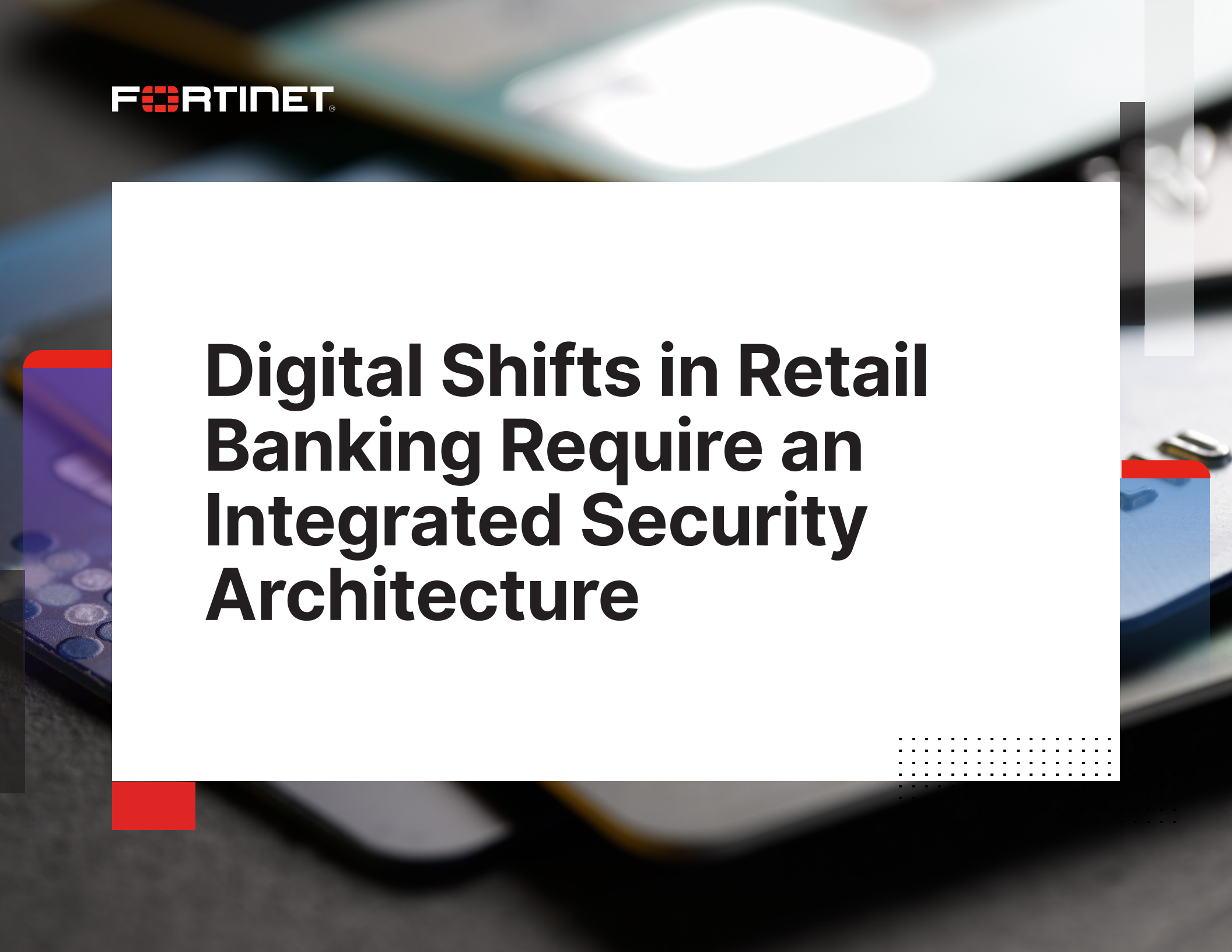

Digital Shifts in Retail Banking Require an Integrated Security Architecture

Table of Contents

Executive Overview

The COVID-19 pandemic is accelerating consumer preference for mobile and online banking. In April 2020 alone, there was a 200% jump in new mobile banking registrations worldwide, and an 85% rise in mobile banking traffic.[1] As a result, many retail banks are fast-tracking adoption of new digital tools, services, and capabilities to support recommended preventative measures, meet growing customer demands, and to keep online-centric competitors from siphoning off market share.

The accelerated pace of digitization in banking comes with challenges, from an expanded network attack surface, to a rising volume of targeted attacks, and to ever-increasing regulatory pressure. With any successful breach having the potential to ruin even robust financial institutions, CISOs must work with their executive leadership to prioritize a comprehensive cybersecurity strategy aligned to the current push to digitize.

A Mad Rush To Adopt New Banking Tools

Until recently, retail banks around the world have been slow to adopt digital innovation. Bank executives frequently cite cybersecurity and privacy concerns (80%), outdated data management (68%), and identifying the right partners (73%) as primary barriers to moving to an online banking platform.[2] But as COVID-19 accelerates the digital transition for many organizations, cyber criminals are looking to take advantage. Since the early days of the pandemic, banks have seen a 238% surge in cyberattacks.[3]

Among direct financial losses, lost revenue due to network downtime, brand degradation, legal costs, and regulatory penalties, a single, successful security breach can cause millions of dollars in damages and ultimately ruin even a robust financial organization.

Typical barriers to success include overly complex IT and security infrastructure, a rising tide of sophisticated attacks, new compliance requirements, and a lack of skilled security talent available to help implement and manage cyber defenses. To embrace digital change under these less-than-optimal conditions, financial leaders must make smart decisions with the overall health and resiliency of their institutions in mind. And this begins by embracing cybersecurity at a cultural level across the organization.

Over half (57%) of consumers now say they prefer internet banking (up from 49% pre-COVID-19), and 55% now prefer banking mobile apps (compared with 47% previously).[4]

The average total cost of a single data breach in 2020 is $3.86 million.[5]

How Can Banks Mitigate the Risks of Digitalization?

Even before COVID-19, retail banks were under tremendous pressure to compete with a variety of newcomers, from online-only suitors to major companies like Apple, Amazon, and Facebook launching services designed to displace traditional banking. The rush to catch up in the digital innovation race greatly multiplies all the inherent risks. With increasing technology adoption and a growing number of organizations being targeted each day for theft, damage, or disruption, banks need to reevaluate their cybersecurity as an enabler during this transition—and perhaps the most important one.

While reevaluating security defenses may seem like another daunting task under already stressful conditions, an effective cybersecurity strategy for digital banking systems starts with just four key capabilities:

- Ensure visibility across the digital attack surface
- Deploy protection against sophisticated threats
- Adapt an intelligent and structured security architecture
- Simplify compliance processes

In a recent global survey, only 40% of respondents said they expect to return to physical bank branches post-COVID-19—indicating that the shift to online is likely to stay.[6]

Visibility Across the Digital Attack Surface

Financial services organizations have historically experienced up to 300 times as many cyberattacks per year compared to companies in other industries.[7] Since the start of the pandemic, targeted attacks against banks have been on the rise. The combined effects of rising threat volume with a rapidly expanding attack surface (as a result of digitalization) is a recipe for disaster. It sharply increases the likelihood of a significant event occurring that compromises or otherwise damages the organization.

Regardless of the industry, organizations cannot protect anything that they cannot see. New mobile and online tools or services extend the reach of the network and create numerous new "edges"—vulnerable surface area that expands the opportunities for outside attack. Protecting these new network edges requires comprehensive **visibility** across all possible attack vectors as well as an integrated security platform designed for detection of the latest threats.

Protection Against Sophisticated Threats

Banks and financial institutions will remain a prime target for attacks for obvious reasons; 86% of successful breaches are motivated by financial gains.[8] The methods that cyber criminals employ—from ransomware to phishing schemes to targeting vulnerable open-source components in applications—will continue to expand and grow more sophisticated.

Sophisticated threats are on the rise, but many banks are in a precarious position when it comes to protection. Their business units are often siloed. Their infrastructure often includes legacy systems and software that may not be supported with regular patches. And—like every industry—they typically lack all the cybersecurity staff they need as a result of a historic shortage of skilled candidates on the job market. A majority (68%) of organizations continue to struggle with recruiting, hiring, and retaining cybersecurity talent.[9]

Bank CISOs need to ensure continuous protection across their entire deployed infrastructure, including all devices, networks, and applications. They need solutions that can **share local threat information** across the network infrastructure to defend against coordinated multiprong attacks. Cybersecurity also needs the benefit of the latest **global threat intelligence research** in order to repel new malware variants, previously unknown attacks, and the latest zero-day threats. And in order to compensate for limited staff resources, security should also offer features for **automated protection responses** against attacks.

Three out of every four businesses have had at least one breach over the past year attributed to a gap in cybersecurity skills.[10]

An Intelligent and Structured Security Architecture

Digitization adds new layers to the already complex IT systems that banks have in place. To compensate for the new risk exposures that online and mobile banking brings, it will be tempting for many CISOs to try and bolt on additional point security products to cover exposures one gap at a time. Unfortunately, this approach only makes the problems of an overly complex and disconnected IT ecosystem even worse.

Complexity is the enemy of an effective security posture. Most organizations already have too many vendors, too many alerts, and not enough skilled staff to triage and respond to potential threats. Automatic prevention, detection, and response to cyber threats starts with one common feature: **an integrated security architecture.** When all the parts of the cybersecurity ecosystem are connected and can communicate, this opens the door for **automated controls** based on defined policies. It allows manual tasks to be replaced by **automated workflows** to reduce the burden on human staff. And it provides a system of real-time data sharing that can feed the latest applications of **artificial intelligence (AI)** and **machine learning (ML)** at the specific solution levels of cyber defenses.

Simplified Compliance

When it comes regulatory requirements, retail banks must be able to prove their compliance with a growing list of laws (global, national, regional), industry regulations, and security standards. An integrated, end-to-end cybersecurity architecture makes compliance auditing and reporting processes much easier.

As digitalization transforms the shape and spread of the organizational network, sensitive data goes with it. Whether it is customer information stored in the cloud, an application that manages mobile transactions, or the credential for a bring your own device (BYOD) of an employee working from home, effective security must be able to show that all sensitive data is safe and accounted for at all times.

A cybersecurity platform that supports more **accurate reporting** and **efficient management** of sensitive private data can help organizations **eliminate operational costs** associated with compliance audits (e.g., dedicated staff hours spent on manual compiling of reports), while reducing the risk of incurring severe regulatory penalties that result from a successful breach or compliance violation.

The coronavirus pandemic has forced some financial institutions to reduce staff or reassign personnel at a time when compliance risks for bank are heightened.[11]

Competitive Services Depend on Comprehensive Protection

As traditional banks face immediate pressure to embrace digital innovation in order to meet customer needs during the pandemic and even beyond, cybersecurity must not be a separate or subordinate line item. For the success and survival of retail banking during this unprecedented moment of transition, CISOs should be prepared to lead their organizations toward a strategy designed for the future of their infrastructure and an increasingly harsh threat landscape. An integrated security architecture offers simplicity, visibility, and advanced protection that can scale with networks for years to come.

[1] Ellen Sheng, "Coronavirus crisis mobile banking surge is a shift that's likely to stick," CNBC, May 27, 2020.

[2] "World Retail Banking Report 2020: 57% of Consumers Prefer Internet Banking in the COVID-19 Era,"Business Wire, June 11, 2020.

[3] Charlie Osborne, "COVID-19 blamed for 238% surge in cyberattacks against banks," ZDNet, May 14, 2020.

[4] "World Retail Banking Report 2020: 57% of Consumers Prefer Internet Banking in the COVID-19 Era," Business Wire, June 11, 2020.

[5] "Cost of a Data Breach Report 2020," IBM and Ponemon Institute, August 2020.

[6] Ellen Sheng, "Coronavirus crisis mobile banking surge is a shift that's likely to stick," CNBC, May 27, 2020.

[7] Tom Kellermann, "Cybercriminals banking on finance: Mitigating escalation," HelpNetSecurity, June 17, 2020.

[8] "2020 Data Breach Investigations Report," Verizon, May 2020.

[9] "Fortinet Survey Finds Widespread Impact from Cybersecurity Skills Shortage," Fortinet, May 22, 2020.

[10] Ibid.

[11] Mengqi Sun, "Banks Face Increasing Compliance Risks, OCC Says," The Wall Street Journal, June 30, 2020.

www.fortinet.com

April 20, 2021 11:26 AM

ebook-retail-banking

752904-A-0-EN