Whitepaper

Inside IT Decision-Makers' Minds: Security & Compliance in the Hybrid Workforce

DIZZION

Introduction: The Evolution of Hybrid Work Environments

The rise of hybrid work environments has become pivotal in the modern workplace, reshaping how and where we work. Today, 83% of the global workforce is championing a revolutionary hybrid work model, blending remote work with in-office collaboration, as cited by Accenture.[1]

Contrary to some expectations that the work-from-home trend would eventually become a thing of the past, this change raises concerns about security and compliance, emphasizing the critical need for stringent cybersecurity measures. This white paper is designed to guide you through the maze of security and compliance challenges that hybrid work brings.

In this guide, we will delve into:

Key priorities of IT decision-makers and top trends shaping the future of work

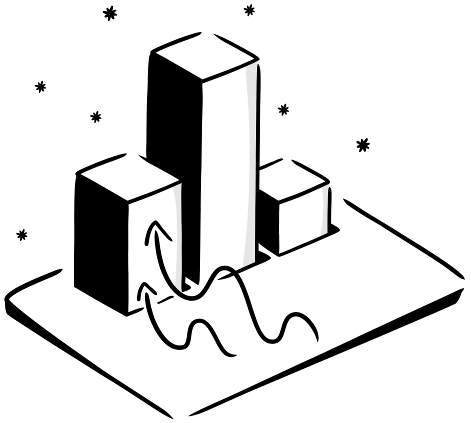
How digital workspaces, security, and compliance come together for a safe hybrid work environment

Top IT initiatives for the next 12 months and how they'll redefine your approach

[1] Accenture, "Future of Work 2021 Research," November 29, 2022, https://www.accenture.com/us-en/insights/consulting/future-work.

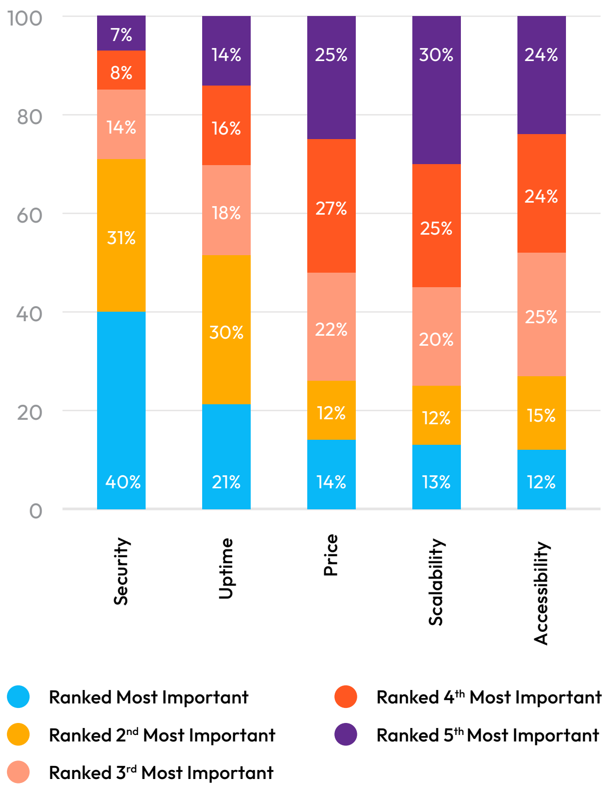
Inside IT Decision-Makers' Minds: Revealed Priorities

To better understand how IT leaders are navigating this new landscape, Foundry Research conducted a Rapid Response MarketPulse Survey on behalf of Dizzion and VMware. The survey collected responses from 147 senior IT decision-makers across North America within organizations with 500 or more employees. Conducted online in July 2023, the survey provides a comprehensive snapshot of the current trends and priorities shaping IT strategies in the era of hybrid work.



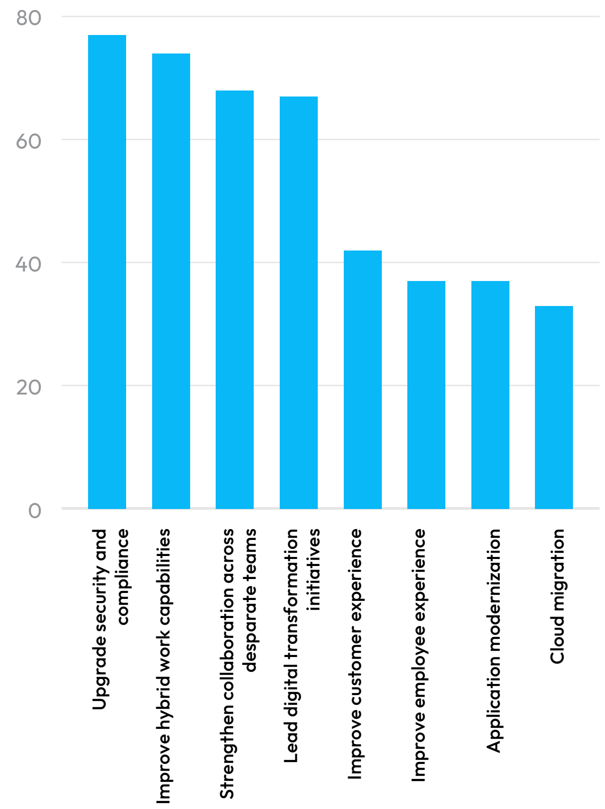
Key Findings from the Survey

Priorities for End Users (including retail locations, third-party contractors, developers, etc.)



Security and uptime are considered the most important factors by IT decision-makers when evaluating technology solutions for end users.

Top IT Initiatives Over the Next 12 Months



Over the next year, security, hybrid work capabilities, and digital transformation are the key priorities for IT decision-makers.

Biggest Trends Impacting Organizations Over the Next 12 Months

Presented According to Average Rank (In order of importance, from highest to lowest)	Ranked #1	Ranked #2 or #3	Ranked #4 or #5	Ranked #6, #7 or #8
#1 Supporting a hybrid workforce	13%	31%	26%	30%
#2 Accelerated digital transformation	10%	32%	27%	31%
#3 Strategic planning for the future	17%	23%	23%	37%
#4 Immersive customer experience	11%	24%	31%	34%
#5 Increasing cybersecurity	15%	24%	25%	36%
#6 Inflation and supply chain	12%	24%	27%	37%
#7 Regulatory requirements	12%	23%	23%	42%
#8 Offshoring talent	10%	17%	18%	55%

Several trends are set to shape the technology landscape over the next 12 months, with supporting a hybrid workforce and accelerated digital transformation at the forefront.

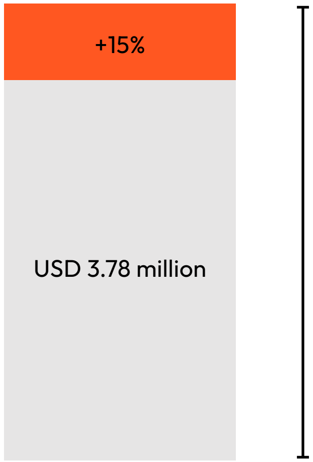
These findings set the stage for the subsequent sections of this white paper, which delve deeper into the implications of these trends and offer actionable insights for organizations navigating the evolving technology landscape.

Why Your Hybrid Team Needs a Secure Digital Workspace

In a world where hybrid work models have become the norm, digital workspaces are the foundation that enables teams to collaborate seamlessly, regardless of physical location. These virtual environments go beyond mere convenience; they ensure that employees can securely access their work resources, applications, and data, whether they're working from the office, home, or elsewhere. But what exactly makes secure digital workspaces so crucial?

The Stakes Are High: A Glimpse into the Numbers

Recent reports highlight the increasingly critical role secure digital workspaces play in safeguarding businesses. According to the IBM Data Breach Report 2023, the average cost of a data breach has reached an all-time high of USD 4.45 million.[2] This financial wake-up call amplifies the need for robust security measures, especially in a hybrid landscape where endpoints multiply.



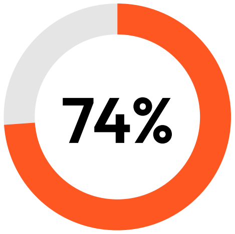
The global average cost of a data breach in 2023 was **USD 4.45 million,** a **15%** increase over 3 years.[3]

Beyond the Cost: The Ripple Effects of Breaches

Data breaches and non-compliance issues have consequences that go beyond financial losses. They can harm a company's reputation, erode customer trust, and result in legal troubles that can be very damaging. For example, failing to comply with industry-specific regulations like HIPAA and PCI can lead to hefty fines and legal consequences. This situation becomes even more critical considering that 67% of IT decision-makers, according to the survey, are leading digital transformation initiatives. In a world where transformation and vulnerability go hand in hand, secure digital workspaces are a must.

Guardians of the Hybrid Realm

Think of secure digital workspaces as the guardians of your hybrid work environment. They go beyond making remote work possible for employees; they help protect your organization against the looming threat of cyberattacks. Data encryption, secure remote access, and identity management are their shields, while compliance reporting and third-party app management stand as their vigilant watchmen. With a robust digital workspace in place, your organization can confidently tackle today's cybersecurity challenges that come with hybrid work.



of all breaches involve the human element,[4] highlighting the need for identity and access management within digital workspaces that minimize these risks.

[2] IBM, "Cost of a Data Breach Report 2023," https://www.ibm.com/reports/data-breach.

[3] Ibid.

[4] Verizon, "Verizon 2023 Data Breach Investigations Report," https://www.verizon.com/business/resources/reports/dbir.

Navigating Third-Party Apps Management Challenges

Managing third-party apps is an integral part of maintaining a secure digital workspace. These applications can enhance productivity and streamline operations, but they also presents significant challenges, including introducing new security vulnerabilities that can lead to data breaches and non-compliance issues.

The challenges associated with third-party apps management are multifaceted. They range from ensuring data security and maintaining regulatory compliance to exerting control over the third-party applications used within an organization. Each app, depending on its security posture, can expose your organization to varying degrees of risk.

Adding to these complexities, an alarming 82% of breaches involved data stored in the cloud—public, private or multiple environments.[5] This statistic underscores the need for organizations to seek solutions that provide visibility across hybrid environments and protect sensitive data as it moves across clouds, databases, apps, and services.

Secure digital workspaces offer a solution to these challenges by providing a controlled environment where third-party apps can be effectively managed. They enable IT departments to monitor app usage, enforce data encryption and security policies, and rapidly respond to potential threats. This level of oversight is crucial for identifying potential vulnerabilities and taking proactive measures to mitigate them. In the age of cloud dominance, securing your digital workspace is not only necessary, but a business imperative.

[5] IBM, "Cost of a Data Breach Report 2023," https://www.ibm.com/reports/data-breach.

Dizzion: Enabling Secure Hybrid Workspaces

As you navigate the world of secure digital spaces, Dizzion emerges as a reliable go-to solution provider. Established in 2011, Dizzion delivers digital workspaces to help your organization flexibly engage hybrid, distributed, and third-party teams at scale, unlocking the modern workforce. Our digital workspace solutions free your IT team from the cost and complexity of delivering and securing a high-performing digital user experience. We respect the trust our clients and partners place in us to build and manage your team's digital workspaces. We've built our organization to match that responsibility with proactive service from a team that you can rely on.

Dizzion's Offerings and Significance in Hybrid Work and Security

Dizzion's proven end-user cloud platform is tailored to maximize work-from-anywhere success while safeguarding organizations across various sectors, including business process outsourcing, financial services, healthcare, and insurance. With real HIPAA, PCI-DSS, NIST 800-53, SOC 2 Type II, and GDPR compliance, Dizzion ensures that your organization's sensitive data remains protected, no matter where your employees are located.

Dizzion's Approach to Security and Compliance

Here are some key features that set Dizzion apart:

Advanced Encryption:
Dizzion employs advanced encryption techniques to secure your data both in transit and at rest, ensuring confidentiality and protection from threats.

Secure Third-Party App Management:
Dizzion provides robust tools for managing third-party applications within your workspace, maintaining control over software to reduce security risks.

Report on Compliance (ROC):
Dizzion offers comprehensive compliance reporting features that make it easy for your organization to stay on top of regulatory requirements such as HIPAA and PCI-DSS.

Identity and Access Management:
Dizzion ensures only authorized users can access your digital workspace and corporate data.

These features create a secure, compliant, and highly efficient workspace, allowing your organization to embrace hybrid work without compromising data security. Leverage Dizzion's PCI DSS, HIPAA HITECH, NIST 800-53, SOC 2 Type II, and GDPR compliant virtual desktops to make audits simpler and less costly.

DIZZION

As hybrid work shapes the future, Dizzion is here to make it your reality with confidence and security. Visit www.dizzion.com to learn more.

Direct Contact

Sales Inquiries:
888-225-2974 Opt. 1
sales@dizzion.com

Social

in