PYMNTS | AMERICAN EXPRESS

March 2023

How SMBs Can Fight the Fraud Threats of Remote Work

B2B and Digital Payments Tracker® Series

■ Read the previous edition

JANUARY 2023

B2B and Digital Payments Tracker® Series

What's Inside

PYMNTS | AMERICAN EXPRESS

Acknowledgment

The B2B and Digital Payments Tracker® Series is produced in collaboration with American Express, and PYMNTS is grateful for the company's support and insight. PYMNTS retains full editorial control over the following findings, methodology and data analysis.

© 2023 PYMNTS All Rights Reserved

Need to Know

New Work Trends Bring Security Risks

Hybrid work models have been a positive development for many companies and their employees. Remote working, whether from home or a coffee shop, provides flexibility and often saves costs for commuters as well as reducing businesses' needs to acquire additional space. The rise of remote work, however, has brought with it new challenges related to security.

Unsecured Wi-Fi networks, software weaknesses and employees' poor cybersecurity habits leave organizations exposed to external actors seeking to exploit any vulnerability. Existing fraud prevention measures have proven no match for remote working, which makes it more difficult for businesses to monitor employee behavior and increases fraud risk.

Remote work has exacerbated companies' fraud and cybersecurity concerns.

86%

Share of companies that say remote working has negatively affected fraud prevention at their organizations

50%

Share of companies that say working from home has negatively impacted their ability to respond to fraud

Need to Know

Business travel is taking off, but fraud risks abound.

Remote work also serves as a prime setting for internal, or occupational, fraud, which is fraud committed by employees themselves. The return of business travel since the pandemic grounded most trips, for example, is creating growth in travel and expense reimbursement fraud. This fraud is costly, especially since many incidents take about 18 months to be noticed. On average, an organization can expect to lose $152,000 from a single expense fraud scheme. Among the highest-risk areas of expense fraud are conference registrations, business meals, hotels, transportation, mileage and miscellaneous expenses.

Occupational fraud is costly and spreading throughout organizations.

85%

Share of reported occupational fraudsters who display behavioral red flags

29%

Share of reported occupational fraud that occurs due to lack of internal controls

Need to Know

Navigating new work fraud threats is especially challenging for SMBs.

Managing the new work environment's escalated threats can be a particular challenge for small to mid-sized businesses (SMBs), with budget constraints and sparse security teams serving as major obstacles. More than two-thirds of SMBs have security teams of fewer than five individuals, and 67% spend less than $50,000 per year on cybersecurity. Although 59% plan to increase their security budgets this year, an almost equal share — 57% — worry that inflation will cut into these plans and necessitate budget cuts. To address resource limitations, 58% are turning to third-party security management.

Fraud management is an issue for nearly all companies, but SMBs find it particularly difficult.

91%

Share of companies that regard fraud management as a challenge

68%

Share of SMBs that have security teams consisting of fewer than five individuals

59%

Share of SMBs that plan to increase their security budgets this year

57%

Share of SMBs that worry inflation may cut their plans to increase security budgets this year

News and Trends

Recognizing the Stakes, More SMBs Get Serious About Security

More SMBs are taking steps to guard against bad actors, and they are not afraid to allocate more budget to fight fraud. A recent report found that security represents a significant portion of most SMBs' IT budgets, with 42% of SMBs increasing their IT security allocations. With ransomware a prominent threat, antivirus software and email/spam protection are the leading solutions chosen by SMBs, at 57% and 53%, respectively. In the next year, network security, cloud security and cyberinsurance are where most SMBs plan to invest.

Share of SMBs with cyberinsurance that think a ransomware attack will happen in the next year

Share of SMBs without cyberinsurance that think a ransomware attack will happen in the next year

Card-not-present fraud grows along with eCommerce

As eCommerce has grown, so has card-not-present fraud (CNP). Accounting for $9.5 billion in losses, CNP fraud now represents the leading type of credit card fraud and will comprise 73% of card payment fraud this year, a 57% increase from 2019.

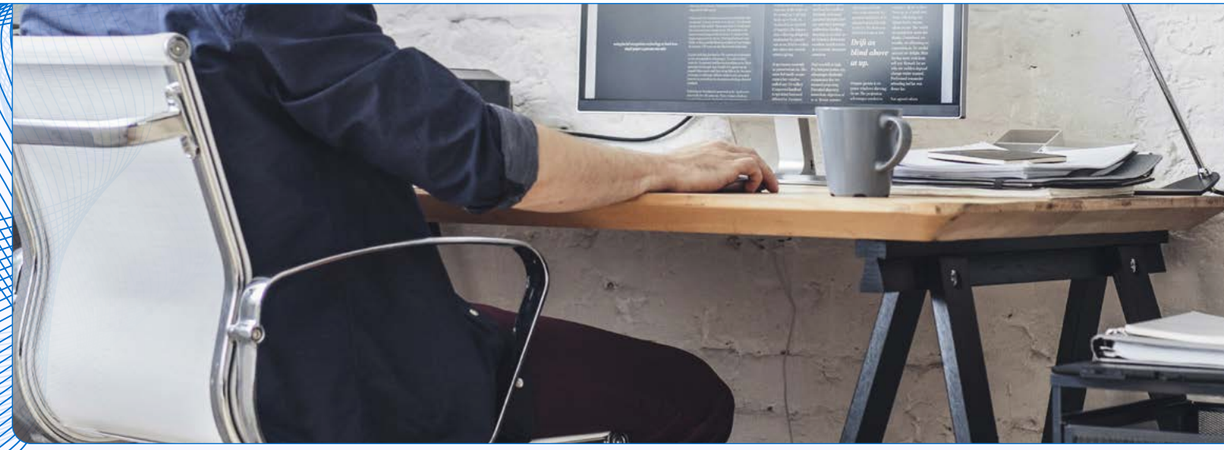
While eCommerce sales and CNP fraud losses are expected to normalize through the next few years, it is vital for merchants and issuers to identify ways to address heightened security for these specific channels. The pandemic's acceleration of eCommerce means that more fraudsters and more types of fraud are on the horizon.

PYMNTS Intelligence

How SMBs Can Fight the Fraud Threats of Remote Work

Remote working was a boon to businesses during the pandemic, as technology allowed many companies to remain productive when much of the world was shutting down. Along with greater technological dependence, however, came greater threats to organizations, such as cyberattacks, data breaches, fraud, bribery and corruption. The widespread use of personal devices, unsecured networks and unprotected software created a broad attack surface through which bad actors could prey on employees, posing significant risks to whole organizations.

While external threats such as cyberattacks emerged as the single most disruptive fraud risks during the digital shift, remote work also put companies at greater risk from internal threats. When misconduct was the most disruptive fraud type, it was more than twice as likely to come from internal than external sources. More importantly, unintentional internal threats arising from human vulnerability — including poor security habits and susceptibility to social engineering tactics — work hand in hand with external threats to form the most common cause of data breaches.



PYMNTS Intelligence

Greater security challenges in a remote work environment

While research finds that 88% of SMBs are concerned about damaging attack vectors such as ransomware, the initial compromise in a remote work environment generally comes from employees clicking on malicious links or unwittingly providing credentials to bad actors. Breaches often result from fraudsters deceiving employees with phishing schemes seeking personal information. The primary source of payments fraud, meanwhile, is business email compromise (BEC), in which criminals pose as legitimate entities or executives to mislead employees into making fraudulent business-to-business (B2B) payments.

Remote work presents increased security challenges for companies.

Physical distance makes it harder to maintain regular processes and control.

The use of less-secured home Wi-Fi, remote desktop applications and personal devices presents new opportunities for fraudsters to gain access to sensitive payment systems and data.

The risk of insider fraud increases, with employees' actions less visible when working remotely.

Invoice fraud, for example, involves the diversion of payments through replica emails made to look as if they come from familiar suppliers or other known sources. A recent report noted that U.S. businesses are losing an average of $300,000 per year to invoice fraud, with 25% of finance professionals unable even to hazard a guess at these losses due to opaque processes and sloppy paper trails.

PYMNTS Intelligence

Business travel elevates risks

With business travel taking off again, more employees are using devices and networks that are not secure. Companies with more employees working remotely face greater costs resulting from data breaches, and the U.S. has emerged as the biggest target for fraudsters. With two in five remote employees transferring unsecured data from their company's system to personal accounts, vulnerabilities can be nearly impossible to avoid. Employing zero-trust access with multifactor authentication is crucial in this environment, and with bring-your-own-device models growing 58% since 2020, companies must address remote policies and monitoring, or else risk employees' data security.

PYMNTS Intelligence

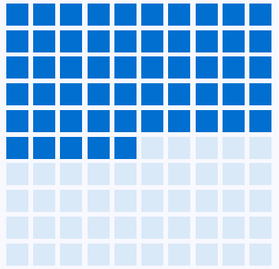
How SMBs can shore up their defenses

Unfortunately, most businesses still rely on single-factor usernames and passwords for user authentication. With leaked credentials such as these regularly available to criminals on the dark web, the first step businesses should take to secure their remote workforces is to implement multifactor authentication. A similar due-diligence strategy to mitigate BEC fraud would involve confirmation of payment requests before money transfers are possible. Staff training is also essential to raise awareness of phishing and BEC schemes as well as best security practices such as good password hygiene.

Finance, IT and security teams must work in concert to protect payment systems beyond the standard network, server and data security, automating processes to allow for no errors. Technology partners can help alleviate costs for SMBs. Companies that adopt a proactive, multilayer approach to securing their distributed workforces will be best prepared as the new work landscape continues to unfold.

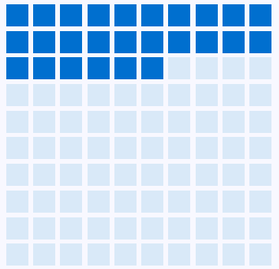
55%

Share of U.S workers who admit to taking a risky cybersecurity action



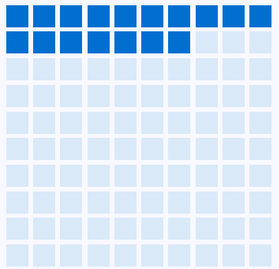
26%

Portion of U.S. workers who have clicked suspicious email links leading to dangerous websites



17%

Share of U.S. workers who have accidentally compromised their credentials



50%

Portion of U.S. workers who can accurately define the term “phishing”

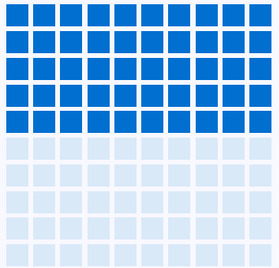
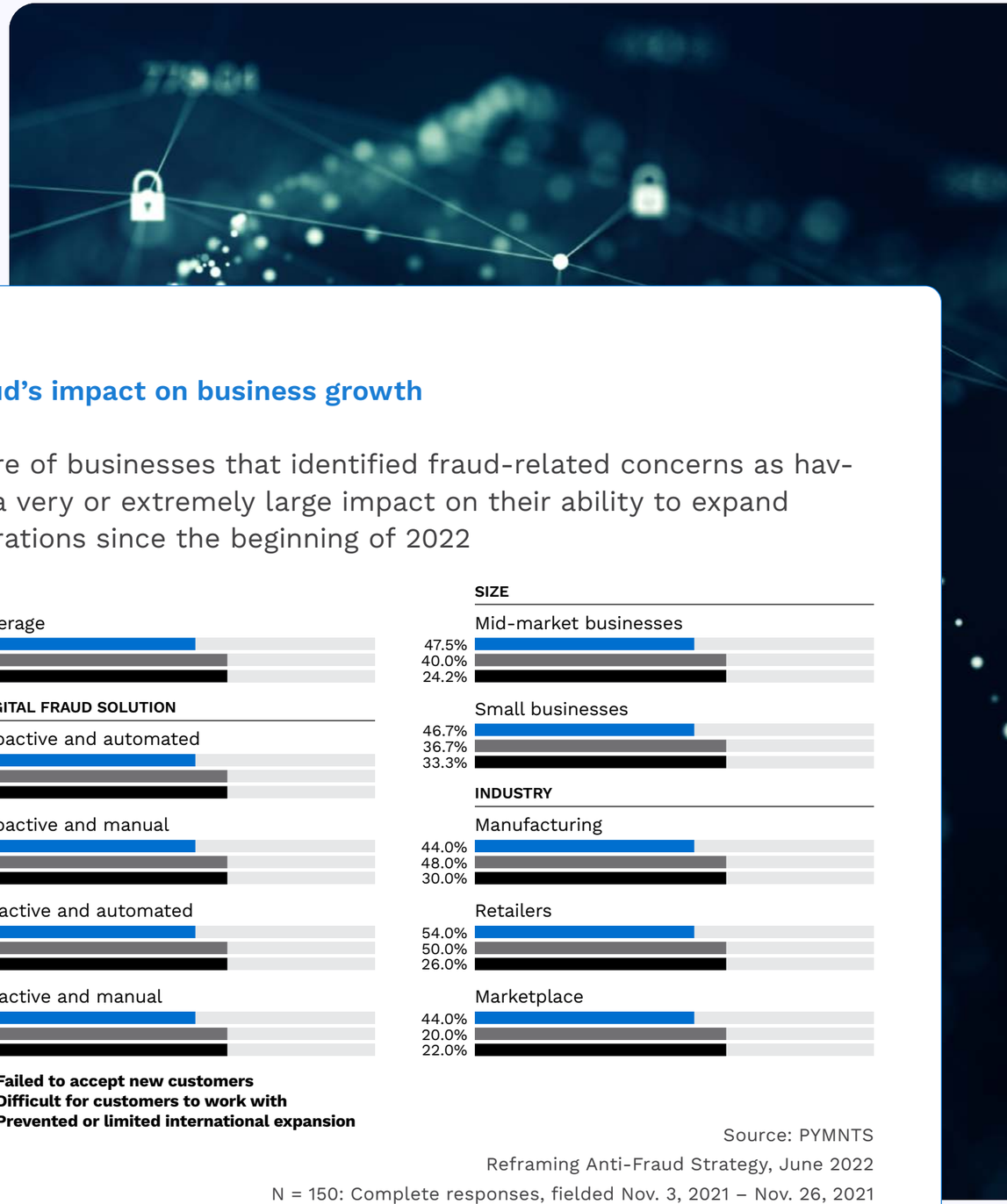


Chart of the Month

Fraud-Fighting Automation Makes All the Difference to SMBs' Growth

Fraud is about as unforgiving a hurdle as companies must face. In fact, fraud-related concerns are more likely to stunt the growth of small businesses than mid-market counterparts, according to PYMNTS research. One in three small businesses saw their international expansion plans prevented or limited. Those organizations that are proactive about addressing how they fight fraud and employ automation stand a far greater chance of maintaining their growth plans, with only 5% reporting that digital fraud thwarted overseas growth. They are also better at acquiring new customers and can offer a more frictionless experience.



Fraud's impact on business growth

Share of businesses that identified fraud-related concerns as having a very or extremely large impact on their ability to expand operations since the beginning of 2022

Source: PYMNTS

Reframing Anti-Fraud Strategy, June 2022

N = 150: Complete responses, fielded Nov. 3, 2021 – Nov. 26, 2021

Insider POV

As Remote Work and Travel Normalize, SMBs Tackle Challenge of Payment Fraud

Michael Nardy, founder and CEO of Electronic Payments, explains why having a trusted partner for payments protection is so important to SMBs.

MICHAEL NARDY
Founder and CEO

ElectronicPayments®

> **One of the biggest things we've seen is [that] merchants sometimes are not willing to understand that a credit card merchant account is not just this thing they can get from their local sales rep but [that] it requires a level of expertise [to] implement this particular payment solution properly.**

Michael Nardy admits his recent family vacation to England was his first leisure trip to Europe. For the founder and CEO of a globally recognized merchant services provider, he mentions this somewhat apologetically. The trip, however, which featured ample shopping opportunities with his two daughters, revealed a bit about the future of payments.

He hopped on a bus with a simple tap-on screen that registered his fare. Most stores his family shopped in did not accept cash, and ATMs were virtually nonexistent. He could send a payment to someone on his contact list from simply connecting it to his payment card via his mobile phone.

Insider POV

"It's almost [like] if you didn't have a payment card, whether it's tied to a bank or credit line, you couldn't function," Nardy said. "That's just going to accelerate faster. And we'll see what kind of fraud comes with that."

Since remote work has become normalized and more people — like Nardy — are traveling for business and pleasure, bad actors have had ample opportunity to fine-tune their methods and force businesses across many industries to focus more on digital fraud prevention. Fraudsters, however, have a knack for catching up to technology.

As more advanced digital solutions move into the point of sale (POS), merchants must take a pragmatic view of protecting their transactions and customers. Through a quarter-century of growing Electronic Payments, that is exactly how Nardy has approached providing payment processing, POS and technical support for SMBs across the U.S. and internationally. Electronic Payments now boasts a staff of 150, a network of more than 1,000 agents and a successful combination of cutting-edge technology, transparency and dedicated service.

Fraud has been especially problematic as merchants have dealt with successive headwinds like the pandemic, supply chain disruptions and rising inflation. Merchants need money coming in, and they will do just about anything, Nardy said, to ensure they can receive a payment — even if it might bear the earmarks of fraudulent activity. He sees a leveling off from pandemic-fueled spikes in fraud among his company's merchants as they have adopted new fraud-fighting technologies, whether a properly formulated online shopping cart with 3D Secure or American Express's Safe Key. Many issues still persist, though, such as peer-to-peer (P2P) payment fraud.

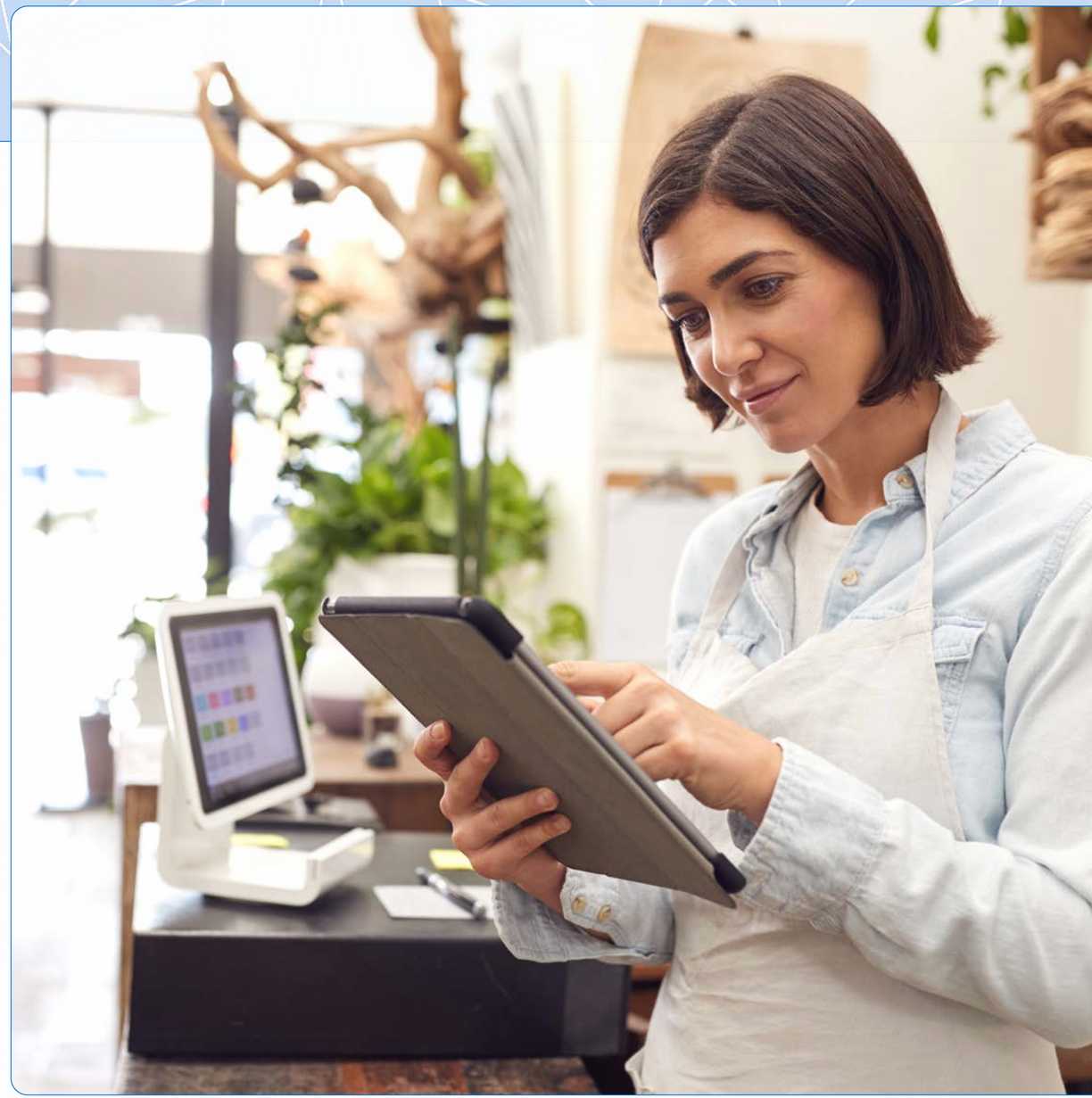
Smaller retailers and mom-and-pop shops seem to struggle the most in keeping up with fraud because they are often so distracted by day-to-day operations and so dependent on revenue coming in that they are unable to recognize an attack that could be prevented with the right help. Nardy noted how posting a simple electronic payment link on a website — one that might be without IP filtering, for example — can be downright devastating, considering how easily card-testing fraudsters can access and utilize the payment link to do their dirty work.

Insider POV

It is for this reason that Nardy brings a boutique approach to clients, aiming to fully understand their specific businesses and potential vulnerabilities and fully educating them on how they can play a role in defending their revenue. When he founded Electronic Payments, Nardy was barely 20 years old, and he would talk to every potential customer about their pain points.

Nardy believes that merchants, especially if they do not have the time or expertise, need to find someone who does to help them navigate payment options and fraud defense. Trust is key, and being open to a conversation with a consultant can pay huge dividends, especially for those companies with remote operations or frequent business travel.

“It’s really our job as the acquirer to assist that customer and explain to them and say ‘Look, you got this chargeback because you took this type of payment and you didn’t have this particular technology or you didn’t do it in this particular [fashion]. So let’s work with you to fix that problem so it doesn’t happen again,’” Nardy said.



© 2023 PYMNTS All Rights Reserved

Companies to Watch

New Fraud Defense Tools for SMBs

TD SYNNEX

As threats within cloud environments proliferate, TD SYNNEX launched its fraud defense tool, SMB Fraud Defense Click-to-Run, which integrates with Microsoft Azure services for SMBs and helps solidify security posture to mitigate potential risks. By integrating Microsoft Azure Active Directory, organizations can enforce Conditional Access policies to improve control of how corporate resources are accessed.

CISCO

For better protection of hybrid work and the multicloud environments that connect employees wherever they are, Cisco introduced new risk-based capabilities to its security portfolio to mitigate vulnerabilities and remove friction across organizations' entire IT ecosystems. Cisco's Risk-Based Authentication helps strike a balance between usability and security via real-time contextual signals, and its industry-first Business Risk Observability tool enhances Cisco's Full-Stack Observability solution.

What's Next

Remote Work Will Expand Even More in Coming Years

Remote work is becoming less of a trend and more of a permanent fixture in the modern business environment. Working away from the office has proven so successful and beneficial to both companies and employees that the anticipated growth rate for full-time remote working has more than doubled from 30% to 65% through 2025. Some 62% of hiring managers are planning for their teams to be more remote in the future. Considering how technology issues are the leading problem for remote work, companies that are able to partner with the right solution providers and effectively train their employees will have the best experiences working away from the office.

32%

Share of hiring managers who found productivity has increased with remote work

56%

Share of hiring managers who believe the shift to remote work has gone better than anticipated

© 2023 PYMNTS All Rights Reserved

About

PYMNTS

PYMNTS is where the best minds and the best content meet on the web to learn about “What’s Next” in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

AMERICAN EXPRESS

American Express is a globally integrated payments company, providing customers with access to products, insights and experiences that enrich lives and build business success. Learn more at americanexpress.com, and connect with us on Facebook, Instagram, LinkedIn, Twitter and YouTube.

Key links to products, services and corporate responsibility information: charge and credit cards, Business Class for Merchants, business credit cards, travel services, gift cards, prepaid cards, merchant services, Accertify, InAuth, corporate card, business travel and corporate responsibility.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at feedback@pymnts.com.

Disclaimer

The B2B and Digital Payments Tracker® Series may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED “AS IS” AND ON AN “AS AVAILABLE” BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS is the property of PYMNTS and cannot be reproduced without its prior written permission.

The B2B and Digital Payments Tracker® Series is a registered trademark of What’s Next Media & Analytics, LLC (“PYMNTS”).