EBOOK

Hybrid Cloud Application Delivery in Financial Services

How Firms are Addressing the Requirements of Digital Transformation, Security, and Compliance

A10

Table of Contents

INTRODUCTION

Financial services organizations are undergoing rapid digital transformation to meet changing customer needs and preferences, and to compete with a new generation of digital-native competitors. Hybrid cloud environments play a key role in this strategy, allowing greater speed, flexibility, and visibility over application delivery than on-premises data centers while reducing costs.

But the move to hybrid cloud introduces new challenges as well. As they plot their strategy for transformation, firms must:

- Make critical technical decisions about the clouds and form factors best suited to host their hybrid environment
- Secure web applications against threats including ransomware, data theft, and DDoS attacks through measures such as a DDoS protection and the Zero Trust model
- Maintain regulatory compliance, governance, and auditability across complex, fast-evolving infrastructures

To gain insight into the current state of financial services technology and its future directions, A10 Networks and Gatepoint Research conducted a survey asking senior decision-makers about their current plans, concerns, and priorities for their hybrid cloud environments, including:

- Where do you host applications?
- Are you planning to migrate more applications to the cloud?
- What are your greatest security concerns?
- Which capabilities are most important for financial platforms running in hybrid cloud?

The results of the survey offer a snapshot of an industry in transition, as decision-makers seek to keep control over security and compliance, and maintain operational consistency, even as they tap into the agility and scalability of the cloud.

TODAY'S FINANCIAL SERVICES TECHNOLOGY LANDSCAPE

The survey shows financial services are between businesses and making a steady move to the cloud for application delivery, although on-premises data centers continue to play an important role.

The Traditional Data Center Is Very Much Alive

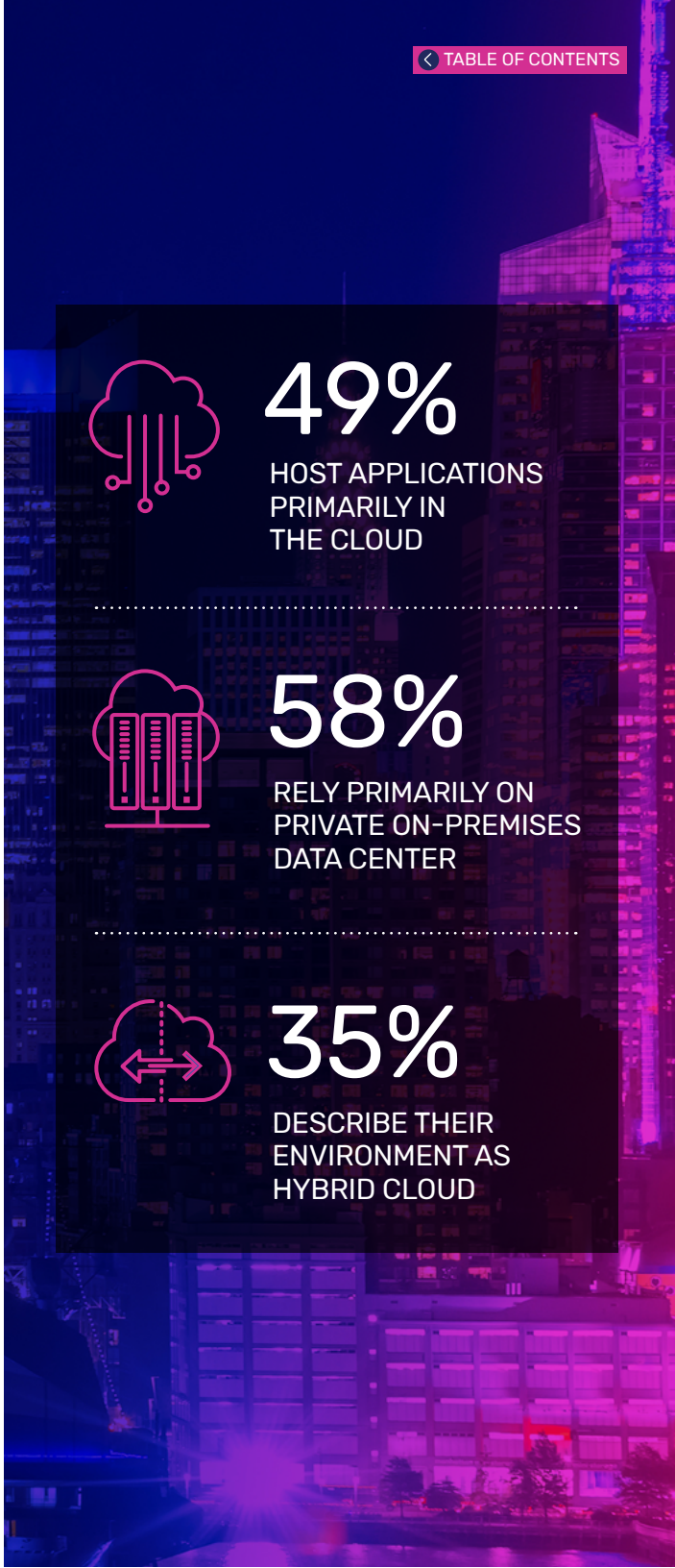
Although adoption of public cloud infrastructure is strong, with almost half of those surveyed (49 percent), hosting applications primarily in the cloud, a majority of respondents (58 percent) continue to rely primarily on their private on-premises data center for application delivery. 35 percent of organizations described their environment as hybrid cloud, though with an emphasis on their own private data center. All in all, these responses show that even as transformation continues, the traditional data center remains prominent in financial services technology strategy.

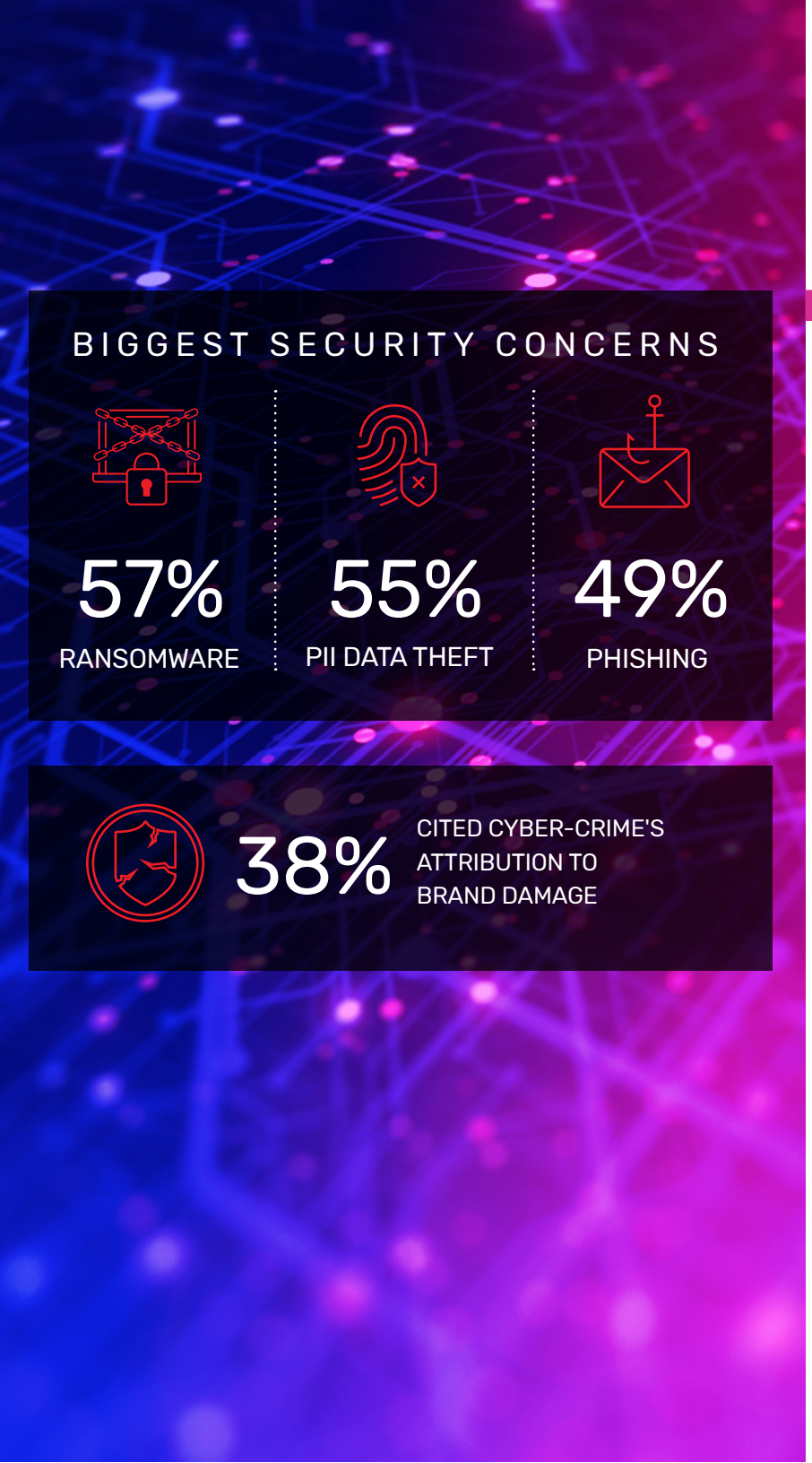
Cloud Adoption Is Increasing for Application Delivery

The balance between on-premises and cloud infrastructure may well continue to shift in the near future. Asked about their plans for the coming year, 57 percent of decision-makers reported that they intend to move more applications to the cloud.

Traffic Is Steady—Or Surging

While half of respondents reported "business as usual" under COVID-19 in terms of application services traffic from customers, nearly as many (47 percent) reported rising demand, with 22 percent seeing an increase of more than 10 percent. Meanwhile, only 3 percent have seen traffic decrease—while 5 percent have seen a dramatic jump of 51 - 100 percent.





RANSOMWARE AND PII THEFT LEAD SECURITY CONCERNS

Financial services organizations today face a broad spectrum of security threats, including many targeting sensitive customer data. Asked about their biggest security concerns or consequences, respondents named ransomware (57 percent), personally identifiable information (PII) data theft (55 percent), and phishing or fake sites (49 percent).

Brand Concerns Run High in Financial Services

While threats to customers and their data ranked highest, dangers to the company's brand image and reputation followed not far behind. 38 percent of leaders cited concerns about hacking and cyber defacement, tied with brand damage and loss of confidence.

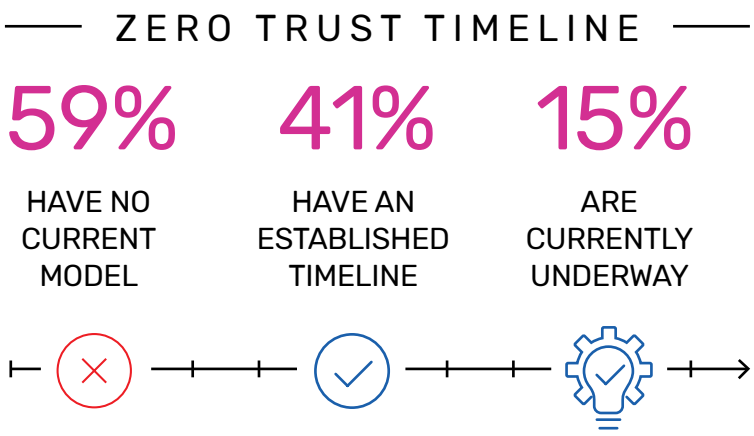
Nearly as many (37 percent) were concerned about DDoS attacks, which can undermine a firm's perception among customers through impaired service quality and customer experience.

Meanwhile, insider attacks remain an issue, named by 28 percent of respondents, if not quite at the same level as most external threats.

ZERO TRUST MODEL COMES ONTO THE HORIZON

To address the changing security landscape, many organizations have begun initiatives around the Zero Trust model, in which traditional concepts of secured zones, perimeters, and network segments are updated with a new understanding that a threat can come from anywhere or anyone inside or outside the organization.

As of June 2020, 41 percent of respondents had already established a timeline for their Zero Trust model initiative with 15 percent having projects currently underway. Still, nearly two-thirds (59 percent) have no current plans or initiatives around the Zero Trust model.



MOVING TO IMPROVE FLEXIBILITY, AGILITY, SCALABILITY—AND SECURITY

Technologies and strategies planned for the coming year reflect a key focus on the competitive requirements of fast-paced digital markets. The top-two initiatives, each cited by 34 percent of respondents, were moving from hardware appliances to more flexible software form factors; and deploying hybrid cloud automation, management, and analytics to increase operational efficiency.

Strengthening DDoS Protection —and Catching Up on TLS

With DDoS attacks a prime concern, 29 percent of respondents planned to deploy or replace an existing web application firewall (WAF) or DDoS protection solution. Surprisingly, even several years after the introduction of modern Perfect Forward Secrecy (PFS) and Elliptical Curve Cryptography (ECC) encryption standards for enhanced security, a full 29 percent of organizations were only now working to upgrade their Transport Layer Security (TLS) capabilities to support these technologies.

Look Before You Leap to the Cloud

Even as cloud adoption continues to be strong, 5 percent of decision-makers intend to repatriate applications from private cloud environments to their private data center. While not a high number, this is not entirely insignificant. Given the diversity of form factors, architectures, and deployment methods to choose from, it's clearly important to make sure that the approach fits the organization's needs before proceeding.

ADDRESSING THE REQUIREMENTS OF HYBRID CLOUD AND RISING DEMAND

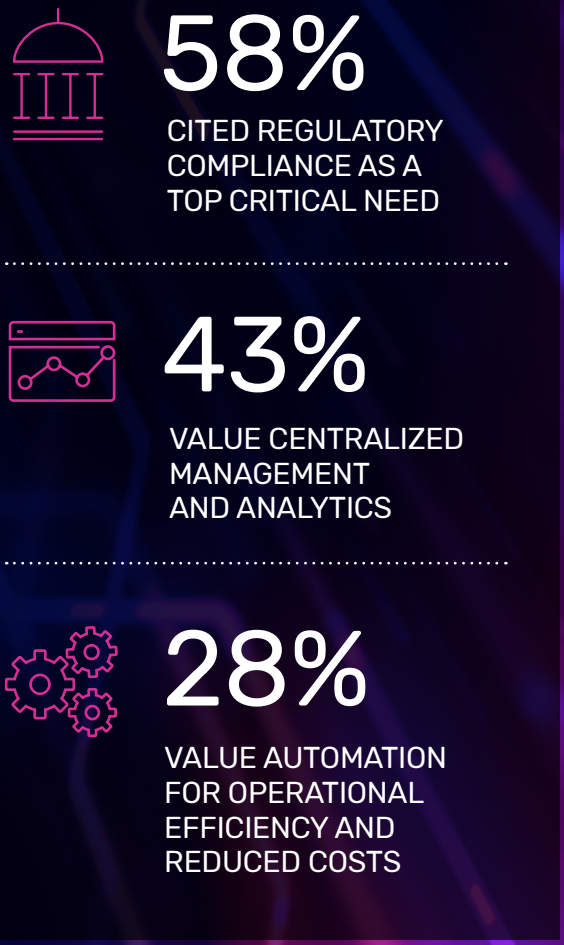
Moving forward, decision-makers view capabilities related to risk as especially important for their financial platforms. Asked about the most important capabilities for financial platforms running in hybrid cloud environments, 58 percent agreed that regulatory compliance is a top must-have. Nearly half of respondents included comprehensive application security and redundancy/disaster recovery in their top-three list.

Ensuring Consistent Application Delivery

In addition to the importance placed on redundancy/disaster recovery, many respondents (43 percent) named centralized management and analytics as important capabilities. Along with elastic scale for variable/seasonable demands (25 percent), this shows a recognition of the requirements to provide an effective service through redundancy, scalability, and a sound infrastructure.

Cost Is a Consideration—If Not a Top Priority

Compared with risk-related and operational priorities, cost saw considerably less emphasis in the survey. While 28 percent of respondents placed importance on automation for operational efficiency and reduced costs, just 18 percent prioritized flexible licensing and pricing.



DESIRED BENEFITS FROM NEW TECHNOLOGY INVESTMENTS

As they plan new technology investments, decision-makers are motivated foremost by risk reduction—far outpacing business factors such as revenue, customer experience, and competitive advantage.

Sound Operations First—Then Financial Services Business Advantage

By a large majority (74 percent), security was the most likely benefit to spur funding for new technology. Operational considerations followed, including operational improvements (65 percent) and cost savings (63 percent). Regulatory compliance, emphasized earlier in the survey as a priority for a hybrid cloud requirement, was not necessarily top-of-mind in the technology funding stage—but still of high importance (57 percent).

Innovations designed to impact business performance weren't ranked quite as highly. Revenue generation was named as a highly important benefit by only 35 percent, followed by customer satisfaction at 32 percent. Even in an industry undergoing rapid digital transformation, just 32 percent of decision-makers cited business advantage from new technology as a prime factor—and only 17 percent were moved by the ability to accelerate development speed.

METHODOLOGY

Between April and May 2020, Gatepoint Research invited selected IT executives to participate in a survey themed Financial Services Technology and Hybrid Cloud Application Delivery Trends. Candidates were contacted via email and 65 executives have participated to date, including 5 percent holding the title CxO, 35 percent VPs, 48 percent directors, and 12 percent managers.

Survey participants represent firms in the financial services sectors, and work for firms with a wide range of revenue levels:

- 22 percent work in Fortune 1,000 companies with revenues over $1.5 billion
- 25 percent work in large firms whose revenues are between $500 million and $1.5 billion
- 11 percent work in mid-market firms with $250 million to $500 million in revenues
- 42 percent work in small companies with less than $250 million in revenues

About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit www.a10networks.com and follow us @A10Networks.

LEARN MORE
ABOUT A10 NETWORKS

CONTACT US
a10networks.com/contact

Part Number: A10-EB-14134-EN-01 August 2020