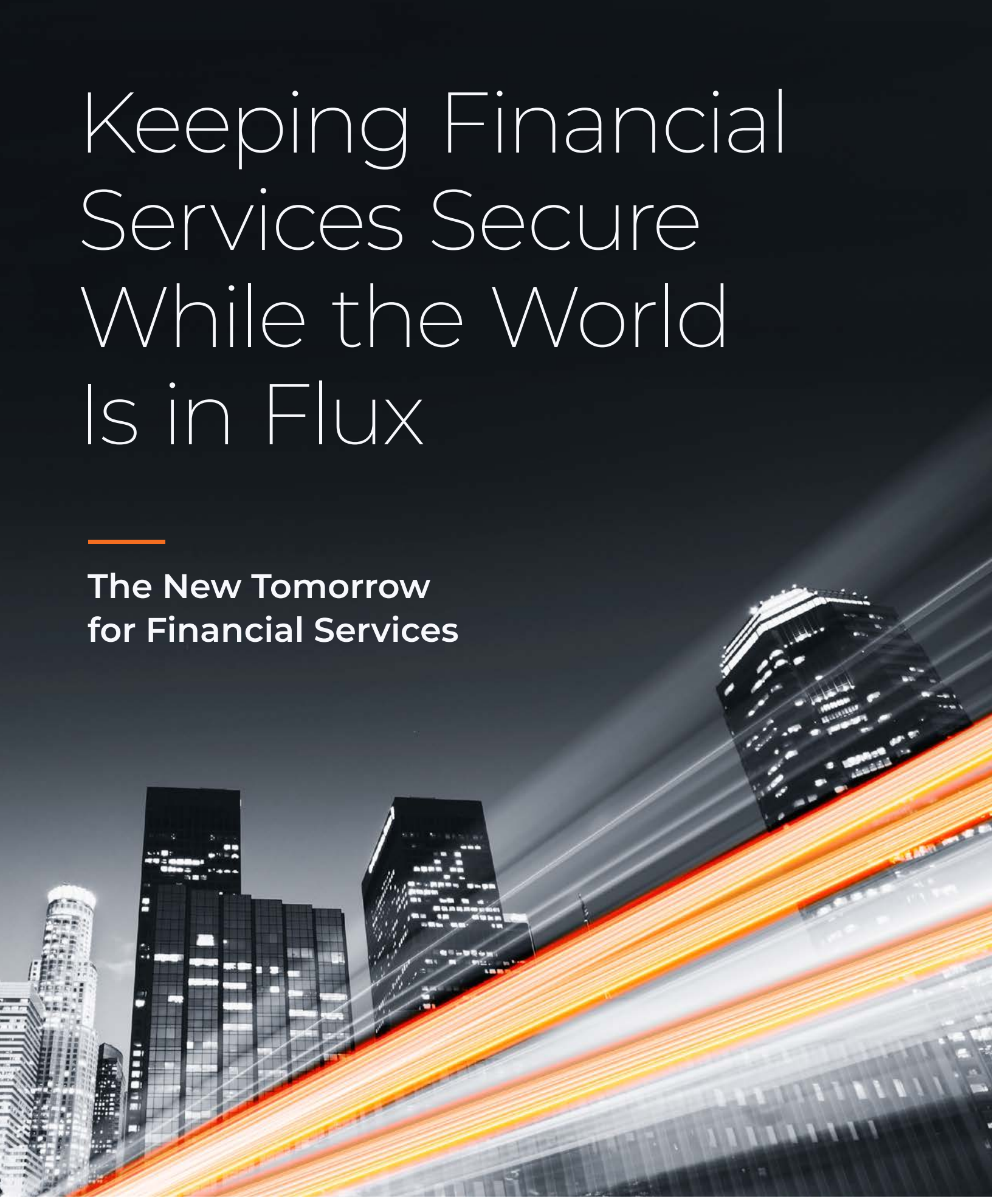
Keeping Financial Services Secure While the World Is in Flux

The New Tomorrow for Financial Services



Gigamon®

Executive Summary

While the financial services industry is well acquainted with the concept of VUCA — volatility, uncertainty, complexity and ambiguity — today's current events define a new reality. Successfully navigating through these turbulent times will require enduring resilience.

This whitepaper discusses the impact of global events on the IT network in financial services, and how NetOps and InfoSec can work together to use visibility, analytics and automation to deliver network agility, security and cost management for the new tomorrow.

For network operations (NetOps) and InfoSec teams, resilience means supporting the organization as it turns inside out to rapidly roll out a work-from-home model. It means shielding company and customer assets from opportunistic cybercriminals eager to take advantage of a rapidly shifting situation, a larger attack surface and an IT team stretched thin. Resilience also means enabling the acceleration of digital transformation to deliver new capabilities today, not months from today. Finally, resilience means doing more with the network and tools than ever before in the face of economic uncertainty.

While the situation in financial services may be fluid for some time, there is a constant for the IT network: the need for performance and security in a rapidly shifting IT environment. To stay in control as the world is in flux, NetOps and InfoSec teams need to maximize network visibility to manage security, performance and reliability, while getting more out of the network, staff and tools.

Resilience means doing more with the network and tools than ever before.

Instant and Ongoing Disruption

The financial services industry is adept at overcoming challenges such as economic and geopolitical shifts, regulatory changes, intense competition from challengers outside of the industry and changing consumer needs. Now the industry is in the midst of sudden and dramatic changes that impact nearly all the "usual" business drivers and disruptors in completely new ways.

WORK FROM HOME

The sudden shift to remote work dramatically increased the pressure on existing IT infrastructure, as previously untested numbers of users and volumes of information began to clog the wide area network (WAN) and virtual private network (VPN). It also created blind spots and increased the attack surface of the enterprise.

INCREASED DEMAND FOR MOBILE BANKING AND DIGITAL SERVICES

To respond to increased customer reliance on mobile applications and digital services, IT organizations had to quickly ramp up capacity for their existing capabilities.

NEW CAPABILITIES

At the same time, companies on a multiyear roadmap for digital transformation are condensing the plan to move up delivery of new capabilities within days or weeks as situations continue to change around the world.

Over the longer term, financial services companies will resume their efforts around:

CLOUD ADOPTION

While financial services organizations were already turning to the cloud to enable modernization and digital transformation, they'll need to further accelerate adoption to increase agility and deliver new capabilities faster than ever.

DISTRIBUTED APPLICATIONS

Modernization projects are another way financial services companies are becoming more agile and responsive. This means modernizing existing monolithic applications by rearchitecting them into microservices, creating a distributed application environment. Monetizing their microservices creates new revenue streams by making functionality available to third parties to use via application programming interfaces (APIs).

ECOSYSTEM/OPEN BANKING

Recognizing that it's faster and more cost-effective to partner with third parties (such as fintechs) to provide customers with the services and products they need and want today, financial services companies are creating ecosystems that offer a seamless customer experience across both in-house and third-party applications.

That's not all. As the new tomorrow takes shape, financial services companies will continue discovering how artificial intelligence, robotic process automation, blockchain and other technologies can help them drive greater efficiency, improve fraud detection, reinvent their business model and much more. For example, robotic process automation can streamline and improve insurance policy issuance and accounts receivable processing.

As everyone adapts to this time of unprecedented change, the technology we depend on has never been more critical or more foundational to our businesses, employees and customers.

A Prime Target for Cybercriminals

Even in the best of times, the financial services sector is one of the most targeted industries for cyberattack. Today, with the world in flux and IT spread thin, attackers see new opportunities to gain access to a rich depository of not only financial accounts but high-value, sensitive data.

Boston Consulting Group reports that "financial services firms are 300 times as likely as other companies to be targeted by a cyberattack — and dealing with those attacks and their aftermath carries a higher cost for banks and wealth managers than for any other sector."[1]

While digital transformation is imperative in today's environment, it also creates new IT complexity and expands the attack surface for cyberthreats — making financial services companies even more susceptible to attack.

Given these sobering facts, financial institutions have been spending an average of around $2,300 on cybersecurity annually per full-time employee, according to a survey conducted by Deloitte and the Financial Services Information Sharing and Analysis Center. The amount equates to between 6 and 14 percent of the IT budget that is spent on cybersecurity. The report also highlighted that higher cybersecurity spending doesn't translate into a higher cybersecurity maturity level.[2]

[1] Zakrzewski, Anna, Tjun Tang, Galina Appell, Renaud Fages, Andrew Hardie, Nicole Hildebrandt, Michael Kahlich, Martin Mende, Federico Muxi, and Andre Xavier. "Global Wealth 2019: Reigniting Radical Growth." BCG. Boston Consulting Group, June 20, 2019. https://www.bcg.com/publications/2019/global-wealth-reigniting-radical-growth.aspx.

[2] "Pursuing Cybersecurity Maturity at Financial Institutions," Deloitte Center for Financial Services and the Financial Services Information Sharing and Analysis Center, May 2019. https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/financial-services/DI_Pursuing-cybersecurity-maturity-at-financial-institutions.pdf.

BY THE NUMBERS

The Impact of Cyberattacks in Financial Services

41%

of U.S. financial institutions experienced a data breach in 2019[6]

62%

of exposed data from breaches in 2019 came from the financial services industry[7]

$388

is the average cost per record of a mega breach, respectively, the second highest cost per breached record after healthcare[8]

66%

of people say they would stop doing business with a financial company that had slow or ineffective communication after a data breach

45%

say they would tell their family and friends to stop doing business with the company[9]

Sources: IDC/Thales, Bitglass, Experian

Lost Revenue and Customers

While downtime or degradation of services in any industry can mean significant negative impacts, for the financial services industry, disruption of service can be devastating. Estimates of annual losses due to cyberattacks across the industry add up to tens of billions of dollars.[3]

The average cost of a data breach across all industries is $3.92 million, including lost revenue, remediation and notification, noncompliance penalties, legal fees and lawsuits. However, the average — at $5.86 million — is far higher for the financial services industry, second only to healthcare. Furthermore, the costs are ongoing over a period of years, with 67 percent of the costs occurring in the first year when the breach happens, 22 percent in the second year and 11 percent occurring after two years post-breach.[4]

Lost business is the biggest contributor to the cost of a data breach, with the average cost across all industries being $1.42 million, which is 36 percent of the total cost. One reason that the average overall cost of a data breach is higher for financial services is that the industry has a greater-than-expected customer turnover rate following a data breach. Financial services companies experience an average of 5.9 percent abnormal customer turnover after a breach compared to the overall average of 3.9 percent for all industries, again second only to healthcare.[5]

[3] "Global Wealth: Reigniting Radical Growth," Boston Consulting Group, 2019.

[4] "Cost of a Data Breach Report 2019," Ponemon Institute, 2019.

[5] "Cost of a Data Breach Report 2019," Ponemon Institute, 2019.

[6] "Thales Study: U.S. Financial Institutions Have Highest Rate of Data Breaches Despite Strict Compliance Mandates," Thales press release, December 2019.

[7] "The Changing Face of Data Security: 2019 Thales Data Threat Report," Thales. Research and analysis from IDC, November 2019. https://go.thalesesecurity.com/rs/480-LWA-970/images/2019-DTR-Retail-ar.pdf.

[8] Lugo, Juan. "The Financial Matrix: Bitglass' 2019 Financial Breach Report." Bitglass. Bitglass, December 16, 2019. https://www.bitglass.com/blog/the-financial-matrix-bitglass-2019-financial-breach-report.

[9] Alix, Laura. "Prompt Notification Would Ease Pain of Data Breaches: Survey." American Banker. American Banker, August 30, 2019. https://www.americanbanker.com/news/prompt-notification-would-ease-pain-of-data-breaches-survey.

The Challenges Facing NetOps and InfoSec

Unprecedented change means unprecedented challenges. For the financial services InfoSec team, it must shoulder even more burden as it focuses on keeping the organization secure and enables business agility. Specifically, the team must:

+ Identify security vulnerabilities in the network and mitigate them
+ Detect and respond to cyberthreats on the network
+ Manage security across an increasingly complex network environment
+ Support security efforts with limited staff as the cybersecurity talent shortage grows
+ Reduce friction with DevOps teams that need to deliver innovation faster than ever before

Likewise, the NetOps team is juggling seemingly competing challenges: managing a dynamic and complex environment, supporting unplanned growth in data and traffic, and delivering network service levels that support the business as it and the world rapidly transform. Therefore, the NetOps team must:

+ Assure the constant resilience, performance and security of IT networks
+ Identify and eliminate potential bottlenecks that impact performance
+ Scale networks quickly to support increased traffic and data volume
+ Manage increasingly complex network environments
+ Do more faster to keep up with the changing IT environment with the same level of staffing

Managing the network and defending it against cyberattack shouldn't be approached in isolation. Yet, without common tools to address their challenges, the NetOps and InfoSec teams often experience friction as well as duplicate efforts and missed opportunities to collaborate.

VISIBILITY AND ANALYTICS: THE COMMON GROUND BETWEEN NETOPS AND INFOSEC

To meet their company's need for security and performance in a rapidly shifting environment and optimize costs with an uncertain budget, NetOps and InfoSec teams should look for a single solution that provides the following capabilities:

+ Real-time visibility into all network traffic to understand and optimize performance and improve security
+ Analytics to optimize and manage network performance to accommodate and secure increasing volumes of data and traffic
+ A single pane of glass that simplifies network and security operations across physical, virtual and cloud environments
+ Threat detection and response to find and remediate threats on the network faster and minimize disruption
+ Automation to free up staff and allow them to do more, faster

Industry analyst group Gartner identifies improvements in visibility and agility as one of the key benefits of what it calls NetOps 2.0, a set of principles that provide "new ways to operate networks" to keep pace with digital business. The firm recommends investing in network analytics and automation to reduce friction and improve collaboration between NetOps, SecOps (InfoSec) and DevOps teams, leading to the reduction of manual effort and streamlined value delivery. Adding network analytics and automation tools helps close the skills gap that exists in most organizations, especially as they move to the cloud as the main deployment platform for new applications.[10]

By aligning NetOps, SecOps and DevOps, Gartner believes that organizations can reduce duplication and friction between these groups, leading to a 25 percent reduction in the time to deliver new applications and services.[11]

[10] "NetOps 2.0: Embrace Network Automation and Analytics to Win in the Era of ContinuousNext," Gartner, October 2019. https://www.gartner.com/en/documents/3970170/netops-2-0-embrace-network-automation-and-analytics-to-w.

[11] "NetOps 2.0: Embrace Network Automation and Analytics to Win in the Era of ContinuousNext," Gartner, October 2019

Final Thoughts

Maintaining control while the world is in flux requires network agility, security and cost management.

To achieve this, NetOps and InfoSec teams need visibility, analytics and automation as their foundational building blocks for an optimized, secure network.

The Gigamon Visibility and Analytics Fabric™ delivers visibility, availability and security solutions that power the highest levels of innovation. It provides a unified visibility architecture across physical, virtual and cloud environments to eliminate blind spots and simplify management, saving time and money and helping businesses stay prepared for the new tomorrow.

TRUSTED BY THE WORLD'S LEADING ORGANIZATIONS

Seven of the top 10 global banks rely on Gigamon, as do hundreds of other banks, insurers, credit unions and regulatory authorities.

About Gigamon

Gigamon is the first company to deliver unified network visibility and analytics on all data in transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation.

In short, we enable you to run fast, stay secure and innovate. Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations, including 80 percent of the Fortune 100. Headquartered in Silicon Valley, Gigamon operates globally.

For the full story on how Gigamon can help you, please visit gigamon.com.

© 2020 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer or otherwise revise this publication without notice.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com