

Transforming Financial services

with a secure and compliant
Apple ecosystem with HCLTech
powered by Jamf

Reimagining banks and financial institutions with Apple-first experiences

In today's financial landscape, security, compliance, and seamless digital experiences are critical. Financial services organizations must protect sensitive data, meet stringent regulatory requirements, and ensure a secure digital workspace—all while providing employees with the best-in-class Apple experience.

As a trusted partner of Jamf, HCLTech delivers comprehensive Apple device security and management solutions tailored for financial services. With deep expertise in the banking and financial sector and an award-winning digital workplace practice, we integrate Jamf's cutting-edge security and compliance solutions into financial institutions' IT environments.

HCLTech's Jamf solutions for Financial services

Zero-trust security and compliance with Jamf Protect, ZTNA and Jamf Trust

Regulatory compliance

Jamf Protect ensures compliance with financial regulations such as GLBA, PCI DSS, and SOX by providing real-time security insights, behavioral analytics and compliance monitoring. This helps financial organizations achieve compliance and significantly reduce payment fraud incidents on mobile banking platforms.

Zero Trust Network Access (ZTNA)

With Jamf Trust and Jamf ZTNA, financial institutions can implement identity-based, least-privilege access to banking applications, securing hybrid and remote workforces.

Mobile Threat Defense (MTD)

Jamf Protect detects mobile threats in real time, preventing phishing attacks, malware, fraudulent app installations, suspicious network traffic, unauthorized root access attempts and unauthorized access to sensitive banking applications.

Advanced Executive Threat Protection with Jamf (JETP) for high-value financial users

Forensic mobile security for VIP users

C-level executives, investment bankers, and senior wealth managers are prime targets for cyber espionage and credential theft. Jamf Executive Threat Protection (JETP) provides continuous forensic scanning of mobile devices, detecting sophisticated Pegasus-like spyware infections, zero-day exploits and Advanced Persistent Threats (APTs), ensuring sensitive client data and high-profile deals remain secure. This approach helps stop targeted cyberattacks on wealth advisors, preventing unauthorized access to multi-million-dollar client portfolios.



Secure Mac and iPhone fleet management with Jamf Pro

Automated compliance enforcement

HCLTech's managed Jamf Pro services ensure all Apple devices are configured to adhere to financial security policies.

Enhanced employee experience

Secure zero-touch deployment of MacBooks & iPhones with automated policy enforcement, ensures frontline bankers and executives can work seamlessly while staying compliant.

Data Loss Prevention (DLP)

Automated restriction of USB access, unauthorized software, and non-compliant network connections on corporate MacBooks prevents data breaches.

Strengthening security with Apple's Managed Device Attestation

Enhanced device compliance and trust

Apple's Managed Device Attestation, supported by Jamf, provides hardware-based cryptographic attestation at the moment of enrollment, ensuring that only legitimate Apple devices gain access to financial services networks.

Protection from advanced spoofing attacks

Prevents hackers from spoofing non-Apple or compromised devices to gain unauthorized access to core banking systems.

Onboarding and instant secure access

Banks can authenticate and provision Apple devices instantly with strong cryptographic evidence of legitimacy, ensuring a secure and seamless onboarding process for employees.

Jamf Network Relay – A game-changer for secure financial transactions

HCLTech integrates Jamf's **Network Relay Service** with financial networks, enhancing device authentication and network security. This is critical for highly regulated banking environments requiring encrypted communication.

Seamless secure connectivity

Financial institutions often face networking challenges for remote workers and branch offices. Jamf's Network Relay Service eliminates connectivity issues by ensuring secure and continuous access to internal banking applications.

With Jamf's Network Relay Service, mobile banking transactions are encrypted and routed through secure network relays, eliminating the risk of phishing attacks targeting bank employees or VIP customers.

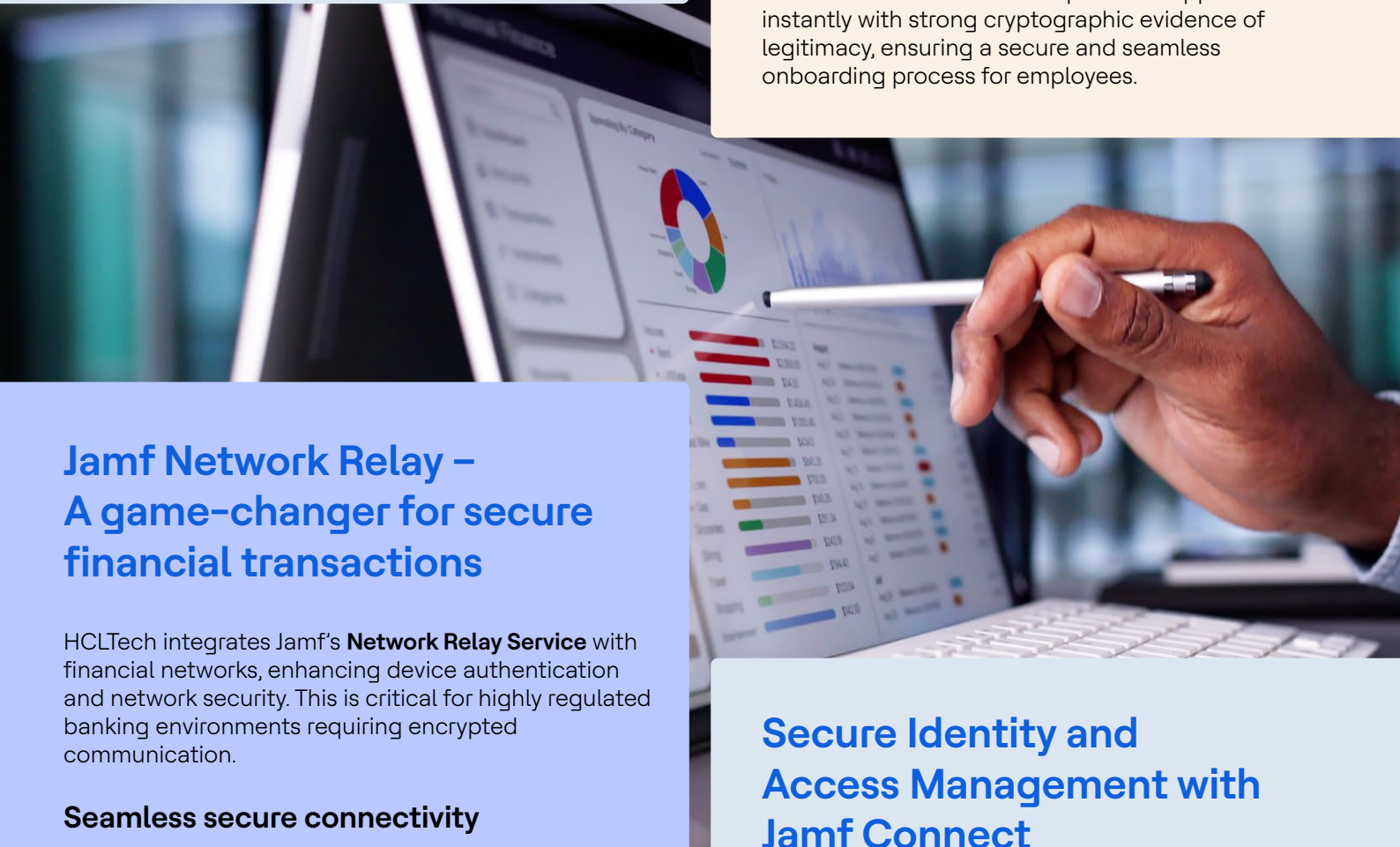
Secure Identity and Access Management with Jamf Connect

Seamless and secure authentication

Enforces cloud-based identity authentication and passwordless sign-ins for banking employees.

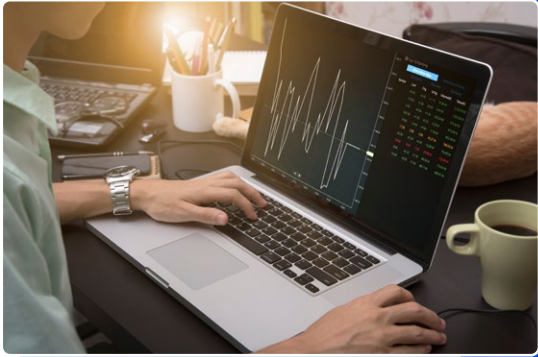
Prevents unauthorized user access

Ensures only verified employees can log in to banking apps by enforcing strict authentication policies.



Real-world use cases for Financial services

Preventing fraud in high-frequency trading environments



Challenge



Financial traders executing high-value transactions are prime targets for cybercriminals who attempt to install stealth malware on Apple devices to intercept trade secrets and manipulate market activity.

Solution



HCLTech deploys Jamf Executive Threat Protection (JETP) and Mobile Threat Defense (MTD) to monitor for unauthorized network access, credential harvesting attempts, and keylogging software on trading desk MacBooks and iPhones.

Impact



Prevents millisecond-level trade data leaks, ensuring market integrity and securing high-value assets in hedge funds, investment banks, and wealth management firms.

Securing customer mobile banking and preventing phishing attacks



Challenge

Retail banks face increasing fraud via phishing, social engineering, and fake banking apps targeting Apple mobile users.



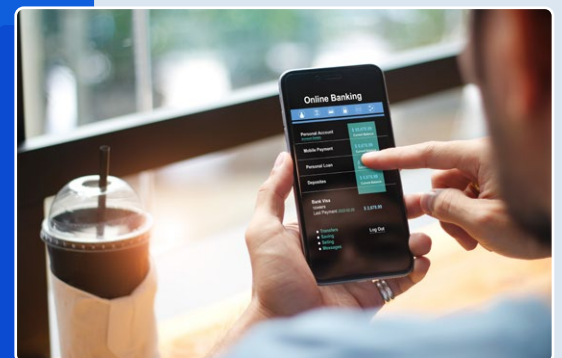
Solution

HCLTech leverages Jamf Protect's Mobile Threat Defense to detect fraudulent app installations, alert customers of phishing attempts, and enforce biometric authentication for high-risk transactions.

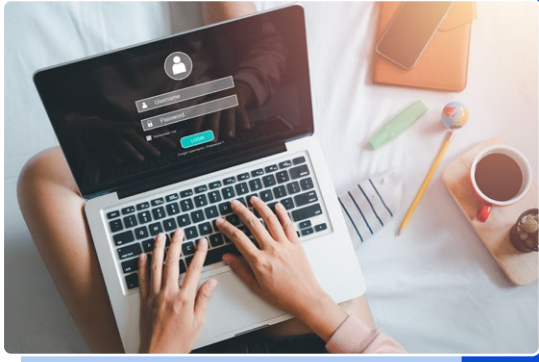


Impact

Reduces fraudulent transactions significantly, ensuring customer trust and PCI DSS compliance across mobile banking platforms.



Fraud prevention with Apple's Managed Device Attestation



Challenge



Banks need to ensure only legitimate Apple devices access customer records, core banking apps, and financial APIs, preventing device spoofing fraud.

Solution



HCLTech implements Apple's Managed Device Attestation with Jamf, enabling hardware-level cryptographic attestation during device onboarding.

Impact



Prevents impersonation fraud, blocking unauthorized Apple device clones from accessing sensitive financial infrastructure.

High-speed, secure access for investment teams and remote trading desks

Challenge



Remote investment teams need fast, secure access to real-time financial data while avoiding VPN slowdowns or geo-blocking issues.

Solution



HCLTech integrates Jamf's Network Relay Service to create secure, high-performance connections for traders and analysts needing low-latency access to Bloomberg, Reuters Eikon and AI-powered trading models.

Impact



Ensures uninterrupted, secure trading activity, reducing latency and allowing hedge funds to execute trades with minimal risk of data breaches.



Onboarding and connectivity for bank branch employees with Jamf Network Relay



Challenge



New employees in branch locations often face delays in device setup and connectivity issues, impacting productivity.

Solution



HCLTech can enable zero-touch enrollment with Jamf Pro and Jamf's Network Relay Service, ensuring instant connectivity and configuration of critical banking applications.

Impact



This reduces onboarding time significantly allowing branch employees to securely access customer support systems and transaction platforms from day one.

Self Service+ for enhanced employee productivity in banking

Challenge



Banks need a way to empower employees with self-service IT tools while ensuring compliance.

Solution



HCLTech can deploy Jamf's Self Service+, providing a secure, banking-approved app catalog where employees can install pre-approved tools (e.g., Bloomberg Terminal, Reuters Eikon) without IT intervention.

Impact



This reduces IT support tickets significantly, enhances employee autonomy, and ensures secure access to business-critical applications.



Preventing unauthorized access to trading platforms with Jamf Connect



Challenge



Investment firms and trading desks need to enforce strict authentication policies to prevent unauthorized access to financial applications.

Solution



HCLTech can implement Jamf Connect to enforce biometric authentication and single sign-on (SSO) for financial applications.

Impact



This prevents credential theft, enforces compliance with internal security policies, and ensures that only authorized traders can access sensitive investment data.

Enhancing security for BYO devices in financial institutions

Challenge



Many banks and financial services organizations have adopted Bring Your Own (BYO) device models to reduce operational costs and offer flexibility to employees. However, most rely solely on Mobile App Management (MAAM), skipping MDM-based enrollment or Apple's User-Initiated Enrollment, which leaves gaps in device-level security and limits control over sensitive financial applications.

Solution



HCLTech can implement Apple's User-Initiated Enrollment with Jamf's BYOD support, enabling secure, privacy-preserving management of personal devices. This approach leverages Apple's best practices for BYO, including a clear separation of personal and corporate data, paired with Jamf Protect and Jamf Trust for mobile threat defense and zero-trust access.

Impact



This elevates mobile security for personal devices used in banking operations, reduces exposure to phishing or data leakage risks, and ensures regulatory compliance without compromising employee privacy. It also offers a smooth, self-service-driven onboarding experience for BYO users.



Streamlining shared device use in branch banking with Jamf Setup & Reset



Challenge

Branch staff often share iPads or other Apple devices across different roles (e.g., teller, relationship manager, service desk), leading to operational friction and increased support overhead. Employees spend valuable time reconfiguring devices or risk accessing apps irrelevant to their function.



Solution

HCLTech can deploy Jamf Setup and Jamf Reset to enable “pick-and-go” device functionality. Employees can select their role (e.g., Teller, Personal Banker, Branch Manager) at the start of the shift, triggering instant configuration of apps and settings based on their profile. Secure SSO-based authentication ensures access control, while Reset wipes the device for the next user in seconds.

Impact:

This reduces device setup time significantly, streamlines branch operations, improves security through role-based access, and provides a seamless experience for employees using shared devices in dynamic environments.



Why HCLTech for Financial services?

- **Deep banking and financial services expertise:** Over 40 years of experience serving global banks and fintech firms.
- **Jamf and Apple specialist:** Advanced Jamf capabilities tailored for financial security. We are also an Apple authorized reseller and managed service provider, besides being a strategic MSP and a resale partner with Jamf.
- **Financial crime prevention:** HCLTech offers financial crime prevention (FCP) services, leveraging domain expertise and experience to provide 24/7 global coverage and protection.
- **Focus on innovation:** We leverage advanced technologies like AI, cloud and digital solutions to help financial institutions streamline operations, enhance customer experiences and drive growth.
- **Fintech solutions:** We offer a wide range of fintech solutions, including banktech, investech, regtech and insurtech, empowering financial institutions to harness the power of technology.



- **Cybersecurity solutions:** HCLTech provides a comprehensive portfolio of cybersecurity services, utilizing AI and predictive analytics for proactive defense against cyber threats.
- **Compliance and regulatory expertise:** We help financial institutions stay compliant with evolving financial regulations and requirements. Pre-built GLBA, SOX, PCI DSS, and GDPR compliance policies integrated with Jamf.
- **Strong client relationships:** HCLTech emphasizes building long-term partnerships with clients, focusing on shared goals and success. Our clients include 2 top retail banks across each geography, 5 out of 10 top global investment banks, 7 out of 10 top Life and P&C insurance companies, 12 out of 25 top fintech firms.
- **Global 24/7 security operations:** Continuous monitoring, proactive threat hunting and rapid incident response.

Secure your Financial enterprise with HCLTech and Jamf

As financial institutions embrace Apple devices for productivity and innovation, security and compliance must be non-negotiable. With HCLTech's expertise and Jamf's industry-leading solutions, your organization can stay ahead of cyber threats, ensure regulatory compliance, and enable a seamless Apple experience.

Get in touch

For a customized consultation, reach out to us at dwp@hcltech.com. Let's transform your financial IT security today!

HCLTech | Supercharging Progress™

HCLTech is a global technology company, home to more than 220,000 people across 60 countries, delivering industry-leading capabilities centered around digital, engineering, cloud and AI, powered by a broad portfolio of technology services and products. We work with clients across all major verticals, providing industry solutions for Financial Services, Manufacturing, Life Sciences and Healthcare, Technology and Services, Telecom and Media, Retail and CPG, and Public Services. Consolidated revenues as of 12 months ending December 2024 totaled \$13.8 billion. To learn how we can supercharge progress for you, visit hcltech.com.

hcltech.com

