPDP, and industry regulations.



Reduced risk:

Cuts the cost and impact of dealing with known threats.



Operational agility:

Protects hybrid workforces and digital ecosystems without compromising performance.



Customer confidence:

Secures cloud apps, content, and user data to preserve trust and brand reputation.

SOC for banking resilience

Always-On cyber defence

Managed and on-prem SOC deliver cloud-based, AI-enabled, 24x7x365 cyber defence. Built on Zero Trust and compliance-first principles, they provide end-to-end visibility across customer channels, payment systems, core infrastructure, and hybrid cloud environments.

Key features include:






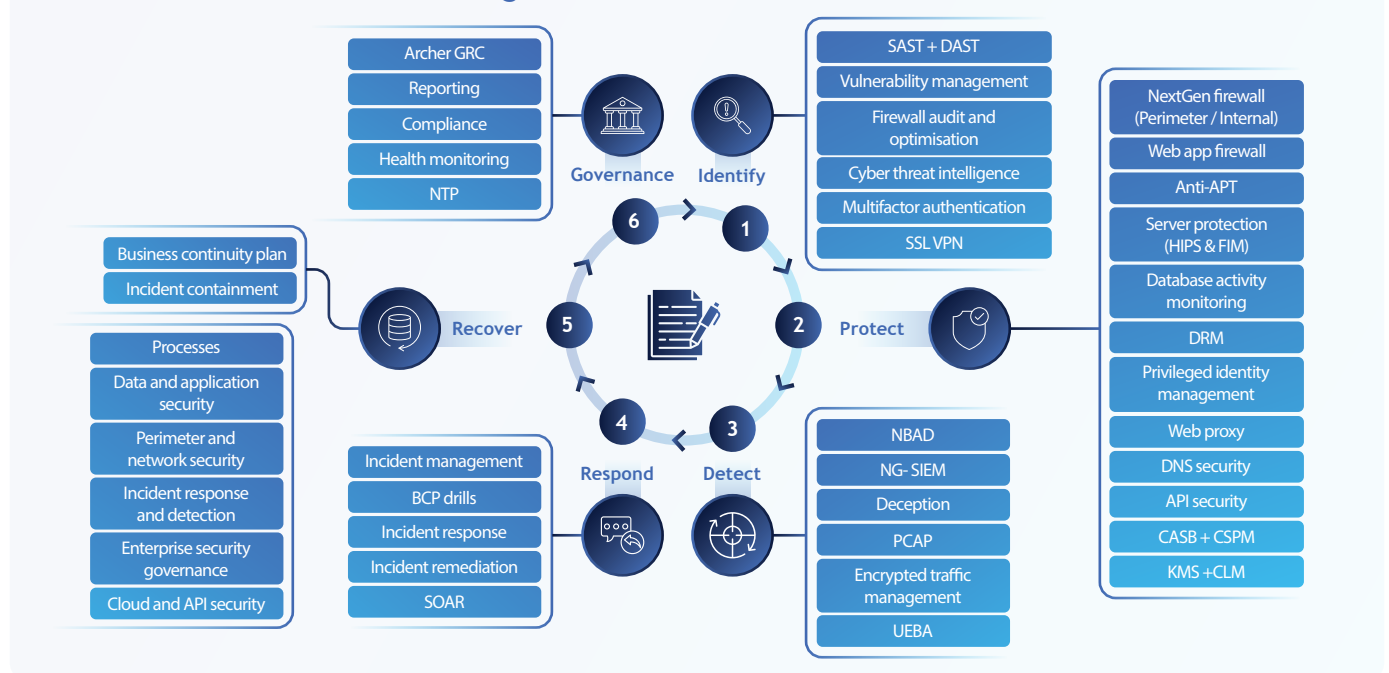
- 
AI-Driven threat detection:
 Correlates billions of logs, events, and flows using advanced machine learning models to identify anomalies missed by rule-based systems.
- 
Proactive threat hunting:
 AI-augmented analysts continuously search for Indicators of Compromise (IoCs) across banking networks and endpoints.
- 
Compliance-integrated monitoring:
 Pre-built dashboards and automated workflows aligned with Basel III, RBI, GDPR, PCI DSS, and DPDP requirements.
- 
Rapid incident response:
 AI-automated playbooks enable faster containment of phishing, ransomware, DDoS, and insider threats.
- 
Global intelligence backbone:
 Enriched with threat feeds and telemetry from global network footprint.

Figure: NIST framework for SOC



NIST Cybersecurity Framework (CSF) provides a structured approach to managing and reducing cybersecurity risks, and it can be effectively integrated into a Security Operations Center (SOC).

The framework's core functions - Identify, Protect, Detect, Respond, and Recover - align with the key activities of a SOC, helping to standardise and can power robust SOC operations.

AI at the core of SOC operations



AI-Driven threat detection

- **Use Case:** Identify sophisticated attacks (phishing, ransomware, insider misuse) across customer channels, payment systems, and core banking networks.
- **AI Enablement:** ML models correlate billions of logs and events to detect anomalies that signature or rule-based systems miss.



Proactive threat hunting

- **Use Case:** Uncover hidden Indicators of Compromise (IoCs) in ATM, mobile banking, and interbank transaction systems.
- **AI Enablement:** AI augments analysts with anomaly scoring and pattern recognition to flag emerging threats before they escalate.



Real-time incident response

- **Use Case:** Contain cyber incidents such as DDoS, malware outbreaks, or compromised accounts in seconds.
- **AI Enablement:** AI-powered orchestration automates playbooks (e.g., isolating endpoints, blocking malicious IPs) to accelerate containment.



Fraud and account takeover prevention

- **Use Case:** Detect unusual customer login patterns or payment anomalies that signal account compromise.
- **AI Enablement:** AI models analyse behavioural biometrics, geolocation, and device fingerprints to stop fraudulent access attempts.



Regulatory and compliance assurance

- **Use Case:** Ensure adherence to RBI, Basel III, PCI DSS, GDPR, and DPDP compliance requirements.
- **AI Enablement:** AI automates compliance checks, correlates audit logs, and generates real-time regulatory dashboards.



Operational efficiency

- **Use Case:** Reduce analyst fatigue and improve SOC efficiency.
- **AI Enablement:** AI filters noise, prioritises high-risk alerts, and continuously learns from past incidents to sharpen detection.

Business impact for banks



Continuous assurance:

24/7 protection for customer-facing channels, core infrastructure, and critical payment systems.



Regulatory confidence:

Streamlined compliance reporting and audit readiness across global and local mandates.



Reduced risk exposure:

Faster detection and response minimise financial, reputational, and regulatory impact.



Customer trust:

Secure, always-on services strengthen loyalty and brand resilience in an era of digital-first banking.

Governance, risk and compliance management

Reactive fixes and fragmented controls increase exposure and erode trust. Governance, Risk and Compliance (GRC) services take a holistic approach to assess maturity, close gaps, and ensure regulatory readiness against sophisticated attacks.

Key Capabilities



Cybersecurity Maturity Assessment (CMA):

Evaluate security posture across the NIST-aligned domains—Identify, Protect, Detect, Respond, and Recover.



Compliance audits and gap assessments:

Map current controls against global regulations and industry standards, ensuring compliance with mandates like GDPR, DPDP, PCI DSS, and ISO.



Data privacy and protection:

Identify risks in how sensitive data is handled and establish privacy-first processes.



Advanced testing services:

Vulnerability Assessment and Penetration Testing (VA-PT), web and mobile app security testing (DAST), phishing simulation, and red teaming to uncover real-world weaknesses.



Continuous monitoring:

Website defacement tracking and digital exposure monitoring to safeguard brand reputation.



OT security consulting:

Secure industrial and operational technology environments with tailored controls.

AI-Driven GRC intelligence for banking



AI-Enhanced cybersecurity maturity assessment

- **Use Case:** Continuously assess a bank's security posture across domains (Identify, Protect, Detect, Respond, Recover).
- **AI Enablement:** AI correlates threat intelligence, incident history, and control performance to give dynamic maturity scores and recommend prioritised actions.



AI-Driven compliance monitoring

- **Use Case:** Ensure adherence to Basel III, GDPR, DPDP, PCI DSS, and local banking regulations.
- **AI Enablement:** AI automates compliance checks, flags deviations in real time, and generates audit-ready reports, reducing manual overhead.



AI in risk and exposure analytics

- **Use Case:** Identify gaps in banking infrastructure (apps, APIs, OT systems) that could lead to non-compliance or breaches.
- **AI Enablement:** AI scans configurations and transaction logs at scale, simulates attack scenarios, and prioritises exposures by business impact.

**AI-Powered vulnerability and penetration testing**

- **Use Case:** Detect vulnerabilities in web/mobile banking apps, payment platforms, and ATM/PoS ecosystems.
- **AI Enablement:** AI automates penetration testing, learns from emerging exploit patterns, and simulates real-world adversary techniques.

**AI in fraud and insider threat simulation**

- **Use Case:** Prevent compliance breaches caused by phishing, credential misuse, or rogue insiders.
- **AI Enablement:** AI analyses behavioural anomalies in user access, runs phishing simulations, and provides predictive insights to mitigate insider risks.

**AI for continuous digital risk monitoring**

- **Use Case:** Monitor digital exposure, website defacement, and brand misuse targeting banks.
- **AI Enablement:** AI-driven crawlers scan the deep/dark web, track anomalies across digital assets, and provide early alerts on brand or data misuse.

Business impact**Reduced risk:**

Identify and close gaps before attackers exploit them.

**Regulatory confidence:**

Meet complex compliance obligations with ease.

**Operational resilience:**

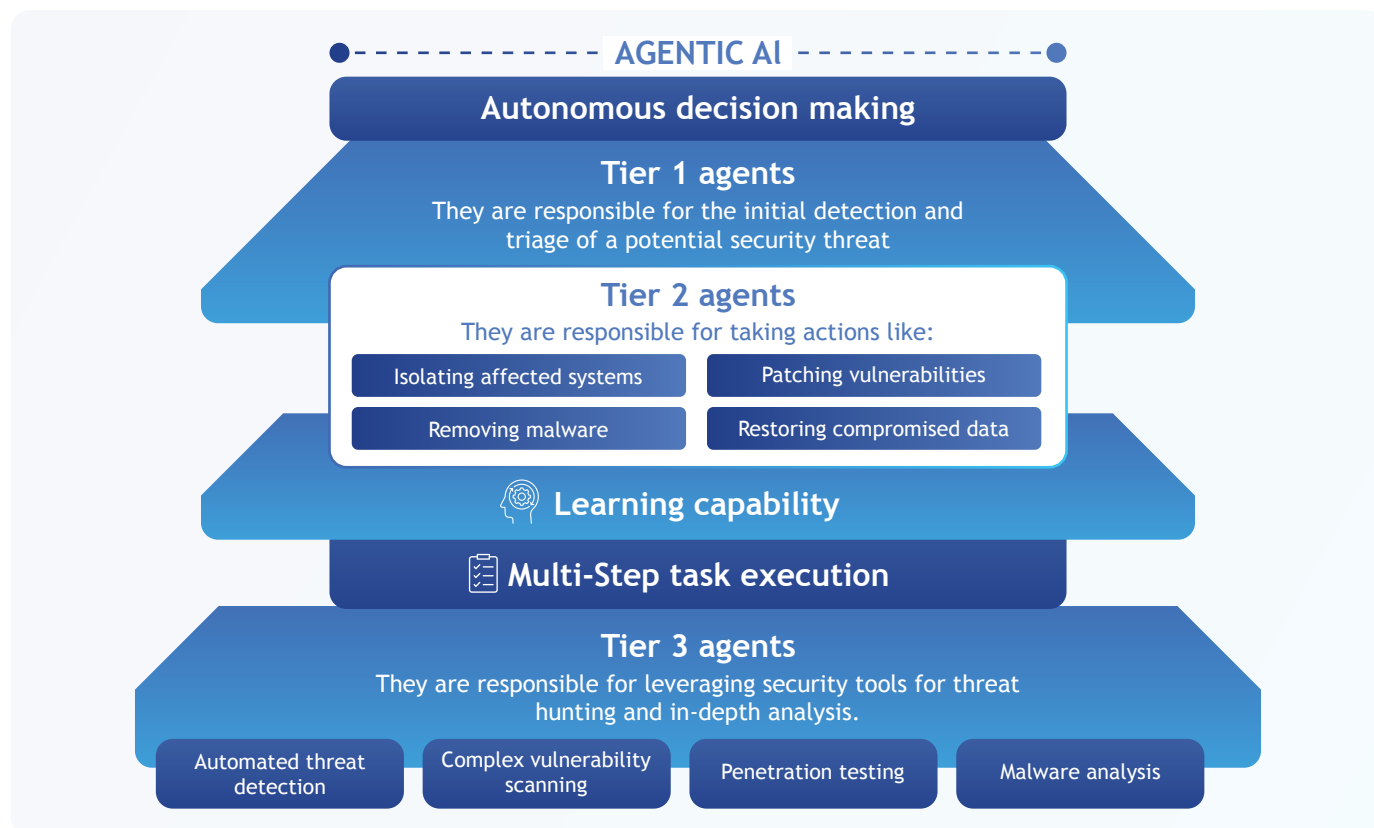
Minimise disruptions through proactive risk management.

**Brand protection:**

Safeguard reputation by preventing breaches and defacements.

Customer channel and endpoint security

Customer-facing digital platforms—such as mobile apps, online banking, ATMs, and call centres—are high-impact targets. A single compromised session can lead to account takeover, data loss, or reputational damage.



Mobile and web app protection:

Behavioural analytics, app shielding, and in-app threat detection ensure safe digital experiences.



Adaptive authentication and biometrics:

Multi-factor authentication based on behaviour, context, and device data balances security and convenience.



ATM, POS and Kiosk endpoint security:

Our EDR platform safeguards physical interfaces with real-time monitoring and threat response.



Call centre cyber hygiene:

Screen activity monitoring, secure desktops, and data loss prevention (DLP) tools ensure secure agent environments.



Bot and DDoS defence:

Global edge protection filters out automated threats and ensures consistent availability of customer services.

Digital Growth Is unstoppable and hence, Cybersecurity must now evolve from reactive defence to proactive value-chain-wide risk management.

AI powered customer channel and endpoint security



AI-Powered channel threat detection

- **Use Case:** Secure mobile apps, internet banking portals, and APIs from DDoS, API abuse, and session hijacking.
- **AI Enablement:** AI/ML models analyse traffic behaviour in real time, distinguishing normal customer activity from automated bot attacks, reducing false positives.



AI-Driven authentication and identity protection

- **Use Case:** Strengthen login security for customers across channels (mobile, ATM, internet banking).
- **AI Enablement:** AI applies adaptive MFA, evaluates device fingerprints, geolocation, and behavioral biometrics to spot anomalies and block account takeovers.



AI for ATM, IoT and endpoint security

- **Use Case:** Protect smart ATMs, kiosks, PoS terminals, and employee endpoints from malware, skimming, and firmware exploits.
- **AI Enablement:** AI continuously monitors endpoint telemetry, flags abnormal activity, and applies predictive patching before vulnerabilities are exploited.



AI-Enabled fraud and phishing detection

- **Use Case:** Identify phishing attempts, rogue apps, or impersonated banking channels targeting customers.
- **AI Enablement:** AI scans traffic, emails, and app ecosystems for fraudulent domains and abnormal communication patterns, issuing early alerts.



AI in customer trust and brand protection

- **Use Case:** Prevent attacks on downstream customer-facing systems that could damage reputation or erode trust.
- **AI Enablement:** AI-driven digital risk monitoring scans web, social, and dark web for impersonation attempts and fake banking sites, taking proactive takedown actions.



Success stories

SOC deployment for large public sector bank



Challenges

- Needed to migrate to the latest **SIEM, SOAR, and UEBA technologies** for advanced threat detection and response.
- Required **application security and AI-based cloud security** to strengthen resilience across hybrid environments.
- Lacked unified visibility and **dashboards with advanced analytics** to detect and respond to cyberattacks faster.



Solution

- Deployed an extensive **multi-layered security landscape** spanning 4+ sites including DC, Near-DC, and DR setups.
- Managed **4 lakh EPS (Events Per Second)** scale, integrating **28+ security technologies and services**.
- Implemented advanced tools: SIEM, SOAR, UEBA, PIM, API Security, CASB, CSPM, KMS, SAST/DAST, VA-PT, MFA, DRM, NBAD, DAM, MTV Scan, MTP, DLP, EPP, Data Classification, WAF, ETM, DDoS, SWG, NGIPS, Anti-APT, DNS Security, SMG, Micro Packet Capture, Firewall Analyser, Anti-Fraud, Threat Intelligence, Decoy, EDR.
- Provided **dedicated on-site resources** to ensure operational efficiency and compliance with banking regulations.



Impact

- Achieved **continuous A/A+ ratings in national cyber drills** for the past six years.
- Scaled from **35K EPS to over 2 lakhs**, now projected at **4 lakh EPS**, ensuring future-ready resilience.
- Integrated **5,000+ devices**, with the number continuing to grow across the bank's environment.
- Acted upon **50+ threat intelligence alerts (Tata CTI)** on average, strengthening proactive threat defence.
- Ensured **safe, compliant, and uninterrupted banking operations**, meeting all regulatory standards.

Kotak Mahindra Asset Management Company (KMAMC) strengthens cybersecurity



Challenges

- KMAMC faced limited visibility into threats, manual monitoring, and delayed threat responses, which created gaps in cybersecurity and increased vulnerability.



Solution

- KMAMC partnered with Tata Communications to implement a Managed SIEM solution, expanding to SOAR and UEBA. This provided real-time threat intelligence, automated alerts, and enhanced governance.



Impact

- **Improved security:** Real-time visibility and proactive threat detection enhanced security resilience.
- **Operational efficiency:** Automation and better governance reduced delays and improved response times.
- **Business continuity:** The phased deployment ensured no business disruptions, boosting trust and operational stability.

The collaboration with Tata Communications transformed KMAMC's cybersecurity, shifting from reactive to proactive defence.



Strategic cybersecurity advantage for banks

Tata Communications enables banks with an AI-driven, cloud-native cybersecurity fabric that strengthens trust, ensures compliance, and powers secure innovation.



Resilient operations:

AI detection, Zero Trust, and cloud recovery keep services uninterrupted.



Rapid response and compliance:

SOC-driven automation reduces response times, breach impact, and audit fatigue.



Customer trust:

Multi-layered AI security—biometrics, endpoint defence, and bot protection—ensures safe digital experiences.



Competitive edge:

Strong cyber posture accelerates open banking, fintech partnerships, and market credibility.



Efficiency and lower TCO:

70%+ savings through automation and centralised SOC visibility.

With Tata Communications, banks can innovate confidently and lead the digital-first future with security at the core.



Digital banking has created unprecedented opportunities while simultaneously expanding the cyber-attack surface. To enable this Digital transformation, **NexGen Banking** functions, including **Core technology infrastructure, operations and regulations, partner APIs, and customer-facing channels**, all require resilient and trusted protection. In this emerging scenario, Security must be embedded across every layer of the **Hyperconnected banking ecosystem**.

Tata Communications addresses this need through its comprehensive portfolio aligned to the solutions outlined in this whitepaper:

**Network security:**

Protecting hybrid WAN, interbank connections, and payment rails (SWIFT, UPI, RTGS) with managed firewalls, DDoS protection, and secure SD-WAN overlays.

**Cloud security:**

Safeguarding workloads across multi-cloud and hybrid environments through encryption, secure access, and compliance-ready monitoring.

**Security Operations (SOC):**

Delivering continuous threat detection, rapid incident response, and predictive intelligence through managed SOC services tailored for banking risk landscapes.

**Governance, Risk and Compliance management (GRC):**

Ensuring regulatory alignment and operational resilience through policy orchestration, audit-ready reporting, and integrated risk management frameworks.

**Customer channel security:**

Enabling safe engagement across mobile, branch, and contact centre environments with advanced authentication, endpoint protection, and secure collaboration platforms.

Through these solutions, Tata Communications enables banks to achieve critical outcomes of **Resilience, Trust and Compliance, and Agility and Innovation**—while staying aligned to global and local regulatory expectations.

By embedding these solutions into the banking digital core, Tata Communications ensures that growth and innovation remain secure, sustainable, and future-ready.

Contributors

Vivek Vishnu, Digital Transformation Specialist and Cyber Security Architect



Sudhir Garg, Global Marketing Director, ABM and Industry Marketing



Akshay Ganju, Senior Global Marketing Manager, BFSI, ABM and Industry Marketing





About Tata Communications

Tata Communications serves 300 of the Fortune 500 companies, enabling their digital transformation journeys through a portfolio of integrated, globally managed services that deliver localised customer experiences. Through its network, cloud, mobility, Internet of Things (IoT), collaboration and security services. Over 35% of global internet traffic is routed on-net through the company's widely distributed global network. The company's capabilities are underpinned by its global network. It is the world's largest wholly owned subsea fiber backbone with 500,000+ km of round the globe optical fiber and a Tier-1 IP network with connectivity to more than 190 countries and territories. Tata Communications has also been recognised as a leader in the Gartner Magic Quadrant for network services for 12 consecutive years.