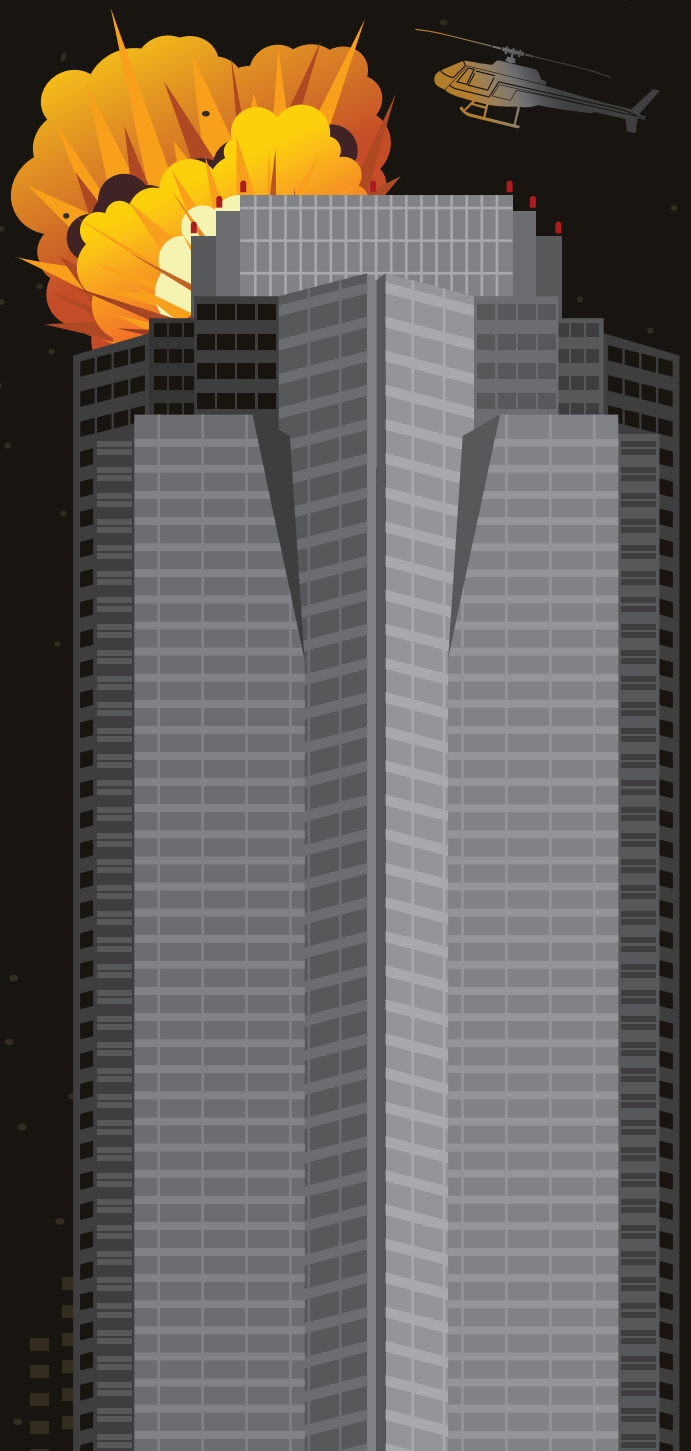
CLOUD HARD 2018

SECURITY WITH A VENGEANCE



bitglass

Enterprises around the globe are migrating to cloud at an astounding rate—trading in their on-premises productivity and messaging tools for more cost effective cloud platforms that enable collaboration and mobility. While application teams are eager to make the switch, security teams are often hesitant given the new risks posed by these platforms.

In partnership with the Information Security Community, Bitglass surveyed over 570 cybersecurity and IT professionals to learn how organizations are approaching cloud security. Read on to learn about the state of traditional tools, security measures IT leaders are taking, and cloud priorities for 2018.

TRADITIONAL TOOLS

The cloud security market is growing in large part because traditional security infrastructure has failed. Where next-gen firewalls and built-in capabilities are insufficient for regulatory compliance, internal compliance, and cloud data protection, dedicated cloud security becomes critical.

84% say traditional security solutions don't work or have limited functionality in the cloud.

Asked about top drivers for considering cloud security, **47%** indicated these solutions offer faster time to deployment and cost savings as compared to traditional solutions.

ENTERPRISES FLYING BLIND

IT departments in many major organizations are operating without visibility into cloud app activity.

While **78%** have visibility into user logins, only **58%** have visibility into file downloads and **56%** into file uploads.

Less than half (**44%**) have visibility into external sharing and DLP policy violations.

Only **15%** can see anomalous behavior across apps.

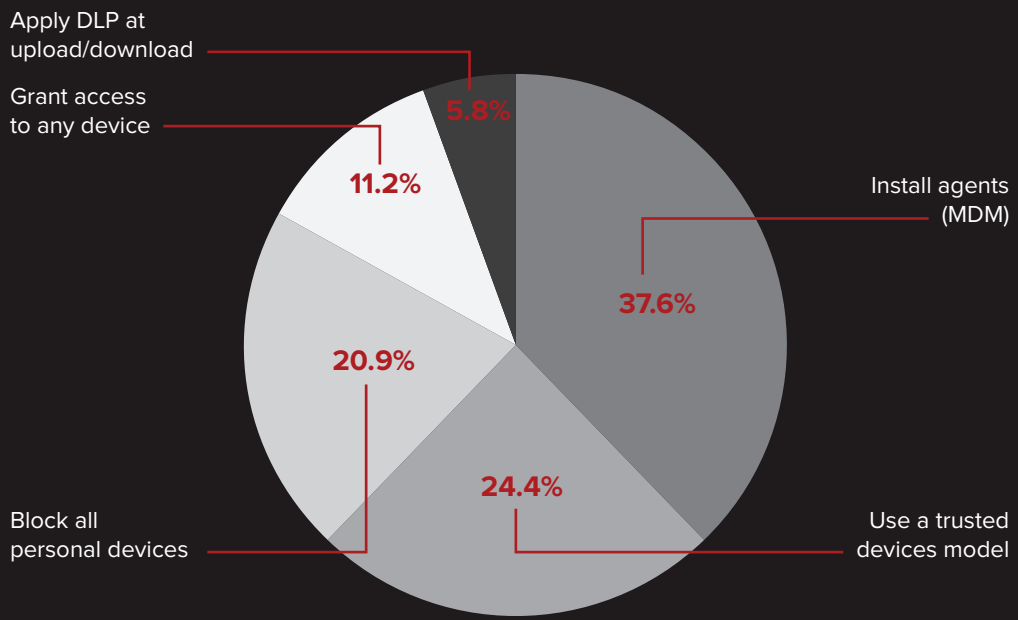
RELYING ON THE INEFFECTIVE

Despite ineffectiveness of traditional security solutions, many still have major gaps in their cloud security infrastructure. Mobile, for example, is a core component of cloud access yet few have the proper controls for BYO mobile security.

69% of organizations rely solely on endpoint solutions for malware protection, tools which cannot detect or block malware at rest in the cloud or employees' BYO devices.

To protect mobile data, **38%** of organizations install agents and **24%** use a trusted device model, where only provisioned corporate-owned devices are allowed access to company systems.

11% have no mobile access control solution in place, granting access to any smartphone or tablet.



TOP PRIORITIES AND THREATS FORESEEN

Asked about the top IT priorities for 2018, most selected ‘Securing Cloud Apps Already in Use’ as the number one or number two priority, indicating that these existing managed and unmanaged apps pose the greatest risk to cloud data. Many also selected regulatory compliance. The top priorities as selected by respondents are:

PRIORITIES

No. 1 Securing cloud apps already in use

No. 2 Regulatory compliance

No. 3 Defending against cloud malware

No. 4 Discovering unmanaged cloud apps

No. 5 Securing mobile

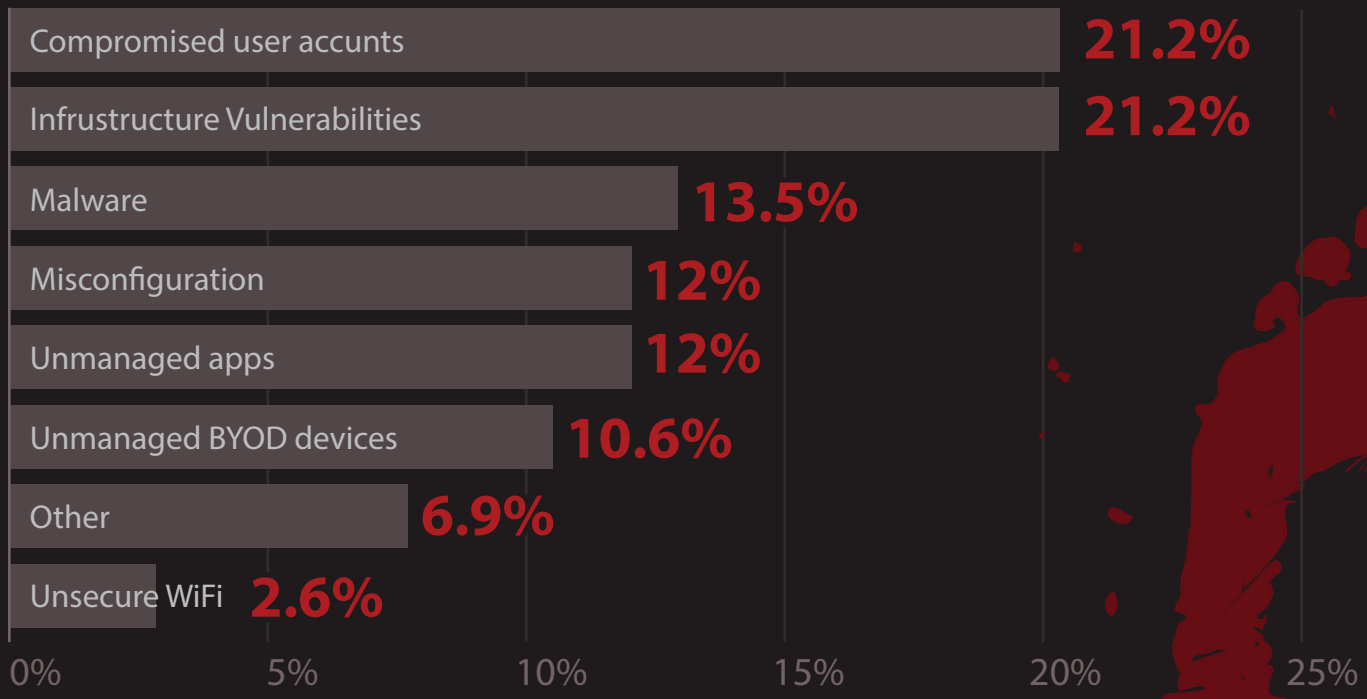
No. 6 Preventing AWS misconfigurations

FUTURE OF DATA PROTECTION

Asked about data protection in the cloud, 65% use access controls, more than any other security tool, indicating growing adoption of data protection solutions like CASBs. 59% use encryption or tokenization.

Solutions said to help build confidence in cloud security are encryption (49%), visibility and audit capabilities (46%), and setting/enforcing policies across cloud apps (45%).

The most concerning data leakage vectors were compromised accounts (21%), followed by vulnerabilities in app infrastructure, (21%), malware (14%) and unsanctioned cloud apps (12%).



WRAP-UP

Continued demand for certain capabilities is driving growth in cloud security. Organizations need solutions that address very real concerns around data outflows to unmanaged apps, misconfiguration, and risk of credential compromise. As a result, thousands of organizations are in the process of identifying and evaluating different approaches to data protection.

While point solutions for identity, device management, and data loss prevention are all readily available, they can be costly and fail to provide a single point of control and visibility for cloud data. Instead of this disjointed approach, organizations need comprehensive, fully integrated security platforms.

bitglass

Phone: (408) 337-0190
Email: info@bitglass.com

www.bitglass.com

ABOUT BITGLASS

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.