



# WHITEPAPER



## THE FINANCIAL INDUSTRY'S ANSWER TO FIGHTING CYBERATTACKS

DEFENDING SENSITIVE DATA IN AN AGE OF DIGITAL TRANSFORMATION





## INTRODUCTION

---

*More than any other industry, the financial sector holds all that is dear and true to cybercriminals: money. With digital transformation and Software as a Service (SaaS) in full force among financial institutions, they are now more open than ever before to being exploited by attackers.*

Yet, to compete in the market place, banks, credit unions and brokerage firms must do all they can digitally to enhance the customer experience. A 2018 retail banking satisfaction study found that companies providing their customers with a higher quality service experience than their competitors acquire customers at a faster rate, retain a larger portion of those customers, and command a higher price for their services and products.<sup>1</sup>

Digital services are increasing in the financial industry, while the need for human-centered interaction is decreasing.<sup>2</sup> Digital payments, blockchain technology, and robotic process automation (RPA) are some of the technological advances that assess credit quality, automate client interaction, and optimize the execution of stock trades. While digital transformation benefits customers and financial institutions, if not managed correctly, it carries a number of security risks.

### WHO SHOULD READ THIS WHITE PAPER?



CISOs/CSOs



CIOs



Directors of Security/IT



Security Architects

# THE FINANCIAL INDUSTRY PROBLEM

Financial companies must change with the times, yet they must defend their environments from the multitude of different types of attacks that stem from vulnerabilities arising from the newest services. Gartner predicts that by 2020, 60 percent of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk.<sup>3</sup>

The Ponemon 2017 Cost of Cybercrime study found the average cost of cybercrime for financial services companies globally has increased by more than 40 percent over the past three years, from \$12.97 million per firm in 2014 to \$18.28 million in 2017 – significantly higher than the average cost of \$11.7 million per firm across all industries included in the study.<sup>4</sup>

Small and medium-sized financial institutions aren't exempt from the clutches of an attacker. According to a 2017 Nationwide Insurance Company report, although 53 percent of cybercrime perpetrated against financial institutions in the past five years has

been against firms making more than \$1 billion yearly, since 2012 the average target company size has decreased 28 percent.<sup>5</sup>

In the UK in 2017, 56 percent of banking systems were found to contain high-risk vulnerabilities, according to Positive Technologies, an enterprise security solutions provider. In its 2018 report *Financial Application Vulnerabilities*, the most common online bank vulnerabilities in 2017 were Cross-Site Scripting (75% of systems) and poor protection from data interception (69%), allowing attacks such as reading cookie values or stealing customer credentials.<sup>6</sup> In 13 percent of mobile applications, arbitrary code execution was possible, a vulnerability that the study found to be typical for the server side of applications. By exploiting such a vulnerability, an intruder could obtain full control over the server.

The above are just a few examples of current vulnerabilities found in the financial industry. As the industry expands its digital footprint, more vulnerabilities will follow in devices, applications and processes.



“ In the UK in 2017, **56%** of banking systems were found to contain high-risk vulnerabilities ”

*Positive Technologies, Financial Application Vulnerabilities, 2018*



## DIGITAL TRANSFORMATION IMPACTS CYBERSECURITY

---

In the early 2000s, financial institutions were offering just a few online services that allowed people to open an account, access their account history, and transfer funds to different accounts. In the mid-2000s, new online services included the ability to pay bills, obtain trust and stock statements, trade stocks and mutual funds, chat in real-time with customer service representatives, and obtain immediate email responses and news alerts. The internet allowed customers to access their accounts 24/7, and customer acquisition became less expensive and more effective. There was a lot of data to be secured back then, but that data was all held on premises, and a company only had to worry about securing its network. Then came something new: cloud services.

As security risks facing organizations large and small grow more prevalent and sophisticated, outsourcing security has become an increasingly attractive option.

Cloud services allow companies to quickly implement new services, scale services to fit needs, and provide innovative technology. Cloud data center traffic will represent 95 percent of total data center traffic by 2021, compared to 88 percent in 2016, according to research from Cisco.<sup>7</sup> However, as data moves to the cloud, so does the attention of attackers, and it's up to both cloud providers and the companies housing data with them to protect that data.

Many of the new web-facing applications that are being created to compete with peer-to-peer services for loans and payments are housed in the cloud. Wherever they're housed, mobile wallets and payment apps bring more vulnerabilities to websites. According to the 2017 Application Security Statistics Report, the finance and insurance industries each had on their websites an average of 5.5 vulnerabilities, of which 2.2 were classified as critical.

Moreover, financial institutions are incorporating Robotic Process Automation (RPA) to improve accuracy and workflow, to interact quicker with customers, and save time and resources

by completing tasks in seconds that otherwise could take hours. Functioning 24/7, RPA helps resolve customer queries, reduces the time it takes to onboard new customers, automates accounts payable processes, speeds up the dispatch of credit cards, identifies potential fraud, and can handle many other operational tasks automatically. However, unauthorized users could access or manipulate the private data software robots handle.

Blockchain-backed solutions are another example of the digital transformation occurring throughout the industry and are being embraced by banks to cut transaction times, reduce costs, and execute overseas transactions. A blockchain is a decentralized ledger of data blocks that is linked and secured with cryptography. While the technology has generated significant interest and offers an inherent level of security, blockchain-backed applications can have their vulnerabilities. Financial organizations that adopt private blockchain solutions still have to worry about access management, coding vulnerabilities, and other potential security issues.

IoT has not bypassed the banking industry either. Collecting and exchanging information from objects, such as watches, wristbands, and key fobs allows users to pay bills and track their spending. Data collected through IoT can aid banks in decision making by helping them to gain insights into their customers' spending patterns, ATM usage, and financing needs. If the past serves as any indication, some of these devices are likely to host remote access services or web applications. Like any server or application, there could be vulnerabilities present that allow for exploitation. For those devices which don't host services, compromise is still a possibility if a savvy attacker can execute network-based attacks.

Flaws and all, digital banking is here to stay. Retail banking executives surveyed by CEB, now Gartner, estimated that by 2019 banks will need to make roughly half of all sales using digital capability.<sup>8</sup>

“

Financial organizations that adopt private blockchain solutions still have to worry about access management, coding vulnerabilities, and other potential security issues.

”

## THE SOLUTION

---

Having unified visibility across cloud and on-premises environments is a critical first step in securing both the Internet of Things and other systems, applications, and infrastructure. A threat can only be remediated if it is seen. If an attacker breaks into a security camera or a web-facing app, a company must be able to spot the traffic and be able to quarantine the threat before malicious activity begins. That's now possible to do even if a company does not have its own security team.

By leveraging the power of the cloud, Security-as-a-Service (SECaaS) providers automatically scale up as a retailer's environment grows with the newest devices and applications. A team of trusted experts that specialize in protecting cloud, on-premises, and hybrid IT environments watch over environments 24/7/365, detect threats as soon as they appear, and automatically remediate them. These outsourced security providers meet help organizations meet compliance requirements, alleviate the need to hire and maintain security researchers and analysts, as well as the need to purchase and manage expensive equipment like IDS/IPS, firewalls and SIEM tools.

### SECaaS PROVIDES A VARIETY OF SECURITY SERVICES, INCLUDING THOSE LISTED BELOW:

- » Intrusion detection
- » Malware protection with constant updates
- » Log and event monitoring
- » Active threat hunting
- » Vulnerability scanning and patch monitoring

### WHEN CHOOSING AN SECaaS, LOOK FOR ONE THAT PROVIDES THE FOLLOWING BENEFITS:



Intelligence-driven, proactive security that provides threat alerts and remediation



Unified visibility and control for any environment



Simplified, continuous audit-ready compliance



Reduce dwell time for attackers



Pay-per-use consumption



Supported environments (On-prem, Cloud, and Hybrid)

# REFERENCES

---

- 1 The J.D. Power 2018 U.S. Retail Banking Satisfaction Study
- 2 Gartner 2017 Emerging Trends Barometer Survey
- 3 Gartner Special Report Looks at Cybersecurity at the Speed of Digital Business, June 16, 2016
- 4 Ponemon 2017 Cost of Cybercrime Study: Insights on the Security Investments that Make a Difference
- 5 2017 Nationwide Composition of Cyber Incidents within the financial industry from 2012-2017
- 6 Positive Technologies, Financial Application Vulnerabilities, 2018
- 7 2018 Cisco Global Cloud Index: Forecast and Methodology, 2016-2021
- 8 CEB, The Digital Tipping Point, 2016

The logo consists of two orange rectangular boxes side-by-side, separated by a thin vertical line. The word "ARMOR" is written in a bold, black, sans-serif font across the center of these boxes, with a trademark symbol (TM) at the end.

ARMOR™



ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167

18030716 Copyright © 2018. Armor, Inc., All rights reserved.