2021

Cybersecurity INSIDERS

BYOD SECURITY REPORT

bitglass

INTRODUCTION

The recent COVID-19 pandemic and resulting surge of employees working from home significantly increased security and privacy risks introduced by the use of personal mobile devices.

As mobility and remote work environments keep growing, so do challenges from managing device access to handling the most pressing concerns of mobile security.

The 2021 BYOD Security Report reveals these security challenges and offers fresh insights on the state of securing mobility, the technology choices organizations are making, and their response to the growing security risks associated with remote work and enterprise mobility.

Key findings include:

- Overall, a massive 82% of organizations actively enable BYOD to at least some extent. BYOD is typically associated with company employees bringing unmanaged devices into the workplace (70%), but also applies to other groups like contractors (26%), partners (21%), customers (18%), and suppliers (14%).
- The main barriers to BYOD adoption are the concern about information security (30%), employee privacy concerns (15%), and support cost concerns (9%). Regardless of the specific barrier, the fact is that organizations need to think differently (and deploy different kinds of solutions) when it comes to securing BYOD.
- At the top of the list of security concerns is data leakage or loss (62%). Other critical concerns include users downloading unsafe apps or content (54%), lost or stolen devices (53%), and unauthorized access to company data and systems (51%). There are countless ways that data can leak through BYOD, making the implementation of appropriate security measures critical.
- While 22% of organizations confirmed that unmanaged devices accessing corporate resources downloaded malware in the last 12 months, an alarming 49% were unsure or unable to disclose whether the same could be said of them. This lack of visibility can prove fatal.

We would like to thank Bitglass for supporting this important industry research. We hope you find this report informative and helpful as you continue your efforts in securing your organizations against evolving threats.

Thank you,

Holger Schulze

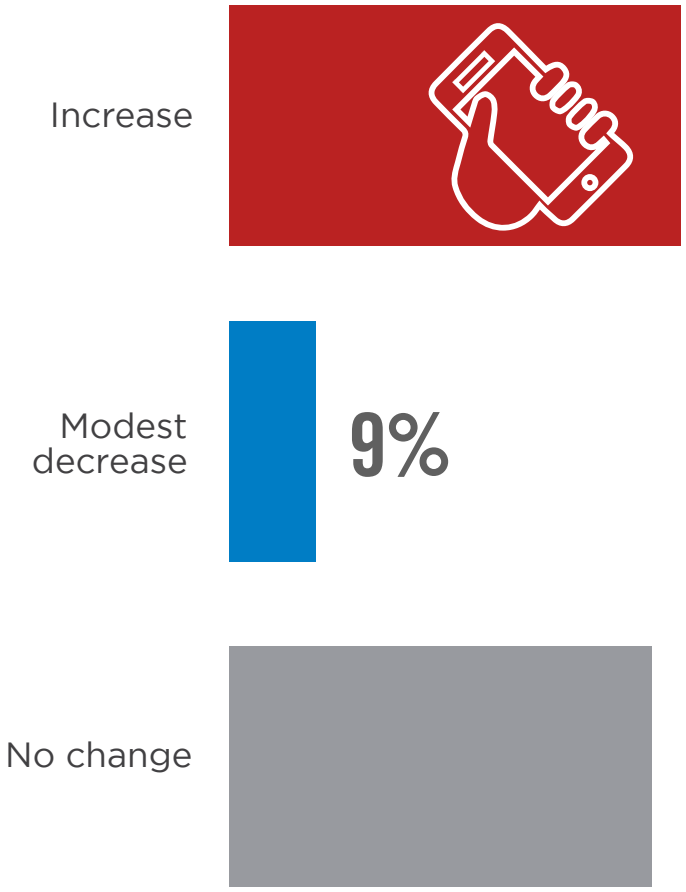
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

IMPACT OF REMOTE WORK

Because of the massive shift to remote work due to the recent COVID-19 pandemic, the number of BYOD has increased – almost half percent of organizations report an increase (47%). This trend will challenge the use of security measures designed for managed endpoints.

How has the shift to remote work affected the number of BYOD being used in your organization?



47%

Of organizations saw a significant increase of BYOD due to shift to remote work.

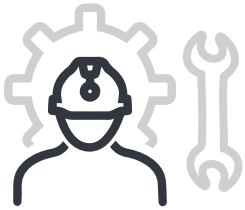
BYOD USER GROUPS

While BYOD is typically associated with company employees bringing unmanaged devices into the workplace (70%), the concept also applies to a variety of other groups affiliated with an organization. Respondents said their organizations also enable BYOD for extended workforce (such as contractors, partners and suppliers) (61%) and customers (18%). Overall, organizations actively enable BYOD to at least some extent.

What user group(s) does your organization enable BYOD for?

70%

Employees

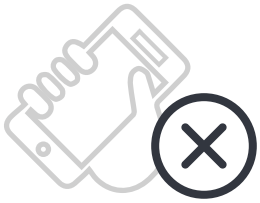


61%

Extended workforce

18%

Customers



18%

We don't enable BYOD

Other 5%

BENEFITS OF BYOD

Organizations realize a number of significant benefits from adopting BYOD for mobile and remote users, especially during the COVID-19 pandemic. The most common benefit mentioned in our survey is improved employee productivity (68%). Following that is greater employee satisfaction (53%) and reduced cost (45%). Clearly, there is much to gain by enabling unmanaged device access.

What are the main benefits of BYOD for your company?

68%

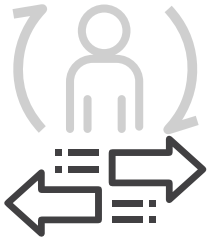
Improved employee productivity

53%

Greater employee satisfaction

45%

Reduced cost



7%

Improved employee mobility

Other 9%

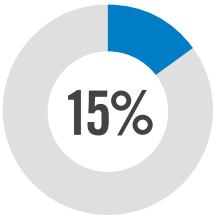
ADOPTION BARRIERS

What's keeping organizations from adopting BYOD at a faster rate? The main barrier is the concern about information security, cited by 30% of respondents. Somewhat less significant are employee privacy concerns (15%) and support cost concerns (9%). Regardless of the specific barrier, the fact is that organizations need to think differently (and deploy different kinds of solutions) when it comes to securing BYOD.

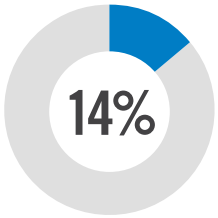
What do you believe is the number one inhibitor to BYOD adoption in your organization?

30%

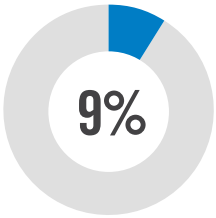
Company information security concerns



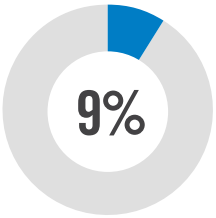
Employee privacy concerns (e.g., over EMM software)



We don't experience any resistance to BYOD adoption



Support cost concerns



We offer managed/ company owned devices as alternatives

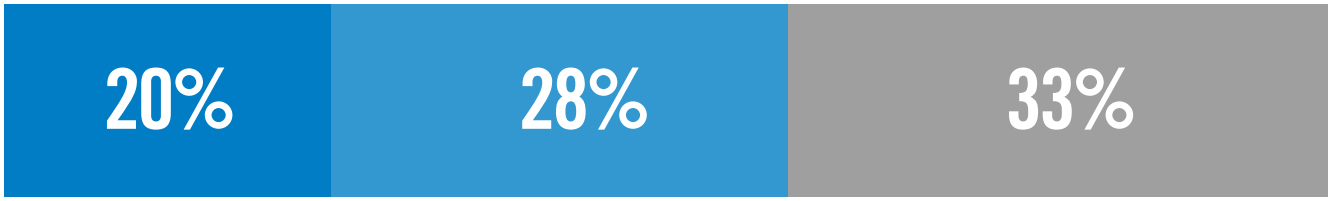
Employees don't want to take on the additional expense 7% | Management opposition 3% | User experience concerns (e.g., battery life, don't like app choices, etc.) 2% | Other 5%

BYOD PRIVACY AND ADOPTION

We asked survey participants how BYOD adoption might change if IT could not view or alter personal data and apps. About half (48%) expect BYOD adoption to increase.

How would BYOD adoption change if IT couldn't view or alter personal data and apps in your organization?

48% Expect BYOD adoption to increase



BYOD adoption would increase dramatically

BYOD adoption would increase somewhat

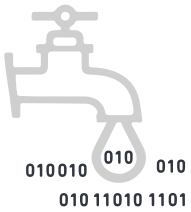
BYOD adoption would not change

Not sure 19%

SECURITY CONCERNS

Cybersecurity professionals continue to have a variety of security concerns regarding BYOD. At the top of the list is data leakage or loss (62%). Other critical concerns include users downloading unsafe apps or content (54%), lost or stolen devices (53%), and unauthorized access to company data and systems (51%). There are countless ways that data can leak through BYOD, making the implementation of appropriate security measures critical.

What are your main security concerns related to BYOD?



62%

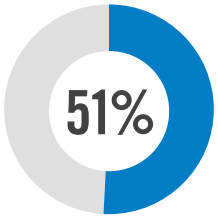
Data leakage/loss
(e.g., corporate data removal at employee separation or device disposal)

54%

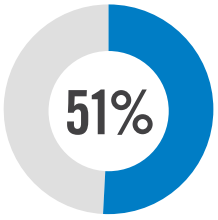
Users download unsafe apps or content

53%

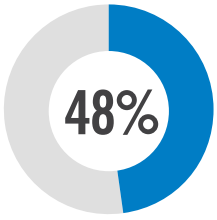
Lost or stolen devices



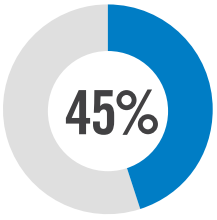
Unauthorized access to company data and systems



Malware



Vulnerability exploits



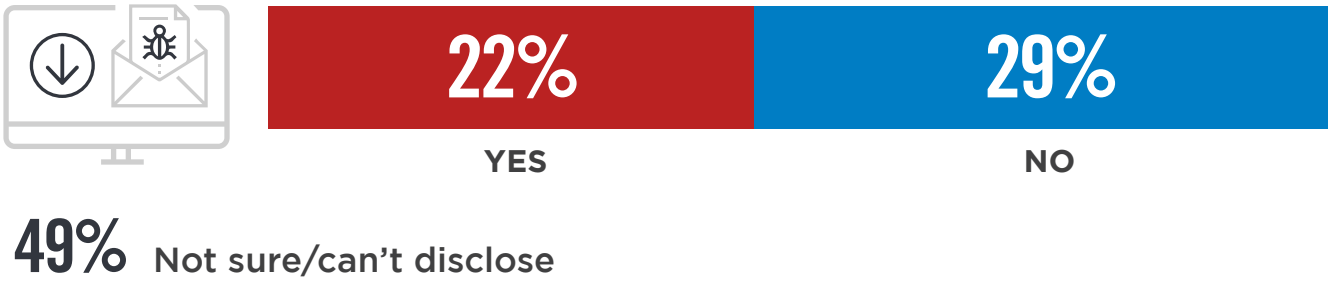
Inability to control endpoint security

Device management 43% | Ensuring that security software is up-to-date 38% | Compliance with regulations 35% | None 3% | Other 3%

MALWARE INCIDENTS

While 22% of organizations surveyed can confirm that unmanaged devices accessing corporate resources have been used to download malware in the last 12 months, an alarming 49% were unsure or unable to disclose whether the same could be said of them. This lack of visibility can prove fatal.

Have any of your BYOD downloaded malware in the past 12 months?



49% Not sure/can't disclose

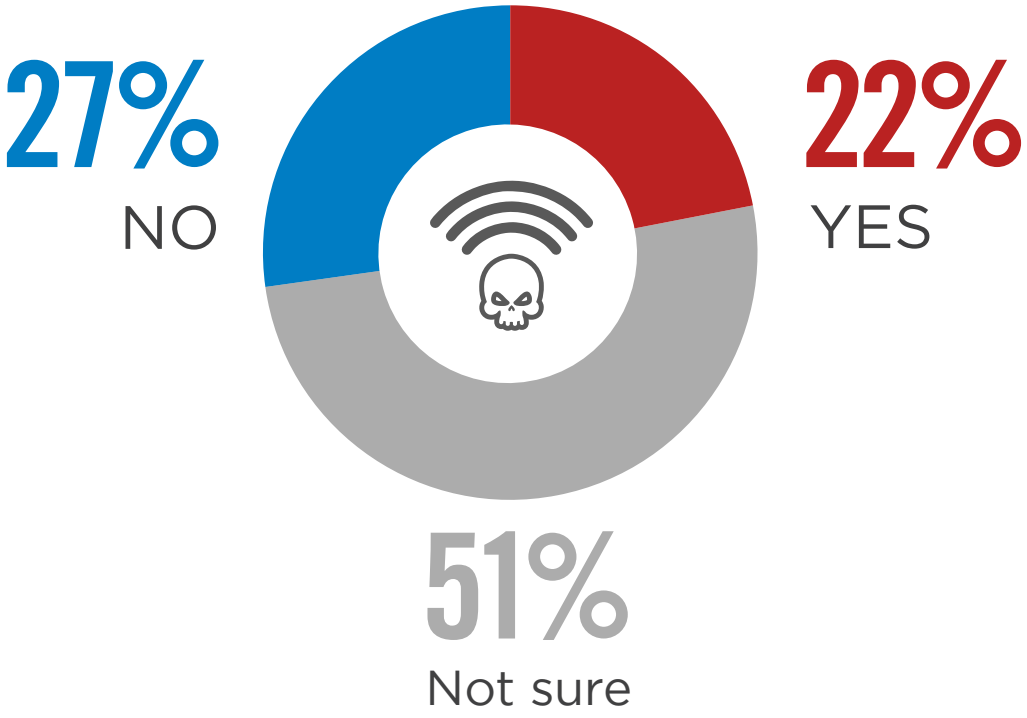
41% of organizations rely on endpoint malware protection for BYOD — an approach that is not ideal for personal devices which are hard to control and manage. Cloud-based malware protection tools are often a far better fit but are used far less often (11%). Unfortunately, 30% of firms don't protect against malware for BYOD at all.

Which of the following do you use for malware protection on BYOD?

MALICIOUS WIFI ACCESS

22% of organizations confirm their employee-owned devices have connected to malicious WiFi networks in the past 12 months. Equally alarming is the fact that more than half of organizations have no way of knowing their vulnerability to malicious WiFi (51%) on personal devices.

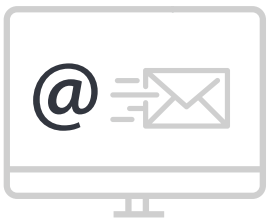
Have any of your BYOD connected to a malicious WiFi in the past 12 months?



APP VISIBILITY

Many organizations lack visibility into applications on BYOD. Device apps that organizations have the most visibility into include email (74%), followed by calendar (58%), contacts (55%), and messaging (51%). Lacking this fundamental level of visibility across these basic applications does not bode well for enterprise BYOD security.

Which of the following applications do you have visibility into on BYOD?



74%

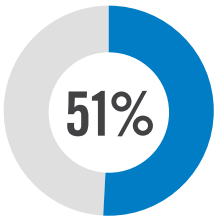
Email

58%

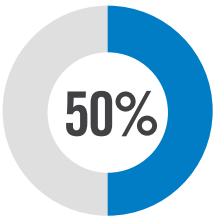
Calendar

55%

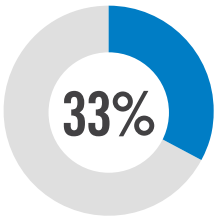
Contacts



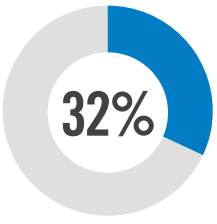
Messaging



File sharing



Cloud backup



Document editing

Virtual desktop 24% | Other 11%

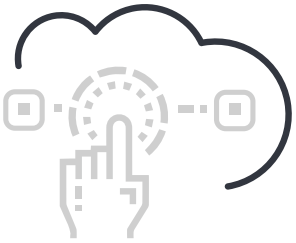
MESSAGING SECURITY

The most commonly deployed security capabilities for mobile enterprise messaging include control over shared files (44%), control over connected cloud apps (38%), and visibility over messages shared in private channels (29%). An alarming third of organizations (29%) report having no visibility or control over mobile enterprise messaging. As these applications can be used to share sensitive information and files, organizations must ensure they have all of the necessary capabilities to secure messaging.

What security capabilities do you have in place for mobile enterprise messaging?

44%

Control over shared files



38%

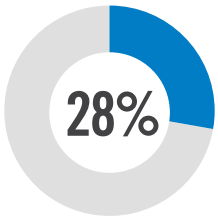
Control over connected cloud apps

29%

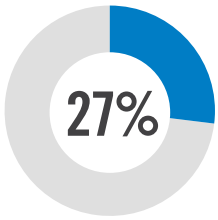
Visibility over messages shared in private channels

29%

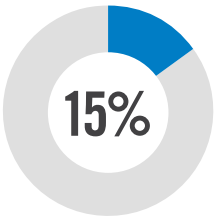
No visibility or control



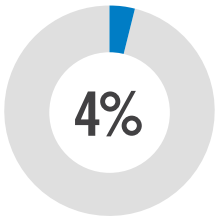
Visibility over messages shared in public channels



Control over external collaborator permissions



Detecting malware



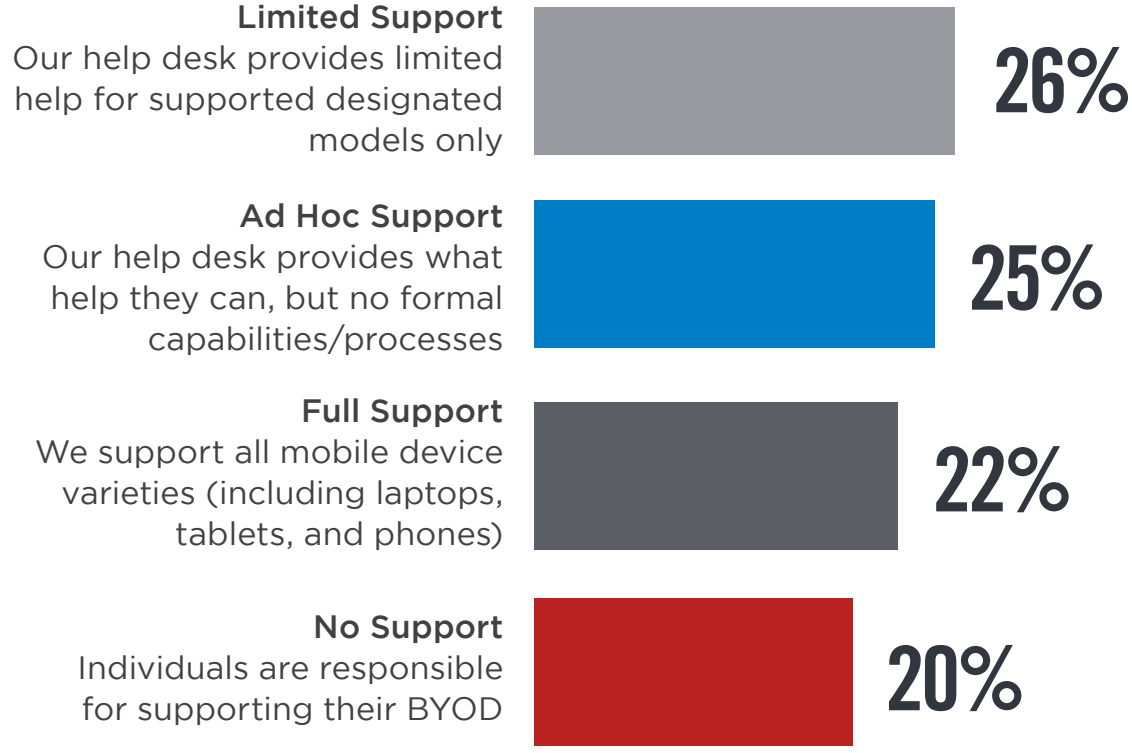
Control over messages shared in private channels

Detecting sensitive data patterns via DLP 4% | Control over messages shared in public channels 3% | Other 5%

BYOD SUPPORT

The different support levels for BYOD are fairly evenly distributed. A quarter of organizations provide limited help for supported designated models only (26%). Another quarter provide ad hoc support but without formal capabilities and processes (25%). Less than a quarter (22%) provide full support of all mobile device varieties (including laptops, tablets, and phones). An alarming 20% provide no dedicated BYOD user support whatsoever, meaning individuals have to troubleshoot any unmanaged device issues that may occur in the course of their work, slowing productivity.

How do you currently support BYOD users experiencing device/access issues?

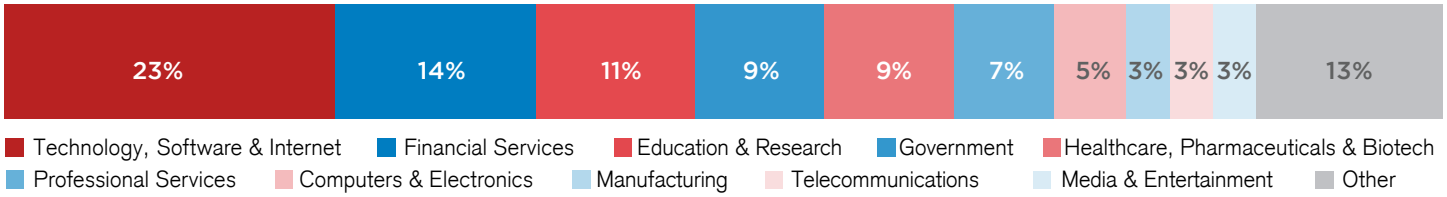


Other 7%

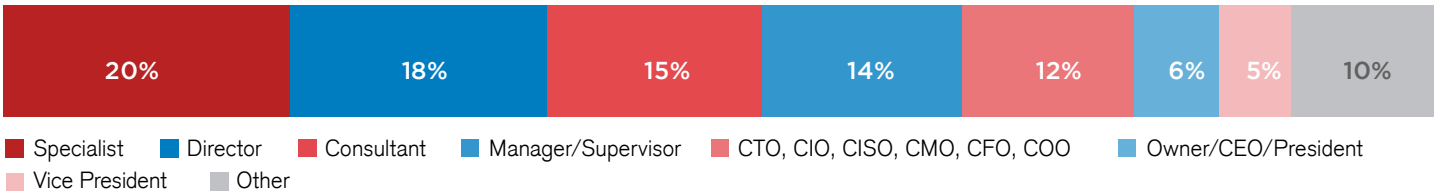
METHODOLOGY & DEMOGRAPHICS

The 2021 BYOD Security Report is based on the results of a comprehensive online survey of 271 cybersecurity professionals, conducted in April 2021, to gain deep insight into mobile BYOD security threats faced by organizations and the solutions to prevent and remediate them. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

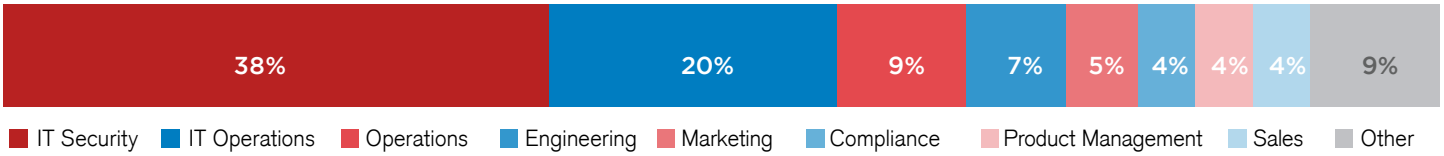
INDUSTRY



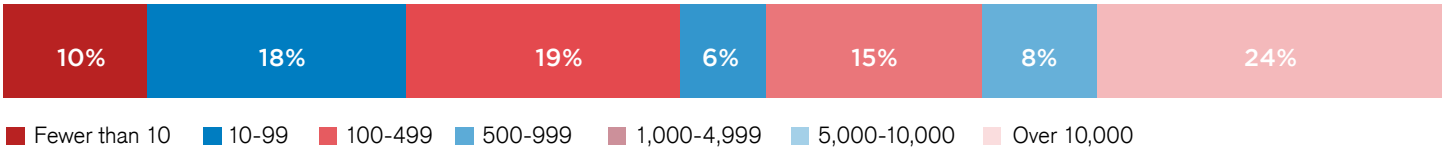
CAREER LEVEL



DEPARTMENT



COMPANY SIZE



Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.

www.bitglass.com