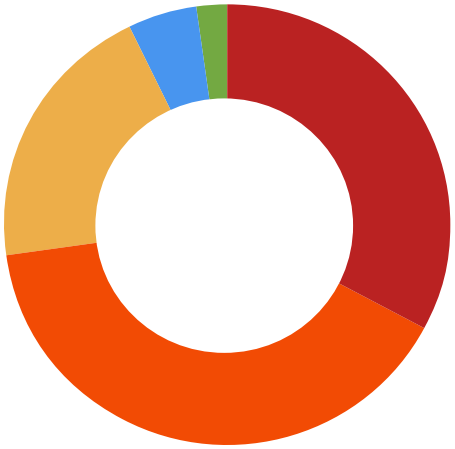

bitglass
2020
Cloud
Security
Report

Enterprise use of cloud-based resources has been on the rise for years. However, the global pandemic has forced organizations around the world to shift to a remote style of work and, consequently, embrace the cloud more than ever before. This rapid change creates questions about the state of enterprise security, and whether organizations are properly equipped to defend themselves in the cloud. To answer these questions, Bitglass partnered with a leading cybersecurity community and surveyed IT and security professionals about cloud security in their organizations.

The Security of the Cloud

93% of those surveyed were moderately to extremely concerned about the security of the public cloud. Interestingly, 73% of respondents said that cloud applications were as secure or more secure than on-premises apps. This apparent contradiction shows that organizations recognize the public cloud as inherently safe, but are struggling with their responsibility to use it securely.

How concerned are you about the security of the public cloud?



- **33%** – Extremely
- **40%** – Very
- **20%** – Moderately
- **5%** – Slightly
- **2%** – Not at all

Are public cloud apps / SaaS more or less secure than on-premises applications?

- **45%** – About the same
- **28%** – Cloud apps are more secure than on-prem apps
- **27%** – Cloud apps are less secure than on-prem apps

Cloud-Based Architectures

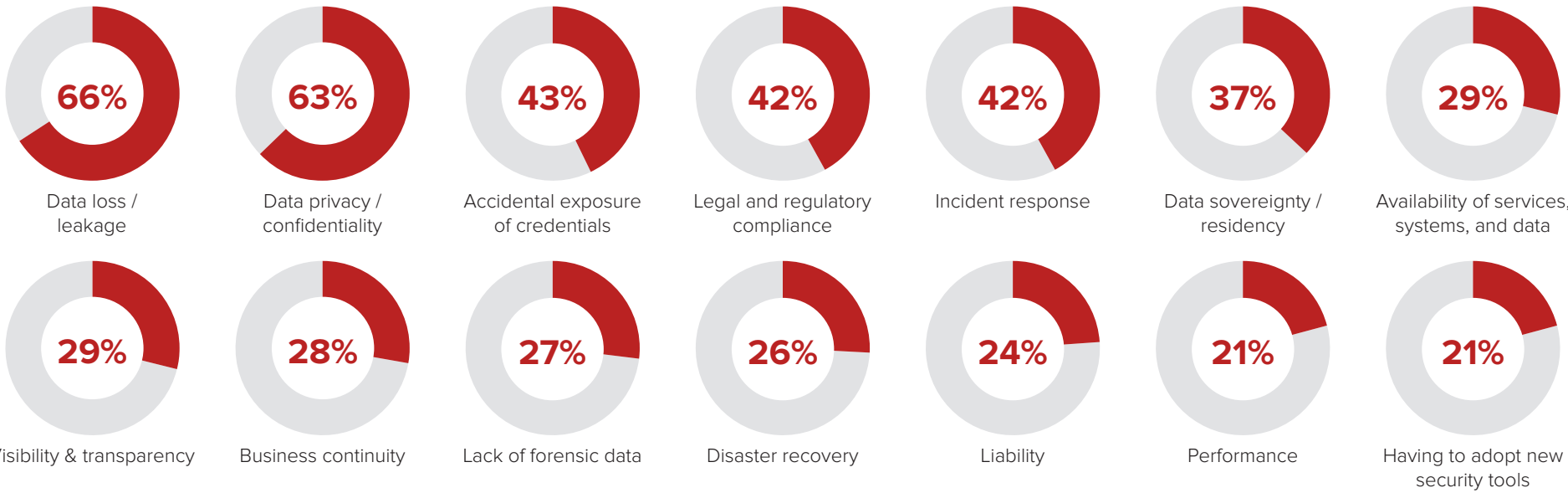
Network security tools and appliances provide limited to totally ineffective security in the cloud (as recognized by 82% of survey respondents). Consequently, modern organizations need specialized, independent cloud security that departs from these legacy approaches. Platforms architected in the public cloud have multiple advantages over those that are deployed via appliances in vendors' private networks or data centers.

94% of respondents identified architecture as something that moderately to extremely affects performance, scalability, and uptime. Without these three items, security suffers and business continuity is disrupted.

Cloud Security Concerns

Cited by 66% of survey respondents, data leakage was the leading cloud security concern. In many ways, data leakage is the threat that underpins and breeds the other concerns shown in the chart here. For example, data flowing to undesirable locations can violate data subject privacy and lead to regulatory noncompliance, while concerns about compromised credentials are typically rooted in a fear of unauthorized access to corporate systems and, consequently, data. Arguably, concerns like business continuity (28%) and performance (21%) should have been selected far more frequently. If a security solution is unable to perform consistently, data protection will be limited and enterprise operations can be ground to a halt.

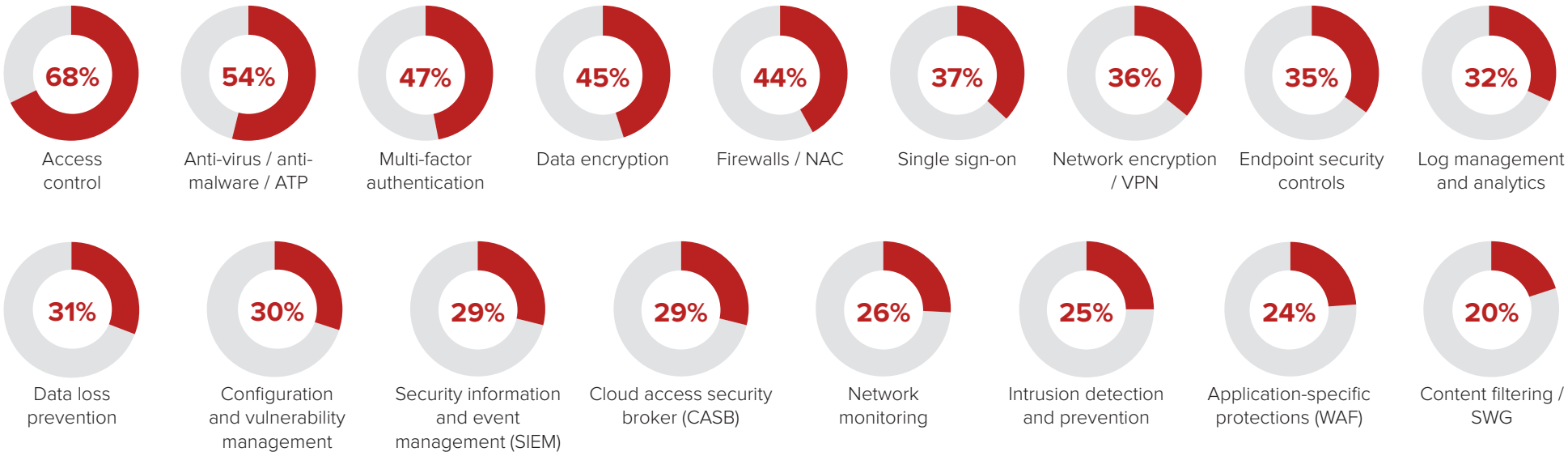
What are your biggest cloud security concerns?



Cloud Security Capabilities in Use

The deployment of data loss prevention (31%) is surprisingly low given the fact that data leakage was the leading cloud security concern, as mentioned on the preceding page. Additionally, single sign-on (37%) and multi-factor authentication (47%) are basic requirements for proper authentication in the cloud and, by extension, intelligent, granular security. Consequently, they, along with cloud access security brokers (29%), are examples of underutilized but critically important technologies. Unfortunately, it seems that some organizations still try to use inappropriate tools like firewalls (44%), network encryption (36%), and network monitoring (26%) to secure the use of the cloud. Rather than relying upon on-premises tools or limited native controls built into cloud resources like SaaS apps, organizations must utilize specialized security capabilities designed for the cloud.

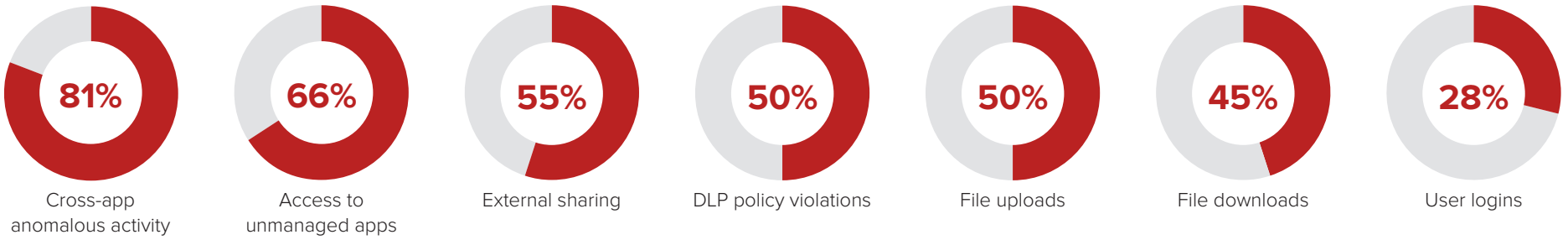
What security capabilities have you deployed in the cloud?



Visibility in the Cloud

Maintaining visibility over corporate data and user activity is a core requirement for ensuring proper cybersecurity. Unfortunately, many organizations lack the ability to track and log key activities in the cloud. Specifically, roughly half of respondents are unable to maintain visibility into file downloads (45%), file uploads (50%), DLP policy violations (50%), and external sharing (55%) in the cloud. This does not bode well for the average enterprise's cloud security posture. Additionally, 81% of companies cannot identify cross-application anomalous activity, something which will continue to grow in importance as organizations increasingly expand their cloud footprints.

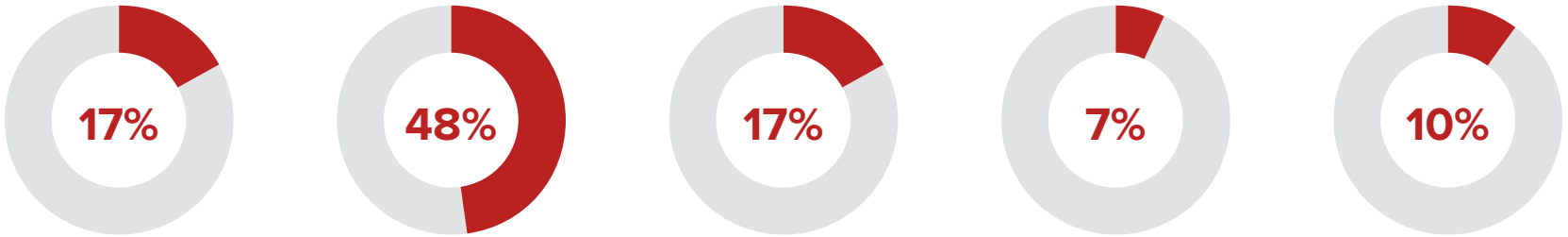
For which of the following cloud activities do you lack visibility?



Consolidated Ease of Use

As organizations deploy growing numbers of cloud-based resources, managing their security becomes a challenge. Native security controls vary in functionality, must be configured separately, and are enforced only on individual apps and resources. Unfortunately, some independent security solutions are also limited in terms of where they can apply policies. In either case, IT is tasked with managing disjointed dashboards that provide disparate levels of protection across the enterprise cloud footprint. This is a time-consuming endeavor. Consequently, 79% of organizations believe it would be moderately to extremely helpful to have a single security platform with a single dashboard for configuring policies that deliver consistent, comprehensive protections across the enterprise cloud footprint.

How many separate solution dashboards do your admins have to access to configure the policies that secure your cloud footprint?

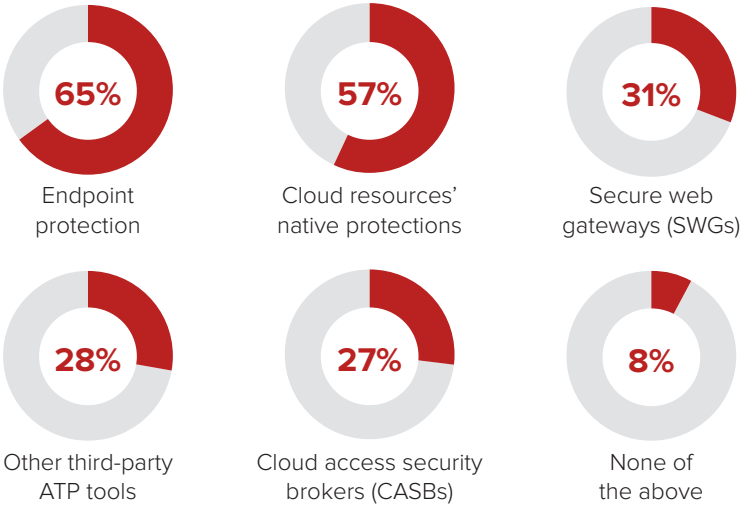


Defenses to Be Updated

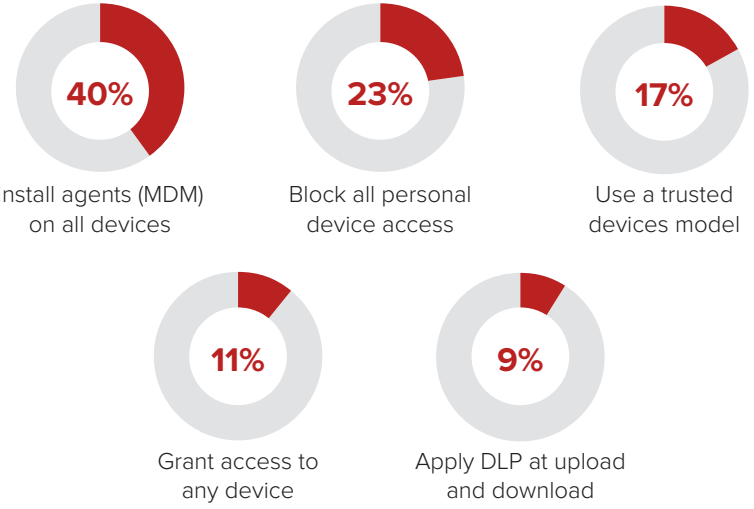
For a variety of reasons, organizations often use outdated or ill-suited tools to secure cloud environments. For example, most survey respondents rely upon endpoint protection (65%) or native threat protection built into cloud resources (57%) in order to defend against malware in the cloud. However, endpoint antivirus tools are not designed for the cloud and are poor fits for personal devices, while most cloud resources lack native malware protection entirely. Instead, organizations should turn to cloud access security brokers and other specialized, third-party technologies in order to defend against malware in the cloud.

In a similar fashion, organizations are relying upon poorly suited tools and strategies to secure cloud data on employees' personal devices. The top two approaches are to use agent-based tools like MDM (40%), or to block all personal device access (23%). MDM is not designed for personal devices and invades user privacy when deployed on such endpoints, while blocking personal devices altogether impedes organizational productivity and dynamism. Instead, organizations should safely enable BYOD with agentless security solutions and data loss prevention capabilities.

What anti-malware tools does your organization currently use to secure cloud data?



What does your organization do to secure cloud data on employees' personal devices?



Wrap-Up

The rises of cloud computing, bring your own device, and remote work have forever shifted the cybersecurity needs of organizations around the globe. Today, security personnel are tasked with securing more environments and defending against more threats than ever before. Unfortunately, this report has revealed that there is still much work to be done.

To better address their modern security needs, organizations should leverage multi-faceted security platforms that are capable of providing comprehensive and consistent security for any interaction between any device, app, web destination, on-prem resource, or infrastructure. This also ensures consolidated ease of management and saves time for administrators. Ideally, such a platform will be deployed in the public cloud in order to maximize performance, scalability, and uptime, eliminate the need for hardware appliances, and save organizations money.

These platforms should provide:

- Identity management capabilities like single sign-on and multi-factor authentication that can verify users' identities wherever they go
- Data loss prevention functionality designed to prevent leakage across the cloud, the web, and on premises
- Advanced threat protection that leverages behavior-based protections to scan for threats at upload, at download, and at rest
- An agentless option for securing personal devices that respects end-user privacy while enforcing granular, intelligent protections

If you want to test a platform that meets all of the above requirements and more, request a **free trial of Bitglass** today.

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.