HYPORI™
VIRTUAL MOBILITY

How to Face COVID-19 Cybersecurity Challenges in the Financial Services Industry

WHITEPAPER

Summary

Digitization is not new to financial institutions. Even before COVID-19, most financial services firms sought efficiency and increased customer satisfaction in modern technology. Digitization adoption rates varied based on firm size, agility, openness to change, and other factors, but it was widespread.

When the pandemic hit, many companies had to accelerate digitization efforts, often without comprehensive transformation plans. Offices closed, and remote work became the norm. At the time, anything that could be virtual shifted, including operations, customer engagement, and distribution. But, for CISOs and cybersecurity teams, this change created significant risk and exposure. Increased mobile device use gave cybercriminals new attack surfaces, and COVID-19 fears made all users more vulnerable to scams.

The Situation

Cybersecurity was a top industry priority before the pandemic, but the new threat concern is now greater than ever. In a continually evolving technological environment, agility and responsiveness are critical, and these firms face a few fundamental challenges.

The enterprise must quickly resolve issues related to a significant shift to remote working. Mobile device use in the workplace means multiple network entry points. Because widespread remote working was unexpected, related security protocols may not be in place or have been circumvented to facilitate productivity.

Cyberthreats are on the rise across the board, but the financial services industry is taking a particularly big hit. According to a VMWare Carbon Black report, between February and April 2020—the global COVID-19 surge—cyberattacks increased by 238% among financial institutions. In 2020, bad actors targeted 27% of all cyberattacks at either financial services or healthcare. Ransomware currently represents a particularly dangerous threat. During the COVID-19 global surge, such attacks increased nine-fold.

Digitization, mobile device use, and new technologies like cloud computing are prevalent in financial institutions today. To stay up-to-date and protected in a $1.5 trillion cybercrime economy, they need comprehensive, adaptable, and cost-effective approaches to cybersecurity that protect their consumers' privacy and secure their organizations' networks.

The Problem

For cybercriminals, attacking financial institutions—where the money is—presents many profit opportunities. While other bad actors, including nation-states, also target the financial sector for political and ideological leverage, money always matters. According to Verizon's 2020 Data Breach Investigations Report, 86% of all breaches are financially motivated.

Today's financial institutions face some new and many exacerbated cyber threats. Credential and identity theft, for example, are a significant and growing problem as cybercriminals take advantage of an expanded attack surface due to increased mobile device use and a larger remote workforce.

Because of COVID-19, financial institution-managed government funding programs offered loans to small businesses presenting a fraud opportunity for bad actors. Breached Federal Disaster Loan claims impacted 8,000 small businesses in the US. COVID-19-related fraud is widespread and continues, targeting individuals, financial institutions, and even governments.

With the pandemic-related rapid shifts to increased mobile device use and remote work, cloud technology use skyrocketed. According to Gartner, Inc., the global public cloud services market will grow to nearly $258 billion in 2020 and is forecast to reach $364 billion by 2022. Because COVID-19 caused, in many cases, accelerated cloud migrations for some organizations, cohesive strategies were not in place, leaving them vulnerable to cyberattacks.

Finally, as a heavily regulated industry, financial services requires compliance with and adherence to federal standards. Regulatory compliance is a significant factor in any financial institution's cybersecurity protocols.

The financial services industry faces many cybersecurity challenges that have intensified as a result of COVID-19. Financial institutions are changing the way they work, and they need next-gen technology to keep them safe and productive.

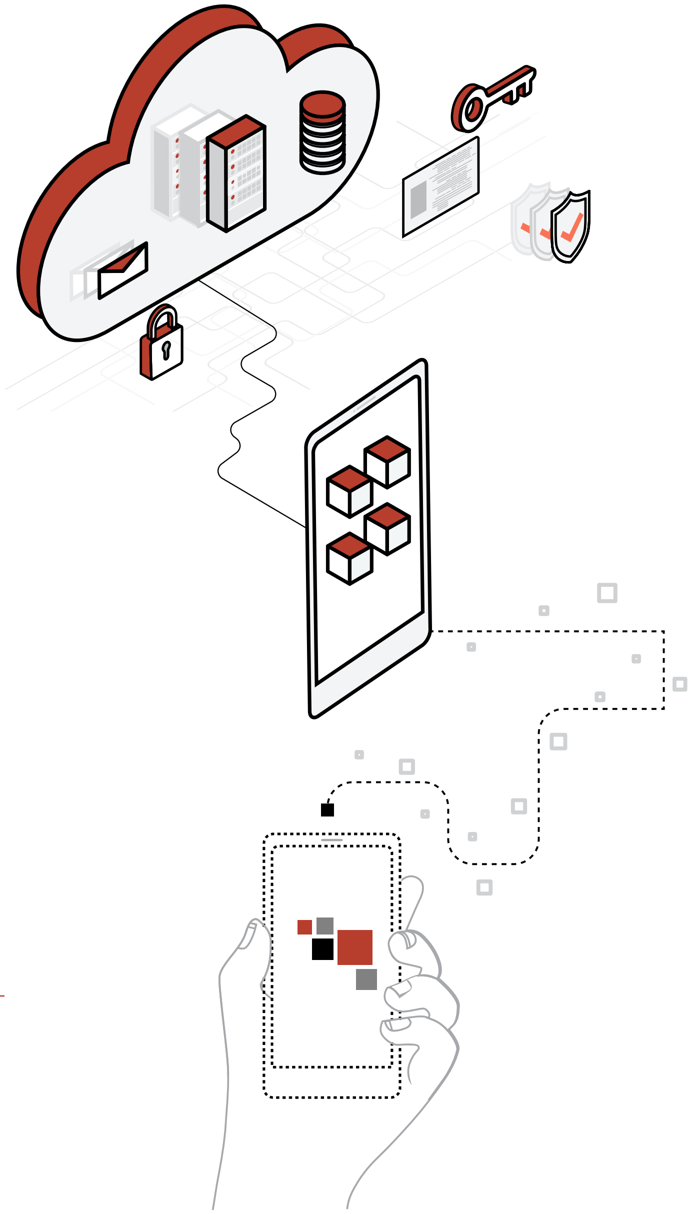
The Solution

Hypori Virtual Mobility™ delivers highly secure, regulatory-compliant enterprise mobility that protects employee mobile devices and secures sensitive customer and enterprise data. Hypori's solution securely contains all organization data on a fully-featured virtual mobile device in the company-owned data center with 100% separation of personal and enterprise data.

Hypori is also centrally managed, reducing administrative costs and labor. Organizations do not need to access end-user devices, ensuring employee privacy, and there's no company exposure should devices be compromised. With Hypori, cybersecurity management shifts from vulnerable personal devices to a secure data center. No data is ever at rest on mobile devices allowing the remote workforce secure enterprise data access in an intuitive, confidential environment.

Hypori delivers a military-grade secure, centrally managed, admin-friendly Virtual Mobility Solution for your financial institution that is regulatory compliant, cost-efficient, and user-intuitive.

To learn more about Hypori Virtual Mobility, contact us for a demonstration today.



Contact us

info@hypori.com

*The National Security Agency Commercial Solutions for Classified (CSfC) provides DoD entities the ability to conduct secure classified communications using Commercial-off-the-Shelf (COTS) products. Under this program the Mobile Access Capability Package v2.0 provides a framework for how to secure these communications from mobile end user devices into government enterprise resources. Under the MACP v 2.0, communications must be established using an inner and outer tunnel to provide the secure communications path. Intelligent Waves, LLC's Hypori Client v4.1 for iOS and Android is eligible to be used as a TLS Software Application Product component in a CSfC solution. This means that in combination with a CSfC eligible TLS Protected Server, Hypori is eligible to provide the inner tunnel for secure communications.

11 March 2019

hypori.com